UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

Manual sobre los delitos relacionados con la identidad

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO
Viena

Manual sobre los delitos relacionados con la identidad

NACIONES UNIDAS
Nueva York, 2013

La presente publicación no ha sido revisada a fondo por los servicios de edición.

Producción de la publicación: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas en Viena.

Prólogo

El presente Manual fue elaborado tras la publicación del estudio de las Naciones Unidas sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos en 2007, encargado por la UNODC y presentado a la Comisión de Prevención del Delito y Justicia Penal en su 16º período de sesiones (E/CN.15/2007/8 y Add.1 a 3), de conformidad con la resolución 2004/26 del Consejo Económico y Social. El estudio aportó una contribución doble. En primer lugar, adoptó un enfoque amplio del concepto de "delito relacionado con la identidad" y lo concibió de manera que abarcara todas las conductas ilícitas relativas a la identidad, incluidos los delitos frecuentemente denominados "fraude de identidad" y "hurto de identidad". En segundo lugar, abordó los problemas planteados por el delito relacionado con la identidad desde una perspectiva nueva de derecho penal, así como el uso indebido de la identidad como una forma particular del delito, por oposición al criterio tradicional de tipificar otros actos delictivos cometidos con identidades falsas. El estudio también abordó las diferencias y las contradicciones en los conceptos y las definiciones, en los distintos contextos nacionales, relativos al fraude y la falsificación de la identidad y su uso indebido con fines delictivos, y esclareció varios aspectos que revelan el carácter multifacético y complejo del problema.

El Manual se basa en los resultados y recomendaciones del estudio mencionado y se focaliza en determinadas cuestiones jurídicas y políticas relativas al delito de identidad. Su principal objetivo es exponer diversas opciones y consideraciones que han de tenerse en cuenta al abordar cuestiones relacionadas con la justicia penal en el plano nacional (como la tipología de los delitos, los diferentes criterios para su tipificación y la protección de las víctimas), los problemas concretos de la cooperación internacional en materia penal y la posibilidad de crear sinergias y alianzas entre los sectores público y privado, sobre todo en la esfera de la prevención de los delitos relacionados con la identidad. Los documentos de investigación junto con el material práctico contribuyen a esclarecer los diferentes aspectos y parámetros de los complejos problemas que plantea esta forma de delincuencia.

Dada la variedad de los temas abarcados, el Manual está destinado a los legisladores, los responsables de formular políticas, los fiscales, las autoridades encargadas de hacer cumplir la ley, los profesionales de servicios pertinentes, así como otros interesados (representantes de las organizaciones internacionales e intergubernamentales competentes, del sector privado y los círculos académicos).

El Manual también puede servir de referencia en los programas de asistencia técnica y las actividades de fomento de la capacidad encaminadas a ampliar los conocimientos especializados para abordar las cuestiones de carácter jurídico, institucional y operacional relacionadas con los delitos de identidad como nueva forma de delincuencia, en consonancia con las orientaciones contenidas en las Declaraciones de Bangkok y de Salvador y con los resultados del 11º y 12º Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.

Además, como instrumento de asistencia técnica, el Manual representa un primer esfuerzo con miras a la aplicación de los mandatos correspondientes a las resoluciones 2004/26, 2007/20 y 2009/22 del ECOSOC, en las que se pide: *a)* que se utilice la información obtenida en el estudio de las Naciones Unidas mencionado *supra* con objeto de elaborar prácticas, directrices y otro material útil para la prevención e investigación de la falsificación de identidad y su uso indebido con fines delictivos; y *b)* que se reúna, elabore y difunda material de asistencia técnica sobre el delito relacionado con la identidad, más concreto y basado en temas específicos, incluidos los manuales y la compilación de directrices o prácticas útiles.

Por último, el presente Manual se benefició de las conclusiones, las directrices y las recomendaciones resultantes de las reuniones del Grupo básico de expertos sobre delitos relacionados con la identidad, establecido por la UNODC en 2007, abierto a múltiples interesados, a fin de reunir a los representantes de los Estados Miembros y las organizaciones internacionales, así como a los representantes del sector privado y expertos académicos. El establecimiento de un grupo básico resultó ser una iniciativa positiva encaminada a facilitar el intercambio de opiniones, información y conocimientos especializados entre los distintos participantes con objeto de orientar lo mejor posible la acción estratégica, política y jurídica, para combatir los delitos relacionados con la identidad y promover el entendimiento recíproco y la cooperación con ese fin.

Agradecimientos

El presente Manual es el resultado de un proyecto de la Subdivisión de Lucha contra la Corrupción y los Delitos Económicos de la UNODC, de conformidad con lo dispuesto en las resoluciones 2007/20 y 2009/22 del Consejo Económico y Social sobre "Cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad", y en consonancia con su programa temático titulado "Medidas contra la corrupción y los delitos económicos" (2010-2011).

La elaboración del Manual forma parte de la labor de la UNODC que consiste en crear nuevos instrumentos para ayudar a los Estados Miembros a fortalecer sus capacidades jurídicas, institucionales y operacionales con miras a combatir a nivel nacional el fraude económico y los delitos relativos a la identidad, en el marco de una cooperación internacional eficaz.

La UNODC desea expresar su reconocimiento a los siguientes expertos que aportaron una contribución sustantiva al Manual:

- Sr. Marco Gercke, Profesor de derecho, especializado en delito cibernético, Universidad de Colonia (Alemania);
- Sr. Gilberto Martins de Almeida, Martins de Almeida Advogados, Río de Janeiro (Brasil);
- Sra. Philippa Lawson, Asociada, Centro Internacional de Reforma del Derecho Penal y de Política de la Justicia Penal (Canadá);
- Sra. Raluca Simion, Asesora Jurídica, Dirección de Derecho Internacional y Cooperación Judicial, Ministerio de Justicia (Rumania); y
- Sr. Cormac Callanan, Director General, Aconite Internet Solutions Limited.

La UNODC también agradece especialmente la colaboración de todas las personas que participaron en este proyecto con comentarios y observaciones, y en particular a los miembros del Grupo básico de expertos sobre delitos relacionados con la identidad, establecido en 2007 por la UNODC para reunir conocimientos y experiencia de numerosas partes interesadas, formular estrategias, promover nuevas investigaciones y acordar medidas prácticas de lucha contra los delitos relacionados con la identidad.

La UNODC se vale de esta oportunidad para expresar su agradecimiento al Gobierno del Canadá por su apoyo financiero a la elaboración del Manual.

El Sr. Demosthenes Chryssikos, Funcionario de prevención del delito y justicia penal, Subdivisión de Lucha contra la Corrupción y los Delitos Económicos, se encargó de la recopilación y adaptación del material de este Manual.

Merece un especial reconocimiento la Sra. Dildora Djuraeva, consultora, por su importante contribución a este proyecto.

Índice

ENFOQUES JURÍDICOS PARA TIPIFICAR EL DELITO DE HURTO DE IDENTIDAD*

Marco Gercke
Profesor de derecho, especializado en delito cibernético
Universidad de Colonia, Alemania

* El presente estudio fue preparado como documento de trabajo de la tercera reunión del Grupo básico de expertos sobre delitos relacionados con la identidad, celebrada en Viena (Austria), del 20 al 22 de enero de 2009. También fue presentado como documento de sesión a la Comisión de Prevención del Delito y Justicia Penal en su 18º reunión, celebrada en Viena, del 16 al 24 de abril de 2009 (E/CN.15/2009/CRP.13). Las opiniones expresadas en este documento pertenecen al autor y no reflejan los puntos de vista de las Naciones Unidas.

Índice

I. ALCANCE DEL ESTUDIO

1. Perfil del análisis

El estudio se centra en tres aspectos fundamentales de la respuesta jurídica relativa al hurto de identidad. Tal como se explica más adelante, la expresión "hurto de identidad" se emplea para describir una esfera de delitos bastante heterogénea[1]. Debido tanto a su alcance como a sus consecuencias, elaborar una respuesta apropiada a dicha amenaza es al mismo tiempo un desafío y una necesidad. El propósito del presente estudio no es proporcionar una estrategia completa para abordar el problema del hurto de identidad, sino centrarse en una parte de dicha estrategia: la respuesta jurídica basada en el derecho penal.

2. Aspectos no abarcados en el estudio

Si bien en el estudio no se abordan varios otros elementos de la estrategia amplia contra el hurto de identidad, se mencionan brevemente a continuación.

Medidas preventivas

Se han adoptado diferentes medidas técnicas y jurídicas para prevenir el hurto de identidad. Abarcan desde la restricción de publicar información crucial relacionada con la

[1] Véase, *infra*, el capítulo 4.

identidad[2], los requisitos en materia de notificación de las violaciones de datos personales[3], hasta una mejor protección de las grandes bases de datos[4].

Aplicación de medidas de seguridad

La aplicación de medidas de seguridad adicionales, tales como el número de identificación personal (NIP), o la información biométrica[5] puede contribuir a prevenir el uso abusivo de información personal de identidad que se intercambia más frecuentemente[6].

Soluciones de gestión de la identidad

Las medidas técnicas relativas a la gestión de la información relativa a la identidad, así como las estrategias destinadas a reducir lo más posible el alcance de dicha información que es necesaria para realizar transacciones comerciales electrónicas, pueden influir sobre el riesgo de hurto de identidad[7].

---

[2] Véase en este contexto, Social Security Numbers, More could be done to protect SSNs, Statement of *C. M. Fagnoni*, Managing Director Education. Workforce and Income Security, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, 2006, GAO, Documento de la Oficina General de Contabilidad: GAO-06-586T, página 10 y ss.

[3] Requisitos de notificación que obligan a los organismos e instituciones en que se produce una violación de datos personales a informar a las personas cuya información personal ha sido afectada por el incidente. Con respecto al Data Breach Notification Regime, véase: *Stevens*, Federal Information Security and Data Breach Notification Laws, 3 de abril de 2008, CRS Report for Congress, Document RL34120; *Faulkner*, Hacking Into Data Breach Notification Laws, *Florida Law Review*, vol. 59, 2007, página 1097 y ss.; *Turner*, Towards a Rational Personal Data Breach Notification Regime, Information Policy Institute, junio de 2006; Recommendations for Identity Theft Related Data Breach Notification, Identity Theft Task Force, 19 de septiembre de 2006, disponible en: http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf (última consulta: octubre de 2008); Privacy, Lessons Learned about Data Breach Notification, Report to Congressional Requesters, 2007, Documento de la Oficina General de Contabilidad: GAO-07-657; Social Security Numbers, More could be done to protect SSNs, *supra* núm. 2, página 12 y ss. Con respecto al debate sobre las consecuencias de notificar las violaciones de datos personales para la prevención del hurto de identidad, véase: *Romanosky/Relang/Acquisti*, Do Data Breach Disclosure Laws Reduce Identity Theft?, Seventh Workshop on the Economics of Information Security, Center for Digital Strategies, Tuck School of Business, disponible en: http://weis2008.econinfosec.org/papers/Romanosky.pdf (última consulta: octubre de 2008); Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited. However, the full extend is unknown; Report to Congressional Requesters, 2007, Documento de la Oficina General de Contabilidad: GAO-07-737, página 32 y ss.

[4] Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of *G. C. Wilshusen*, Director, Information Security Issues, 2007, Documento de la Oficina General de Contabilidad: GAO-07_935T, página 17.

[5] Véase The Use of Technology to Combat Identity Theft, Report on the Study Conducted Pursuant to Section 157 on the Fair and Accurate Credit Transaction Act of 2003, 2005, disponible en: https://www.treasury.gov/offices/domestic-finance/financial-institution/cip/biometrics_study.pdf (última consulta: octubre de 2008).

[6] Véase, *White/Fisher*, Assessing Our Knowledge of Identity Theft: The Challenge of Effective Prevention and Control Efforts, *Criminal Justice Policy Review 2008*, vol. 19, 2008, página 16 y ss. con más referencias.

[7] Respecto de las estrategias de gestión de la identidad véase, *Sury*, Identity-Management und Recht, *Informatik-Spektrum*, vol. 27, No. 3, 2004, página 287 y ss.

Seguimiento de la conducta del usuario

La aplicación de soluciones técnicas para el seguimiento y el análisis de las transacciones relacionadas con la identidad puede ayudar a identificar actividades sospechosas[8].

Mejora de las investigaciones

Se puede progresar más mejorando las técnicas de investigación, por ejemplo, interrogando a los sospechosos de hurto de identidad[9].

Cooperación internacional

Con frecuencia el hurto de identidad tiene una dimensión transnacional[10]. Esto sucede especialmente en las estafas realizadas a través de Internet[11]. En los casos que tienen una dimensión transnacional, la capacidad de los organismos nacionales encargados de hacer aplicar la ley es limitada debido al principio de soberanía nacional. Este principio fundamental de derecho internacional restringe la autorización de llevar a cabo investigaciones en territorios extranjeros[12]. Por consiguiente, las investigaciones internacionales requieren la cooperación de los organismos encargados de velar por el cumplimiento de la ley sobre la base de marcos jurídicos para la cooperación internacional[13]. Mejorar la cooperación puede aumentar significativamente la capacidad de ubicar y procesar a infractores involucrados en delitos transnacionales.

---

[8] Sobre los sistemas automáticos de detección para la prevención del fraude, véase Money Laundering, Extend of Money Laundering through Credit Card is Unknown, Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, US Senate, 2002, Documento de la Oficina General de Contabilidad: GAO-02-670; sobre el seguimiento del uso de la identidad, véase, *Mashima*/*Ahamad*, Towards a User-Centric Identity-Usage Monitoring System, in Internet Monitoring and Protection, The Third International Conference, 2008, página 47 y ss.; *Fawcett*/*Provost*, Adaptive Fraud Detection, *Data Mining and Knowledge Discovery*, vol. 1, No. 3, 1997, página 291 y ss.; *Bolton*/*Hand*, Statistical Fraud Detection: A Review, 2002, disponible en: http://metalab.uniten.edu.my/~abdrahim/ntl/Statistical%20Fraud%20Detection%20A%20Review.pdf (última consulta: octubre de 2008); Critical with regard to the related surveillance of the customer, véase *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, *Bulletin of Science Technology Society*, 2007, vol. 27, 2008, página 11 y ss.; *Stoddart*, Who Watches the Watchers? Towards an Ethic or Surveillance in a Digital Age, *Studies in Christian Ethics*, 2008, vol. 21, 2008, página 363 y ss.

[9] Véase, *Copes*/*Vieraitis*/*Jochum*, Bridging the Gap between Research and Practice: How Neutralization Theory can inform Reid Interrogations of Identity Thieves, *Journal of Criminal Justice Education*, vol. 18, No. 3, 2007, página 444 y ss.

[10] Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, 2007 E/CN.15/2007/8/Add. 3, página 16; respecto de la cooperación internacional en los casos de hurto de identidad, véase: *Elston*/*Stein*, International Cooperation in Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, disponible en: http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf (última consulta: octubre de 2008).

[11] Respecto de las dimensiones transnacionales del delito cibertnético, véase: *Keyser*, The Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, vol. 12, núm. 2, página 289, disponible en: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf (última consulta: octubre de 2008); *Sofaer*/*Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer*/*Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, página 1 y ss., disponible en: http://media.hoover.org/documents/0817999825_1.pdf (última consulta: octubre de 2008).

[12] La soberanía nacional es un principio fundamental del derecho internacional. Véase, *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, página 1, disponible en: http://www.law.uga.edu/intl/roth.pdf (última consulta: octubre de 2008).

[13] Respecto a la cooperación en los casos de hurto de identidad transnacionales, véase OECD Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, página 45. En lo que respecta a la necesidad de cooperación internacional en la lucha contra el delito cibernético, véanse *Putnam*/*Elliott*, International Responses to Cyber Crime, en *Sofaer*/*Goodman*, Transnational Dimension of Cyber Crime and Terrorism, *supra* núm. 11, página 35; *Sofaer*/*Goodman*, Cyber Crime and Security – The Transnational Dimension, *ibid*.

Si se trata de delitos de identidad muy graves, los Estados Miembros cuentan con argumentos convincentes y fiables para invocar, en el marco de la cooperación internacional, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, como base jurídica. En lo que respecta a los demás "factores habilitantes" pertinentes para la aplicación de la Convención, el aspecto transnacional parece ser, en la mayoría de los casos, un elemento inherente del delito relacionado con la identidad, mientras que la intervención de un grupo delictivo organizado podría estar más o menos implícita cuando los medios utilizados para cometer un delito superen las posibilidades de delincuentes individuales[14].

Educación

La educación de los miembros de la sociedad civil sobre el riesgo relacionado con la publicación y el uso no protegido de información de iden tidad, así como las estrategias de protección contra los delitos relacionados con el hurto de identidad, pueden reducir el riesgo de ataques realizados con éxito[15]. Esto es especialmente importante con respecto a las estafas basadas en la ingeniería social como las estafas de "peska"[16].

Consecuencias del hurto de identidad

Aparte de los criterios no relacionados con el derecho penal, el estudio no ahondará en las cuestiones financieras y penales vinculadas con el hurto de identidad. Por lo tanto, no se abordarán más en detalle las consecuencias de dicho delito. En esta publicación se indicarán varios estudios realizados en que se analizan las consecuencias económicas de los delitos de hurto de identidad[17]. Estos delitos representan para la economía británica una pérdida anual estimada de 1.300 millones de libras. En 2005, el perjuicio causado ascendió a más de 50.000 millones de dólares de los EE.UU.[18]. En la mayoría de los estudios se destaca que el hurto de identidad plantea un reto para las sociedades, así como para los

[14] De conformidad con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional uno de los objetivos de un grupo delictivo organizado es generar un "beneficio económico u otro beneficio de orden material" (Artículo 2). Aunque los delitos relacionados con la identidad no son necesariamente de naturaleza económica, en su mayoría están comprendidos en el ámbito de aplicación de la Convención, ya que se incluyen los delitos no económicos relacionados con la identidad, vinculados a un grupo delictivo organizado que también esté implicado en delitos económicos. Además, el significado de la expresión "beneficio económico u otro beneficio de orden material" es relativamente amplio y comprende, por ejemplo, el tráfico de pornografía infantil con fines de gratificación sexual. Por lo tanto, abarca delitos de identidad en que se haya tratado de alguna manera a la información de identificación o de identidad sustraída o fabricada como mercancía ilícita, es decir, que se haya comprado, vendido o permutado, y los casos en que la identificación se haya utilizado indebidamente con miras a obtener beneficios personales o colectivos, incluidos beneficios que no fueran económicos, como el de poder entrar a otro país.

[15] Véase, *White/Fisher*, Assessing Our Knowledge of Identity Theft…, *supra* núm. 6, página 15 y ss.; *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003; IECD Scoping Paper on Online Identity Theft, *supra* núm. 13, página 35.

[16] El término "peska" se utiliza para describir un acto que tiene por objeto lograr que la víctima revele información personal o confidencial. Se empleó inicialmente para describir la utilización de los correos electrónicos para "peskar" contraseñas y datos financieros en un mar de usuarios de Internet. El empleo de la grafía "k" se relaciona con las convenciones terminológicas de uso común en la piratería informática. Véase *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, página 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, disponible en: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf (última consulta: octubre de 2008).

[17] 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[18] Véase Javelin Strategy and Research 2006 Identity Fraud Survey, Consumer Report, disponible en: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf (última consulta: octubre de 2008).

organismos encargados de hacer cumplir la ley, no solo por el número de delitos, sino también por las pérdidas que ocasionan[19]. La principal dificultad relacionada con la interpretación de los estudios reside en que están basados en definiciones diferentes del concepto de "hurto de identidad" y suelen referirse solo a un país.

Debe tenerse en cuenta que las consecuencias del hurto de identidad no se limitan a las pérdidas económicas que afectan directamente a la víctima. Es necesario considerar asimismo el daño que suponen para su reputación, los perjuicios ocasionados a las instituciones financieras, el costo de la labor de los organismos encargados de hacer cumplir la ley, así como de las medidas preventivas[20].

Análisis de la situación de la víctima

Los problemas de las víctimas son sumamente importantes porque el delito de hurto de identidad se ha convertido en un fenómeno de gran amplitud con toda una serie de posibles repercusiones para la víctima[21]. Cabe preguntarse quién debe considerase víctima, ¿las instituciones financieras que con frecuencia se hacen cargo de las pérdidas causadas por delitos financieros relacionados con el hurto de identidad o las personas cuya información personal fue utilizada?[22]. El objetivo específico del presente estudio no permite analizar en profundidad estas cuestiones (que se abordan por separado en el presente Manual).

[19] Véanse, por ejemplo, los estudios mencionados *supra*, núm. 17.

[20] En relación con los aspectos que deben tenerse en cuenta para estimar la pérdida, véase Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, Documento de la Oficina General de Contabilidad: GAO/GGD-98-100BR, página 10 y ss. Personal Information, Data breaches are frequent, but evidence of resulting identity theft is limited…, *supra* núm. 4 página 2; *White*/*Fisher*, Assessing Our Knowledge of Identity Theft…, *supra* núm. 6, página 4.

[21] En este contexto véase, OECD Scoping Paper on Online Identity Theft, *supra* núm. 13, página 27.

[22] Véase: Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, *supra* núm. 20, página 11; Identity Theft, Available Data Indicate Growth in Prevalence and Cost, Statement of *R. Stana*, Documento de la Oficina General de Contabilidad: GAO-02-424T, 2002, página 5; *Levi*/*Burrows*, Measuring the Impact of Fraud in the UK, *British Journal of Criminology*, 2008, vol. 48, página 12; *Elston*/*Stein*, International Cooperation in Online Identity Theft Investigations…, *supra* núm. 10, página 5.

II. SINOPSIS DE LA ESTRUCTURA

El estudio se divide en tres partes principales. En la primera parte[23] se analiza el fenómeno de los delitos tipificados como "hurto de identidad". Además, se examina el tipo de información relativa a la identidad que buscan los delincuentes y los métodos utilizados para cometer los delitos. Este análisis sirve de base para determinar en qué medida los diferentes enfoques jurídicos abordan este fenómeno.

En la segunda parte del estudio[24] se examinan los criterios existentes para definir el hurto de identidad y, a partir de los resultados del análisis relativo al fenómeno y la definición, se elabora una tipología del hurto de identidad.

En la tercera parte[25] se esbozan los argumentos a favor y en contra de la creación de un enfoque específico para tipificar el hurto de identidad y se exponen los enfoques existentes. También se presentan elementos que pueden ser necesarios para la elaborar un enfoque nacional, sobre la base de los resultados de la primera y segunda parte del estudio.

[23] Véase *infra*, capítulo 3.
[24] Véase *infra*, capítulos 4 y 5.
[25] Véase *infra*, capítulo 6.

III. FENÓMENO

1. De la interacción personal al intercambio de información relacionada con la identidad

Teniendo en cuenta la amplia cobertura de los medios de comunicación[26], los resultados de varias encuestas que analizan el alcance y los perjuicios imputables al hurto de identidad[27], así como los numerosos estudios jurídicos y técnicos[28] publicados en los últimos años, el hurto de identidad parecería ser un fenómeno del siglo XXI[29]. Sin embargo, no es así. En el decenio de 1980 la prensa ya se hacía eco del uso indebido de información relacionada con la identidad[30] y de elementos conexos, como el hecho de que en algunos países la falsificación de documentos es un delito tipificado desde hace más de un siglo[31]. Lo que ha cambiado son las estafas a que recurren los delincuentes. Mientras que en decenio de 1980 predominaba el clásico robo de correspondencia, el uso cada vez más frecuente de la información digital ha ofrecido nuevas posibilidades de acceso a la información relacionada con la identidad[32]. El proceso mediante el cual las sociedades industriales se han transformado en sociedades[33] de la información influyó significativamente en el desarrollo del fenómeno. Sin embargo, pese al gran número de casos de hurto cometidos a través de Internet, la digitalización

[26] Véase, por ejemplo, *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, disponible en: http://edition.cnn.com/2006/US/05/18/identity.theft/ (última consulta: octubre de 2008); Identity Fraud, *NY Times* Topics, disponible en: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html (última consulta: octubre de 2008); *Stone*, U.S. Congress Looks at Identity Theft, International Herald Tribune, 22.03.2007, disponible en: http://www.iht.com/articles/2007/03/21/business/identity.php (última consulta: octubre de 2008).

[27] Véase *supra* núm. 17.

[28] Véase, por ejemplo, *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, *Lex Electronica*, vol. 11, núm. 1, 2006, disponible en: http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf (última consulta: octubre de 2008); *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, disponible en: http://www.privacyrights.org/ar/id_theft.htm (última consulta: octubre de 2008).

[29] *Hoar*, Identity Theft: The Crime of the New Millennium, *Oregon Law Review*, vol. 80, 2001, páginas 1421 y ss.; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, vol. 49, 2008, página 8.

[30] Véase, *Goodrich*, Identity Theft Awareness in North Central West Virginia, *supra* núm. 15, página 1.

[31] Véase, Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, página 5.

[32] *McCusker*, Transnational Organized Cybercrime: Distinguishing Threat From Reality, *Crime, Law and Social Change*, vol. 46, página 270.

[33] A diferencia de la sociedad industrial, los miembros de la sociedad de la información ya no están conectados por su participación en la industrialización, sino a través de su acceso y uso de las tecnologías de la información. Puede consultarse más información sobre la sociedad de la información en: *Masuda*, The Information Society as Post-Industrial Society, The Institute for Information Society, 1980; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe, Springer-Verlag, 2006; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society, Springer Science and Business Inc., 2005; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society, disponible en http://www.cils.org/WSIS/WSIS.htm (última consulta: octubre de 2008); *Hornby/Clarke*, Challenge and Change in the Information Society, Facet, 2003.

en sí no ha permitido cometer los delitos, sino que ha creado nuevos blancos y propiciado nuevos tipos de fraudes[34].

2. La información relacionada con la identidad como objetivo

Creciente interés por la información relacionada con la identidad

La importancia del hurto de identidad en el siglo XXI se debe al creciente interés por la información de identidad en el ámbito financiero, al igual que en el ámbito económico y en las relaciones sociales. En el pasado, predominaban el "prestigio" y las buenas relaciones personales tanto en los negocios como en las operaciones cotidianas[35]. Con el advenimiento del comercio electrónico, se hizo casi imposible el contacto personal y, por consiguiente, cobró mucha más importancia la información relacionada con la identidad para poder participar en la interacción social y económica[36]. Es un proceso fundamental, que puede calificarse de instrumentalización[37], y que consiste en traducir una identidad en información cuantificable relacionada con la identidad. También lo es la distinción entre, por un lado, la identidad de una persona definida[38] como el conjunto de los datos personales y, por otro lado, la información cuantificable relacionada con la identidad que permite reconocer a una persona.

Hoy día, requisitos tales como la confianza y la seguridad[39], necesarios en las transacciones que no se realizan en persona, se aplican no solo en las operaciones electrónicas sino también en el sector económico en general. Un ejemplo es el uso de tarjetas de crédito que requieren un número NIP (número de identificación personal) para comprar productos en un supermercado. Es un número que no sirve para identificar al cliente sino para legitimar la autorización del pago.

Consecuencias de la digitalización

La digitalización y la globalización de los servicios basados en redes han promovido el aumento del uso de información relacionada con la identidad. La mayoría de las empresas, así como las transacciones federales, dependen del tratamiento de datos electrónicos mediante sistemas automatizados[40]. El acceso a la información relacionada con la identidad permite a los delincuentes intervenir en muchos ámbitos de la vida social. Por otra parte, esa información, además de procesarse, generalmente se almacena en bases de datos, que son por ese motivo un blanco potencial para los delincuentes.

---

[34] *Clarke*, Technology, Criminology and Crime Science, *European Journal on Criminal Policy and Research*, vol. 10, 2004, página 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, *supra* núm. 20, página 51.
[35] *Elston/Stein*, International Cooperation in Online Identity Theft Investigations…, *supra* núm. 10, página 1.
[36] Véase *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, página 555.
[37] *Ceaton*, The Cultural Phenomenon of Identity Theft …, *supra* núm. 8, página 20
[38] Véase la *Enciclopedia Británica* 2007.
[39] *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, 533.
[40] Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, *supra* núm. 4, página 4.

Categorías tradicionales de datos buscados por los delincuentes

Como consecuencia de la digitalización han cambiado las categorías de información relacionada con la identidad que buscan los delincuentes. Antes de la digitalización, el objetivo del delincuente era la información tradicional relacionada con la identidad, como el número de pasaporte y la información contenida en las partidas de nacimiento. Las categorías más comunes de información tradicional relacionada con la identidad figuran a continuación.

Número de seguridad social (NSS)

El NSS que se utiliza en los Estados Unidos es un ejemplo clásico de dato relacionado con la identidad que buscan los delincuentes. La Ley de Seguridad Social de 1935 autorizó a la Administración de la Seguridad Social a elaborar y mantener un sistema de registro para administrar el programa de la seguridad social[41]. En la actualidad, los organismos gubernamentales estadounidenses utilizan generalmente el NSS para administrar registros, ubicar empleados, elaborar informes de nómina y estadísticas[42]. Sin embargo, no solo los servicios públicos utilizan el NSS. El sector privado también lo suele emplear con fines de identificación[43]. Los revendedores de información, los organismos de salud y las instituciones financieras utilizan el número de seguridad social con fines de correlación y para la identificación de clientes nuevos o existentes[44]. Los delincuentes pueden utilizar el NSS y obtener información del pasaporte para abrir cuentas financieras, manejar cuentas existentes, pedir un crédito o contraer deudas[45]. Con respecto al hurto de identidad, el principal problema que plantea el número de seguridad social es que no fue previsto inicialmente[46] como instrumento de identificación y, por ende, no va acompañado de las medidas necesarias de protección de la identidad. Si bien la Ley de protección de la información personal de 1974[47] restringió la divulgación del número de seguridad social por parte de los organismos públicos, los casos más recientes de hurto de identidad ponen de manifiesto que los delincuentes han logrado acceder a los registros públicos de la seguridad social[48].

Información del pasaporte

En la mayoría de los países, el pasaporte es el principal medio de identificación[49]. Los organismos públicos y las empresas privadas lo utilizan con fines de verificación e

[41] Social Security Numbers, More could be done to protect SSNs, Statement of *C. M. Fagnoni*, Managing Director Education. Workforce and Income Security, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, Cámara de Representantes, 2006, Documento de la Oficina General de Contabilidad: GAO-06-586T, página 3.

[42] *Ibid.*

[43] *Garfinkel*, Database Nation: The Death of Privacy in the 21st Century, O'Reilly, 2000, páginas 33 y 34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, *Harvard Journal of Law & Technology*, vol. 15, núm. 2, 2002, página 350.

[44] *Supra* núm. 41, página 8.

[45] Véase *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, disponible en: http://www.privacyrights.org/ar/id_theft.htm (última consulta: octubre de 2008).

[46] *Garfinkel*, Database nation…, *supra* núm. 41.

[47] *Supra* núm. 41.

[48] Social Security Numbers, Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate, Documento de la Oficina General de Contabilidad: GAO-07-752, 2007, página 1.

[49] *Wang/Chen/Atabakhsh*, Criminal Identity Deception and Deception Detection in Law Enforcement, *Group Decision and Negotiation*, vol. 13, 2004, página 119.

identificación de personas[50]. Si los delincuentes logran acceder a la información de interés que figura en el pasaporte pueden utilizarla para cometer otros delitos.

Permiso de conducir

Los permisos de conducir también pueden servir de instrumento de identificación[51]. Se supo que los secuestradores de los atentados del 11 de septiembre aprovecharon una laguna de la legislación del Estado de Virginia para obtener permisos de conducir con documentos falsificados[52].

Información del estado de cuenta bancario y del número de la tarjeta de crédito

Al igual que el NSS, la información de los estados de cuenta es otro dato muy buscado para hacerse con la identidad de una persona[53]. Esto incluye cuentas corrientes y en cajas de ahorros, tarjetas de crédito, de débito e información sobre planificación financiera. Constituye una importante fuente de información para los impostores potenciales que planeen cometer un delito financiero.

Partidas de nacimiento

Uno de los delitos de robo de la identidad más conocidos en el Reino Unido, que no requiere información digital, está relacionado con las partidas de nacimiento[54]. Obtener información sobre un niño fallecido y utilizarla para solicitar una partida de nacimiento solía ser una forma relativamente sencilla de conseguir un certificado de nacimiento mediante información falsa sobre la identidad[55].

Nuevas categorías de información relativa a la identidad que buscan los delincuentes

Como la información sobre la identidad mencionada no ha perdido importancia a raíz de la digitalización, conserva su atractivo para los delincuentes[56]. Con respecto a esta información, el principal cambio que introdujo el proceso de digitalización consistió en la

[50] *Stein*, Statement during the Hearing on the Role of Social Security Numbers (SSNs) in Identity Theft and Issues related to Enhancing Privacy, 2006, página 6, disponible en: http://www.bits.org/downloads/Testimony/SteinTestinomyMar06.pdf (última consulta: octubre de 2008).

[51] *Supra* núm. 49.

[52] *Elston/Stein*, International Cooperation in Online Identity Theft Investigations…, *supra* núm. 11, página 4; con respecto al uso de identidades falsas por parte de los terroristas del 11 de septiembre, véase *Wang/Chen/Atabakhsh*, Criminal Identity Deception…, *supra* no. 49.

[53] Véase Identity Theft, Greater Awareness and Use of Existing Data Are Necessary, Informe al Honorable Sam Johnson, Cámara de Representantes, Documento de la Oficina General de Contabilidad: GAO-02-766, 2002, página 9; *Emigh*, Online Identity Theft: Phishing Technologies, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, página 6.

[54] Puede consultarse información adicional en: http://www.aboutidentitytheft.co.uk/your-birth-certificate.html (última consulta: octubre de 2008).

[55] *Levi*, Combating Identity and Other Forms of Payment Fraud in the UK: An Analytical History, publicado en *McNally/Newman*, Perspectives on Identity Theft.

[56] Véase *Gercke*, Internet-related Identity Theft, 2007, disponible en: http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf (última consulta: octubre de 2008).

forma de obtener la información[57]. Sin embargo, la digitalización al crear nuevas categorías de información de identidad promovió otros cambios[58]. En la actualidad, la información sobre las cuentas y las contraseñas, las direcciones de correo electrónico y las direcciones IP se han convertido en elementos tan importantes como los pasaportes o el NSS para verificar e identificar operaciones realizadas en redes. Las nuevas categorías más comunes de información de identidad que interesan a los delincuentes se exponen a continuación.

Información sobre cuentas y contraseñas

El acceso a los sistemas de control de servicios en red, como el correo electrónico, los servicios bancarios en línea o de servidores, suele requerir una contraseña. Por lo tanto, la obtención de contraseñas para acceder a servicios en línea se ha convertido en una prioridad para la comisión de delitos relacionados con la identidad[59]. Conseguir información sobre las cuentas, además de permitir al delincuente hacer uso del servicio correspondiente y realizar transacciones en línea, enviar correos electrónicos o vender bienes en una plataforma de subastas, le puede dar acceso a otros servicios. Esto es muy importante en el caso de las direcciones de correo electrónico, muchas veces utilizadas como instrumento de identificación[60].

Dirección de acceso al soporte físico y dirección de protocolo Internet

Con el fin de autenticar clientes y usuarios, los operadores utilizan parámetros individuales tales como direcciones de protocolo Internet[61] (dirección IP) o direcciones de acceso al soporte físico[62] (dirección MAC). El delincuente puede falsificar la dirección MAC[63] o tener acceso a la red informática de la víctima para utilizar su dirección IP[64] a fin de apoderarse de su identidad.

---

[57] Véase *infra*, capítulo 3.3.

[58] Con respecto a las categorías típicas de datos utilizados con fines de identificación, véase Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, *supra* núm. 10, página 6.

[59] Véase, *Shamah*, Password Theft: Rethinking an old crime in a new area, *Mich. Telecomm. Tech. Law Review*, vol. 12, 2006, página 335 y ss.

[60] Respecto de la identificación de una persona a través de la dirección de correo electrónico, véase *Garfinkel*, Email-based identification and authentication: an alternative to PKI?, *Security & Privacy*, vol. 1, issue 6, 2003, página 20 y ss.

[61] La dirección IP (dirección de protocolo Internet) es una identificación numérica que se asigna a un dispositivo que forma parte de una red de ordenadores. Para obtener una definición de dirección IP y más información sobre su funcionamiento, véase: Understanding IP Addressing, 3COM White Paper, 2001, disponible en: http://www.3com.com /other/pdfs/infra/corpinfo/en_US/501302.pdf (última consulta: octubre de 2008).

[62] La dirección MAC (dirección de acceso al soporte físico) es un identificador único que se asigna a los dispositivos de conexión a la red.

[63] Con respecto a los medios de manipulación y detección de tales falsificaciones, véase *Wrigth*, Detecting Wireless LAN Mac Address Spoofing, 2003, disponible en: http://forskningsnett.uninett.no/wlan/download/wlan-mac-spoof.pdf (última consulta: octubre de 2008); *Guo/Chiueh*, Sequence Number-Based MAC Address Spoof Detection, disponible en: http://www.ecsl.cs.sunysb.edu/tr/TR182.pdf (última consulta: octubre de 2008).

[64] Con respecto a las dificultades que plantean las investigaciones sobre el delito cibernético que incluye el uso abusivo de las redes inalámbricas, véase *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime in Cybercrime & Security, Instituto de Auditores Internos-2; *Urbas/Krone*, Mobile and Wireless Technologies: Security and Risk Factors, Instituto Australiano de Criminología, 2006, disponible en: http://www.aic.gov.au/publications/tandi2 /tandi329t.html (última consulta: octubre de 2008).

3. Nuevos métodos derivados de la digitalización para obtener información

Resulta extremadamente difícil describir el hurto de identidad definiendo los métodos utilizados para cometer el delito[65]. Varios métodos diferentes corresponden al concepto de "hurto de identidad"[66], que abarcan desde el clásico hurto de correspondencia[67] hasta sofisticadas operaciones de *peska*[68].

Estafas tradicionales

A continuación figuran las estafas más corrientes realizadas con datos de identidad no digitales:

Reexpedición del correo postal

Reexpedir la correspondencia enviada a la víctima permite a los delincuentes obtener acceso a la información personal que se manda por correo[69] e impide que la víctima detecte actividades sospechosas[70].

Robo de correspondencia y de fuentes de información personal

Debido a que numerosos documentos importantes se envían por correo postal, el acceso a esta fuente sigue siendo un buen método para obtener información relativa a la identidad[71]. Otros posibles blancos del robo destinado a obtener información relacionada con la identidad son las carteras, los pasaportes, los permisos de conducir, las agendas, los calendarios y otros elementos con información personal[72].

Hurgar en la basura

La expresión "hurgar en la basura" se utiliza para describir el proceso de revisar los contenedores de residuos en busca de documentos con datos personales[73].

Ataques internos

En la encuesta sobre el delito informático y la seguridad llevada a cabo en 2007 por el Instituto de Seguridad Informática (CSI)[74] se señalaba que más del 35% de los

[65] Véase *infra* el capítulo 3.5.

[66] Para hacerse una idea general de las diferentes técnicas utilizadas para cometer un hurto de identidad, véase Techniques of Identity Theft, CIPPIC Canadian Internet Policy and Public Interest Clinic Working Paper No. 2 (ID Theft Series), 2007.

[67] En una encuesta realizada en 2003 se mencionó el hurto de correspondencia (el 68% de los participantes) como principal preocupación. Véase, *Gayer*, Policing Privacy, Law Enforcement's Response to Identity Theft, CALPIRG Education Fund, 2003, página 10.

[68] Sobre la semántica del término "peska", véase *supra* núm. 16 (que se refiere a *Gercke*, Criminal Responsibility for Phishing and Identity Theft, *ibid.*); véase también, *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, disponible en: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf (última consulta: octubre de 2008).

[69] Por ejemplo, tarjetas de crédito, contraseñas, estados de cuenta.

[70] Véase, Techniques of Identity Theft, CIPPIC Working Paper, *supra* núm. 66, página 6.

[71] En una encuesta realizada en 2003, el 68% de los participantes indicaron que el hurto de correspondencia era la principal preocupación. Véase *Gayer*, Policing Privacy, Law Enforcement's Response to Identity Theft, 2003, página 10.

[72] *Ibid.*, página 11.

[73] Véase *Zaidi*, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada, *Loyola Consumer Law Review*, vol. 19, issue 2, 2007, página 101; *Gayer*, Policing Privacy…, *supra* núm. 71; *Siegel*, Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age, *Penn State Law Review*, vol 111, núm. 3, página 784; Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, página 6.

[74] La encuesta sobre delito informático y seguridad de 2007 del Instituto de Seguridad Informática (CSI) analizó, entre otras cosas, las consecuencias económicas del negocio del delito cibernético. Se basa en las respuestas de 494 profesionales de la seguridad informática de empresas de los Estados Unidos, organismos gubernamentales e instituciones financieras. Puede consultarse en: http://www.gocsi.com/ (última consulta: octubre de 2008).

encuestados atribuía más del 20% de las pérdidas de la organización a sus propios empleados. Los resultados de este estudio confirman los informes según los cuales los empleados habían obtenido miles de datos de instrumentos crediticios y de tarjetas de crédito[75]. Una de las razones del éxito de estos ataques se debe a que muchas medidas de seguridad están diseñadas para prevenir ataques exteriores.

Utilización de información pública

Los registros públicos contienen gran variedad de información relacionada con la identidad[76]. El delincuente puede obtener de esta fuente información para utilizarla con fines delictivos.

Estafas relacionadas con la información digital

Como se ha señalado, la digitalización ha promovido la aparición de nuevos métodos para conseguir información relacionada con la identidad. La información digital, accesible mediante las tecnologías de la información, supone varias ventajas para los delincuentes, así como dificultades para los organismos encargados de hacer cumplir la ley[77]. La tecnología informática y de redes permite que el delincuente obtenga muchos datos personales con el mínimo esfuerzo[78]. Hoy día, las estafas de este tipo son las siguientes:

a) *Skimming (copia de la tarjeta con un dispositivo de lectura de datos)*
En los últimos tiempos, la manipulación de cajeros automáticos para obtener información de la tarjeta de crédito de la víctima y sus códigos de acceso se ha convertido en un importante motivo de preocupación[79].

b) *Peska o pharming*
El término "peska" se utiliza para describir los actos con los que se trata de inducir a la víctima mediante técnicas[80] de ingeniería[81] social a revelar datos personales o confidenciales. No es un delito nuevo, sino que desde hace decenios se lo conoce como "hurto mediante engaño"[82]. Si bien existen diferentes tipos de ataques de *peska*[83], los perpetrados a través del correo electrónico siguen tres etapas: en la

[75] El informe 2005 Identity Theft: Managing the Risk se refiere a un incidente en que un empleado de una empresa estadounidense que suministraba informes sobre créditos a los bancos utilizó contraseñas confidenciales para acceder a los informes de crédito de más de 30.000 consumidores y descargarlos, durante un período de tres años. Véase, 2005 Identity Theft: Managing the Risk, Insight Consulting, página 2, disponible en: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf (última consulta: octubre de 2008); sobre los riesgos relacionados véase también: *Goodrich*, Identity Theft Awareness in North Central West Virginia, *supra* núm. 15, página 11.

[76] Social Security Numbers, Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, Senado de los Estados Unidos, Documento de la Oficina General de Contabilidad: GAO-07-752, 2007, página 1.

[77] Véase al respecto el capítulo 3.5. *infra*.

[78] *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, *Crime, Law and Social Change*, vol. 46, página 270; *Elston/Stein*, International Cooperation in Online Identity Theft Investigations…, *supra* núm. 10, página 2; *Faulkner*, Hacking Into Data Breach Notification *Laws, Florida Law Review*, vol. 59, 2007, página 1089.

[79] Véase, Techniques of Identity Theft, CIPPIC Working Paper *supra* núm. 66, página 9.

[80] *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, disponible en: http://www.securityfocus.com/infocus/1527 (última consulta: octubre de 2008).

[81] El término "peska" se empleó originalmente para describir la utilización de los correos electrónicos para "peskar" contraseñas, *supra* núm. 16; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, disponible en: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf (última consulta: octubre de 2008).

[82] Véase, *Epstein/Brown*, Cybersecurity in the Payment Card Industry, *University of Chicago Law Review*, vol. 75, 2008, página 205.

[83] Véase, *Gonsalves*, Phishers Snare Victims with VoIP, 2006, disponible en: http://www.techweb.com/wire/security/186701001 (última consulta: octubre de 2008).

primera, los delincuentes identifican a las compañías legítimas que ofrecen servicios en línea y que se comunican con sus clientes electrónicamente[84]. En la segunda, los delincuentes diseñan sitios web similares ("sitios falsos") a los sitios legítimos de la compañía considerada. Para dirigir a los usuarios a estos sitios falsos, los delincuentes con frecuencia envían correos electrónicos similares a los que envía la compañía legítima[85]. Otra técnica utilizada para dirigir al usuario al sitio falso es la manipulación del sistema de nombres de dominio (DNS o SND), conocida como "pharming"[86]. En la tercera etapa, los delincuentes usan la información revelada por la víctima, por ejemplo, para entrar a sus cuentas y transferir dinero, solicitar pasaportes o abrir nuevas cuentas. El creciente número de ataques de este tipo llevados a cabo con éxito muestra la gravedad de la amenaza[87].

Programas informáticos malignos

Los delincuentes en busca de información relativa a la identidad se valen cada vez más de estos programas malignos para obtener información confidencial, como contraseñas, números de tarjetas de crédito y de seguridad social[88]. Mediante la instalación[89] de pequeños programas informáticos en la computadora de la víctima, los delincuentes pueden interceptar comunicaciones, registrar las pulsaciones del teclado y buscar información almacenada en el ordenador.

Piratería informática (hacking)

Se entiende por "piratería informática" el acceso ilegal a un sistema informático[90]. Es uno de los delitos informáticos más antiguos[91], y en los últimos años se ha convertido en un fenómeno de gran escala[92]. Aparte de objetivos ya conocidos, como la NASA, la Fuerza Aérea de los Estados Unidos, el Pentágono, Yahoo, Google, eBay y el Gobierno de Alemania[93], los infractores se orientan cada vez más hacia sistemas

[84] Con respecto a las diferentes fases de "peska", véase OECD Scoping Paper on Online Identity Theft, *supra* núm. 13, página 18.

[85] La "peska" tiene muchas semejanzas con los correos basura o spam. Por tanto, es probable que los grupos delictivos organizados que envían correos de este tipo también estén involucrados en estafas de peska, ya que utilizan las mismas bases de datos. En cuanto al correo basura, véase *supra*: Los delincuentes han desarrollado técnicas avanzadas para evitar que los usuarios se den cuenta de que no están en el sitio web real. Puede consultarse: http://www.antiphishing.org/phishing_archive/phishing_archive.html (última visita: octubre de 2008).

[86] Se pueden consultar detalles adicionales en: Techniques of Identity Theft, CIPPIC Working Paper *supra* núm. 66.

[87] En algunos ataques de "peska", el 5% de las víctimas proporcionó información confidencial sobre sitios web falsos. Véase *Dhamija/Tygar/Hearst*, Why Phishing Works, disponible en: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf (última consulta: octubre de 2008), página 1, que se refiere a *Loftesness*, Responding to "Phishing" Attacks, Glenbrook Partners, 2004.

[88] Véase "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", página 4 y ss., disponible en: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

[89] Con respecto a los distintos procesos de instalación, véase "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", página 21 y ss., disponible en: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf (última consulta: octubre de 2008).

[90] En los primeros años de desarrollo de la tecnología de la información, por "hacking" (piratería informática) se entendía el intento de obtener del sistema (software o hardware) más de lo que permitía. En este contexto, el término "piratería informática" o "hacking" se utilizaba con frecuencia para describir una actividad constructiva.

[91] Véase, *Levy*, Hackers: heroes of the computer revolution, Dell. Pub., 1994; Hacking Offences, Instituto Australiano de Criminología, 2005, disponible en: http://www.aic.gov.au/publications/htcb/htcb005.pdf (última consulta: octubre de 2008); *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, Routledge, 2001, página 61.

[92] Véanse las estadísticas proporcionadas por HackerWatch. La comunidad en línea HackerWatch publica informes sobre la piratería informática. Según sus fuentes, se comunicaron más de 250 millones de incidentes. Véase, *Biegel*, Beyond our Control? Confronting the Limits of our Legal System in the Age of Cyberspace, Massachusetts Institute of Technology, 2001, página 231 y ss. en el mes de agosto de 2007. Fuente: http://www.hackerwatch.org.

[93] Para hacerse una idea de las víctimas de los ataques de piratería informática, véase http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history (última consulta: octubre de 2008); *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, *European Journal of International Law*, 2002, núm. 5, página 825 y ss., en relación con el impacto, véase *Biegel*, Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, página 231 y ss.

informáticos de usuarios comunes. En cuanto acceden al sistema informático pueden obtener información relacionada con la identidad. Sus objetivos también pueden ser los sistemas informáticos con grandes bases de datos que contienen información sobre la identidad[94].

Hurto y obtención de material de almacenamiento

Si bien se suele considerar que el hurto es un delito tradicional, el robo de dispositivos informáticos y de almacenamiento especiales para acceder a la información de identidad almacenada persigue otra finalidad. El interés de los delincuentes no es el valor del equipo físico, sino la información que contiene[95]. Los métodos empleados abarcan desde la compra legítima de equipos de segunda mano, que en muchos casos conservan la información confidencial no debidamente eliminada, hasta el robo de sistemas informáticos[96]. La encuesta de 2007 sobre delito informático y seguridad del Instituto de Seguridad Informática (CSI)[97] mostró que casi el 15% de las pérdidas de los entrevistados estaban relacionadas con el robo de datos confidenciales y de computadoras portátiles[98]. Si bien es discutible que el robo de equipos se considere un delito informático, las estadísticas ponen de manifiesto la importancia de los métodos físicos para obtener datos relacionados con la identidad[99].

Además de la apropiación indebida, la información puede obtenerse a partir de computadoras y material de almacenamiento extraviados. En los últimos años, se publicaron varios informes sobre incidentes en que se había perdido material de almacenamiento con grandes bases de datos sobre la identidad[100].

Nuevos métodos para utilizar la información pública disponible

Como ya se ha señalado, los infractores no necesariamente tienen que cometer delitos para obtener información relacionada con la identidad, ya que se encuentra disponible en grandes cantidades[101]. Por ejemplo, los delincuentes pueden utilizar buscadores de Internet para obtener información sobre la identidad. Los términos "googlehacking" o "googledorks" describen el uso de complejos buscadores para filtrar de una gran cantidad de

[94] Véase, Techniques of Identity Theft, CIPPIC Working Paper *supra* núm. 66, página 19; Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, *supra* núm. 4, página 11.

[95] *Ceaton*, The Cultural Phenomenon of Identity Theft…, *supra* núm. 8, página 15.

[96] En este contexto, véase Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited…, *supra* núm. 3, página 19.

[97] La encuesta sobre delito informático y seguridad de 2007 del Instituto de Seguridad Informática (CSI) analizó, entre otras cosas, las consecuencias económicas del negocio del delito cibernético. Se basa en las respuestas de 494 profesionales de la seguridad informática de empresas de los Estados Unidos, organismos gubernamentales e instituciones financieras. La encuesta se encuentra disponible en: http://www.gocsi.com/ (última consulta: octubre de 2008).

[98] Encuesta sobre delito informático y seguridad de 2007 del CSI, página 15, disponible en: http://www.gocsi.com (última consulta: octubre de 2008).

[99] Con respecto a la definición de delito informático y delito cibernético, véase *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, página 3; Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, vol. 18, disponible en: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 (última consulta: octubre de 2008).

[100] Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; *supra* núm. 3, página 19; Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, *supra* núm. 4, página 7; *Levi/Burrows*, Measuring the Impact of Fraud in the UK, *supra* núm. 22, página 3.

[101] Acerca de la publicación no intencional en redes de información sobre la identidad, véase Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; *supra* núm. 3, página 7.

resultados de búsqueda, información relacionada con la seguridad informática, así como información personal que podría emplearse en estafas de hurto de identidad[102,103]. Los informes ponen de manifiesto el riesgo que puede suponer el uso legal de buscadores de Internet con fines ilegales[104]. Incluso se pueden usar los populares sistemas de intercambio de archivos para obtener información relacionada con la identidad[105].

Un nuevo fenómeno estrechamente vinculado con el desarrollo de nuevos servicios de Internet basados en contenidos creados por el usuario son las redes sociales[106]. Facebook y Myspace son ejemplos de servicios en línea diseñados para que el usuario se presente a sí mismo y se mantenga en contacto con otros usuarios[107]. La información que suministran incluye desde el nombre y la fecha de nacimiento, hasta sus inclinaciones sexuales. Mediante el acceso a estas redes los delincuentes pueden obtener la información sobre la identidad que los usuarios publican voluntariamente, para luego utilizarla con fines delictivos[108].

4. Formas de utilizar la información obtenida

Las consecuencias de la digitalización en las formas en que los delincuentes utilizan la información de identidad son menos graves en comparación con las consecuencias de los métodos empleados para su obtención. Las formas más corrientes de utilizar la información sobre la identidad figuran a continuación.

Comisión de delitos financieros

En la mayoría de los casos, el acceso a datos relacionados con la identidad permite al infractor cometer otros delitos[109]. De ahí que los infractores no se interesen solamente por los datos, sino por la posibilidad de utilizarlos para actividades delictivas. Por ejemplo, pueden manejar cuentas financieras existentes o crear cuentas nuevas suplantando la identidad de la víctima, y realizar transferencias o compras con esas cuentas[110].

---

[102] *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, Syngress Publishing Inc., 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, O'Reilly, 2006.

[103] *Ibid.*

[104] Véase, *Nogguchi*, Search engines lift cover of privacy, *The Washington Post*, 09.02.2004, disponible en: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/ (última consulta: octubre de 2008).

[105] Véase, Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, disponible en: http://oversight.house.gov/documents/20071017134802.pdf (última consulta: octubre de 2008).

[106] Respecto de las preocupaciones sobre la privacidad relacionadas con esas redes sociales, véase *Hansen/Meissner* (ed.), Linking digital identities, página 8. El resumen se encuentra disponible en inglés (páginas 8 a 9). El informe está disponible en línea en: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (última consulta: octubre de 2008).

[107] Con respecto al comportamiento de compartir la identidad en las redes sociales, véase, *Stutzman*, An Evaluation of Identity-Sharing Behavior in Social Network Communities, disponible en: http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf (última consulta: octubre de 2008).

[108] En cuanto al riesgo de hurto de identidad relacionado con esas redes sociales, véase, *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, 2005, página 73, disponible en: http://wiki.cs.columbia.edu:8080/download/attachments/1979/Information+Revelation+and+Privacy+in+Online+Social+Networks-gross.pdf (última consulta: octubre de 2008). Acerca del uso de las redes sociales para realizar ataques de peska más eficaces, véase, *Jagatic/Johnson/Jakobsson/Menczer*, Social Phishing, 2005, disponible en: http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf (última consulta: octubre de 2008).

[109] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, página 3, disponible en: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (última consulta: octubre de 2008).

[110] Puede consultarse más información acerca de los distintos delitos en el núm. 109, *supra*.

Venta de la información

Otro de los métodos es vender la información[111] para su utilización por otros infractores. Por ejemplo, los historiales de tarjetas de crédito se llegan a vender incluso por 60 dólares de los EE.UU.[112]. En este contexto, la motivación del delincuente es generar una ganancia directa sin cometer el delito para el cual se necesita la información obtenida. Así, la información puede ser utilizada para falsificar documentos de identidad complejos o aprovecharse de las vulnerabilidades de las compañías de seguros, engañando o sobornando a funcionarios para obtener documentos auténticos y venderlos posteriormente a otros infractores, que los utilizarán en nuevos delitos, como viajes ilícitos, inmigración ilegal u otras actividades[113].

Encubrimiento de la identidad

Los delincuentes pueden utilizar la información que obtienen para ocultar su verdadera identidad[114]. Asimismo, pueden solicitar y usar instrumentos de identificación para inducir a error en las investigaciones, o usar la cuenta bancaria de la víctima para operaciones de blanqueo de dinero. Además, ocultándose tras una identidad falsa, los infractores pueden burlar las medidas de identificación y de prevención del terrorismo. En el informe del Secretario General de las Naciones Unidas sobre las Recomendaciones para una estrategia mundial de lucha contra el terrorismo se destaca la importancia de diseñar mecanismos para reconocer el robo de identidad en la lucha contra el terrorismo[115].

Los desafíos que plantea la capacidad de ocultar la identidad se ponen de manifiesto al examinar la importancia que tienen las rutinas de identificación para prevenir actividades de blanqueo de dinero. Muchas de las medidas encaminadas a combatir el blanqueo de capitales se basan en el principio "conozca a su cliente", y, por ende, dependen directamente de elementos relativos a la identidad. Los métodos de blanqueo de capitales comprenden la utilización de tecnologías de la información, las comunicaciones y la tecnología comercial que permite generar información de identificación falsa, además de facilitar las transferencias a distancia, gracias a la información de identidad falsa a fin de ocultar bienes objeto de blanqueo[116].

---

[111] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, vol. 11, núm. 1, 2006, página 17, disponible en: http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf (última consulta: octubre de 2008).

[112] Véase 2005 Identity Theft: Managing the Risk, Insight Consulting, página 2, disponible en: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf (última consulta: octubre de 2008).

[113] Véase *supra* núm. 10, párrafo 18.

[114] En este contexto, véanse los Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, *supra* núm. 10, página 10.

[115] Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo, 27 de abril de 2006, A/60/825, página 13.

[116] En cuanto a la relación entre los delitos relacionados con la identidad y los de blanqueo de dinero, véase *supra*, núm. 114, página 12.

5. Aumento de los robos de identidad relacionados con la informática y los problemas que plantean a la investigación

Como se ha señalado, la digitalización, así como los procesos de instrumentalización, han desarrollado las oportunidades y los métodos de cometer delitos relacionados con el hurto de identidad. En la actualidad, la información digital es un objetivo esencial para robar la identidad y, en numerosos casos, se utiliza la tecnología de la información para cometer los correspondientes delitos. Los factores coadyuvantes son los siguientes:

Disponibilidad de grandes bases de datos

En cuanto al uso extensivo de las tecnologías de la información, casi todos los organismos públicos y empresas generan información relacionada con la identidad y la almacenan en bases de datos[117]. Los informes sobre la pérdida y el robo de bases de datos con información relativa a la identidad de millones de clientes muestran la amenaza que supone el almacenamiento centralizado de este tipo de información[118].

Tendencia a almacenar más información

En la actualidad, los expertos critican el hecho de que se almacene cada vez más información sobre las actividades de los usuarios en Internet[119]. Los ejemplos incluyen desde el almacenamiento de actividades de búsqueda hasta el almacenamiento de datos de tráfico en países que tienen la obligación de conservarlos[120].

Capacidad de reproducir grandes bases de datos en poco tiempo

La copia de un gran número de documentos tangibles requiere el acceso físico a los documentos, tiempo para reproducirlos y, en general, supone una pérdida de calidad que revela que el documento no es el original. En comparación con el proceso de copia física, con sus inconvenientes, la reproducción en línea de bases de datos tiene varias ventajas. Al estar disponibles en línea, el acceso físico no es necesario. Además, la información digital se puede copiar en un tiempo bastante reducido sin comprometer la calidad[121].

---

[117] Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, *supra* núm. 4, página 4.

[118] Con respecto a los informes sobre el hurto y la pérdida de bases de datos que contienen información relacionada con la identidad, véase Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; *supra* núm. 3, página 19; Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, *supra* núm. 4, página 7; *Levi/Burrows*, Measuring the Impact of Fraud in the UK, *supra* núm. 22, página 3.

[119] Véase, por ejemplo, la declaración de Bruce Schneier en la Conferencia de los Administradores de los Sistemas de Registro (ASR), 2008, Londres, Heise News, 29 de octubre de 2008, disponible en: http://www.heise.de/newsticker/meldung/118119 (última consulta: octubre de 2008); en este contexto, véase también: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, página 8.

[120] En relación con la Directiva de conservación de datos de la UE, véase *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, *Chicago Journal of International Law*, 2007, vol. 8, núm. 1, disponible en: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J.__Int'l_L._233_(2007).pdf (última consulta: octubre de 2008); *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 2005, página 365 y ss.

[121] Se observa una evolución similar con respecto a la violación de estos derechos. La digitalización ha abierto las puertas a nuevas formas de violación de estos derechos. Este tipo de violaciones se basan en una reproducción rápida y precisa. Antes de la era de la digitalización, la copia de un disco o una cinta de vídeo suponía una pérdida de calidad. En la actualidad es posible reproducir las fuentes digitales sin que el original pierda calidad, lo que permite, por lo tanto, cualquier reproducción.

Información pública relativa a la identidad

Como se destacó anteriormente, la información relacionada con la identidad se encuentra disponible en redes a gran escala. Simplemente navegando en las redes sociales, los delincuentes pueden reunir datos útiles para cometer delitos relacionados con el hurto de identidad[122].

Capacidad para utilizar más recursos

Algunos grupos de delincuentes organizados tienen acceso a un considerable número de sistemas informáticos que pueden usar para llevar a cabo ataques automatizados[123]. Un ejemplo de cómo se puede utilizar un gran número de sistemas informáticos para cometer un delito es el ataque perpetrado contra los sitios web del Gobierno de Estonia[124]. El estudio de esos ataques ha puesto de manifiesto que pudieron haberse cometido mediante millares de ordenadores que formaban parte de un "botnet" (redes de zombi)[125]. En los informes se subraya que estos "botnets" no solo se utilizan para llevar a cabo ataques, sino también para cometer delitos relacionados con el hurto de identidad[126].

Capacidad para actuar a nivel mundial

Como se ha señalado, la comisión de un delito cibernético no requiere en general que el delincuente se encuentre en el mismo lugar que la víctima. Así pues, numerosos delitos cibernéticos pueden afectar a más de un país[127]. Los infractores pueden tratar de evitar su enjuiciamiento operando desde países con una legislación deficiente sobre delitos cibernéticos[128]. Para poder combatir el delito cibernético eficazmente deben eliminarse los "refugios seguros" que permiten a los delincuentes ocultar sus actividades[129]. Como en la actualidad no existen normas jurídicas para combatir el robo de identidad resulta muy difícil entablar una cooperación estrecha entre los diferentes organismos encargados de hacer cumplir la ley de cada país[130].

---

[122] En cuanto al riesgo de hurto de identidad relacionado con tales redes sociales, véase *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, 2005, página 73, disponible en: http://wiki.cs.columbia.edu:8080/download/attachments/1979/Information+Revelation+and+Privacy+in+Online+Social+Networks-gross.pdf (última consulta: octubre de 2008).

[123] Véase, Emerging Cybersecurity Issues Threaten Federal Information Systems, Oficina General de Contabilidad, 2005, disponible en: http://www.gao.gov/new.items/d05231.pdf (última consulta: octubre de 2008).

[124] Para consultar más información sobre estos ataques, véase *Lewis*, Cyber Attacks Explained, 2007, disponible en: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf (última consulta: octubre de 2008); A cyber-riot, *The Economist*, 10.05.2007, disponible en: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598 (última consulta: octubre de 2008); Digital Fears Emerge After Data Siege in Estonia, *The New York Times*, 29.05.2007, disponible en: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print (última consulta: octubre de 2008).

[125] Véase *Toth*, Estonia under cyberattack, disponible en http://www.cert.hu/dmdocuments/Estonia_attack2.pdf (última consulta: octubre de 2008).

[126] Véase IT worker charged with harvesting bots to commit ID theft, *Computer Fraud & Security*, diciembre de 2007, página 4.

[127] Respecto del alcance de los ataques cibernéticos transnacionales más perjudiciales, véase *Sofaer/Goodman*, Cyber Crime and Security, *supra* núm. 11, página 7.

[128] Un ejemplo son los delitos relacionados con la peska. La mayoría de sitios se almacenan en los Estados Unidos (32%), China (13%), Federación de Rusia (7%) y la República de Corea (6%). Aparte de los Estados Unidos ninguno de esos países ha firmado y ratificado acuerdos específicos de crimen cibernético internacional que les permita y obligue a participar efectivamente en las investigaciones internacionales.

[129] Este tema fue abordado por varias organizaciones internacionales. En la resolución 55/63 de la Asamblea General de las Naciones Unidas se señala que: "los Estados deben velar por que en su legislación y en la práctica se eliminen los refugios seguros para quienes utilicen la tecnología de la información con fines delictivos". El texto completo de la resolución puede consultarse en www.unodc.org/pdf/crime/a_res_55/res5563e.pdf (última consulta: octubre de 2008). El plan de acción del Grupo de los 8 subraya que deben eliminarse los refugios seguros para quienes utilicen indebidamente las tecnologías de la información.

[130] Véase *Elston/Stein*, International Cooperation in Online Identity Theft Investigations…, *supra* núm. 10, página 1.

Capacidad de utilizar medios de comunicación anónimos

Internet ofrece a los delincuentes la posibilidad de ocultar eficazmente su identidad. Dos ejemplos de ello son el uso de terminales públicas de Internet[131] y la reexpedición de correo por remitentes anónimos[132]. En estos casos, es extremadamente difícil identificar a los infractores[133].

Facilidad de manipulación de la información digital

Los delitos relacionados con el hurto de la identidad suelen traer aparejada la falsificación de la información conseguida. La información digital no solo puede copiarse rápidamente sin pérdida de calidad[134], sino que cada vez es más fácil de modificar cuando no existen medidas[135] de protección[136].

[131] Con respecto a los enfoques legislativos que requieren una identificación previa al uso de terminales públicas, véase el artículo 7, del Decreto Ley italiano núm. 144. Para consultar más en detalle, véase *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, página 94 y ss.

[132] Véase *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, Conference on Communications and Multimedia Security, 1999.

[133] Véase *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, página 294; *Elston/Stein*, International Cooperation in Online Identity Theft Investigations… *supra* núm. 10, página 11.

[134] *Ibid*.

[135] Por ejemplo, el uso de firmas electrónicas.

[136] Véase en este contexto, Discussion Paper Identity Crime, Model Criminal Law Officers' Committee *supra* núm. 31, página 8.

IV. DEFINICIÓN DE HURTO DE IDENTIDAD

En las diferentes jurisdicciones existe una gran diversidad de definiciones del hurto de identidad[137], y ni siquiera se utilizan las mismas palabras para describirlo. Mientras que en la mayoría de las publicaciones de los Estados Unidos se hace referencia a "hurto de identidad", en el Reino Unido es muy popular la expresión "falsificación de identidad"[138]. También se utilizan otras expresiones como "delitos relacionados con la identidad", "peska", "apropiación de cuenta" o "robo de cuenta".

1. Definiciones generales

Combinar la obtención de los datos con el uso de la identidad

"El hurto de identidad […] ocurre cuando una persona […] obtiene datos pertenecientes a otra –la víctima– y se hace pasar por esta última"[139]. La definición contiene dos elementos clave: el objeto (datos o documentos pertenecientes a otro) y dos elementos necesarios para llevar a cabo el acto delictivo. El primer elemento consiste en obtener la información[140], y el segundo es la necesidad de hacerse pasar por la víctima. Por consiguiente, la definición no abarca el mero hecho de obtener la información, ni tampoco el de hacerse con información ajena con la intención de venderla.

Acto punible en que la identidad es blanco o instrumento

"Los delitos relacionados con la identidad abarcan todos los actos punibles en que la identidad es el blanco o el instrumento principal[141]. La definición es bastante amplia. No especifica el objeto que abarca ni los actos delictivos. Fue el resultado de un intento por definir una categoría de nivel superior que incluye varios delitos relacionados con la

[137] Véase, OECD Scoping Paper on Online Identity Theft, *supra* núm. 13, anexo 1; *Gercke*, Internet-related Identity Theft, 2007, disponible en: http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf (última consulta: octubre de 2008).

[138] Respecto de los distintos enfoques de los países acerca de la definición, véase *Paget*, Identity Theft, McAfee White Paper, página 15, 2007, disponible en: http://www.mcafee.com/us/threat_center/white_paper.html (última consulta: octubre de 2008); *Mitchison/Wilikens/Breitenbach/Urry/Portesi*, Identity Theft – A discussion paper, página 22, disponible en: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf (última consulta: octubre de 2008).

[139] *Mitchison/Wilikens/Breitenbach/Urry/Portesi*, Identity Theft – A discussion paper, *supra*.

[140] Respecto de la penalización de la obtención de información relacionada con la identidad, véase *infra* el capítulo 5.2.2.

[141] Véase *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, página 556.

identidad, tales como el robo y la falsificación de identidad[142]. Se trata también del enfoque seguido en el estudio de las Naciones Unidas sobre "el fraude y la falsificación de identidad y su uso indebido con fines delictivos"[143]. En algunos contextos también se utilizó la expresión "uso indebido de la identidad" que tiene un significado análogo pero no lleva implícita la presunción de que determinada conducta es un delito en sí o deba ser tipificada como tal. Dado su amplio alcance, la definición no resulta apropiada para servir de base a una disposición de derecho penal aunque es útil desde el punto de vista metodológico para tener en cuenta diversas conductas que han de examinarse al elaborar tipologías concretas y adoptar posibles medidas legislativas sobre la penalización.

Falsificación u otra actividad ilegal en que la identidad es blanco o instrumento

"El hurto de identidad constituye un fraude u otra actividad ilegal en que se utiliza la identidad de una persona como principal blanco o instrumento sin su consentimiento"[144]. Esta definición de la expresión "hurto de identidad" es muy similar a la anterior. Contiene dos elementos fundamentales: el objeto (la identidad) y el acto correspondiente (el fraude u otra actividad ilegal). No se dan más detalles para describir el objeto ni el acto.

Usurpación de identidad

"La expresión 'hurto de identidad' podría ser empleada para describir el robo o la usurpación de una identidad existente (o de una parte importante de la misma), con o sin consentimiento, independientemente de que la víctima esté viva o muerta"[145]. Esta definición también contiene dos elementos: el objeto (la identidad) y el acto correspondiente (la usurpación). Comparada con otras definiciones, proporciona una descripción más detallada del objeto, aunque la definición del acto se basa en la obtención de la identidad. En consecuencia, no abarca la transferencia de información relativa a la identidad ni la utilización de dicha información.

Impostura o adopción de un nombre

"La falsificación de identidad se produce cuando una persona adopta un nombre totalmente ficticio o usurpa el nombre de otra persona con o sin su consentimiento"[146]. Esta definición contiene dos elementos: el objeto (identidad ficticia o real) y el acto correspondiente (usurpación o adopción). No se define más en detalle ni el objeto ni el acto. La disposición está centrada en la obtención de la identidad y, según la interpretación de "impostura" o "adopción", en la utilización de esa identidad. Por consiguiente, es poco probable que abarque la transferencia o la venta de información relacionada con la identidad. Su rasgo singular es que la definición se refiere al acto de usurpar o adoptar un

[142] *Ibid*.
[143] Véase *supra*, núm. 10, párrafo 4.
[144] *Supra*, núm. 141.
[145] *Paget*, Identity Theft, McAfee White Paper, página 5, 2007, disponible en: http://www.mcafee.com/us/threat_center/white_paper.html (última consulta: octubre de 2008).
[146] Identity Fraud: A Study, United Kingdom Cabinet Office, 2002, página 11, disponible en: http://www.ips.gov.uk/identity/downloads/id-fraud-report.pdf (última consulta: octubre de 2008).

nombre falso. A primera vista este criterio parece plantear dificultades ya que, por ejemplo, el famoso actor británico Richard Jenkins, que usaba el nombre "Richard Burton", así como el famoso escritor estadounidense Truman Steckfus-Persons, que llevaba el nombre "Truman Capote", cometían un delito por utilizar un seudónimo. Sin embargo, el criterio tiene en cuenta el hecho de que en las investigaciones actuales[147] se pone de relieve que la mayoría de los delitos de hurto de identidad se relacionan con identidades ficticias (sintéticas)[148]. Otra preocupación reside en que la penalización solo se limita a los nombres. No incluye ninguna otra información relativa a la identidad.

Definiciones utilizadas en encuestas

Se observa una incoherencia similar en las encuestas que enumeran y analizan actos relacionados con el hurto de identidad, por lo cual es necesario definir el alcance de la encuesta, como se indica a continuación:

Comisión Federal de Comercio de los Estados Unidos
La encuesta "Consumer Fraud and Identity Theft Complaint Data" publicada por la Comisión Federal de Comercio de los Estados Unidos, contiene información relacionada con la definición de hurto de identidad: "El fraude con tarjeta de crédito (26%) fue la forma más común de hurto de identidad"[149]. En el contexto del estudio relativo al hurto de identidad, el hecho de obtener información de identidad ("hurto") no se disoció del delito que supone utilizar esa información (fraude con tarjetas de crédito).

Grupo consultivo en materia de fraude del Reino Unido
En un informe publicado por el Grupo consultivo en materia de fraude del Reino Unido, dos actos se consideran necesarios. En el estudio se enuncian determinadas formas de hurto de identidad, por ejemplo: "el estafador obtendrá una copia certificada de la partida de nacimiento de la víctima (verdadera y legal) y solicitará documentos de identificación utilizando esa partida. Los documentos de identificación podrían ser pasaportes, permisos de conducir y pólizas de seguros nacionales"[150]. En este ejemplo el delito implica la comisión de dos actos: la obtención y la utilización de información relativa a la identidad.

Definiciones jurídicas

Como se examina detenidamente a continuación, por el momento solo unos pocos Estados han decidido penalizar los delitos relacionados con la identidad mediante una

[147] Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, página 4 con referencia a US National Fraud Ring Analysis, ID Analytics, 2008.
[148] En cuanto a las identidades sintéticas relacionadas con las estafas de hurto de identidad, véase: McFadden, Synthetic identity theft on the rise, *Yahoo Finance*, 16 de mayo de 2007, disponible en: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1.
[149] Consumer Fraud and Identity Theft Complaint Data, January – December 2005, Federal Trade Commission, 2006, página 3, disponible en: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (última consulta: octubre de 2008).
[150] Véase, Identity Theft: Do you know the signs? The Fraud Advisory Panel, página 1, disponible en: http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf (última consulta: octubre de 2008).

disposición penal específica[151]. En el momento de redactar el presente estudio, en los Estados Unidos se adoptaban los enfoques más conocidos para definir el robo de identidad, mientras que en el Canadá está pendiente de promulgación una ley especial sobre el tema (en una etapa ulterior, fue adoptado el proyecto de ley S-4 como una enmienda al Código Penal del Canadá (hurto de identidad y conducta dolosa conexa)). A continuación se reseña brevemente el enfoque legislativo de los Estados Unidos:

Disposición 18 U.S.C. § 1028

En la disposición 18 U.S.C. § 1028 a) 7) se establece lo siguiente: "Quien [...] transfiere, posee o utiliza sin autorización legítima un medio de identificación de otra persona con la intención de cometer, o ayudar a cometer cualquier actividad ilícita o relacionada con ésta, que constituya una violación de la legislación federal o un delito en virtud de las leyes estatales o locales comete un robo de identidad". Esta definición también contiene tres elementos: el objeto (los medios de identificación), el acto (transferir, poseer o utilizar) y la intención que vincula al acto con otras actividades delictivas (intención de cometer o ayudar a cometer cualquier actividad ilícita). La disposición se basa en un enfoque amplio en el caso de los dos actos, así como de los delitos intencionales. A diferencia de la manera en que se utiliza la expresión "hurto de identidad" en la "Consumer Fraud and Identity Theft Complaint Data" no es especialmente obligatorio, con arreglo a la disposición § 1028 a) 7), que el acto se relacione con un fraude.

Disposición 15 U.S.C. 1681a

La Comisión Federal de Comercio de los Estados Unidos da otra definición. La disposición 15 U.S.C. 1681a q) 3) contiene una breve definición de hurto de identidad: "se entiende por 'hurto de identidad' un fraude cometido utilizando información relativa a la identidad de otra persona, con sujeción a una definición más amplia que la Comisión pueda prescribir por reglamento". La principal diferencia con la descripción proporcionada en la disposición 18 U.S.C. § 1028 a) 7) reside en que en la disposición 15 U.S.C. 1681a q) 3), al igual que en la de la encuesta "Consumer Fraud and Identity Theft Complaint Data", se vincula el robo de identidad con el fraude. Esto limita la aplicación de la disposición en otros casos en que el delincuente utilice dicha información para cometer otros delitos. Además, pese a que la disposición define un acto que contiene la palabra "hurto", solo penaliza el uso de la información y no el acto de obtenerla.

Sobre la base de la disposición 15 U.S.C. 1681a q) 3), la Comisión Federal de Comercio ofrece una descripción más detallada de hurto de identidad[152]:

a) Por "hurto de identidad" se entiende un fraude que se comete o intenta cometer utilizando la información de identidad de otra persona sin autoridad legítima.

[151] Para hacerse una idea general de la legislación relacionada con el hurto de identidad en Europa, véase *Owen/Keats/Gill*, The Fight Against Identity Fraud…, *supra* núm. 159; *Mitchison/Wilikens/Breitenbach/Urry/Portesi*, Identity Theft, *supra* núm. 138; Legislative Approaches To Identity Theft…, *supra* núm. 159; Una reseña general de la legislación en Australia, los Estados Unidos y el Reino Unido figura en: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, 2007.

[152] Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, Federal Register 69, no. 82.

b) Por "información de identificación" se entiende cualquier nombre o número que pueda utilizarse, por separado o conjuntamente con cualquier otra información, para identificar a una persona determinada, incluidos:

1) El nombre, el número de la seguridad social, la fecha de nacimiento, el permiso de conducir expedido por un Estado o Gobierno, o un número de identificación, número de registro de extranjero, número de pasaporte, número de empleado o de identificación fiscal (NIF).
2) Datos biométricos únicos como las huellas digitales, la huella vocal, la retina o el iris, u otra representación física única.
3) El número particular de identificación electrónica, la dirección o el número de ruta bancario (ABA).
4) La información de identidad de las telecomunicaciones o del dispositivo de acceso.

Al igual que en la disposición 15 U.S.C. 1681a q) 3), la definición vincula la expresión hurto de identidad con el fraude y solo se refiere al hecho de utilizar la información relacionada con la identidad.

Resultados provisionales

Las definiciones utilizadas difieren más en cuanto a la descripción más o menos precisa de los hechos aludidos. Con respecto a la necesidad de que las disposiciones penales tengan una redacción más precisa, ninguna de las definiciones generales y las usadas en las encuestas pueden servir de base para elaborar una respuesta jurídica. La falta de precisión obedece a los diferentes criterios empleados. Las diferencias en el énfasis que se pone en las expresiones "hurto de identidad" y "falsificación de identidad" solo es una parte visible del problema[153]. Una de las razones es que algunas definiciones tienden a ser demasiado amplias[154]. Si se analiza la utilización de las expresiones "hurto de identidad" y "falsificación de identidad" en los medios de comunicación y las encuestas[155] se observa también una tendencia a calificar los delitos tradicionales, como el fraude con tarjetas de crédito, de "hurto de identidad"[156]. El Grupo Intergubernamental de Expertos de las Naciones Unidas encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, sugirió por lo tanto que las expresiones "delito de identidad" y "delito relacionado con la identidad" se utilizaran para abarcar las subcategorías "hurto de identidad" y "falsificación de identidad"[157].

La expresión "delito de identidad" se utiliza generalmente para referirse a todo tipo de conductas ilícitas relacionadas con la identidad, en particular el hurto y la falsificación de

[153] Véase *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, *supra* núm. 141.
[154] *Levi*, Combating Identity and Other Forms of Payment Fraud in the UK…, *supra* núm. 55.
[155] Véase, por ejemplo, Consumer Fraud and Identity Theft Complaint Data, January – December 2005, Federal Trade Commission, 2006, página 3 – disponible en: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (última consulta: octubre de 2008).
[156] *Levi*, Combating Identity and Other Forms of Payment Fraud in the United Kingdom, *supra* núm. 55.
[157] OECD Scoping Paper on Online Identity Theft, *supra* núm. 13, página 60.

identidad[158]. En este contexto, el componente "delito" suele ser más un concepto puesto que la mayoría de los Estados todavía no han adoptado leyes sobre estas infracciones[159]. El delito de identidad abarca delitos preparatorios o constitutivos como el de falsificación y de suplantación de la identidad. El problema que plantea la definición es que el uso indebido de la identidad puede guardar relación con la información de identidad propiamente dicha o con otra información vinculada a esta. En el segundo caso, tal vez no se le podría considerar delito de identidad, aunque sus efectos serían aproximadamente iguales.

En general, la falta de una definición precisa no dificulta la adopción de medidas jurídicas eficaces, como se desprende de la reseña de la legislación en materia de hurto de identidad. Sin embargo, la falta de una definición tiene dos consecuencias principales[160]. En primer lugar, es más difícil identificar la verdadera magnitud del problema ya que las distintas definiciones dificultan la comparación de los resultados de las encuestas. En segundo lugar, sin un acuerdo sobre los principios básicos, como la definición, resulta más difícil adoptar un enfoque internacional y coordinar las investigaciones internacionales. La existencia de criterios comunes o convergentes para una definición son una base importante de la cooperación internacional, con inclusión del intercambio transfronterizo de pruebas, la extradición de delincuentes y la asistencia jurídica recíproca[161].

[158] Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, *supra* núm. 10, página 4.

[159] Para hacerse una idea general de la legislación relacionada con el hurto de identidad en Europa, véase *Owen*/*Keats*/*Gill*, The Fight Against Identity Fraud: A Brief Study of the EU, the UK, France, Germany, and the Netherlands, Perpetuity Research & Consultancy International, 2006; *Mitchison*/*Wilikens*/*Breitenbach*/*Urry*/*Portesi*, Identity Theft, *supra* núm. 138; Legislative Approaches To Identity Theft: An Overview, CIPPIC Working Paper núm. 3, 2007. Una reseña de la legislación de Australia, los Estados Unidos y el Reino Unido figura en: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, 2007. Respecto de la penalización en los Estados Miembros de la OCDE, véase OECD Scoping Paper on Online Identity Theft, *supra* núm. 13.

[160] Véase, *White*/*Fisher*, Assessing Our Knowledge of Identity Theft…, *supra* núm. 6.

[161] Acerca de la cooperación de casos de hurto de identidad transnacionales, véase OECD Scoping Paper on Online Identity Theft, *supra* núm. 13, página 45.

V. TIPOLOGÍA

1. Problemas relacionados con la creación de una tipología

La visión general que se tiene del fenómeno[162] de hurto de identidad, así como las diferentes definiciones[163], muestran que hay muy pocos criterios comunes. Varían sobremanera las formas de obtener la información relativa a la identidad. Los métodos más comunes comienzan por el simple robo de correspondencia y llegan hasta complejas estafas. Teniendo en cuenta la disponibilidad de la información relativa a la identidad en las redes sociales[164], donde los usuarios la publican voluntariamente, hacerse con esta información no es necesariamente un delito. Análogamente hay diversos tipos de datos que interesan a los infractores, como el número de seguridad social y las direcciones de correo electrónico. Ni siquiera se observa una motivación sistemática en los infractores en pos de información. Mientras que algunos utilizan la información robada para realizar actividades delictivas, otros la venden o la utilizan para obstaculizar la labor de investigación.

2. Principios comunes

Pese a la diversidad observada, la visión general del fenómeno del hurto de identidad, así como su definición, muestran al menos una cierta coincidencia que puede servir para extraer principios comunes con miras a elaborar una tipología.

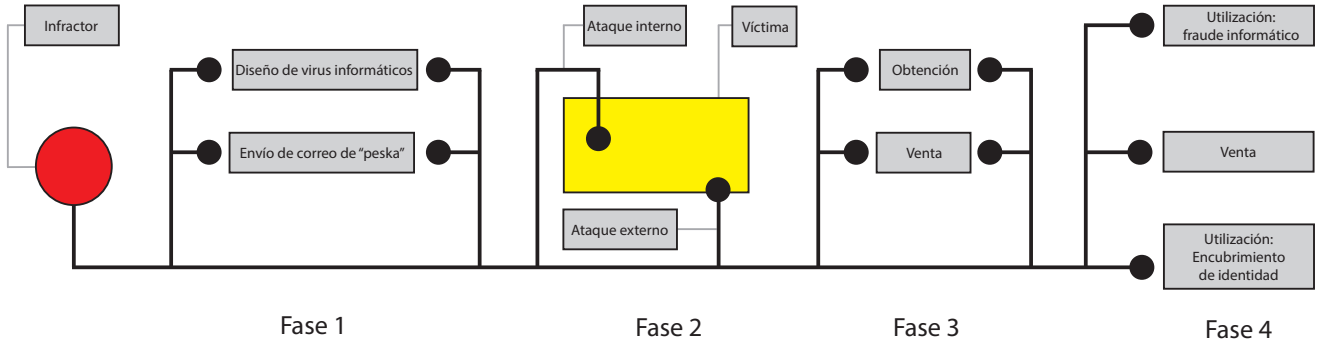
Cuatro elementos principales

La definición de los delitos relacionados con la identidad contiene en general cuatro categorías diferentes de elementos: el objeto (información relacionada con la identidad), los actos delictivos (que incluyen desde la obtención de la información hasta su utilización), el elemento de intencionalidad (que va desde el conocimiento hasta una intención especial) y, por último, la falta de autorización de la víctima. Se necesitan estos cuatro elementos para establecer una disposición de derecho penal en que se defina una estructura.

[162] Véase *supra*, capítulo 3.
[163] Véase *supra*, capítulo 4.
[164] En cuanto al riesgo de hurto de identidad relacionado con tales redes sociales, véase, *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, *supra* núm. 122, página 73.

Distinción de cuatro fases

Se pueden distinguir cuatro fases diferentes en la comisión de delitos relativos a la identidad[165]:



Fase 1

La primera fase se caracteriza por ser preparatoria. Utilizar el término preparatorio puede inducir a error puesto que a menudo ya existe una interacción con la víctima[166]. La tipificación del acto en la fase 1 permite abordar el problema de las actitudes nacionales divergentes sobre la configuración de los actos preparatorios en las primeras etapas de la conducta. El concepto jurídico de preparación plantea interrogantes sobre la forma en que cada legislación define y definirá el delito y las etapas preparatorias conexas.

Fase 2

En la segunda fase, los delincuentes obtienen la información relacionada con la identidad. Como se indicó anteriormente[167], existen varias maneras de conseguir la información.

Fase 3

La inclusión de la tercera fase responde al hecho de que la información relativa a la identidad no siempre es utilizada por el infractor que la obtuvo, sino que en primer lugar un grupo de delincuentes organizados la transfiere a otro[168].

Fase 4

En la última fase, los infractores utilizan la información relacionada con la identidad para cometer delitos u ocultar su verdadera identidad.

---

[165] El modelo fue elaborado por el autor del estudio en el contexto de un estudio sobre el hurto de identidad relacionado con Internet llevado a cabo para el Consejo de Europa en 2007. Véase *Gercke*, Internet-related Identity Theft – A Discussion Paper, Council of Europe, 2007.

[166] Esto es especialmente importante en los casos de peska. Con respecto a las diferentes fases de peska, véase OECD Scoping Paper on Online Identity Theft, *supra* núm. 13, página 18.

[167] Véase *supra*, capítulo 4.3.

[168] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, página 17, *Lex Electronica*, vol. 11, núm. 1, 2006, disponible en: http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf (última consulta: octubre de 2008); OECD Scoping Paper on Online Identity Theft, *supra* núm. 13, página 15.

3. La relación con la información de identidad existe, pero no hay cohesión

Uno de los pocos criterios comunes de los delitos relacionados con la identidad es una interacción con la información de identidad. Las muy variadas formas en que se cometen los actos no permiten hallar una única categoría que los englobe. En este contexto no resultan útiles los conceptos de "hurto de identidad" ni de "falsificación de identidad". Una de las principales preocupaciones[169] relacionadas con el uso de la expresión "hurto de identidad" reside en que los delincuentes casi nunca sustraen el elemento tangible (lo cual es un requisito esencial de la mayoría de las disposiciones penales relativas al robo en las distintas legislaciones)[170,171]. Aparte de cuestiones de orden dogmático, el término hurto o robo no es preciso porque la persona cuya propiedad se sustrae suele ser la única víctima, mientras que en los casos de hurto de identidad, la persona cuya información se utiliza indebidamente no siempre es la única víctima[172]. Tampoco es adecuada la expresión "falsificación de identidad" porque la motivación de los delincuentes que se apropian de información de identidad no siempre se relaciona con la falsificación. Si bien una expresión común podría ser útil, para examinar las soluciones jurídicas se recomienda diferenciar con mayor precisión los delitos relacionados con la identidad[173].

[169] Respecto de estas preocupaciones, véase *Koops*/*Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, *supra* núm. 141, página 553; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, 2008, página 8.

[170] En cuanto a los diferentes enfoques dogmáticos en el Derecho Romano, véase *Epstein*/*Brown*, Cybersecurity in the Payment Card Industry, *University of Chicago Law Review*, vol. 75, 2008, página 204.

[171] Véase *Ceaton*, The Cultural Phenomenon of Identity Theft…, *supra* núm. 8, página 13, con más referencias.

[172] Con respecto a la determinación de la víctima, véase Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, página 11; Identity Theft, Available Data Indicate Growth in Prevalence and Cost, Statement of *R. Stana*, Documento de la Oficina General de Contabilidad: GAO-02-424T, 2002, página 5; *Levi*/*Burrows*, Measuring the Impact of Fraud in the UK, *supra* núm. 22, página 12; *Elston*/*Stein*, International Cooperation in Online Identity Theft Investigations…, *supra* núm. 10, página 5.

[173] *Levi*/*Burrows*, Measuring the Impact of Fraud in the United Kingdom, *supra* núm. 22.

VI. ENFOQUES JURÍDICOS

La tipificación de los delitos relacionados con la identidad puede contribuir a dar una respuesta[174]. El presente capítulo contiene una reseña general de las discusiones sobre la importancia de una tipificación, los enfoques nacionales e internacionales, y determina los criterios fundamentales en la elaboración de una disposición de derecho penal para los delitos relativos a la identidad.

1. Argumentos a favor y en contra de un delito específico de hurto de identidad

Si bien varios países pueden enjuiciar a los autores de determinadas etapas de los delitos de hurto de identidad sobre la base de disposiciones penales tradicionales que se refieren al fraude y la falsificación, solo unos pocos Estados aplican disposiciones específicas que tipifican el hurto de identidad como un delito especial[175]. Así pues, es una solución que no se considera necesaria a nivel mundial. Una situación similar se observa en el debate académico. La principal razón por la cual los Estados deciden tipificar el hurto de identidad es el reconocimiento de que el delito primario del uso indebido de la identidad puede dar lugar a una variedad de delitos secundarios y, de esa forma, se habilita al sistema de justicia penal para que intervenga desde un principio[176].

2. Preocupaciones generales sobre la tipificación del hurto de identidad

La tipificación del hurto de identidad plantea problemas a algunos expertos[177]. Por ejemplo, Ceaton señala que la legislación sobre el hurto de identidad no resuelve el problema relacionado con dicho fenómeno, pero "sienta las bases del fenómeno cultural del hurto

[174] Una visión general de otros enfoques de la prevención y la lucha contra el hurto de identidad figura *supra* en el capítulo 1, así como en OECD Policy Guidance on Online Identity Theft, 2008.

[175] Una visión general sobre la legislación relacionada con el hurto de identidad en Europa figura en: *Owen*/*Keats*/*Gill*, The Fight Against Identity Fraud: *supra* núm. 159; *Mitchison*/*Wilikens*/*Breitenbach*/*Urry*/*Portesi*, Identity Theft – A discussion paper, *supra* núm. 138, página 23 y ss.; Legislative Approaches To Identity Theft…, *supra* núm. 159. Para consultar una reseña de la legislación de Australia, los Estados Unidos y el Reino Unido, véase Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31; sobre la penalización en los Estados Miembros de la OCDE, véase OECD Scoping Paper on Online Identity Theft, *supra* núm. 13.

[176] Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, *supra* núm. 10, página 3.

[177] Véase *Ceaton*, The Cultural Phenomenon of Identity Theft…, *supra* núm. 8, página 13 y ss.

de identidad –o lo que también se ha llamado el mito del hurto de identidad– que a su vez actúa como un sólido instrumento para racionalizar la web, así como para que la identidad sea operacional. [...] Así pues, ciudadanos que de otra forma podrían cuestionar la conveniencia de reducir la identidad a una información cuantificable, que luego se concentra en algunas burocracias masivas, por el contrario se preocupan por triturar sus documentos antes de deshacerse de los mismos".

Si bien la crítica fundamental se refiere al derecho penal, en general se centra en soluciones jurídicas. Ceaton, al igual que la mayoría de los expertos, hace hincapié en que las soluciones jurídicas no pueden ser el único fundamento de una estrategia encaminada a limitar el hurto de identidad. Ya se ha señalado[178] que para elaborar la estrategia es preciso tener en cuenta varios elementos. Sin embargo, por ello no necesariamente quedan excluidas las medidas jurídicas[179]. A fin de prevenir un comportamiento que conlleva perjuicios para miembros de la sociedad o Estados puede ser legítimo e incluso necesario decidir la aplicación de disposiciones penales.

3. Aplicabilidad de las disposiciones tradicionales del derecho penal

En general, el hurto de identidad nunca es un delito aislado[180]. Como se subrayó anteriormente, se utiliza la expresión hurto de identidad para indicar una combinación de diferentes actos[181], que abarcan desde el hurto de documentos de identidad hasta el uso fraudulento de información sobre la identidad. Al estudiar los llamados casos de "hurto de identidad", suele observase que delitos tradicionales como el fraude con tarjetas de crédito se califican simplemente de "hurto de identidad"[182]. En la mayoría de los países es larga la historia de la penalización de los delitos de hurto y de fraude. Basándose en los estudios mencionados, la mayoría de los delitos relativos a la identidad se realizan con la intención de cometer un fraude, en cuyo caso sus autores pueden ser procesados generalmente en el marco de las disposiciones penales tradicionales.

Incluso en los casos de hurto de identidad relacionados con Internet, para poder proceder al enjuiciamiento no es indispensable utilizar una denominación específica[183]. En los diez últimos años, muchos países actualizaron sus leyes para penalizar delitos informáticos, como el fraude informático y el acceso ilegal a sistemas informáticos. Habida cuenta de la dimensión transnacional de muchos delitos cibernéticos[184], así como de las diferentes normativas de los países interesados que son susceptibles de entorpecer la labor de

[178] Véase *supra*, capítulo 1.
[179] *Van der Meulen*, The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom and the European Union, Report commissioned by the National Infrastructure Cybercrime Programme (NICC), páginas 25 y 26; FIDIS, deliverable 5.3: A Multidisciplinary Article on Identity-related Crime, páginas 25 y 26; FIDIS, deliverable 5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, páginas 116 y 117.
[180] Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, *supra* núm. 20, página 2.
[181] Véase *supra*, capítulo 4.
[182] *Levi*, Combating Identity and Other Forms of Payment Fraud in the United Kingdom…, *supra* núm. 55.
[183] *Gercke*, Internet-related Identity Theft, *supra* núm. 165.
[184] Acerca del alcance de los ataques cibernéticos transnacionales más perjudiciales, véase *Sofaer/Goodman*, Cyber Crime and Security, *supra* núm. 11, página 7.

investigación[185], varias organizaciones internacionales han centrado su atención en este tema. Su propósito es armonizar las distintas legislaciones nacionales y organizar la cooperación internacional[186]. Una iniciativa importante ha sido el Convenio sobre el delito cibernético del Consejo de Europa, firmado en octubre de 2008 por 45 países[187], que ha servido para armonizar las leyes sin necesidad de una firma formal[188]. Este Convenio contiene varias disposiciones penales sustantivas para tipificar actos que normalmente forman parte de las estafas relativas a la identidad realizadas a través de Internet, como el acceso ilegal (artículo 2) y el uso indebido de dispositivos (artículo 6)[189].

Sin embargo, pese a la aplicabilidad general de las disposiciones penales tradicionales sustantivas, determinados delitos relacionados con la identidad no están comprendidos en esas disposiciones ni en los instrumentos internacionales, como el Convenio mencionado. Un ejemplo es la transferencia y la venta de información relacionada con la identidad[190]. Si bien la obtención de dicha información y su utilización en actividades fraudulentas podrían tipificarse como hurto y fraude, delitos como el intercambio y la comercialización de esa información no son objeto de un reconocimiento amplio ni tampoco se abordan integralmente en el Convenio sobre el delito cibernético. La adopción de una disposición penal específica podría contribuir a subsanar esas deficiencias normativas.

4. Definición precisa del objeto de la protección jurídica

Como se ha señalado, la información relacionada con la identidad cumple un importante papel en la vida social. La mayoría de las disposiciones penales tradicionales que podrían aplicarse para el enjuiciamiento en relación con determinados aspectos de delitos como el fraude y la falsificación de la identidad no fueron concebidas para proteger la información relativa a la identidad, sino que tienen en cuenta otros valores fundamentales, como la confianza del mercado en la fiabilidad de los documentos. Si el legislador dispusiera de un criterio específico para tipificar el hurto de identidad podría responder al creciente interés que promueve la información relativa a la identidad, mediante la adopción de una disposición penal que la proteja jurídicamente.

---

[185] Esas dificultades han radicado con frecuencia en el requisito de la doble incriminación. Respecto al principio de la doble incriminación véase: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, *Brigham Young University Law Review*, 1992, página 191 y ss., disponible en: http://lawreview.byu.edu/archives/1992/1/haf.pdf (última consulta: octubre de 2008).

[186] Para tener una visión general sobre las tendencias recientes, véase *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, página 7 y ss.

[187] La lista de los países firmantes y ratificantes se encuentra disponible en el sitio web del Consejo de Europa, http://www.coe.int.

[188] Acerca del Convenio, véase *Sofaer*, Toward an International Convention on Cyber Security in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, página 225, disponible en: http://media.hoover.org/documents/0817999825_221.pdf (última consulta: octubre de 2008); *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, CRi, 2006, página 140 y ss.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, *supra* núm. 186, página 7 y ss.; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, *Entertainment Law Review*, 2002, núm. 1, disponible en: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf (última consulta: octubre de 2008); *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, disponible en: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf (última consulta: octubre de 2008); *Broadhurst*, Development in the Global Law Enforcement of Cyber-Crime, in *Policing: An International Journal of Police Strategies and Management*, vol. 29, núm. 2, 2006, página 408 y ss.; Adoption of Convention on Cybercrime, *International Journal of International Law*, vol. 95, núm. 4, 2001, página 889 y ss.

[189] Un análisis más exhaustivo de la aplicación de las disposiciones mencionadas en el Convenio sobre el delito cibernético con respecto a los delitos relacionados con la identidad figura en: *Gercke*, Internet-related Identity Theft, *supra* núm. 165, página 23 y ss.

[190] *Ibid.*, página 27.

5. Aspectos prácticos relacionados con la investigación

Ya hemos indicado que el hurto de identidad no suele ser un delito aislado[191]. Su tipificación habilitaría a los organismos encargados de hacer cumplir la ley a procesar al autor del primer acto delictivo. Con ello se facilitaría la identificación del infractor, y de esa manera se evitaría que cometiera otros delitos[192].

6. Incompatibilidad de las dimensiones nacional e internacional

Los delitos de hurto de identidad tienen con frecuencia una dimensión transnacional[193]. Dada la participación de grupos de delincuentes organizados, es muy probable que persista la tendencia a la globalización de los delitos[194]. La dimensión transnacional plantea problemas en relación con los criterios nacionales de tipificación del hurto de identidad. El hecho de que las diferentes normas nacionales pueden obstaculizar las investigaciones internacionales hace que se dé prelación a los instrumentos internacionales sobre los nacionales, o al menos a que se los considere complementarios. Sin embargo, en la actualidad se carece de instrumentos jurídicos de alcance internacional. En consecuencia, por el momento la incompatibilidad que podría existir entre las soluciones nacionales y las internacionales solo existe en la teoría.

7. Enfoques internacionales

En la actualidad, solo se establecen marcos jurídicos nacionales para tipificar el hurto de identidad[195]. Hasta el momento, ninguna de las organizaciones internacionales que se ocupan de temas relacionados con el derecho penal ha preparado instrumentos legislativos especiales sobre el hurto de identidad que contengan disposiciones para tipificar los actos pertinentes. Si bien, por un lado, no existen normas penales de alcance mundial, por otro, las organizaciones internacionales y regionales han intensificado sus actividades en este ámbito.

---

[191] Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, *supra* núm. 20, página 2.

[192] Identity Fraud: A Study, United Kingdom Cabinet Office, 2002, página 5, disponible en: http://www.ips.gov.uk /identity/downloads/ id-fraud-report.pdf (última consulta: octubre de 2008).

[193] *Elston*/*Stein*, International Cooperation in Online Identity Theft Investigations…, *supra* núm. 10.

[194] Con respecto a las dimensiones del crimen organizado, véase, *McCusker*, Transnational Organized Cybercrime: Distinguishing Threat From Reality, *Crime Law Social Change*, vol. 46, página 273; *Choo*/*Smith*; Criminal Exploitation of Online Systems by Organized Crime Groups, *Asian Criminology*, 2008, página 37 y ss.; Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, *supra* núm. 10, página 11.

[195] Puede consultarse una reseña de la legislación relacionada con el hurto de identidad en Europa en *Owen*/*Keats*/*Gill*, The Fight Against Identity Fraud…, *supra* núm. 159; *Mitchison*/*Wilikens*/*Breitenbach*/*Urry*/*Portesi* – Identity Theft, *supra* núm. 138; Legislative Approaches To Identity Theft…, *supra* núm. 159; para una reseña general de la legislación en Australia, los EE.UU. y el Reino Unido, véase: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, 2007. Respecto de la penalización en los Estados Miembros de la OCDE, véase, OECD Scoping Paper on Online Identity Theft, *supra* núm. 13.

Las Naciones Unidas

Los problemas planteados por los delitos relacionados con la identidad han cobrado una importancia primordial en el programa de prevención del delito y justicia penal de las Naciones Unidas. En la Declaración de Bangkok sobre "Sinergias y repuestas: alianzas estratégicas en materia de prevención del delito y justicia penal"[196], aprobada por la Asamblea General en su resolución 60/177, de 16 de diciembre de 2005, se destacó la importancia fundamental de combatir la falsificación de documentos y de identidad a fin de poner freno a la delincuencia organizada y el terrorismo[197]. También se exhortó a los Estados Miembros a "mejorar la cooperación internacional, incluso a través de la asistencia técnica, para combatir la falsificación de documentos y de identidad, en particular la utilización fraudulenta de documentos de viaje, mejorando las medidas de seguridad", así como a aprobar una legislación nacional apropiada"[198].

De conformidad con la resolución 2004/26 del Consejo Económico y Social (ECOSOC), la UNODC encargó la preparación de un estudio sobre "el fraude y la falsificación de identidad y su uso indebido con fines delictivos", que fue publicado a principios de 2007[199]. El estudio siguió un enfoque más amplio que el adoptado por la OCDE. En primer lugar, la expresión general "delitos relacionados con la identidad" abarca toda clase de conductas ilícitas relacionadas con la identidad, incluidos los delitos de "falsificación de identidad" y "hurto de identidad". En segundo lugar, se consideraron todos actos delictivos relacionados con el hurto de identidad, cometidos por medio de Internet o de otra forma, haciendo más hincapié en delitos y pautas más complejos debido a los vínculos existentes con la delincuencia organizada transnacional y otras actividades delictivas. Por último, los delitos relacionados con la identidad fueron considerados conjuntamente con el fraude, debido a su estrecha relación, así como a las instrucciones específicas al respecto del mandato del ECOSOC.

En el informe del Secretario General sobre las recomendaciones para una estrategia mundial de lucha contra el terrorismo se destaca la importancia de diseñar mecanismos para combatir el hurto de identidad en el marco de la lucha contra el terrorismo[200]. Además, en varias resoluciones de las Naciones Unidas se mencionan los problemas relacionados con el hurto de identidad, así como la necesidad de una respuesta apropiada. Un ejemplo de ello es la resolución sobre el fortalecimiento del programa de las Naciones Unidas en materia de prevención del delito y justicia penal[201] en que se señala el hurto de identidad

---

[196] La Declaración de Bangkok sobre "Sinergias y repuestas: alianzas estratégicas en materia de prevención del delito y justicia penal", 2005, aprobada por la Asamblea General en su resolución 60/177, de 16 de diciembre de 2005, se encuentra disponible en: http://www.un.org/events/11thcongress/declaration.htm (última consulta: octubre de 2008).

[197] Con respecto a los vínculos que existen entre los delitos relacionados con la identidad y el crimen organizado y el terrorismo, véase, Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, *supra* núm. 10, página 11.

[198] Declaración de Bangkok sobre "Sinergias y repuestas: alianzas estratégicas en materia de prevención del delito y justicia penal", 2005, párrafo 27.

[199] El informe con los resultados y conclusiones del estudio sobre "el fraude y la falsificación de identidad y su uso indebido con fines delictivos" fue presentado a la Comisión de Prevención del Delito y Justicia Penal en su 16º período de sesiones (E/CN.15/2007/8 y Add.1 a 3).

[200] Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo, 27 de abril de 2006 (A/60/825), página 13.

[201] Resolución de la Asamblea General de las Naciones Unidas titulada Fortalecimiento del Programa de las Naciones Unidas en materia de prevención del delito y justicia penal, en particular de su capacidad de cooperación técnica, A/RES/62/175, 2008, página 3.

como una de las nuevas cuestiones de política que debe ser examinada por la UNODC. Sobre la base de las resoluciones 2004/26[202] y 2007/20[203] del ECOSOC, la UNODC estableció un grupo de expertos para que intercambiaran opiniones sobre la mejor forma de proceder en este ámbito[204].

Organización de Cooperación y Desarrollo Económicos (OCDE)

En 1999, el Consejo de la OCDE aprobó un conjunto de directrices con miras a proteger el comercio electrónico[205] que contenían medidas para la elaboración de estrategias de prevención del hurto de identidad. Dado su carácter no vinculante, las directrices no contenían criterios que permitieran tipificar los aspectos específicos del hurto de identidad. En 2003, la OCDE elaboró otras directrices sobre aspectos del fraude transfronterizo[206]. Al igual que las directrices de 1999, las de 2003 no abordaban específicamente un criterio para tipificar el hurto de identidad, pero se podían utilizar para elaborar un marco más amplio que permitiera llevar a cabo investigaciones eficaces y procesar a los delincuentes. En 2008, la OCDE publicó un estudio sobre el hurto de identidad en línea (*Scoping Paper on Online Identity Theft*)[207], que además de analizar en detalle las diferentes estafas relacionadas con el hurto de identidad realizadas a través de Internet, abordaba cuestiones relacionadas con las víctimas, y los ámbitos de aplicación de la ley. También en 2008, la OCDE publicó un documento titulado "Policy Guidance on Online Identity Theft"[208], que daba una perspectiva general de las diferentes estrategias para responder al hurto de identidad relacionado con Internet.

La Unión Europea

La Unión Europea ha elaborado diferentes instrumentos jurídicos que abordan la información relacionada con la identidad, como la Directiva de la UE sobre la privacidad[209], así como la tipificación de determinados aspectos del fraude[210] y los delitos relacionados

[202] Resolución 2004/26 del ECOSOC sobre la cooperación internacional en materia de prevención e investigación del fraude, la falsificación de identidad y su uso indebido con fines delictivos y los delitos conexos y enjuiciamiento y castigo de sus autores.

[203] Resolución 2007/20 del ECOSOC sobre la cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad.

[204] Los informes relacionados con las actividades del grupo básico de expertos se encuentran a disposición del público. Véase: Primera reunión del Grupo básico de expertos sobre delitos relacionados con la identidad, celebrada en Cormier Mont Blanc (Italia), del 29 al 30 de noviembre de 2007, disponible en: http://www.unodc.org/documents/organized-crime/Courmayeur_report.pdf (última consulta: octubre de 2008); Segunda reunión del Grupo básico de expertos sobre delitos relacionados con la identidad, celebrada en Viena (Austria), 2 y 3 de junio de 2008, disponible en: http://www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf (última consulta: octubre de 2008).

[205] Directrices de la OCDE para la Protección de los Consumidores en el Contexto del Comercio Electrónico, disponible en: http://www.oecd.org/dataoecd/18/13/34023235.pdf (última consulta: octubre de 2008).

[206] Directrices de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, disponible en: http://www.oecd.org/document/56/0,3343,en_2649_34267_2515000_1_1_1_1,00.html.

[207] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL.

[208] OECD Policy Guidance on Online Identity Theft, 2008.

[209] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[210] Decisión Marco del Consejo 2001/413/JAI, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

con Internet, como el acceso ilegal a los sistemas informáticos[211]. No obstante, ninguno de ellos contiene disposiciones penales que aborden específicamente el hurto de identidad.

Sin embargo, las dificultades que plantean las actividades delictivas conexas ya han sido reconocidas a nivel de la Unión Europea como una importante cuestión normativa[212]. Por su parte, la Comisión Europea indicó que "la cooperación policial y judicial en el seno de la Unión Europea se vería facilitada si el hurto de identidad se tipificara como delito en todos los Estados miembros"[213]. Esta propuesta allanó el camino para celebrar consultas con objeto de determinar si era necesario y conveniente que los Estados miembros promulgaran leyes específicas en la materia, ya que es razonable prever un creciente interés de la opinión pública europea por una prevención eficaz de los delitos relativos a la identidad. En julio de 2007, la Comisión (DG Justicia, Libertad y Seguridad) inició un estudio comparativo sobre las definiciones de la expresión "hurto de identidad" utilizadas en los Estados miembros de la UE y sus consecuencias penales[214].

Consejo de Europa

En 2001, el Convenio sobre el delito cibernético del Consejo de Europa quedó abierto para la firma[215]. En la ceremonia, 30 países firmaron el Convenio (incluidos los cuatro países no miembros del Consejo de Europa y que habían participado en las negociaciones: el Canadá, los Estados Unidos de América, el Japón y Sudáfrica). En octubre de 2008, 45 Estados[216] habían firmado el instrumento y 23 lo habían[217] ratificado[218]. El Convenio, que contiene disposiciones sustantivas para tipificar actos como el acceso ilegal a sistemas informáticos o la interferencia de los sistemas, es considerado actualmente un instrumento

[211] Decisión Marco del Consejo 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información; para más información, véase: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, página 468 y ss.

[212] En el marco de la campaña de concienciación para mejorar la prevención del hurto de identidad y el fraude de pago, la Dirección General de Justicia, Libertad y Seguridad (DG JLS) y la Dirección General del Mercado Interior de la Comisión Europea organizaron una conferencia titulada "Maintaining the integrity of identities and payments: Two challenges for fraud prevention", celebrada en Bruselas, del 22 al 23 de noviembre de 2006. En la Conferencia se procuró recalcar la importancia de una participación más amplia de los responsables de formular políticas y de los altos representantes de las administraciones nacionales, así como de proporcionar una plataforma para que los responsables de formular políticas pudieran examinar las posibles iniciativas de la UE al respecto. Entre los temas abordados en la Conferencia figuraron una posible legislación penal de la UE sobre el hurto de identidad, modelos de formación para la aplicación de la ley/investigadores financieros, el intercambio de información y cuestiones relativas a la privacidad.

[213] Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones –Hacia una política general de lucha contra la ciberdelincuencia", COM(2007)267, de 22 de mayo de 2007.

[214] Una vez finalizado, este estudio incluirá recomendaciones sobre las mejores prácticas.

[215] Con respecto al Convenio, véase, *Sofaer*, Toward an International Convention on Cyber Security, *supra* núm. 188, página 225; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, *ibid*, página 140 y ss.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, *supra* núm. 186, página 7 y ss.; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, *supra* núm. 188; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, disponible en: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf (última consulta: octubre de 2008); *Broadhurst*, Development in the Global Law Enforcement Of Cyber-Crime, *supra* núm. 188, página 408 y ss.; Adoption of Convention on Cybercrime, *ibid*, página 889 y ss.

[216] Albania, Alemania, Armenia, Austria, Azerbaiyán, Bélgica, Bosnia y Herzegovina, Bulgaria, Canadá, Croacia, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Estonia, ex República Yugoslava de Macedonia, Finlandia, Francia, Georgia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, Moldova, Montenegro, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumania, Serbia, Sudáfrica, Suecia, Suiza y Ucrania.

[217] Albania, Armenia, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Eslovaquia, Eslovenia, Estados Unidos, Estonia, ex República Yugoslava de Macedonia, Finlandia, Francia, Hungría, Islandia, Italia, Letonia, Lituania, Noruega, Países Bajos, Rumania y Ucrania.

[218] La ratificación del Convenio es necesaria conforme a lo dispuesto en su artículo 36.

importante en la lucha contra el delito cibernético y cuenta con el apoyo de diferentes organizaciones internacionales[219].

En 2007, el Consejo de Europa publicó un estudio en que se analizaban los diferentes criterios de la tipificación del hurto de identidad relacionado con Internet. Se ponía de relieve que, si bien las disposiciones del Convenio sobre el delito cibernético eran aplicables en los casos de hurto de identidad, no había disposiciones específicas que abordaran el hurto de identidad en sí que fueran aplicables a todos los actos conexos[220].

8. Enfoques nacionales

Hemos indicado que algunos países ya han aplicado disposiciones que trascienden los criterios tradicionales de tipificación de la falsificación o el fraude, y que se centran especialmente en los actos relacionados con el hurto de identidad.

Estados Unidos

En 1998, los Estados Unidos introdujeron la disposición 18 U.S.C. § 1028 a) 7) que tipificaba específicamente los actos relacionados con el hurto de identidad[221]. Comprende diversos delitos relacionados con el hurto de identidad. En 2004, se introdujeron sanciones por hurto de identidad agravado. En 2007, se presentó un proyecto de ley relativo a la aplicación y resarcimiento en caso de hurto de identidad que procuraba subsanar las deficiencias de la legislación. Recientemente la ley fue aprobada en el Senado de los Estados Unidos pero aún no ha entrado en vigor:

> *1028. Fraude y actividades relacionadas con documentos de identificación, características de autenticación e información*
>
> *a)* Quien, en la circunstancia descrita en el inciso *c)* de este artículo:
>
> [...]

[219] En la Resolución de la 6ª Conferencia Internacional sobre Delito Cibernético, celebrada en El Cairo, la Interpol destacó la importancia del Convenio sobre el delito cibernético, en los siguientes términos: "Que se utilice el Convenio sobre Ciberdelincuencia del Consejo de Europa como referencia en materia de normas internacionales procedimentales y legales mínimas para la lucha contra la ciberdelincuencia. Se instará a los países a suscribirlo. Este Convenio se distribuirá a todos los países miembros de Interpol en los cuatro idiomas oficiales", disponible en: http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp (última consulta: octubre de 2008); el Programa de Túnez de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) de 2005 dice en el párrafo 40: "Instamos a los gobiernos a que, en cooperación con otras partes interesadas, promulguen leyes que hagan posible la investigación y enjuiciamiento de la ciberdelincuencia, respetando los marcos existentes, por ejemplo, las resoluciones de la Asamblea General de las Naciones Unidas 55/63 y 56/121 sobre la "Lucha contra la utilización de la tecnología de la información con fines delictivos" y el Convenio sobre el delito cibernético del Consejo de Europa", disponible en: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_ agenda.pdf (última consulta: octubre de 2008).

[220] *Gercke*, Internet-related Identity Theft, *supra* núm. 165.

[221] Identity Theft and Assumption Deterrence Act 1998. Para una más amplia información sobre la ley, véase *Zaidi*, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada, *Loyola Consumer Law Review*, vol. 19, issue 2, página 99 y ss.; *Finkelstein*, Memorandum for Assistant Regional Council on Identity Theft and Assumption Deterrence Act of 1998, 1999, disponible en: http://www.unclefed.com/ForTaxProfs/irs-wd/1999/9911041.pdf; *Gordon/Willox/Rebovich/Regan/Gordon*, Identity Fraud: A Critical National and Global Threat, Journal of Economic Management, 2004, vol. 2, issue 1.

(7) Transfiera, posea o utilice, sin autorización legítima, un medio de identificación de otra persona con la intención de cometer, o ayudar a cometer cualquier actividad ilícita o relacionada con ésta que constituya una violación de la legislación federal, o constituya un delito en virtud de las leyes estatales o locales; o

[...]

será sancionado conforme a lo previsto en el inciso *b)* de este artículo.

1028A. Hurto de identidad agravado

a) Delitos:

1) En general, quien, durante y en relación con uno de los delitos graves enumerados en el inciso *c)*, de manera intencional, transfiera, posea o utilice sin autorización legítima, medios de identificación de otra persona deberá, además de ser objeto de la sanción prevista para ese delito, ser condenado a dos años de prisión.

Como ya se ha destacado, es una disposición de amplio alcance para tipificar varias formas de hurto de identidad. Al penalizar la "transferencia" de medios de identificación con la intención de cometer un delito, la disposición permite el enjuiciamiento correspondiente en relación con la fase 3 mencionada *supra*, que no suele figurar en los enfoques tradicionales. No obstante, como las disposiciones 18 U.S.C. § 1028 a) 7) y 18 U.S.C. 1028A a) 1) se centran en la interacción directa con datos relativos a la identidad, no abarcan los actos preparatorios, tales como el envío de correos electrónicos de *peska* y el diseño de programas malignos que podrían servir para obtener información de identidad. La ley sobre la aplicación y resarcimiento en caso de hurto de identidad, de 2007, procura subsanar esas deficiencias, por ejemplo, tipificando los actos relacionados con *spyware* (programas informáticos de espionaje) y *keyloggers* (registro de pulsaciones del teclado).

Canadá

En 2007, el Canadá introdujo un proyecto de ley para configurar un delito específico relacionado con el hurto de identidad[222]. El proyecto de ley contiene dos importantes disposiciones: la 402.1 define la información relacionada con la identidad, y la 402.2 se refiere a los actos tipificados.

402.1

A los efectos de los artículos 402.2 y 403, se entenderá por la expresión "información de identidad" toda información –incluida la información biológica y psicológica– que pueda utilizarse por separado o conjuntamente con otra información para identificar o intentar identificar a una persona, como ser huellas digitales, huella vocal, imagen

[222] Véase, http://www.parl.gc.ca/LEGISINFO/index.asp?List=ls&Query=5333&Session=15&Language=e#idtheft (última consulta: octubre de 2008). En octubre de 2009, se adoptó el proyecto de ley S-4 como una enmienda al Código Penal canadiense (hurto de identidad y el uso indebido conexo).

de la retina, imagen del iris, ADN, nombre, dirección, fecha de nacimiento, firma escrita, firma electrónica, firma digital, nombre de usuario, número de tarjeta de crédito o de débito, número de cuenta de una institución financiera, número de pasaporte, número de seguridad social, número de seguro de salud, número del permiso de conducir o clave de acceso.

402.2

1) Comete un delito quien, de forma intencional, obtenga o posea información de identidad de otra persona en circunstancias que razonablemente permitan inferir que será utilizada para cometer un delito que incluye el fraude, el engaño o la mentira como elementos del delito.

2) Comete un delito quien transmita, ponga a disposición, distribuya, venda u ofrezca en venta información de identidad de otra persona, o la posea con algunos de estos propósitos, si tiene la certeza de que esa información será utilizada para cometer un delito que incluye el fraude, el engaño o la mentira como elementos del delito, o si incurre en imprudencia.

3) A los efectos de los incisos 1) y 2), un delito punible mencionado en cualquiera de esos incisos incluye un delito en virtud de cualquiera de los siguientes artículos:
   a) artículo 57 (falsificación o expedición de pasaporte falso);
   b) artículo 58 (utilización fraudulenta de certificados de nacionalidad);
   c) artículo 130 (suplantación de un agente de policía);
   d) artículo 131 (falso testimonio);
   e) artículo 342 (robo, falsificación, etc., de una tarjeta de crédito);
   f) artículo 362 (declaración falsa o fraudulenta);
   g) artículo 366 (falsificación);
   h) artículo 368 (expedición, tráfico o posesión intencionales de documentos falsos);
   i) artículo 380 (fraude); y
   j) artículo 403 (falsificación de identidad).

El proyecto de ley contiene una serie de elementos interesantes. En primer lugar, proporciona ejemplos de la información de identidad a que se refiere, sin restringir su aplicación[223]. Además, enumera una serie de delitos, lo cual si bien reduce la aplicabilidad es fuente de gran precisión. Por último, abarca una gran variedad de delitos. Al igual que en el enfoque de los Estados Unidos, el proyecto de ley canadiense no comprende los actos preparatorios como el envío de correos electrónicos de *peska*, ni el diseño de programas informáticos malignos[224].

[223] Las palabras "como ser" en la disposición 402.1 dan lugar a una interpretación amplia cuando fuera necesario, por ejemplo, en razón de la evolución tecnológica.

[224] Esto no significa necesariamente que esos actos no sean tipificados en distintas disposiciones.

9. Elementos esenciales de un enfoque jurídico

Una respuesta jurídica al hurto de identidad que no se limite a una adaptación de los instrumentos tradicionales y que consista en elaborar una disposición específica requiere previamente la adopción de varias decisiones y ajustes. A continuación se reseñan los elementos esenciales pertinentes.

Identidad

Es necesario definir la información de identidad protegida. El acceso de manera ilícita a una computadora para obtener información comercial confidencial configura un delito relativo a la información digital. Sin embargo, no se considera un delito relacionado con la identidad porque no existe un vínculo con información relacionada con la identidad. En la definición, es necesario tener en cuenta los siguientes aspectos.

Alcance de la definición

Es necesario decidir el alcance, más amplio o más preciso, de la definición de información relacionada con la identidad[225]. La decisión depende del sistema jurídico subyacente, de la tradición jurídica, y de la importancia regional de determinados datos relacionados con la identidad[226]. Si bien una enumeración suele ser más precisa, se corre el riesgo de que su aplicación resulte difícil si se producen transformaciones tecnológicas fundamentales.

Algunos datos digitales, como contraseñas, nombres de cuentas e información de acceso, pueden no considerarse elementos de la identidad jurídica de una persona. Sin embargo, teniendo en cuenta el uso de ciertos datos para acceder a los servicios digitales[227], es necesario decidir si esa información debe incluirse en la definición[228].

Identidades sintéticas

Además, es necesario determinar si deben considerarse solo los actos relacionados con identidades reales, o si se debería incluir el uso de información relacionada con una identidad ficticia[229]. Como ya se ha dicho, a primera vista no parece ser apropiado tipificar como delito el uso de identidades ficticias, como en los casos que no tienen consecuencias para el usuario legítimo de una identidad. No obstante, el hecho de que el acto no afecte a una persona física no significa que no cause un daño. La utilización de identidades sintéticas por los delincuentes puede entorpecer las tareas de investigación y dificultar su identificación[230]. Una gran parte de los

[225] En favor de un enfoque más amplio, véase, Discussion Paper Identity Crime, Model Criminal Law Officers' Committee *supra* núm. 31, página 25.

[226] Un ejemplo es el número de la seguridad social (NSS), que es muy importante en los Estados Unidos pero no en Europa. Con respecto al NSS, véase *Sobel*, The Demeaning of Identity and Personhood in National Identification Systems, *Harvard Journal of Law & Technology*, vol. 15, núm. 2, 2002, página 350.

[227] Véase *supra* capítulo 3.2.4.

[228] Paget, Identity Theft, McAfee White Paper, página 4, 2007, disponible en: http://www.mcafee.com/us/threat_center/white_paper.html (última consulta: octubre de 2008).

[229] Para hacerse una idea general de los argumentos en favor de la inclusión de identidades sintéticas, véase Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, página 25.

[230] Respecto de las identidades sintéticas relacionadas con el hurto de identidad, véase Schneier, Synthetic Identity Theft, 05.11.2007, disponible en: http://www.schneier.com/blog/archives/2007/11/synthetic_ident.html (última consulta: octubre de 2008); *McFadden*, Detecting Synthetic Identity Fraud, disponible en: http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp (última consulta: octubre de 2008).

casos de fraude no están basados en identidades verdaderas, sino en identidades sintéticas[231]. Los resultados de un estudio llevado a cabo por ID Analytics, mostraron que en menos del 15% de todos los casos se utilizaron identidades verdaderas[232]. Las identidades sintéticas pueden basarse únicamente en datos generados o ser una combinación de datos generados y reales[233]. Por lo tanto, en el proceso de redacción de las disposiciones es necesario decidir si la interferencia con una identidad existente es un requisito necesario para la tipificación.

Actos y fases

En segundo lugar, es necesario determinar los actos que deberían tipificarse como delitos. La distinción entre las cuatro fases expuestas *supra* podría ayudar a prevenir tanto carencias como superposiciones.

Fase 1 (actos preparatorios)
En general, todos aquellos delitos que no se cometen espontáneamente requieren una etapa preparatoria que con frecuencia no es un acto penalizado. Con respecto a los delitos relacionados con la identidad, es preciso decidir si los actos preparatorios, como el diseño de programas informáticos malignos o el envío de correos electrónicos de *peska*, deberían ser tipificados como delitos. El hecho de que los autores del Convenio sobre el delito cibernético incluyeran una disposición sobre la penalización del diseño de programas informáticos para cometer determinados delitos relacionados con las computadoras, como el acceso ilegal a sistemas informáticos, demuestra que existe una tendencia a tipificar los actos preparatorios. Por otra parte, es un criterio que suscita preocupaciones relativas a una posible penalización excesiva. Los actos relacionados con la fase 1 podrían no tipificarse, especialmente si el sistema de derecho penal nacional no reconoce generalmente como delitos los actos preparatorios.

Fase 2 (obtención de la información)
La obtención de información relacionada con la identidad es un aspecto ampliamente aceptado del delito de hurto de identidad. Los delincuentes utilizan diferentes métodos para hacerse con la información. Los enfoques nacionales mencionados más arriba abarcan los diversos métodos y tipifican como delito la "obtención" y la "transferencia" de información relacionada con la identidad.

En este contexto, es necesario tener en cuenta dos situaciones concretas. En primer lugar, varias estafas relacionadas con el hurto de identidad se basan en la revelación por la propia víctima de información sobre su identidad gracias a la acción de mecanismos de ingeniería social que se imponen a la víctima sin que esta lo advierta. En esos casos, es probable que las disposiciones que incluyan el acto de "obtener" puedan aplicarse más fácilmente si se compara con las disposiciones que requieren la

[231] Véase ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf (última consulta: octubre de 2008).
[232] *Ibid.*
[233] Véase 2007 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 2007, página 10, disponible en: http://www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf (última consulta: octubre de 2008).

"transferencia" por el infractor de información relacionada con la identidad. La segunda situación, en que podrían observarse dificultades similares, es la obtención de información relacionada con la identidad, que pertenece al dominio público.

Fase 3 (proceso de transferencia)
La fase 3 se caracteriza por una transferencia de la información relacionada con la identidad[234]. Los criterios que incluyen actos como la transferencia o, más concretamente, la transmisión o venta de información son generalmente aplicables en estos casos. En los países cuya legislación no reconoce efectivamente delitos específicos relacionados con el hurto de identidad y que, por tanto, recurren a disposiciones penales tradicionales sobre el fraude y la falsificación, el procesamiento de los autores de este tipo de actos es relativamente más difícil.

Fase 4 (uso con fines delictivos)
Las motivaciones de los delincuentes que se apoderan y utilizan la información relacionada con la identidad son tan variadas como los métodos utilizados para su obtención. En general, existen dos criterios diferentes relacionados con la tipificación de los actos de esta fase. Las formas más corrientes de utilizar la información relacionada con la identidad (por ejemplo, cometer un fraude) ya están previstas en las disposiciones penales tradicionales, pero algunos enfoques no incluyen los actos relacionados con la fase 4, sino tan solo un vínculo con esos delitos en la medida en que exigen la intención de cometer el acto delictivo[235]. Otros enfoques tipifican el acto de utilizar la información relacionada con la identidad (con la intención de cometer una actividad ilegal) además del propio delito.

Sin autorización o ilegalmente

Es necesario decidir si la tipificación requiere que el delincuente actúe sin el consentimiento de la persona de cuya información de identidad se trata. En general, deben excluirse los actos autorizados y legítimos a fin de garantizar que la tipificación del delito de hurto de identidad no afecte negativamente a la posibilidad de intercambiar información de identidad en la actividad empresarial cuando sea necesario[236]. Sin embargo, como se ha indicado, descartar los actos en que la información utilizada ha sido revelada voluntariamente, podría excluir de la penalización actividades como la *peska* o el uso de información pública.

Deshonestidad

Evitar una interferencia con las actividades legítimas es un requisito esencial de la tipificación del hurto de identidad. Uno de los métodos considerados para evitar tal interferencia consiste en exigir la deshonestidad como requisito adicional para penalizar un acto[237].

[234] Acerca de la importancia de tipificar esta fase del delito, véase Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, página 25.
[235] Con respecto a la intención de cometer otros delitos, véase *infra* capítulo 6.9.7.
[236] Por ejemplo, puede ser necesario para la facturación de las tarjetas de crédito.
[237] Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, *supra* núm. 31, página 27.

Evitar una penalización no deseada supone ventajas, pero la prueba de la deshonestidad puede resultar difícil.

Intención de cometer otro delito

En general, el hurto de identidad no es un delito aislado. Para evitar una penalización excesiva, el delito podría limitarse a los actos que están vinculados con la comisión de otros delitos. En el enfoque de los Estados Unidos y el proyecto de ley del Canadá se contempla este vínculo. Mientras que la legislación de los Estados Unidos exige que el delincuente actúe con la intención de cometer cualquier actividad ilegal, el proyecto de ley canadiense solo exige circunstancias que permitan inferir que se utilizará la información para cometer un delito procesable. En lo que respecta a la transferencia de la información relacionada con la identidad, el proyecto canadiense va más allá y penaliza a los delincuentes que actúan de manera imprudente por no tener en cuenta la posibilidad de que la información se utilizara para cometer una infracción.

Elemento de intencionalidad

Por último, es necesario tomar una decisión sobre el elemento de intencionalidad (en la atribución de la intención especial antes mencionada). Tanto la legislación de los Estados Unidos como el proyecto de ley canadiense exigen que el delincuente actúe con pleno conocimiento.

REFERENCIAS

Publicaciones

1. *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, *Entertainment Law Review*, 2002, núm. 1, disponible en: http://elr.lls.edu/issues/v23-issue1/aldesco. pdf (última consulta: octubre de 2008).
2. *Biegel*, Beyond our Control? Confronting the Limits of our Legal System in the Age of Cyberspace, Massachusetts Institute of Technology, 2001.
3. *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, *Chicago Journal of International Law*, 2007, vol. 8, núm. 1, disponible en: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J.__Int'l_L._233_(2007).pdf (última consulta: octubre de 2008).
4. *Bolton/Hand*, Statistical Fraud Detection: A Review, 2002, disponible en: http://metalab.uniten.edu.my/~abdrahim/ntl/Statistical%20Fraud%20Detection%20A%20Review.pdf (última consulta: octubre de 2008).
5. *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 2005.
6. *Broadhurst*, Development in the global law enforcement of cyber-crime, in *Policing: An International Journal of Police Strategies and Management*, vol. 29, núm. 2, 2006.
7. *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, vol. 11, núm. 1, 2006, disponible en: http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf (última consulta: octubre de 2008).
8. *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, *Bulletin of Science Technology Society*, 2007, Vol. 27, 2008.
9. *Clarke*, Technology, Criminology and Crime Science, *European Journal on Criminal Policy and Research*, vol. 10, 2004.
10. *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, Kluwer Academic Publishers, 1999.
11. *Copes/Vieraitis/Jochum*, Bridging the Gap between Research and Practice: How Neutralization Theroy can inform Reid Interrogations of Identity Thieves, *Journal of Criminal Justice Education*, vol. 18, núm. 3, 2007.
12. *Dhamija/Tygar/Hearst*, Why Phishing Works, disponible en: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf (última consulta: octubre de 2008).

13. *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, O'Reilly, 2006.

14. *Elston/Stein*, International Cooperation in Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, disponible en: http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf (última consulta: octubre de 2008).

15. *Emigh*, Online Identity Theft: Phishing Technologies, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005.

16. *Epstein/Brown*, Cybersecurity in the Payment Card Industry, *University of Chicago Law Review*, vol. 75, 2008.

17. *Faulkner*, Hacking Into Data Breach Notification Laws, *Florida Law Review*, vol. 59, 2007.

18. *Fawcett/Provost*, Adaptive Fraud Detection, *Data Mining and Knowledge Discovery*, vol. 1, núm. 3, 1997.

19. *Garfinkel*, Database nation: The Death of Privacy in the 21st Century, O'Reilly, 2000.

20. *Gayer*, Policing Privacy, Law Enforcement's Response to Identity Theft, CALPIRG Education Fund, 2003.

21. *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005.

22. *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008.

23. *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, CRi, 2006.

24. *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008.

25. *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, disponible en: http://www.privacyrights.org/ar/id_theft.htm (última consulta: octubre de 2008).

26. *Gonsalves*, Phishers Snare Victims with VoIP, 2006, disponible en: http://www.techweb.com/wire/security/186701001 (última consulta: octubre de 2008).

27. *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003.

28. *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, disponible en: http://www.securityfocus.com/infocus/1527 (última consulta: octubre de 2008).

29. *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, 2005, disponible en: http://wiki.cs.columbia.edu:8080/download/attachments/1979/Information+Revelation+and+Privacy+in+Online+Social+Networks-gross.pdf (última consulta: octubre de 2008).

30. *Guo/Chiueh*, Sequence Number-Based MAC Address Spoof Detection, disponible en: http://www.ecsl.cs.sunysb.edu/tr/TR182.pdf (última consulta: octubre de 2008).

31. *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, *Brigham Young University Law Review*, 1992, disponible en: http://lawreview.byu.edu/archives/1992/1/haf.pdf (última consulta: octubre de 2008).

32. *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, vol. 18, disponible en: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 (última consulta: octubre de 2008).

33. *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006.

34. *Hansen/Meissner* (ed.), Linking digital identities, 2007, disponible en: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (última consulta: octubre de 2008).

35. *Hoar*, Identity Theft: The Crime of the New Millennium, *Oregon Law Review*, vol. 80, 2001.

36. *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3.

37. *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006.

38. *Jagatic/Johnson/Jakobsson/Menczer*, Social Phishing, 2005, disponible en: http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf (última consulta: octubre de 2008).

39. *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, núm. 5.

40. *Kang*, Wireless Network Security—Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2.

41. *Keyser*, The Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, vol. 12, núm. 2, disponible en: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf (última consulta: octubre de 2008).

42. *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006.

43. *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, 2008.

44. *Levi*, Combating Identity and Other Forms of Payment Fraud in the UK: An Analytical History, published in *McNally/Newman*, Perspectives on Identity Theft.

45. *Levi/Burrows*, Measuring the Impact of Fraud in the UK, *British Journal of Criminology*, vol. 48, 2008.

46. *Lewis*, Cyber Attacks Explained, 2007, disponible en: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf (última consulta: octubre de 2008).

47. *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005.

48. *Mashima/Ahamad*, Towards a User-Centric Identity-Usage Monitoring System in: Internet Monitoring and Protection, 2008.

49. *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, *Crime, Law and Social Change*, vol. 46.

50. *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, disponible en: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf (última consulta: octubre de 2008).

51. *Owen/Keats/Gill*, The Fight Against Identity Fraud: A Brief Study of the EU, the United Kingdom, France, Germany, and the Netherlands, Perpetuity Research & Consultancy International, 2006.

52. *Paget*, Identity Theft, McAfee White Paper, 2007, disponible en: http://www. mcafee.com/us/threat_center/white_paper.html (última consulta: octubre de 2008).

53. *Putnam/Elliott*, "International Responses to Cyber Crime", in *Sofaer/Goodman*, "Transnational Dimension of Cyber Crime and Terrorism", 2001.

54. *Romanosky/Relang/Acquisti*, Do Data Breach Disclosure Laws Reduce Identity Theft?, Seventh Workshop on the Economics of Information Security, Center for Digital Strategies, Tuck School of Business, disponible en: http://weis2008.econinfosec.org/papers/Romanosky.pdf (última consulta: octubre de 2008).

55. *Roth*, "State Sovereignty, International Legality, and Moral Disagreement", 2005, disponible en: http://www.law.uga.edu/intl/roth.pdf (última consulta: octubre de 2008).

56. *Siegel*, Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age, *Penn State Law Review*, vol. 111, núm. 3.

57. *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, *Harvard Journal of Law & Technology*, vol. 15, núm. 2, 2002.

58. *Sofaer/Goodman*, Cyber Crime and Security—The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, página 1 y ss., disponible en: http://media.hoover.org/documents/0817999825_1.pdf (última consulta: octubre de 2008).

59. *Shamah*, Password Theft: Rethinking an old crime in a new area, *Mich. Telecomm. Tech. Law Review*, vol. 12, 2006.

60. *Stevens*, Federal Information Security and Data Breach Notification Laws, 3rd April 2008, CRS Report for Congress, Document RL34120.

61. *Stoddart*, Who Watches the Watchers? Towards an Ethic or Surveillance in a Digital Age, *Studies in Christian Ethics*, 2008, vol. 21, 2008.

62. *Stutzman*, An Evaluation of Identity-Sharing Behavior in Social Network Communities, disponible en: http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf (última consulta: octubre de 2008).

63. *Sury*, Identity-Management und Recht, *Informatik-Spektrum*, vol. 27, núm. 3, 2004.

64. *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, Routledge 2001.

65. *Turner*, Towards a Rational Personal Data Breach Notification Regime, Information Policy Institute, junio de 2006.

66. *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Instituto Australiano de Criminología, 2006, disponible en: http://www.aic.gov.au/publications/tandi2/tandi329t.html (última consulta: octubre de 2008).

67. *Van der Meulen*, The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom and the European Union, Report commissioned by the National Infrastructure Cybercrime Programme (NICC).

68. *Wang/Chen/Atabakhsh*, Criminal Identity Deception and Deception Detection in *Law Enforcement*, *Group Decision and Negotiation*, vol. 13, 2004.

69. *White/Fisher*, Assessing Our Knowledge of Identity Theft: The Challenge of Effective Prevention and Control Efforts, *Criminal Justice Policy Review*, 2008, vol. 19, 2008.

70. *Wrigth*, Detecting Wireless LAN Mac Address Spoofing, 2003, disponible en: http://forskningsnett.uninett.no/wlan/download/wlan-mac-spoof.pdf (última consulta: octubre de 2008).

71. *Zaidi*, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada, *Loyola Consumer Law Review*, vol. 19, issue 2, 2007.

Estudios/encuestas/informes/documentos de debate

72. 2003 Federal Trade Commission Identity Theft Survey Report.

73. 2006 Better Bureau Identity Fraud Survey.

74. 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data.

75. 2007 Javelin Strategy and Research Identity Fraud Survey.

76. Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007.

77. Identity Fraud: A Study, United Kingdom Cabinet Office, 2002, disponible en: http://www.ips.gov.uk/identity/downloads/id-fraud-report.pdf (última consulta: octubre de 2008).

78. Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, Documento de la Oficina General de Contabilidad: GAO/GGD-98-100BR.

79. Identity Theft—A discussion paper, disponible en: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf (última consulta: octubre de 2008).

80. Identity Theft, Available Data Indicate Growth in Prevalence and Cost, Statement of *R. Stana*, Documento de la Oficina General de Contabilidad: GAO-02-424T.

81. Identity Theft, Greater Awareness and Use of Existing Data Are Necessary, Report to the Honourable Sam Johnson, House of Representatives, Documento de la Oficina General de Contabilidad: GAO-02-766.

82. Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, Documento de la Oficina General de Contabilidad: GAO-07-935T.

83. Internet-related Identity Theft, 2007, disponible en: http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf (última consulta: octubre de 2008).

84. Lessons Learned about Data Breach Notification, Report to Congressional Requesters, 2007, Documento de la Oficina General de Contabilidad: GAO-07-657.

85. Money Laundering, Extend of Money Laundering through Credit Card is Unknown, Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, US Senate, 2002, Documento de la Oficina General de Contabilidad: GAO-02-670.

86. OECD Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL.

87. OECD Policy Guidance on Identity Theft, 2007.

88. Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; However, the full extend is unknown; Report to Congressional Requesters, 2007, Documento de la Oficina General de Contabilidad: GAO-07-737.

89. Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, 2007, E/CN.15/2007/8/Add.3.

90. Social Security Numbers, Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate, Documento de la Oficina General de Contabilidad: GAO-07-752.

91. Social Security Numbers, More could be done to protect SSNs, Statement of *C. M. Fagnoni*, Managing Director Education. Workforce and Income Security, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, 2006, Documento de la Oficina General de Contabilidad: GAO-06-586T.

92. Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series), 2007.

93. The Use of Technology to Combat Identity Theft, Report on the Study Conducted Pursuant to Section 157 on the Fair and Accurate Credit Transaction Act of 2003, 2005, disponible en: https://www.treasury.gov/offices/domestic-finance/financial-institution/cip/biometrics_study.pdf (última consulta: octubre de 2008).

94. The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, página 4 y ss., disponible en: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf (última consulta: octubre de 2008).

95. Naciones Unidas: Informe del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos E/CN.15/2007/8 y Add.1 a 3.

TIPOLOGÍA Y CRITERIOS DE LA TIPIFICACIÓN DEL DELITO DE IDENTIDAD: COMPENDIO DE EJEMPLOS DE LEYES PERTINENTES*

Gilberto Martins de Almeida
Martins de Almeida Advogados, Río de Janeiro, Brasil

*El presente Compendio se preparó originalmente como documento de trabajo de la cuarta reunión del Grupo básico de expertos sobre delitos relacionados con la identidad, organizada por la Oficina de las Naciones Unidas contra la Droga y el Delito y celebrada en Viena (Austria) del 18 al 22 de enero de 2010. Las opiniones expresadas en el presente Compendio pertenecen al autor y no reflejan los puntos de vista de las Naciones Unidas.

Índice

I. INTRODUCCIÓN

De conformidad con la resolución 2004/26 del Consejo Económico y Social (ECOSOC), la UNODC encargó la preparación de un estudio sobre "el fraude y la falsificación de la identidad y su uso indebido con fines delictivos", que fue publicado a principios de 2007. En el estudio se adoptó un enfoque amplio desde tres puntos de vista. En primer lugar, se empleó la expresión general "delito de identidad" para abarcar todas las formas de conducta ilícita relacionadas con la identidad, incluidos los delitos cuya descripción no suele ser uniforme, como la "falsificación de identidad" y el "hurto de identidad". En segundo lugar, se tuvieron en cuenta todos los actos delictivos relacionados con el hurto de identidad incluida su comisión en línea o de otra forma, haciendo especial hincapié en los sistemas y pautas delictivos complejos debido a los vínculos con la delincuencia organizada transnacional y otras actividades delictivas. En tercer lugar, los delitos relacionados con la identidad se consideraron conjuntamente con el fraude, dada su interrelación y atendiendo a las indicaciones específicas del mandado del ECOSOC.

Los resultados del estudio[1] se basaron en la información proporcionada por 46 Estados Miembros, incluidos muchos Estados miembros de la OCDE. La principal contribución de ese estudio consistió en examinar el problema desde una perspectiva nueva de derecho penal, y desde el punto de vista del uso indebido de la identidad como una forma particular del delito, por oposición al criterio tradicional de tipificar otros actos delictivos cometidos con identidades falsas. En el estudio también se abordaron las diferencias y las contradicciones entre los conceptos y las definiciones en los distintos contextos nacionales, relativas al fraude y la falsificación de la identidad y su uso indebido con fines delictivos, y se esclarecieron varios aspectos que revelan el carácter multifacético y complejo del problema.

Basándose en los resultados y las recomendaciones del estudio y, en cumplimiento con lo dispuesto en la resolución 2007/20 del Consejo Económico y Social, la UNODC puso en marcha una plataforma consultiva sobre los delitos relacionados con la identidad con objeto de reunir a destacados representantes del sector público, dirigentes de empresas, representantes de organizaciones internacionales y regionales y otras partes interesadas, con el fin de compartir experiencias, elaborar estrategias, facilitar la realización de investigaciones adicionales y acordar la adopción de medidas prácticas contra los delitos relacionados con la identidad. Como medida inicial, se estableció un grupo básico de expertos encargado de intercambiar opiniones sobre la mejor manera de proceder y las iniciativas más apropiadas que es preciso llevar adelante en el marco de la plataforma.

[1] El texto completo del estudio se encuentra disponible en: http://www.unodc.org/unodc/en/organized-crime/index.html# IDCRIME.

En todas las reuniones del Grupo básico, los expertos reconocieron que los problemas planteados por el delito relativo a la identidad son nuevos y exigen una labor adicional encaminada al establecimiento de una clasificación apropiada del delito sobre la base de una tipología básica u otro marco de referencia. El Grupo de expertos consideró que era necesario establecer esa tipología antes de examinar las respuestas legislativas más apropiadas a los delitos relacionados con la identidad.

Con respecto a las respuestas legislativas, se indicó que si bien varios Estados estaban tipificando o considerando la posibilidad de tipificar nuevos delitos para combatir el uso indebido de la identidad, otros no estaban todavía convencidos de que una nueva perspectiva en materia de penalización supusiera una mejora suficiente con respecto a la actual situación en que ya había delitos reconocidos, como el fraude, la falsificación y la suplantación de identidad. Por lo tanto, el Grupo recomendó a la UNODC que tomase medidas con objeto de sensibilizar sobre las cuestiones jurídicas que estaban en juego y las opciones políticas disponibles a ese efecto.

Los expertos reconocieron asimismo que la UNODC podría además desempeñar un importante papel que consistiría en elaborar materiales para ayudar a los países que desearan tipificar nuevos delitos. Así pues, se recomendó a la UNODC que elaborara materiales, como planes y opciones normativas, así como formulaciones generales para tenerlos en cuenta al configurar los delitos, y descripciones de los tipos de conducta que se podrían tipificar.

El Consejo Económico y Social, por recomendación de la Comisión de Prevención del Delito y Justicia Penal, en su 18º período de sesiones, aprobó la resolución 2009/22 de 30 de julio de 2009, en la cual pedía a la UNODC que, en consulta con los Estados Miembros y teniendo en cuenta a las organizaciones intergubernamentales pertinentes y, de conformidad con las normas y los procedimientos del Consejo Económico y Social, expertos de instituciones académicas, organizaciones no gubernamentales pertinentes y el sector privado, reunieran, elaboraran y difundieran, entre otras cosas, "material y directrices sobre la tipología de los delitos relacionados con la identidad y sobre cuestiones de penalización pertinentes, a fin de prestar asistencia a los Estados Miembros que lo solicitaran en lo que respecta a la tipificación de nuevos delitos relacionados con la identidad y a la modernización de los delitos existentes, teniendo presente la labor de otras organizaciones intergubernamentales que se ocupan de cuestiones conexas".

El presente compendio se preparó de conformidad con las indicaciones y directrices mencionadas. El proyecto correspondiente fue presentado al Grupo básico de expertos sobre el delito relacionado con la identidad, en su cuarta reunión (Viena, 18 a 22 de enero de 2010), para su examen y aprobación.

1. Objetivo, alcance y contenido del compendio

Este compendio se propone ante todo hacer un inventario de las disposiciones jurídicas de distintas jurisdicciones nacionales sobre el delito de identidad o de las disposiciones conexas.

El objetivo final del presente trabajo es difundir información práctica susceptible de contribuir a la elaboración de estudios ulteriores o de manuales de asistencia técnica y capacitación.

No se procura hacer un análisis de fondo ni formular observaciones sustantivas sobre el panorama descrito, ni sobre cualquier otro tema particular. A este respecto, se deberán consultar documentos anteriores presentados[2] al Grupo básico de expertos.

Con respecto a cualquiera de los temas abordados, tampoco pretende reproducir de forma exhaustiva las disposiciones jurídicas pertinentes vigentes en los países considerados. Ofrece en cambio un mosaico compuesto por una gran diversidad de criterios legislativos correspondientes a las distintas formas de delitos de identidad. Por consiguiente, se da una visión variada de la legislación de países de diferentes regiones y se describen distintas experiencias y perfiles nacionales.

En razón de la gran diversidad de los criterios nacionales en la materia, se incluye en el compendio la formulación de un enfoque conceptual sistemático relativo a los delitos de identidad.

Sobre la base de la labor realizada por el Grupo básico de expertos, en este documento se ha efectuado una actualización y una ampliación a fin de abordar cualquier delito relacionado con la identidad, además del hurto de identidad, sobre la base de: *a)* un cuestionario dirigido a los participantes del Grupo básico en diciembre de 2009, *b)* las deliberaciones celebradas en ocasión de la cuarta reunión del Grupo, y *c)* la consulta de los textos jurídicos y técnicos más recientes, incluidas las últimas publicaciones de 2009 sobre la materia, tal como se indica en la bibliografía.

Cabe mencionar que si bien los datos sobre todos los países examinados figuran, por motivos de orden gráfico, en los mismos cuadros (apéndices A.1, A.2 y A.3), corresponden a investigaciones realizadas en distintas oportunidades y proceden de fuentes diferentes.

El examen relativo a los siguientes países tuvo en cuenta datos correspondientes a diciembre de 2009: Alemania, Argentina, Australia, Austria, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Croacia, Ecuador, España, Estados Unidos de América, Finlandia, Francia, Hungría, India, Italia, Japón, Letonia, México, Nigeria, Noruega, Perú, Portugal, Reino Unido, Sudáfrica, Suecia, Suiza, Turquía y Venezuela.

En el examen de los siguientes países se tuvo en cuenta información correspondiente a septiembre de 2010: Albania, Armenia, Azerbaiyán, Bahrein, Barbados, Botswana, Bulgaria, Canadá, China, Chipre, Egipto, Emiratos Árabes Unidos, Estonia, ex República Yugoslava de Macedonia, Federación de Rusia, Filipinas, Georgia, Indonesia, Iraq, Irlanda, Jamaica, Kazajstán, Kirguistán, Kuwait, Lituania, Malasia, Omán, Qatar, República Árabe Siria, República Checa, República de Moldova, Singapur, Tayikistán, Ucrania, Uzbekistán y Yemen.

[2] En particular, el documento sobre los enfoques jurídicos para tipificar el robo de identidad, preparado por el Dr. Marco Gercke, y presentado a la Comisión de Prevención del Delito y Justicia Penal en su 18º período de sesiones (Viena, 16 a 24 de abril de 2010) (véase E/CN.15/2009/CRP.13).

En el compendio también se tuvo en cuenta información obtenida por la UNODC en respuesta a un "cuestionario sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos", distribuido en 2006 para reunir material. Esa información se refería a los siguientes países: Alemania, Arabia Saudita, Belarús, Croacia, Eslovaquia, Eslovenia, Estados Unidos de América, Federación de Rusia, Finlandia, Grecia, Hungría, Italia, Japón, Jordania, Letonia, Líbano, Mauricio, Marruecos, Noruega, Países Bajos, Reino Unido, República de Corea, Rumania, Suecia, Suiza y Turquía.

Todos los datos disponibles fueron verificados hasta el 29 de septiembre de 2010.

En el texto de las disposiciones citadas a título de ejemplo en el capítulo 3 se indica la fuente de información correspondiente, así como la de las publicaciones o páginas web donde figuran.

En los cuadros A.1, A.2 y A.3 se indican las legislaciones de los países que contienen disposiciones relacionadas con la identidad.

La columna "legislación" de los cuadros contiene las disposiciones referidas especialmente a los delitos relativos a la identidad que fueron encontradas, mientras que las demás columnas se completaron con disposiciones generales. La ausencia de información en las columnas indica que, en el marco del presente trabajo, no se encontraron leyes ni disposiciones especialmente relacionadas con la identidad.

Para ampliar el número de países objeto de estudio, así como para completar, validar y actualizar el contenido de los cuadros[3], incluida la presentación de todas las leyes nacionales aplicables, además de las examinadas en este trabajo, como los códigos penales nacionales y las leyes sobre el delito cibernético y la privacidad, sería necesario distribuir a un mayor número de destinatarios un cuestionario amplio, de ser posible en nombre de las Naciones Unidas.

2. Terminología

La terminología utilizada ha sido definida y explicada en publicaciones y documentos anteriores encargados por la UNODC. No obstante, ciertas disposiciones citadas contienen la definición de algunos tipos de delitos o elementos que forman parte de la tipología correspondiente.

[3] Incluida la presentación de todos los tipos de leyes nacionales aplicables, además de las examinadas en el marco de este trabajo (que se refiere principalmente a investigaciones sobre las leyes relativas al delito cibernético y a la privacidad).

II. MATRIZ DE LA TIPOLOGÍA Y CRITERIOS DE LA TIPIFICACIÓN DEL DELITO DE IDENTIDAD

En este capítulo se reseñan los resultados estadísticos positivos del estudio, que aparecen en los cuadros A.1, A.2 y A.3 adjuntos. El número de países mencionados en las estadísticas refleja el número de campos que llevan la palabra "sí" en las respectivas columnas. Las notas que acompañan cada tema no tienen por objeto establecer conclusiones científicas, sino que se limitan a destacar esferas que podrían requerir más atención.

1. Legislación sobre el delito de identidad: definiciones, medios o formato de la información relativa a la identidad e información de identidad protegida

Diferentes leyes con inclusión de definiciones de información relativa a la identidad

Con respecto a los distintos tipos de legislación en que figuran definiciones de la información relacionada con la identidad, los resultados del estudio son los siguientes:

- Definiciones en códigos penales: 24 países (Albania, Alemania, Argentina, Austria, Azerbaiyán, Brasil, Bulgaria, China, Colombia, Ecuador, España, Estados Unidos de América, Estonia, Francia, Georgia, Italia, Japón, Kazajstán, México, Nigeria, Perú, Suecia, Suiza y Turquía).
- Definiciones en leyes sobre la privacidad: 2 países (Australia y la Federación de Rusia).
- Definiciones en leyes sobre tecnología de la información: 1 país (la India).
- Definiciones en otras leyes: 14 países (Bolivia (Estado Plurinacional de), Canadá, Chile, Costa Rica, Filipinas, Francia, Hungría, Japón, Portugal, República de Moldova, Reino Unido, Rumania, Sudáfrica y Venezuela).

Aunque la mayoría de las definiciones figuran en los códigos penales nacionales, otras muchas se encuentran en leyes relativas a diversos temas, lo que parece reflejar la gran variedad de percepciones del delito de identidad.

También merece la pena señalar que el número de definiciones contenidas en leyes sobre privacidad o tecnología de la información es relativamente reducido, probablemente

porque en la mayoría de los países examinados el delito de identidad no está estrechamente vinculado con la privacidad o la tecnología.

Diversidad de los términos utilizados en las definiciones de la información relativa a la identidad

Con respecto a las diferentes opciones terminológicas utilizadas en las definiciones de la información relativa a la identidad, el estudio indica el empleo de términos variados, a saber:

- Datos, información, base de datos o documentos "personales": 14 países (Argentina, Australia, Austria, Bulgaria, Colombia, Ecuador, España, Estonia, Federación de Rusia, Hungría, Perú, República de Moldova, Sudáfrica y Venezuela).
- "Computadoras" o "datos de sistema", o expresiones similares referidas a la tecnología: 10 países (Azerbaiyán, Bolivia, Chile, Georgia, Italia, Japón, Kazajstán, Kirguistán, Nigeria y Rumania).
- "Secretos" o "datos confidenciales": 2 países (Costa Rica y Portugal).
- "Datos": 2 países (Francia y Suecia).
- "Información de identidad", "documento de identidad", "identidades", "tarjetas de identificación" o "documento de identificación": 7 países (Albania, Alemania, Canadá, China, Filipinas, India y México).

En su mayoría las disposiciones se basan en el carácter "personal" de la información como principal elemento para calificar a la información sobre la identidad, seguido de cerca por el aspecto "tecnológico" de ese tipo de información. Así pues, se parte del supuesto de que el fenómeno de la digitalización influye significativamente en la información relativa a la identidad, además de plantear un interrogante sobre el objetivo principal de la tipología, que requiere determinar si debería centrarse en el aspecto intrínseco de la identidad de los delitos correspondientes o, de lo contrario, si estos delitos deberían quedar en cierta medida incluidos en aspectos específicos de cuestiones relacionadas con la tecnología.

El hecho de que numerosos países hayan agrupado a los delitos sobre la identidad bajo el calificativo general y ambiguo de "personal" parece indicar que si bien estos delitos representan hoy día un importante (y creciente) porcentaje de los delitos, la mayoría de los países examinados todavía no han adquirido conciencia de la conveniencia de abordarlos más concretamente en su legislación.

El escaso número de referencias a información de "identidad" o "documento de identificación" guarda relación con las pocas referencias a la confidencialidad, lo que parece indicar que en general la identidad se percibe vinculada al carácter "personal" (y, tal vez más concretamente, a la privacidad).

Diversidad de formatos o medios de la información relativa a la identidad

En relación con los distintos tipos de formato o medios de la información relativa a la identidad se obtuvieron los siguientes resultados:

- Cualquier medio o formato: 11 países (Albania, Australia, Austria, Bulgaria, Canadá, China, Francia, Hungría, India, Nigeria y Sudáfrica).
- Formato o medio electrónico: 20 países (Argentina, Azerbaiyán, Bolivia (Estado Plurinacional de), Chile, Colombia, Costa Rica, Ecuador, España, Estonia, Federación de Rusia, Filipinas, Georgia, Italia, Japón, Kazajstán, Kirguistán, México, Perú, República de Moldova y Venezuela).
- Documentos: 4 países (Alemania, Brasil, Turquía y Reino Unido).

Es considerable el número de casos en que se observa una muy estrecha relación entre la información relativa a la identidad y los medios electrónicos, que supera con creces el número de referencias a los medios de almacenamiento en documentos.

Teniendo en cuenta que el delito de identidad puede cometerse no solo por medios electrónicos (por ejemplo, delitos de falsificación "material" o apropiación indebida de pasaportes), quizás convenga tratar de determinar si la importancia de la relación entre la información relativa a la identidad y los medios electrónicos es proporcional a la importancia de su relación con otros tipos de formatos o medios.

Diversos tipos de información relativa a la identidad protegidos por leyes nacionales

Con respecto a los diferentes tipos de información o documentos relativos a la identidad que están protegidos en las legislaciones nacionales, se obtuvieron los resultados siguientes:

- Número de seguridad social, número de identificación personal (NIP) o número del seguro de salud: 9 países (Albania, Argentina, Austria, Canadá, Chile, España, Estados Unidos de América, Italia y Sudáfrica).
- Nombre, dirección, fecha de nacimiento o firma escrita: 4 países (Albania, Argentina, Canadá y Sudáfrica).
- Certificado de nacimiento, de estado civil, de defunción, tarjeta de identidad, pasaporte o documento de inmigración: 6 países (Albania, Alemania, Brasil, Canadá, Reino Unido y Sudáfrica).
- Permiso de conducir, tarjeta de reservista (militar), credencial de elector: 6 países (Alemania, Brasil, Canadá, Estados Unidos de América, Reino Unido y Sudáfrica).
- Número de tarjeta de crédito o de débito, o número de cuenta bancaria: 5 países (Canadá, Estados Unidos de América, Japón, Reino Unido y Sudáfrica).
- Contraseña o clave de ingreso en el correo electrónico o de acceso a la computadora o de navegación en la web, dirección MAC o IP, firma electrónica o digital o nombre de usuario: 4 países (Canadá, Estados Unidos de América, India y Japón).
- Huellas digitales, huella vocal, imagen de la retina y del iris o perfil de ADN: 2 países (Canadá y Sudáfrica).

En los ejemplos proporcionados, los soportes no electrónicos de información relativa a la identidad superan el número de soportes exclusivamente electrónicos. A primera vista parecería contradecir la conclusión de la prevalencia de la relación entre la información relativa a la identidad y los medios electrónicos. Sin embargo, cabe señalar que incluso documentos que no son originalmente electrónicos (tarjeta de seguridad social, pasaporte, etc.) suelen elaborarse o reproducirse por medios electrónicos y, por consiguiente, son susceptibles de una apropiación abusiva electrónica (de la imagen, o de datos o información pertinente). En otros términos, podría haber algunos elementos de delitos electrónicos sobre la identidad aun cuando el documento correspondiente no fuera originalmente (o por definición) electrónico.

Además, la representación digital de formas más recientes de identificación personal (como la imagen de la retina, del iris o el ADN), que los delincuentes probablemente busquen cada vez más, consolida la relación entre los medios electrónicos y la información relativa a la identidad.

2. Tipología de los delitos de identidad: elementos objetivos y clasificación de las conductas conexas

Con arreglo a los resultados del estudio puede hacerse la siguiente clasificación de las tipologías de delitos de identidad centrados en elementos objetivos de las conductas pertinentes.

Elaboración de documentos falsificados o falsificación de documentos auténticos

Los siguientes países consideraron esa tipología en su legislación nacional: Albania, Alemania, Argentina, Brasil, Estados Unidos de América, Japón, Reino Unido y Sudáfrica.

Utilización individual ilegítima de información relativa a la identidad

Los siguientes países consideraron esa tipología en su legislación nacional: Albania, Alemania, Argentina, Brasil, Canadá, Estados Unidos de América, India, Japón, Reino Unido y Sudáfrica. Las conductas pertinentes se referían, por ejemplo, a la posesión, la utilización, la retención, la obtención, el control, la adquisición de información relativa a la identidad, así como el acceso ilegítimo a esa información.

Utilización colectiva ilegítima de información relativa a la identidad

Los siguientes países consideraron esa tipología en su legislación nacional: Albania, Alemania, Argentina, Brasil, Canadá, Estados Unidos de América, Japón, Reino Unido y Sudáfrica. Las conductas pertinentes se referían, por ejemplo, a la transferencia, la puesta a disposición o publicación en línea, la transmisión, la distribución, la venta o el suministro, la puesta en venta o la oferta (o la posesión a ese efecto) y la difusión de información relativa a la identidad.

Tráfico de información relativa a la identidad

Los siguientes países consideraron esa tipología en su legislación nacional: Alemania, Argentina y Sudáfrica. Las conductas pertinentes se referían, por ejemplo, a la transferencia, el transporte, la eliminación (u obtención del control con ese fin) y el almacenamiento de información relativa a la identidad, así como la importación o exportación de esa información.

Daño causado a la información relativa a la identidad de terceros

Los siguientes países consideraron esa tipología en su legislación nacional: Alemania, Brasil y Sudáfrica. Las conductas pertinentes se referían, por ejemplo, a la provocación o afirmación de un error, al engaño por simulación de la existencia de hechos falsos, la destrucción, ocultación, distorsión o supresión de hechos verdaderos y la influencia en el resultado de una operación de tratamiento de datos.

Intento/conspiración/ayuda/instigación

Los siguientes países consideraron esa tipología en su legislación nacional: Alemania, Estados Unidos de América, Japón y Sudáfrica.

3. Tipología de los delitos de identidad: elementos subjetivos y requisitos

Los resultados obtenidos respecto de los diversos elementos subjetivos y requisitos de los delitos de identidad son los siguientes:

Intención de cometer, ayudar a cometer o instigar un acto ilegal
Se observó esa intención en la legislación de cinco países: Alemania, Argentina, Canadá, Estados Unidos de América y Sudáfrica.

Intención de estafar
Figura esta intención en la legislación de siete países: Alemania, Argentina, Brasil, Canadá, Estados Unidos de América, India y Reino Unido.

Intención de engañar
Se observó en la legislación de ocho países: Alemania, Argentina, Brasil, Canadá, Estados Unidos de América, India, Japón y Sudáfrica.

Intención de obtener para sí o para un tercero un beneficio o ventaja material
Se observó en la legislación de tres países: Alemania, Brasil y Sudáfrica.

Intención de utilizar un documento para certificar y registrar hechos personales
Solo figura en la legislación del Reino Unido.

Concienciación, creencia o imprudencia con respecto a la obtención o posesión de información de identidad ajena
Solo figura en la legislación del Canadá.

Concienciación, creencia o imprudencia con respecto a la falsedad u obtención indebida de documentos
Presente solo en la legislación del Reino Unido.

Concienciación, creencia o imprudencia con respecto a la utilización de la información para cometer un delito
Presente en la legislación de dos países: el Canadá y el Reino Unido.

Lo expuesto *supra* indica que muchos países que han aprobado leyes sobre el delito de identidad exigen el elemento de intencionalidad. Por el contrario, solo unos pocos de los ejemplos proporcionados se refieren a la concienciación, la creencia y la imprudencia. Dada la naturaleza "inestable" de la información almacenada en bases de datos electrónicas cabe preguntarse si será exigible el elemento de intención, o si será admisible la presunción de intención, en qué medida y a la luz de qué circunstancias.

III. COMPENDIO DE EJEMPLOS DE LEYES PERTINENTES

En este capítulo se presentan extractos de disposiciones de leyes de los países objeto de estudio. Las notas de introducción de algunos temas no tienen por objeto describir ni analizar las disposiciones consideradas, sino destacar algunos aspectos que quizás merezcan un examen especial.

1. "Datos personales"

La protección de la información relativa a la identidad se regula generalmente en el contexto de las leyes sobre la privacidad. Si bien la protección de la privacidad se centra principalmente en actos que pueden caracterizar una injerencia de la privacidad, puede abarcar algunas definiciones que también guardan relación con la información relativa a la identidad, por ejemplo, del concepto de "datos personales" puede referirse no solamente a determinados elementos asociados a una persona (generalmente denominados "datos especiales"), sino a algunos datos que la permiten identificar.

Hungría, Ley LXIII de 1992 sobre la protección de los datos personales y la revelación de datos de interés público:

> 1. Datos personales: se entenderá por datos personales cualquier dato relacionado con una determinada persona natural (identificada o identificable) (en adelante denominada "el interesado"), así como cualquier conclusión relativa al interesado que pueda inferirse de esos datos. En el proceso de tratamiento de datos se considerará que esos datos son personales mientras sea posible restablecer su relación con el interesado.
>
> 2. Datos especiales: se entenderá por datos especiales cualquier dato relacionado con:
>
> *a)* el origen racial, nacional o étnico, la opinión política o la afiliación a un partido, las creencias religiosas o convicciones ideológicas, o la afiliación a cualquier organización de defensa de intereses;
>
> *b)* el estado de salud, las adicciones patológicas, la vida sexual o antecedentes penales personales […]

Alemania, Ley Federal de protección de datos[4], artículo 3, párrafos 1 y 9:

> 1) Se entiende por "datos personales" cualquier información relativa a las circunstancias personales o materiales de una persona identificada o identificable (el interesado)".
>
> […]
>
> 9) Se entiende por "categorías especiales de datos" personales la información sobre el origen racial y étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, la salud o la vida sexual de una persona.

Suecia, Ley sobre datos personales, artículo 3[5]:

> Se entiende por datos personales todo tipo de información que pueda referirse directa o indirectamente a una persona natural mientras se encuentre en vida.

2. "Estado civil"

Los datos sobre el "estado civil" de una persona están directa o indirectamente vinculados con los datos pertinentes sobre su identidad, a menos que se conserve el estado civil con fines estadísticos y se eliminen los datos. Si se conservan los datos sobre la identidad y no se protege el vínculo con el estado civil (por ejemplo, mediante un código atribuido al azar), los datos sobre el estado civil pueden calificarse de información relativa a la identidad.

Alemania, Código Penal[6], artículo 169, Falsificación del estado civil:

> 1) Quien declare falsamente la filiación de un niño o proporcione los datos del estado civil de un tercero ante una autoridad pública responsable de mantener los registros del estado civil o determinar el estado civil podrá ser sancionado con una pena de prisión de dos años como máximo o con una multa.
>
> 2) El acto de intentarlo también será punible.

3. "Información de identidad"

Hay diferentes fuentes de información para identificar a una persona que pueden constituir la denominada "información de identidad". La información de identidad se refiere al contenido de la información, independientemente del lugar en que haya sido registrada, comunicada o almacenada.

---

[4] Ley Federal de protección de datos de 1 de enero de 2002; véase: http://www.bdd.de/Download/bdsg_eng.pdf.

[5] Ley sobre datos personales de 1998: 204, publicada el 29 de abril de 1998; véase: http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf.

[6] Código Penal de Alemania en su versión promulgada el 13 de noviembre de 1998; Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3322, modificado en último término por el artículo 3 de la Ley de 2 de octubre de 2009, Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3214, véase: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169.

Canadá, Proyecto de ley S-4 por el que se modifica el Código Penal (hurto de identidad y el uso indebido conexo), artículo 402.1:

> 402.1 A los efectos de los artículos 402.2 y 403, se entenderá por la expresión "información de identidad" toda información —incluida la información biológica y psicológica— que pueda utilizarse por separado o conjuntamente con otra información para identificar o intentar identificar a una persona, como huellas digitales, huella vocal, imagen de la retina, imagen del iris, ADN, nombre, dirección, fecha de nacimiento, firma escrita, firma electrónica, firma digital, nombre de usuario, número de tarjeta de crédito o de débito, número de cuenta de una institución financiera, número de pasaporte, número de seguridad social, número de seguro de salud, número del permiso de conducir o clave de acceso.

4. "Medios de identificación"

La naturaleza de la expresión "medios de identificación" no requiere explicación, pero hay definiciones de la misma y su aplicación proporciona ejemplos interesantes.

Estados Unidos, 18 USC artículo 1028, capítulo 47, Fraude y declaraciones falsas:

> 7) Por "medios de identificación" se entiende el nombre o número que pueda utilizarse, por separado o conjuntamente con cualquier otra información, para identificar a una persona determinada, incluidos:
>
> *a)* el nombre, el número de seguridad social, la fecha de nacimiento, el permiso de conducir o el número de identificación oficiales expedidos por el Estado o el Gobierno, el número de registro de extranjero, el número de pasaporte oficial, el número de identificación de empleado o de identificación fiscal;
>
> *b)* datos biométricos únicos, como las huellas digitales, la huella vocal, la imagen de la retina o del iris o la representación de otro rasgo físico único;
>
> *c)* el número único de identificación electrónica, la dirección o el número de ruta bancario; o
>
> *d)* la información de identificación para las telecomunicaciones o el dispositivo de acceso (definido en el artículo 1029 *e)*) […].

5. "Documento de identidad" o "documento de identificación"

Las leyes sobre los delitos de identidad se refieren a los tipos de documentos que pueden contener información sobre la identidad en la medida en que ilustran o delimitan las hipótesis que sirven de base para su aplicación. En la formulación de las disposiciones correspondientes puede combinarse una afirmación genérica (sobre el objeto del documento) con una enumeración concreta de documentos.

Reino Unido, Ley sobre tarjetas de identidad[7], artículo 26:

> 1) En el artículo 25 se entiende por "documento de identidad" todo documento expedido o supuestamente expedido como:
>
> - Tarjeta de identidad;
> - Documento de acreditación;
> - Documento de inmigración;
> - Pasaporte del Reino Unido […];
> - Pasaporte expedido por las autoridades de un país o territorio distintos del Reino Unido o en nombre de esas autoridades, o por una organización internacional o en nombre de esa organización;
> - Documento que puede utilizarse (en algunas o todas las circunstancias) en lugar de un pasaporte;
> - Permiso de conducir del Reino Unido; o
> - Permiso de conducir expedido por las autoridades de un país o un territorio distintos del Reino Unido o en nombre de esas autoridades.

Estados Unidos, 18 USC artículo 1028, capítulo 47, Fraude o declaraciones falsas:

> 3) Se entiende por el término "documento de identificación" un documento elaborado o expedido por el Gobierno de los Estados Unidos o bajo su autoridad, por un Estado, una circunscripción política de un Estado, un gobierno extranjero, una circunscripción política de un gobierno extranjero, una organización internacional gubernamental o una organización internacional cuasi-gubernamental que, una vez completado con información relativa a una persona determinada, es un tipo de documento cuyo fin es la identificación de personas o que generalmente se acepta con ese fin […].

Alemania, Código Penal[8], artículo 273, Modificación de los documentos oficiales de identificación:

> 1) Quien con el fin de cometer un fraude en el comercio lícito:
>
> *a)* suprima, haga irreconocible, cubra o elimine un asiento en un documento oficial de identidad o retire una sola página de un documento oficial de identidad; o
>
> *b)* utilice un documento oficial de identidad modificado de esa forma;
>
> podrá ser condenado a una pena de prisión de hasta tres años o a una multa, a menos que el delito sea punible de conformidad con el artículo 267 o el artículo 274.

[7] Ley sobre tarjetas de identidad de 2006; véase, http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf.

[8] Código Penal de Alemania en la versión promulgada el 13 de noviembre de 1998, Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3322, modificado en último término por el artículo 3 de la Ley de 2 de octubre de 2009, Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3214; véase: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169.

2) El intento de cometer ese acto será punible.

Canadá, Proyecto de ley S-4 por el que se modifica el Código Penal (hurto de identidad y conducta indebida correspondiente), artículo 56.1:

> Documentos de identidad 1) Comete un delito quien, sin justificación legítima, procura obtener, poseer, transferir, vender u ofrecer en venta un documento de identidad que se relacione o tenga la intención de relacionarse, total o parcialmente, con otra persona.
>
> […]
>
> Definición de "documento de identidad" 3) A los efectos del presente artículo, se entenderá por "documento de identidad" una tarjeta con el número de seguridad social, un permiso de conducir, una tarjeta de seguro de salud, una partida de nacimiento, un certificado de defunción, un pasaporte conforme a la definición del apartado 57 5), un documento que simplifique el procedimiento de ingreso al territorio del Canadá, un certificado de nacionalidad, un documento que indique la condición de inmigrante en el Canadá, un certificado de condición de aborigen o una tarjeta de identificación de empleado con la fotografía y la firma del empleado, o cualquier documento similar, expedido o supuestamente expedido por un organismo del gobierno federal o de un gobierno provincial o extranjero.

6. Falsificación y expedición o uso indebido de certificados de salud

Algunos documentos, en razón de la importancia de su contenido en relación con el delito de identidad, han merecido la atención especial de los legisladores. Un ejemplo es el certificado de salud, cuya falsificación y expedición o utilización indebida se han abordado especialmente.

Alemania, Código Penal[9], artículo 277, Falsificación de certificados de salud:

> Quien valiéndose del título de doctor en medicina o de otro facultativo colegiado, sin tener derecho a hacerlo, o valiéndose ilegalmente del nombre de personas que poseen los títulos mencionados, expidan un certificado sobre su propio estado de salud o el de un tercero, o falsifiquen un certificado auténtico y lo utilicen con el fin de engañar a las autoridades públicas o a las compañías de seguros podrán ser condenados a una pena de prisión de un año como máximo o a una multa.

Ibid., artículo 278, Expedición de certificados de salud incorrectos:

> Los médicos y otros facultativos colegiados que intencionalmente y con conocimiento expidan un certificado incorrecto relacionado con el estado de salud de una persona

[9] Código Penal de Alemania en la versión promulgada el 13 de noviembre de 1998, Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3322, modificado en último término por el artículo 3 de la Ley de 2 de octubre de 2009, Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3214; véase: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169.

> para su utilización ante una autoridad pública o una compañía de seguros podrán ser condenados a una pena de prisión de dos años como máximo o a una multa.

Ibid., artículo 279, Utilización de certificados de salud incorrectos:

> Quien, con el fin de engañar a una autoridad pública o a una compañía de seguros sobre su propio estado de salud o el de un tercero, utilice un certificado del tipo indicado en el artículo 277 y en el artículo 278, podrá ser condenado a una pena de prisión de un año como máximo o a una multa.

7. Declaración falsa para el pasaporte

Diversas jurisdicciones consideran muy importantes las cuestiones relacionadas con la protección de la integridad de los pasaportes. En algunas disposiciones legislativas se aborda el problema de la información falsa facilitada para conseguir la expedición de un pasaporte.

Nigeria, Código Penal[10], artículo 190 A:

> Quien, con objeto de obtener un pasaporte para sí o para cualquier otra persona, de forma intencional, haga o incite a hacer en cualquier solicitud escrita dirigida a un funcionario público una declaración sustancialmente falsa comete un delito y puede ser condenado a una pena de prisión de un año.

8. Pasaportes y permisos de porte de armas falsos

En algunas legislaciones nacionales se aborda la cuestión de los pasaportes falsos conjuntamente con los per misos falsos de porte de armas.

Chile, Código Penal[11], artículos 199 y 200:

> El empleado público que expidiere un pasaporte o porte de armas bajo nombre supuesto o lo diere en blanco, sufrirá las penas de reclusión menor en sus grados mínimo a medio e inhabilitación absoluta temporal para cargos y oficios públicos en los mismos grados.
>
> El que hiciere un pasaporte o porte de armas falso, será castigado con reclusión menor en su grado medio y multa de seis a diez sueldos vitales. Las mismas penas se impondrán al que en un pasaporte o porte de armas verdadero mudare el nombre de la persona a cuyo favor se halle expedido, o el de la autoridad que lo expidió, o que altere en él alguna otra circunstancia esencial.

[10] Código Penal de Nigeria de 1990, capítulo 18; véase: http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm.
[11] Código penal de Chile, de 12 de noviembre de 1874, artículos 199 y 200; véase: http://www.servicioweb.cl/juridico/Codigo%20Penal%20de%20Chile%20libro2.htm.

9. Código de identificación

La información de identidad puede consistir en un simple código que permite la identificación de una persona. Ese código puede existir en forma "intangible" (por ejemplo, electrónicamente) o estar incorporado en un dispositivo (por ejemplo, en un generador de claves o "token") para tener acceso a un equipo.

Japón, Ley sobre el acceso no autorizado a una computadora[12], artículo 4:

> Ninguna persona podrá proporcionar a otra el código de identificación para el acceso a la función de control por un tercero que no sea el administrador de esa función de control o el usuario autorizado de tal código de identificación, indicando que es el código de identificación para ser utilizado específicamente en una computadora determinada, o a petición de una persona que posea ese conocimiento, salvo en el caso en que realice esos actos el administrador o que cuenten con la aprobación del administrador o del usuario autorizado.

10. Marcas de identificación

Algunas leyes nacionales describen marcas de identificación y abordan las conductas ilícitas conexas.

Hungría, Código Penal[13], artículo 277/A, Falsificación de marcas de identificación personal:

> Las "marcas de identificación" son signos que permiten identificar a una persona por ser característicos de su cuerpo o por haber sido incorporados por esa persona en un documento (por ejemplo, la huella digital de una persona en un pasaporte).
>
> 1) Quien:
>
> *a)* suprima o falsifique de otra forma una marca de identificación personal,
>
> *b)* adquiera o utilice un artículo cuya marca de identificación personal esté falsificada o sea falsa, o cuya marca de identificación personal se haya suprimido, comete un delito y podrá ser condenado a una pena de prisión de hasta tres años.
>
> 2) La pena de prisión podrá ser de cinco años si el delito descrito en el apartado 1) se ha cometido:
>
> *a)* con carácter profesional, o
>
> *b)* en el marco de una conspiración para delinquir.

[12] Ley núm. 128, de 1999.
[13] Ley núm. LXIII de 1992; véase: http://abiweb.obh.hu/adatved/indexek/AVTV-EN.htm.

11. Huellas genéticas

El código genético de una persona puede permitir su identificación y, por consiguiente, está protegido contra el intento de obtención, acceso o revelación indebidos. También se considera un delito la búsqueda del código genético sin fines médicos o científicos.

Francia, Código Penal[14], artículo 226-28:

> El hecho de buscar la identificación de una persona por sus huellas genéticas sin fines médicos ni científicos o fuera de una medida indagatoria o de instrucción diligenciada durante un procedimiento judicial será castigado con un año de prisión o 15.000 euros de multa.
>
> Será castigado con las mismas penas el hecho de divulgar informaciones relativas a la identificación de una persona por sus huellas genéticas o de proceder a la identificación de una persona por sus huellas genéticas sin ser titular de la acreditación prevista por el artículo L. 145-16 del Código de Salud Pública.

12. Uso indebido de una firma electrónica

Debido a sus características de seguridad especiales, la firma electrónica conlleva una fuerte presunción de que su usuario es realmente la persona que se dice que es. Por consiguiente, se tipifica como delito el uso indebido de la firma electrónica.

India, Ley de tecnología de la información[15], artículo 66C, Castigo del delito relacionado con la identidad:

> Quien, de manera fraudulenta o deshonesta utilice la firma electrónica, la contraseña o cualquier otro medio único de identificación de cualquier otra persona, podrá ser condenado con una pena de prisión por un período de hasta tres años y también con una multa de 100.000 rupias como máximo.

13. Usurpación de identidad

La usurpación de identidad es la utilización por una persona de la identidad de otra persona para engañar a terceros haciéndoles creer que es quien pretende suplantar.

[14] Código Penal de Francia, Ley núm. 1994-653, de 29 de julio de 1994, artículo 8, Diario Oficial de 30 de julio de 1994; Ordenanza núm. 2000-916, de 19 de septiembre de 2000, artículo 3, Diario Oficial de 22 de septiembre (entrada en vigor el 1 de enero de 2002).

[15] Ley de tecnología de la información (enmienda), de 2008.

Nigeria, Código Penal[16], artículos 484 y 485:

> Quien, con intención de estafar a una persona, se presente como otra persona, en vida o fallecida, comete un delito y se le podrá condenar a una pena de prisión de tres años. Si el delincuente suplanta a una persona con derecho por testamento o por ley a una propiedad concreta y comete el delito para obtener esa propiedad o su posesión, podrá ser condenada a una pena de prisión de 14 años.
>
> Quien, sin autorización o justificación legítimas, cuya carga de la prueba le incumbe, haga con el nombre de otra persona, ante cualquier tribunal o persona legalmente autorizada a ese efecto, una declaración de responsabilidad de cualquier clase o de reconocimiento de un título u otro instrumento comete un delito y podrá ser condenado a una pena de prisión de siete años.

14. Falsificación de documento de identificación

Además de la obtención o utilización indebida de información sobre la identidad, el acto de falsificar un documento que acredita la identidad de una persona puede considerarse un delito.

Argentina, Código Penal[17], artículo 292:

> […] Si el documento falsificado o adulterado fuere de los destinados a acreditar la identidad de las personas o la titularidad del dominio o habilitación para circular de vehículos automotores, la pena será de tres a ocho años.

Noruega, Código Penal[18], artículos 179 y 182:

> Se entiende por documentos en este código cualquier objeto que contenga una declaración por escrito o de otra forma que constituya la prueba de cualquier derecho, obligación o exención de obligación o parezca estar destinado a servir como prueba.
>
> Quien con intención ilícita utilice como auténtico o verdadero cualquier documento falso o falsificado, o que esté adjunto a ese documento, podrá ser condenado a multas o penas de prisión de dos años como máximo, pero no de más de cuatro años si el documento considerado es un documento noruego o un documento extranjero oficial. Si el documento ha sido utilizado con la intención de obtener una prueba para una queja legítima o para la protección contra una queja legítima, la sanción podrá ser una multa o una pena de prisión de un año como máximo.

[16] Código Penal de Nigeria de 1990, véase: http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm.
[17] Modificado por la Ley Federal núm. 24.410/95.
[18] Código Penal de Noruega, Ley de 22 de mayo de 1902, núm. 10, véase: http://www.ub.uio.no/ujur/ulovdata/lov-19020522-010-eng.pdf.

Finlandia, Código Penal[19], capítulo 16, artículo 5, Delitos contra las autoridades públicas:

> Quien para inducir a error a una autoridad pública proporcione un nombre falso o proporcione información falsa o engañosa sobre su identidad, o con ese propósito utilice el documento de identidad, el pasaporte, el permiso de conducir u otro certificado similar perteneciente a otra persona, podrá ser condenado por falsificación de identidad a una multa o a una pena de prisión de seis meses como máximo.

Ibid., capítulo 33, Delitos de falsificación, artículo 1, Falsificación (769/1990):

> Quien elabore un documento u otro instrumento falso o falsifique dicho documento o instrumento para ser utilizado como prueba engañosa o utilice un instrumento falso o falsificado como prueba engañosa podrá ser condenado por falsificación a una multa o a una pena de prisión de dos años como máximo. El intento también es punible.

Letonia, Código Penal[20], artículo 177:

> 1) Quien ingrese deliberadamente datos falsos en un sistema automatizado de tratamiento de datos para adquirir la propiedad de otra persona o los derechos a esa propiedad, o adquirir otros beneficios materiales, a fin de influir en la gestión de los recursos correspondientes (fraude informático), podrá ser condenado a una pena de privación de libertad de no más de cinco años o de detención provisional o de servicio comunitario, o a una multa que no sea más de ocho veces el salario mínimo mensual.
>
> 2) Quien cometa un fraude informático, de manera repetida, o forme parte de un grupo que cometa ese fraude previa concertación de un acuerdo, podrá ser condenado a una pena de privación de libertad de no más de ocho años o a la confiscación de la propiedad o a una multa que no sea más de 150 veces el salario mínimo mensual.
>
> 3) Quien cometa un fraude informático, si ha sido cometido a gran escala, podrá ser condenado a una pena de privación de libertad de no menos de ocho años y de quince años como máximo, o a una multa que no sea más de 200 veces el salario mínimo mensual, con o sin confiscación de la propiedad.

15. Falsificación de la identidad en un documento expedido por un organismo público

Los legisladores han dedicado especial atención a las circunstancias en que un organismo público expide un documento falsificado.

[19] Código Penal de Finlandia (39/1889, incluidas las modificaciones hasta 940/2008), artículo 5, *Proporcionar información de identificación falsa* (563/1998); véase: http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf.

[20] Código Penal de Letonia, Ley de 12 de febrero de 2004, capítulo XVIII, Delitos contra la propiedad, artículo 177; véase: http://www.legislationline.org/download/action/download/id/1683/file/4b5d86c3826746957aa400893abc.htm/preview.

Francia, Código Penal[21], artículo 441-2:

> La falsificación de un documento expedido por un organismo público con el fin de establecer un derecho, una identidad o una capacidad, o para conceder una autorización será castigada con cinco años de prisión y una multa de 75.000 euros.

16. Documento falso

La definición de un documento falso puede ser importante para el concepto de falsificación de un documento, aun cuando esté relacionado con una identidad falsa.

Nigeria, Código Penal[22], artículo 464:

> Se considerará falso un documento o un escrito:
>
> […]
>
> *c)* Si la totalidad o una parte sustancial del documento o escrito parece haber sido elaborada por una persona o en nombre de una persona que, de hecho, no existe; o
>
> *d)* Si el documento o escrito se realiza en nombre de una persona real, ya sea por esa persona o con su autorización, con la intención fraudulenta de que parezca haber sido realizado por una persona, real o ficticia, que no sea quien lo elabora o quien autoriza su elaboración.

Turquía, Código Penal[23], artículo 157:

> Quien mediante ardid y en detrimento de terceros engañe a otra persona para obtener un beneficio indebido para sí o para un tercero podrá ser condenado a una pena de prisión de uno a cinco años y a una multa correspondiente a cinco mil días.

Croacia, Código Penal[24], artículo 224a, Fraude informático:

> 1) Quien, con el fin de obtener ganancias pecuniarias ilegales para sí o para un tercero, ingrese, utilice, adultere, suprima o inutilice datos electrónicos o programas informáticos o inutilice u obstaculice el funcionamiento o el uso del sistema informático o del programa informático causando de esa forma un daño a un tercero, podrá ser condenado a una pena de prisión de seis meses a cinco años.
>
> 2) Quien cometa el delito mencionado en el párrafo 1 con el único propósito de causar daño a un tercero podrá ser condenado a una pena de prisión de tres meses a tres años.

---

[21] Ordenanza núm. 2000-916, de 19 de septiembre de 2000, artículo 3, Diario Oficial de 22 de septiembre de 2000 (entrada en vigor el 1 de enero de 2002).

[22] Código Penal de Nigeria, de 1990, capítulo 43, artículo 464; véase: http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm.

[23] Código Penal de Turquía, Ley núm. 5237, aprobada el 26 de septiembre de 2004 (Diario Oficial núm. 25611, de 12 de octubre de 2004); véase: http://www.legislationline.org/documents/action/popup/id/6872/preview.

[24] Diario Oficial de la República de Croacia, *"Narodne novine"*, núm. 110, de 21 de octubre de 1997 (entrado en vigor el 1 de enero de 1998); véase: http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Code.pdf.

3) Quien, sin autorización, produzca, obtenga, venda, posea o haga accesible para un tercero, dispositivos, equipos, programas informáticos o datos electrónicos especiales creados y adaptados para perpetrar los delitos mencionados en los párrafos 1 o 2 del presente artículo podrá ser condenado al pago de una multa o a una pena de prisión de tres años como máximo.

4) Los dispositivos, equipos, datos electrónicos o programas informáticos especiales creados, utilizados o adaptados para cometer delitos y que hayan sido utilizados para perpetrar el delito mencionado en el párrafo 1 y 2 del presente artículo serán decomisados.

5) Quien intente cometer el delito mencionado en los párrafos 2 y 3 del presente artículo será castigado.

17. Violación de datos personales y sitios web

Como ya se ha señalado, los datos y los códigos personales pueden representar información relativa a la identidad. Si bien los delitos de identidad no siempre se basan en cuestiones de privacidad, la violación de datos y de códigos personales puede implicar la obtención o el uso indebidos de información sobre la identidad.

Chile, Código Penal[25], artículos 269F y 269G:

Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses […].

Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses […].

18. Skimming

Skimming es la práctica que consiste en copiar datos personales contenidos en registros electrónicos como, por ejemplo, la banda magnética de las tarjetas de crédito, mediante pequeños dispositivos que leen la información allí registrada.

[25] Código Penal de Chile, de 12 de noviembre de 1874, artículos 269F y 269G; véase: http://www.servicioweb.cl/juridico/Codigo%20Penal%20de%20Chile%20libro2.htm.

Japón, Ley núm. 128 de 1999[26], artículo 161-2, Fabricación ilegal de registros electromagnéticos:

> 1. Una persona que, con la intención de administrar indebidamente la actividad económica de otra persona, fabrica ilegalmente un registro electromagnético a efectos de administrar esa actividad y está relacionada con el derecho, el deber o la certificación de hecho, podrá ser condenada a una pena de prisión con trabajos forzados de no más de cinco años o a una multa que no exceda de 500.000 yenes.
>
> 2. Si el delito establecido en el párrafo anterior se comete contra un registro electromagnético que debe ser preparado por una oficina pública o un funcionario público, el autor podrá ser condenado a una pena de prisión con trabajos forzados de no más de diez años o a una multa que no exceda de un millón de yenes.
>
> 3. Una persona que, con la intención indicada en el párrafo 1, instala un registro electromagnético fabricado ilegalmente para administrar la actividad económica de otra persona, que guarde relación con el derecho, el deber o la certificación de hecho, podrá ser condenado a la misma pena prescrita para la persona que fabrique ilegalmente ese registro electromagnético.
>
> 4. El intento de cometer el delito establecido en el párrafo anterior será punible.

Japón, Código Penal[27], artículo 163-2, Fabricación ilegal de tarjetas de pago con registro electromagnético:

> 1. Una persona que, con el fin de administrar indebidamente las actividades financieras de otra persona, fabrique ilegalmente un registro electromagnético para dicha administración y elabore una tarjeta de crédito u otra tarjeta de pago para efectuar pagos, podrá ser condenada a una pena de prisión con trabajos forzados de no más de diez años o a una multa que no exceda de un millón de yenes. Una persona que fabrique ilegalmente un registro electromagnético para crear una tarjeta de débito con el fin de retirar dinero podrá ser condenada a la misma pena.
>
> 2. Una persona que, con el fin especificado en el párrafo anterior, instale para su uso un registro electromagnético fabricado ilegalmente, como se ha descrito en el mismo párrafo, para la administración de las actividades financieras de otra persona, será objeto del trato prescrito en ese párrafo.
>
> 3. Una persona que, con el fin descrito en el párrafo 1, transfiera, preste o importe una tarjeta creada con un registro electromagnético ilegal, según se especifica en el mismo párrafo, será objeto del trato prescrito en ese párrafo.

[26] Ley de acceso informático no autorizado (Ley núm. 128 de 1999); véase: http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf.

[27] Ley núm. 45, de 1907.

19. Delitos relacionados con registros electromagnéticos y tarjetas de pago con registros electromagnéticos

Japón, Código Penal, artículo 163-3, Posesión de tarjetas de pago con registros electromagnéticos ilegales:

> 1. Una persona que, con el fin establecido en el párrafo 1 del artículo anterior, posee la tarjeta descrita en el párrafo 3 de ese artículo podrá ser condenada a una pena de prisión con trabajos forzados de no más de cinco años o una multa que no exceda de 500.000 yenes.

Ibid., artículo 163-4, Preparación de la fabricación ilegal de tarjetas de pago con registros electromagnéticos:

> 1. Una persona que, con el fin de cometer el acto descrito en el artículo 163-2, párrafo 1, obtiene la información correspondiente al registro electromagnético especificado en ese párrafo, podrá ser condenado a una pena de prisión con trabajos forzados de no más de tres años o a una multa que no exceda de 500.000 yenes. Una persona que, conociendo la intención de quien procura obtener la información, se la proporciona, podrá ser condenada a la misma pena.
>
> 2. Una persona que, con el fin establecido en el párrafo anterior, conserva información obtenida ilícitamente correspondiente a un registro electromagnético como se establece en el artículo 163-2, párrafo 1, será objeto del mismo trato que el prescrito en el párrafo anterior.
>
> 3. Una persona que, con el fin establecido en el párrafo 1, prepara instrumentos o materiales, será objeto del mismo trato que el prescrito en ese párrafo.

Argentina, Ley Federal núm. 25.930, artículo 173:

> 15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.

Venezuela, Ley 37.313/2001, artículos 16 y 17:

> *Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.* Toda persona que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente […].
>
> […] En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes [...].
>
> *Apropiación de tarjetas inteligentes o de un instrumento destinado a los mismos fines,* […].
>
> [...] La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

20. Utilización no autorizada de datos de una tarjeta de crédito

Canadá, Proyecto de ley S-4 por el que se modifica el Código Penal (hurto de identidad y conducta indebida conexa):

> Toda persona que, de manera fraudulenta y sin buena fe, posee, utilice, hace objeto de tráfico o permite a otra persona que utilice los datos de la tarjeta de crédito, incluida la información personal de autenticación, independientemente de que los datos sean o no auténticos, que permitan a una persona utilizar una tarjeta de crédito u obtener servicios proporcionados por el emisor de una tarjeta de crédito a los titulares de las tarjetas de crédito será culpable de […].

21. Hurto de identidad

Algunas definiciones del hurto de identidad lo vinculan con el fraude, mientras que otras no lo relacionan con la comisión de un fraude. El término "hurto" puede utilizarse en el sentido de uso, más que en el sentido de obtención.

Estados Unidos, 18 U.S.C. § 1028 *a)* 7), Acto de hurto de identidad:

> Quien transfiere, posee o utilice sin autorización legítima un medio de identificación de otra persona con la intención de cometer o ayudar a cometer cualquier actividad ilícita o relacionada con esta, que constituya una violación de la legislación federal o un delito en virtud de las leyes estatales o locales.

Ibid., 15 U.S.C. 1681a *q)* 3), Definición de hurto de identidad:

Hurto de identidad: se entiende por "hurto de identidad" un fraude cometido utilizando información relativa a la identidad de otra persona, con sujeción a una definición más amplia que la Comisión pueda prescribir por reglamento.

> *a)* Por "hurto de identidad" se entiende un fraude que se comete o intenta cometer utilizando la información de identidad de otra persona sin autorización legítima.
>
> *b)* Por "información de identificación" se entiende cualquier nombre o número que pueda utilizarse, por separado o conjuntamente con cualquier otra información, para identificar a una persona determinada, incluidos:
>
> 1) El nombre, el número de seguridad social, la fecha de nacimiento, el permiso de conducir expedidos por un Estado o Gobierno, o un número de identificación, número de registro de extranjero, número de pasaporte oficial, número de empleado o de identificación fiscal.
>
> 2) Datos biométricos únicos como las huellas digitales, la huella vocal, la imagen de la retina o del iris, u otra representación física única.

3) El número particular de identificación electrónica, la dirección o el número de ruta bancario.

4) La información de identidad de las telecomunicaciones o del dispositivo de acceso.

Canadá, Proyecto de ley S-4 por el que se enmienda el Código Penal (hurto de identidad y conducta indebida conexa), artículo 402.2:

1) Hurto de identidad: comete un delito quien, de forma intencional, obtenga o posea información de identidad de otra persona en circunstancias que razonablemente permitan inferir que será utilizada para cometer un delito que incluye el fraude, el engaño o la mentira como elementos del delito.

Ibid., artículo 402.1:

A los efectos de los artículos 402.2 y 403, se entenderá por la expresión "información de identidad" toda información —incluida la información biológica y psicológica— que pueda utilizarse por separado o conjuntamente con otra información para identificar o intentar identificar a una persona, como huellas digitales, huella vocal, imagen de la retina, imagen del iris, perfil de ADN, nombre, dirección, fecha de nacimiento, firma escrita, firma electrónica, firma digital, nombre de usuario, número de tarjeta de crédito o de débito, número de cuenta de una institución financiera, número de pasaporte, número de seguridad social, número del seguro de salud, número del permiso de conducir o clave de acceso.

22. Hurto de identidad vinculado con las computadoras

Estados Unidos 18 U.S.C. § 1030 *a)* 2), Fraude y actividad conexa relacionada con las computadoras:

2) [Quien] acceda deliberadamente a una computadora sin autorización o sin autorización suficiente para hacerlo, y obtenga de esa forma:

A) Información contenida en un registro financiero de una institución financiera, o de un emisor de tarjetas definido en el artículo 1602 *n)* del título 15, o contenido en un expediente de un organismo de información sobre el consumidor acerca de un consumidor, conforme a las definiciones que figuran en la Fair Credit Reporting Act (Ley de información sobre créditos) (15 U.S.C. 1681 y ss.);

B) Información de cualquier departamento u organismo de los Estados Unidos; o

C) Información de cualquier computadora protegida si en el acto ha intervenido una comunicación interestatal o extranjera;

23. Preparación

El concepto jurídico de preparación plantea interrogantes con respecto a la forma en que la legislación define o debe definir un delito y sus etapas preparatorias.

Alemania, Código Penal[28], artículo 275, Preparación para la falsificación de documentos oficiales de identificación:

> 1) Quien prepare la falsificación de documentos oficiales de identidad mediante la fabricación, la obtención para sí o para un tercero, la oferta en venta, el almacenamiento, la entrega a un tercero, o la importación o exportación de:
>
> 1. Planchas, marcos, tipos, clichés, negativos, stencils o equipos similares que por su naturaleza sean apropiados para cometer el acto; o
>
> 2. Papel, idéntico o prácticamente igual que el tipo de papel destinado a la producción de documentos oficiales de identidad y especialmente protegido contra las imitaciones; o
>
> 3. Formularios en blanco para los documentos oficiales de identificación,
>
> podrá ser condenado a una pena de prisión de dos años como máximo o a una multa.
>
> 2) Si el infractor actúa profesionalmente o como miembro de una banda que ha organizado la comisión de forma continua de los delitos mencionados en el apartado 1), el castigo será una pena de prisión de tres meses a cinco años.
>
> 3) Los apartados 2) y 3) del artículo 149 se aplicarán en consecuencia.

Alemania, Código Penal[29], artículo 202c:

Preparación de la interceptación de datos y espionaje de datos.

> 1) Quien prepare un delito con arreglo a lo dispuesto en el artículo 202a o 202b produciendo, obteniendo para sí o para un tercero, vendiendo, entregando a un tercero, divulgando o poniendo a disposición de terceros de cualquier otra forma:
>
> 1. Contraseñas o claves de acceso o cualquier otro código de protección, que permita el acceso a datos (§ 202a apartado 2)), o
>
> 2. Programas informáticos, con el objeto de cometer el delito mencionado, podrá ser condenado a una pena de prisión de un año como máximo o a una multa.

[28] Código Penal de Alemania en su versión promulgada el 13 de noviembre de 1998; Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3322, modificado en último término por el artículo 3 de la Ley de 2 de octubre de 2009; Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, pág. 3314; véase: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169.

[29] *Ibid.*

24. Obtención

En las legislaciones nacionales se abordan distintos medios por cuales los delincuentes toman posesión de la información relativa a la identidad.

Reino Unido, Ley sobre tarjetas de identidad de 2006, artículo 8:

> A los efectos del presente artículo […]; y se ha obtenido indebidamente un documento de identidad si se ha proporcionado información falsa en la solicitud de expedición del documento o en relación con esa solicitud, o en una solicitud para su modificación, a la persona que lo haya expedido o (según proceda) a una persona facultada para modificarlo […].

Francia, Código Penal[30], artículo 441-6:

> El hecho de hacerse expedir indebidamente por una administración pública o por un organismo encargado de una misión de servicio público, por el medio fraudulento que sea, un documento destinado a establecer un derecho, una identidad o una capacidad, o a conceder una autorización será castigado con dos años de prisión y una multa de 30.000 euros.
>
> Será castigado con las mismas penas el hecho de prestar una declaración falsa con el fin de obtener de una administración pública o de un organismo encargado de una misión de servicio público un subsidio, un pago o una ventaja indebidos.

Francia, Código Penal[31], artículo 441-5:

> El hecho de proporcionar fraudulentamente a otra persona un documento expedido por una administración pública con el fin de establecer un derecho, una identidad o una capacidad o para conceder una autorización será castigado con cinco años de prisión y una multa de 75.000 euros.
>
> Las penas se elevarán a siete años de prisión y a 100.000 euros de multa cuando la infracción se cometa:
>
> 1) por una persona depositaria de la autoridad pública o encargada de una misión de servicio público que actúe en el ejercicio de sus funciones;
>
> 2) de forma habitual;
>
> 3) o con el propósito de facilitar la comisión de un delito o de obtener la impunidad de su autor.

[30] Código Penal de Francia, artículo 441-6, Ordenanza núm. 2000-916 de 19 de septiembre de 2000, artículo 3, Diario Oficial de 22 de septiembre de 2000 (entrada en vigor el 1 de enero de 2002); véase: http://www.cyberlawdb.com/docs/france/penalcode.pdf.

[31] Código Penal de Francia, Ordenanza núm. 2000-916 de 19 de septiembre de 2000, artículo 3, Diario Oficial de 22 de septiembre de 2000 (entrada en vigor el 1 de enero de 2002); véase: http://www.cyberlawdb.com/docs/france/penalcode.pdf.

25. Transferencia

Una vez que la información relativa a la identidad se encuentre en posesión del infractor, este no necesariamente la utilizará y podrá transferirla (inclusive mediante su venta).

Canadá, Proyecto de ley S-4 por el que se modifica el Código Penal (hurto de identidad y conducta indebida conexa), artículo 402.2:

> 2) Comete un delito quien transmita, ponga a disposición, distribuya, venda u ofrezca en venta información de identidad de otra persona, o la posea con algunos de esos propósitos, si tiene la certeza de que esa información será utilizada para cometer un delito que incluye el fraude, el engaño o la mentira como elementos del delito o si incurre en imprudencia.

26. Utilización

Al final de la sucesión de actos, el infractor utiliza la información relativa a la identidad para cometer otros delitos.

Canadá, Proyecto de ley S-4 por el que se modifica el Código Penal (hurto de identidad y conducta indebida conexa), artículo 402.2:

> 3) A los efectos de los incisos 1) y 2), un delito punible mencionado en cualquiera de esos incisos incluye un delito en virtud de cualquiera de los siguientes artículos:
>
> *a)* artículo 57 (falsificación o expedición de pasaporte falso);
>
> *b)* artículo 58 (utilización fraudulenta de certificados de nacionalidad);
>
> *c)* artículo 130 (suplantación de un agente de policía);
>
> *d)* artículo 131 (falso testimonio);
>
> *e)* artículo 342 (robo, falsificación, etc., de una tarjeta de crédito);
>
> *f)* artículo 362 (declaración falsa o fraudulenta);
>
> *g)* artículo 366 (falsificación);
>
> *h)* artículo 368 (utilización, tráfico o posesión de documentos falsos);
>
> *i)* artículo 380 (fraude); y
>
> *j)* artículo 403 (falsificación de identidad).

Estados Unidos, 18 U.S.C. art. 1028, capítulo 47, Fraude y declaraciones falsas:

> 3) Una multa con arreglo a este título o una pena de prisión de no más de veinte años, o ambas penas, si el delito se comete:
>
> a) para facilitar un delito de tráfico de drogas (definido en el artículo 929 a) 2));
>
> b) en relación con un delito de sangre (definido en el artículo 924 c) 3)); o

c) después de que una declaración de culpabilidad anterior en virtud de este artículo se haga definitiva.

Una multa con arreglo a este título o una pena de prisión de no más de treinta años o ambas, si el delito se comete para facilitar un acto de terrorismo nacional (definido en el artículo 2331 5) de este título) o un acto de terrorismo internacional (definido en el artículo 2331 1) de este título) […].

27. Posesión

Si bien la posesión de documentos o de equipos relacionada con el delito de identidad es difícil de legislar, ya que hay datos y dispositivos que pueden no utilizarse nunca para realizar actividades ilícitas o pueden ser utilizados algunas veces con fines legítimos, algunos países han tomado la iniciativa de regular esta cuestión:

Reino Unido, Ley sobre tarjetas de identidad[32], artículo 25:

Comete un delito una persona que tiene en su posesión o bajo su control, con una excusa razonable:

a) Un documento de identidad falso;

b) Un documento de identidad obtenido indebidamente;

c) Un documento de identidad perteneciente a otra persona; o

d) Cualquier equipo, artículo o material que, a su entender, es o ha sido especialmente diseñado o adaptado para la fabricación de documentos de identidad falsos o ha de ser utilizado para fabricar esos documentos.

Francia, Código Penal[33], artículo 441-3:

La tenencia fraudulenta de algunos de los documentos falsos definidos en el artículo 441-2 será castigada con dos años de prisión y una multa de 30.000 euros.

La pena se elevará a cinco años de prisión y a 75.000 euros de multa en caso de tenencia fraudulenta de varios documentos falsos.

28. Uso indebido con fines delictivos

Se han tipificado en legislaciones nacionales diferentes modalidades de uso indebido de información relativa a la identidad.

[32] Ley sobre tarjetas de identidad, de 2006.
[33] Ordenanza núm. 2000-916, de 19 de septiembre de 2000, artículo 3, Diario Oficial de 22 de septiembre de 2000 (entrada en vigor el 1 de enero de 2002).

Alemania, Código Penal[34], artículos 276 y 281:

> Obtención de documentos de identificación oficiales falsos:
>
> 1) Quien:
>
> 1. importe o exporte; o,
>
> 2. con la intención de utilizar para permitir el engaño en relaciones legales, obtenga para sí o para un tercero, almacene o entregue a un tercero un documento de identificación oficial falso o falsificado o un documento de identificación oficial que contenga una acreditación falsa, del tipo indicado en los artículos 271 y 348, podrá ser condenado a una pena de prisión de no más de dos años o a una multa.
>
> 2) Si el autor actúa en el marco de una relación comercial o como miembro de una banda de delincuentes, que ha organizado la comisión continua de delitos objeto del apartado 1), podrá imponerse una pena de prisión de tres meses a cinco años.
>
> Uso indebido de documentos de identificación:
>
> 1) Quien, a los efectos de engañar en el marco de relaciones legales, utilice un documento de identificación expedido para otra persona, o quien, con objeto de engañar en el marco de legislaciones legales, dé a un tercero un documento de identificación que no haya sido expedido para esa persona, podrá ser condenado a una pena de prisión de no más de un año o a una multa. El intento de cometer el acto es punible.
>
> 2) Se considerarán equivalentes a un documento de identificación los certificados y otros documentos que se utilizan en las transacciones como documentos de identificación.

Suecia, Código Penal[35], artículo 12:

> Una persona que usa indebidamente un pasaporte, un certificado o un documento análogo expedido en nombre de una persona determinada haciéndose pasar esa persona o un tercero por el destinatario del documento, o que transmite el documento que será indebidamente utilizado de esa forma o transmite un documento falso, que fuera elaborado a partir de una copia carbónica o una reproducción fotográfica o por otro medio, haciéndolo pasar por un ejemplar auténtico de un determinado documento, será, si el acto pone en peligro la prueba, condenado por uso indebido de un documento a una multa o a una pena de prisión de seis meses como máximo o, si el delito es grave, a una pena de prisión de dos años como máximo.

[34] Código Penal de Alemania, en la versión promulgada el 13 de noviembre de 1998, Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, página 3322, modificado por última vez por el artículo 3 de la Ley de 2 de octubre de 2009, Diario Oficial de la República Federal de Alemania [*Bundesgesetzblatt*] I, página 3214, véase: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169.

[35] Código Penal de Suecia, de 1965, capítulo 15, sobre falsa declaración, falso proceso y otras declaraciones falsas, artículo 12; véase: http://www.cyberlawdb.com/docs/sweden/penalcode.pdf.

29. Circunstancias agravantes

Los legisladores también han centrado su atención en las circunstancias agravantes relacionadas con los delitos de identidad.

Estados Unidos, 18 U.S.C. § 1028 a) 7), hurto de identidad agravado:

> Delitos:
>
> 1) *En general*: Quien durante y en relación con uno de los delitos graves previstos en el apartado *c)*, de forma intencional, transfiera, posea o utilice, sin autorización legítima, medios de identificación de otra persona, además de ser condenado a la pena prevista para ese delito, podrá ser condenado a una pena de prisión de dos años.
>
> 2) *Delito de terrorismo*: Quien, durante y en relación con uno de los delitos graves enumerados en el artículo 2332b *g)* 5) B), de forma intencional, transfiera, posea o utilice, sin autorización legítima, un medio de identificación de otra persona o un documento de identificación falso podrá ser condenado a una pena de prisión de cinco años, que se sumará a la pena prevista para el delito considerado.

Chile, Código Penal[36], artículo 269H, Circunstancias de agravación punitiva:

> Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
>
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
>
> 2. Por servidor público en ejercicio de sus funciones.
>
> 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
>
> 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
>
> 5. Obteniendo provecho para sí o para un tercero.
>
> 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
>
> 7. Utilizando como instrumento a un tercero de buena fe.
>
> 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

[36] Código Penal de Chile, de 12 de noviembre de 1874; véase: http://www.servicioweb.cl/juridico/Codigo%20Penal%20de%20Chile%20libro2.htm.

Francia, Código Penal, artículo 441-2[37]:

Las penas se elevarán a siete años de prisión y a 100.000 euros de multa cuando la falsificación o el uso de lo falsificado se cometa:

1. por una persona depositaria de la autoridad pública o encargada de una misión de servicio público que actúe en el ejercicio de sus funciones;

2. de forma habitual;

3. o con el propósito de facilitar la comisión de un delito o de proporcionar impunidad a su autor.

30. Fraude/fraude de identidad

Los legisladores también han abordado la información relativa a la identidad en relación con el fraude en general o delitos especiales de fraude de identidad.

Canadá, Proyecto de ley S-4 por el que se modifica el Código Penal (hurto de identidad y conducta indebida conexa), artículo 403 (fraude de identidad):

1) Comete un delito quien suplante fraudulentamente a otra persona, que esté en vida o haya fallecido,

a) con la intención de obtener una ventaja para sí o para un tercero;

b) con la intención de obtener una propiedad o un interés en una propiedad;

c) con la intención de causar un daño a la persona suplantada o a un tercero; o

d) con la intención de evitar la detención o el enjuiciamiento o de obstruir o distorsionar el funcionamiento de la justicia o de oponerse a ella.

31. Intento de cometer otro delito

La legislación de algunos países examinados establece un vínculo entre el delito de identidad y la intención de cometer otros delitos.

Reino Unido, Ley sobre tarjetas de identidad[38], artículos 1 a 4:

1) Comete un delito quien con la intención necesaria tiene en su posesión o bajo su control:

a) un documento de identidad que es falso y que sabe o considera que es falso;

[37] Código Penal de Francia, Ley núm. 1996-647, de 22 de julio de 1996, artículo 2, Diario Oficial de 23 de julio de 1996; véase: http://www.cyberlawdb.com/docs/france/penalcode.pdf.
[38] Ley de tarjetas de identidad de 2006.

b) un documento de identidad obtenido indebidamente y que sabe o considera que ha sido obtenido indebidamente; o

c) un documento de identidad relacionado con otra persona.

2) La intención necesaria a los efectos de 1) es:

a) la intención de utilizar el documento para establecer hechos registrables sobre sí; o

b) la intención de permitir a otra persona o de inducir a otra persona a utilizarlo para establecer, afirmar o verificar hechos registrables sobre sí o sobre cualquier otra persona (con excepción, en el caso de un documento a que se refiera el inciso *c)* del apartado 1) del individuo con el que se relaciona).

3) Comete un delito quien con la intención necesaria de conseguir o tener en su posesión o bajo su control:

a) cualquier equipo que según entiende, esté o haya sido especialmente diseñado o adaptado para fabricar documentos de identidad falsos; o

b) cualquier artículo o material que, según entiende, esté o haya sido especialmente diseñado o adaptado para ser utilizado en la fabricación de documentos de identidad falsos.

4) La intención necesaria a los efectos de 3) es:

a) que esa persona u otra persona prevea fabricar un documento de identidad falso; y

b) que ese documento sea utilizado por alguien para establecer, afirmar o verificar hechos registrables acerca de una persona.

Nigeria, Código Penal[39], artículo 479:

> Quien, a sabiendas y con la intención de ser inscrito en un registro de nacimiento, defunción o matrimonio, hace una declaración falsa relativa a cualquier elemento cuya inscripción en ese registro prescriba la ley, comete un delito grave y podrá ser condenado a una pena de prisión de tres años.

[39] Código Penal de Nigeria de 1990, capítulo 18; véase: http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm.

ANEXOS

A.1. Legislación sobre el delito de identidad: definiciones, medios o formatos de la información relativa a la identidad, información de identidad protegida

País	Legislación	Conceptos de información relacionada con la identidad				
		Denominación	Forma de información	Núm. de seguridad social/ núm. de identificación personal/núm. de seguro de salud	Nombre/ dirección/fecha de nacimiento/firma escrita	
ALBANIA	Código Penal	Documentos de identidad	Todas	Sí	Sí	
ALEMANIA	Código Penal	Documentos de identificación	Documental			
ARGENTINA	Código Penal	Base de datos personal	Bases de datos, archivos de datos	Sí	Sí	
AUSTRALIA	Ley de Privacidad (1988)	Información personal	Cualquier información u opinión			
AUSTRIA	Código Penal y Ley 565/78	Datos personales	Todas	Sí		
AZERBAIYÁN	Código Penal	Ley de protección de datos informáticos	Computadoras, sistemas, redes			
BOLIVIA (Estado Plurinacional de)	Ley 1768/97	Datos informáticos	Soporte electrónico			
BRASIL	Código Penal	-	Documental			
BULGARIA	Código Penal	Datos personales, contraseñas	Todas			
CANADÁ	Proyecto de Ley S-4	-	Todas (incluidas las biológicas/ fisiológicas)	Sí	Sí	
CHILE	Ley 19.223/93	Sistema de datos	Datos contenidos en un sistema	Sí		
CHINA	Código Penal	Tarjetas de identificación nacional	Todas			
COLOMBIA	Código Penal	Datos personales	Bases de datos			
COSTA RICA	Ley 8148	Secreta	Medios electrónicos			

Categorías de la información relacionada con la identidad					
	Nacimiento/estado civil o certificado de defunción/tarjeta de identidad/pasaporte/ documento de inmigración	**Permiso de conducir/ tarjeta de situación militar/tarjeta de elector en elecciones políticas**	**Núm. de tarjeta de crédito o débito/ núm. de cuenta bancaria**	**Contraseña de acceso a e-mail o navegación en la web/dirección MAC o IP/firma electrónica o digital/ nombre de usuario**	**Huella dactilar/huella vocal/imagen de la retina o del iris/perfil de ADN**
	Sí				
	Sí	Sí			
	Sí	Sí			
	Sí	Sí	Sí	Sí	Sí

País	Legislación	Conceptos de información relacionada con la identidad				
		Denominación	Forma de información	Núm. de seguridad social/ núm. de identificación personal/núm. de seguro de salud	Nombre/ dirección/fecha de nacimiento/firma escrita	
ECUADOR	Código Penal (modificado en 2002)	Doc. personal, datos familiares o personales restringidos	Datos y medios electrónicos			
ESPAÑA	Código Penal-Ley 10/1995	Datos personales	Medios de comunicación informáticos, archivos electrónicos o telemáticos	Sí		
ESTADOS UNIDOS	Código de los EE.UU., título 18, capítulo 47			Sí		
ESTONIA	Código Penal	Información personal sensible	Computadoras, bancos de datos			
FEDERACIÓN DE RUSIA	Ley Federal núm. 152-FZ/2006 (Ley sobre datos personales)	Datos personales, datos de identidad	Bases de datos, sistemas de información, biométrica			
FILIPINAS	Ley de dispositivos de acceso de 1998	Identidades, número de NIP	Tarjeta, placa, código, equipo			
FRANCIA	Código Penal y Ley 88-19/88	Datos	Todos			
GEORGIA	Código Penal	Ley de protección de datos informáticos	Computadoras, sistemas, redes			
HUNGRÍA	Ley LXIII de 1992	Datos personales	Todas			
INDIA	Ley de tecnologías de la información (2008)	Información de identidad	Todas			
ITALIA	Código Penal	Sistemas informáticos relacionados con el orden público	Código, palabras clave	Sí		
JAPÓN	Código Penal y Ley 128/99	Registros electromagnéticos, código de identificación	Electromagnética			

Categorías de la información relacionada con la identidad					
	Nacimiento/estado civil o certificado de defunción/tarjeta de identidad/pasaporte/ documento de inmigración	**Permiso de conducir/ tarjeta de situación militar/tarjeta de elector en elecciones políticas**	**Núm. de tarjeta de crédito o débito/ núm. de cuenta bancaria**	**Contraseña de acceso a e-mail o navegación en la web/dirección MAC o IP/firma electrónica o digital/ nombre de usuario**	**Huella dactilar/huella vocal/imagen de la retina o del iris/perfil de ADN**
	Sí	Sí	Sí	Sí	
				Sí	
			Sí	Sí	

País	Legislación	Conceptos de información relacionada con la identidad				
		Denominación	Forma de información	Núm. de seguridad social/ núm. de identificación personal/núm. de seguro de salud	Nombre/ dirección/fecha de nacimiento/firma escrita	
KAZAJSTÁN	Código Penal	Ley de protección de datos informáticos	Computadoras, sistemas, redes			
KIRGUISTÁN	Código Penal	Ley de protección de datos informáticos	Computadoras, sistemas, redes			
MÉXICO	Código Penal (modificado en 1999)	Datos contenidos en los sistemas de instituciones financieras	Datos			
NIGERIA	Código Penal	Documentos electrónicos	Todas			
PERÚ	Código Penal	Acceso indebido a bases de datos	Base de datos o sistema			
PORTUGAL	Ley 109/91	Datos confidenciales				
REINO UNIDO	Ley sobre Fraude/Ley sobre tarjetas de identidad		Documental			
REPÚBLICA DE MOLDOVA	Ley núm. 17-XVI/2007	Datos personales	Sistemas de información, biométrica			
RUMANIA	Ley Anticorrup-ción	Datos sobre los usuarios				
SUDÁFRICA	Ley ECT (de comercio electrónico)	Información personal	Todas	Sí	Sí	
SUECIA	Código Penal	Datos	Marca falsa			
SUIZA	Código Penal					
TURQUÍA	Código Penal	Tarjeta de crédito o bancaria falsificadas	Tarjeta de crédito o bancaria			
VENEZUELA	Ley 37.313/2001	Datos o información personales o patrimonial	Datos			

Categorías de la información relacionada con la identidad					
	Nacimiento/estado civil o certificado de defunción/tarjeta de identidad/pasaporte/ documento de inmigración	**Permiso de conducir/ tarjeta de situación militar/tarjeta de elector en elecciones políticas**	**Núm. de tarjeta de crédito o débito/ núm. de cuenta bancaria**	**Contraseña de acceso a e-mail o navegación en la web/dirección MAC o IP/firma electrónica o digital/ nombre de usuario**	**Huella dactilar/huella vocal/imagen de la retina o del iris/perfil de ADN**
	Sí	Sí	Sí		
	Sí	Sí	Sí		Sí

A.2. Tipología de los delitos de identidad y clasificación de las conductas

País	Legislación	Elaboración de un documento falso o falsificación de un documento auténtico	Uso individual indebido de información relativa a la identidad		
		Elaborar/alterar/interferir/autenticar/reunir/hacer/adaptar/modificar	Poseer/utilizar/retener/obtener/controlar/dar o presentar información falsa/acceder (incluida la violación de la protección de acceso)/adquirir/asignar	Omitir/suprimir	
ALBANIA	Código Penal	Sí	Sí		
ALEMANIA	Código Penal	Sí	Sí	Sí	
ARGENTINA	Código Penal	Sí	Sí		
BRASIL	Código Penal	Sí	Sí	Sí	
CANADÁ	Proyecto de Ley S-4		Sí		
ESTADOS UNIDOS	Código de los EE.UU.	Sí	Sí		
INDIA	Ley de TI (2008)	Sí	Sí		
JAPÓN	Ley 128, de 1999	Sí	Sí		
REINO UNIDO	Ley de fraude/ Ley de tarjetas de identidad	Sí	Sí		
SUDÁFRICA	Ley ECT	Sí	Sí		

A.3. Tipología de los delitos de identidad: elementos subjetivos y requisitos

País	Legislación	Intención				
		Cometer/ayudar/instigar un acto ilegal	Estafar	Engañar	Obtener para sí o un tercero un beneficio o ventaja material ilícita	
Albania	Código Penal					
Alemania	Código Penal	Sí	Sí	Sí	Sí	
Argentina	Código Penal	Sí	Sí	Sí		
Australia	Ley de privacidad (1988)					
Brasil	Código Penal		Sí	Sí	Sí	
Canadá	Proyecto de Ley S-4	Sí	Sí	Sí	Sí	
Estados Unidos	Código de los EE.UU.	Sí	Sí	Sí		
India	Ley de TI (2008)		Sí	Sí		
Japón	Ley 128, de 1999			Sí		
Reino Unido	Ley de fraude/Ley de tarjetas de identidad		Sí			
Sudáfrica	Ley ECT	Sí		Sí	Sí	

	Uso colectivo indebido de información relativa a la identidad	Tráfico de información relativa a la identidad	Daños a la información relativa a la identidad de un tercero	Intento/ conspiración/ ayuda/ instigación
	Transferir/poner a disposición en línea/transmitir/distribuir/ vender o suministrar/ofrecer para la venta o para el suministro (o poseer con ese fin)/entregar/difundir	Transferir/transportar/ eliminar (u obtener el control con ese fin)/ almacenar/importar o exportar	Provocar o afirmar un error/pretender la existencia de datos falsos/destruir, ocultar, distorsionar o suprimir hechos verdaderos/influir en el resultado de una operación de tratamiento de datos	
	Sí			
	Sí	Sí	Sí	Sí
	Sí	Sí		
	Sí		Sí	
	Sí	Sí		
	Sí	Sí		Sí
	Sí			Sí
	Sí			
	Sí		Sí	Sí

			Conciencia o imprudencia		
	Utilizar documentos para certificar o registrar hechos personales	Falta de autorización o permiso	Respecto de la obtención o posesión de información de identidad ajena	Respecto de la falsedad u obtención indebida de documentos	Respecto de la utilización de la información para cometer un delito
		Sí			
			Sí		Sí
		Sí			
	Sí			Sí	Sí
		Sí			

Ejemplos de leyes nacionales y fuentes pertinentes

País	Legislación	Fuente
ALBANIA	Código Penal y Ley núm. 7895 de 27 de enero de 1995	http://www.cyberlawdb.com/docs/albania/albania.pdf
ALEMANIA	Ley Federal de Protección de Datos	http://www.bdd.de/Download/bdsg_eng.pdf
ARABIA SAUDITA	Ley contra el delito cibernético núm. 11428, de 26 marzo de 2007	http://www.saudiembassy.net/announcement/announcement03260701.aspx
ARGENTINA	Código Penal y Ley núm. 25.286/2008	http://www.cyberlawdb.com/docs/argentina/argentina.pdf
ARMENIA	Código Penal	http://www.cyberlawdb.com/docs/armenia/armenia.pdf
AUSTRALIA	Ley de Privacidad, 1988	http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/CDFBC6BC359968E4CA257758001791A7?OpenDocument
AUSTRIA	Código Penal y Ley Federal relativa a la protección de datos personales	http://www.dsk.gv.at/site/6230/default.aspx#E15 http://www.cyberlawdb.com/docs/austria/austria.pdf
AZERBAIYÁN	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
BARBADOS	Ley sobre uso indebido de computadoras, de 18 de julio de 2005	http://www.cyberlawdb.com/docs/barbados/computer_misuse.pdf
BELARÚS	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
BOLIVIA (Estado Plurinacional de)	Código Penal	http://www.oas.org/juridico/spanish/gapeca_sp_docs_bol1.pdf
BOTSWANA	Código Penal	http://www.laws.gov.bw/
BRASIL	Código Penal	http://www.amperj.org.br/store/legislacao/codigos/cp_DL2848.pdf
BULGARIA	Código Penal	http://www.cyberlawdb.com/docs/bulgaria/bulgaria.pdf
CANADÁ	Proyecto de ley S-4, 2009	http://www2.parl.gc.ca/content/hoc/Bills/402/Government/S-4/S-4_4/S-4_4.PDF
CHILE	Ley núm. 19223	http://www.leychile.cl/Navegar?idNorma=30590&buscar=19.223
CHINA	Código Penal	http://www.colaw.cn/findlaw/crime/criminallaw3.html
CHIPRE	Ley núm. 22(III)04	http://www.cyberlawdb.com/docs/cyprus/cyprus.pdf
COLOMBIA	Código Penal y Ley núm. 1273/2009	http://www.derechos.org/nizkor/colombia/doc/penal.html http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html
COSTA RICA	Ley núm. 4573	http://www.pgr.go.cr/scij/scripts/TextoCompleto.dll?Texto&nNorma=47430&nVersion=50318&nTamanoLetra=10&strWebNormativa=http://www.pgr.go.cr/scij/&strODBC=DSN=SCIJ_NRM;UID=sa;PWD=scij;DATABASE=SCIJ_NRM;&strServidor=\\pgr04&strUnidad=D:&strJavaScript=NO

País	Legislación	Fuente
CROACIA	Código Penal	http://www.cyberlawdb.com/docs/croatia/croatia.pdf
ECUADOR	Código Penal	http://www.miliarium.com/Paginas/Leyes/Internacional/Ecuador/General/cp.pdf
EMIRATOS ÁRABES UNIDOS	Ley Federal núm. (2), de 2006	http://www.aecert.ae/Prevention_of_Information_Technology_Crimes_English.pdf
ESLOVAQUIA	Código Penal	http://www.cyberlawdb.com/docs/slovakia/slovakia.pdf
ESPAÑA	Código Penal	http://www.delitosinformaticos.com/legislacion/espana.shtml
ESTADOS UNIDOS	Código Penal	http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_47.html
ESTONIA	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
EX REPÚBLICA YUGOSLAVA DE MACEDONIA	Código Penal	http://www.cyberlawdb.com/docs/macedonia/macedonia.pdf
FEDERACIÓN DE RUSIA	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
FILIPINAS	Ley de comercio electrónico	http://www.cyberlawdb.com/docs/philippines/philippines.pdf
FRANCIA	Código Penal y Ley 88-19/88	http://www.crime-research.org/articles/cybercrime-in-france-overview/2
GEORGIA	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
HUNGRÍA	Ley núm. LXIII de 1992	http://abiweb.obh.hu/adatved/indexek/AVTV-EN.htm
INDIA	Ley de tecnología de la información, de 2008	http://cybercrime.planetindia.net/it-act-2008.htm
INDONESIA	Código Penal	http://www.cyberlawdb.com/docs/indonesia/indonesia.pdf
IRLANDA	Ley de Justicia Penal, de 2001	http://www.irishstatutebook.ie/2001/en/act/pub/0050/print.html
ISRAEL	Ley de computadoras, de 1995	http://www.cybercrimelaw.net/Israel.html
ITALIA	Código Penal	http://it.wikisource.org/wiki/Codice_penale/Libro_II http://guide.supereva.it/diritto/interventi/2001/04/39144.shtml http://www.cyberlawdb.com/docs/italy/italy.pdf
JAMAICA	Ley de interceptación de comunicaciones	http://www.cyberlawdb.com/docs/jamaica/intercep_commun.pdf
JAPÓN	Código Penal y Ley No. 128/99	http://www.npa.go.jp/english/kokusai9/White_Paper_2009_4.pdf
KAZAJSTÁN	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
KIRGUISTÁN	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
LITUANIA	Código Penal y Código de Procedimiento Penal	http://www.cyberlawdb.com/docs/lithuania/lithuania.pdf

País	Legislación	Fuente
MALASIA	Ley de delitos informáticos, de 1997	http://www.cyberlawdb.com/docs/malaysia/cc.pdf
MÉXICO	Código Penal	http://www.delitosinformaticos.com/delitos/ensayomexico.shtml
NIGERIA	Código Penal	http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm#Chapter18
PERÚ	Código Penal	http://www.policiainformatica.gob.pe/pdf/ley27309.pdf
PORTUGAL	Código Penal	http://bdjur.almedina.net/citem.php?field=node_id&value=1224791
REINO UNIDO	Ley sobre el fraude, de 2006, y Ley sobre tarjetas de identidad, de 2006	http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf.
REPÚBLICA CHECA	Código Penal y Código de Procedimiento Penal	http://www.cyberlawdb.com/docs/czech/czech.pdf
REPÚBLICA DE MOLDOVA	Código Penal	http://www.cyberlawdb.com/docs/moldova/moldova.pdf
RUMANIA	Ley anticorrupción	http://www.crime-research.org/library/Romania.html
SINGAPUR	Ley de uso indebido de computadoras	http://www.cyberlawdb.com/docs/singapore/cma.pdf
SUDÁFRICA	Ley ECT, de 2002	http://www.internet.org.za/ect_act.html
SUECIA	Ley de datos personales	http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf
SUIZA	Código Penal	http://www.rhf.admin.ch/rhf/it/home/straf/recht/multilateral/ccc.html
TAYIKISTÁN	Código Penal	http://www.crime-research.org/library/Romania.html
TURQUÍA	Código Penal	http://www.cyberlawdb.com/docs/turkey/turkey.pdf
UCRANIA	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
UZBEKISTÁN	Código Penal	http://www.crime-research.org/library/Criminal_Codes.html
VENEZUELA	Ley núm. 37.313/2001	http://fundabit.me.gob.ve/documento/LECDI.pdf
ZAMBIA	Ley de uso indebido de computadoras y delitos informáticos	http://www.parliament.gov.zm/index.php?option=com_docman&task=doc_view&gid=112

BIBLIOGRAFÍA

1. *Aboso, Gustavo Eduardo, y Zapata, Maria Florência*, "Cibercriminalidad y Derecho Penal", Montevideo, Bef, 2006, págs. 79 a 82.
2. Cahiers de la Securité, núm. 6, Institut Nacional des Hautes Études de Securité, octubre a diciembre de 2008, págs. 42 a 48.
3. *Cifuentes, Santos*, "Derechos Personalísimos", Buenos Aires, Astrea, 2008, págs. 703 a 711.
4. *Cruz, Danielle da Rocha Cruz*, "Criminalidade informática—tipificação penal das condutas ilícitas realizadas com cartões de crédito", Rio de Janeiro, Forense, 2006, págs. 84 a 89, 190 a 200.
5. *Desgens-Pasanau, Guillaume*, "L'identité à l'ère numérique", Paris, Dalloz, 2009, págs. 98 a 105, 117 a 119.
6. "Essential Elements of Criminal Laws to Address Identity-Related Crime", febrero de 2009, circulated by the G8 Lyon-Roma Anti-Crime and Terrorism Group Criminal and Legal Affairs Subgroup.
7. *Faggioli, Garbiele*, "Computer Crimes", Napoli, Esselibri, 2002, págs. 25 y 28.
8. *Feliciano, Guilherme Guimarães*, "Informática e Criminalidade", Ribeirão Preto, Nacional de Direito, 2001, págs. 94 y 111.
9. *Fillia, Leonardo César, y otros*, "Análisis integrado de la criminalidad informática", Buenos Aires, Fabián J. Di Plácido, 2007, págs. 71 a 74, 182 a 195.
10. *Gil, Antonio de Loureiro*, "Fraudes informatizadas", São Paulo, Atlas, 1996, pág. 192.
11. *Godart, Didier*, "Securité Informatique—risques, strategies et solutions", Liège, CCI, 2005, pág. 95.
12. "Internet et la société de contrôle : le piège ?", Cités, Paris, Presses Universitaires de France, 2009, pág. 11.
13. *Iteanu, Olivier*, "L´identité numérique en question", Paris, Eyrolles, 2008, págs. 137 a 149.
14. *Jaber, Abbas*, "Les infractions commises sur Internet", Paris, L´Harmattan, 2009, págs. 34 a 35, 59 a 62.
15. *Leiva, Renato Javier Fijena*, "Chile, la Protección Penal de la Intimidad y el Delito Informático", Santiago, Editorial Jurídica de Chile, 1992, págs. 56 a 69.
16. *Palazzi, Pablo A.*, "Los Delitos Informáticos en el Código Penal", Buenos Aires, Abeledo-Perrot, 2009, pág. 130.
17. *Poullet, Yves*, "Derecho a la intimidad y a la protección de datos personales", Buenos Aires, Heliasta, 2009, págs. 113 a 138.
18. *Quéméner, Myriam*, y *Ferry, Joël*, "Cybercriminalité—défi mondial et réponses", Paris, Economica, 2007, pág. 106.

19. *Riquert, Marcelo A.*, "Delincuencia Informática en Argentina y el Mercosur", Buenos Aires, Ediar, 2009, págs. 122, 139 y 140.

20. *Riquert, Marcelo A.*, "Informática y Derecho Penal Argentino", Buenos Aires, AdHoc, 1999, pág. 41.

21. *Rodríguez, José Julio Fernández,* "Secreto e intervención de las comunicaciones en Internet", Madrid, Civitas, 2004, págs. 71, 168 y 169.

22. *Rosende, Eduardo E.*, "Derecho Penal e Informática—Especial referencia a las amenazas lógico informáticas", Buenos Aires, Fabián J. Di Plácido, 2008, págs. 218 a 274.

23. *Sarzana, Carlo*, "Informatica e Diritto Penale", Milano, Giuffrè, 1994, págs. 69, 247 a 463.

24. *Shalhoub, Zeinab Karake* y *Al Qasimi, Sheikha Lubna*, "Cyber Law and Cyber Security in Developing and Emerging Economies", Cheltenham, Elgar, 2010, págs. 175 a 184.

25. *Suarez, José Maria Alvarez-Cienfuegos*, "La defensa de la intimidad de los ciudadanos y la tecnología informática", Pamplona, Aranzadi, 1999, pág. 81.

26. *Sueiro, Carlos, y otros*, "Análisis integrado de la criminalidad informática", Buenos Aires, Fabián J. di Plácido, 2007, págs. 71 a 72, 183 a 195.

27. *Uicich, Rodolfo D.*, "El derecho a la intimidad en Internet y en las comunicaciones electrónicas", Buenos Aires, AdHoc, 2009, págs. 81 a 90.

28. Convención de las Naciones Unidas contra la Delincuencia Organizada Internacional y sus Protocolos, artículos 2, 3 y 31.

29. *Vianna, Julio Lima*, "Fundamentos de Direito Penal Informático—do acesso não autorizado a sistemas computacionais", Rio de Janeiro, Forense, 2003, págs. 35 a 44.

30. *Vieira, Jair Lot*, "Crimes na Internet, interpretados pelos tribunais—repertório de jurisprudência e legislação", Bauru, Edipro, 2009, págs. 123 y 124.

31. *Vieira, Tatiana Malta*, "O direito à privacidade na sociedade da informação", Porto Alegre, Fabris, 2007, págs. 267 a 274.

32. *Zaniolo, Pedro Augusto*, "Crimes Modernos—o impacto da tecnologia no Direito", Curitiba, Juruá, 2007, págs. 161 a 163, 235 y 236.

CUESTIONES RELATIVAS A LAS VÍCTIMAS DE LOS DELITOS RELACIONADOS CON LA IDENTIDAD: DOCUMENTO DE DEBATE*

Philippa Lawson
Asociada, Centro Internacional de Reforma del Derecho Penal y Política de Justicia Penal, Canadá

* El presente documento de debate se preparó como documento de trabajo de la tercera reunión del Grupo básico de expertos sobre el delito relacionado con la identidad, celebrada en Viena, Austria, del 20 al 22 de enero de 2009. También fue presentado como documento de sesión de la Comisión de Prevención del Delito y Justicia Penal en su 18º período de sesiones, celebrado en Viena del 16 al 24 de abril de 2009 (E/CN.15/2009/CRP.14). Las opiniones expresadas en este documento pertenecen al autor y no reflejan los puntos de vista de las Naciones Unidas.

Índice

I. INTRODUCCIÓN

El presente documento de debate fue encargado por la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC) en relación con su estudio de 2004 sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, y los mandatos emanados de las resoluciones 2004/26 y 2007/20 del Consejo Económico y Social. Su propósito es ayudar a la UNODC a formular estrategias y medidas prácticas para combatir los delitos relacionados con la identidad, mejorar la comunicación entre los criminólogos y los expertos en victimología y determinar las esferas que es preciso investigar más a fondo sobre esta forma de delincuencia. El documento de debate abarca las siguientes cuestiones:

a) La variedad y tipos de víctimas de los delitos relacionados con la identidad;

b) Las bases jurídicas para resarcir a las víctimas, incluido un análisis de los temas relacionados con los derechos de identidad, la reputación y la intimidad; y

c) Una lista de las prácticas de apoyo y resarcimiento a las víctimas por parte de los sectores público y privado.

1. Terminología

En consonancia con el informe del Secretario General sobre los resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos[1], el término "delito relacionado con la identidad" que figura en este documento se refiere a todas las formas de dolo que se comete utilizando la identidad de otra persona, así como los actos preparatorios que incluyen la recopilación, manipulación e intercambio de información de identidad. Incluye actos que podrían no estar reconocidos jurídicamente como delitos. La mayoría de estos actos pueden ser considerados como "hurto de identidad" o "fraude de identidad", refiriéndose el primero a la apropiación indebida de información o documentos de identidad auténticos y el segundo al uso de información de identidad para engañar a otros. Actos tales como el tráfico de datos personales no se consideran ni "hurto" ni "fraude".

[1] E/CN.15/2007/8.

Los términos “ladrón”, “defraudador” y “delincuente” se utilizan en este documento para referirse a la persona que comete dolo, independientemente de que haya cometido o no un delito reconocido.

El término “derechos” se utiliza en sentido amplio para referirse a los derechos humanos tal y como se establece en los instrumentos internacionales y regionales, las constituciones y leyes nacionales de derechos humanos, así como a los derechos legales que se derivan de las obligaciones establecidas por la ley o de las doctrinas del derecho consuetudinario.

II. VARIEDAD Y TIPOS DE VÍCTIMAS DE DELITOS RELACIONADOS CON LA IDENTIDAD

1. Variedad de víctimas de delitos relacionados con la identidad

Los delitos relacionados con la identidad dejan a su paso una gran variedad de víctimas, que pueden ser particulares, empresas o gobiernos.

Esos delitos suelen entrañar la suplantación de otra persona para obtener algún tipo de beneficio o para evitar ser detectado. Los *particulares* son las principales víctimas de los delitos relacionados con la identidad, en la medida en que su identidad, y por lo tanto su reputación, es desvirtuada o utilizada indebidamente.

Las *empresas y otras entidades privadas* son víctimas cuando sus identidades empresariales son objeto de apropiación indebida y se utilizan con fines no autorizados y fraudulentos[2]. Dicho fraude de identidad empresarial se lleva a cabo para hacer caer en una trampa a alguien para que facilite sus datos personales (por ejemplo, mediante la "peska") o para obtener el producto de operaciones inmobiliarias o empresariales fraudulentas. Otras entidades no constituidas en sociedades también pueden resultar afectadas por la apropiación indebida de sus identidades y sufrir el consiguiente daño en sus finanzas y su reputación.

Las organizaciones privadas también resultan perjudicadas económicamente cuando son víctimas de delitos de identidad. Esas pérdidas pueden repercutir en su totalidad o en parte en los consumidores a través de una subida de los precios.

Los *gobiernos* también son víctimas cuando los delincuentes utilizan sus servicios y prestaciones con fines fraudulentos. Los costes de ese fraude recaen a la larga en los contribuyentes.

El presente documento se centra en gran parte en las víctimas particulares.

Alcance de la victimización de las personas

Las estadísticas sobre la incidencia de los delitos relacionados con la identidad son escasas fuera de los Estados Unidos, e incluso en ese país solo proporcionan una idea vaga, en el

[2] Este documento solo aborda brevemente el hurto de identidad empresarial en la tipología de las víctimas de la sección "La naturaleza del daño sufrido", y en el análisis del derecho de reparación de las víctimas en virtud del derecho civil ("*Derecho a la propiedad intelectual*"), *infra*.

mejor de los casos, lo que refleja que no se ha reconocido hasta hace poco el valor de recopilar dichos datos y de las dificultades que supone dicha tarea. Según una de las principales encuestas realizadas en los Estados Unidos, un 5% de los estadounidenses fueron víctimas de delitos relacionados con la identidad en 2006, lo que representa un aumento de más del 50% desde 2003[3]. En el Canadá, una encuesta llevada a cabo en 2008 puso de manifiesto que "alrededor de 1 de cada 10 canadienses informan de que han sido víctimas del hurto de identidad"[4], mientras que otra encuesta en el mismo año puso de relieve que un 6,5% de la población adulta canadiense había sido víctima de algún tipo de fraude de identidad durante el año anterior, y que solo unos pocos casos habían sido denunciados ante la policía, las agencias de informes de crédito o la agencia canadiense de informes de fraude[5]. Un estudio reciente llevado a cabo en el Reino Unido constató que en 2007 las denuncias de las víctimas de fraude de identidad ante la agencia nacional de informes de crédito habían aumentado un 66% en comparación con el año anterior[6], y que en el primer semestre de 2008 se habían incrementado casi un 50% con respecto al mismo período en 2007[7]. El sector financiero del Reino Unido también comunicó altas tasas de crecimiento del fraude económico relacionado con la identidad, que en 2008 representó más del 200% en el caso de las apropiaciones indebidas de cuentas[8].

Pese a las vastas discrepancias, las estadísticas sugieren un marcado aumento de la incidencia en todo el mundo de los delitos relacionados con la identidad y los perjuicios que causan a las tres categorías de víctimas.

Alcance geográfico

En cuanto al alcance geográfico, la prevalencia de los casos de delitos relacionados con la identidad es más pronunciada en los Estados Unidos y otros países de habla inglesa, si bien representa una creciente preocupación para algunas jurisdicciones europeas[9]. La disponibilidad y alcance de los mecanismos y servicios concebidos para brindar asistencia a las víctimas de delitos relacionados con la identidad refleja esta aparente realidad, siendo mucho más accesibles para las víctimas en los Estados Unidos que en ningún otro país. Sin embargo, es posible que esta aparente desigualdad en la victimización no sea sino un reflejo de las diferencias en el reconocimiento y la denuncia de los delitos de identidad entre las distintas jurisdicciones.

Alcance demográfico

Las víctimas individuales de los delitos relacionados con la identidad pertenecen a todos los grupos demográficos, indistintamente de su edad, género, ingresos económicos,

[3] Gartner Inc., comunicado de prensa (6 de marzo de 2007).
[4] EKOS Research Associates, citado en Criminal Intelligence Service Canada, *Annual Report 2008*, "Feature Focus: Identity Theft and Identity Fraud in Canada".
[5] *Sproule and Archer*, Measuring Identity Theft in Canada: 2008 Consumer Survey, MeRC Working Paper Nº. 23 (julio de 2008) ["Sproule and Archer"].
[6] Experian UK, comunicado de prensa (28 de mayo de 2008); véase también: "Privacy Watchdog concerned over surge in identity fraud", *The Press and Journal* (16 de junio de 2008).
[7] Experian UK, comunicado de prensa (8 de octubre de 2008).
[8] CIFAS, comunicado de prensa: "2008 Fraud Trends" (26 de enero de 2009).
[9] FIDIS, "D12.7: Identity-related crime in Europe—Big Problem or Big Hype?" (9 de junio de 2008) ["FIDIS"], pág. 62.

educación y origen étnico. No existe un perfil específico de la típica víctima, aunque determinados tipos de delitos de esta índole o de lugares donde se cometen apuntan a algunos grupos particularmente vulnerables[10].

Por ejemplo, los niños parecen ser un blanco peculiar del fraude en que se utilizan números de la seguridad social u otros datos de identificación, cuya detección no suele ser rápida. Este es el caso, por ejemplo, del fraude laboral al que recurren los inmigrantes ilegales en el sur de los Estados Unidos[11]. Un estudio reciente llevado a cabo por Javelin Research en dicho país mostró que los niños, independientemente de su edad, corren el riesgo de ser víctimas del hurto de identidad. Bajo el número de la seguridad social de uno de los niños objeto del estudio figuraban siete identidades, con varios miles de dólares por concepto de gastos médicos, alquiler de viviendas y cuentas acreedoras en trámite de cobro, mientras que el número correspondiente a otro niño estaba vinculado a una deuda de 325.000 dólares. Asimismo, un adolescente de 14 años tenía a su nombre una hipoteca de más de 600.000 dólares y posteriormente la casa fue embargada[12].

En los Estados Unidos las estadísticas basadas en las denuncias sugieren que las personas de entre 18 y 29 años de edad son en general más propensas a ser víctimas de los delitos relacionados con la identidad, y que la tasa de victimización disminuye con la edad (a diferencia de muchas otras formas de fraude, cuyo principal objetivo son las personas de edad avanzada)[13]. En el Canadá, este mismo tipo de estadísticas muestran a las personas de mediana edad, de entre 35 y 54 años, como las más afectadas por el fraude o hurto de tarjetas de crédito o débito[14]. Un estudio llevado a cabo en el Reino Unido reveló algunas tendencias en relación con la edad y el género en lo que respecta al "fraude de tarjetas de plástico": los hombres de entre 35 y 44 años y las mujeres de entre 16 y 24 años de edad eran más propensos a ser víctimas de este tipo de fraude[15].

Según la compañía Experian, los *inquilinos* son los que corren particularmente el riesgo de ser víctimas del hurto de identidad, ya que "las personas cuyas viviendas son alquiladas suelen tener buzones contiguos y tienden a mudarse con más frecuencia que los propietarios de casas. Ello ofrece a los delincuentes más oportunidades de utilizar indebidamente los historiales de crédito que no se mantienen actualizados"[16].

Personas fallecidas

Cuando se crean identidades totalmente nuevas con el fin de obtener documentos oficiales de identidad, acceder a servicios públicos o evadir la acción de las autoridades, las *personas fallecidas* ofrecen buenas oportunidades de fraude porque jamás podrán detectarlo.

[10] Grupo de trabajo binacional sobre el fraude masivo transfronterizo en la comercialización (Canadá-Estados Unidos), *Report on Identity Theft* (octubre de 2004).
[11] *Steven Malanga*, "Identity Theft in America goes Hand and Hand with Illegal Immigration", véase: http://www.usbc.org/opinion/2008/spring/identity.htm.
[12] Javelin Strategy and Research, comunicado de prensa: "Recent Javelin Study Shows Children Are At Risk for Identity Theft" (28 de octubre de 2008).
[13] FTC, Consumer Fraud and Identity Theft Complaint Data, enero (diciembre de 2007), pág. 15.
[14] Criminal Intelligence Service Canada, *Annual Report 2008*, "Feature Focus: Identity Theft and Identity Fraud in Canada".
[15] Home Office Statistical Bulletin, Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (15 de mayo de 2007), pág.35.
[16] Experian UK, comunicado de prensa (8 de octubre de 2008).

Aunque en estos casos no resultan victimizadas personas en vida, las administraciones públicas y las empresas defraudadas sufren pérdidas. Según una publicación oficial australiana, "un delincuente de Melbourne se hizo el certificado de nacimiento de cuatro bebés que habían muerto en la década de 1970, tras lo cual, por un período de ocho meses, cobró 20.857 dólares australianos en prestaciones de desempleo recibidas en nombre de ellos. Cuando fue detenido, el infractor tenía en su posesión un bolso lleno de documentos probatorios de identidad falsos con los que apoyaba sus pretensiones de asistencia social. Los mismos incluían licencias de conducir de vehículos automotores, cuentas de teléfonos móviles, tarjetas de estudiante, documentos sobre el alquiler y tarjetas de acceso a cuentas bancarias"[17].

La policía canadiense descubrió una trampa consistente en la venta de documentación minuciosa de identidad de personas, fallecidas cuando eran niños, para uso de extranjeros que tenían aproximadamente la misma edad de los fallecidos, lo que les permitía luego obtener pasaportes canadienses y otros documentos oficiales utilizando sus propias fotografías junto con el nombre, la fecha y lugar de nacimiento y otra información de la víctima. Valiéndose de esta documentación llegaron a acceder al sistema de asistencia médica canadiense[18].

Identidades sintéticas

Con frecuencia, los delincuentes fabrican identidades ficticias combinando datos reales y falsos o información de más de una víctima. De hecho, en la actualidad se estima que dicho fraude de identidad "sintética" representa la mitad de todos los casos de falsificación de identidad en los Estados Unidos[19]. El fraude de identidad sintética puede ser más difícil de detectar que el que se comete utilizando el "nombre verdadero", ya que los datos registrados de actividades fraudulentas no aparecen inmediatamente en los informes de crédito de la víctima o en otros registros que figuren a su nombre.

En los casos de fraude de identidad sintética observados actualmente en los Estados Unidos, es típico que el delincuente combine el número de la seguridad social de una víctima con el nombre y la fecha de nacimiento de otra persona. Aunque el titular real de ese número puede no verse afectado por los delitos posteriores que se cometan usándolo, a la larga podría ser relacionado con los mismos si los acreedores, cobradores de deudas, autoridades fiscales, organismos encargados de hacer cumplir la ley u otras autoridades de represión del fraude vinculan el número de la seguridad social con su nombre. Estos casos pueden ser particularmente perjudiciales y de difícil solución para las víctimas debido a la demora en su detección y a la frecuente confusión que crea la combinación de información de identidad[20].

---

[17] Australian National Crime Prevention Program, *Identity Theft Information Kit* (mayo de 2004), disponible en línea en: http://www.crimereduction.homeoffice.gov.uk/theft1.htm.

[18] *Joe Pendleton*, Director de los Servicios de Investigaciones Especiales, Alberta, "The Growing Threat of Medical Identity theft in Canada", documento presentado en la Electronic Health Privacy Conference, Ottawa, (3 de noviembre de 2008), disponible en línea en http://www.ehip.ca; reseñada en *Pauline Tam*, "ID theft Scams Target Canada's Healthcare System", The Ottawa Citizen (3 de noviembre de 2008).

[19] *Allen Jost*, Vicepresidente, Business Strategy, ID Analytics; entrevista telefónica (3 de febrero de 2009).

[20] Véase *Leslie McFadden*, "Detecting Synthetic Identity Fraud", disponible en línea en: http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp (16 de mayo de 2007).

Incluso si las personas cuyos datos de identidad se utilicen en un fraude de identidad sintética no se vieran afectadas por el mismo, esta forma de delito resulta extremadamente costosa para las empresas, los consumidores y la economía en general.

2. Tipologías de las víctimas

Las víctimas de los delitos relacionados con la identidad se pueden clasificar de diferentes maneras. Cada tipología permite considerar aspectos precisos de dichas víctimas que pueden resultar útiles para elaborar políticas en respuesta al problema. Las tipologías analizadas a continuación categorizan a las víctimas según: *a)* la naturaleza del acto delictivo; *b)* el método utilizado para obtener o robar los datos: responsabilidad de la víctima; *c)* la naturaleza del daño sufrido; *d)* el alcance del daño sufrido; y *f)* la identificabilidad del autor y su relación con la víctima.

Según la naturaleza del acto delictivo

Los delitos relacionados con la identidad tienen formas muy diferentes. Las consecuencias que suponen para las víctimas varían según la naturaleza del acto, como también varían los enfoques adecuados para prevenir y remediar tales actos. Por lo tanto puede ser útil a efectos normativos categorizar a las víctimas atendiendo a la naturaleza del delito en cuestión. Sin embargo, tal vez resulte difícil una clasificación precisa según este criterio porque en muchos casos hay solapamientos entre los tipos de fraude[21].

La Comisión Federal de Comercio de los Estados Unidos divide el delito relacionado con la identidad (al cual denomina "hurto de identidad") en cuatro categorías: "cuentas existentes de tarjetas de crédito", "cuentas existentes de tarjetas no de crédito", "cuentas nuevas" y "otras". Esta clasificación obedece a los actuales grados de incidencia en dicho país. El fraude de identidad con fines no económicos incluye el fraude para recibir prestaciones del Estado, el fraude laboral, el fraude en cuestiones de alquiler, el fraude inmobiliario, el fraude postal, el fraude fiscal y el fraude de evasión de acciones penales. Quienes cometen estos delitos de apropiación de identidad son con frecuencia individuos que tratan de no ser detectados por las autoridades, como es el caso de los inmigrantes ilegales, portadores de drogas y delincuentes involucrados en operaciones de blanqueo de dinero[22].

En algunos casos la información de identidad de la víctima no se utiliza de manera fraudulenta, sino que el delito es únicamente la obtención no autorizada, la transferencia o el uso de esa información.

A continuación figura una tipología de las víctimas según la naturaleza del acto delictivo:

[21] Synovate, *2006 Identity Theft Survey Report*, preparado para la Comisión Federal de Comercio (noviembre de 2007) ["Synovate"], Figura 2, pág.13; Identity Theft Resource Center, *Identity Theft: The Aftermath 2007*, ["ITRC, Aftermath"] cuadros 1A y 1B.

[22] UK Cabinet Office, *Identity Fraud: A Study* (julio de 2002).

Mera adquisición no autorizada, transferencia o manipulación de información de identidad

Un paso preliminar necesario para el fraude de identidad es obtener la información identificativa de otra persona. Esto puede llevarse a cabo de manera tanto lícita como ilícita, con o sin el conocimiento de la víctima, directamente de ella o por otros medios. La víctima raramente autoriza dicho acto, incluso si el acto de la obtención en sí no es ilícito (por ejemplo, hurgando en la basura, aprovechando deficiencias de seguridad). Si se descubre, la mera apropiación de información personal por un desconocido, o la mera exposición al riesgo de un posible acceso de delincuentes a los datos personales, origina en las víctimas sentimientos de atropello y ansiedad.

Una vez obtenida, la información, puede venderse en el mercado negro, utilizarse para crear identidades sintéticas o manipularse para un uso fraudulento futuro. Es poco probable que las víctimas se den cuenta de dichas actividades a menos que se cometa algún tipo de fraude.

Fraude económico o financiero

La forma más común de delito relacionado con la identidad que se conoce en América del Norte y el Reino Unido es el realizado para obtener beneficios financieros (con frecuencia denominado "fraude de identidad con fines financieros, aunque conforme a la terminología adoptada por la UNODC aquí se denomina "fraude económico")[23]. Ello se debe a que en dichos países existen mercados muy desarrollados de crédito y fácil acceso de los consumidores al mismo, lo que ofrece a los suplantadores de identidad amplias oportunidades para aprovecharse de un sistema diseñado para facilitar el crédito. El fraude económico puede dividirse en dos categorías: el acceso a cuentas existentes y la creación de cuentas nuevas.

Cuentas existentes

El Servicio de Prevención del Fraude del Reino Unido (CIFAS) ha señalado un aumento considerable del uso fraudulento de cuentas existentes, distinguiendo entre la "asunción de una cuenta", que en 2008 registró un aumento del 207% con respecto a 2007, y el "uso indebido de una cuenta", que mostró un incremento del 69% durante el mismo período[24].

Tarjetas y dispositivos de pago: La forma más común de fraude de identidad denunciada en América del Norte es el uso sin autorización de la tarjeta de crédito de otra persona. El "fraude de tarjetas de plástico" es también la principal forma de fraude de identidad en el Reino Unido. La mayor parte de los gastos directos que se derivan de dicho fraude no los asume la víctima, sino las compañías emisoras de tarjetas de crédito[25], que posteriormente repercuten dichos costos en los titulares de la tarjeta, generalmente a través de altas tasas de interés. Algunas partes interesadas no consideran que

[23] ITRC, *Aftermath*, cuadros 1A y 1B; Grupo de expertos en materia de prevención del fraude, *Report on Identity Theft/Fraud* (22 de octubre de 2007) ["FPEG"], págs. 8 y 9.

[24] CIFAS, comunicado de prensa: 2008 Fraud Trends (26 de enero de 2009). En el caso de "asunción de una cuenta" los delincuentes utilizan información sobre la víctima para detraer y manejar la cuenta de manera fraudulenta en su propio beneficio. En cambio, el "uso indebido" simplemente implica la utilización fraudulenta de una cuenta existente, por ejemplo para pagos con tarjeta o compras por catálogo.

[25] Por ejemplo, la ley Truth in Lending de los Estados Unidos limita la responsabilidad del consumidor por gastos no autorizados de tarjeta de crédito a un máximo de 50 dólares: 15 USC. art. 1601 y ss., y su reglamento de aplicación Z, 12 C.F.R. art. 226; véase especialmente: 15 USC. art. 1643; 12 C.F.R. art. 226.12 b). En el Canadá existen leyes similares. Las compañías emisoras de tarjetas de crédito han adoptado políticas de responsabilidad cero que limitan aún más la responsabilidad del consumidor en caso de transacciones fraudulentas.

se trate en realidad de un fraude de identidad, ya que el acto no implica la suplantación de la personalidad de la víctima más que para tener acceso a la cuenta en cuestión, y en general las consecuencias para las víctimas son limitadas o fácilmente reparables. Sin embargo, el fraude de las tarjetas de pago provoca generalmente perjuicios considerables para las compañías defraudadas y los sistemas económicos.

Otras cuentas existentes: Los defraudadores también utilizan la información de identidad de las víctimas para acceder a sus cuentas bancarias o de inversión (a través de tarjetas de débito, servicios bancarios en línea, transferencia electrónica de fondos, cheques falsos u otros medios), y a sus cuentas de teléfono. Los titulares de cuentas individuales están menos protegidos del riesgo de resultar responsables de las pérdidas derivadas de este tipo de fraude, aunque el sector financiero va adoptando con frecuencia creciente códigos de buenas prácticas para poner a los consumidores a cubierto de responsabilidad por transacciones electrónicas fraudulentas, a menos que se demuestre que el titular actuó sin el debido cuidado[26]. En los Estados Unidos, la ley protege a los consumidores del riesgo de responsabilidad por transferencias electrónicas de fondos no autorizadas en función del momento en que los afectados las notifiquen a la institución financiera pertinente[27].

Cuentas nuevas

Con frecuencia, los delincuentes abren cuentas financieras nuevas a nombre de las víctimas. En los Estados Unidos, las formas más comunes de fraude mediante cuentas nuevas son las relacionadas con tarjetas de crédito, empresas de suministros públicos y servicios telefónicos. Los infractores utilizan la información personal de las víctimas para abrir cuentas nuevas a nombre de las mismas con el fin de poder gastar sin tener que pagar.

También solicitan préstamos bancarios e hipotecas a nombre de las víctimas, quienes posteriormente sufren las consecuencias derivadas del impago del prestatario.

Los beneficios del fraude

Los delincuentes en materia de identidad utilizan información personal de otros para obtener beneficios del sector público, atención sanitaria, devolución de impuestos, así como permisos de conducir, pasaportes y otros documentos emitidos por las autoridades. En el caso de estos últimos, los delincuentes con frecuencia se hacen pasar por una persona fallecida con el fin de hacer mínimas las posibilidades de que se descubra el fraude. Por ejemplo, en el Reino Unido ha habido ciudadanos interpelados por la policía para que respondieran por delitos supuestamente cometidos por un hijo suyo muerto en la infancia[28]. Con frecuencia también se utilizan documentos falsos para tener acceso a servicios.

El fraude fiscal relacionado con la identidad

En los últimos años esta forma de fraude de identidad se ha incrementado extraordinariamente en los Estados Unidos, pues los delincuentes se procuran las devoluciones

[26] Véase, por ejemplo, el Banking Code del Reino Unido (marzo de 2008), secs. 12.11 a 12.13, disponible en línea en: http://www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf

[27] *Electronic Fund Transfer Act*, 15 USC. art. 1693 y ss., y su reglamento de aplicación E, 12 C.F.R. art. 205; véase especialmente 15 USC. art. 1693g; 12 C.F.R. art. 205.6(b).

[28] United Kingdom Cabinet Office, *Identity Fraud: A Study* (julio de 2002), párr. 1.2

de impuestos suplantando la identidad de contribuyentes auténticos, declarando numerosas personas a cargo, horas de trabajo falsas, y otros datos concebidos para hacer máximo el reembolso[29]. Es posible que inmigrantes ilegales u otras personas, utilicen identidades usurpadas para conseguir empleo y posteriormente desaparecer sin pagar los impuestos correspondientes, dejando a la víctima con una gran deuda fiscal pendiente. En los Estados Unidos, una contribuyente tuvo que hacer frente a una deuda de impuestos atrasados por un millón de dólares, pese a que era ama de casa. Posteriormente se realizó una investigación que reveló que 218 inmigrantes ilegales estaban utilizando su número de seguridad social. Entre 2002 y 2005 numerosos delincuentes en la esfera de la identidad utilizaron el nombre y número de seguridad social de un trabajador mexicano-estadounidense para obtener empleo en Kansas, Tejas y Nueva Jersey. La víctima tuvo que hacer frente a reiteradas acusaciones de declaración incompleta de ingresos y grandes demoras para recibir las devoluciones de impuestos que se le debían[30].

El fraude de identidad con fines médicos

En los Estados Unidos el fraude en el ámbito de la atención sanitaria es un problema especial, ya que no existe un seguro médico nacional universal[31]. Los delincuentes utilizan la identidad de otros para obtener medicamentos, tratamientos médicos costosos o reembolsos de seguros fraudulentos, lo que deja a la víctima con facturas médicas pendientes, historiales médicos contaminados y dificultades para mantener u obtener un seguro médico.

Por ejemplo un ciudadano estadounidense se percató de que había sido víctima de fraude de identidad con fines médicos cuando recibió una llamada de una agencia de cobro reclamando el pago de una factura de 41.188 dólares de un hospital en el que nunca había sido ingresado. Alguien había usado su nombre y número de seguridad social para ser operado. Dos años más tarde, seguía sufriendo las consecuencias de un crédito dañado, "luchaba desesperadamente para evitar la bancarrota" y desconocía si su historial médico había sido rectificado[32].

Se sabe de la existencia de un mercado negro de documentos para obtener la ciudadanía canadiense (utilizando la identidad de niños fallecidos) a través de los cuales los norteamericanos sin seguro médico acceden de manera fraudulenta al sistema de salud estatal canadiense.

El fraude de permisos de conducir

Esta forma de fraude relacionado con la identidad puede perjudicar el historial de conducción de la víctima y dejarle a su cargo multas sin pagar, con la consecuencia quizá de una suspensión o revocación del permiso de conducir. Según una organización canadiense, "con frecuencia, las víctimas de hurto y fraude de identidad no se percatan de que existe un problema hasta que llega el momento de renovar el seguro de su coche o su permiso de conducir, debido a las multas pendientes de pago, que

[29] Comisión Federal de Comercio, Consumer Fraud and Identity Theft Complaint Data, January—December 2007 ["FTC, 2007 Complaint Data"].
[30] *Kevin McCoy*, "Identity thieves tax the system", *USA Today* (10 de abril de 2008).
[31] Véase: http://www.worldprivacyforum.org/medicalidentitytheft.html.
[32] Max Alexander, "Your Medical Records, Stolen!", ReadersDigest.com.

debe efectuarse antes de proceder a la renovación del seguro o del permiso"[33]. Los delincuentes también utilizan la información de ese permiso para llevar a cabo otras actividades fraudulentas aprovechando que dicho documento se utiliza ampliamente con fines de verificación.

Pero incluso cuando no implique la suplantación de la personalidad de víctimas vivas, el fraude relativo a permisos de conducir origina riesgos para la seguridad pública y representa gastos importantes para el tesoro público. Se calcula que en el Reino Unido las tareas de detección e investigación de fraude durante el procesamiento de solicitudes y verificación de permisos de conducir cuestan a las arcas nacionales unos 7 millones de libras anuales[34].

Fraude en el ámbito inmobiliario

En este tipo de fraude los delincuentes utilizan identidades robadas o documentos falsificados para transferir a su nombre un título de propiedad registrado, sin conocimiento del verdadero propietario. El infractor normalmente obtiene un préstamo hipotecario sobre la propiedad en cuestión y una vez recibe el dinero, desaparece. Las víctimas de este tipo de fraude pueden llegar a perder su título inmobiliario[35]. Una propietaria canadiense tuvo que llevar su caso al tribunal superior de la provincia para poder recuperar el título de su propiedad después de que alguien se hiciera pasar por ella y transfiriera el título a otro infractor, quien tras obtener un préstamo hipotecario cuantioso sobre la propiedad desapareció[36]. En la actualidad el fraude en el ámbito inmobiliario constituye un serio problema en el Canadá, y en los Estados Unidos este delito encabeza la lista de predicciones para 2009 elaborada por la entidad Identity Theft Resource Center[37].

Fraude relacionado con el empleo

En los últimos años, los Estados Unidos han observado un pronunciado aumento de casos de fraude relacionados con el empleo, en los que los delincuentes se hacen pasar por ciudadanos estadounidenses (utilizando a veces el número de la seguridad social de niños) para obtener un empleo que de otra manera no podrían conseguir legalmente, o para trabajar sin pagar impuestos[38]. Este tipo de fraude puede significar para las víctimas tener que pagar impuestos sobre ingresos que nunca percibieron y verse privadas de acceso a prestaciones públicas.

Fraude en materia de alquiler

Las personas con antecedentes penales o deshonrosos también se hacen pasar por otros para alquilar viviendas. Las víctimas pueden verse perjudicadas con un historial de incumplimiento de pago, daños a la propiedad u otros problemas relacionados con el alquiler.

---

[33] British Columbia Crime Prevention Association, Identity Theft Victim's Toolkit (febrero de 2007).

[34] United Kingdom Identity Fraud Steering Committee, "New Estimate of Cost of Identity Fraud to UK Economy" (9 de octubre de 2008).

[35] Law Society of Upper Canada, Report to Convocation, *Mortgage Fraud* (24 de marzo de 2005).

[36] Dale Anne Freed, "Mortgage Fraud Victory; Woman wins back home as court reverses decision", *The Toronto Star* (7 de febrero de 2007).

[37] *Ibid*.; "Mortgage fraud hits $1.5b. per year", *Calgary Herald* (18 de marzo de 2006); Identity Theft Resource Center, comunicado de prensa "Identity Theft Predictions 2009" (18 de diciembre de 2008).

[38] Federal Trade Commission, 2007 Complaint Data.

Fraude con fines de evasión penal

Los delincuentes pueden usurpar la identidad de otra persona con la finalidad de eludir a las autoridades encargadas de hacer cumplir la ley. Hay víctimas de este tipo de fraude que han sido prendidas, retenidas y detenidas por delitos que nunca cometieron. Por ejemplo, en 2008, una mujer estadounidense, madre de dos hijos, fue detenida y encarcelada por un corto período de tiempo por un robo que se cometió utilizando su nombre. El verdadero delincuente había utilizado información de identidad que había robado del vehículo de la víctima cuatro años antes. La víctima tuvo que gastar 3.500 dólares en honorarios de abogado a fin de limpiar su nombre[39].

Fraude en la esfera postal

Una táctica común de los delincuentes es redireccionar la correspondencia de la víctima mediante una notificación de cambio de domicilio hecha a nombre de la misma. Este tipo de fraude es normalmente una etapa intermedia en tramas de fraude mayores, que permite a los ladrones reunir más información personal sobre sus víctimas para un futuro uso fraudulento.

La responsabilidad de las víctimas según el método de reunión o robo de datos

La división de las víctimas de hurto de identidad en categorías según el método utilizado puede ser útil para juzgar la responsabilidad de las mismas, ya que permite diferenciar a grandes rasgos entre los casos en función del grado de control que tenía la víctima para evitar desde un principio que el hurto o fraude se cometiera. Sin embargo, este planteamiento debería considerarse con cautela, ya que incluso cuando la información se toma directamente de la víctima, puede resultar injusto juzgarla como la única parte responsable. Así sucede cuando, por ejemplo, el método utilizado fue subrepticio o difícil de detectar, o cuando en el método juegan un papel los servicios de terceros (por ejemplo, equipos o programas informáticos, servicios de banca en línea) anunciados y vendidos a la víctima sin advertencias o adecuadas instrucciones para prevenir el fraude.

Negligencia de las víctimas

Los ladrones de identidad se aprovechan del descuido de las víctimas y se hacen con sus datos de identidad a través de métodos o fuentes tales como:

- El hallazgo de carteras o información de cuentas y contraseñas perdidas;
- Hurgando entre la basura;
- El hurto de una cartera, chequera, tarjeta de crédito o correspondencia[40];
- Fisgando en comunicaciones inalámbricas realizadas en condiciones inseguras[41];

[39] Información de KVBC TV, Las Vegas NV (13 de mayo de 2008), consultada el 31 de enero de 2009 en línea en: www.youridentitysafe.com.

[40] Tal vez la víctima no haya podido hacer mucho por evitar el robo.

[41] Los proveedores de servicios inalámbricos tienen cierta responsabilidad de informar debidamente a las personas de los riesgos inherentes a las comunicaciones inalámbricas realizadas en condiciones inseguras, y proporcionarles medios sencillos para hacer que las comunicaciones sean seguras.

- Accediendo a páginas web personales;
- Visitando sitios de redes sociales[42].

Engaño de las víctimas

En muchos casos, se engaña a las víctimas para que proporcionen sus datos, ya sea directamente o a través de programas informáticos ocultos o mecanismos fraudulentos de pago electrónico. Según sea el contexto y la conducta engañosa en cuestión, puede resultar injusto atribuir la responsabilidad a la víctima. Entre tales métodos de hurto de identidad figuran:

- "Ingeniería social": engaño de las víctimas para que proporcionen información personal reservada haciéndose pasar por un tercero de confianza, a través del teléfono, correo electrónico (peska) o mensajes instantáneos ("SMSishing");
- El robo de datos para la clonación de tarjetas ("skimming") a través de cajeros automáticos, cámaras ocultas;
- La instalación solapada de un programa malicioso ("malware") en la computadora de la víctima (por ejemplo, en el momento en que esta descarga otras aplicaciones) y su utilización para reunir información personal de la misma por medios tales como el registro de pulsaciones de las teclas o "click-jacking"[43].

Divulgación pública por terceros

En algunos casos, los datos de identidad individuales se hacen públicos a través de terceros, con frecuencia, sin el consentimiento de la víctima. Las entidades públicas y privadas suelen no tener en cuenta las consecuencias de la publicación de datos personales en línea. Los delincuentes pueden aprovecharse de la información hecha pública a través de:

- Los registros públicos en línea (por ejemplo, cortes o tribunales);
- Sitios web de empleadores o asociaciones;
- Sitios que anuncian la desaparición de personas después de un desastre;
- Anuncios de defunciones.

Negligencia, engaño de terceros

Muchos de los datos que utilizan los delincuentes (especialmente de tarjetas de pago y de cuentas) se obtienen de terceros, a través de una variedad de medios, entre ellos los que se mencionan a continuación. En tales casos, las víctimas no pueden evitar el hurto y, con frecuencia, ni siquiera se enteran.

- Hurgar en la basura ("dumpster diving"), servirse de equipamiento informático usado;

[42] Los sitios de redes sociales en Internet tienen cierta responsabilidad de advertir a los usuarios, especialmente a los jóvenes, acerca de los riesgos asociados con la divulgación de datos personales en el respectivo sitio.

[43] Incorporando enlaces ocultos que funcionan sin conocimiento del usuario, cuando este selecciona los enlaces visibles en una página web.

- Robar ordenadores, archivos;
- Sobornar a empleados para que recopilen y proporcionen datos de los clientes;
- Engañar a empleados para obtener información de clientes ("pretexting");
- Comprar o abonarse de modo fraudulento a los servicios de un agente buscador de datos de clientes ("databroker");
- Piratear sistemas informáticos y bases de datos;
- Aprovechar los fallos de seguridad.

Tipología según el daño sufrido por las personas o las empresas[44]

Debido a que cualquier caso de delito relacionado con la identidad puede causar muy diferentes tipos de perjuicio a cada víctima, puede resultar difícil categorizar a las mismas con arreglo al tipo de daño sufrido. Sin embargo, esta tipología es particularmente útil para elaborar programas de reparación a las víctimas, ya que hace una diferenciación entre los tipos de daños sufridos, cada uno de los cuales requiere medidas de reparación diferentes.

Víctimas individuales

Pérdidas financieras directas

Las víctimas individuales pueden sufrir una pérdida financiera directa en forma de deudas originadas de modo fraudulento, honorarios conexos, gastos de mitigación del daño (por ejemplo, servicios de supervisión de créditos) y restablecimiento del historial, o pérdida del título de propiedad.

Una encuesta llevada a cabo en los Estados Unidos indica que en 2007[45], el delito relacionado con la identidad costó a las víctimas individuales un promedio de 691 dólares (más de la mitad de ellas no tuvieron ningún gasto), mientras que otra encuesta realizada en 2006 por encargo de la Comisión Federal de Comercio reveló que el 10% de las víctimas del delito relacionado con la identidad tuvo que pagar de su bolsillo 1.200 dólares o más, y el 5% más perjudicado sufrió gastos de al menos 5.000 dólares[46]. Una tercera encuesta en el mismo país reveló que en 2006 el promedio de pérdidas por víctima fue de 3.257 dólares, en comparación con 1.408 dólares en 2005, mientras que el porcentaje de los fondos que los consumidores lograron recuperar disminuyó de un 87% en 2005 a un 61% en 2006[47]. En 2007, las víctimas que contactaron al Identity Theft Resource Center (Centro de recursos para el hurto de identidad), tuvieron que desembolsar un promedio de 550 dólares por concepto de daños en una cuenta existente, y de 1.865 dólares para poner en orden las cuentas nuevas que habían sido abiertas de manera fraudulenta a su nombre[48].

[44] A los fines de esta tipología, se consideran tanto entidades (públicas o privadas) como víctimas individuales.
[45] Javelin Strategy and Research, comunicado de prensa: "Identity Fraud, Part 1: A $45 Billion Snowball" (27 de septiembre de 2008).
[46] Synovate, pág. 6.
[47] *Gartner*, comunicado de prensa (6 de marzo de 2007).
[48] ITRC, *Aftermath*, Resumen.

Según una encuesta canadiense reciente, las víctimas del delito relacionado con la identidad gastaron más de 155 millones de dólares canadienses en solucionar problemas dimanantes de dicho delito, con un costo promedio de 92 dólares por víctima, o de 151 dólares, sin contar el fraude de tarjetas de crédito[49].

Pérdidas financieras indirectas

El costo financiero indirecto derivado del delito relacionado con la identidad es con frecuencia mayor que el costo directo individual. El costo indirecto incluye tasas de seguro y tasas de interés más altas, la denegación de crédito, la incapacidad de utilizar tarjetas de crédito existentes, la imposibilidad de obtener préstamos, la dificultad para obtener o acceder a cuentas bancarias, y la pérdida de ingresos (debida por ejemplo a la pérdida de reputación o a las horas de permiso laboral tomadas)[50]. En los Estados Unidos, un considerable número de víctimas informó de que había tenido dificultades para que las agencias de crédito eliminaran de sus expedientes información errónea o para prevenir que se volviera a incluir información negativa en su historial de crédito[51].

Daños a la reputación

Las víctimas de fraude de identidad sufren diversos daños a su reputación, lo cual puede causar serias dificultades para obtener o mantener un crédito, el empleo, la vivienda, el seguro médico, otros seguros, el permiso de conducir, el pasaporte, y otros documentos de identidad emitidos por las autoridades o por instituciones (por ejemplo, de educación). El daño a la reputación también puede causar dificultades a la hora de cruzar fronteras. El perjuicio causado puede tener consecuencias verdaderamente tremendas para las relaciones familiares o sociales, especialmente cuando las víctimas son detenidas por delitos que nunca cometieron. Por ejemplo, un ciudadano del Reino Unido perdió su trabajo y fue rechazado por familiares después de ser detenido por consumir pornografía infantil (un defraudador de identidad había utilizado los datos de su tarjeta de crédito para acceder a un sitio web de pornografía infantil)[52].

Historial clínico inexacto o imposibilidad de obtener un seguro médico

El fraude de identidad en la esfera médica puede derivar en serias consecuencias a la hora de obtener tratamiento médico si el historial clínico de la víctima es incorrecto, o si la víctima se ve imposibilitada de obtener atención médica debido a la existencia de facturas a su nombre pendientes de pago. Es poco probable que esto signifique un problema en los Estados cuyo sistema de salud sea de financiación pública, excepto en el caso de extranjeros que recurran al fraude de identidad para acceder a un sistema así financiado[53].

Retención o detención improcedente

Numerosos ciudadanos estadounidenses han sido detenidos por delitos cometidos por otros, los cuales se hicieron pasar por ellos utilizando información de identidad

[49] *Sproule* y *Archer*, página 17.
[50] Synovate, pág. 7.
[51] ITRC, *Aftermath*, Resumen.
[52] *Marc Sigsworth*, "I was falsely branded a paedophile", BBC News online, 2008/04/03.
[53] Como se ha indicado antes, hay constancia de que ciudadanos estadounidenses han accedido de manera fraudulenta al sistema de salud canadiense utilizando la identidad de canadienses fallecidos.

robada. Es alarmante que el 62% de los que respondieron a una encuesta de víctimas llevada a cabo recientemente por el mencionado Centro de recursos para el hurto de identidad, indicara que los delitos financieros cometidos por malhechores habían originado la emisión de órdenes de detención contra víctimas (más de 2,5 veces que en 2006 y el doble que en 2004)[54].

Acoso de las agencias de cobro

Con frecuencia, las víctimas del fraude de identidad financiero no descubren el problema más que cuando empiezan a recibir llamadas de agencias de cobro reclamando el pago de facturas por gastos en los que nunca incurrieron o por préstamos que nunca solicitaron. Según la encuesta de víctimas de 2007 del Centro de recursos para el hurto de identidad, el 82% de las víctimas se enteraron del delito de identidad a raíz de una "acción adversa", en lugar de haber recibido una notificación proactiva de las empresas o de haberse supervisado su historial de créditos.

Con frecuencia las agencias de cobro y los acreedores se niegan a rectificar el historial de la víctima pese a tener pruebas concluyentes. Más de la mitad de las víctimas que respondieron al cuestionario dijeron que las agencias de cobro continuaron molestándolos respecto a deudas contraídas de manera fraudulenta después de que hubieran aclarado la situación.

Tiempo preciso y dificultades para restablecer la reputación

Es posible que la víctima de un delito de identidad tenga que destinar cientos de horas durante un período de varios años para finalmente corregir todos los registros contaminados y recuperar su buen nombre. Según una encuesta de 2007, el tiempo promedio por víctima fue de 40 horas[55]. Con arreglo a una encuesta llevada a cabo en el Canadá, se estima que las víctimas dedicaron un total de 21 millones de horas tratando de restablecer la información sobre su identidad, lo que representa un promedio de 13 horas por víctima, y de 17 horas si se excluye el fraude relativo a tarjetas de crédito[56]. Las víctimas que se dirigieron en 2007 al Centro de recursos para el hurto de identidad, de Estados Unidos, destinaron un promedio de 116 horas a reparar el daño ocasionado en cuentas existentes, y un promedio de 158 horas a aclarar la apertura fraudulenta de cuentas nuevas. En casos graves se destinaron miles de horas o "demasiadas para contarlas". En el 70% de los casos, llevó hasta un año rectificar la información errónea, en el 12% de los casos, entre uno y dos años, y en el 19% de los casos denunciados, dos años o más[57].

Angustia psicológica y emocional

El daño emocional y psicológico que sufren las víctimas de delitos relacionados con la identidad puede llegar a ser profundo, especialmente cuando se trata de víctimas de casos de fraude muy graves o de difícil solución[58]. De hecho, la angustia psicológica que experimentan algunas de ellas ha sido comparada con la de las víctimas de delitos violentos. Según un psicólogo estadounidense que se especializa en el

[54] *Aftermath*, op cit.
[55] Javelin Strategy and Research, comunicado de prensa: "Though national statistics are trending downward, millions of Americans still at risk for identity theft" (8 de octubre de 2008).
[56] *Sproule* y *Archer*, pág. 17.
[57] ITRC, *Aftermath*, Resumen.
[58] *Ibid.*, págs. 26 a 29: "Emotional Impact on Victims".

tratamiento de víctimas de delito "muchas víctimas y personas afectadas por el hurto de identidad sufren muchos de los síntomas psicológicos, de comportamiento y emocionales que las víctimas de delitos violentos [...] algunas de ellas sienten agotamiento, se tornan destructivas o incluso llegan a pensar en el suicidio"[59].

"La rabia que se siente es enorme en estos casos, y se tiene la sensación de padecer una gran injusticia", comenta un investigador canadiense que estudia los efectos del delito de identidad en las víctimas. "Realmente puede destruir la confianza de la gente en el sistema, y no se trata solamente del hecho de que su identidad fue robada. Las víctimas también se sienten frustradas e impotentes cuando tratan de restablecer su credibilidad"[60].

Una víctima declara: "Tengo 25 años, soy joven y sano, debería estar disfrutando de la vida, pero en cambio, vivo estresado y paranoico por mi situación financiera, que solía ser excelente"[61]. Otra víctima destaca: "El hurto de mi identidad ocurrió cuando estaba trabajando en un proyecto para ayudar a otros a 'recuperarse'. Desde el momento en que descubrí lo que pasaba, la indignación que sentí por la traición provocó que volviera a sufrir convulsiones, lo que aumentó las tensiones emocionales y muchas otras cosas". Otra víctima asegura "Fue un atropello. Fue casi como si me hubieran violado, y nadie hizo nada al respecto". "Creo que hubiera sido más fácil entrar en mi casa y verla completamente saqueada, al menos hubiera sabido qué hacer. Solo recuerdo que lloré mucho y pensaba '¿por qué? ¿por qué me pasan estas cosas a mí?'"

Incluso las víctimas de simples hurtos de identidad sin fraude pueden sufrir una angustia considerable por la preocupación de pensar en los fraudes que se podrían cometer en su nombre. Una de estas víctimas, que fue notificada de un fallo de seguridad en la información sobre la cuenta de inversión de su esposo y de un posterior intento de apertura de una cuenta a nombre del mismo, dice: "Nos sentimos tremendamente asqueados y absolutamente atropellados. Nos pasamos semanas imaginando situaciones horribles en torno a cómo el buen nombre de mi marido y su historial de crédito iban a ser afectados, si no destruidos, por un tironero informático"[62]. Otra víctima declara: "Fue horrible. Es tremendamente ultrajante. Mi caso no fue grave, solo que ahora vivo asustada por lo que podría pasar en el futuro, dado que mi información personal sigue todavía por ahí"[63].

Empresas

Pérdida financiera directa

Cuando las empresas son objeto de fraude mediante el uso de identidades fabricadas o identidades de personas fallecidas, sufren las pérdidas consiguientes. Asimismo, cuando se utiliza la información de identidad de personas vivas para acceder a cuentas o abrirlas, con frecuencia las empresas indemnizan a los clientes afectados por las

[59] *Dr. Charles Nelson*, citado en ITRC, *Aftermath*, pág. 27.
[60] *Jessica Van Vliet*, citada en *Karen Kleiss*, "Woman had her bank accounts drained, found herself under investigation for fraud", *The Edmonton Journal*, 20 de diciembre de 2008.
[61] *Aftermath*, página 31.
[62] *Licia Corbella*, "I.D. theft hits home", *Calgary Sun* (23 de noviembre de 2007).
[63] ITRC, *Aftermath*, página 31.

pérdidas correspondientes. En 2007 las empresas que contactaron con el Centro de recursos para el hurto de identidad de Estados Unidos denunciaron un promedio de pérdidas de aproximadamente 50.000 dólares[64].

Vale la pena destacar que, aunque las empresas son las víctimas en tales casos, pueden traspasar los costes a los consumidores cobrando altas tasas de interés. Así sucederá cuando el delito relacionado con la identidad sea un problema para todo el sector (tal como el de las tarjetas de pago).

Daño a la reputación
Las empresas víctimas del hurto de identidad pueden ver dañada su reputación como resultado tanto del error de identidad (por ejemplo, cuando una marca registrada se usa de manera fraudulenta), como de la pérdida de confianza de los clientes en su capacidad de prevenir el fraude de identidad.

Pérdida de la benevolencia de clientes
El daño a la reputación puede derivar en una pérdida de benevolencia por parte de los consumidores que los incline a cambiar a otros proveedores considerados menos inseguros.

Costos de mejora de los sistemas para combatir la delincuencia relacionada con la identidad
Las formas y técnicas de la delincuencia relacionada con la identidad evolucionan constantemente y, en algunos casos, se intensifican, lo que exige que las empresas evalúen y mejoren regularmente sus sistemas de protección.

Administraciones públicas y contribuyentes

Carga financiera para los sistemas de salud y bienestar
Las administraciones públicas sufren daños cuando el delito relacionado con la identidad implica el acceso fraudulento a servicios nacionales o la obtención indebida de documentos emitidos por las autoridades, daños cuyo coste se traspasa a los contribuyentes.

Inexactitud de la información sobre los ciudadanos consignada en registros
Son varias las consecuencias posibles de la inexactitud de la información consignada en registros causada por los defraudadores en materia de identidad, entre ellas:

- Daño a la integridad de los sistemas de registros estatales: salud, asistencia social y prestaciones públicas, permisos de conducir, pasaportes, viajes, impuestos, inmigración, contratación pública;
- Comprometer la seguridad estatal (por ejemplo, listas de vigilancia de terroristas);
- Poner en peligro la seguridad pública (conductores peligrosos, delincuentes no detectados);
- Comprometer las políticas de inmigración;

[64] *Ibid.*, puntos salientes.

- Comprometer la atención sanitaria;
- Pérdida de la confianza de los ciudadanos en el Estado;
- Mayor susceptibilidad a la corrupción y la delincuencia organizada.

Costos de mejora de los sistemas para combatir la delincuencia relacionada con la identidad
Al igual que las empresas, las autoridades públicas han de permanecer constantemente en alerta frente a las formas en que evoluciona el delito, y deben contar con sistemas eficaces para prevenirlo, detectarlo y atenuarlo.

Costos de los servicios de represión de la delincuencia en materia de identidad
Debido a su naturaleza, con frecuencia compleja y refinada, la delincuencia relacionada con la identidad exige una inversión importante en recursos de represión. Las fuerzas policiales no cuentan con los medios suficientes, tanto cuantitativa como cualitativamente, para investigar y perseguir este tipo de delito, especialmente cuando se trata de grupos de delincuentes organizados que operan a través de sistemas jurídicos distintos. Como eso es lo que sucede tanto a nivel nacional como mundial, se necesitan mecanismos internacionales más sofisticados de cooperación internacional en la investigación de tales delitos.

Según el grado de daño sufrido

Otra tipología, posiblemente útil, de las víctimas del delito relacionado con la identidad se basa en el grado de daño sufrido. Este enfoque tiene en consideración la naturaleza del delito y el tipo de daño ocasionado, mencionados anteriormente, pero con la diferencia de que se centra en el *grado* de sufrimiento de la víctima. Por ello puede ser útil para decidir cómo priorizar los servicios de reparación a la víctima, por ejemplo.

Conviene tener en cuenta dos salvedades importantes con respecto a esta tipología: en primer lugar, tal categorización no tiene en cuenta los costos ocasionados a las empresas, las administraciones públicas, la economía y los consumidores en general. Incluso cuando los daños causados a las víctimas son mínimos, las empresas afectadas deben hacer frente a costos importantes que tal vez traspasen a los consumidores, o a las administraciones, que posteriormente los cargan a los contribuyentes. En segundo lugar, el carácter subjetivo de la angustia emocional y psicológica, quizá la consecuencia más común y con frecuencia la más seria para las víctimas del delito relacionado con la identidad, puede hacer especialmente difícil su cuantificación y por lo tanto especificar la categoría a la cual pertenece una determinada víctima.

No obstante, a continuación se expone un posible enfoque:

Daño mínimo
Las víctimas del delito relacionado con la identidad comprendidas en esta categoría sufren un daño que:

- Resulta de un acto único o una serie de actos que afectan a una sola cuenta, operación o relación;

- Se puede rectificar de manera sencilla y fácil;
- Se compensa en su totalidad (pérdidas monetarias); y
- No supone un daño duradero para la reputación o la salud.

Un simple fraude con tarjeta de pago entraría en esta categoría, siempre y cuando la víctima obtenga una compensación total.

Daño significativo
Las víctimas comprendidas en esta categoría sufren un daño que:

- Presupone actos reiterados que afectan a más de una cuenta, operación o relación; y
- Es difícil y lleva mucho tiempo rectificar, o
- Implica una compensación que no es fácil obtener, o
- Es duradero (por ejemplo, para la reputación, la salud, etc.).

Es probable que la mayoría de las víctimas del delito relacionado con la identidad entren en esta amplia categoría, la cual puede dividirse a su vez en las siguientes subcategorías:

Daño significativo: de fácil solución
Las víctimas logran recomponer sus antecedentes satisfactoriamente sin excesivo esfuerzo y no sufren daños duraderos a su reputación o salud.

Daño significativo: difícil de solucionar pero sin trauma
Las víctimas sufren un daño prolongado a su reputación y crédito, deben destinar un tiempo considerable a rectificar sus antecedentes, o sufren importantes pérdidas financieras, pero no experimentan un trauma emocional o psicológico severo.

Daño significativo: trauma prolongado
Las víctimas experimentan un trauma severo y un daño considerable y de larga duración a su salud y reputación.

Según la escala del delito

El delito relacionado con la identidad puede cometerse a pequeña o gran escala. La escala puede ser minúscula como en el caso de un único delincuente y una sola víctima, o enorme como en el de una red delictiva internacional cuyo objetivo sean millones de usuarios de Internet. Dado que hay más probabilidad de que los fraudes a gran escala se denuncien y las autoridades actúen en consecuencia, sus víctimas tienden a recibir más asistencia que las de los delitos menores.

Pero mientras que el número de víctimas puede ser relevante por los costos que suponga para la economía en general y, por lo tanto, para la asignación de recursos a los servicios de policía, tiene menos relevancia desde la perspectiva de la víctima individual. Incluso un fraude de identidad a pequeña escala puede ser devastador para la víctima si conlleva

responsabilidades financieras importantes o una suplantación total de la personalidad para evadir la acción de las autoridades.

Según la identificabilidad del infractor y su relación con la víctima

Algunos estudios llevados a cabo en los Estados Unidos y el Canadá sugieren que una importante proporción de delitos relacionados con la identidad son cometidos por personas conocidas de la víctima, tales como familiares, allegados, vecinos, colegas y personal de servicio doméstico[65]. Sin embargo, las últimas estadísticas apuntan a que esa proporción disminuye y la gran mayoría de las víctimas saben poco o nada acerca de la identidad del infractor[66].

La identificación del autor del delito es un factor importante para la reparación a la víctima en la medida en que facilita las tareas de investigación y permite a la víctima entablar una acción legal. Cuanto más difícil es identificar a los infractores, más difícil es encausarlos y castigarlos. Por otro lado, los fraudes de identidad cometidos por personas cercanas a la víctima posiblemente requieran más tiempo para detectarse y, por lo tanto, sean más perjudiciales para la misma[67].

[65] ITRC, *Aftermath*, cuadro 7, págs. 14 y 15; *Sproule* y *Archer*, págs. 22 y 23.
[66] Synovate, pág. 28, gráfico 9; *Sproule* y *Archer*, págs. 22 y 23.
[67] *Sproule* y *Archer*, pág. 23.

III. BASES LEGALES PARA LA RESTITUCIÓN DE LA IDENTIDAD DE LA VÍCTIMA

Las víctimas de delitos relacionados con la identidad tienen grandes dificultades para recuperar su reputación y su información de identidad. Convencer a las autoridades de su inocencia, localizar y corregir antecedentes contaminados, tratar con burocracias muchas veces bizantinas, y prevenir futuros fraudes cometidos en su nombre es una tarea agotadora, que lleva mucho tiempo y a menudo extremadamente estresante. Para algunas víctimas, el proceso de restitución no acaba nunca. Por lo tanto, nunca se insistirá lo suficiente en la necesidad de ayudar a la víctima a rectificar y restablecer su historial.

Existe una serie de bases legales y cuasi legales de las que pueden valerse las víctimas del delito relacionado con la identidad para obtener diferentes tipos de reparación. Entre ellas figuran los códigos, las leyes y las declaraciones de los "derechos de las víctimas"; la disponibilidad de medios de restitución por la vía penal; las causas suficientes de acción civil; y los derechos humanos relativos a la identidad, la privacidad y la reputación. A continuación se examina cada una de esas bases.

1. Base normativa de la reparación a las víctimas: iniciativas sobre los derechos de las víctimas

Declaración de las Naciones Unidas sobre los principios fundamentales de justicia para las víctimas de delitos y del abuso de poder

En 1985, la Asamblea General de las Naciones Unidas aprobó la Declaración sobre los principios fundamentales de justicia para las víctimas de delitos y del abuso de poder[68]. Esta Declaración exhorta a los Estados Miembros a aplicar sus disposiciones, que se centran en la asistencia, el tratamiento y la reparación a las víctimas. Entre las disposiciones notables de la Declaración respecto a los afectados por un delito relacionado con la identidad figuran las siguientes:

> 5. Se establecerán y reforzarán, cuando sea necesario, mecanismos judiciales y administrativos que permitan a las víctimas obtener reparación mediante procedimientos oficiales u oficiosos que sean expeditos, justos, poco costosos y accesibles. Se

[68] Resolución 40/34 de la Asamblea General (29 de noviembre de 1985). En la actualidad se está elaborando un proyecto de convención de las Naciones Unidas sobre justicia y apoyo a las víctimas de delitos y de abusos de poder, con el fin de promover la aplicación y cumplimiento más a fondo de los principios fundamentales contenidos en la Declaración.

informará a las víctimas de sus derechos para obtener reparación mediante esos mecanismos.

[...]

8. Los delincuentes o los terceros responsables de su conducta resarcirán equitativamente, cuando proceda, a las víctimas, sus familiares o las personas a su cargo. Ese resarcimiento comprenderá la devolución de los bienes o el pago por los daños o pérdidas sufridos, el reembolso de los gastos realizados como consecuencia de la victimización, la prestación de servicios y la restitución de derechos.

[...]

12. Cuando no sea suficiente la indemnización procedente del delincuente o de otras fuentes, los Estados procurarán indemnizar financieramente:

a) A las víctimas de delitos que hayan sufrido importantes lesiones corporales o menoscabo de su salud física o mental como consecuencia de delitos graves;

[...]

14. Las víctimas recibirán la asistencia material, médica, psicológica y social que sea necesaria, por conducto de los medios gubernamentales, voluntarios, comunitarios y autóctonos.

[...]

16. Se proporcionará al personal de policía, de justicia, de salud, de servicios sociales y demás personal interesado capacitación que lo haga receptivo a las necesidades de las víctimas y directrices que garanticen una ayuda apropiada y rápida.

En la Declaración, el término "víctimas" se define con amplitud de modo que incluya las situaciones en las cuales no sea posible identificar, aprehender, juzgar o condenar al infractor, independientemente de la relación familiar que pueda existir entre él y la víctima. Sin embargo, al igual que otras declaraciones y textos legales sobre los derechos de las víctimas, se aplica únicamente a aquellas personas que hayan sufrido daños "como consecuencia de acciones u omisiones que violen la legislación penal vigente en los Estados Miembros". Así pues, en la medida en que los delitos relacionados con la identidad no se tipifiquen como tales en las legislaciones nacionales, la Declaración de las Naciones Unidas no resulta de gran utilidad.

No obstante, la Declaración proporciona a las víctimas de delito en materia de identidad una base normativa sólida para solicitar asistencia del Estado y medidas facilitadoras del proceso de reparación, en particular cuando dichos delitos sean reconocidos como tales a nivel nacional.

Otras resoluciones, directrices internacionales, etc.

La resolución 2004/26 del Consejo Económico y Social de las Naciones Unidas sobre cooperación internacional en materia de prevención, investigación, enjuiciamiento y

castigo del fraude, la falsificación de identidad y su uso indebido con fines delictivos y los delitos conexos alienta expresamente a los Estados Miembros a que "faciliten la identificación, la localización, el embargo preventivo, la incautación y el decomiso del producto del fraude y de la falsificación de identidad y su uso indebido con fines delictivos", entre otras medidas de carácter más preventivo. La restitución penal puede ser de utilidad para las víctimas en los casos en que los infractores sean procesados.

La Organización de Cooperación y Desarrollo Económicos (OCDE) ha publicado una serie de directrices y recomendaciones de interés dirigidas a sus Estados miembros, entre ellas las siguientes:

- Las Directrices de 1980 sobre la protección de la vida privada y la transmisión transfronteriza de datos personales (examinadas más detenidamente en el marco de la "Protección de datos").

- El Principio 2 de las Directrices de 2002 sobre la seguridad de los sistemas y redes de información, que hace hincapié en la responsabilidad de aquellos que diseñan, suministran y operan sistemas y redes de información, observando que "todos los participantes son responsables de la seguridad de los sistemas y redes de información" y que "los participantes deben ser responsables en cuanto corresponde a sus funciones individuales". Es decir, las víctimas individuales deberían tener que soportar pérdidas solamente en la medida en que sean responsables, y las entidades cuya conducta negligente contribuyó al hurto o fraude deberían asumir una parte equitativa de dichas pérdidas.

- Las Directrices de 2003 para la protección de los consumidores de prácticas comerciales transfronterizas fraudulentas y engañosas, las cuales establecen, entre otras cosas, que los países miembros procurarán:

  "[establecer] mecanismos efectivos que permitan resarcir el daño causado a los consumidores víctimas de prácticas comerciales fraudulentas y engañosas" (Parte II.A.4); y deberían

  "estudiar conjuntamente el efecto del resarcimiento al consumidor al enfrentar el problema de las prácticas comerciales fraudulentas y engañosas, prestando atención especial al desarrollo de sistemas efectivos de resarcimiento transfronterizo" (Parte VI).

- Recomendación de la OCDE de 2007 sobre resolución de disputas y resarcimiento a consumidores, la cual establece una serie de prescripciones específicas destinadas a mejorar los mecanismos de resarcimiento a nivel nacional y transfronterizo, además de la recomendación general de que:

  "Los países miembros deberían revisar sus marcos existentes para la resolución de disputas y resarcimiento con el fin de garantizar que se proporcione a los consumidores el acceso a mecanismos justos, fáciles de usar, oportunos y efectivos para la resolución de disputas y el resarcimiento, sin costo o carga innecesaria.

Al hacerlo, los países miembros deberían asegurar que sus marcos nacionales proporcionan una combinación de diferentes mecanismos para la resolución de disputas y el resarcimiento con el fin de responder a las variadas naturalezas y características de las quejas de los consumidores".

Iniciativas nacionales de asistencia a las víctimas del delito relacionado con la identidad

De conformidad con la Declaración de las Naciones Unidas, varios Estados han tomado medidas para prestar asistencia a las víctimas del delito, incluida la promulgación de leyes relativas a los derechos de las víctimas[69]. Pese a sus títulos, dichas leyes no crean por lo general derechos exigibles para las víctimas, sino que suelen ofrecer servicios de apoyo, autorizan a las víctimas para declarar ante el tribunal los efectos que han sufrido, y establecen regímenes en virtud de los cuales algunas víctimas pueden solicitar ayuda o compensación financiera (véase *infra*)[70].

Algunos sistemas jurídicos también han adoptado formalmente principios no establecidos por ley, similares a los de la Declaración de las Naciones Unidas, que estipulan que las víctimas tengan acceso a diversos tipos de apoyo y servicios de protección, que sean informadas, previa solicitud, sobre la marcha de la investigación y el procesamiento; y que sus opiniones y preocupaciones sean tomadas en cuenta por los investigadores y fiscales[71].

Si bien tales iniciativas sobre los derechos de las víctimas pueden ser útiles en algunos casos de delitos relacionados con la identidad, en general tienen por objeto tipos de delito diferentes y no abordan las necesidades primarias de las víctimas del fraude de identidad, entre las que figuran, en primer lugar, la reparación de su buen nombre y la integridad de la información de identidad que ha sido dañada.

Ya sea como parte de la legislación sobre derechos de las víctimas o por separado, muchos Estados han instituido regímenes de indemnización por lesiones, según los cuales los sufrimientos de las víctimas de delitos violentos pueden ser compensados. Los afectados deben solicitar a la autoridad competente una indemnización, que puede ser concedida o no. Sin embargo, dichas compensaciones se otorgan en general únicamente a las víctimas y sus familiares que hayan sufrido graves lesiones físicas, trauma emocional o muerte como resultado de un delito violento[72]. Dado el limitado enfoque de estos regímenes de delitos violentos, es poco probable que las víctimas del delito relacionado con la identidad tengan derecho a dicha compensación.

[69] Por ejemplo Nueva Zelandia, *Victims' Rights Act*, 2002.

[70] Véase, por ejemplo, *James Blindell*, Review of the Legal Status and Rights of Victims of Identity Theft in Australasia, Australasian Centre for Policing Research, Report Series No.145.2 (2006).

[71] *Ibid*.

[72] *Blindell, op cit*. Véanse también los regímenes legislativos de la compensación de lesiones de origen criminal en el Canadá y los Estados Unidos.

2. Base legal para la restitución: normativa penal

Convenciones internacionales sobre normativa penal

Están en curso iniciativas para llevar a la práctica la Declaración de las Naciones Unidas sobre los principios fundamentales de justicia para las víctimas de delitos y del abuso de poder mediante una nueva convención de las Naciones Unidas[73]. Entre tanto, algunas convenciones internacionales vigentes aplicables a la delincuencia en materia de identidad abordan los temas relacionados con las víctimas de diversas maneras. Quizás la más relevante sea la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional[74] ("Convención de Palermo"), cuyo artículo 25 prevé de manera explícita asistencia y protección a las víctimas, como se indica a continuación:

> 1. Cada Estado Parte adoptará medidas apropiadas dentro de sus posibilidades para prestar asistencia y protección a las víctimas de los delitos comprendidos en la presente Convención, en particular en casos de amenaza de represalia o intimidación.
>
> 2. Cada Estado Parte establecerá procedimientos adecuados que permitan a las víctimas de los delitos comprendidos en la presente Convención obtener indemnización y restitución.
>
> 3. Cada Estado Parte permitirá, con sujeción a su derecho interno, que se presenten y examinen las opiniones y preocupaciones de las víctimas en las etapas pertinentes de las actuaciones penales contra los delincuentes sin que ello menoscabe los derechos de la defensa.

Tanto la Convención de Palermo como la Convención de las Naciones Unidas contra la Corrupción[75] ("Convención de Mérida") incluyen disposiciones que establecen la devolución de los bienes decomisados o el producto del delito a los Estados Parte que lo soliciten, para que estos puedan indemnizar a las víctimas o devolver los bienes o el producto a sus legítimos dueños[76]. La Convención de Palermo también exige que los Estados Parte establezcan o mejoren programas específicos de capacitación relativos, entre otras cosas, a los "métodos utilizados para proteger a las víctimas y los testigos"[77].

Restitución en el marco de las leyes penales nacionales

Tal como se menciona más adelante en el contexto de "Mejores prácticas", algunos ordenamientos jurídicos prevén la restitución a las víctimas en su legislación penal. La restitución normalmente procede solo en los casos en que haya una sentencia condenatoria, y

---

[73] International Victimology Institute, Tilburg University ("INTERVICT"), disponible en línea en: http://www.tilburguniversity.nl/intervict/undeclaration/. El actual proyecto de convención se titula "Convención de las Naciones Unidas sobre justicia y apoyo a las víctimas de delitos y del abuso de poder".

[74] Resolución 55/25 de la Asamblea General (15 de noviembre de 2000).

[75] Resolución 58/4 de la Asamblea General (31 de octubre de 2003).

[76] Convención de Palermo, Artículo 14 2); Convención de Mérida, Artículo 57 3) *c)*.

[77] Artículo 29 1) *i)*.

solo para ciertos tipos de delito. Además, suele estar limitada a una indemnización por los gastos reales contraídos como resultado directo del delito.

Por lo tanto, la restitución penal de las víctimas del delito relacionado con la identidad es asequible únicamente en los pocos casos en los cuales los infractores son procesados por la vía penal y culminan con una condena. Exige capacidad de pago por parte del delincuente, aunque no siempre existe. Por otro lado, si la restitución se limita a la compensación por gastos documentados, pagados del propio bolsillo, es poco su valor cuando los principales perjuicios sufridos por la víctima son emocionales o dependen del tiempo gastado o los ingresos perdidos. Por último, la restitución penal resulta de escasa utilidad en la medida en que no restablece la información de identidad ni el buen nombre de la víctima.

3. Base legal para la restitución: normativa civil

Legislación sobre información crediticia

Las leyes sobre información crediticia regulan las actividades de las agencias de informes sobre créditos, es decir, las agencias que crean, administran y procuran acceso a los historiales de crédito de consumidores particulares. Dichas agencias son un pilar de las economías modernas basadas en el crédito y juegan un papel fundamental en cuanto al fraude económico relacionado con la identidad, en la medida en que reúnen, guardan y dan a conocer los datos fraudulentos cuyo resultado es la victimización. Las leyes que regulan estas agencias normalmente imponen límites con respecto a la información que puede obtenerse y a quien se puede dar a conocer, exigen que la agencia tome todas las medidas razonables para asegurarse de que la información en su poder es precisa e imparcial, y ofrecen a los consumidores el derecho a acceder a sus informes y a corregir los errores[78].

En respuesta al reciente aumento de casos de fraude económico relacionado con la identidad, en varios sistemas jurídicos de América del Norte se han enmendado las leyes sobre información crediticia para, entre otras cosas, dar a las víctimas del hurto de identidad la posibilidad de insertar un aviso de "alerta de fraude" o de "congelación" de sus expedientes de crédito, lo que limita las posibilidades que tienen los delincuentes para obtener crédito a nombre de las mismas. Tales leyes son de importancia crucial para las víctimas de fraude económico de identidad al efecto de detectar y prevenir más fraudes, y las mismas se examinan con más detalle en la siguiente sección, en el contexto de "Mejores prácticas—Agencias de información crediticia".

Así, la legislación sobre esa información reconoce a las víctimas derechos directos para controlar el intercambio de sus datos financieros y para reparar el historial de sus finanzas. Otras leyes civiles, que se examinan a continuación, prevén derechos indirectos de reparación a las víctimas a través de denuncias formales ante las autoridades o de acciones civiles.

[78] Por ejemplo, Fair Credit Reporting Act, 15 USC. art. 1681 y ss.; Ontario Consumer Reporting Act, R.S.O. 1990, c.C-33.

Legislación sobre protección del consumidor

La legislación sobre protección del consumidor también es relevante en la medida en que ofrece a los consumidores víctimas de delito relacionado con la identidad vías de recurso frente a las deudas contraídas de manera fraudulenta[79]. En algunos Estados, la ley protege a los consumidores en cuanto a la responsabilidad por el costo derivado de operaciones fraudulentas llevadas a cabo por delincuentes suplantadores de identidad en determinadas situaciones. Por ejemplo, en los Estados Unidos, la responsabilidad del consumidor por un cargo sin autorización a una tarjeta de crédito se limita a 50 dólares, siempre y cuando se notifique a la compañía emisora de la tarjeta de crédito en un plazo de 60 días, y la responsabilidad por un cargo a una tarjeta de débito se limita a 50 dólares si se denuncia en un plazo de dos días hábiles, y a 500 dólares si se denuncia más tarde. De conformidad con la Directiva del Consejo Europeo relativa a la comercialización a distancia de servicios financieros: "Los Estados miembros velarán por que existan medidas apropiadas para que: el consumidor pueda solicitar la anulación del pago en caso de utilización fraudulenta de su tarjeta de pago en el marco de contratos a distancia; en caso de dicha utilización fraudulenta se abonen en cuenta al consumidor las sumas abonadas en concepto de pago o se le restituyan"[80].

Leyes de protección de datos

Del ámbito general del derecho a la privacidad, que se examina más adelante, emana un gran cúmulo de leyes y principios rectores para la protección de datos a nivel nacional, regional e internacional, que son aplicables tanto en el sector público como en el privado[81]. Estas leyes son especialmente importantes para las víctimas de delitos relacionados con la identidad ya que su finalidad específica es brindar protección contra dichos delitos y otros usos indebidos de la información personal. Además de establecer las obligaciones de protección de datos aplicables a los sectores público y privado, por lo general proporcionan a las víctimas una vía para buscar reparación.

Fundamentos de las leyes de protección de datos

Los documentos internacionales que prescriben la adopción de leyes de protección de datos a nivel nacional, o cuyo fin es facilitar a los Estados la redacción de leyes sobre protección de datos, son, entre otros, los siguientes:

- Directrices de la OCDE sobre la protección de la vida privada y la transmisión transfronteriza de datos personales (1980)[82];
- Convenio del Consejo de Europa para la protección de las personas en relación con el proceso automático de datos personales (1981)[83];

[79] Dicha legislación también figura en el inventario de las prácticas del sector público para la reparación de las víctimas, *infra*.
[80] Directiva 2002/65/CE, artículo 8.
[81] Electronic Privacy Information Centre and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007). ["EPIC et al".]
[82] Véase: www.oecd.org.
[83] Convenio del Consejo de Europa núm. 108 (18 de septiembre de 1980).

- Principios rectores de las Naciones Unidas relativos a los ficheros computadorizados de datos personales (1990)[84];
- Directiva de la Unión Europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ("Directiva de protección de datos") (1995)[85];
- Marco relativo a la privacidad, Asociación de Cooperación Económica en Asia y el Pacífico (APEC) (2004)[86].

En el último decenio, el número de países que han adoptado leyes integrales o sectoriales de protección de datos para el sector privado ha aumentado enormemente, debido en gran parte al extraordinario incremento de riesgos como la delincuencia relacionada con la identidad a raíz de la informatización de los datos y al enorme crecimiento de la transmisión transfronteriza de datos.

Contenido de las leyes de protección de datos

Dichas leyes se basan en los principios establecidos en las Directrices de la OCDE y en la Convención del Consejo de Europa, entre otros documentos[87]. Estos principios rigen la recopilación, conservación, uso y divulgación de "datos personales", que generalmente se definen como toda información de cualquier tipo o cualquier forma sobre una persona identificable. Los principios para una información correcta tal como se establecen en las directrices de la OCDE y demás documentos afines son:

- *La limitación de la recogida* (únicamente recogida de datos personales por medios justos y legales, con el consentimiento del sujeto implicado siempre que así proceda, y solo cuando sea necesario para propósitos especificados);
- *La calidad de los datos* (los datos personales deben ser exactos, completos y actuales en la medida necesaria para dichos propósitos);
- *La especificación del propósito* (se deben especificar los propósitos para los cuales se recogen los datos personales, a más tardar en el momento de la recogida; en caso de que surjan nuevos propósitos habrá que especificarlos de nuevo);
- *La limitación del uso* (los datos personales no se utilizarán ni divulgarán salvo con el consentimiento del sujeto implicado o por imposición legal);
- *La salvaguardia de la seguridad* (los datos personales se protegerán aplicando salvaguardias razonables contra riesgos tales como pérdida o acceso no autorizado, destrucción, uso, modificación o divulgación);
- *La transparencia* (los responsables del control de datos deben actuar con transparencia en cuanto a las prácticas y políticas relativas a los datos personales);

[84] Aprobados por resolución 45/95 de la Asamblea General (14 de diciembre de 1990).
[85] Directiva 95/46/CE.
[86] APEC Privacy Framework (2005).
[87] Véase, por ejemplo, National Standard of Canada CAN/CSA-Q830-96, Model Code for the Protection of Personal Information, adoptado como texto legal Schedule 1 de Personal Information Protection and Electronic Documents Act, S.C.2000, c.5.

- *La participación individual* (toda persona tendrá derecho a acceder a los datos sobre la misma que obren en poder de los responsables del control y a hacer que se rectifiquen los datos inexactos);
- *La responsabilidad* (los responsables del control de datos deben rendir cuentas del cumplimiento de las medidas para dar efectividad a estos principios).

Muchos países han adoptado en sus legislaciones nacionales estos derechos y obligaciones u otros afines, ya sea en forma de leyes integrales o intersectoriales (como por ejemplo, en Europa, Canadá y Australia), o de leyes para sectores y temas específicos, tales como las que rigen el sector financiero, la información en la esfera sanitaria y la privacidad infantil en línea en los Estados Unidos.

Aplicabilidad a la delincuencia relacionada con la identidad

Los derechos a la privacidad en materia de información, en particular las leyes de protección de datos, son de importancia directa para las víctimas de delitos relacionados con la identidad. Estas leyes establecen obligaciones de reducir al mínimo los datos y garantizar su seguridad, precisamente para proteger dicha información contra el acceso y uso no autorizados. El incumplimiento de esas obligaciones legales por parte de las entidades es con frecuencia un factor causativo de la delincuencia en la esfera de la identidad.

Las leyes de protección de datos establecen, entre otras, las siguientes obligaciones de las entidades:

Minimizar la reunión y retención de datos

Los delincuentes se aprovechan de la proliferación de bases de datos cada vez más extensas y repletas de información personal, creadas y mantenidas por entidades públicas y privadas. Aunque muchas de ellas están celosamente protegidas, la seguridad absoluta no existe y difícilmente pasa un día sin que se anuncie un fallo de seguridad que deje datos personales expuestos al posible abuso de los usurpadores de identidad. Las entidades podrían reducir significativamente el riesgo de acceso no autorizado o el uso de los datos personales que obren en su poder simplemente limitándose a reunir únicamente los datos que necesiten y destruyéndolos tan pronto dejen de necesitarlos. En un reciente caso de hurto y fraude de identidad a gran escala en América del Norte los delincuentes accedieron a una base de datos de un importante distribuidor, que contenía información detallada de las tarjetas de crédito de los clientes y otros pormenores, algunos de los cuales jamás debieron recabarse y que, en su mayoría, no deberían haberse conservado por un período tan largo como se hizo[88].

Tomar medidas razonables para garantizar la seguridad de la información

Esto incluye proteger los datos frente a las amenazas exteriores utilizando, por ejemplo, cortafuegos informáticos, mecanismos físicos de bloqueo y otros métodos, formas correctas de eliminación de los registros y medios electrónicos, así como cuidar de

[88] Office of the Privacy Commissioner of Canada y Office of the Information and Privacy Commissioner of Alberta, Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies Inc./ Winners Merchant International L.P. (25 de septiembre de 2007).

que el personal reciba la debida capacitación y los sistemas se vigilen para prevenir fallos de seguridad.

También incluye proteger los datos frente a las amenazas internas adoptando medidas como la preselección y supervisión de los empleados y controlando el acceso para restringir sus posibilidades de utilizar las bases de datos personales.

Las medidas de seguridad incluyen también la autenticación efectiva de quienes solicitan datos o servicios de crédito. La falta de una autenticación adecuada de los solicitantes de créditos, prestaciones públicas, documentos de identidad u otros servicios es una característica común de la criminalidad en materia de identidad: los delincuentes triunfan en sus fraudes porque las entidades en cuestión se lo permiten.

Notificar las violaciones de la seguridad a las personas afectadas y las autoridades
Dado el reciente aumento de los delitos relacionados con la identidad, se han adoptado disposiciones sobre la notificación de las violaciones de la seguridad en la legislación de muchos sistemas jurídicos, y muchos otros están considerando la posibilidad de adoptarlas. Las normas de notificación de las violaciones de la seguridad exigen que las entidades comuniquen a las personas afectadas y a las autoridades competentes las infracciones a causa de las cuales los datos personales queden expuestos a acceso no autorizado y posible hurto de identidad. Tales normas buscan lograr dos propósitos: permitir a las eventuales víctimas mitigar el daño tomando medidas preventivas, y servir de aliciente para que las entidades procuren prevenir tales violaciones (evitando de ese modo el daño a la reputación y los costos de notificación).

Derechos a reparación conforme a las leyes de protección de datos

Las leyes de protección de datos prevén regímenes de aplicación variados, encomendándolos en algunos casos a servicios estatales y, en otros, al sector privado por conducto de una autoridad responsable o de los tribunales. La eficacia de estos mecanismos de aplicación varía según los Estados, y tanto el modelo público como el privado han sido criticados por tolerar serios incumplimientos[89].

Con arreglo a la mayoría de las leyes de protección de datos, los que sufren daños como resultado del incumplimiento de esas leyes por alguna entidad tienen derecho a reparación. En algunos regímenes, las víctimas pueden presentar denuncias y obtener órdenes vinculantes de una autoridad especial de protección de datos establecida para tal fin[90]. Según otros modelos, deben solicitar judicialmente una compensación u otro tipo de reparación aplicable[91]. En la mayoría de los casos, sus derechos de reparación se limitan a una compensación por los daños sufridos, que en algunos regímenes incluye el daño emocional.

[89] Véase, por ejemplo, *Chris Connolly*, The US Safe Harbor: Fact or Fiction? (Galexia, 2008), y CIPPIC, "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up" (abril de 2006).
[90] Por ejemplo, leyes de protección de datos en el sector privado en las provincias de Quebec, Alberta y British Columbia (Canadá).
[91] Este es el caso conforme a la ley federal aplicable al sector privado del Canadá (Personal Information Protection and Electronic Documents Act).

Existen pocos indicios de que las víctimas de delitos relacionados con la identidad se hayan valido de estos derechos de reclamación. Esto se debe posiblemente a varios factores, entre ellos la baja probabilidad de obtener un fallo de indemnización que justifique los gastos judiciales, así como los impedimentos de la víctima para determinar cómo, cuándo y dónde obtuvo su información el delincuente y la consiguiente dificultad de establecer una relación de causalidad entre el fraude en cuestión y el incumplimiento de las leyes de protección de datos por parte de una entidad.

Otras leyes sobre la privacidad

Además de las leyes de protección de datos y los derechos constitucionales, muchos países han consagrado en su legislación o reconocido judicialmente otros derechos de privacidad aplicables al sector privado[92]. Concretamente, muchos códigos civiles estipulan un derecho a la privacidad que puede dar lugar a acciones procesales[93]. Estas leyes normalmente prohíben o hacen punibles los actos de invasión de la privacidad tales como:

- El uso sin autorización del nombre o imagen de una persona para obtener un beneficio comercial o de otro tipo;
- El fisgoneo, espionaje u otras formas de observación de la vida privada;
- La escucha o la grabación solapada de telecomunicaciones privadas; y
- El uso no autorizado de cartas personales, diarios o documentos particulares de otra persona.

Por ejemplo, una demandante en Quebec (Canadá) obtuvo una indemnización de una revista que había publicado en portada una fotografía suya sin autorización. Según la ley de Quebec, la publicación no autorizada de dicha fotografía constituyó una violación de la privacidad de la víctima y resultó en un fallo de indemnización[94].

Estas acciones también son posibles en el marco del ilícito civil de "apropiación indebida de la personalidad", reconocido por algunos tribunales de derecho consuetudinario[95]. En tal caso se reconoce implícitamente el derecho de la persona a controlar y comercializar su propia imagen. Las personas (con frecuencia famosas), cuyas imágenes habían sido explotadas de este modo, obtuvieron indemnizaciones para compensar la pérdida de control sobre la imagen y la pérdida de control respecto a quién o a qué se había asociado su imagen. Dicha apropiación indebida es claramente análoga a la de la identidad en el contexto de la suplantación de personas y es posible que ese acto punible civil pueda ampliarse y abarcar a los ladrones y defraudadores de identidad. Hay factores que podrían limitar su aplicación, como el tipo y alcance de la información personal obtenida indebidamente y del daño causado a la víctima.

---

[92] Cuatro provincias canadienses (British Columbia, Manitoba, Newfoundland y Saskatchewan) han establecido delitos punibles de invasión de la privacidad, sin prueba del daño, contra cualquiera que conscientemente y sin alegar un derecho viola la privacidad de otra persona. La provincia de Quebec prohíbe actos de invasión de privacidad similares en su Código Civil (artículos 35 y 36), así como muchos otros ordenamientos en el ámbito civil.

[93] Por ejemplo, el Código Civil francés, artículos 9 y 1382; Código Civil de Quebec, S.Q., 1991, c. 64, artículos 35 y 36.

[94] *Aubry v. Editions Vice-Versa* Inc., [1998]1.S.C.R. 591.

[95] Véase, por ejemplo: *Horton v. Tim Donut Ltd.* (1997), 75 C.P.R. (3d) 467 (Ont.C.A.).

En algunos sistemas basados en el derecho consuetudinario existe también, en fase naciente, el ilícito civil de invasión de la privacidad, lo que podría ser útil para las víctimas del delito relacionado con la identidad[96]. Esta causa de acción legal considera la intromisión en los espacios de aislamiento o soledad o en los asuntos privados de una persona, un ilícito civil por cuyo daño se puede conceder indemnización.

Pero tienen un fundamento legal más sólido los derechos a la privacidad explícitamente amparados por ley, como en el caso de Quebec mencionado anteriormente. Ha habido por lo menos un caso de fraude de identidad que se litigó favorablemente en el marco del derecho civil a la privacidad francés, en el cual se decretó que el infractor compensara a la víctima por el daño emocional, y al seguro médico público por los gastos conexos[97].

Estas leyes brindan a las víctimas de delito relacionado con la identidad bases legales claras para obtener una indemnización por sus pérdidas (por ejemplo, por el uso no autorizado del nombre y documentos personales de la víctima), pero carecen de utilidad a menos que la víctima pueda identificar al infractor. Ahora bien, con frecuencia las víctimas de fraude de identidad se ven en la imposibilidad de identificarlo. Incluso en los casos en que sí pueden hacerlo, tal vez el infractor resulte ser "inmune al fallo" (es decir, incapaz de pagar la indemnización ordenada por el tribunal) cuando la víctima obtenga el decreto judicial. Otros factores tales como el bajo monto de las indemnizaciones y las altas costas restringen la litigación por parte de las víctimas al amparo de estas leyes de privacidad.

Otras leyes en el ámbito civil

Causas de acción contra los infractores

Leyes sobre ilícitos civiles en general

Las leyes sobre ilícitos civiles y otras leyes generales de índole civil prevén numerosas causas de acción, muchas de las cuales podrían aplicarse a los delincuentes en cuestiones de identidad. Con arreglo al derecho consuetudinario, tales actos punibles incluyen la impostura, el fraude, las actividades molestas (interferencia en el disfrute de la propiedad), interferencia intencional o negligente en la propiedad (translimitación), provocación intencional de angustia emocional y difamación.

Una víctima de fraude de identidad puede demandar al autor del delito en virtud de dichas causas de acción, y buscar compensación tanto por daños materiales como inmateriales, tales como el dolor y el sufrimiento. Sin embargo, dichas causas de acción no son demasiado útiles cuando el autor es desconocido, se encuentra en una jurisdicción remota o existen otras dificultades para identificarlo y hacer que pague.

[96] Tradicionalmente, el derecho consuetudinario no reconocía la invasión de la privacidad como ilícito civil independiente, pero algunos tribunales (por ejemplo, en el Canadá) están empezando a reconocerlo como tal, invocando la necesidad de que el derecho evolucione en consonancia con los valores constitucionales. Véase, por ejemplo: *Savik Enterprises Ltd. v. Nunavut,* [2004] Nu.J. núm. 1 (Nun.C.J.); *Somwar v. McDonald's Restaurants of Canada Ltd.,* [2006] O.J. núm. 64 (Ont. S.C.J.).

[97] Véase, FIDIS, pág. 40.

Difamación

Las leyes sobre difamación tienen el fin de proteger a las personas y empresas de los daños causados a su reputación por comentarios falsos y despectivos sobre ellas. Estos comentarios pueden ser verbales (maledicencia) o escritos (libelo). Los mismos deben ser publicados o comunicados de otra forma a un tercero, y constituir un ataque directo a la víctima para que puedan ser punibles por ley. La difamación es en gran medida un asunto de derecho civil, pero hay casos graves que, según el ordenamiento jurídico, pueden ser tratados como delitos.

La difamación guarda una clara similitud con el fraude de identidad en cuanto causa daños a la reputación de las víctimas. Pero para que haya difamación tienen que existir declaraciones orales o escritas sobre la víctima. En cambio, el fraude de identidad normalmente entraña un daño a la reputación de manera indirecta, resultante de acciones y no de declaraciones del infractor. De todas formas, es posible que se considere que la firma fraudulenta de documentos en nombre de otra persona o la presentación de información crediticia falsa por una agencia de crédito constituyen difamación en cuanto causan daño a la reputación de la víctima[98]. Las disposiciones legales sobre difamación también podrían ser de utilidad a las empresas víctimas del hurto de identidad, en la medida en que la publicación y el uso fraudulentos del nombre y logotipo de la empresa asignen principalmente daños a la reputación de la misma.

Derechos de propiedad intelectual

En virtud de las leyes sobre marcas registradas, las víctimas de hurto o fraude de identidad empresarial (es decir, la apropiación indebida de la identidad de una empresa) están facultadas para demandar y obtener indemnización por los daños que causen quienes vulneren esos derechos. Las disposiciones legales sobre marcas registradas tienen precisamente el fin de ofrecer remedio para tales violaciones, y parecerían proporcionar a las víctimas de dicho hurto o fraude una base definida para interponer demanda contra los infractores[99].

Los autores (individuales o empresariales) de obras están amparados por leyes de propiedad intelectual destinadas a proteger sus creaciones contra usos no autorizados. Según el sistema jurídico aplicable, tales derechos incluyen el derecho económico de los autores a que sus obras no se presenten de manera perjudicial para las futuras ventas, el derecho de los famosos a que no se abuse de su imagen física con el fin de crear una apariencia de aval falsa, y el derecho moral a que las obras no sean objeto de trato despectivo[100]. En algunos casos de delincuencia relacionada con la identidad podría haber violación de estos derechos, si tales casos no tienen mucho realce en la literatura sobre la materia y es probable que sean raros, dado que con frecuencia el fraude de identidad no supone la utilización de obras creativas de las víctimas.

[98] No se ha encontrado jurisprudencia ni comentario revestido de autoridad sobre este tema.

[99] Por ejemplo Microsoft ha denunciado violaciones de su marca registrada en varias demandas contra impostores que utilizaban el nombre de la empresa para conseguir engañosamente datos a través del correo electrónico. Véase, por ejemplo: *Todd Bishop*, "Microsoft casts net for phish culprits", *Seattle Post-Intelligencer* (1 de abril de 2005).

[100] Por ejemplo, s.14.1 de la ley canadiense *Copyright Act*, R.S.C. 1985, c.C-42. Aunque se puede renunciar a ellos según las disposiciones legales canadienses sobre derechos de autor, los derechos morales son irrenunciables en muchos otros sistemas jurídicos.

Causas de acción contra las entidades que facilitaron el delito

Las disposiciones legales de posible aplicación a las entidades cuyas acciones u omisiones facilitaron el delito relacionado con la identidad son probablemente más útiles para las víctimas del delito, ya que en el caso de dichas entidades es relativamente fácil identificarlas, interponer demanda y cobrar indemnización. Las causas de acción son, entre otras, el incumplimiento de contrato, la negligencia y el abuso de confianza[101].

En los Estados Unidos ha habido cierto número de acciones judiciales contra terceros cuyos actos o negligencia contribuyeron al hurto o fraude de identidad, algunas de las cuales se resolvieron satisfactoriamente. Las alegaciones en estos casos se dividen en cuatro categorías principales: negligencia en la seguridad de la información personal, venta negligente de información, fallo de un banco en la prevención del hurto o fraude de identidad, o la mitigación de los daños, y responsabilidad de las agencias de información crediticia por no prevenir o reparar los casos de fraude. Tal como sucede en las demandas de indemnización por fallos de seguridad que derivan en una agresión violenta, se acusa a la parte demandada de no haber tomado las precauciones razonables para proteger a la víctima de daños previsibles causados por un tercero[102].

Con arreglo a la normativa civil alemana, los tribunales han dictaminado que, una vez que una entidad tiene conocimiento de que una cuenta anterior fue abierta de manera fraudulenta a nombre de otra persona, deberá tomar medidas preventivas que impidan una acción similar respecto a la víctima.

En cualquiera de los casos, para resarcirse de las pérdidas es preciso que la víctima pruebe que tales negligencias o fallos contribuyeron a producirlas. En el contexto del fraude de identidad con frecuencia es difícil establecer una relación causal porque la víctima normalmente suele tener poca información acerca de la manera en que se cometió el fraude. Además, algunos tribunales se muestran reacios a conceder indemnización por un ilícito civil (negligencia) en los casos de "pura pérdida económica" (es decir, una pérdida económica no relacionada directamente con el daño físico a la víctima o a su propiedad)[103]. Esta doctrina limita aún más las posibilidades que tienen las víctimas de la delincuencia relacionada con la identidad de obtener una reparación al amparo de las disposiciones sobre ilícito civil.

Insuficiencias de la litigación como vía de reparación a las víctimas de la delincuencia relacionada con la identidad

Como se ha señalado anteriormente las víctimas de delitos en materia de identidad no parecen haber aprovechado plenamente las vías de recurso que brinda la normativa civil.

---

[101] El ilícito civil de "abuso de confianza" tiene el fin de proteger la información privada que se da a conocer en confianza, y para una demanda por abuso de confianza normalmente es necesario que la información sea de carácter confidencial, que se haya comunicado en confianza y que su divulgación vaya en detrimento del demandante.

[102] Véase: *Jeffrey Dion and James Ferguson*, "Civil Liability for Identity theft", (1 de febrero de 2007); disponible en línea en http://goliath.ecnext.com/coms2/gi_0199-6285492/Civil-liability-for-identity-theft.html. Véase también: W*ood and Schecter,* "Identity Theft: Developments in Third Party Liability", American Bar Association, *Section of Litigation Consumer and Personal Rights Newsletter*, vol. VIII, núm. 3 (verano de 2002), disponible en línea en: http://www.jenner.com/files/tbl_s20Publications/RelatedDocumentsPDFs1252/380/Identity_Theft.pdf.

[103] *Jennifer Chandler*, "Negligence Liability for Breaches of Data Security", 23 *Banking & Finance Law Review* (2008), págs. 223 a 247.

Ello no es sorprendente dados los muchos obstáculos y la falta de incentivos que supone entablar un litigio en el contexto de este tipo de delincuencia, aspecto en el que suelen figurar:

- La falta de posibilidades de identificar al infractor y a la entidad o entidades que facilitaron el delito;
- La falta de posibilidades de probar una relación causal entre la negligencia de la entidad y las pérdidas sufridas;
- La imprevisibilidad de los litigios en cuanto a fallos y vías de reparación;
- Las costas exorbitantes de los litigios, incluso las causadas por la obtención de pruebas;
- La probabilidad de una escasa indemnización en caso de ganar;
- La escasa probabilidad de cobrar al autor del delito la indemnización concedida;
- La inevitable exposición en público de los asuntos privados; y
- La carga emocional que representa el litigio.

Como se indica en un informe reciente acerca de los derechos de las víctimas del hurto de identidad en Australia, "el principal factor disuasivo para entablar este tipo de acciones son las costas de asistencia letrada y peritos que pueden acarrear, no solo las costas del demandante, sino también las de la parte demandada si la acción fracasa. Además, el tribunal puede exigir a los que entablen la acción (antes de la vista del caso) que presenten promesas o garantías respecto de las costas en caso de que el resultado no sea satisfactorio"[104].

4. Derechos humanos pertinentes

Algunos derechos humanos reconocidos en la normativa nacional e internacional pueden ser relevantes, e incluso dar origen a obligaciones legales, en lo que atañe a las medidas estatales de reparación a las víctimas de la delincuencia relacionada con la identidad. Se trata en particular de los derechos a la identidad, la reputación y la privacidad, cada uno de los cuales se examina a continuación.

Aplicación de los derechos humanos internacionales y constitucionales a las relaciones en el sector privado

Normalmente los derechos constitucionales se limitan en su aplicación directa al sector público, y únicamente inciden indirectamente en el sector privado por su plasmación en las leyes que afectan a los organismos privados, y por su rango institucional de normas superiores que impregnan y guían la interpretación de las leyes que regulan las relaciones privadas. La mayoría de los tribunales se han mostrado reticentes a ampliar los derechos humanos vigentes en el sector público de forma que determine obligaciones de dicho

[104] *Blindell* (2006).

sector en relación con asuntos de la esfera privada (tal como la obligación de reparar a las víctimas de un delito). Sin embargo, los derechos garantizados por la Constitución pueden servir de base para definir obligaciones del sector público de protección a los ciudadanos frente a la delincuencia en el sector privado[105]. En algunos sistemas jurídicos, los derechos constitucionales son aplicables directamente al sector privado[106].

Al margen de las disposiciones explícitas que extienden las garantías constitucionales al sector privado, la aplicación de los derechos constitucionales a dicho sector es especialmente relevante en la doctrina europea de la *Drittwirkung*, en virtud de la cual los derechos humanos fundamentales establecidos en los documentos constitucionales pueden constituir la base de derechos y obligaciones entre actores del sector privado. Si bien esta doctrina sigue siendo objeto de controversia, ha sido aplicada en una serie de casos. Por ejemplo, el Tribunal Europeo de Derechos Humanos ha fallado que el artículo 8 del Convenio Europeo de Derechos Humanos ("CEDH")[107] es aplicable a las violaciones de la privacidad entre actores privados, de modo que requiere la adopción de medidas protectoras (por ejemplo, otras leyes penales) por el Estado cuando las ya existentes (por ejemplo en derecho civil) son inadecuadas[108], dictaminando en un caso reciente lo siguiente:

> 42. El Tribunal reitera que, aunque el propósito del artículo 8 es fundamentalmente proteger a la persona contra una intervención arbitraria de las autoridades públicas, no obliga al Estado a abstenerse de tal injerencia: además de ese cometido principalmente negativo, pueden existir obligaciones positivas inherentes a un respeto efectivo de la vida privada o familiar (véase *Airey c. Irlanda*, fallo del 9 de octubre de 1979, Serie A núm. 32, párr. 32).
>
> 43. Estas obligaciones pueden implicar la adopción de medidas destinadas a garantizar el respeto a la vida privada, incluso en el ámbito de las relaciones entre los particulares mismos. Existen diferentes maneras de garantizar el respeto a la vida privada, y la naturaleza de la obligación del Estado dependerá del aspecto concreto de la vida privada en cuestión. La elección de los medios para asegurar el cumplimiento del artículo 8 en el ámbito de la protección contra las acciones de particulares entra, en principio, en el margen de apreciación del Estado, pero la disuasión efectiva contra actos graves, en los que valores fundamentales y aspectos esenciales de la vida privada están en juego, requiere disposiciones efectivas de derecho penal (véanse: *X e Y contra los Países Bajos*, párrs. 23, 24 y 27; *August contra el Reino Unido* (dec.), núm. 36505/02, 21 de enero de 2003 y M.C. contra Bulgaria, núm. 39272/98, párr. 150, CEDH 2003-XII).
>
> [...]

[105] Véase: *Dawn Oliver and Jörg Fedtke, eds., Human Rights and the Private Sphere: A Comparative Study* (Routledge, 2007).

[106] Por ejemplo, el artículo 25 1) de la Constitución griega establece: "Estos derechos también se aplican a las relaciones entre los particulares cuando así proceda".

[107] Es decir, el derecho de respeto a la vida privada y familiar. Para un análisis más a fondo de este derecho, véase más adelante la sección "Derecho a la privacidad".

[108] *X e Y c. los Países Bajos* (1985), Caso núm. 16/1983/72/110 del CEDH. En este caso se juzgaba la no actuación por parte de autoridades estatales contra un delito de violación de una persona discapacitada mental adulta debido a una laguna en la legislación.

> 46. [...] el Tribunal señala que no ha excluido la posibilidad de que la obligación positiva del Estado, a tenor del artículo 8, de salvaguardar la integridad física y moral de la persona se extienda a cuestiones relativas a la efectividad de una investigación criminal, aún cuando la responsabilidad penal de los funcionarios del Estado no esté en juego (véase *Osman c. el Reino Unido*, fallo del 28 de octubre de 1998, Informes 1998-VIII, párr. 128). Para el Tribunal, los Estados tienen la obligación positiva, inherente al artículo 8 del Convenio, de penalizar los delitos contra la persona, incluidas las tentativas de delito, y de reforzar el efecto disuasivo de la penalización aplicando en la práctica las disposiciones del derecho penal por medio de actividades de investigación y procesamiento eficaces (véase, *mutatis mutandis, M.C. c. Bulgaria*, mencionado *supra*, párr. 153)[109].

Derecho a la identidad

Naturaleza del derecho

La identidad es una necesidad intrínseca de la persona. Es fundamental para que la misma pueda establecer y mantener vínculos psicológicos, sociales y culturales, y que pueda formar parte de agrupaciones humanas como la familia, la sociedad y la nación. Sin una identidad reconocida, las personas no pueden participar plenamente en la sociedad ni ejercer sus derechos civiles y políticos. Los elementos de la identidad incluyen, entre otros, atributos tales como el nombre y la nacionalidad, las características biométricas como las huellas dactilares, la información biográfica como la fecha de nacimiento, los antecedentes familiares y laborales.

El derecho a la identidad civil (en particular, al nombre, nacionalidad, inscripción en registro, personalidad jurídica) sirve de base de la que emanan derechos políticos, sociales y económicos (así como obligaciones). Es origen de los derechos a la ciudadanía y la participación democrática, a la personalidad ante las instituciones y mecanismos del Estado, a prestaciones y programas estatales, incluidas la atención de salud y la educación, y a derechos en la esfera privada como los concernientes al empleo, la propiedad de bienes y el crédito.

Base jurídica

En el derecho positivo internacional, el derecho a la identidad se ha tratado como un derecho autónomo y expresión o elemento de otros derechos tales como el derecho a ser inscrito en registro, el derecho a un nombre, el derecho a la nacionalidad y el derecho a la

[109] *K.U. c. Finlandia*, Apel. núm. 2872/02 (2 de diciembre de 2008). En este caso el Tribunal declaró por unanimidad que se había producido una violación del artículo 8 de los derechos prescritos por el CEDH al no actuar las autoridades finlandesas para proteger el derecho de un niño al respeto de su vida privada, a raíz de un anuncio de naturaleza sexual publicado de manera fraudulenta a nombre del niño en un sitio de citas en Internet. En particular se consideró que Finlandia había violado el derecho a la privacidad de los demandantes al no contar con una disposición legal que permitiese a los proveedores de servicios de Internet identificar a la persona que había publicado dicho anuncio en situaciones de este tipo.

personalidad jurídica[110]. Estos derechos están reconocidos en algunas convenciones internacionales de derechos humanos y en otros documentos, entre ellos:

- Declaración Universal de Derechos Humanos, 1948 (Artículo 6: "Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica"; Artículo 15 "Toda persona tiene derecho a una nacionalidad");
- Declaración Americana de los Derechos y Deberes del Hombre, 1948 (Artículo XVII. "Toda persona tiene derecho a que se le reconozca en cualquier parte como sujeto de derechos y obligaciones, y a gozar de los derechos civiles fundamentales"; Artículo XIX: "Toda persona tiene derecho a la nacionalidad que legalmente le corresponda y el de cambiarla, si así lo desea, por la de cualquier otro país que esté dispuesto a otorgársela");
- Pacto Internacional de Derechos Civiles y Políticos, 1966 (Artículo 16: "Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica"; Artículo 24.2: "Todo niño será inscrito inmediatamente después de su nacimiento y deberá tener un nombre". Artículo 24.3: "Todo niño tiene derecho a adquirir una nacionalidad");
- Convención de las Naciones Unidas sobre los Derechos del Niño, 1989 (Artículo 7: "El niño será inscrito inmediatamente después de su nacimiento y tendrá derecho desde que nace a un nombre, a adquirir una nacionalidad y, en la medida de lo posible, a conocer a sus padres y a ser cuidado por ellos"; Artículo 8: "1. Los Estados Partes se comprometen a respetar el derecho del niño a preservar su identidad, incluidos la nacionalidad, el nombre y las relaciones familiares de conformidad con la ley sin injerencias ilícitas. 2. Cuando un niño sea privado ilegalmente de algunos de los elementos de su identidad o de todos ellos, los Estados Partes deberán prestar la asistencia y protección apropiadas con miras a restablecer rápidamente su identidad").

Aplicación del derecho en términos generales

En los últimos años el derecho a la identidad se ha promovido como base para el registro civil universal y la identificación nacional en ciertas regiones, en un esfuerzo por garantizar que todos los ciudadanos puedan disfrutar de los derechos fundamentales[111]. En este contexto, se considera que es fundamento de la obligación del Estado de garantizar la inscripción de todos los ciudadanos y prestarles asistencia para recuperar sus documentos de identidad perdidos a resultas de una guerra civil, desplazamientos, desastres naturales u otras causas.

También se hace mención del derecho a la identidad en el marco de las iniciativas para restablecer la identidad de los niños secuestrados, cuyas identidades fueron alteradas por sus secuestradores (especialmente en el contexto de la desaparición forzada de sus padres).

[110] Consejo Permanente de la Organización de los Estados Americanos, Comisión de Asuntos Jurídicos y Políticos, *Reflexiones preliminares sobre la universalidad del registro civil y el derecho a la identidad*, OEA/Ser.GCP/CAJP-2482/07 (16 de abril de 2007).

[111] Consejo Permanente de la Organización de los Estados Americanos, Comisión de Asuntos Jurídicos y Políticos, proyecto de resolución: Programa interamericano para el registro civil universal y el "derecho a la identidad", OEA/Ser.G, CP/CAJP-2465/07 rev. 4 (15 de mayo de 2007).

El artículo 20.3 de la Declaración de las Naciones Unidas sobre la protección de todas las personas contra las desapariciones forzadas[112] aborda este tema de la siguiente manera:

> La apropiación de niños de padres víctimas de desaparición forzada o de niños nacidos durante el cautiverio de una madre víctima de una desaparición forzada, así como la falsificación o supresión de documentos que atestigüen su verdadera identidad, constituyen delitos de naturaleza sumamente grave que deberán ser castigados como tales.

Como se ha indicado anteriormente, el artículo 8 de la Convención de las Naciones Unidas sobre los Derechos del Niño aborda el tema del restablecimiento de la identidad en el contexto de la privación ilegal de la identidad de un niño, estipulando que:

> 2. Cuando un niño sea privado ilegalmente de algunos de los elementos de su identidad o de todos ellos, los Estados Partes deberán prestar la asistencia y protección apropiadas con miras a restablecer rápidamente su identidad.

Aplicación a la delincuencia relacionada con la identidad

El derecho a la identidad no ha tenido mucho impulso (si acaso ha tenido alguno) como base para los programas y medidas para ayudar a las víctimas de delitos, a no ser en los limitados marcos antes mencionados, es decir, ante todo, la generación de información de identidad, y el restablecimiento de la misma en el contexto de: *a)* la pérdida de documentos como consecuencia de desastres naturales, y *b)* la alteración de la identidad de niños por sus secuestradores.

No obstante, cabe sostener que podría aplicarse la misma base jurídica del restablecimiento en el contexto de la información de identidad que ha sido considerablemente alterada a causa de su uso fraudulento, o en el caso de los adultos víctimas de delitos relacionados con la identidad, que han sido privados de la integridad de sus identidades jurídicas o contractuales como resultado de actos de delincuentes, cuando el Estado no ha tomado las medidas adecuadas para protegerlos contra esos fraudes.

Una diferencia importante, sin embargo, es que en las aplicaciones actuales del derecho a la identidad, las "víctimas" individuales o bien carecen de la información de identidad en cuestión (nombre, nacionalidad, inscripción en un registro), o han perdido las pruebas acreditativas de su identidad, o nunca han conocido su verdadera identidad. En cambio, el delito relacionado con la identidad, tal como se analiza en este documento, supone la apropiación y uso indebidos de la información de identidad reconocida de otra persona. La víctima de este tipo de delitos no "pierde" la identidad propiamente dicha, y con frecuencia ni siquiera pierde posesión de la información de identidad pertinente.

[112] Resolución 47/133 de la Asamblea General de las Naciones Unidas, 47° período de sesiones, Supl. núm. 49, art. 20, Documento de las Naciones Unidas A/47/49 (1992).

Derecho a la privacidad

Naturaleza del derecho

La privacidad se reconoce en general como un derecho humano fundamental, aunque no absoluto, en que se sustentan la dignidad y la autonomía humanas, así como otros derechos tales como los de libertad de asociación y de expresión. La privacidad puede desglosarse en conceptos diferentes pero relacionados entre sí, como:

- Privacidad territorial: por ejemplo, el derecho a estar a cubierto de intromisiones en el hogar o en el lugar de trabajo;
- Privacidad de la persona física: por ejemplo, el derecho a estar a cubierto de prácticas invasivas como pruebas genéticas, pruebas de drogas y registro de cavidades corporales;
- Privacidad psicológica: por ejemplo, el derecho a guardar secretos;
- Privacidad de comunicarse: por ejemplo, el derecho a mantener comunicaciones en privado; y
- Privacidad de la información: por ejemplo, el derecho a controlar la reunión, uso y divulgación de información sobre sí mismo.

El derecho a la privacidad está estrechamente vinculado a los derechos de identidad y de reputación. Por ejemplo, la Comisión Europea de Derechos Humanos (creada a la par que el Tribunal Europeo de Derechos Humanos para supervisar la aplicación del Convenio Europeo de Derechos Humanos) declaró en 1976 que:

> Para muchos autores anglosajones y franceses, el derecho de respeto a la "vida privada" es el derecho a la privacidad, el derecho a vivir, en tanto que así se desee, a cubierto de la publicidad [...]. No obstante, en opinión de la Comisión, el derecho al respeto de la vida privada no termina ahí. Comprende también, en cierta medida, el derecho a iniciar y cultivar relaciones con otras personas, especialmente en el ámbito emocional, para el desarrollo y la realización de la propia personalidad[113].

Base jurídica

Los derechos a la privacidad están reconocidos en muchos tratados internacionales y regionales, de derechos humanos, entre ellos la Declaración Universal de Derechos Humanos, cuyo artículo 12 establece:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Los mismos términos figuran en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 14 de la Convención Internacional de las Naciones Unidas sobre

[113] *X c. Islandia*, 5 Comisión Europea de Derechos Humanos 86.87 (1976).

la protección de los derechos de los trabajadores migratorios, y el artículo 16 de la Convención sobre los Derechos del Niño.

El artículo 11 de la Convención Americana sobre Derechos Humanos estipula:

> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
>
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
>
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

El artículo 8 del Convenio Europeo de Derechos Humanos (CEDH) establece:

> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

Este Convenio es vinculante para todos los miembros de la Unión Europea y existe una jurisprudencia amplia y creciente sobre su artículo 8.

La gran mayoría de los países de todo el mundo incluyen en sus constituciones el derecho a alguna forma de privacidad, como la inviolabilidad de la vivienda y el secreto de las comunicaciones. La Carta Canadiense de Derechos y Libertades, por ejemplo, establece el derecho a la vida, la libertad y la seguridad de la persona, así como el derecho a gozar de protección contra los registros y las incautaciones abusivos, lo cual, como se ha determinado, incluye derechos de privacidad[114]. Las constituciones escritas más recientes incluyen derechos específicos de acceso y control de la información personal[115].

Los derechos de privacidad también se recogen en la legislación nacional sobre derechos humanos que carece de jerarquía constitucional, pero exige que las leyes del sistema jurídico en cuestión se interpreten en consonancia con los derechos establecidos en el instrumento pertinente[116].

Aplicabilidad a la delincuencia relacionada con la identidad

En sentido general, la delincuencia relacionada con la identidad conlleva violaciones directas del derecho a la privacidad. Al igual que los derechos en materia de identidad y reputación, los derechos de privacidad componen una base normativa sólida de actuación estatal para asistir a las víctimas de fraudes de identidad. En los ámbitos donde se encuentran más desarrollados (por ejemplo, en la legislación europea y norteamericana), los derechos de privacidad pueden también originar una base jurídica que permita adoptar medidas eficaces de reparación a las víctimas de violaciones de la privacidad como los delitos relacionados con la identidad.

[114] Secciones 7 y 8.
[115] EPIC et al.
[116] Por ejemplo, la *Australian Capital Territory's Human Rights Act 2004* (s.12) y la *Australian state of Victoria's Charter of Human Rights and Responsibilities*.

Debido a la existencia del principio de *Drittwirkung* en Europa, la argumentación, basada en los derechos humanos, que propugna la actuación estatal para asistir a las víctimas de la delincuencia en materia de identidad es más sólida en este continente que en América del Norte. En un caso del CEDH mencionado anteriormente[117], se ordenó a los Países Bajos indemnizar a una víctima de agresión sexual por considerarse que la protección que otorgaban las leyes penales y las civiles contra tal injerencia en derechos fundamentales era insuficiente. El razonamiento en este caso es muy aplicable a muchos delitos relacionados con la identidad, en los cuales también concurren una grave violación de la privacidad; la necesidad de protección y disuasión de tales actos *erga omnes*; el hecho de que la normativa penal no proscribe con claridad el acto en cuestión; la inexistencia de una investigación criminal; la consiguiente dificultad del demandante para aportar pruebas que evidencien el acto ilícito, la culpa, el daño y el vínculo causal entre el acto y el daño; y el hecho de que los procedimientos civiles son largos y suponen problemas de carácter emocional para la víctima.

Derecho a la reputación

Otro derecho humano de importancia para las víctimas de la delincuencia relacionada con la identidad es el derecho a la reputación. El derecho a la protección contra ataques a la propia reputación está estrechamente vinculado con el derecho a la privacidad; de hecho, con frecuencia ambos se conjugan en instrumentos de derechos humanos, incluidos los mencionados anteriormente en la sección sobre el derecho a la privacidad.

Los derechos a la reputación también figuran en muchas constituciones nacionales y a menudo, aunque no siempre, se vinculan con los derechos a la privacidad. Por ejemplo, el artículo 38 de la Constitución china declara que la dignidad personal de los ciudadanos de la República Popular de China (RPC) es inviolable y prohíbe el insulto, el libelo, la acusación o la incriminación falsas contra todo ciudadano por cualquier medio.

Al igual que sucede con los derechos de identidad y privacidad, el reconocimiento a nivel internacional y constitucional del derecho a la reputación ofrece una posible base jurídica para programas y medidas estatales de asistencia a las víctimas de delitos relacionados con la identidad. Por ejemplo, de acuerdo con la doctrina europea de *Drittwirkung*, podría alegarse que el hecho de que un Estado no tipifique como delito el hurto o fraude de identidad, y en consecuencia no actúe penalmente contra los culpables, da origen a la responsabilidad estatal por las pérdidas de la víctima, cuando el derecho de la víctima a la reputación, garantizado constitucionalmente, resulte seriamente dañado.

5. Marco jurídico de la cooperación internacional para la asistencia a las víctimas de delitos

El actual marco de instrumentos internacionales, multilaterales y bilaterales de cooperación en materia penal se centra en facilitar la investigación y persecución de los delitos y,

[117] *X e Y c. los Países Bajos, op cit.*

en general, no aborda los asuntos relacionados con las víctimas. Los tratados de asistencia judicial recíproca, por ejemplo, a menudo no contemplan (si acaso lo hacen alguna vez) la reparación a la víctima. En cambio, tienden a centrarse en las medidas de cooperación para ayudar a los investigadores y fiscales, tales como las facultades para hacer comparecer a los testigos, obligar a la presentación de documentos y otros medios de prueba reales, dictar órdenes de registro y emitir notificaciones judiciales.

Otras convenciones de derecho penal de interés en cuanto a la delincuencia relacionada con la identidad tienen por objeto establecer normas internacionales en materia de derecho penal sustantivo o procesal, y no se pronuncian sobre la cooperación internacional en lo que respecta específicamente al tratamiento y asistencia a las víctimas del delito. Por ejemplo, aunque las Convenciones de Palermo y de Mérida, mencionadas anteriormente, exigen que los Estados parte adopten ciertas medidas para prestar asistencia a las víctimas de la delincuencia organizada y de la corrupción, respectivamente, sus disposiciones sobre cooperación internacional no tienen aplicación explícita para la reparación a las víctimas. Por su parte, el Convenio sobre el delito cibernético del Consejo de Europa persigue el fin específico de "hacer más eficaces las investigaciones y procedimientos penales relativos a las infracciones penales vinculadas a sistemas y datos informáticos, así como permitir la recogida de pruebas electrónicas de una infracción penal". Hace un llamamiento a las Partes para que cooperen entre ellas en las investigaciones y el procesamiento de la "forma más amplia posible", pero no trata las cuestiones relativas a las víctimas[118].

Sin embargo, como se ha indicado anteriormente, existe un proyecto de convención sobre justicia y apoyo a las víctimas de delitos y de abusos de poder. Si se adoptara, podría llenar ese vacío previendo modalidades de cooperación internacional, no solo para la investigación y persecución de los delitos, sino también en lo que respecta a la protección de las víctimas "ya sea en forma de redes directamente relacionadas con el sistema judicial o de vínculos entre organizaciones que proporcionan apoyo a las víctimas"[119].

[118] Consejo de Europa, Convenio sobre el delito cibernético, STCE núm. 185.
[119] Proyecto de convención, disponible en línea en: http://www.tilburguniversity.nl/intervict/undeclaration/convention.pdf.

IV. INVENTARIO DE PRÁCTICAS RELATIVAS A LA REPARACIÓN DE LAS VÍCTIMAS

A continuación se presenta un inventario de las medidas adoptadas por gobiernos y entidades del sector privado para prestar asistencia y reparar el daño ocasionado a cada víctima. Esas medidas van desde las de carácter informativo y educativo hasta las destinadas a dejar establecidos derechos efectivos y soluciones jurídicas ejecutables en favor de las víctimas. Pueden aplicarse de manera voluntaria o ser impuestas por ley, según el tipo de medida y la entidad que las dicte.

En el inventario se hace una distinción entre las prácticas del sector público y las del privado. La mayoría de los ejemplos citados se refieren a América del Norte y, en menor medida, a Europa. Ello es un reflejo de la información en inglés que tuvieron a su alcance los investigadores a partir de fuentes de acceso público. Sin embargo, también parece ser un reflejo de la atención mucho mayor que se presta a los delitos relacionados con la identidad en los Estados Unidos en comparación con otros países y, posiblemente, de la mayor incidencia que tienen esos delitos en ese país cuando se lo compara con otros[120]. Es preciso estudiar más a fondo la cuestión para determinar los tipos y la incidencia de los delitos relacionados con la identidad y las prácticas pertinentes en materia de reparación de las víctimas, especialmente en Asia, África y América del Sur.

Muchas de las prácticas que se enumeran solo tienen sentido en países con sistemas económicos y estructuras institucionales similares a los de los Estados Unidos u otros países occidentales (por ejemplo, las prácticas de las agencias de verificación de antecedentes crediticios y las agencias de cobro de deudas son pertinentes solo en los lugares en que existen esos tipos de organizaciones). Otras asumen un nivel de recursos institucionales o de madurez que podría no darse en todos los países. Por ese motivo, el inventario no debe considerarse como un conjunto de recomendaciones aplicables a todos los Estados, sino más bien como una selección de medidas de interés adoptadas por determinados Estados (y entidades privadas en varios otros) que han reconocido la necesidad de combatir los delitos relacionados con la identidad. Las medidas que cada Estado decida adoptar deberían reflejar su estructura institucional y económica, así como su experiencia en lo que se refiere a los delitos relacionados con la identidad.

[120] *Nicole van der Meulen*, "The Spread of Identity theft: Developments and Initiatives within the European Union", *The Police Chief*, vol. 74, núm. 5 (mayo de 2007).

1. Prácticas en el sector público

Los gobiernos tienen distintas maneras de prestar asistencia a las víctimas de los delitos relacionados con la identidad, ya sea directamente por conducto de organismos estatales, o indirectamente mediante la regulación de las entidades del sector privado. Es poco probable que muchas de las prácticas que se mencionan en la sección titulada "Prácticas en el sector privado" existan sin que intervenga el Estado promulgando leyes o códigos de prácticas ejecutables. Ahora bien, la distinción entre las prácticas se ha establecido en función de las entidades que las aplican, sean obligatorias o no. Por lo tanto, la siguiente lista de prácticas del sector público se centra en las medidas que los organismos estatales pueden adoptar para prestar asistencia a las víctimas de delitos en materia de identidad. La lista se divide en cuatro categorías: fomento de la capacidad institucional para enfrentar dichos delitos, previsión de medidas de reparación a las víctimas, facilitación de las iniciativas de autoayuda de las víctimas y prevención de una nueva victimización.

Fomento de la capacidad institucional de asistencia a las víctimas

Las autoridades públicas necesitan fomentar su propia capacidad interna para enfrentar de manera eficaz los delitos relacionados con la identidad y las consecuencias de los mismos para las víctimas. Ello incluye el desarrollo de capacidad no solo para prevenir y detectar esos delitos, sino también para mitigar sus efectos en las víctimas. Afortunadamente, muchas prácticas de fomento de la capacidad sirven para ambos fines. Por eso, buen número de las que se enumeran a continuación son aplicables tanto para prevenir o detectar como para ofrecer reparación a la víctima. Las autoridades también pueden ayudar al sector privado a aumentar su capacidad de asistencia a los afectados por fraudes de identidad. La lista que sigue incluye medidas estatales centradas en el fomento de la capacidad de los sectores público y privado.

Determinación y coordinación de los organismos estatales que se ocupan de las víctimas de los delitos relacionados con la identidad

Dado que el fraude de identidad repercute en diferentes ramas del poder público (dependencias expedidoras de documentos oficiales, entidades proveedoras de servicios y prestaciones, organismos de represión de la delincuencia, entre otros), una respuesta efectiva de las autoridades al problema exige la coordinación entre los distintos actores implicados. Esto es válido tanto a efectos de reparación a las víctimas como a efectos de prevención. Se deben dar a las víctimas posibilidades de rectificar los registros falseados y obtener los documentos nuevos que necesiten sin necesidad de esforzarse demasiado.

El primer paso es determinar los organismos estatales que desempeñan una función en lo tocante al delito relacionado con la identidad y entender esa función. De este modo se pueden elaborar prácticas óptimas para cada organismo. Pero la coordinación entre ellos es fundamental si se quiere brindar un buen servicio a las víctimas.

Entre las mejores prácticas en este ámbito cabe citar el enfoque adoptado en los Estados Unidos, en virtud del cual el Congreso nombró a la Comisión Federal de Comercio (CFC) como organismo principal en materia de fraudes de identidad, y en 2006 el Presidente

nombró un grupo de trabajo de alto nivel encargado de elaborar un enfoque coordinado entre los organismos nacionales para combatir ese delito[121]. De conformidad con su mandato, en abril de 2007, el grupo de trabajo presentó un plan estratégico que incluía numerosas recomendaciones para reducir la incidencia y las consecuencias de los delitos en materia de identidad, y en octubre de 2008, presentó un informe sobre la aplicación de esas recomendaciones, muchas de las cuales tratan de medidas de reparación a las víctimas.

Son ejemplos de coordinación de actividades concretas del sector público los siguientes:

- El establecimiento de un grupo de trabajo compuesto por fiscales, investigadores y analistas de organismos tales como la División Penal del Departamento de Justicia de los Estados Unidos, bufetes de abogados estadounidenses, el FBI, el Departamento del Tesoro, la CFC, el Servicio de Seguridad Diplomática, el Servicio Secreto de los Estados Unidos y el Servicio de Inspección Postal de los Estados Unidos, los cuales se reúnen mensualmente para examinar las tendencias nacientes en la esfera del delito relacionado con la identidad, intercambiar mejores prácticas y recibir informes de representantes de entidades gubernamentales y del sector privado que se ocupan de combatir dicho delito;

- La participación de la Oficina para las víctimas de la criminalidad, del Departamento de Justicia de los Estados Unidos, en grupos de trabajo federales que intercambian información y fomentan la colaboración para abordar temas afines al delito relacionado con la identidad;

- El Centro de intercambio de datos sobre el hurto de identidad de los Estados Unidos: base de datos nacional establecida por la CFC que contiene más de 1,6 millones de denuncias presentadas por víctimas del fraude de identidad. Más de 1.650 autoridades federales, estatales y locales de los servicios de represión y otras conjunciones regulatorias tienen acceso a ese Centro de intercambio para llevar a cabo investigaciones, obtener información sobre las víctimas de dicho fraude y conocer qué otros organismos intervienen en una investigación;

- La Red Nacional de los Estados Unidos para la represión de los delitos relacionados con la identidad (NICLE), que permite la actuación autorizada de los servicios represivos a nivel federal, estatal y local para introducir y recuperar datos sobre esos delitos a través de la Red de sistemas regionales de intercambio de información, un sistema centralizado para el uso compartido de datos. La Red NICLE está diseñada para dar cabida a los datos de la CFC, los organismos de represión de la delincuencia y los sectores bancario y de comercio minorista.

- El sistema "RECOL" (información en línea) sobre la delincuencia económica, la acción concertada de los organismos de represión del delito canadienses y el Internet Fraud Complaint Centre (Centro de denuncias de fraudes cometidos a través de Internet) que, entre otras cosas, orienta a las víctimas hacia las autoridades adecuadas para la correspondiente investigación[122].

[121] Véase el sitio web del Grupo de trabajo presidencial sobre el hurto de identidad, disponible en línea en: http://www.idtheft.gov.

[122] Véase: http://www.recol.ca.

Coordinación con el sector privado en cuestiones que afectan a las víctimas del delito relacionado con la identidad

Con frecuencia las víctimas ven frustrados sus intentos de restablecer su situación debido a la falta de coordinación e intercambio de información entre las entidades de los sectores privado y público. A este respecto, son ejemplos de prácticas e iniciativas útiles los siguientes:

- El Identity Fraud Steering Committee (Comité directivo sobre el fraude de identidad) del Reino Unido, iniciativa de colaboración entre el sector público y el privado, promovida por el Ministerio del Interior británico para coordinar las actividades relativas al fraude de identidad que estén en curso en ambos sectores y concretar nuevos proyectos e iniciativas con miras a reprimir ese delito[123];

- Los arreglos de la CFC y entidades privadas para compartir la información sobre denuncias proveniente del Centro de intercambio de datos sobre el hurto de identidad (antes mencionado) a fin de resolver problemas relacionados con el fraude de identidad;

- Diversas iniciativas encaminadas a garantizar que las víctimas de tal fraude puedan obtener copias de los documentos relativos al mismo facilitadas por las empresas con las que el delincuente tuvo tratos; tales iniciativas incluyen celebrar reuniones entre organismos gubernamentales y el sector de servicios financieros, distribuir material didáctico y crear una dirección de correo electrónico para presentar denuncias y obtener asistencia respecto a este problema concreto;

- La iniciativa "Identity Shield", acción de carácter público-privado en que participan la Unidad del FBI para la fusión de iniciativas y recursos cibernéticos (CIRFU, por sus siglas en inglés), la Alianza nacional de análisis cibernético-forense y capacitación, el Servicio de Inspección Postal de los Estados Unidos y el sector privado. En el marco de este proyecto, CIRFU recopila los datos personales que los autores de hurtos de identidad han dejado en Internet y los notifica a las principales agencias de información al consumidor, así como a las instituciones financieras afectadas. La unidad CIRFU y el Centro de denuncias de fraudes cometidos a través de Internet (IC3) también colaboran en la denuncia de delitos a los organismos de represión pertinentes;

- El establecimiento en todas las partes de los Estados Unidos de equipos de tareas que prestan asistencia en la lucha contra la delincuencia relativa a la identidad. En estos equipos colaboran aproximadamente 2.000 miembros de entidades estatales, locales, el sector privado y el mundo académico;

- La campaña de la CFC titulada "AvoID Theft" (evitar el hurto de identidad), por la que se invita a las empresas a que colaboren con la CFC para educar al público en lo que atañe a los delitos relacionados con la identidad[124].

[123] Véase: http://www.identity-theft.org.uk/committee.asp.
[124] Véase: http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html.

Participación en marcos relevantes de cooperación a nivel internacional, bilateral y regional

Hoy día existe una serie de redes y organizaciones internacionales, bilaterales y regionales que centran su actividad en el establecimiento de normas e iniciativas de cooperación para luchar contra el fraude transfronterizo, el delito y los problemas conexos[125]. Debido a las graves consecuencias que acarrea para las víctimas y las economías en general, se reconoce cada vez más la necesidad de abordar la delincuencia relacionada con la identidad como asunto de particular importancia. Mediante el intercambio de información y mejores prácticas de identidad a través de las fronteras, y la colaboración en la lucha contra el fraude los Estados pueden mejorar su capacidad de prestar asistencia a las víctimas de tales delitos, y de prevenirlos. Algunas iniciativas de este tipo son:

- El Grupo básico de expertos de las Naciones Unidas sobre el delito relacionado con la identidad (en colaboración con el cual se preparó el presente documento), organizado por la Oficina de las Naciones Unidas contra la Droga y el Delito de conformidad con la resolución aprobada por la Comisión de Prevención del Delito y Justicia Penal en 2007, relativa a la cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad[126];

- La elaboración de directrices, recomendaciones y manuales para los Estados miembros de la OCDE sobre temas tales como la seguridad de los sistemas y las redes de información, la protección de la privacidad y la circulación transfronteriza de datos personales, el fraude transfronterizo, el comercio electrónico, la solución de controversias con los consumidores y la compensación[127];

- La Red Internacional de Protección del Consumidor y Aplicación de la Ley (RIPCAL), mediante la cual las autoridades de protección del consumidor de 36 países colaboran e intercambian información sobre los fraudes contra el consumidor, por medio de teleconferencias mensuales, informes nacionales y el sitio web econsumer.gov[128];

- El Plan de Acción de Londres, red mundial de los sectores público y privado cuyo objetivo central es la cooperación internacional para luchar contra el correo electrónico basura[129];

- La Red G8 24/7 contra la delincuencia de alta tecnología, que abarca 45 países, facilita el intercambio de información entre los Estados sobre las investigaciones de lucha contra los delincuentes cibernéticos en curso, incluidas las relacionadas con los delitos en materia de identidad[130].

---

[125] Para una lista y descripción más completas de dichas iniciativas, véase: Comité de la OCDE sobre política en relación con el consumidor, Dirección para la Ciencia, la Tecnología y la Industria, *Scoping Paper on Online Identity Theft*, DSTI/CP(2007)3/FINAL (19 de febrero de 2008) ["OECD"], págs. 45 a 55.

[126] E/RES/2007/20 (26 de julio de 2007); véase también E/RES/2004/26 (21 de julio de 2004).

[127] Véase: OCDE, *op cit*, págs. 45 y 46.

[128] Según informaciones de la OCDE, *ibid.*

[129] *Ibid.*; una técnica muy empleada por los defraudadores de identidad para obtener datos personales de las víctimas es la "peska", es decir, el uso de correos electrónicos no solicitados para inducir engañosamente a las personas a proporcionar datos de su cuenta y de otro tipo.

[130] *Ibid.*

Designación de un organismo central encargado de hacer frente a la delincuencia relacionada con la identidad

Sería aconsejable ahorrar a las víctimas la tarea que supone depender de una serie de organismos para obtener información sobre sus derechos, los servicios públicos a los que pueden recurrir y otros asuntos relacionados con el restablecimiento de su situación. Pero también interesa a las autoridades contar con una plataforma central de información sobre los delitos relacionados con la identidad para fomentar su capacidad, así como por motivos de eficiencia y eficacia. Con el tiempo, un organismo central adquirirá experiencia y por lo tanto será más efectivo en su acción frente a esta forma de delito, tan variada y con frecuencia compleja.

En virtud de la Ley de 1998 de los Estados Unidos sobre disuasión del hurto y la suplantación de identidad, en la que se tipificó como delito el "hurto de identidad"[131], se encomendó a la CFC la tarea de crear un servicio central de información, asistencia y derivación de denuncias para las víctimas de la delincuencia en esa materia[132]. En consecuencia, la CFC estableció un servicio que incluye lo siguiente:

- Un centro de intercambio de información sobre las denuncias de delitos relacionados con la identidad;
- Un sitio web que contiene información importante para las víctimas;
- Una línea telefónica especial para aconsejar y orientar a las víctimas, mediante la cual también se recogen datos sobre la incidencia del delito en cuestión;
- Derivación de las denuncias de las víctimas a las entidades competentes; y
- Labores de contacto (en particular con los organismos de represión del delito estatales y locales) y de educación del consumidor, dichos organismos y el sector privado.

La CFC se ha convertido así en la principal fuente de información sobre el delito relacionado con la identidad en los Estados Unidos y en un elemento fundamental de la estrategia nacional para combatirlo. Aunque otros organismos gubernamentales cumplen importantes funciones (por ejemplo la Oficina para las Víctimas de la Criminalidad del Departamento de Justicia y los órganos de represión nacionales y locales), encomendando a la CFC la creación de un servicio centralizado de denuncias y educación del consumidor destinado a las víctimas de fraudes de identidad se ha evitado una duplicación innecesaria de actividades, ofreciendo a la vez mejor servicio a los afectados.

Ampliación de los programas existentes de ayuda a las víctimas de delitos para abarcar los relacionados con la identidad

Muchos Estados cuentan con servicios y programas destinados específicamente a prestar asistencia, dar apoyo y compensar a las víctimas de delitos. Dichos programas tienden a centrarse en las víctimas de actos violentos o de otras infracciones de naturaleza

[131] Definiéndolo de manera amplia que incluye el fraude de identidad y los actos conexos: 18 USC. § 1028.
[132] Pub. L. núm. 105-318 § 5, 112 Stat. 3010 (1998).

totalmente diferente a la de las transgresiones relacionadas con la identidad, y no siempre cuentan con medios satisfactorios para ayudar a las víctimas de esas transgresiones, aún cuando la legislación penal las tipifique como delitos.

Algunas entidades del sector público, cuyo cometido es prestar ayuda a las víctimas de la delincuencia, ofrecen al menos asistencia indirecta a los afectados por fraudes de identidad. Por ejemplo, la Oficina para las Víctimas de la Criminalidad en los Estados Unidos realiza trabajos de sensibilización sobre las consecuencias de esos delitos para quienes los sufren, ha promovido varias iniciativas de ayuda a tales víctimas, y brinda apoyo a los proveedores de servicios, los profesionales afines, las entidades policiales y demás encargados de prestar asistencia[133].

Asimismo, algunas leyes de derechos de las víctimas, como la promulgada en Nueva Zelandia, amparan a los afectados por delitos relacionados con la identidad siempre que hayan sufrido una pérdida financiera directa[134].

Respaldo a las iniciativas y programas del sector privado en apoyo de las víctimas

Con frecuencia el apoyo a las víctimas pueden prestarlo con mayor eficacia organismos no públicos dedicados a esa tarea. En los Estados Unidos, donde el delito relacionado con la identidad parece tener mayor prevalencia, existe una serie de organizaciones de este tipo. En 2007, el Gobierno del país asignó 1,7 millones de dólares, por conducto de su Oficina para las Víctimas de la Criminalidad a las organizaciones nacionales, regionales, estatales y locales de ayuda a las víctimas de delitos, a fin de respaldar los programas de asistencia a las afectadas por fraude de identidad[135].

El Departamento de Justicia de los Estados Unidos colabora actualmente con la American Bar Association (Asociación Americana de Abogados) para establecer un programa de apoyo a los letrados que representan gratuitamente a las víctimas de delitos relacionados con la identidad.

Suministro de material educativo y capacitación para los funcionarios policiales y otros responsables que se ocupen de las víctimas de delitos relacionados con la identidad

Lo primero que suelen hacer las víctimas es acudir a la policía solicitando ayuda y, con frecuencia, reciben respuestas poco útiles. Además, en Norteamérica la obtención de un "informe policial" oficial suele ser crucial para que las víctimas de delitos relacionados con la identidad puedan rehacer su buen nombre. Sin embargo, los organismos policiales muchas veces se niegan a atender tales solicitudes. La Asociación Internacional de Jefes de Policía, junto con el Bank of America, ha publicado información y un manual para uso de los organismos policiales en su trato con las víctimas del delito relacionado con la identidad, disponibles en su sitio web www.idsafety.org.

---

[133] Véase: http://www.ojp.gov/ovc/publications/infores/focuson2005/identitytheft/welcome.html.
[134] *Victims' Rights Act 2002* (N.Z.) 2002/39.
[135] Véase el comunicado de prensa disponible en: http://www.ojp.usdoj.gov/newsroom/pressreleases/2007/OVC08006.htm.

La CFC ha preparado, exclusivamente para servicios policiales, un CD-ROM titulado "*Fighting Identity Theft: A Law Enforcer's Resource*" (La lucha contra el hurto de identidad: material de instrucción para guardianes de la ley) y ha repartido miles de ejemplares por las jefaturas de policía de todo el país. El disco contiene material ilustrativo variado dirigido a los funcionarios policiales y los primeros intervinientes en la asistencia a las víctimas en el proceso de recuperación, por ejemplo cartas modelo a las empresas pidiéndoles que faciliten, sin citación bajo apercibimiento, toda constancia escrita relacionada con el delito en materia de identidad tanto a la víctima como a la agencia investigadora. El CD-ROM también ofrece asesoramiento sobre la coordinación con otros servicios policiales, la sensibilización a nivel comunitario sobre este tipo de delito y la formulación de sugerencias a las empresas locales acerca de la seguridad de los datos. Contiene enlaces con las leyes pertinentes y explica la forma en que los organismos de policía pueden acceder al Centro de intercambio de datos sobre el hurto de identidad de la CFC, el cual contiene más de 1,6 millones de denuncias consultables presentadas por consumidores.

La Oficina para las Víctimas de la Criminalidad, de los Estados Unidos, organiza cursos destinados específicamente a capacitar a funcionarios policiales y personal asesor de las víctimas para la gestión satisfactoria de los casos de delito en materia de identidad[136].

La CFC y otros organismos de los Estados Unidos también ofrecen a los servicios policiales de todo el país seminarios sobre el hurto de identidad de un día de duración. En estos seminarios, que abarcan una amplia gama de temas relacionados con el fraude de identidad, hay una buena parte dedicada a la forma de ayudar a las víctimas a iniciar el proceso de recuperación, y se hace hincapié en la importancia de los informes policiales y de facilitar acceso a las múltiples posibilidades de rectificación de la situación de las víctimas que se ofrecen tanto a la policía como a las propias víctimas[137].

Hay víctimas que recurren a la asistencia de abogados. La CFC y el Departamento de Justicia han elaborado una versión inicial de un manual del procurador sobre el hurto de identidad, en el cual se brinda a los profesionales *pro bono* orientación sobre las cuestiones jurídicas fundamentales, planteadas en el marco de la legislación federal, respecto a las cuales las víctimas podrían necesitar asistencia. En el manual se presentarán herramientas y recursos que faciliten a los procuradores *pro bono* la prestación de ayuda a las víctimas que tengan dificultades para rectificar sus antecedentes de solvencia crediticia o en materia penal[138].

Previsión de medidas de compensación a las víctimas

Previsión de una reparación a las víctimas del fraude de identidad en los casos de fallo condenatorio

Las víctimas de delitos relacionados con la identidad deberían tener derecho a reparación, a cargo de los delincuentes que hayan sido condenados, por sus pérdidas directas e

[136] Véanse, por ejemplo: http://www.sei2003.com/ovcttac2008/SanDiego-Identitytheft.htm y http://www.ovcttac.gov/trainingCenter/workshop_descriptions.cfm#WS5.

[137] Grupo de trabajo presidencial sobre el hurto de identidad, "Combating Identity theft", vol. II, parte O.

[138] Informe del Grupo de trabajo presidencial sobre el hurto de identidad, disponible en línea en: http://www.idtheft.gov/reports/IDTReport2008.pdf, página 26.

indirectas, incluido el valor del tiempo gastado tratando de remediar el daño causado por el delito.

De conformidad con la Ley de 1998 de los Estados Unidos, sobre disuasión del hurto y la suplantación de identidad, las víctimas del fraude de identidad tienen derecho a una reparación que incluye el pago de todo gasto, incluso en concepto de honorarios de abogados, contraído por ellas *a)* en gestiones para rectificar su historial crediticio o calificación crediticia; o *b)* en relación con todo procedimiento civil o administrativo entablado para liquidar cualquier deuda, gravamen u otra obligación de la víctima resultante de las acciones del acusado[139]. Se han propuesto enmiendas similares al Código Penal canadiense que permitan obtener reparación a las víctimas de delitos en materia de identidad[140].

La Ley de los Estados Unidos sobre disuasión del hurto y la suplantación de identidad, promulgada recientemente, prevé una reparación adicional que cubra "el valor del tiempo gastado razonablemente por la víctima tratando de remediar el daño, planeado o real, que sufra a consecuencia del delito"[141]. Esta disposición es importante dado el tiempo que las víctimas de delitos relacionados con la identidad tienen que gastar, por lo general, para rectificar sus datos de identidad y rehacer su reputación.

Aplicar enfoques de justicia restaurativa cuando proceda

Los procesos de "justicia restaurativa" pueden resultar pertinentes en determinados casos de delitos relacionados con la identidad; por ejemplo, cuando el infractor es alguien que conoce a la víctima o vive en su misma comunidad. La justicia restaurativa es un enfoque de la justicia penal centrado en las víctimas que adquiere cada vez más popularidad y que se aplica en algunas jurisdicciones. La justicia restaurativa es una teoría de la justicia que hace hincapié en la reparación del daño ocasionado o puesto de manifiesto por una conducta delictiva[142] y en la que se prevé el diálogo entre el infractor y la víctima; mediante este se espera que el infractor asuma la responsabilidad de sus actos y pida disculpas u ofrezca algún tipo de compensación a la víctima. Por lo tanto, su aplicación sería oportuna o posible en determinados casos de delitos relacionados con la identidad.

Crear derechos de acción legal para las víctimas de los delitos relacionados con la identidad

Debería ser posible para las víctimas recibir indemnización a través de los tribunales civiles, tanto a cargo de los infractores (si son identificados) como de aquellos cuya negligencia contribuyó a los daños. Como se indica en la sección sobre normativa civil del capítulo II, existen algunas causas de acción que serían aplicables en los sistemas de derecho consuetudinario, y varias disposiciones sobre el particular a tenor de los códigos de inspiración romana. Sin embargo, las costas e incertidumbres de los litigios y los problemas que supone establecer la causalidad en los casos de fraude de identidad tienen un enorme efecto disuasivo para tales demandas. Unos derechos de acción legal concebidos para

[139] 18 USC. 3663A c) 1) A).
[140] Proyecto de ley C-27, presentado al Parlamento en su 39ª reunión.
[141] 18 USC. 3663 b).
[142] Véase: http://www.restorativejustice.org.

superar algunos de estos obstáculos podrían facilitar a las víctimas el recurso a los tribunales de lo civil con miras a una reparación.

Los estados de California, Connecticut, Iowa, Louisiana, Nueva Jersey y Pensilvania han promulgado legislación que establece causas de acción específicas para los delitos relacionados con la identidad, algunas de las cuales permiten a las víctimas obtener una indemnización triple por daños y perjuicios y por honorarios de abogados.

Dadas las dificultades, a menudo insuperables, con que tropiezan las víctimas para identificar y llevar a los tribunales a los delincuentes en materia de identidad, es importante que estos derechos de acción también se apliquen a los terceros cuyos actos o negligencia facilitaron el delito. En este sentido, a fines de 2005 se supo que el Gobierno surcoreano tenía pensado implantar legislación que obligara a las instituciones financieras a compensar a sus clientes por las pérdidas resultantes del hurto o fraude de identidad económico, excepto si las víctimas hubieran descuidado la protección de los pormenores de sus tarjetas de crédito, números de identificación personal y contraseñas. Esta iniciativa se tomó a raíz de que el Korea Exchange Bank se negara a compensar a los clientes que habían sufrido pérdidas por una trampa bancaria en línea, alegando que no indemnizaría a las víctimas a menos que pudieran demostrar que el banco tuvo la culpa[143].

Promover la autoayuda de las víctimas

Publicar información ajustada a las necesidades de las víctimas de los delitos relativos a la identidad

Las víctimas de los fraudes de identidad no saben con frecuencia a dónde acudir, y a menudo se sienten abrumadas por las dificultades que supone restablecer su buen nombre y su información de identidad personal. Las autoridades públicas deberían proporcionarles, como mínimo, la información necesaria para encargarse ellas mismas de tal restablecimiento.

Como parte de su Programa Nacional de Prevención del Delito, el Gobierno australiano publicó en 2004 una colección de instrumentos que incluyen una sección sobre el modo de proceder en casos de hurto de identidad, una lista de sitios donde obtener información sobre el fraude de identidad y asistencia, formularios para declarar el hurto o fraude y las pérdidas conexas, y una lista de comprobación rápida con fines preventivos y restaurativos[144].

Abrir un sitio web específico sobre la delincuencia relativa a la identidad con información para las víctimas

Una buena práctica, fácil y evidentemente útil, es abrir un sitio web único de ámbito nacional con información exhaustiva y una relación de recursos para las víctimas de los

[143] Véase: "Korean Banks forced to compensate hacking victims", Finextra.com (diciembre de 2005); disponible en línea en: http://www.finextra.com/fullstory.asp?id=14634.

[144] Véase el enlace de "ID Theft Kit" en: http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity#q3.

delitos referentes a la identidad. En el Reino Unido, organizaciones del sector público y privado se han asociado para crear el sitio web www.identity-theft.org.uk, un depósito central de información sobre tales delitos[145]. Por su parte, Australia también ha creado un sitio web central para informar a las víctimas y otros afectados sobre esos delitos[146]. En los Estados Unidos la Comisión Federal de Comercio (CFC) ha puesto en servicio hace algunos años un sitio similar[147], y el Grupo presidencial de trabajo sobre hurto de identidad ha creado recientemente el sitio www.idtheft.gov. Ambos ofrecen a las víctimas información completa y enlaces para recursos diversos en los Estados Unidos.

La Asociación Internacional de Jefes de Policía y el Bank of America han abierto, en una acción concertada, el sitio web www.idsafety.org, el cual incluye información pormenorizada, una declaración de derechos y una colección de herramientas para las víctimas.

Establecer un centro de apoyo o una línea de atención a las víctimas

Cuando la información proporcionada en línea y la autoayuda resulten insuficientes, las víctimas de los delitos relacionados con la identidad deberían tener acceso a una línea gratuita para recibir asesoramiento, orientación y asistencia sin ningún gasto en el proceso de restablecimiento de su información personal. Esto podría llevarse a cabo recurriendo a organizaciones de apoyo a las víctimas ya existentes o por otros medios.

Como se ha señalado, la CFC ofrece servicios de orientación a las víctimas de esos delitos a través de su línea telefónica especial 1-877-ID-THEFT. Algunos grupos sin ánimo de lucro y organizaciones de víctimas de delitos, tales como VICARS (Iniciativa pro víctimas para orientación, defensa y restablecimiento de datos), bufete sin ánimo de lucro que brinda servicios en la región sudoccidental de los Estados Unidos[148], y centros de recursos para las víctimas de la delincuencia en general, como los existentes en Maryland, (EE. UU.)[149] y los Países Bajos[150], también ofrecen este tipo de servicios.

Publicar una "Declaración de derechos de las víctimas del fraude de identidad"

La primera vez que una persona es víctima de un delito relacionado con la identidad ignora por lo general no solo qué medidas ha de tomar para restablecer su reputación, sino también cuáles son sus derechos reconocidos por la ley. La página web de la CFC presenta una "Declaración de derechos de las víctimas del hurto de identidad", en la cual se resumen las posibilidades que se ofrecen a las víctimas en los Estados Unidos[151]. Ello les facilita un buen compendio de sus opciones, lo que facilita el proceso de restablecimiento.

---

[145] http://www.identity-theft.org.uk/.
[146] http://www.stopidtheft.com.au/.
[147] Véase: http://www.ftc.gov/bcp/edu/microsites/idtheft/.
[148] Véase una descripción más detallada de su misión y servicios en: http://www.idvictim.org/AboutUs.cfm?pagename=AboutUs.
[149] Véase: http://www.mdcrimevictims.org/_pages/id_theft.html.
[150] Véase: http://www.slachtofferhulp.nl/.
[151] Véase una lista completa en: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html.

Elaborar una declaración jurada modelo o un formulario de denuncias para uso de las víctimas en el proceso de restablecimiento

Normalmente, las víctimas de delitos relacionados con la identidad tienen que tratar con muy diversas entidades a fin de enmendar sus datos personales consignados en registros y restablecer su reputación. Con frecuencia, cada organización exige una gran cantidad de documentos. Crear un formulario común para que las víctimas lo utilicen con los diferentes organismos les ahorrará mucho tiempo y esfuerzo en el proceso de restablecimiento.

La CFC, junto con responsables de los servicios policiales y representantes de instituciones financieras, el sector que opera con datos de los consumidores y grupos de defensa del consumidor, han elaborado un formulario universal de denuncia de hurtos de identidad para uso de las víctimas. Este formulario se ha diseñado para su incorporación en los sistemas de informes de los departamentos de policía, facilitando así la preparación y disponibilidad de los informes policiales ("Informes sobre hurto de identidad") que las víctimas necesitan en los Estados Unidos para ejercer muchos de sus derechos, tales como insertar una alerta de fraude por siete años en su expediente de crédito o que se bloquee la información fraudulenta que figure en sus informes de situación crediticia. El formulario se encuentra disponible en línea en: www.idtheft.gov.

Algunos organismos gubernamentales canadienses también han colaborado en la creación de un modelo de declaración de hurto de identidad diseñado como ayuda a las víctimas para notificar el hurto o fraude a las entidades financieras y otras empresas, así como para proporcionar la información necesaria para iniciar una investigación[152]. El objetivo de este modelo no es reemplazar los formularios específicos de cada organismo necesarios en el proceso de restablecimiento.

Proporcionar a las víctimas, previa petición, un informe policial oficial

Uno de los mayores obstáculos para la reparación a las víctimas es la dificultad de obtener un informe policial a fin de que las entidades financieras y demás instituciones tomen las denuncias en serio. En muchos casos, la policía se niega a proporcionar dichos informes, a menos que las entidades financieras lo exijan.

Además de instruir a los servicios policiales sobre la importancia de suministrar dichos informes, los organismos gubernamentales y las organizaciones pro víctimas en los Estados Unidos han facilitado el acceso a tales informes por medio de un modelo de formulario de denuncia de hurto de identidad y un modelo de carta para la policía[153].

Establecer un procedimiento para corregir los datos de registros oficiales

Uno de los aspectos más dificultosos y frustrantes del restablecimiento de la personalidad de las víctimas de los delitos de identidad es la rectificación del contenido de registros oficiales. Las complicaciones burocráticas habituales se ven agravadas irónicamente por el

[152] Véase: http://www.phonebusters.com/images/IDtheftStatement.pdf.
[153] Véase: http://www.ftc.gov/bcp/edu/microsites/idtheft/tools.html.

riesgo de que las solicitudes de documentación básica nueva o corregida, invalidación de antecedentes penales o cambios en otros registros se prestan a un abuso fácil por parte de los ladrones y defraudadores de identidad. Sin embargo, las víctimas necesitan un procedimiento relativamente simple, poco costoso y accesible, a través del cual puedan restablecer su reputación y seguir adelante con su vida.

Varios Estados han establecido un procedimiento formal para eliminar los antecedentes penales generados de manera fraudulenta a resultas del hurto de identidad[154].

Notificar a las personas afectadas los fallos de seguridad que expongan sus datos a posibles fraudes de identidad

Los delincuentes de identidad pueden aprovecharse, y en efecto a veces lo hacen, de los fallos de seguridad que exponen los datos personales a un acceso no autorizado. Si los afectados ignoran este riesgo, es de suponer que no tomarán medidas específicas para prevenir o atenuar el uso fraudulento de la información de identidad en cuestión. Por este motivo, en casi toda Norteamérica se han aprobado leyes sobre notificación de fallos de seguridad que obligan a las entidades a informar a los particulares sobre los fallos que expongan sus datos a posibles delitos relacionados con la identidad[155]. Sin embargo, muchas de estas leyes no se aplican a los organismos del sector público.

Prevenir una nueva victimización

El delito relacionado con la identidad suele ser prolongado en el tiempo, con el resultado de una repetida victimización a lo largo de muchos años. Aun cuando las víctimas cierren las cuentas afectadas y obtengan datos de identidad nuevos, los infractores pueden continuar suplantando con éxito su personalidad y abrir nuevas cuentas, obtener prestaciones en nombre de la víctima o evadir la acción de las autoridades. Por eso las prácticas óptimas de asistencia a las víctimas deben incluir medidas para detectar y prevenir la comisión de más fraudes una vez se descubran.

Establecer un procedimiento que certifique la autenticidad de una víctima

Un servicio sumamente valioso consiste en que el Estado suministre un documento oficial que certifique que la persona es víctima del fraude de identidad cuando este se lleve a cabo para evadir la acción de ley, pues las víctimas corren el riesgo de ser detenidas por delitos cometidos por otros en su nombre. Dichos documentos son de gran utilidad también durante los trámites de restablecimiento de los datos, así como para ayudar a las víctimas en su autenticación ante acreedores y entidades emisoras de documentos.

Por ejemplo, con arreglo al Programa de la Fiscalía General de Ohio de pasaportes para verificación del hurto de identidad, las víctimas pueden solicitar un nuevo pasaporte tras presentar un informe policial. Mediante la utilización de tecnologías biométricas y

[154] Véase: http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-expunge.html, donde figura una lista de todos los Estados en que existe tal disposición, así como un enlace a la ley pertinente.
[155] Véase: http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

similares para crear identificadores digitales, con el pasaporte se ayuda a las víctimas a identificarse y defenderse de cargos criminales fraudulentos, restablecer su historial de crédito e impedir que siga el uso indebido de su información personal. Dicho programa también previene el asiento por duplicado de datos personales de la víctima[156]. Varios estados norteamericanos han puesto en marcha programas análogos[157].

Mantenerse al tanto de los documentos de identidad robados, perdidos y fraudulentos

Manteniéndose informados de los documentos de identidad robados, perdidos o de naturaleza fraudulenta y facilitando esta información a las entidades con fines de autentificación, los Estados pueden facilitar la detección de las tentativas de fraude de identidad y, por lo tanto, proteger a las víctimas contra la continuación del daño.

Los Países Bajos, Bélgica, Alemania y la Interpol manejan bases de datos que llevan cuenta de los documentos de identidad robados, perdidos y fraudulentos con el fin de detectar los fraudes de identidad. La base de datos holandesa es accesible para entidades del sector público y el privado e incluye un registro de defunciones para facilitar la detección de casos de uso fraudulento de identidad de personas fallecidas. Existen cientos de terminales desde los cuales se puede acceder a esta base informática. La base de datos belga permite verificar a través de Internet los números de tarjetas de identidad robadas. Por su parte, la base de datos alemana, cuyo funcionamiento está a cargo de la policía, almacena registros de tarjetas de pago perdidas o robadas y es accesible para los comerciantes. El Servicio de búsqueda automatizada de la base de datos para documentos de viaje robados (ASF-STD) de la Interpol contiene detalles de más de 11 millones de documentos de viaje, y su acceso está restringido a las autoridades policiales. En cambio, tanto el sector público como el privado tienen acceso a la base de datos de la Interpol de tarjetas de pago falsificadas.

Regular o proporcionar información o advertencias públicas sobre los servicios de reparación a las víctimas ofrecidos en el sector privado contra pago de honorarios

En los Estados Unidos se está desarrollando un nuevo sector de servicios a las víctimas de la delincuencia relacionada con la identidad[158]. En algunos casos, las entidades comerciales cometen una nueva victimización pues tratan de aprovecharse del creciente temor de los afectados a esos delitos. Algunos de estos servicios ofrecen precios razonables a ciertas víctimas, pero muchos cobran honorarios considerables por prestaciones que son gratuitas para los ciudadanos o de escasa utilidad para los perjudicados. Se aprovechan de las víctimas que no conocen sus derechos y que con frecuencia buscan ayuda desesperadamente.

La Comisión Federal de Comercio (CFC) ha publicado una hoja informativa para los consumidores sobre dichos servicios titulada “Comprar o no comprar”. Se podría poner

[156] Véase: http://www.ag.state.oh.us/victim/idtheft/index.asp.

[157] Véase: http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-passport.html, donde se ofrece un enlace a los Estados con un programa tipo de pasaportes, así como enlaces a las leyes correspondientes.

[158] Véanse, por ejemplo: www.prepaidlegal.com, www.trustedID.com, www.myidesite.com, www.creditfyi.com, www.idcure.com, www.identitytheft911.com, www.myidfix.com.

más empeño en proteger a las víctimas (y a los consumidores en general) contra la explotación por este floreciente sector.

Efectuar una autenticación minuciosa de los solicitantes de documentos de identidad

Una práctica óptima, elemental en los organismos públicos para prevenir la victimización, es tomar precauciones especiales a la hora de autenticar solicitudes de documentos de identidad, cambios de dirección u otra documentación de identidad[159].

2. Prácticas en el sector privado

Las entidades del sector privado cumplen una importante función en lo que respecta a los delitos relacionados con la identidad. Las agencias de información crediticia (también llamadas "oficinas de crédito"), las entidades financieras, los proveedores de servicios, los minoristas y demás otorgantes de crédito, así como las agencias de cobro, se ven todos afectados en los casos de fraude económico de identidad, y con frecuencia los empleadores, propietarios de viviendas, abogados, servicios públicos y agencias de servicios postales son también engañados por los delincuentes. En algunos casos la entidad en cuestión asume voluntariamente mejores prácticas. La probabilidad de que esto suceda es mayor cuando se ha establecido un código de conducta y se presiona a las empresas para que lo cumplan. Es necesario legislar cuando las fuerzas del mercado no suponen un incentivo suficiente para que las empresas adopten mejores prácticas. Por esta razón, muchas de las que figuran a continuación las impone la ley.

Las siguientes prácticas se ordenan por tipo de entidad: agencias de información crediticia, otorgantes de crédito y emisoras de documentos, agencias de cobro, proveedores de servicios de Internet y todas las entidades con datos personales en su poder.

Agencias de información crediticia

Las entidades que reúnen información crediticia sobre los consumidores y la intercambian con los otorgantes de crédito para evaluar riesgos tienen un papel central en el contexto del fraude económico de identidad, ya que la información que proporcionan sirve de base a esos otorgantes y otros actores para decidir si conceden o no un préstamo u otros servicios a una persona. Además, cuando las víctimas acuden en busca de información y asistencia en caso de delito relacionado con la identidad, con frecuencia se les remite a oficinas de crédito para averiguar las dimensiones del fraude e iniciar el proceso de restablecimiento de su crédito. Existen tres oficinas de crédito que predominan en América del Norte: Equifax, Experian y TransUnion. Las dos primeras también operan en el Reino Unido.

[159] La autenticación minuciosa es una medida general de prevención y por lo tanto se menciona brevemente. Debe llevarse a cabo en lo posible sin recabar o retener datos personales, con el fin de no aumentar la vulnerabilidad al delito relacionado con la identidad.

Proporcionar a las víctimas un apoyo fácilmente accesible y activo

En muchos casos son una gran frustración para las víctimas de fraude económico de identidad las dificultades con que tropiezan a la hora de contactar y obtener información de las oficinas de crédito. A pesar de que estas oficinas suelen ofrecer líneas gratuitas de asistencia, navegar por su sistema telefónico de contestaciones pregrabadas y llegar a contactar con una persona real puede resultar extremadamente difícil y tomar mucho tiempo. Las oficinas de crédito tienen la posibilidad y el deber de dar un servicio mucho mejor a las víctimas. En los Estados Unidos, TransUnion ofrece un número de teléfono especial gratuito a través del cual pueden pedirse bloqueos del crédito, medidas de vigilancia e información sobre el crédito, lo que supone un paso en la dirección correcta[160].

Facilitar a las víctimas un resumen escrito de derechos

Las víctimas suelen permanecer ignorantes de sus derechos hasta que descubren el fraude, y si es un fraude financiero, por lo general se les encamina a las oficinas de crédito para reparar el daño. Por lo tanto, estas oficinas deberían proporcionar a las víctimas de fraude de identidad un resumen de derechos, tanto con carácter general en su sitio web como en respuesta a las consultas de las mismas.

En virtud de una ley sobre información crediticia justa (Fair Credit Reporting Act ("FCRA")), las oficinas de crédito de los Estados Unidos tienen la obligación de presentar a las víctimas de delito relacionado con la identidad una declaración de derechos específica aprobada por la CFC con arreglo a la legislación en esa materia[161]. Esto se suma a la declaración general de derechos de los consumidores que las oficinas de crédito han de proporcionar.

Brindar a todos los consumidores la opción de "bloquear el crédito"

Con frecuencia las víctimas de fraude de identidad económico se ven imposibilitadas de obtener un crédito cuando las agencias de información crediticia suministran a los posibles acreedores información inexacta. Mediante el "bloqueo del crédito" se restringe el acceso a la información crediticia sobre la persona en cuestión, de modo que los acreedores y otros interesados no pueden acceder a ella a menos que la persona levante el bloqueo. Debido a que las empresas suelen verificar tal información antes de conceder un crédito, gracias al bloqueo será improbable que los delincuentes puedan abrir nuevas cuentas a nombre de la víctima.

El bloqueo del crédito es quizá la herramienta más útil con que cuentan las víctimas de fraude de identidad económico (como todos aquellos que simplemente quieren evitar cualquier fraude de identidad). El bloqueo debería ser gratuito, aplicarse durante el tiempo que el consumidor lo desee y levantarse únicamente notificando al consumidor.

En la mayor parte de Norteamérica existen leyes que obligan a las oficinas de crédito a ofrecer servicios de bloqueo a las víctimas de los delitos relacionados con la identidad o a

[160] Véase: http://www.transunion.com/corporate/personal/consumerSupport/contactUs.page.
[161] 15 USC. 1681g) ["FCRA"], s.609 d).

los consumidores en general. En el resto de estados norteamericanos, las oficinas de crédito ofrecen este servicio de manera voluntaria. Su costo y condiciones varían según el lugar, si bien son gratuitos para las víctimas de delitos relacionados con la identidad en casi todos los estados[162].

Si no existe el servicio de bloqueo del crédito, las agencias de información crediticia deberían al menos bloquear la notificación de esa información cuando sea supuestamente fraudulenta. Según la FCRA, las oficinas de crédito de los Estados Unidos deben bloquear inmediatamente la notificación de cualquier información consignada en el expediente de un consumidor que el consumidor identifique como resultado de un supuesto robo o fraude de identidad, previa comprobación de la identidad y la documentación conexa de la víctima[163]. Las oficinas también deben notificar a quienes aporten dicha información sobre la posibilidad de que la misma sea fraudulenta.

Inscribir "alertas de fraude" en los expedientes de crédito a petición de los consumidores

Una "alerta de fraude" es un aviso que se incluye en un expediente de crédito para advertir a potenciales acreedores de que el consumidor podría ser víctima de un fraude. Si bien no protege tanto como el bloqueo del crédito, la alerta de fraude puede servir para evitar que continúe la victimización si los otorgantes de crédito la respetan. Las agencias de información crediticia deberían proporcionar servicios de alerta de fraude gratuitos a las víctimas de los delitos relacionados con la identidad que tengan móviles económicos.

Las tres principales oficinas de crédito de América del Norte ofrecen alertas de fraude sin cargo. En algunos sistemas jurídicos, la ley exige esta práctica, mientras que en otros es voluntaria[164]. De conformidad con la ley estadounidense, la alerta de fraude es, en principio, efectiva durante 90 días, pero puede prorrogarse por siete años, a petición del consumidor, si este presenta a la oficina de crédito un informe de la policía en el que conste que es víctima de delito relacionado con la identidad.

Ofrecer a las víctimas de delitos relacionados con la identidad servicios gratuitos de vigilancia del crédito

Las víctimas de los delitos relacionados con la identidad necesitan tener acceso a sus informes crediticios para poder detectar el uso fraudulento de sus datos personales.

Las oficinas de crédito en los Estados Unidos ofrecen servicios de vigilancia del crédito contra el correspondiente pago, y cobran por acceder en línea a la información crediticia. Estos servicios deberían ser gratuitos para las víctimas de fraudes de identidad. En el Canadá y los Estados Unidos los consumidores tienen derecho a obtener una copia anual

[162] Véase: http://www.consumersunion.org/campaigns/learn_more/003484indiv.html.
[163] FCRA, s.605B.
[164] De conformidad con la FCRA, en los Estados Unidos todos los estados federados están obligados a ofrecer alertas de fraude de forma gratuita. En el Canadá, las alertas se ofrecen de manera voluntaria, excepto en la provincia de Ontario, donde así lo estipula la *Consumer Reporting Act*, R.S.O. 1990, c.C-33, s.12.1.

gratis de su información de crédito[165]. Además, la FCRA da a las víctimas de suplantación de identidad estadounidenses derecho a una segunda copia gratis cuando presentan inicialmente la alerta de fraude, y a dos copias gratis durante el período de 12 meses siguiente a la presentación de una alerta prorrogada (por 7 años)[166].

Coordinar con otras oficinas de crédito las respuestas a las víctimas; prever una sola notificación de alerta de fraude

En muchos países se ocupan de la información crediticia más de una agencia. Como resultado, las víctimas de los delitos económicos relacionados con la identidad deben tratar con varias agencias a fin de rectificar su historial de crédito. No existe ninguna razón que impida a estas agencias coordinar su labor para reducir el esfuerzo que supone a la víctima reparar ese historial.

La FCRA exige que las oficinas de crédito establezcan y mantengan procedimientos para remitirse mutuamente toda denuncia de un consumidor a la agencia declarando un hurto de identidad, o solicitando una alerta de fraude, conforme a la sección 605A o un bloqueo de conformidad con la sección 605B de dicha ley[167]. Con arreglo a la sección 605A, la FCRA exige que la oficina de crédito que reciba una solicitud de alerta de fraude se ponga en contacto con las otras dos, que deben incluirla también en sus expedientes[168]. Esta alerta de fraude conjunta elimina la necesidad de que las víctimas se dirijan a cada una de las agencias por separado. Esta misma práctica puede y debe extenderse a las solicitudes de bloqueo del crédito.

Entidades otorgantes de crédito y emisoras de documentos

Las entidades que otorgan créditos y emiten documentos de identidad desempeñan un papel fundamental respecto al delito de suplantación de la identidad. En primer lugar pueden evitar perjuicios a las víctimas tomando medidas para detectar y prevenir el fraude de identidad (por ejemplo confirmando los cambios de dirección con los titulares de las cuentas y autenticando meticulosamente los datos de todos los solicitantes). En caso de que el fraude de identidad ya se haya producido, pueden ayudar a las víctimas a atenuar los daños de diversas maneras que se indican a continuación.

Notificar a los consumidores si se sospecha una actividad fraudulenta

Las entidades de tarjetas de crédito vigilan la actividad en las cuentas de los titulares para detectar particularidades anormales que podrían provenir del uso fraudulento de la tarjeta. Cuando existe la sospecha de fraude, estas entidades se ponen en contacto con el cliente para determinar si la actividad es fraudulenta. Debería procederse de la misma manera respecto a otras cuentas que, como se sabe, son blanco de los defraudadores de identidad.

---

[165] FCRA, s.612. Véase la legislación provincial sobre información crediticia en el Canadá, por ejemplo la Consumer Reporting Act de Ontario, op cit.
[166] FCRA, s.612.
[167] FCRA, 15 USC. 1681 s), s.612 f).
[168] FCRA, s.605A.

Interrumpir el envío de información inexacta a las oficinas de crédito una vez se haya notificado un supuesto fraude

La FCRA también reconoce a las víctimas de delito relacionado con la identidad el derecho a que los acreedores dejen de suministrar información dimanante de transacciones fraudulentas a las agencias de información sobre los consumidores, una vez la víctima haya presentado un "informe de hurto de identidad" especificando los detalles del caso[169].

Interrumpir el cobro de una deuda si se notifica que fue contraída con ayuda de un fraude de identidad

Los acreedores no deberían poner una deuda en trámite de cobro, o deberían excluirla de tal tramitación si reciben notificación, con documentación de apoyo, como por ejemplo un informe policial, de que la deuda se contrajo de manera fraudulenta utilizando los datos personales del consumidor.

Llevar a cabo una autenticación minuciosa de los datos de todos los solicitantes de crédito

El fraude de identidad podría prevenirse en gran medida y, por consiguiente protegerse a las víctimas contra nuevos fraudes, si las entidades tuviesen más cuidado de autenticar los datos de los solicitantes antes de concederles crédito, servicios u otras prestaciones. Una autenticación exhaustiva es especialmente importante en el caso de las personas que ya han sido objetivo de defraudadores de identidad.

Normalmente la legislación que obliga a las oficinas de crédito a presentar alertas de fraude también exige que los acreedores se pongan en contacto con el consumidor para confirmar la operación, o tomen medidas adicionales para autenticar los datos de un solicitante de crédito antes de concedérselo, cuando exista una alerta de fraude en su expediente[170].

Suministrar información a las víctimas sobre las operaciones en cuestión

En el caso de las víctimas, obtener copias de la solicitud de apertura y las operaciones del impostor es un paso importante para recuperar la sanidad financiera. Con arreglo a la ley sobre información crediticia justa (FCRA), las víctimas de delito relacionado con la identidad en los Estados Unidos tienen el derecho, una vez probada su identidad, de obtener copias de los documentos relacionados con el delito (por ejemplo solicitudes de crédito, registros de operaciones, etc.) de las compañías con las que trató el delincuente, y especificar los organismos de represión del delito a los cuales se enviará en su nombre dicha información[171].

[169] FCRA, s.623 a).
[170] FCRA, s.605A; *Ontario Consumer Reporting Act.* S.12.3.
[171] FCRA, s.609 e).

No responsabilizar a los consumidores de las operaciones fraudulentas ajenas a su voluntad

Las compañías de tarjetas de crédito normalmente ofrecen servicios de responsabilidad limitada o nula para los titulares de tarjetas, siempre y cuando las sospechas de fraude se denuncien con prontitud. De conformidad con la FCRA de los Estados Unidos esto es una obligación[172], si bien en otros sistemas jurídicos es una práctica voluntaria.

Otras formas de pago por vía electrónica, tales como las tarjetas de débito y las operaciones de banca en línea, no suelen implicar esa protección de la responsabilidad del consumidor. Sin embargo, los códigos de conducta voluntarios para la transferencia electrónica de fondos en el Canadá, Australia y el Reino Unido limitan la responsabilidad del consumidor en caso de operaciones fraudulentas, siempre que el mismo haya actuado de manera responsable[173].

Agencias de cobro

En muchos Estados la cobranza de deudas corre a cargo de empresas privadas (agencias de cobro) contratadas por los acreedores. Con frecuencia, las víctimas de delito relacionado con la identidad no se percatan del fraude hasta que reciben una llamada de una agencia de cobro reclamando el pago de una deuda de la cual no tienen el menor conocimiento. Una queja habitual de los afectados es que dichas agencias continúan acosándolos por deudas que no contrajeron. Las agencias de cobro pueden mitigar el daño causado a las víctimas de esos delitos, sin dejar por ello de cumplir sus obligaciones para con los acreedores, de las siguientes maneras:

Notificando a los acreedores el supuesto delito relacionado con la identidad una vez la víctima haya informado del mismo

De conformidad con la FCRA, una vez la víctima haya notificado que la información referente a la deuda puede ser fraudulenta o resultado de un fraude de identidad, los agentes de cobro deben informar a los acreedores en cuyo nombre actúan de que posiblemente así sea[174].

Proporcionando a la víctima información sobre la supuesta deuda

La FCRA también exige que los agentes de cobro a quienes se haya notificado que la deuda se ha generado de manera fraudulenta o a raíz de un hurto de identidad, presenten, a petición del consumidor, información sobre la supuesta deuda[175].

---

[172] 15 USC. 1693g.

[173] Canadian Code of Practice for Consumer Debit Card Transactions (revisado en 2004); Australian Electronic Funds Transfer Code of Conduct; The Banking Code (British Bankers' Association; marzo de 2008), instrumentos cada uno de los cuales ha sido adoptado por las principales instituciones financieras del respectivo Estado.

[174] FCRA, s.615.

[175] *Ibid*.

Deberes de toda entidad con datos personales en su poder

Además de mejores prácticas para la prevención de los delitos relacionados con la identidad, toda entidad que tenga en sus manos datos personales puede y debe adoptar prácticas de ayuda a las víctimas, especialmente en las situaciones en las que la propia entidad tal vez haya contribuido al riesgo de comisión del delito, como las siguientes.

Tener establecida una política que asegure la mitigación a tiempo y eficaz de los fallos de seguridad

Dado el extraordinario crecimiento de las bases de datos informáticas que almacenan datos personales, y el intercambio de dicha información, los ciudadanos corren más peligro que nunca de que tales datos queden expuestos a la acción de los defraudadores de identidad a causa de fallos de seguridad. De hecho, la gestión de fallos de seguridad se ha convertido en un importante problema en los Estados Unidos, donde la incidencia de casos denunciados sigue en aumento[176]. Las entidades deben adoptar políticas claras y detalladas para hacer frente a dichos fallos si ocurren, incluidas medidas para limitar la vulnerabilidad de los datos en riesgo de captación no autorizada y uso fraudulento, y prestar asistencia a las eventuales víctimas para reducir el perjuicio resultante del fraude de identidad facilitado por tales fallos.

Notificar los fallos de seguridad a los afectados

Con frecuencia, las víctimas de los delitos relacionados con la identidad no se enteran de lo ocurrido hasta que sufren un gran daño. Cuando las entidades descubran que por su propia negligencia o descuido ha aumentado la posibilidad de tal delito, sería lógico que informaran a los que pudieran verse afectados por el aumento del riesgo. En los Estados Unidos la mayoría de los estados federados han aprobado leyes sobre notificación de fallos de seguridad, que exigen que las entidades avisen a los clientes de las deficiencias que podrían dejar sus datos expuestos a delitos relacionados con la identidad[177]. En el Japón, las entidades financieras tienen la obligación de informar a las autoridades cuando se producen filtraciones de datos, y el Gabinete de la Presidencia ha formulado una política básica sobre la protección de información, que establece que las entidades afectadas por las infracciones en materia de datos deberían hacerlo público a fin de prevenir daños accesorios[178]. En el Canadá, los Comisionados de Protección de Datos Personales han publicado directrices para las entidades en respuesta a los fallos de seguridad[179], y el Comisionado de Protección de Datos en Australia ha publicado el borrador de una guía de notificación voluntaria de fallos de seguridad[180]. La UE está estudiando enmiendas a la Directiva relativa a la protección de la intimidad en las comunicaciones electrónicas (aplicable a los proveedores de servicios de telecomunicaciones) que incorporarían el requisito de notificación en caso de fallos de seguridad[181].

---

[176] Véase una relación de infracciones en materia de datos personales, en: http://datalossdb.org/ (global) y http://www.privacyrights.org/ar/ChronDataBreaches.htm (Estados Unidos).

[177] Véase: http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

[178] OCDE, op cit, págs. 40 y 41.

[179] Véase: http://www.privcom.gc.ca/information/guide/index_e.asp.

[180] Véase: http://www.privacy.gov.au/publications/breach_0408.html.

[181] *Nicole van der Meulen*, "Year of Preventing Identity Crime: Moving Forward? Identity-related crime in the European Arena", *The Police Chief*, vol. LXXV, núm. 8 (agosto de 2008).

Ofrecer a los empleados y clientes servicios de restablecimiento de la identidad

En los Estados Unidos una amplia gama de empresas privadas ofrece en la actualidad una serie de servicios a las víctimas o posibles víctimas de delitos relacionados con la identidad. Dichos servicios incluyen seguro para casos de hurto o fraude de identidad; servicios de vigilancia, control y reparación del crédito; y servicios generales de restablecimiento de la identidad. Mientras algunos de ellos resultan de poca utilidad para las víctimas, otros suponen una valiosa ayuda que supera la que ya se pone a su disposición de forma gratuita.

Algunos empleadores ofrecen a su personal un seguro contra el hurto o fraude de identidad como parte de su paquete de prestaciones[182]. Otra posibilidad es que los empleadores cubran los gastos de un servicio de restablecimiento de la identidad de los empleados que hayan sido víctimas.

Las organizaciones por cuyos fallos de seguridad hayan quedado expuestos datos personales a posibles delitos relacionados con la identidad suelen ofrecer a los afectados servicios de vigilancia del crédito.

[182] PrePaid Legal Services Inc. y Kroll son dos empresas que ofrecen estos productos a los empleados. Véanse: http://www.prepaidlegal.com/ y http://www.kroll.com/services/fraud_solutions/.

HURTO DE IDENTIDAD: INVENTARIO DE MEJORES PRÁCTICAS DE COLABORACIÓN DE LOS SECTORES PÚBLICO Y PRIVADO PARA PREVENIR EL FRAUDE ECONÓMICO Y LA DELINCUENCIA RELACIONADA CON LA IDENTIDAD*

Cormac Callanan
Director Gerente de Aconite Internet Solutions Limited

* El presente estudio se preparó para su uso como documento de trabajo de la cuarta reunión del grupo básico de expertos sobre el delito relacionado con la identidad, celebrada en Viena, Austria, del 18 al 22 de enero de 2010. También se presentó como documento de sesión a la Comisión de Prevención del Delito y Justicia Penal en su 19º período de sesiones, celebrado en Viena del 17 al 21 de mayo de 2010 (E/CN.15/2010/CRP.4). Las opiniones que se expresan en este documento son las del autor y no reflejan los puntos de vista de las Naciones Unidas.

Índice

I. ANTECEDENTES

1. Hurto de identidad

Estudios recientes[1] en el ámbito del hurto de identidad, realizados por encargo de la UNODC, muestran la necesidad de una colaboración entre los sectores público y privado para combatir esta actividad de los delincuentes cibernéticos.

Como señaló Gercke en la Conferencia sobre fraude y hurto de identidad[2], es muy difícil encontrar una definición de hurto de identidad que sea coherente. En la mayoría de las definiciones se considera que la expresión se refiere al fraude que se comete después utilizando la identidad robada, y se deja de lado el mero robo de identidad cometido previamente. Por ejemplo, el Departamento de Justicia de los Estados Unidos define el hurto de identidad y el fraude de identidad como términos con que se designan todos los tipos de delito en los cuales alguien obtiene y utiliza ilegalmente los datos personales de otra persona, de modo que entraña fraude o engaño, normalmente con el fin de obtener un beneficio económico. En muchos casos, los perjuicios que sufren las víctimas pueden incluir no solo las pérdidas directas, sino también otros costos financieros considerables acarreados por las gestiones para restablecer su reputación en la comunidad y rectificar la información errónea originada por el delincuente[3].

La empresa Javelin Research[4] sostiene que, si bien la expresión "hurto de identidad" tiene un alcance global reflejado ampliamente en su uso por la mayoría de los medios de difusión, las autoridades públicas y los grupos de defensa del consumidor sin ánimo de lucro que tratan este tema, es importante distinguir entre el mero desvelo de la información personal y el uso indebido real de dicha información para obtener un beneficio económico.

Según la mencionada empresa, el hurto de identidad se da cuando alguien accede a información personal ajena sin autorización explícita. Hay fraude de identidad cuando un delincuente usa indebidamente esa información personal, conseguida de manera ilegal, para obtener un beneficio económico, realizando compras o retiros de efectivo fraudulentos, abriendo cuentas falsas o intentando beneficiarse de servicios de empleo o de salud. Los delincuentes pueden utilizar, para lucrarse a costa de las víctimas, datos de identificación personal como el número de seguridad social, el número de cuenta bancaria o tarjeta

[1] *Dr. Marco Gercke,* Legal Approaches to Criminalize Identity Theft for the UNODC (E/CN.15/2009/CRP.13); *Philippa Lawson,* Identity-Related Crime Victim Issues: A Discussion Paper (E/CN.15/2009/CRP.14).

[2] Conferencia sobre fraude y hurto de identidad, Tomar, Portugal, 7 a 9 de noviembre de 2007, Hurto de identidad relacionado con Internet-documento de debate.

[3] Véase: www.justice.gov/criminal/fraud/websites/idtheft.html.

[4] Javelin Research 2009 Identity Fraud Survey Report: Consumer Version. *Prevent- Detect- Resolve*, febrero de 2009, www.javelinstrategy.com/products/CEDDA7/127/delivery.pdf (última consulta: 8 de enero de 2010).

de crédito, contraseñas, el número de tarjeta telefónica, la fecha de nacimiento, el nombre, la dirección, etc.

Como señala Gercke se han establecido diferentes medidas técnicas y jurídicas para prevenir el hurto de identidad. Dichas medidas van desde las restricciones sobre la publicación de información sensible relacionada con la identidad, a las exigencias de notificar las violaciones de datos y a una mejor protección de las grandes bases de datos[5].

Lawson considera en su estudio que es preciso facilitar las iniciativas de autoayuda de las víctimas de delitos relacionados con la identidad, incluso publicando información a la medida de sus necesidades. Con frecuencia, las víctimas no saben adonde dirigirse, y a menudo se sienten abrumadas por los problemas con que se enfrentan para restablecer su reputación y datos de identidad. Como mínimo, las autoridades públicas deberían suministrar a las víctimas la información necesaria para procurarse restablecimiento y reparación por su cuenta[6].

La Conferencia de la Comisión Europea sobre el diálogo del sector público y el privado en la lucha contra las actividades ilegales en línea, reunida en Bruselas el 27 de noviembre de 2009, se organizó con el propósito de establecer una plataforma informal de diálogo donde debatir las distintas cuestiones y temas relacionados con la lucha contra las actividades ilegales en línea entre las partes interesadas del sector público y el privado, así como con los operadores de líneas telefónicas directas de denuncia establecidas por ONG. La creación de esa plataforma de diálogo se basa en las conclusiones del Consejo, de 27 de noviembre de 2008, sobre una estrategia de trabajo concertada y medidas concretas contra el delito cibernético.

El análisis[7] de las estructuras de cooperación sistemática entre los organismos de represión del delito y los proveedores de servicios de Internet muestran que la cooperación se desarrolla en dos direcciones:

- Los organismos de represión son, por un lado, responsables de la prevención e investigación de los delitos, y por el otro, conocen bien las tendencias del delito cibernético;
- El sector de Internet es, por un lado, víctima del delito, y por el otro, buen conocedor de las tendencias del delito cibernético y tiene en sus manos datos sobre los clientes que son los autores o las víctimas de los actos delictivos.

En términos generales, el sector de Internet y los organismos de represión de la delincuencia tienen un interés común, que es prevenir, detectar e investigar los delitos cibernéticos y las amenazas a la seguridad nacional y a la infraestructura global de información. La seguridad y protección en línea y la fiabilidad de Internet dependen de la detección temprana de toda actividad delictiva que pudiera socavar el logro de esos objetivos. Pero ello requiere una legislación que sea eficaz y guarde equilibrio entre los instrumentos de investigación y los derechos fundamentales de los ciudadanos, por ejemplo el derecho a la privacidad en las comunicaciones y el derecho a la protección contra actividades delictivas.

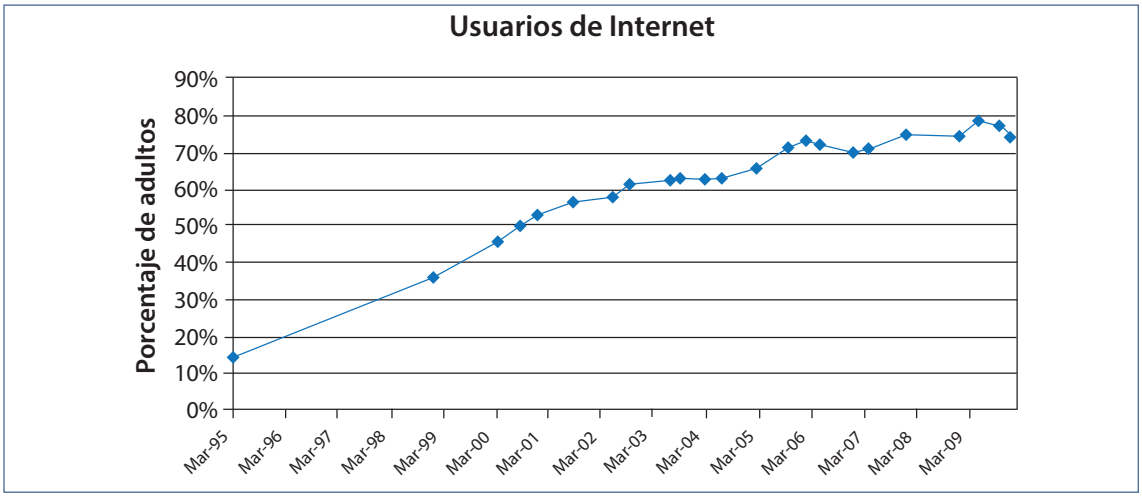
[5] Legal Approaches to Criminalize Identity Theft, *supra*, núm. 1
[6] Identity-Related Crime Victim Issues..., *supra*, núm.1.
[7] Cooperation between service providers and law enforcement against cybercrime - towards common best-of-breed guidelines? Consejo de Europa, marzo de 2008.

2. Panorama de la amenaza

Para elaborar medidas de prevención del fraude, es imprescindible percatarse de la variabilidad existente en el panorama de la amenaza. Es necesario conocer los tipos de fraude que se cometen, dónde viven las víctimas y desde dónde operan los delincuentes.

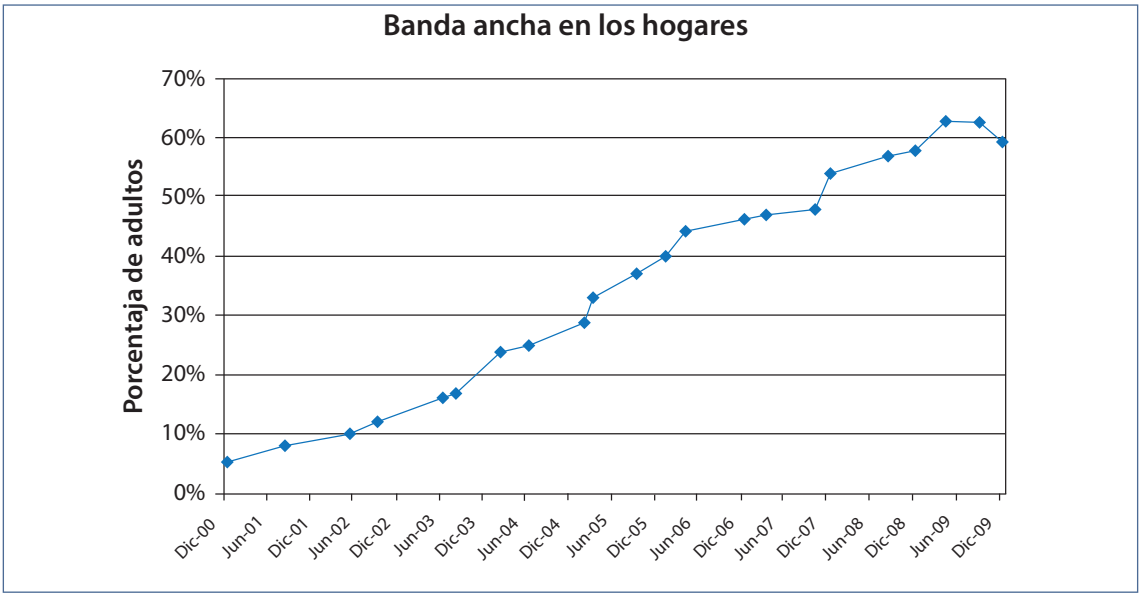
El número de usuarios de Internet continúa creciendo, algo que las investigaciones llevadas a cabo por Pew Internet & American Life Project[8] hacen evidente.

Figura 1. Adultos con servicios en línea en los Estados Unidos



El uso de la banda ancha en los hogares creció de menos del 10% en 2001, a más del 60% en 2009.

Figura 2. Banda ancha en los hogares de los Estados Unidos



[8] Internet User Profiles Reloaded, Updated Demographics for Internet, Broadband and Wireless Users, 5 de enero de 2010, http://pewresearch.org/pubs/1454/demographic-profiles-internet-broadband-cell-phone-wireless-users (última consulta: 8 de enero de 2010).

3. Contexto estadístico[9]

Se han llevado a cabo numerosos estudios sobre la naturaleza del delito de hurto de identidad. En el sitio web Spendonlife.com se ha recopilado una variedad de estadísticas muy útiles e interesantes que hacen patente la amplitud del delito y su grado de crecimiento. El Centro Javelin Research ha destacado algunas de ellas[10].

Víctimas

- En 2008 hubo 10 millones de víctimas del hurto de identidad en los Estados Unidos (Javelin Strategy and Research, 2009).
- Uno de cada 10 consumidores en los Estados Unidos ha sido víctima del hurto de identidad (Javelin Strategy and Research, 2009).
- 1,6 millones de hogares sufrieron un fraude que no estaba relacionado con el uso de tarjetas de crédito (es decir, fueron afectadas sus cuentas bancarias o tarjetas de débito) (Departamento de Justicia de los Estados Unidos, 2005).
- Los hogares con ingresos superiores a 70.000 dólares tuvieron dos veces más probabilidades de sufrir un hurto de identidad que aquellos con ingresos por debajo de los 50.000 dólares (Departamento de Justicia de los Estados Unidos, 2005).
- En el caso del 7% de las víctimas del hurto de identidad, el robo se cometió para usar su identidad con fines médicos.

Descubrimiento del hurto

- Entre el 38% y el 48% de las víctimas descubren al cabo de tres meses que alguien les ha robado su identidad, mientras que entre el 9% y el 18% de ellas no se dan cuenta del hurto hasta que pasan cuatro años o más (Identity Theft Resource Center Aftermath Study, 2004).
- En septiembre de 2008, sumaban ya 50,2 millones los estadounidenses que utilizaban servicios de vigilancia de su situación crediticia (Javelin Strategy and Research, 2009).
- El 44% de los consumidores examinaban los informes sobre su situación crediticia por medio del sitio AnnualCreditReport.com. Uno de cada siete consumidores recibía de un servicio de vigilancia del crédito su informe al respecto. (Javelin Strategy and Research, 2009).

Recuperación de la normalidad

- Reparar los daños que provoca el hurto de identidad puede llevar hasta 5.840 horas (equivalentes a dos años de trabajo a tiempo completo), según la gravedad del caso (Identity Theft Resource Center Aftermath Study, 2004).

[9] www.spendonlife.com/guide/identity-theft-statistics.
[10] www.javelinstrategy.com/.

- Por término medio, la víctima necesita 330 horas para reparar el daño (Identity Theft Resource Center Aftermath Study, 2004).
- Entre el 26% y el 32% de las víctimas necesitan de 4 a 6 meses para solucionar los problemas causados por el hurto de identidad; entre el 11% y el 23% de las víctimas necesitan de 7 meses a 1 año para resolver sus casos (Identity Theft Resource Center Aftermath Study, 2004).
- Los estadounidenses que tenían un seguro contra el hurto de identidad eran 25,9 millones (dato de septiembre de 2008, tomado de Javelin Strategy and Research, 2009).
- Tras el hurto de identidad, el 46% de las víctimas instalaron en sus computadoras programas antivirus o antiespionaje o bien un cortafuegos, el 23% cambiaron de banco o cooperativa de crédito primarios, y el 22% cambiaron de compañía de tarjetas de crédito (Javelin Strategy and Research, 2009).
- Las víctimas del hurto de identidad debía contactar con múltiples organismos para resolver el fraude: el 66% recurrían a instituciones financieras; el 40% se dirigían a agencias de crédito; el 35% buscaban ayuda de los órganos policiales; el 22% entraban en tratos con los cobradores de deudas; el 20% cooperaban con los servicios de asistencia por hurto de identidad; y el 13% contactaban con la Comisión Federal de Comercio (Javelin Strategy and Research, 2009).

Costos

- En 2008 el fraude sobre cuentas existentes en los Estados Unidos ascendió a 31.000 millones de dólares (Javelin Strategy and Research, 2009).
- A nivel mundial, las empresas pierden 221.000 millones de dólares anuales a causa del hurto de identidad (Aberdeen Group).
- En promedio, las víctimas gastan directamente entre 851 y 1.378 dólares intentando solucionar el caso (Identity Theft Resource Center Aftermath Study, 2004).
- El costo medio por víctima es de 500 dólares (Javelin Strategy and Research, 2009).
- El 47% de las víctimas tienen dificultades para conseguir un nuevo préstamo (Identity Theft Resource Center Aftermath Study, 2004).
- El 70% de las víctimas tienen problemas para eliminar de sus informes de situación crediticia la información negativa resultante del hurto de identidad (Identity Theft Resource Center Aftermath Study, 2004).
- En promedio la pérdida por hogar ascendía a 1.620 dólares (Departamento de Justicia de los Estados Unidos, 2005).

Autores del delito

- El 43% de las víctimas conocían al autor (Identity Theft Resource Center Aftermath Study, 2004).

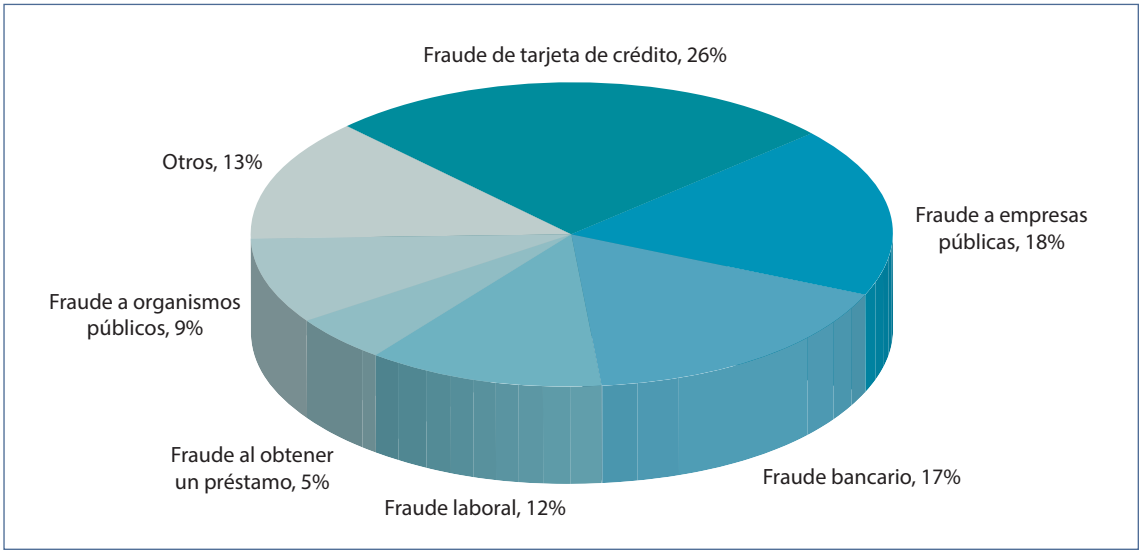
- En los casos de hurto de identidad de niños, lo más frecuente es que el delincuente sea uno de los progenitores (Identity Theft Resource Center Aftermath Study, 2004).

Métodos

- Casi la mitad de todos los hurtos de identidad del robo de carteras o de documentación escrita (43%) (Javelin Strategy and Research, 2009).
- Los métodos en línea representaron solo el 11% (Javelin Strategy and Research, 2009).
- Al 38% de las víctimas de hurtos de identidad se les robó el número de tarjeta de crédito o débito (Javelin Strategy and Research, 2009).
- Al 37% de las víctimas de hurtos de identidad se les robó el número de seguridad social (Javelin Strategy and Research, 2009).
- El 36% de las víctimas de hurtos de identidad vio afectados su nombre y número de teléfono (Javelin Strategy and Research, 2009).
- Para el 24% de las víctimas de hurtos de identidad resultaron afectados sus números de cuentas bancarias (Javelin Strategy and Research, 2009).
- En 2008 más de 35 millones de registros de datos resultaron afectados por vulneraciones de sistemas de información de empresas y entidades públicas (Identity Theft Resource Center Aftermath Study).
- El 59% de los casos de fraude con cuentas nuevas que ocurrieron en 2008 se relacionaron con la apertura de cuentas de tarjetas de crédito y cuentas de tarjetas de crédito emitidas por casas comerciales (Javelin Strategy and Research, 2009).

4. Estadísticas de 2009

Figura 3. Alcance actual del fraude de identidad



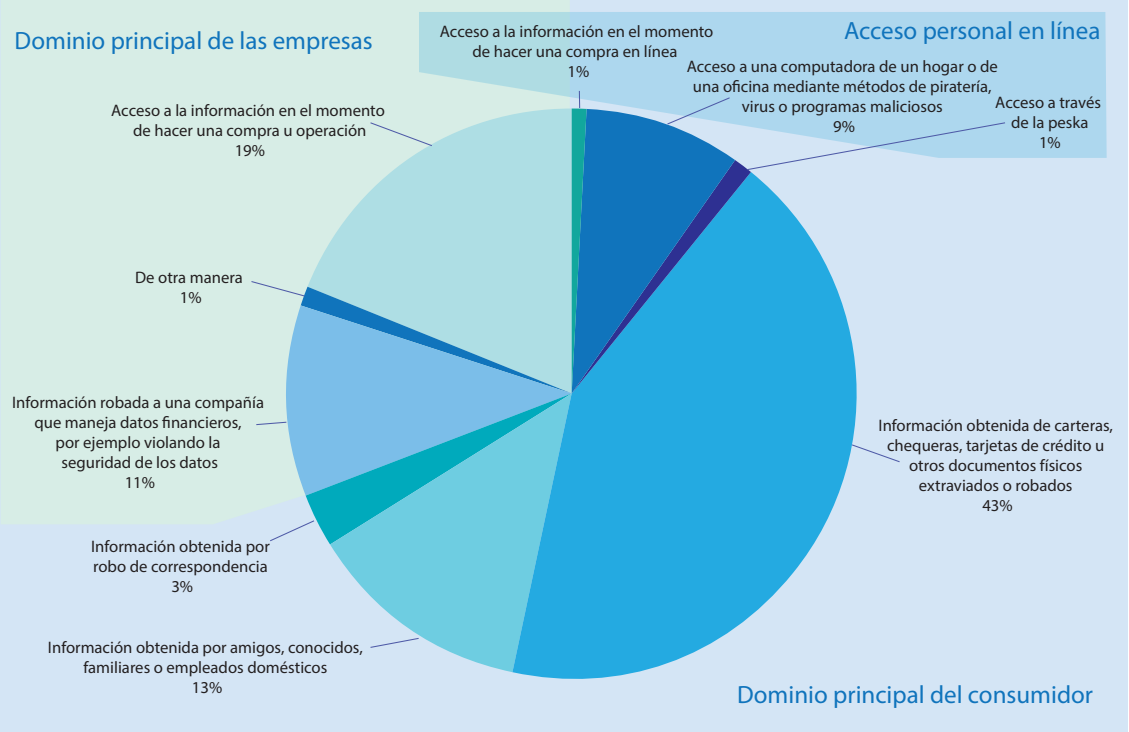
- *Fraude de tarjeta de crédito* (26%)
  El fraude de tarjeta de crédito ocurre cuando alguien obtiene el número de la tarjeta de crédito de otra persona y lo utiliza para hacer una compra.
- *Fraude a empresas públicas* (18%)
  Las cuentas con las empresas de servicios públicos se abren a nombre de un niño o de alguien que no vive en el domicilio. Hay padres en apuros para el suministro de agua, gas y electricidad que se aprovechan del historial crediticio limpio de un hijo para acceder a esos servicios.
- *Fraude bancario* (17%)
  Existen muchas formas de fraude bancario, en particular el robo de un cheque, la modificación de la suma especificada en un cheque y el hurto de la clave de acceso a un cajero automático.
- *Fraude laboral* (12%)
  El fraude laboral ocurre cuando alguien que carece de número de seguridad social válido utiliza el de otra persona para obtener un empleo.
- *Fraude al obtener un préstamo* (5%)
  Este tipo de fraude ocurre cuando alguien solicita un préstamo a nombre de otra persona. Esto puede suceder incluso si el número de seguridad social no se corresponde exactamente con el nombre.
- *Fraude a organismos públicos* (9%)
  Este tipo de fraude incluye el relacionado con asuntos tributarios, de seguridad social y permisos de conducir.
- *Otros* (13%)

5. ¿Cómo se roban los datos de identidad?

Debido al amplio espacio que los medios de comunicación dedican a las estafas en línea, en particular la llamada estafa nigeriana 419, muchos usuarios creen que Internet es la causa de la mayoría de los hurtos y fraudes de identidad cometidos a través de la piratería informática, la peska o un programa malicioso. Sin embargo, en 2008 los casos de fraude en línea representaron solo el 11%[11]. La mayoría de los casos de fraude que se conocen se llevan a cabo por métodos tradicionales, es decir en ocasiones en que el infractor tiene acceso físico directo a la información de la víctima. Entre ellos cabe citar el robo o el extravío de carteras, chequeras o tarjetas de crédito o incluso la escucha a escondidas de una conversación con fines delictivos al realizarse una compra (navegación furtiva).

[11] Javelin Strategy and Research, 2009 Identity Fraud Survey Report: Consumer Version, *Prevent—Detect—Resolve*. Febrero de 2009, página 7. www.javelinstrategy.com/products/CEDDA7/127/delivery.pdf (última consulta: 9 de enero de 2010).

Figura 4. Métodos más comunes de hurto de identidad



En realidad hubo más víctimas del hurto de identidad causadas por amigos, familiares o personal doméstico que se habían apropiado de la información sin permiso. Dado que esas personas conocen los hábitos de compra y las estrategias de supervisión, están mejor informadas para ocultar su rastro por períodos de tiempo más prolongados.

6. Amenazas en línea y globalización

El panorama global de la amenaza está evolucionando, con una presencia de programas maliciosos y otros programas potencialmente no deseados cuyo carácter es cada vez más regional. En distintos lugares están surgiendo esquemas amenazadores muy diversos. Pese a la naturaleza global de Internet, existen diferencias considerables en cuanto a los tipos de amenaza que afectan a los usuarios en diferentes partes del mundo.

Según Microsoft, el ecosistema de la programación maliciosa ha pasado de las amenazas muy visibles, como en el caso de los gusanos autorreproductores, a adoptar formas menos perceptibles que se basan más en la ingeniería social. Este cambio significa que la difusión y efectividad de los programas maliciosos dependen en mayor medida de factores lingüísticos y culturales. Algunas amenazas se extienden por medio de técnicas cuyos destinatarios son las personas que hablan un determinado idioma o utilizan servicios propios de una región geográfica concreta. Otras tienen como objetivo vulnerabilidades o configuraciones y aplicaciones de sistemas operativos extendidos de manera desigual en el mundo. Como resultado, los investigadores en temas de seguridad se enfrentan a un panorama amenazante mucho más complejo que lo que sugeriría un simple análisis de las amenazas principales a nivel mundial.

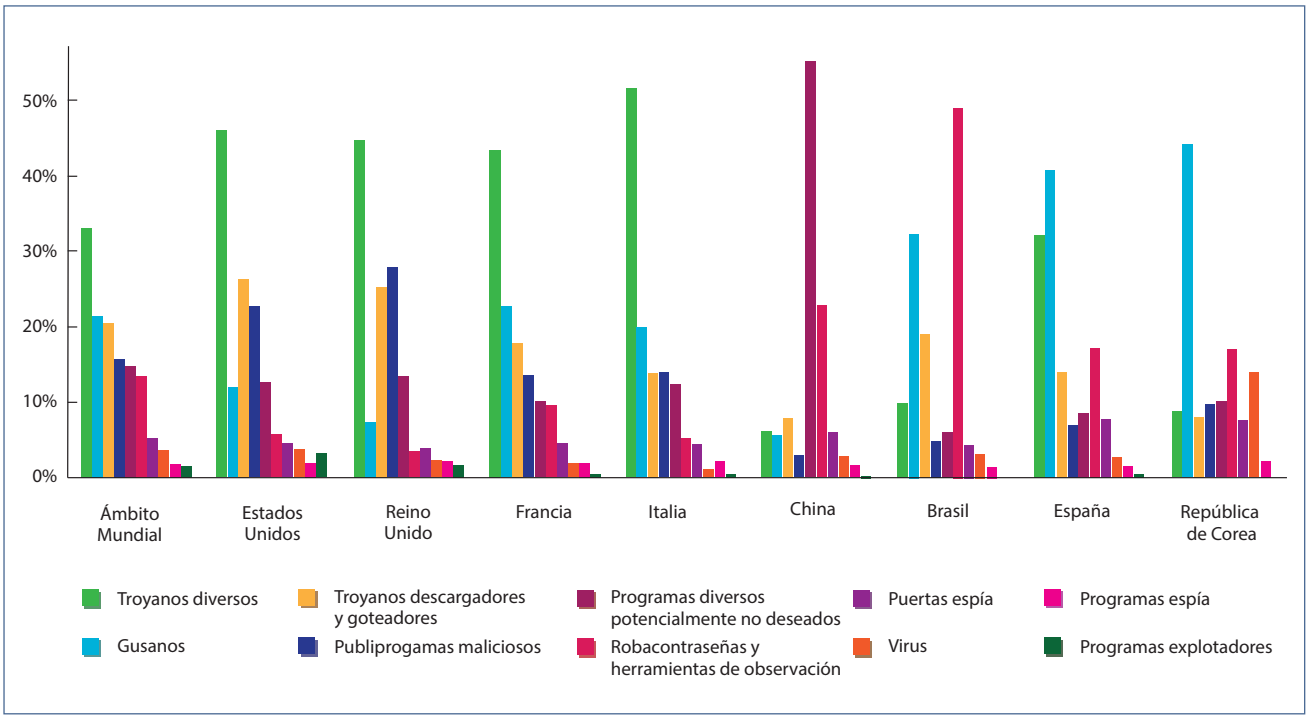
Los 25 lugares donde se desinfectaron los mayores números de computadoras utilizando productos antivirus de Microsoft para equipo de escritorio en el primer semestre de 2009 fueron[12]:

País/región	Computadoras desinfectadas en 1H09	Computadoras desinfectadas en 2H09	Variación
ESTADOS UNIDOS	13.971.056	13.245.712	5,5% ▲
CHINA	2.799.456	3.558.033	-21,3% ▼
BRASIL	2.156.259	1.654.298	30,3% ▲
REINO UNIDO	2.043.431	2.225.016	-8,2% ▼
ESPAÑA	1.853.234	1.544.623	20,0% ▲
FRANCIA	1.703.225	1.815.639	-6,2% ▼
REPÚBLICA DE COREA	1.619.135	1.368.857	18,3% ▲
ITALIA	1.192.867	978.870	21,9% ▲
TURQUÍA	1.161.133	768.939	51,0% ▲
ALEMANIA	1.086.473	1.209.461	-10,2% ▼
MÉXICO	957.697	915.605	4,6% ▲
CANADÁ	942.826	916.263	2,9% ▲
PROVINCIA DE TAIWÁN	781.214	466.929	67,3% ▲
FEDERACIÓN DE RUSIA	581.601	604.598	-3,8% ▼
JAPÓN	553.417	417.269	32,6% ▲
POLONIA	551.419	409.532	34,6% ▲
PAÍSES BAJOS	494.997	641.053	-22,8% ▼
AUSTRALIA	416.435	464.707	-10,4% ▼
PORTUGAL	375.502	337.313	11,3% ▲
BÉLGICA	208.627	267.401	-22,0% ▼
ARABIA SAUDITA	205.157	154.697	32,6% ▲
SUECIA	197.242	287.528	-31,4% ▼
COLOMBIA	183.994	164.986	11,5% ▲
GRECIA	161.639	158.476	2,0% ▲
DINAMARCA	160.001	224.021	-28,6% ▼

Los troyanos representaron la mayor amenaza en los Estados Unidos, el Reino Unido, Francia e Italia; en China predominaron las amenazas basadas en buscadores en determinados idiomas; en Brasil, fueron muy frecuentes los programas maliciosos que tenían como objetivo los servicios de banca en línea; finalmente, en España y la República de Corea, prevalecieron los gusanos, sobresaliendo los que amenazaban a los jugadores en línea.

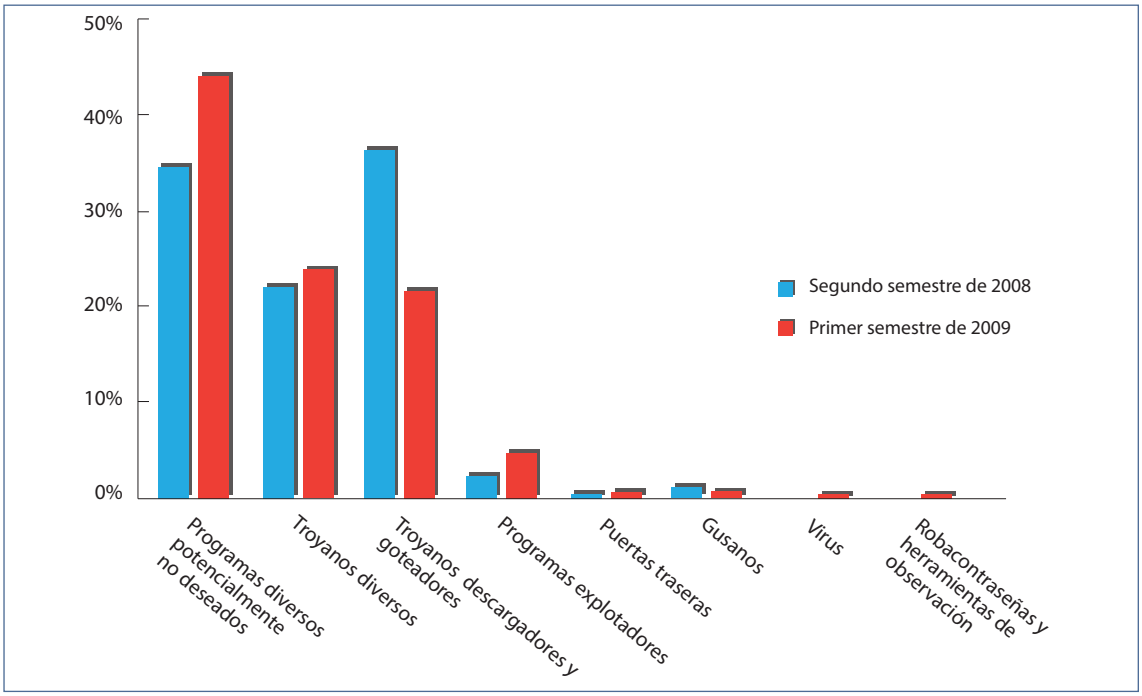
[12] *Microsoft Security Intelligence Report*, volumen 7, enero a junio de 2009, www.microsoft.com/sir (última consulta: 8 de enero de 2010).

Figura 5. Categoría de amenazas a nivel mundial y en los ocho lugares donde se desinfectó el mayor número de computadoras por distribución de frecuencias entre todas las desinfectadas en el primer semestre de 2009



El filtro de Microsoft Smartscreen, que se introdujo en la versión de Internet Explorer 8, ofrece protección contra la peska y los programas maliciosos. En la figura 6 se detallan los esquemas de distribución de programas maliciosos detectados por el filtro Smartscreen en el primer semestre de 2009.

Figura 6. Amenazas presentes en un URL bloqueadas por el filtro Smartscreen, por categorías



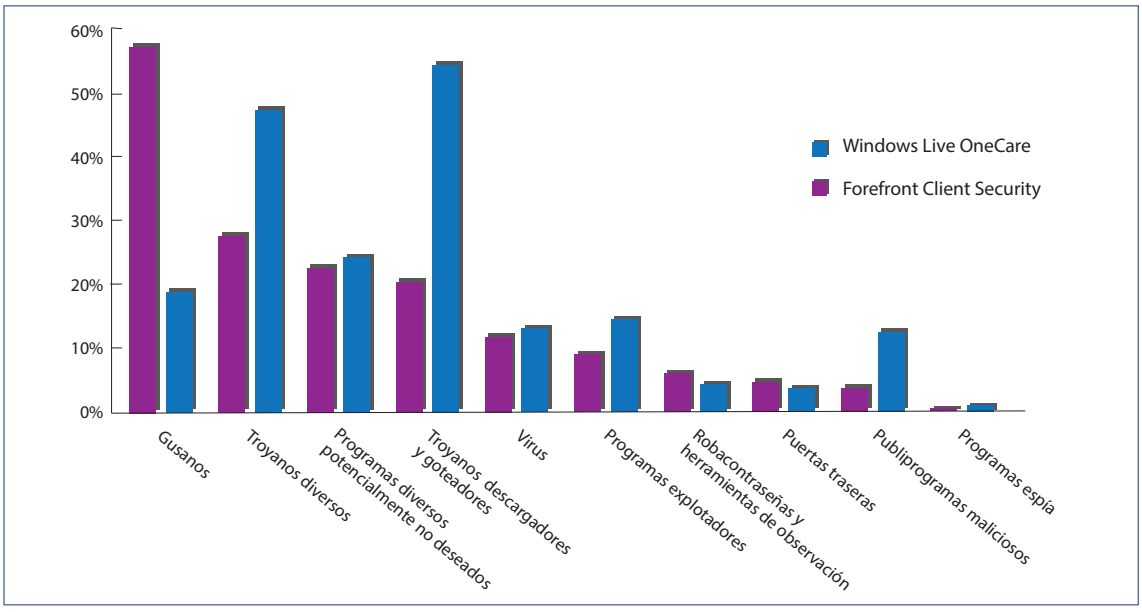
En las computadoras del ámbito empresarial (las que tenían instalado el sistema Microsoft Forefront Client Security)[13] hubo muchas más probabilidades de detectar gusanos durante el primer semestre de 2009 que en las de uso doméstico que funcionaban con el sistema Windows Live OneCare. Mientras que la principal amenaza detectada en el ámbito empresarial fue el gusano Conficker, el mismo no figuró entre las diez amenazas principales descubiertas en las computadoras de uso doméstico (véase la figura 7).

- A diario se detectan más sitios de distribución de programas maliciosos que sitios de peska.
- El hospedaje de programas maliciosos tiende a ser más estable y menos diverso geográficamente.
- Los troyanos diversos (incluidos los programas de seguridad fraudulentos) seguían siendo la categoría más frecuente.
- Los gusanos pasaron de ocupar el quinto lugar en el segundo semestre de 2008 a ser la segunda categoría más frecuente en el primer semestre de 2009.
- La frecuencia de los robacontraseñas y las herramientas de observación también aumentó, debido en parte al incremento de los programas maliciosos cuyo objetivo eran los jugadores en línea.

Las impresiones de peska (número de veces que se visitan sitios de peska) tuvieron un incremento considerable en el primer semestre de 2009, debido principalmente a la gran cantidad de ataques de ese tipo dirigidos contra sitios de redes sociales (véase la figura 8).

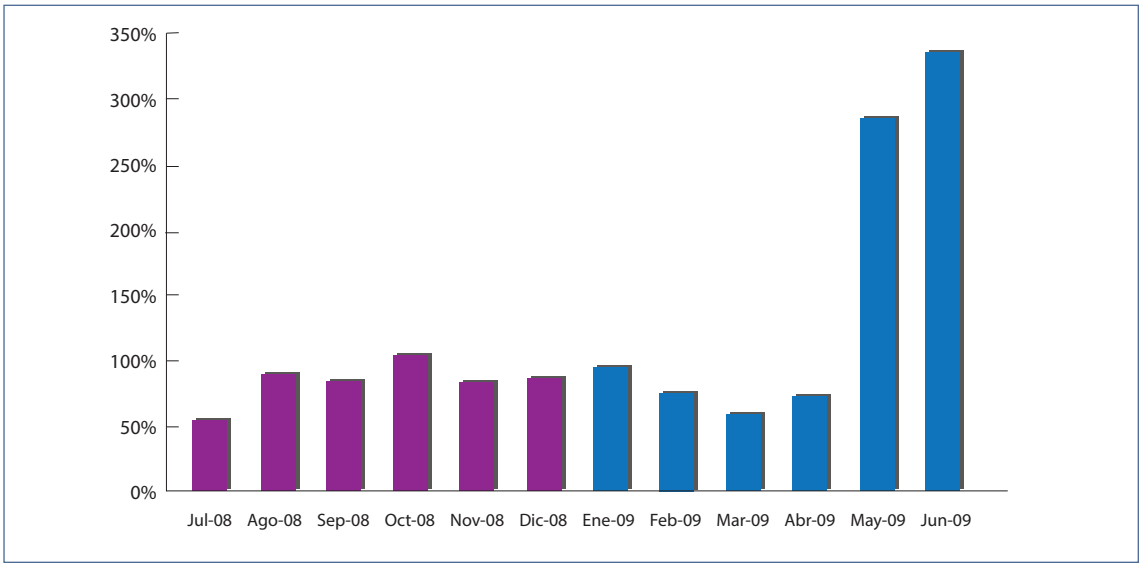
Los "peskadores" continuaron tomando como objetivo una variedad de sitios web más amplia que en el pasado, y algunos de los más atacados en el primer semestre de 2009 fueron los sitios y portales de juegos en línea y los sitios de grandes sociedades.

Figura 7. Categorías de amenaza eliminadas por Windows Live OneCare y Forefront Client Security en el primer semestre de 2009 indicadas como porcentaje de todas las computadoras infectadas que se limpiaron con cada programa



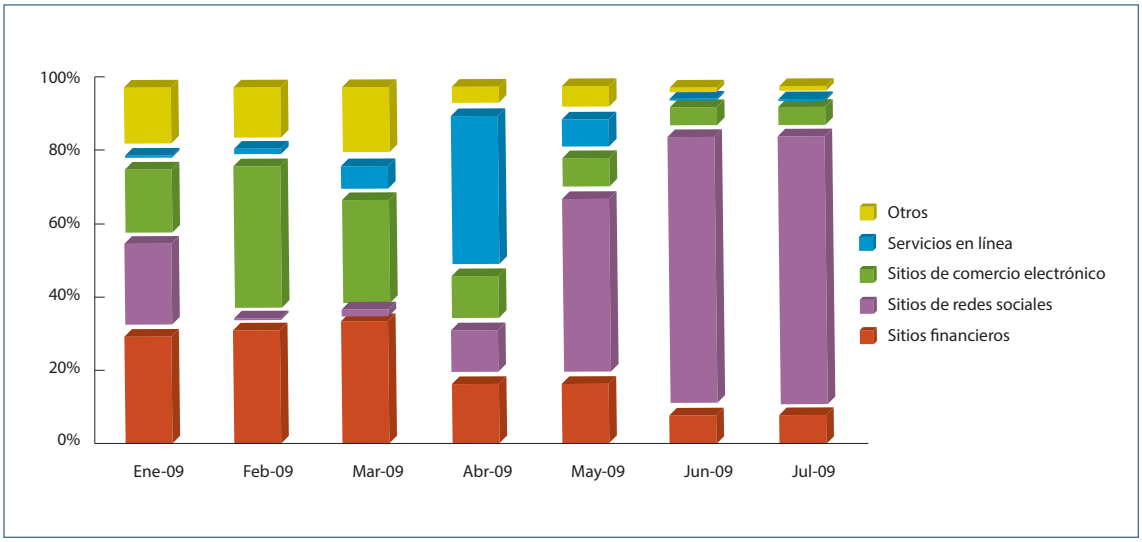
[13] www.microsoft.com/forefront/clientsecurity/en/us/default.aspx (última consulta: 9 de enero de 2010).

Figura 8. Impresiones de peska rastreadas mensualmente en el segundo semestre de 2008 y el primer semestre de 2009, indexadas a enero de 2009



Tras permanecer casi constante durante el segundo semestre de 2008 y hasta abril de 2009, el número de impresiones de peska se cuadruplicó repentinamente en mayo, y continuó creciendo en junio debido en parte a una campaña o campañas cuyo objetivo eran las redes sociales.

Figura 9. Impresiones por cada tipo de sitio de peska y mes en el primer semestre de 2009



Los sitios de instituciones financieras, redes sociales y comercio electrónico siguen siendo el blanco favorito de los intentos de peska. Los investigadores también observaron cierta diversificación hacia otros tipos de entidades, tales como sitios de juegos en línea, portales web y grandes empresas de programas informáticos o telecomunicaciones. A nivel mundial, los sitios de peska reciben hospedaje en sitios gratuitos, servidores de la web inseguros y muchos otros contextos. Llevando a cabo búsquedas geográficas sobre las direcciones IP de los sitios es posible elaborar mapas que muestren la distribución territorial de los mismos y analizar las modalidades.

II. ALCANCE DEL ESTUDIO

1. Finalidad

Elaborar un inventario de las mejores prácticas en materia de colaboración de los sectores público y privado para prevenir el fraude económico y el delito relacionado con la identidad.

2. Antecedentes del estudio

Tomando como punto de partida la publicación en 2007 de un estudio sobre "El fraude y la falsificación de identidad y su uso indebido con fines delictivos", y sobre la base de los mandatos emanados de las resoluciones 2004/26 y 2007/20 del Consejo Económico y Social, la UNODC ha promovido una plataforma consultiva sobre el delito relacionado con la identidad cuyo objetivo es servir a destacados representantes del sector público, dirigentes de empresas, representantes de organizaciones internacionales y regionales y otras partes interesadas como lugar de encuentro para compartir experiencias, elaborar estrategias, facilitar nuevas investigaciones y acordar medidas prácticas contra ese tipo de delito.

En este contexto, se estableció un grupo básico de expertos encargados de intercambiar opiniones sobre la mejor manera de orientar la acción y las iniciativas más apropiadas que es preciso llevar adelante en el marco de la plataforma. El grupo básico se ha reunido hasta ahora en tres oportunidades: en Courmayeur (Italia), el 29 y 30 de noviembre de 2007, y en Viena (Austria), los días 2 y 3 de junio de 2008 y del 20 al 22 de enero de 2009.

En todas las reuniones se reconoció que la cooperación entre los sectores público y privado era fundamental para elaborar un cuadro preciso y completo de los problemas que plantean el fraude económico y el delito relacionado con la identidad, así como para adoptar y aplicar medidas preventivas y reactivas contra los mismos.

Por recomendación de la Comisión de Prevención del Delito y Justicia Penal en su 18º período de sesiones, el Consejo Económico y Social aprobó la resolución 2009/22 de 30 de julio de 2009, en la cual el Consejo pidió a la UNODC que, en consulta con los Estados Miembros y teniendo en cuenta a las organizaciones intergubernamentales pertinentes y, de conformidad con las normas y los procedimientos del Consejo Económico y Social, expertos de instituciones académicas, organizaciones no gubernamentales pertinentes y el sector privado reuniese, elaborase y difundiese, entre otras cosas, "Un conjunto de materiales y prácticas óptimas sobre las asociaciones entre entidades de los sectores público y privado para prevenir el fraude económico y los delitos relacionados con la identidad".

En consonancia con estos principios rectores y disposiciones, la Sección de Lucha contra la Corrupción y los Delitos Económicos de la UNODC emprendió una labor concreta de seguimiento destinada a realizar las recomendaciones del grupo básico de expertos y cumplir el mandato contenido en la resolución 2009/22 del Consejo Económico y Social y, en este contexto, solicita la participación de un consultor para elaborar un inventario de mejores prácticas en la colaboración de los sectores público y privado para prevenir el fraude económico y el delito relacionado con la identidad.

3. Finalidad del estudio y temas concretos objeto del mismo

La finalidad del estudio es recopilar y evaluar material de investigación y datos relevantes y, sobre esa base, elaborar un inventario de mejores prácticas respecto a la colaboración de los sectores público y privado para prevenir el fraude económico y el delito relacionado con la identidad.

En la tarea de reunir el material de investigación y elaborar el inventario, el consultor debía tener en cuenta lo siguiente:

- El informe del grupo intergubernamental de expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos (E/CN.15/2007/8 y Add.1 a 3);
- El informe de la primera reunión del grupo básico de expertos sobre delitos relacionados con la identidad (Courmayeur, Italia, 29 y 30 de noviembre de 2007);
- El informe de la segunda reunión del grupo básico de expertos sobre delitos relacionados con la identidad (Viena, Austria, 2 y 3 de junio de 2008);
- El informe de la tercera reunión del grupo básico de expertos sobre delitos relacionados con la identidad (Viena, Austria, 20 a 22 de enero de 2009);
- Los trabajos en curso en el seno del Grupo de expertos de alto nivel de Lyon del G8 sobre temas relacionados, según proceda;
- Los trabajos del Consejo de Europa sobre el hurto relacionado con Internet, según proceda;
- Los trabajos de la Organización de Cooperación y Desarrollo Económicos (OCDE) sobre el hurto de identidad en línea, según proceda; y
- Otros materiales de interés, si procede.

El consultor elaborará el borrador del inventario bajo la orientación y supervisión de la Sección de Lucha contra la Corrupción y los Delitos Económicos de la UNODC.

El texto final del inventario se utilizará como documento de trabajo en la cuarta reunión del grupo básico de expertos sobre delitos relacionados con la identidad, que se celebrará en Viena (Austria), en enero de 2010.

Los resultados del estudio también se presentarán (como documento de sesión) con fines informativos a la Comisión de Prevención del Delito y Justicia Penal en su 19º período de sesiones, que se celebrará en Viena, del 17 al 21 de mayo de 2010.

III. COLABORACIÓN DE LOS SECTORES PÚBLICO Y PRIVADO

1. Introducción

El delito cibernético, sean cuales fueren las diferentes perspectivas e intereses relacionados con el mismo, representa un enemigo común que solo podrá vencerse mediante mecanismos de asociación y colaboración. Este nuevo enfoque entrañará nuevas estructuras y la intervención activa de todas las partes, aunque corresponderá al sector de Internet una función crucial.

El acelerado desarrollo de Internet en los últimos años es uno de los fenómenos sociales más importantes del siglo, y repercute en los aspectos comerciales, económicos, culturales, sociales y morales de la vida. Ahora bien, en toda evaluación de lo que esto significa, se debe considerar el hecho de que como fenómeno, se encuentra en estado de constante y rápida evolución, y nuestras herramientas tradicionales de medición y análisis no se prestan bien para prever sus efectos o planear las respuestas futuras[14].

Las cuestiones referentes a Internet son de gran amplitud, complejas técnica y jurídicamente, y de dimensiones internacionales. Plantean problemas especiales a la comunidad internacional, los gobiernos, el sector industrial, los educadores, los padres y, de hecho, a los propios usuarios de Internet. Se necesitan nuevas asociaciones, nuevos enfoques y nuevos niveles de flexibilidad para lograr que la explotación de Internet lleve incorporadas medidas de seguridad consabidas específicamente, de modo que aseguren la máxima protección a quienes son vulnerables a sus aspectos negativos.

Debido al carácter fundamental de Internet, existen serios límites respecto a lo que un país puede alcanzar por su cuenta al abordar los temas relativos al delito cibernético. Internet en sí mismo es un fenómeno internacional en todo el sentido de la palabra y toda respuesta eficaz depende de un alto grado de cooperación internacional.

Las respuestas a los desafíos que plantea el delito cibernético tienen que ser lo suficientemente flexibles para reflejar los rápidos cambios en las tecnologías y servicios de Internet. Las medidas que no incluyan posibilidades de revisión y adaptación no son aptas para un entorno caracterizado por esa constante evolución.

Internet opera en un plano internacional. La ley opera en un plano territorial. Por lo tanto, aquí radica el origen de muchas de las cuestiones jurídicas que giran en torno a Internet.

[14] Julio de 1998, "Illegal and harmful use of the Internet", primer informe del Grupo de trabajo Equality and Law Reform del Departamento de Justicia Irlandés, disponible en: http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport_ie.pdf (última consulta: 10 de enero de 2010).

Los materiales contenidos en Internet se destinan a todo el mundo y puede accederse a ellos en todo el mundo. Determinados materiales se almacenan y son accesibles localmente. Otros se hallan fuera del sistema jurídico y solo son accesibles a nivel local. El campo de operatividad de las leyes nacionales puede por lo tanto ser una cuestión compleja que solventar. Las cuestiones de responsabilidad civil a menudo giran en torno a la medida en que una parte determinada ejerce control sobre el contenido ilegal o tiene conocimiento del mismo. Los problemas habituales planteados por el delito cibernético son los de búsqueda y captura transfronterizas, asistencia judicial recíproca, facilidad de movilidad, velocidad de las operaciones, pluralidad de idiomas, pluralidad de culturas y sistemas jurídicos diferentes.

El Sr. Nicola Dileone, miembro del High Technology Crime Centre (Centro contra la delincuencia de alta tecnología) de Europol, relata las dificultades que plantea el delito cibernético internacional y destaca la necesidad de una vigorosa cooperación internacional cuando explica que "un truhán de origen chino con nombre inglés puede tomar como blanco el mercado francés vendiendo un equipo japonés que se puede pagar utilizando un servicio de pago ruso a través de un intermediario letón, a la vez que usa documentación sueca para registrar su dominio en una empresa brasileña, cuya página está hospedada en Tailandia y remite a ella desde Islandia mientras se comunica a través de un servidor de correo electrónico indonesio[15]".

2. Beneficios de la colaboración entre los sectores público y privado

El método principal para abordar los complejos problemas que plantea Internet en la actualidad es el de la colaboración entre los sectores público y privado. Tal colaboración consiste en una alianza o relación estratégica entre dos o más entidades también estratégicas. Las asociaciones fructíferas se basan en la confianza, la igualdad y el entendimiento y las obligaciones mutuas. Pueden ser de carácter formal, caso en que las funciones y obligaciones de cada parte se definen claramente en un acuerdo escrito, o informal, supuesto en que las funciones y obligaciones se asumen o convienen verbalmente.

En la actualidad existe una variedad de alianzas público-privadas en respuesta al delito cibernético, las cuales abarcan el espectro completo de actividades. Existen acciones concertadas entre diversas sociedades que intercambian información relativa a esferas de interés común (por ejemplo, la representada por el Centro FI-ISAC, en el que colaboran entidades financieras), o en las que participa una amplia variedad de interesados (tales como el Plan de Acción de Londres, en el que cooperan organismos policiales, el sector industrial, organizaciones no gubernamentales, etc.). El éxito de estas alianzas público-privadas depende del nivel de participación, las razones de esa participación y el grado de confianza e intercambio en la empresa común.

[15] *Sr. Nicola Dileone*, "European Alert Platform", High Technology Crime Centre, Europol, en el Diálogo entre los sectores público y privado para combatir las actividades ilegales en línea organizado por la Comisión Europea en Bruselas, 27 de noviembre de 2009.

El proyecto de conclusiones del Consejo de la Unión Europea relativas a una estrategia de trabajo concertada y medidas concretas contra la delincuencia informática[16], declara que el principal objetivo es "una asociación más estrecha entre autoridades públicas y sector privado con vistas a una elaboración conjunta de métodos de detección y prevención de los perjuicios causados por las actividades delictivas y de comunicación a los servicios policiales de las informaciones pertinentes relativas a la frecuencia de los delitos por parte de las empresas que sean víctimas de ellos. Se recomienda en particular que la Comisión trabaje en el desarrollo de las líneas directrices adoptadas por la Conferencia sobre cooperación mundial contra la delincuencia informática, reunida bajo los auspicios del Consejo de Europa los días 1 y 2 de abril de 2008, orientadas a mejorar la asociación entre autoridades públicas y sector privado en la lucha contra la delincuencia informática. En este contexto, el Consejo toma nota de las recomendaciones efectuadas tras la reunión de expertos organizada por la Comisión los días 25 y 26 de septiembre de este año, recogidas en anexo".

La primera recomendación que se deriva de las conclusiones del Consejo, recogida en el anexo, es que "debería animarse a las autoridades y al sector privado a encargarse del intercambio de información operativa y estratégica para consolidar su capacidad de descubrir y luchar contra nuevas clases de delincuencia informática. Asimismo debería animarse a las autoridades a informar a los proveedores de servicios sobre las tendencias de la delincuencia informática".

3. Fomento de la sensibilización sobre los principios fundamentales de la cooperación

Un requisito esencial para la cooperación es respetar los principios fundamentales de las partes involucradas:

- Los proveedores de servicios han de mantener un equilibrio constante entre el deber de proteger la información de los clientes, así como cumplir los principios de privacidad establecidos, y el deber de cooperar con los organismos policiales para proteger y promover la seguridad pública.

  En este contexto los proveedores de servicios establecen por lo general programas de cumplimiento de la normativa penal que faciliten ese equilibrio evaluando las exigencias y solicitudes de las autoridades policiales en función de sus obligaciones legales previstas en el sistema jurídico correspondiente.

- El cometido de los organismos policiales es investigar la delincuencia a nivel nacional. Debido a su dimensión internacional y a su naturaleza continuamente cambiante, el delito cibernético exige una estrecha cooperación entre los organismos policiales de los diferentes países, así como el acceso a conocimientos, servicios especializados y registros de conexión en el curso de las investigaciones. El nivel de esos conocimientos y especialización varía en el seno de los organismos y entre los organismos de los diferentes países. La variedad de las leyes procesales penales es también muy pronunciada.

[16] http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf (última consulta: 10 de enero de 2010).

4. Superación de las diferencias nacionales y regionales

Los programas de cumplimiento de la normativa penal varían en gran medida de un proveedor a otro en función de varios factores, entre los que cabe citar, sin carácter limitativo alguno, los tipos de servicios ofrecidos y el lugar donde se almacenan los registros de conexión de los clientes. Hay países, por lo tanto, en que determinados proveedores no ofrecen ningún tipo de apoyo para el cumplimiento de la normativa penal, mientras que en otros países es posible que los mismos proveedores hayan instalado programas de cumplimiento minuciosos.

5. Establecimiento de la base para la cooperación

Así pues, combatir con efectividad el delito cibernético exige un planteamiento bien meditado por las principales partes interesadas. Dada la complejidad y velocidad con que se desarrollan las nuevas tecnologías, manifestadas en los nuevos servicios ofrecidos gratuitamente en línea, son cada vez más insistentes las demandas dirigidas a los proveedores de servicios para que se involucren de un modo más activo, aparte de responder a las peticiones de las autoridades. Los organismos policiales no pueden adquirir por sus medios toda la especialización requerida, y la cooperación con el sector privado no es forzosamente habitual. Pero las autoridades policiales pueden, con ayuda de los proveedores de servicios de Internet, comprender y mantenerse al tanto de las nuevas cuestiones tecnológicas. Es necesario que el sector informático y la policía intercambien experiencias e inquietudes.

Dicha cooperación tiene lugar, a nivel mínimo, cuando un organismo policial recaba información de algún proveedor. Con la experiencia, los proveedores de servicios estarán bien enterados de cuáles son los organismos con derecho a pedir información, y de qué forma. A su vez la policía comprenderá cuál es el mejor momento o modo de obtener la información que busca. La cooperación será óptima cuando los proveedores que denuncian a los defraudadores o infractores para proteger sus servicios comerciales entiendan la necesidad de ir más allá de la simple denuncia de un delito y, con la discreción conveniente, proporcionen, con sujeción a la ley, información confidencial adicional que sirva a los organismos policiales para investigar en mejores condiciones el caso concreto denunciado por el proveedor. Esto también les será útil para investigar más a fondo la delincuencia cibernética en general.

La cooperación contra esos delitos hace necesario establecer un marco que la facilite y permita a las dos partes, y el público en general, comprender mejor su valor.

El 16 de mayo de 2000, en la Conferencia del G8 sobre seguridad y confianza en el ciberespacio, celebrada en el Palacio del Elíseo, el Presidente de la República Francesa, Jacques Chirac, declaró que “los Estados no pueden garantizar la seguridad en Internet a menos que colaboren con (empresas y asociaciones) para establecer las bases de una verdadera co-regulación nacional e internacional”. Y agregó que: “es realmente esencial un diálogo entre los gobiernos y el sector privado. El G8 está convencido de que deberían idearse

soluciones más rápidas o novedosas y de que las autoridades públicas y la industria deben trabajar en sintonía para alcanzarlas"[17].

6. Indicadores fundamentales de una buena colaboración entre los sectores público y privado

- Participación de todos los principales interesados;
- Participación en condiciones de igualdad;
- Confianza, transparencia;
- Reconocimiento de fortalezas y debilidades mutuas;
- Reconocimiento de que los objetivos y funciones principales de cada interesado varían;
- Orientación hacia cuestiones de interés común en lugar de hacia cuestiones conflictivas;
- Comprensión de que no todos los problemas se resolverán a través de estas alianzas;
- Intercambio de conocimientos, información confidencial y experiencias en un ambiente de respeto mutuo.

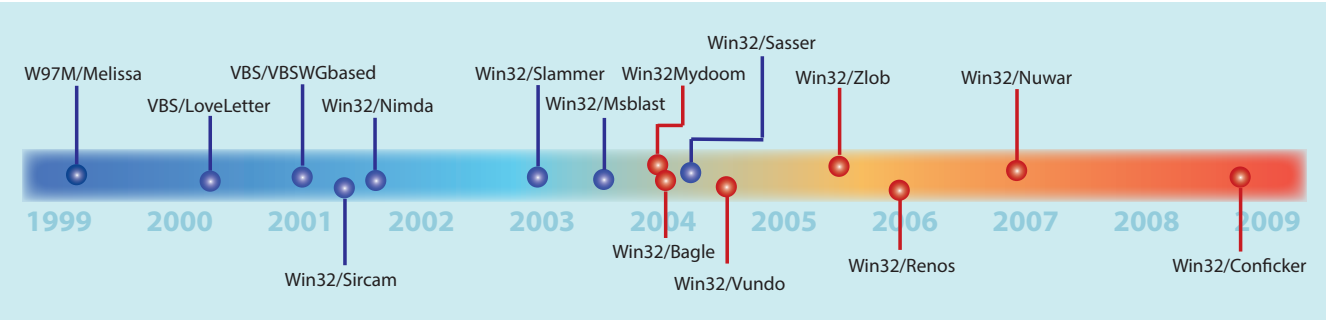
[17] Comunicado de prensa con ocasión de la Conferencia del G8 sobre seguridad y confianza en el ciberespacio, celebrada en París, el miércoles 17 de mayo de 2000, disponible en línea en: www.g7.utoronto.ca/crime/paris2000.htm (última consulta: 10 de enero de 2010).

IV. PREVENCIÓN DEL HURTO DE IDENTIDAD

1. Introducción

La prevención del hurto de información personal no es una tarea costosa, pero exige un cambio de costumbres personales que introduzca en la conducta diaria el hábito de la privacidad de los datos. Rara vez exige gastos en productos de seguridad ni incluso un esfuerzo importante.

Figura 10. Cronología de los programas informáticos maliciosos



La compañía Javelin Strategy and Research[18] especifica seis principios rectores clave para combatir el fraude, que son:

- Estar alerta: vigilar las cuentas financieras con regularidad.
- Preservar la privacidad de los datos personales: reflexionar antes de intercambiar información personal, incluso en los sitios web de las redes sociales.
- Las operaciones en línea son más seguras que las efectuadas fuera de línea siempre que se utilicen los controles de seguridad disponibles.
- Prestar atención al entorno y las personas presentes.
- Asegurarse de que las tarjetas de crédito o débito cuentan con una protección que garantice la exención de responsabilidad frente a la entidad bancaria.
- Enterarse de los servicios de protección de los datos de identidad.

[18] Javelin Strategy and Research, 2009 Identity Fraud Survey Report: Consumer Version, *Prevent—Detect—Resolve*. Febrero de 2009, página 9. www.javelinstrategy.com/products/CEDDA7/127/delivery.pdf (última consulta: 9 de enero de 2010).

Estas sencillas precauciones pueden brindar protección suficiente contra la mayoría de los delitos de hurto de identidad. Por supuesto que no protegen contra ataques a las bases de datos ni a computadores portátiles con información personal perdidas o robadas.

Por ejemplo, las vulnerabilidades de los programas de Microsoft Office que se aprovecharon con más frecuencia en el primer semestre de 2009 fueron también algunas de las más antiguas[19]. Más de la mitad de las vulnerabilidades explotadas fueron detectadas y tratadas ya en las actualizaciones de seguridad cursadas por Microsoft en 2006. El 71,2% de los ataques se efectuaron aprovechando una vulnerabilidad sobre la cual existía una actualización de seguridad (MS06-027) desde hacía tres años. Las computadoras en que se había aplicado esta actualización estuvieron a cubierto de todos esos ataques. La mayoría de los ataques a los programas de Office observados en el primer semestre de 2009 (55,5%) afectaron a las instalaciones de esos programas cuya última actualización databa del período comprendido entre julio de 2003 y junio de 2004. Gran parte de estos ataques afectaron a los usuarios de Office 2003 que no habían aplicado ningún paquete de servicios ni otra actualización de seguridad desde que apareció la versión original de dichos programas en octubre de 2003.

Se sospecha que muchas de estas actualizaciones no se aplicaron porque los programas se habían pirateado antes, lo cual iba a ser detectado y rechazado durante el proceso de actualización. Por supuesto, si los usuarios hubiesen utilizado programas con las licencias adecuadas y aplicado las actualizaciones de seguridad vigentes, habrían tenido éxito muy pocos ataques.

El creciente número de ataques, y la eficacia de los mismos, demuestra el potencial de esta trampa[20]. El número de sitios web exclusivos de peska que se detectaron en junio de 2009[21] ascendió a 49.084, el más alto registrado desde abril de 2007, cuando se denunciaron 55.643 casos al GTAP[22]. Es importante destacar que la estafa no se limita a lograr el acceso a contraseñas para operaciones bancarias en línea. Los infractores han puesto su mira en los códigos de acceso a computadoras y plataformas de subastas, así como a números de la seguridad social.

2. Fomento de la sensibilización

La mayoría de las páginas de descarga no intencionada[23] se hospedan en sitios web legítimos comprometidos. Los infractores acceden a los sitios legítimos por intrusión informática, o a través de códigos maliciosos insertados en formularios en línea escasamente protegidos,

[19] *Microsoft Security Intelligence Report*, vol. 7, enero a junio de 2009, www.microsoft.com/sir (última consulta: 8 de enero de 2010).

[20] En algunos ataques de peska, hasta un 5% de las víctimas suministraron al sitio web información sensible falsa. Véase: *Dhamija/Tygar/Hearst*, Why Phising Works, disponible en: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, página 1, donde se hace referencia a *Loftesness*, Responding to "Phishing" Attacks, Glenbrook Partners (2004).

[21] Phishing Activity Trends Report, primer semestre de 2009, disponible en: www.antiphishing.org/reports/apwg_report_h1_2009.pdf.

[22] Anti-Phishing Working Group. Para más detalles, véase: www.antiphishing.org.

[23] Se trata de un programa que se instala automáticamente en la computadora por el solo el hecho de visitar un sitio web, sin tener que pulsar expresamente en un enlace dentro de la página. Por lo general, son programas espía que proporcionan información al vendedor, y las descargas no intencionadas se activan aprovechando deficiencias en el navegador y en el código del sistema operativo www.yourdictionary.com/computer/drive-by-download (última consulta: 9 de enero de 2010).

por ejemplo en el espacio previsto para comentarios en un blog. Los servidores comprometidos que actúan como explotadores pueden tener un campo de acción gigantesco; un solo servidor explotador puede causar la infección de cientos de miles de páginas web. En 2009 estos servidores originaron miles y miles de páginas infectadas en poco tiempo.

Existe una variedad de estrategias para aumentar la concienciación y sensibilización públicas sobre el tema del hurto de identidad, y brindar apoyo y consejos a las víctimas de dicho delito. Dado el fraude de tarjetas de crédito, hay campañas de concienciación pública e intensificación de los controles de seguridad cuyo fin es inducir a los poseedores de esas tarjetas a cuidar de mantenerlas siempre bajo control.

Algunos ejemplos de los recursos en línea son:

- *Organizaciones no gubernamentales*
  PRC Privacy Rights Clearinghouse (PRC)
  http://www.privacyrights.org/identity-theft-data-breaches
- *Particulares*
  Robert Hartle
  http://www.idtheft.org/
- *Autoridades públicas*
  Departamento de Justicia de los Estados Unidos
  http://www.justice.gov/criminal/fraud/websites/idtheft.html
- *Sector comercial*
  SpendonLife.com http://wwww.spendonlife.com
  Microsoft: http://www.microsoft.com/protect/

3. Informes de seguridad

Los informes de seguridad ofrecen a los consumidores y organizaciones detalles esenciales acerca de la difusión de programas maliciosos, actividades de peska y otras vulnerabilidades informáticas, a fin de aumentar sus posibilidades de combatirlas por medio de las computadoras que estén a su cargo. Estos informes suelen prepararse y distribuirse de forma gratuita, o se presentan en versión más detallada, disponible previo pago.

Son ejemplos de estos informes:

- *AntiPhishing Working Group Phishing Activity Trends Report* (Informe del Grupo de trabajo anti-peska sobre las tendencias de las actividades de peska)

  En este informe se analizan los ataques de peska que denuncian al Grupo las compañías componentes y los investigadores asociados en el plano mundial, a través del sitio web de la organización o por correo electrónico. El Grupo de trabajo también estudia la evolución, proliferación y difusión de los programas delictivos, basándose en las investigaciones de las compañías que lo integran. En la segunda mitad del informe se presentan tablas con estadísticas sobre programas delictivos y otros análisis conexos.

Frecuencia: semestral

Costo: gratuito

- *Javelin Strategy and Research Identity Fraud Survey Report* (Informe de la encuesta sobre fraude de identidad de la empresa Javelin Strategy and Research)

  En el mencionado informe se proporciona a los consumidores orientaciones útiles para prevenir, detectar y resolver fraudes de identidad. En los últimos cinco años Javelin Strategy and Research ha encuestado a cerca de 25.000 personas con el propósito de averiguar las formas en que los consumidores se ven realmente afectados por el fraude de identidad en los Estados Unidos. Los resultados del estudio se utilizan con fines educativos para reducir el riesgo del consumidor de sufrir tal delito. La encuesta telefónica de 2009, que abarcó a casi 4.800 adultos, es el estudio más extenso y actual sobre el fraude de identidad realizado en los Estados Unidos.

  Frecuencia: anual

  Costo: la versión para los consumidores es gratis, el costo de la versión completa se puede consultar en el sitio web.

- *Microsoft Security Intelligence reports* (Informes de inteligencia de seguridad de Microsoft)

  Estos informes ofrecen una visión exhaustiva de los programas informáticos maliciosos y potencialmente no deseados, los programas explotadores, las vulneraciones de la seguridad y la vulnerabilidad de los programas (tanto de Microsoft como de terceros). Los productos de seguridad de Microsoft recogen, con aprobación del usuario, datos de centenares de millones de computadoras de todo el mundo y de algunos de los servicios en línea más activos de Internet. El análisis de estos datos ofrece una perspectiva global y única de las actividades relativas a programas maliciosos y potencialmente no deseados a nivel mundial. Los informes especiales de Microsoft también presentan estrategias, medidas de mitigación y contramedidas.

  Frecuencia: semestral

  Costo: gratuito

- *Symantec Global Internet Security Threat Report*[24] (Informe de Symantec sobre las amenazas mundiales a la seguridad en Internet)

- *Symantec EMEA Internet Security Threat Report*[25] (Informe de Symantec sobre las amenazas en Europa, Oriente Medio y África a la seguridad en Internet)

- *Symantec Government Internet Security Threat Report*[26] (Informe de Symantec sobre las amenazas a nivel nacional a la seguridad en Internet)

[24] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (última consulta: 9 de enero de 2010).

[25] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_emea_internet_security_threat_report_04-2009.en-us.pdf (última consulta: 9 de enero de 2010).

[26] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_government_internet_security_threat_report_04-2009.en-us.pdf (última consulta: 9 de enero de 2010).

Los informes de Symantec sobre las amenazas a la seguridad en Internet en los tres ámbitos indicados proporcionan una vista panorámica y análisis anual de las actividades fraudulentas en línea, un examen de las vulnerabilidades ya conocidas, así como las características destacadas de los códigos maliciosos. También se estudian las tendencias relativas a la peska y el correo basura y se observan las actividades en los servidores de la economía sumergida. A través de su red mundial de inteligencia Symantec™ Global Intelligence Network, Symantec ha creado algunas de las fuentes de datos más completas del mundo sobre las amenazas en Internet. Con más de 240.000 sensores en más de 200 países observa las actividades de ataque por medio de una combinación de productos y servicios propios como Symantec DeepSight™ Threat Management System, Symantec Managed Security Services y productos Norton™ para el consumidor, así como otras fuentes de datos de terceros.

Frecuencia: semestral

Costo: gratuito

- *Websense Security Labs State of Internet Security*[27] (Estado de seguridad en Internet de Websense Security Labs™)

  Websense® Security Labs™ utiliza el sistema Websense ThreatSeeker™ Network, cuya patente está en trámite, para descubrir, clasificar y observar las amenazas en Internet y sus tendencias globales. Con el dispositivo Internet HoneyGrid™, primero en el mundo, el sistema se sirve de cientos de tecnologías, incluidas las basadas en mecanismos como "honeyclients" y "honeypots", sistemas de reputación, aprendizaje automático y sistemas de computación en red avanzados a fin de analizar diariamente más de mil millones de segmentos de contenido en busca de amenazas a la seguridad.

  Frecuencia: semestral

  Costo: gratuito

4. Educación de los usuarios finales

Los servicios basados en las tecnologías de la información y la comunicación (TIC) producen inmensas cantidades de datos personales[28]:

- 65.000 millones de llamadas telefónicas al año;
- 2 millones de correos electrónicos por segundo;
- 1 millón de mensajes instantáneos de Messenger por segundo;
- Un tráfico de 8 terabytes por segundo;
- Un almacenamiento magnético de 255 exabytes;

[27] www.websense.com/site/docs/whitepapers/en/WSL_Q1_Q2_2009_FNL.PDF (última consulta: 9 de enero de 2010).
[28] *Kevin Kelly*, diciembre de 2007, www.ted.com/index.php/talks/kevin_kelly_on_the_next_5_000_days_of_the_web.html (última consulta: 10 de enero de 2010).

- 1 millón de consultas verbales por hora;
- 2.000 millones de nodos de localización activados;
- 600.000 millones de etiquetas de identificación por radiofrecuencia en uso.

La educación de los usuarios finales se realiza en su mayor parte por medio de advertencias en los medios de comunicación (anuncios de interés público en la radio o la televisión) y folletos que distribuyen las oficinas de atención bancaria a los particulares o los proveedores de servicios de Internet. Algunos servicios informáticos ofrecen seminarios en la web (webinarios) o vídeos en línea en You-tube, etc.

5. Formulación de políticas

Consejo de Europa

Convenio sobre el delito cibernético

El Convenio sobre el delito cibernético, que entró en vigor el 1 de julio de 2004, es el primer tratado internacional relativo a los delitos que se cometen por conducto de Internet y otras redes informáticas, y aborda especialmente las infracciones relativas a la propiedad intelectual, el fraude informático, la pornografía infantil y el quebrantamiento de la seguridad en las redes. Asimismo, contiene una serie de disposiciones sobre atribuciones y procedimientos, por ejemplo en lo que atañe al registro de sistemas informáticos y la interceptación de datos.

Su objetivo principal es procurar una política penal común destinada a proteger a la sociedad contra la delincuencia cibernética, en particular mediante la adopción de leyes apropiadas y el fomento de la cooperación internacional.

Directrices para la cooperación entre las autoridades encargadas de aplicar la ley y los proveedores de servicios de Internet contra el ciberdelito

Estas directrices para la cooperación entre las autoridades de represión de la criminalidad y los proveedores de servicios de Internet contra el delito cibernético[29] se adoptaron en la Conferencia Octopus, celebrada el 1 y 2 de abril de 2008.

En ellas se reconoce que la construcción de una sociedad de la información exige el fortalecimiento de la confianza en las tecnologías de la información y las comunicaciones (TIC), la protección de los datos personales y la privacidad, y la promoción de una cultura general de ciberseguridad en un contexto en el que las sociedades de todo el mundo dependen cada vez más de las TIC, por lo que son vulnerables a la ciberdelincuencia.

[29] www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf (también existen versiones en español, francés, rumano, ruso y ucraniano) (última consulta: 10 de enero de 2010).

Las directrices no pretenden sustituir ningún instrumento jurídico existente, sino que presuponen la existencia de unos instrumentos jurídicos adecuados para establecer un sistema equilibrado de instrumentos de investigación, así como salvaguardias conexas y una protección de derechos humanos fundamentales como la libertad de expresión, el respeto de la vida privada, del hogar y de la correspondencia, y el derecho a la protección de los datos. Por lo tanto, se recomienda que los Estados adopten disposiciones en su legislación nacional con miras a aplicar plenamente las disposiciones de procedimiento del Convenio sobre el delito cibernético, y a especificar las autoridades de investigación y las obligaciones de las fuerzas del orden, estableciendo al mismo tiempo las condiciones y salvaguardias previstas en el artículo 15 del Convenio para:

- Asegurar la labor eficiente de las autoridades responsables de velar por la ley;
- Proteger la capacidad de los proveedores de servicios de Internet para prestar servicios;
- Asegurar la conformidad entre las disposiciones nacionales y la normativa mundial;
- Promover la normativa mundial en lugar de soluciones nacionales aisladas; y
- Ayudar a garantizar el debido procedimiento legal y el estado de derecho, incluidos los principios de legalidad, proporcionalidad y necesidad.

A fin de aumentar la ciberseguridad, reducir al mínimo la utilización de los servicios con fines ilegales y fomentar la confianza en las TIC, es fundamental que los proveedores de servicios de Internet y las fuerzas del orden cooperen entre sí de un modo eficiente, tomando debidamente en consideración sus respectivas funciones, el costo de dicha cooperación y los derechos de los ciudadanos.

El objetivo de las directrices es ayudar a las autoridades responsables del cumplimiento de la ley y a los proveedores de servicios de Internet a estructurar sus interacciones en lo tocante a las cuestiones relacionadas con la ciberdelincuencia. Las directrices se basan en buenas prácticas existentes y deberían ser aplicables en cualquier país del mundo, de conformidad con la legislación nacional y el respeto de la libertad de expresión, la privacidad, la protección de los datos personales y otros derechos fundamentales de los ciudadanos.

El Tribunal Europeo de Derechos Humanos se remitió por primera vez a las Directrices en el caso *K.U. c. Finlandia*[30]. Las mismas se citan como texto internacional relevante aplicable en este caso en relación con el derecho al respeto a la vida privada y familiar (artículo 8 del Convenio Europeo de Derechos Humanos).

[30] www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/1429_ECHR_CASE_OF_K.U._v%20Finland.pdf (última consulta: 10 de enero de 2010).

Comisión Europea

En las conclusiones del Consejo de la Unión Europea de 27 de noviembre de 2008 se invitaba a los Estados miembros y a la Comisión, en particular, a redactar, en consulta con los operadores privados, un acuerdo modelo europeo de cooperación entre los organismos responsables del cumplimiento de la ley y los operadores privados.

Las decisiones marco que se enumeran a continuación tipificaron como sancionables, respectivamente: la difusión de pornografía infantil, la incitación al racismo y a la violencia u odio xenófobos, la instigación a cometer atentados terroristas, la captación de terroristas y su adiestramiento, también cuando se lleve a cabo en línea:

> Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil (DO L 13, de 20 de enero de 2004, página 44),
>
> Decisión Marco 2008/913/JAI del Consejo relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal (DO L 328, de 6 de diciembre de 2008, página 55) y,
>
> Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo (DO L 330, de 9 de diciembre de 2008, página 21).

Principales cuestiones tratadas:

- Ante diferentes tipos de contenidos ilícitos, ¿las mismas soluciones?
- Libertad de expresión y casos en que es difícil apreciar la ilegalidad.
- Ante distintas realidades nacionales, ¿las mismas soluciones?
- Códigos de conducta en lo relativo a detección y retirada de contenidos.
- Condiciones generales de los contratos para prevenir la responsabilidad de los operadores privados.
- Elementos de un acuerdo modelo europeo.
- Formato del diálogo entre los organismos policiales y los proveedores de servicios de Internet.
- Objetivos del diálogo entre los organismos policiales y los proveedores de servicios: aumentar la sensibilización y promover la cooperación.

UNODC

Por recomendación de la Comisión de Prevención del Delito y Justicia Penal en su 13º período de sesiones de 2004, el Consejo Económico y Social aprobó la resolución 2004/26 sobre "cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo de los casos de fraude, falsificación de identidad y su uso indebido con fines delictivos y los delitos conexos". En esta resolución, el Consejo alentaba a los Estados

Miembros a que, entre otras cosas "cooperasen entre sí en los esfuerzos por prevenir y combatir el fraude y la falsificación de identidad y su uso indebido con fines delictivos, incluso mediante la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional[31] y demás instrumentos internacionales pertinentes, y a que considerasen la posibilidad de revisar sus leyes nacionales sobre fraude, falsificación de identidad y su uso indebido con fines delictivos, siempre que fuera necesario y apropiado, para facilitar esa cooperación".

Por recomendación de la Comisión de Prevención del Delito y Justicia Penal en su 16º período de sesiones de 2007, el Consejo Económico y Social aprobó la resolución 2007/20 sobre "cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad". En dicha resolución, el Consejo, entre otras cosas, alentó a los Estados Miembros a que:

> 15. Adoptaran las medidas apropiadas para que sus autoridades policiales y judiciales puedan cooperar con más eficacia en la lucha contra el fraude y los delitos relacionados con la identidad, de ser necesario mediante el fortalecimiento de los mecanismos de asistencia judicial recíproca y extradición, teniendo en cuenta el carácter transnacional de esos delitos y aprovechando plenamente los instrumentos jurídicos internacionales pertinentes, incluidas la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas contra la Corrupción;
>
> 16. Consultaran y colaboraran con entidades comerciales pertinentes y otras entidades del sector privado, en la medida de lo posible, con el fin de tener un conocimiento más completo de los problemas que planteaban el fraude económico y los delitos relacionados con la identidad y cooperar con más eficacia en la prevención, la investigación y el enjuiciamiento de esos delitos;
>
> 17. Promovieran el entendimiento mutuo y la cooperación entre las entidades de los sectores público y privado mediante iniciativas encaminadas a reunir a los diversos interesados y facilitar el intercambio de opiniones e información entre ellos, y pedía a la Oficina de las Naciones Unidas contra la Droga y el Delito que, a reserva de la disponibilidad de recursos extrapresupuestarios, facilitara dicha cooperación, en consulta con la secretaría de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, con arreglo a la resolución 2004/26 del Consejo Económico y Social, de 21 de julio de 2004.

Además, por recomendación de la Comisión de Prevención del Delito y Justicia Penal en su 18º período de sesiones de 2009, el Consejo Económico y Social aprobó la resolución 2009/22 sobre "cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad". En esta resolución, el Consejo pidió que:

> 7. La Oficina de las Naciones Unidas contra la Droga y el Delito, en consulta con los Estados Miembros y teniendo en cuenta a las organizaciones intergubernamentales

[31] Resolución 55/25 de la Asamblea General, anexo I.

pertinentes y, de conformidad con las normas y los procedimientos del Consejo Económico y Social, expertos de instituciones académicas, organizaciones no gubernamentales pertinentes y el sector privado, reuniera, elaborase y difundiera:

a) Material y directrices sobre la tipología de los delitos relacionados con la identidad y sobre cuestiones de penalización pertinentes, a fin de prestar asistencia a los Estados Miembros que la soliciten en lo que respecta a la tipificación de nuevos delitos relacionados con la identidad y a la modernización de los delitos existentes, teniendo presente la labor pertinente de otras organizaciones intergubernamentales que se ocupan de cuestiones conexas;

b) Material de asistencia técnica para capacitación, como manuales, recopilaciones de prácticas útiles o directrices y material científico, forense u otros materiales de referencia, destinado a funcionarios encargados de hacer cumplir la ley y fiscales, a fin de aumentar sus conocimientos especializados y su capacidad para prevenir y combatir el fraude económico y los delitos relacionados con la identidad;

c) Un conjunto de prácticas útiles y directrices para prestar asistencia a los Estados Miembros en la determinación de las repercusiones de esos delitos en las víctimas;

d) Un conjunto de materiales y prácticas óptimas sobre las asociaciones entre entidades de los sectores público y privado para prevenir el fraude económico y los delitos relacionados con la identidad;

[...]

10. La Oficina de las Naciones Unidas contra la Droga y el Delito siguiera esforzándose, en consulta con la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, por promover el entendimiento mutuo y el intercambio de opiniones entre entidades de los sectores público y privado sobre cuestiones relativas al fraude económico y los delitos relacionados con la identidad, con miras a facilitar la cooperación entre diversos interesados de ambos sectores, mediante la continuación de la labor del Grupo básico de expertos sobre delitos relacionados con la identidad, cuya composición debería respetar el principio de la distribución geográfica equitativa, y que informase periódicamente a la Comisión de Prevención del Delito y Justicia Penal acerca de los resultados de su labor.

Seminarios y actividades recientes

- El 23 de octubre el Supervisor Europeo de Protección de Datos, junto con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), fueron anfitriones en el Parlamento Europeo del seminario titulado “Responder a las infracciones de seguridad”. El seminario estuvo dedicado a tres objetivos principales, correspondientes al “ciclo de vida de la violación de datos”: intercambiar y explorar mejores prácticas para prevenir y mitigar los casos de violación

de datos desde el punto de vista del responsable de su control; intercambiar mejores prácticas elaboradas por las autoridades de protección de datos, así como los interesados en el ámbito institucional e industrial, sobre la manera de gestionar las violaciones de seguridad, incluida la formulación de procedimientos para investigar las violaciones; finalmente, reunir experiencias de otros sectores y de Estados no miembros de la UE sobre disposiciones relacionadas con la notificación de las violaciones de datos.

- El 27 de noviembre de 2009 la Comisión Europea acogió en Bruselas una conferencia sobre "Diálogo entre los sectores público y privado para combatir las actividades ilegales en línea".
- El 23 y 24 de noviembre de 2009 la OSCE fue anfitriona en Zagreb (Croacia) de una Reunión de Trabajo Nacional de Expertos sobre un enfoque global de la seguridad cibernética, cuyos temas fueron el uso de Internet con propósitos terroristas, la delincuencia cibernética y otras amenazas. Las sesiones versaron sobre el uso de Internet con fines terroristas, ataques cibernéticos por parte de grupos terroristas-contramedidas, marcos jurídicos, mejores prácticas y colaboración del sector público con el privado (CPP); el delito cibernético-contramedidas, marcos jurídicos, mejores prácticas y CPP; y amenazas a infraestructuras críticas/otras amenazas-contramedidas, marcos jurídicos, mejores prácticas y CPP.
- El 9 y 10 de noviembre de 2009 se celebró en Berna (Suiza), la tercera Reunión de la entidad europea FI-ISAC (Centro de intercambio y análisis de información sobre servicios financieros), la cual contó con la participación del sector bancario internacional, organismos responsables del cumplimiento de la ley, equipos informáticos de respuesta de emergencia y responsables de la adopción de políticas a nivel nacional y de la UE, con el objetivo de crear un ambiente de confianza en cuyo marco los interesados pudieran intercambiar libremente información sobre la ciberdelincuencia en el sector financiero y las experiencias derivadas de actividades nacionales de cooperación.

Instituciones financieras

Centro de intercambio y análisis de información sobre servicios financieros-Europa (FI-ISAC)

Es importante que las instituciones financieras intercambien información sobre las vulnerabilidades, los incidentes y las medidas adoptadas, y conozcan el *modus operandi* de los ataques. La seguridad de la información no es un asunto de competitividad. La confianza y los incentivos se desarrollan juntos pero hay que dedicarles tiempo y energía; el intercambio de información es muy satisfactorio en grupos pequeños de composición constante, pues se basa en factores personales.

Dada la importancia de crear confianza, el Centro FI-ISAC aplica un protocolo estricto de intercambio de información llamado protocolo de señales de tráfico. La información, los documentos o las sesiones clasificados como "rojos" se refieren a incidentes en curso e

información proveniente de los servicios policiales o de servicios secretos nacionales. Estas sesiones se desarrollan oralmente y en ellas no hay grabaciones. El color "amarillo" abarca la información que se va a distribuir en el marco del banco o el proveedor de servicios de tecnología de la información y las comunicaciones. Dicha información se considera confidencial, pero no de máximo secreto. Se hace completamente anónima y se difunde por conducto del servidor de distribución cerrado de FI-ISAC. En el caso del color "verde" no hay restricciones a su revelación.

La red FI-ISAC europea, apoyada en la actualidad por la ENISA, cumple muy eficazmente la función de fomentar la sensibilización sobre las cuestiones de seguridad (de la información), en particular, a nivel directivo en las instituciones financieras. Las reuniones que se celebran regularmente son de gran valor para todos los participantes. La sostenibilidad a largo plazo de dichas actividades es un problema importante.

Bederlandse Vereniging van Banken (NVB)[32]

La entidad NVB, compuesta por 90 bancos de los Países Bajos, tiene como objetivo lograr un sector bancario fuerte, sano y competitivo a nivel internacional en el país. Como representante de los intereses comunes del sector, propugna un juego efectivo de las fuerzas del mercado al tiempo que tiene en cuenta los intereses de sus interlocutores.

En 2008 en los Países Bajos hubo:

- 1.700 millones de operaciones en puntos de venta;
- 600 millones de operaciones en cajeros automáticos;
- Más de 50% de los pagos nacionales realizados a través de Internet;
- 28 millones de operaciones por el sistema iDEAL;
- Un fraude por clonación de tarjetas que ascendió a 31 millones de euros;
- Ningún dato estadístico sobre fraude en operaciones bancarias en línea.

Programa NICC (Infraestructura nacional (contra) el delito cibernético, patrocinada por el Departamento de Asuntos Económicos). Adoptando el principio de "aprender haciendo", en 2006 el Gobierno holandés y el sector privado dieron los primeros pasos hacia el desarrollo de una estrategia satisfactoria de lucha contra el delito cibernético, con el establecimiento de una infraestructura nacional contra el delito cibernético (*Nationale Infrastructuur ter bestrijding van Cybercrime, NICC*)[33]. Era necesario un órgano que integrase las distintas actividades e iniciara y facilitara la colaboración entre todas las partes involucradas.

La misión del programa NICC es crear esa infraestructura, no solo introduciendo nuevas características, sino colaborando con las demás partes en todo lo posible e integrando las iniciativas ya existentes a fin de establecer el sistema nacional.

---

[32] *Michael Samson*, National Infrastructure against Cybercrime, A public private partnership—Management of data breaches, Netherlands Bankers' Association, Bruselas, 23 de octubre de 2009, www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar_data_breaches_presentations_EN.zip (última consulta: 10 de enero de 2010).

[33] www.samentegencybercrime.nl/UserFiles/File/Leaflet_NICC.pdf (última consulta: 10 de enero de 2010).

Hay una serie de organizaciones holandesas activas en la lucha contra la ciberdelincuencia que ya participan, como la Unidad de denuncias de delitos cibernéticos (*Meldpunt Cybercrime*), el Equipo para la delincuencia de alta tecnología, de la Agencia Nacional de Servicios Policiales (*Korps Landelijke Politiediensten, KLPD*) y el Servicio de Alerta Nacional (*Waarschuwingsdienst.nl*) de GOVCERT.NL, que es el Equipo de Respuesta a Emergencias Informáticas en el país.

No obstante, la lucha contra la ciberdelincuencia a nivel nacional sigue siendo fragmentaria ya que no existe una visión general de todas las iniciativas. No hay una delimitación clara de competencias, ni existe un enfoque común e integrador de los sectores público y privado. El mapa de la lucha contra el delito cibernético muestra tanto aspectos en que hay solapamientos como "zonas desiertas". El programa NICC estudia la situación de la lucha contra esa delincuencia, descubre los solapamientos y apoya las actividades que contribuyen a repoblar esas zonas desiertas.

El mecanismo impulsor de la infraestructura nacional holandesa es el sistema de intercambio de información sobre el delito cibernético, mediante el cual las organizaciones de los sectores público y privado se transmiten información sensible.

Federación Bancaria Irlandesa

La Federación Bancaria Irlandesa[34] es la entidad principal representativa de la banca y el sector de servicios financieros de Irlanda. Entre sus miembros figuran los bancos e instituciones que prestan servicios financieros, tanto de ámbito nacional como internacional, que operan en el país. Dicha entidad publicó una Guía del consumidor para la prevención del fraude de 2009, en colaboración con la Organización Irlandesa de Servicios de Pago, la An Garda Síochána y el Servicio de Policía de Irlanda del Norte. Participa en un Foro multisectorial sobre la delincuencia de alta tecnología, en el que se reúnen todos los bancos minoristas que operan en Irlanda, la An Garda Síochána, la Asociación de proveedores de servicios de Internet y el Centro para la Investigación de la Ciberdelincuencia de la Escuela Universitaria de Dublín. Su misión es similar a la del FI-ISAC en lo que respecta al intercambio de conocimientos sobre las técnicas que utilizan los delincuentes, lo que ayuda a crear una capacidad de reacción.

En 2008, hubo en Irlanda:

- 202,5 millones de retiros en cajeros automáticos;
- 2,3 millones de tarjetas de crédito en uso (2007);
- 181 millones de operaciones realizadas con 2,9 millones de tarjetas de débito;
- 2,4 millones de clientes registrados para operaciones de banca en línea, contabilizados hasta junio de 2009;
- 67,1 millones de accesos de clientes a balances de cuentas en línea, contabilizados hasta junio de 2009;
- 16,9 millones de pagos en línea efectuados por clientes.

[34] www.ibf.ie/ (última consulta: 10 de enero de 2010).

Sector de servicios informáticos

Asociación de Proveedores Europeos de Servicios de Internet (EuroISPA)

La asociación EuroISPA, reconocida como portavoz del sector de servicios de Internet europeos, es la entidad que agrupa al mayor número de proveedores de esos servicios de todo el mundo, representando a más de 1.700 de ellos establecidos en Europa.

EuroISPA considera que la cooperación entre los sectores público y privado ya existe[35]. Sin embargo, es necesario mejorarla mediante:

- Una mayor sensibilización;
- El fomento de una cultura de cooperación a nivel nacional entre las autoridades administrativas y judiciales y el sector industrial informático;
- La mejora de la cooperación entre los servicios de represión de la delincuencia de todos los Estados miembros;
- La cooperación y el diálogo internacionales más allá de los límites de la UE;
- El fomento de la especialización: la capacitación de jueces y fiscales representa un problema tanto a nivel nacional como internacional;
- El adecuado equilibrio entre los derechos de privacidad y los requisitos exigidos por los servicios de represión del delito;
- La consideración del reembolso de los costos ocasionados por esos requisitos;
- La superación de las dificultades legales originadas por los distintos sistemas jurídicos.

El 20 de marzo de 2006, la EuroISPA patrocinó una mesa redonda en Bruselas, cuyo tema fue un enfoque coordinado del fraude en línea y la lucha contra la peska, organizada con el apoyo de Interpol y Microsoft. En la reunión, el Presidente de EuroISPA, profesor Michael Rotert, declaró que "la peska representa una amenaza para los esfuerzos de todos los interesados del sector por aumentar la disponibilidad y adopción de servicios en línea. Por lo tanto, las asociaciones creadas e impulsadas por el esfuerzo conjunto del sector informático, los responsables de formular políticas, las fuerzas de represión del delito y los consumidores son verdaderamente imprescindibles para que nuestro sector pueda contrarrestar eficazmente esa amenaza. Esperamos que esta iniciativa sirva de estímulo para que aumente el número de interesados en combatir la peska"[36]. Este compromiso de la EuroIPSA en pro de la sensibilización frente a la peska continúa tras el lanzamiento de su página web contra ese delito en octubre de 2005. Dicho sitio, creado con el apoyo de eBay, contiene consejos e información concisa para combatir esa actividad, y puede visitarse en www.euroispa.org/antiphishing [no disponible en línea desde el 10 de junio de 2010, pero accesible en www.archive.com].

[35] Cyber criminality: the private sector perspective, *Michael Rotert*, Vicepresidente de EuroISPA, ponencia presentada conjuntamente con ETNO, Asociación Europea de Operadores de Redes de Telecomunicaciones (que representa a 43 compañías de 36 países), en el Diálogo Público-Privado para Combatir las Actividades Ilegales en Línea, patrocinado por la Comisión Europea en Bruselas, el 27 de noviembre de 2009.

[36] Comunicado de prensa de EuroISPA: 20 de marzo de 2006 "EuroISPA hosts multi-stakeholder event on combating phishing."

Plan de Acción de Londres[37]

El 11 de octubre de 2004 organismos gubernamentales y públicos de 27 países, responsables del cumplimiento de la ley en materia de correo electrónico basura, se reunieron en Londres para deliberar sobre una mayor cooperación internacional en la lucha contra este problema. Participaron en la reunión entidades muy variadas dedicadas al tema, entre ellas organismos de protección de datos, organismos de telecomunicaciones y organismos de protección al consumidor. Varios representantes del sector privado también colaboraron en algunas partes de la reunión.

Como se ha reconocido en diversos foros internacionales, la cooperación mundial y las asociaciones público-privadas son fundamentales para luchar contra los correos basura. Los participantes elaboraron un plan de acción basándose en la reciente labor de organizaciones tales como la Organización de Cooperación y Desarrollo Económicos (OCDE) y su Grupo de trabajo para la lucha contra ese tipo de correo electrónico, la Unión Internacional de Telecomunicaciones (UIT), la Unión Europea (UE), la Red Internacional de Protección del Consumidor y Aplicación de la Ley (ICPEN) y la Asociación de Cooperación Económica en Asia y el Pacífico (APEC).

El objetivo de este plan de acción es promover la cooperación internacional en la lucha contra el correo basura y abordar los problemas conexos como el fraude y la estafa en línea, la peska y la difusión de virus. Los presentes en la reunión también declararon el plan de acción abierto a la participación de otros organismos gubernamentales y públicos interesados, así como de representantes del sector privado adecuados, como forma de ampliar la red de entidades cooperantes en la lucha contra el correo electrónico no deseado.

Sexta cumbre alemana contra el correo basura[38]

La Sexta cumbre alemana contra el correo basura tuvo lugar del 27 al 29 de octubre en Wiesbaden, y se centró en el "fraude de la lotería" y otras formas de fraude con pago por adelantado que se cometen a través del correo electrónico. Organizaron esta reunión las entidades eco, Contact Network of Spam Authorities (CNSA), Plan de Acción de Londres (LAP), Hessen-IT y ENISA. Fue patrocinada por Microsoft, eleven, Cloudmark, IronPort y clara.net. El primer día estuvo reservado exclusivamente a la capacitación de los miembros de CNSA/LAP.

Durante los dos días siguientes, expertos de todo el mundo presentaron y examinaron las últimas novedades jurídicas y técnicas en la esfera del correo basura. Los ponentes fueron representantes de organismos responsables del cumplimiento de la ley, del sector informático, organizaciones dedicadas a fomentar la concienciación pública y universidades. El programa del miércoles se centró, en particular, en los fraudes con pago por adelantado.

[37] www.londonactionplan.com/ (última consulta: 10 de enero de 2010).
[38] www.eco.de/veranstaltungen/6dask.htm (última consulta: 10 de enero de 2010).

V. APOYO A LAS INVESTIGACIONES DEL HURTO DE IDENTIDAD

Además de las conductas delictivas corrientes, que ahora han pasado a desarrollarse también en línea, ha nacido en Internet un nuevo tipo de criminalidad. Ya desde los ataques a la primera generación de computadoras y las redes correspondientes, empezaron a descubrirse nuevos fraudes. Tales delitos, por ejemplo la "peska"[39] y el "hurto de identidad"[40], requieren nuevos métodos de investigación y su persecución eficaz depende en gran medida de los datos y la información que obran en manos de Internet. La falta de cooperación puede ser un grave obstáculo para la investigación.

1. Detección del delito y reunión de pruebas

El hurto de identidad es un delito que puede pasar sin ser detectado por mucho tiempo. Es muy difícil de descubrir y las notificaciones al respecto únicamente provienen de las entidades que extravían los datos.

Vulneración de datos

Existen muchos ejemplos de esta vulneración, entre ellos el caso de los miles de clientes de la aseguradora británica Standard Life, amenazados por el riesgo de ser víctimas de fraude tras el extravío de sus detalles personales por el servicio HM Revenue and Customs (HMRC). Un disco compacto que contenía los datos de 15.000 titulares de pólizas de pensionistas fue enviado por correo desde las oficinas de HMRC en Newcastle hasta la sede de Standard Life en Edimburgo, pero nunca llegó a su destino[41]. El disco contenía los nombres, números de seguro nacional, fechas de nacimiento, direcciones y datos sobre pensiones. Este tipo de información se prestaría fácilmente a abusos si cayese en manos equivocadas. Suponiendo que el disco hubiera sido leído por defraudadores, los mismos podrían haber solicitado préstamos o tarjetas de crédito utilizando nombres falsos.

[39] Con respecto al fenómeno de la "peska", véase: *Dhamija/Tygar/Hearst*, Why Phishing Works, disponible en: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, informe al Ministro de Seguridad Pública y Preparación para Emergencias del Canadá y el Fiscal General de los Estados Unidos, 2006, disponible en: www.usdoj.gov/opa/report_on_phishing.pdf.

[40] En lo referente al "hurto de identidad", véase, por ejemplo: Gercke, Internet-related Identity Theft, 2007, disponible en: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, *Lex Electronica*, vol. 11, núm. 1, 2006, disponible en: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf (última consulta: noviembre de 2007); *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, disponible en: www.privacyrights.org/ar/id_theft.htm (última consulta: noviembre de 2007).

[41] www.theregister.co.uk/2007/11/05/standard_life_lost_cd_security_flap/ (última consulta: 10 de enero de 2010).

Otro ejemplo fue un caso que sucedió en el Reino Unido en marzo de 2007, cuando el servicio HM Revenue and Customs (HMRC) extravió dos discos compactos que contenían detalles individuales de 25 millones de personas, lo que provocó la dimisión del presidente de HMRC, Paul Gray[42], y que el Primer Ministro Gordon Brown tuviera que disculparse en el Parlamento por la pérdida[43]. Se excusó en la Cámara de los Comunes por los "inconvenientes y preocupaciones" causados, y dijo que el Gobierno estaba trabajando para impedir que esa información fuera utilizada con fines fraudulentos. Existen muchos otros ejemplos de incidentes similares de extravío de datos[44] a lo largo de los años.

Notificaciones sobre la vulneración de datos

En 2003 California fue el primer estado en adoptar una ley de notificación de vulneraciones de datos (SB1386), la cual ha servido de modelo a otros estados de Norteamérica para elaborar sus leyes. Estas exigen a las empresas que notifiquen a las personas cuando su información individual haya sido extraviada o robada. Aunque sus particularidades difieren mucho entre los diferentes Estados, el objetivo general es informar al consumidor, incentivar las inversiones en seguridad y reducir el hurto de identidad[45]. Muchas de esas leyes se titulan "prevención del hurto de identidad". Curiosamente, la investigación realizada por Alessandro Acquisti y Sasha Romanosky, de la Universidad Carnegie Mellon, indica que tanto las vulneraciones de datos como los hurtos de identidad van en aumento, pero también da a entender que este delito parece seguir la misma tendencia[46] en dichos Estados, tanto si existe en ellos una ley de notificación como si no existe.

Debido al temor y pánico que causan estos fallos de seguridad de los datos en Europa, la Comisión Europea (CE) estudia en la actualidad la conveniencia de adoptar la obligación de notificar esas vulneraciones[47]. La reforma de la CE en materia de telecomunicaciones dará ocasión de reforzar y clarificar las disposiciones actuales de protección de datos. Cuando ocurra un fallo de seguridad, el operador tendrá que informar a las autoridades y a los particulares que estén en situación de riesgo como consecuencia del extravío de sus datos personales. Además, los operadores de redes deberán notificar a la autoridad competente nacional reguladora todo fallo de seguridad o pérdida de integridad que haya tenido repercusiones significativas en el funcionamiento de redes o servicios. Según la Sra. Viviene Reding, "la transparencia y la información serán los nuevos principios fundamentales para hacer frente a las vulneraciones de la seguridad de los datos".

El Teniente Coronel Eric Freyssinet, miembro de la Dirección General de la Gendarmería Nacional, Subdirección de la Policía Judicial de la Gendarmería francesa, destaca las

[42] http://news.bbc.co.uk/2/hi/uk_news/politics/7104368.stm (última consulta: 10 de enero de 2010).
[43] http://news.bbc.co.uk/2/hi/7104945.stm (última consulta: 10 de enero de 2010).
[44] http://news.bbc.co.uk/2/hi/uk_news/7103911.stm (última consulta: 10 de enero de 2010).
[45] *Alessandro Acquisti, Sasha Romanosky*, Carnegie Mellon University, "Responding to Data Breaches", Parlamento Europeo, 23 de octubre de 2009. www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar_data_breaches_presentations_EN.zip (última consulta: 10 de enero de 2010).
[46] Idem.
[47] "La reforma en materia de telecomunicaciones ha inscrito firmemente en la agenda política europea el tema de la notificación obligatoria de las vulneraciones de datos personales. El paquete de reforma de las telecomunicaciones, ya en espera de un acuerdo definitivo, establecerá las normas relativas a la prevención, gestión y presentación de informes de tales vulneraciones en el sector de las comunicaciones electrónicas". Discurso de la Sra. Viviane Reding, Miembro de la Comisión Europea a cargo de Sociedad de la Información y Medios de Difusión, en el Seminario EDPS-ENISA "Respuesta a las vulneraciones de datos", celebrado en Bruselas, el 23 de octubre de 2009. http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/brussels-20091023.pdf (última consulta: 10 de enero de 2010).

razones por las que la notificación de vulneraciones de datos es un problema para muchas empresas[48]. Esto se debe a que muchas veces un procedimiento judicial se percibe como algo adverso, a causa de la publicidad del juicio, las investigaciones contra las compañías que no custodian los datos personales debidamente, y el temor a las consecuencias de las actividades de los servicios policiales para el sistema. El ponente señala también la necesidad de encontrar un equilibrio entre las obligaciones legales y las mejores prácticas, ya que interesa a todos intercambiar información sobre las vulneraciones y, cuando sea preciso, iniciar investigaciones criminales.

Iniciativa Signal Spam

De todas formas, hay ciertas iniciativas de colaboración del sector público y el sector privado que alientan a los usuarios a dar parte de los delitos. "Signal Spam" es una de ellas, emprendida en Francia con amplia participación de interesados públicos y privados.

El spam o correo basura es un fenómeno polifacético, causa de variadas amenazas a la ciudadanía y la sociedad de la información. Por ello, el Gobierno francés puso en marcha en 2005 una iniciativa nacional destinada a enfrentar este desafío de manera integral y basada en la colaboración entre los sectores público y privado, a la que dio el nombre de Signal Spam.

Signal Spam ofrece a los ciudadanos la posibilidad de denunciar cualquier tipo de correo basura del que sean víctimas, y proporciona a las autoridades y compañías interesadas acceso en tiempo real a esas denuncias para garantizar la seguridad en Internet y facilitar el cumplimiento de la ley. Esta iniciativa es única por el hecho de que en ella se combina la acción de todos los interesados, desde el comercio legítimo por vía electrónica hasta las compañías de seguros, proveedores de servicios de Internet y entidades del sector informático, así como autoridades administrativas y organismos encargados de hacer cumplir la ley.

Gracias a la valiosa información que proporcionan directamente los usuarios, la iniciativa Signal Spam permite a las autoridades públicas evaluar continuamente las amenazas y tomar medidas contra actividades fraudulentas o delictivas en la red. También permite a las empresas detectar los ataques llevados a cabo contra sus servicios y marcas, y mejorar la protección de sus clientes.

El correo basura representa más que nunca un problema para los usuarios de Internet. En junio de 2009 varios institutos calcularon que en todo el mundo se enviaban diariamente entre 180.000 y 200.000 millones de esos mensajes, lo que suponía más del 90% de los correos electrónicos.

Actualmente un usuario europeo recibe en su dirección electrónica profesional o personal un promedio de doce correos basura por día. Este tipo de mensajes, la estafa (es decir, el fraude por vía electrónica) y la peska (las tentativas de hurto de identidad o de acceso a

[48] "Respuesta a las vulneraciones de datos", Parlamento Europeo, Bruselas, 23 de octubre de 2009, www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar_data_breaches_presentations_EN.zip (última consulta: 10 de enero de 2010).

cuentas en línea), son manifestaciones del mismo problema. La denominación genérica "correo basura" denota varios tipos de mensajes que pueden ser portadores de trampas basadas en falsificaciones e incluso de virus.

El Gobierno francés, consciente de la magnitud y complejidad de este fenómeno, decidió actuar. El Tercer Comité Interministerial para la Sociedad de la Información (CISI), en julio de 2003, encargó al Departamento de Desarrollo de los Medios de Comunicación Social la aplicación de una serie de medidas de lucha contra el correo basura.

Este trabajo dio paso a la creación de la asociación sin ánimo de lucro Signal Spam en noviembre de 2005, y a la puesta en marcha, en mayo de 2007, de una herramienta para denunciar tales mensajes, así como de la página web www.signalspam.fr. Esta asociación incluye a la mayoría de las organizaciones francesas, sean gubernamentales o profesionales del sector de Internet, que se ocupan de luchar contra ese tipo de correo. Su objetivo es aunar todos los esfuerzos dirigidos a combatir dicha plaga.

Un requisito previo esencial es que las notificaciones que se reciban tengan valor desde el punto de vista legal y puedan utilizarse en los tribunales, por lo que los usuarios que denuncian mensajes son identificados mediante un procedimiento de registro en el sitio web de Signal Spam. Si lo desean, sus denuncias pueden ser utilizadas en acciones legales y administrativas. El hecho de que entidades públicas y privadas puedan acceder a una base de datos única, a la que llegan directamente las denuncias de los usuarios, da a la iniciativa un carácter excepcional. Desde su lanzamiento, hace dos años, se recibieron 17 millones de alertas. Las denuncias se realizan principalmente a través de componentes enchufables, que el usuario puede descargar e instalar en Microsoft Outlook o Thunderbird.

En la actualidad, los ataques son más específicos y su número va en aumento. Dada la mejora de los filtros tecnológicos, las campañas de correo basura masivas y sin destinatarios determinados son cosa del pasado. Por ejemplo, un ataque de peska solía consistir en el envío de decenas o cientos de miles de correos. Hoy en día, con el fin de buscar objetivos más concretos, el envío es de unos pocos cientos de mensajes. Así, los ataques son más difíciles de detectar mediante los instrumentos y redes de vigilancia que utilizan las autoridades y los operadores de control. Por lo tanto, el fraude que se lleva a cabo por medio de correos electrónicos no se puede identificar ni filtrar únicamente utilizando sensores de captura, y las cuentas de correo electrónico que no pertenecen a una persona real no pueden ser rastreadas. Obtener denuncias de los usuarios reales víctimas de estos ataques se ha convertido en un asunto de suma importancia.

Como consecuencia, el papel de los ciudadanos es crucial para evaluar y detectar las amenazas en línea.

La base de datos de Signal Spam contiene información útil para la lucha contra el correo basura. En el marco de ese objetivo, los datos pueden ser utilizados con múltiples fines, en la esfera civil o la penal, por entidades públicas o privadas, al objeto de garantizar la seguridad de los miembros o clientes de dicha iniciativa. Los fines pueden ser:

- El empleo por los servicios policiales para investigaciones judiciales;
- El uso público para investigar las vulneraciones de la protección de datos;

- La protección de la seguridad de las redes de administración y gobierno;
- La mejora de la seguridad de las redes, por ejemplo para los proveedores de servicios de Internet;
- La mejora de los trámites en el comercio legítimo por correo electrónico;
- La protección de marcas y servicios;
- La facilitación de la distribución de correos electrónicos;
- La protección de marcas y servicios de los clientes;
- La facilitación de investigaciones científicas.

2. Investigación con fines policiales

Es necesaria una cooperación estrecha entre los organismos responsables del cumplimiento de la ley y los proveedores de servicios en muchos ámbitos, y no solo en lo que respecta a los fraudes en línea novedosos y muy sofisticados. Las investigaciones sobre Internet plantean problemas excepcionales que requieren una estrecha colaboración entre los organismos policiales y los proveedores de servicios.

Como ejemplo cabe citar las dimensiones internacionales de la red, dado que en el proceso de transferir contenidos ilegales de un delincuente a otro podrían intervenir varios proveedores a menudo establecidos en distintos países. Rastrear la pista de un delincuente a otro exige una estrecha cooperación internacional entre los organismos responsables del cumplimiento de la ley, dado que esas investigaciones a menudo requieren una acción inmediata.

Estudio de casos: el portal de eBay para combatir la delincuencia

La sociedad eBay creó una organización encargada de reprimir la delincuencia a nivel mundial (GLEO) para promover el uso seguro de sus plataformas y colaborar con los servicios policiales de ámbito local, federal e internacional en un esfuerzo por salvaguardar la seguridad ciudadana, contribuir al cumplimiento de las normas establecidas y abrir causa a los infractores. Los organismos responsables de la aplicación de la ley en América del Norte que necesitan asistencia y constancia escrita para las investigaciones relacionadas con eBay y el sistema de pago PayPal pueden recabar el apoyo de la organización GLEO[49]. El portal para la represión del delito que esta mantiene permite a personal autorizado y legitimado de servicios policiales de todo el mundo solicitar y acceder por vía electrónica a los datos poseídos por eBay. Como ejemplos[50] de cooperación satisfactoria entre eBay y los servicios policiales a nivel mundial cabe citar:

[49] http://pages.ebay.com/securitycenter/law_enforcement.html (última consulta: 10 de enero de 2010)
[50] http://pages.ebay.com/securitycenter/law_case_study.html (última consulta: 10 de enero de 2010).

- *Detención de tres personas por robo de bienes*
  Agentes especiales del Departamento de Represión de la Delincuencia de Florida detuvieron a tres personas por liderar una banda dedicada al hurto en tiendas, que había robado discos Blue-ray DVD por valor de más de 1 millón de dólares en comercios de la región central de Florida. Gregory Marinitz, de 41 años, fue acusado por los siguientes motivos: negocio con bienes robados, delito de primer grado; conspiración organizada para la comisión de fraudes, también delito de primer grado; y negocio con bienes robados por medio de Internet, delito de tercer grado. James Davidson, de 37 años, y Tina Pallay, de 35, fueron acusados de conspiración organizada para la comisión de fraudes. La compañía eBay, de concierto con socios minoristas como Barnes & Noble, Borders, Circuit City y Target colaboró en las investigaciones con el Departamento mencionado.

- *eBay se une a la lucha contra el hurto*
  Una importante cadena internacional de tiendas de comestibles se puso en contacto con eBay en relación con la venta de varios artículos sanitarios, de tocador y de mejora del hogar que corría a cargo de un determinado vendedor en eBay. Después de examinar la cuenta del usuario, y con la asistencia del socio minoritario de eBay, se comprobó que los vendedores en cuestión eran ladrones convictos de comercios de la zona. Tras concluir la investigación, eBay decidió tomar las medidas pertinentes de conformidad con sus políticas y procedimientos. En la actualidad, se realizan las diligencias oportunas del caso, en nombre del minorista y de eBay, ante las instancias de aplicación de la ley.

- *Detención de dos personas por hurto de identidad*
  En noviembre de 2008 Billy Morris Britt, de 36 años, oriundo de Seattle, y Gabriel K. Jang, de 37 años y natural de Renton, fueron detenidos por cargos de fraude electrónico y hurto de identidad con agravantes. Se los acusa de utilizar tarjetas de crédito robadas para adquirir computadoras y otros equipos electrónicos que fueron vendidos posteriormente por millones de dólares en eBay. Los encartados y otros hurtaron las tarjetas de crédito de las taquillas de gimnasios en Washington y Oregón, crearon casi inmediatamente identidades falsas en sus coches y, poco más tarde, compraron costosos equipos electrónicos con las tarjetas robadas, tan solo unas horas después del hurto. Estos equipos los vendieron luego en eBay. Una investigación financiera reveló que 2 millones de dólares, provenientes de la venta de los aparatos, habían pasado por una cuenta de PayPal que Jang venía utilizando desde 2004, y otros 1,3 millones de dólares se habían ingresado en una cuenta corriente que se descubrió que pertenecía a Jang. Los investigadores de eBay y PayPal colaboraron con el Servicio Secreto de los Estados Unidos en Seattle de forma continua durante más de un año hasta la detención.

- *Condena de un individuo en el Reino Unido por falsificación*
  Davut Turk, residente en el Reino Unido, estuvo dos años embolsándose decenas de miles de dólares, gracias a la venta de joyas y adornos caros en eBay. Presentaba sus artículos como si fueran de plata, pero en realidad eran de latón. Esta lucrativa estafa, que le rindió aproximadamente 70.000 dólares, quedó al descubierto por la denuncia de un cliente, que provocó registros en su domicilio y un compartimento de depósito situado en las cercanías. Turk fue recientemente

condenado por 30 delitos relacionados con la denominación comercial y el uso de contrastes falsificados. Las autoridades encontraron más de 200 libras de artículos de plata falsos, que iban desde anillos y collares a candelabros y saleros y pimenteros. Fue condenado a pagar cerca de 10.000 dólares por tasas judiciales y multas. Los investigadores de eBay y PayPal colaboraron con las autoridades de manera continua a lo largo de varios meses. Les fue posible ayudar a los agentes a rastrear los fondos recibidos por este tipo de fraude porque Turk había utilizado PayPal para recibir los pagos de sus víctimas.

3. Capacitación de los servicios de represión del delito

La lucha eficaz contra el delito cibernético requiere la consideración de un enfoque bien meditado por parte del sector informático y las fuerzas del orden. Dada la complejidad y celeridad con que se desarrollan las nuevas tecnologías, por ejemplo los nuevos servicios ofrecidos en línea de manera gratuita, se pide a los proveedores de tales servicios con insistencia creciente que se involucren más activamente, además de responder a los requerimientos de los agentes de la ley. Los organismos policiales no pueden desarrollar por sus propios medios toda la especialización que se requiere, y la cooperación con el sector privado no es forzosamente algo habitual. Existen muy pocos programas de capacitación específicos cuyo objeto sea el hurto de identidad exclusivamente, pues el análisis forense informático es un elemento común a todo tipo de actividad en la esfera del delito cibernético.

Los organismos responsables del cumplimiento de la ley pueden recurrir al sector informático y los proveedores de servicios de Internet para obtener y mantener el conocimiento de las nuevas tecnologías. Tanto ese sector como dichos organismos necesitan intercambiar sus experiencias y problemas.

En el pasado ha sido escasa la cooperación oficial entre los responsables de mantener la ley y el sector informático para promover la formación y fomentar la capacidad de lucha contra el delito cibernético. Los organismos policiales de los diferentes sistemas jurídicos elaboraban tradicionalmente sus propios programas de formación y, en algunas ocasiones, colaboraban con el sector informático y el mundo académico a fin de cumplir objetivos nacionales fijados a corto plazo.

Desde 2002 está en marcha un esfuerzo coordinado para armonizar la capacitación sobre el delito cibernético a través de las fronteras internacionales, especialmente las fronteras europeas. En el marco de esta tarea los países de la UE cooperan con el propósito de realizar un plan elaborado como fruto de un proyecto FALCONE financiado por la Comisión Europea, titulado “Investigación del delito cibernético: establecimiento de un programa internacional de capacitación para el futuro”.

Las organizaciones desarrollan constantemente servicios de apoyo a su personal, tanto nuevo como ya en servicio. En este contexto son necesarios programas de capacitación del personal a fin de dotarlo de los conocimientos y la especialización necesarios para conseguir que su competencia y funciones laborales estén a la altura exigida por las normas internacionales.

Gracias especialmente a la creación del Grupo de trabajo de la Europol sobre armonización de la capacitación en materia de delito cibernético ha sido posible una colaboración más estrecha entre el sector informático, los responsables del cumplimiento de la ley, el mundo académico y las organizaciones internacionales. Asimismo, de la colaboración entre Microsoft e Interpol ha surgido un programa mundial de formación de esos responsables, coordinado por el Centro Internacional para Menores Desaparecidos y Explotados, con sede en Virginia, Estados Unidos.

La crisis económica ha puesto de manifiesto la necesidad de trabajar de manera más inteligente, y en el presente estudio se señalan formas en que los participantes esenciales de los servicios policiales, el sector informático y el ámbito académico pueden concertarse y proponer un enfoque más eficaz para impartir capacitación, tan necesaria, a los agentes de la ley, obtener mejor rendimiento de los recursos disponibles y responder también a las necesidades del sector para el desarrollo de sus conocimientos y competencia en un entorno que además propiciará la especialización adecuada.

Iniciativas actuales

Represión del delito

El subgrupo de la Europol sobre armonización de la capacitación relativa al delito cibernético, creado como consecuencia del éxito de los proyectos financiados por la Comisión Europea, es probablemente el ejemplo más conocido de elaboración de programas de capacitación de miembros de servicios policiales, establecidos por colaboración entre esos servicios, el mundo académico, el sector informático y las organizaciones internacionales. El subgrupo ha establecido un plan quinquenal para elaborar, mantener e impartir capacitación con sus correspondientes títulos en materia de delito cibernético. En el proyecto actual participan unos 30 asociados, pertenecientes a los colectivos citados, y se está buscando financiación adicional para preparar una formación más avanzada en consonancia con las amenazas propias del delito cibernético.

La Interpol promueve la formación y el fomento de la capacidad en todas las partes del mundo por medio de sus cinco grupos de trabajo regionales. Colabora en la iniciativa de la Europol y utiliza el material de capacitación y otros recursos de los socios participantes en el proyecto europeo.

En la región de Asia y el Pacífico existen estrechas relaciones de trabajo entre la policía y el sector informático, y las herramientas que este desarrolla se ponen a disposición de organismos policiales de todo el mundo. Existen otras iniciativas conjuntas referentes a investigaciones específicas, por ejemplo las relacionadas con redes infectadas y servicios que proporciona el sector para dar apoyo a las actividades de represión del delito.

Parece que en la mayoría de las iniciativas, los donantes pertenecen al sector informático y los beneficiarios al ámbito policial. El estudio debería determinar si es posible que las fuerzas de la policía proporcionen capacitación al sector informático.

Un tema que no se ha examinado a fondo es la posibilidad de utilizar las asociaciones que tal vez se establezcan en apoyo de la capacidad de investigación, ayuda que podría

aprovecharse en caso de grandes incidentes cibernéticos internacionales. Los organismos policiales han tendido tradicionalmente a centrarse en los delitos considerados aisladamente pero, en vista del probable aumento de incidentes como los ataques generalizados de denegación de servicio ocurridos recientemente en Estonia, sería útil movilizar en ese sentido a los asociados. Este asunto se considera de interés una vez que se hayan definido las relaciones para llevar a cabo las funciones de capacitación, educación e investigación, por lo que no se trata con más detalle en la presente monografía.

La Interpol, que trabaja para la capacitación de miembros de servicios policiales de todo el mundo, ha establecido hasta la fecha diversos grupos de trabajo sobre delincuencia relacionada con la tecnología de la información en Europa, Asia y el Pacífico, África, África septentrional/Oriente Medio y América. Si bien es muy considerable la capacitación impartida, hasta el momento lo ha sido según criterios pragmáticos, y por lo tanto no existe ningún proceso de titulación o cualificación. Muchas otras organizaciones multilaterales también han emprendido proyectos interregionales de formación, en particular la APEC, la ASEAN y la OEA. Al igual que en el caso de la Interpol, la mayoría de estas actividades obedeció a circunstancias particulares y no produjo un grado progresivo de instrucción que culminara en un título o diploma oficial.

Es importante que en toda propuesta de modelo para una futura cooperación se tenga en cuenta que muchas de las amenazas que plantea el ciberdelito a la Unión Europea provienen de más allá de sus fronteras. Es fundamental que los responsables policiales europeos establezcan vínculos sólidos con sus homólogos de otras regiones del mundo. Es lógico no solo desde una perspectiva de investigación y operacional, sino también desde el punto de vista de la capacitación.

Una de las organizaciones con la cual sería deseable cooperar es la Alianza Internacional Multilateral contra las Amenazas Cibernéticas (IMPACT), con sede en Kuala Lumpur, Malasia. Esta organización ha sido designada por la Unión Internacional de las Telecomunicaciones de las Naciones Unidas como entidad clave para la aplicación del Programa Mundial de Ciberseguridad de las Naciones Unidas, y en tal calidad, es responsable de la coordinación de los incidentes de ciberdelito y terrorismo que ocurren en 191 países de todas las regiones.

La Alianza IMPACT ha establecido un Centro mundial de respuesta cibernética para hacer frente a las amenazas de ese tipo que surjan en tiempo real. Además, cuenta con una extensa red académica de más de 20 universidades en todo el mundo, que realizan investigaciones sobre seguridad y protección en la esfera cibernética. Si bien IMPACT no se centra específicamente en la esfera policial, brinda un modelo para concertar la acción de organismos de policía, autoridades reguladoras, entidades gubernamentales, instituciones académicas y la colectividad de las ONG para responder a la amenaza común que plantean el delito cibernético y el terrorismo.

Como parte del trabajo aquí propuesto para la Unión Europea, un objetivo del presente estudio ha sido determinar los socios adecuados, como la Alianza IMPACT, con los que es posible cooperar para asegurar el adecuado intercambio y armonización de los trabajos de la UE y otras iniciativas internacionales con los de las demás regiones.

Escuela Universitaria de Dublín, Irlanda

Hoy día se acepta que los responsables policiales de todo el mundo que participan en la investigación de los delitos cibernéticos deberían poseer el nivel de educación más alto. De ser posible, deberían obtener una acreditación oficial de esa educación, lo cual reforzaría su posición cuando prestaran testimonio ante los tribunales.

En 1997 la Escuela Universitaria de Dublín colaboró para crear un programa de un año previo a la obtención de un título en informática forense y seguridad de redes, concebido para la Unidad de investigación del delito informático de la policía irlandesa con el fin de mejorar su capacidad de combatir el delito relacionado con la tecnología. Este programa se mantuvo durante tres años y permitió dar educación técnica específica a funcionarios policiales. La Escuela Universitaria también proporcionó *pro bono* asistencia pericial en causas penales en un momento en que los organismos de defensa de la ley trataban de consolidar su competencia en materia de delito cibernético.

En 2006 la Escuela Universitaria estableció el Centro para la investigación del ciberdelito, instalando con tal fin un laboratorio forense de última generación y creando una licenciatura en informática forense e investigación del ciberdelito.

La licenciatura se desarrolló inicialmente con el material elaborado por conducto de los proyectos AGIS, y se concibió como forma de responder a uno de los objetivos señalados en el informe FALCONE inicial, donde se reconoció la necesidad de una titulación superior para la acción policial en la materia. Como respaldo a la labor en curso de desarrollar, administrar e impartir enseñanza y capacitación, la Universidad proporciona en la actualidad fondos para remunerar a dos funcionarios que trabajan a tiempo completo en el Centro, y los locales que requiere el funcionamiento continuado del mismo.

La licenciatura en informática forense e investigación del ciberdelito del CIDC es un programa de acreditación especialmente diseñado en colaboración con responsables del cumplimiento de la ley. El programa se realiza en base a principios no lucrativos y en la actualidad se limita a funcionarios policiales. Se revisa y actualiza constantemente a fin de mantenerlo al día en relación con las amenazas dimanantes del delito cibernético, y se utilizan continuamente las investigaciones universitarias como apoyo para la creación de contenidos.

Desde que comenzó el programa se han licenciado ya o participan en el mismo más de 60 funcionarios de policía de 15 países. El curso se ha diseñado para el aprendizaje en línea, lo que permite a los participantes, ya ocupados en su profesión, estudiar a las horas y al ritmo que juzguen más oportunos.

Además de dar apoyo a las iniciativas europeas y de la Europol, el Centro para la investigación del ciberdelito de la Escuela Universitaria de Dublín está representado en la delegación irlandesa en el Grupo de trabajo de la Interpol sobre delincuencia relacionada con las tecnologías de la información—Europa. Su participación en este Grupo fue motivo de que se pidiera al Centro que prestara asistencia a la Interpol con diversos fines:

- La Interpol encargó al Centro creado por la Escuela Universitaria que preparase un programa de capacitación que sirviera para que los funcionarios policiales

se convirtieran a su vez en auténticos instructores. Esta iniciativa de desarrollo de la capacidad facilitaría la ampliación de las actividades de investigadores competentes de delitos cibernéticos en las regiones donde más se necesitaran. La Interpol y Microsoft pidieron también al Centro que validase la herramienta de análisis forense COFEE. En la actualidad, los expertos del Centro prueban dicha herramienta y elaboran un paquete de capacitación;

- En mayo de 2008 se pidió al Centro, y este aceptó, que aportara servicios de expertos que participaran en una reunión a fin de analizar los resultados de una operación llevada a cabo por la Interpol, relacionada con la incautación de computadoras pertenecientes al grupo terrorista de las FARC, por parte de las autoridades colombianas;
- Las actividades de colaboración de la Interpol con el Centro establecido por la Escuela Universitaria de Dublín condujeron a la redacción de un memorando de entendimiento entre las dos organizaciones, que estará finalizado en abril de 2009. Se concluirá otro memorando de entendimiento entre la Alianza Internacional Multilateral contra las Amenazas Cibernéticas (IMPACT) y el mencionado Centro.

El Centro también colabora estrechamente con la Organización para la Seguridad y la Cooperación en Europa (OSCE), y en la actualidad prepara un programa de capacitación para servicios policiales que se prevé realizar en Serbia a finales de este año.

Universidad de Tecnología de Troyes, Francia

En Francia se ha emprendido una iniciativa de colaboración específica, que ha dado lugar al establecimiento de relaciones entre organismos policiales y el sector académico. En 2001, la Gendarmería Nacional puso en marcha en su "Centro Nacional de Formación de la Policía Judicial" (CNFPJ) en Fontainebleau, el primer programa de formación de investigadores especializados (conocidos como NTECH). Este programa, de cuatro semanas de duración, evolucionó a lo largo de los años hasta llegar a seis semanas de formación que cubren esferas tales como legislación sobre alta tecnología, investigaciones, análisis forense de computadoras, teléfonos móviles y tarjetas inteligentes, así como relaciones con el sector informático.

Actualmente se invita a dicho sector a participar en la formación de los NTECH. Ello incluye la presentación de estudios a cargo de un proveedor de servicios de Internet francés, las tres compañías francesas de sistemas mundiales de comunicaciones móviles, la asociación francesa de proveedores de servicios de Internet y un productor de contenidos (Canal+) francés, entre otros. La información fluye en ambas direcciones y estas sesiones de capacitación son muy valoradas.

La policía y la gendarmería organizan anualmente un seminario conjunto para sus investigadores especializados (NTECH en el caso de la gendarmería y ESCI en el de la policía). Con frecuencia se invita al sector informático a presentar estudios técnicos.

En 2005 se firmó un acuerdo de asociación con la Universidad de Tecnología de Troyes (UTT) a fin de obtener la acreditación académica de ese programa de capacitación, el cual se ha convertido ahora en una diplomatura universitaria que dura un año (cinco semanas

de clase en el CNFPJ, tres semanas en la UTT y el resto del año destinado al trabajo personal y a la preparación de una tesina sobre un tema técnico o de investigación.

Desde 2006, se seleccionan anualmente cinco investigadores especializados NTECH para que cursen un programa de posgrado que ofrece UTT sobre la seguridad de los sistemas de información (junto con los estudiantes habituales). El propósito de la gendarmería es formar a estas personas en temas que se les plantearán en los contextos informáticos propios de sociedades de mediano a gran tamaño o de entidades públicas.

Esta cooperación ha sido beneficiosa para la calidad y el contenido tanto del diploma universitario como del de posgrado.

Unión Europea

Se alienta al sector privado y a las autoridades responsables del cumplimiento de la ley a colaborar mutuamente en la educación, la capacitación y otras actividades que den apoyo a sus servicios y operaciones.

En 2001 se puso en marcha el proyecto FALCONE titulado "Capacitación: investigación de la ciberdelincuencia—construir una plataforma para el futuro". Se trataba de una iniciativa financiada por la Comisión Europea, que brindó a un grupo de expertos, formado por responsables de cumplir la ley y especialistas del mundo académico, la oportunidad de reunirse a fin de examinar y acordar una serie de recomendaciones para configurar en el futuro la capacitación de investigadores del ciberdelito. Participó como asociado el Centro para la investigación del ciberdelito de la Escuela Universitaria de Dublín.

A esta iniciativa le siguieron los proyectos AGIS de 2003-2006, con los que se llevaron a la práctica las recomendaciones del proyecto FALCONE elaborando programas europeos de capacitación en módulos, debidamente acreditados, para los encargados de cumplir la ley. El Centro de la Escuela Universitaria apoyó estos proyectos facilitando servicios de expertos en contenidos, supervisión académica y acreditación, así como servicios de instructores, acogida de reuniones y formulación de recomendaciones en el informe final.

Otro logro del proyecto FALCONE fue la creación de un grupo de trabajo de ámbito europeo encargado de continuar promoviendo y elaborando programas armonizados de capacitación de los responsables de aplicar la ley, función que cumple el Grupo de Europol de armonización de la capacitación para investigar el delito cibernético, creado en 2007. (Desde sus inicios, el Centro de la Escuela Universitaria de Dublín es miembro del mismo y presta asistencia *pro bono*.) En la actualidad, el Grupo desarrolla dos importantes iniciativas programadas para 2009: la reforma de los programas de capacitación existentes y el proyecto ISEC, de tres años de duración, en virtud del cual 30 funcionarios de servicios de aplicación de la ley recibirán el título de posgrado de la Escuela Universitaria de Dublín en informática forense e investigación de la ciberdelincuencia.

El personal del Centro y la Escuela Universitaria y la policía alemana tienen a su cargo la gestión conjunta del proyecto de reforma. La Escuela ha asumido las tareas de administración financiera del proyecto, será la sede de varias reuniones y proporcionará los servicios de un responsable del diseño de la capacitación para todas las versiones reformadas.

Microsoft, en asociación con la Interpol, la UE, universidades y 15 Estados miembros de la UE, ha contribuido a financiar los proyectos AGIS, lo que manifiesta la colaboración entre las entidades públicas y privadas en la lucha contra la ciberdelincuencia. El proyecto promueve programas normalizados de capacitación y redes de información entre los países participantes. Los proyectos AGIS concluyeron y fueron sucedidos por el proyecto ISEC en el marco del nuevo programa de "Prevención y lucha contra la delincuencia integrado en el programa general Seguridad y defensa de las libertades". Microsoft se dispone a participar en este nuevo programa.

Proyecto 2CENTRE, financiado por la Comisión Europea

Una red de centros de excelencia para la capacitación, estudio y educación sobre técnicas de investigación de la ciberdelincuencia (2CENTRE) permitirá elaborar y difundir cursos de formación, con la correspondiente acreditación, adaptables a un marco estructurado y sostenible. El programa da respaldo a la estrategia y el programa de participación paritaria de la Comisión Europea, descrito en su último comunicado "Hacia una política general de lucha contra la ciberdelincuencia", COM (2007) 267, de 22 de mayo de 2007, uno de cuyos objetivos era la necesidad de establecer una acción coordinada para la formación de autoridades judiciales y policiales en estos temas. El proyecto también tiene en cuenta que hay personas en el sector informático que combaten el ciberdelito pero no tienen acceso a programas de capacitación y educación establecidos anteriormente. El mencionado sector, las instancias judiciales y policiales, así como el ámbito académico, son los tres protagonistas principales en esta empresa, y los centros nacionales se desarrollarán en el seno de esta colaboración tripartita. Los profesionales del sector de la ciberdelincuencia tendrán oportunidad de participar en programas de capacitación y educación junto con sus homólogos de servicios judiciales y policiales, así como de contribuir a la creación de nuevos módulos de formación y programas educativos. Otra característica importante del proyecto es la investigación científica de la ciberdelincuencia y el desarrollo de programas informáticos. Se prevé que los diferentes centros tendrán oportunidades de colaborar para el logro de los objetivos comunes.

El proyecto comenzará con dos centros nacionales en Francia e Irlanda, y permitirá crear un centro de coordinación, cuyo trabajo incluirá el establecimiento del mandato de la red, así como de procedimientos comunes que respeten las tradiciones jurídica y cultural nacionales de los participantes actuales y futuros en la red y el desarrollo de métodos de puesta en marcha, control de calidad y otras actividades conexas.

Cada centro nacional trabajará en su propia lista de tareas acordada por los asociados. Las tareas tendrán por objeto mejorar la capacidad de lucha contra la ciberdelincuencia dentro de la UE y fuera de sus límites. Para cada componente del proyecto habrá un consejo asesor que proporcionará orientaciones claras.

La labor se realizará por medio de reuniones e intercambio de visitas y recursos como sitios web para su uso compartido con el equipo encargado del proyecto o con las partes interesadas. Cada proyecto particular dentro del programa general tendrá su propio plan, calendario y equipo de trabajo. Los progresos serán supervisados periódicamente por la junta asesora del respectivo proyecto y el centro de coordinación. El concepto y los planes relativos a 2CENTRE se expondrán en las conferencias y seminarios en que así proceda, con el propósito de obtener apoyo y nuevos miembros.

Como resultado de ese proyecto, financiado por la CE, se establecerán mandatos, prácticas óptimas, así como procedimientos comunes y recomendaciones para el funcionamiento futuro de 2CENTRE. Otros resultados serán un acuerdo con la Europol para intercambiar material de capacitación, un sitio web del proyecto totalmente operativo, una serie de módulos de capacitación en formato CD que se pondrán a disposición de todos los asociados en la iniciativa 2CENTRE, herramientas forenses informáticas listas para su uso, documentos de validación de herramientas, manuales de instrucción o paquetes de capacitación para cada herramienta, publicación de informes que se distribuirán para uso de los asociados en 2CENTRE, elaboración de cursos de aprendizaje en línea, especificaciones sobre la propiedad intelectual destinadas a las partes involucradas, mejora de los programas de formación y educación existentes, así como traducción de una serie de módulos y folletos de productos a otros idiomas.

Consejo de Europa

A fin de combatir la delincuencia cibernética y proteger los sistemas informáticos, las autoridades gubernamentales deberán prever las siguientes medidas:

- Penalización efectiva de ese tipo de delitos. La legislación de los diferentes países debe armonizarse al máximo posible para facilitar la cooperación;
- Procedimientos de investigación y enjuiciamiento, así como capacidad institucional, que permitan a las instancias de justicia penal hacer frente a la delincuencia de alta tecnología;
- Condiciones que faciliten la cooperación directa entre las instituciones estatales, y entre estas y el sector privado;
- Regímenes eficaces de asistencia judicial recíproca, que permitan la cooperación directa entre numerosos países.

El Convenio sobre ciberdelincuencia (STE 185) del Consejo de Europa facilita a los países la tarea de responder a estas necesidades. Se abrió a la firma en noviembre de 2001 y, en diciembre de 2008, había sido ratificado por 23 países y firmado por otros 23. El Protocolo adicional al Convenio sobre la ciberdelincuencia, relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE 189) de enero de 2003, había sido ratificado por 13 Estados y firmado por otros 21. Igualmente importante es que un gran número de países de todas las regiones utilizan el Convenio como guía o modelo legal para mejorar su legislación sobre el delito cibernético.

Con el fin de ayudar a todos los países en general a dar aplicación a este tratado, el Consejo de Europa puso en marcha en 2006 el Proyecto sobre la Ciberdelincuencia (www.coe.int/cybercrime), financiado con cargo al presupuesto del Consejo de Europa y a contribuciones de Estonia y Microsoft. La segunda fase de este proyecto comenzará en marzo de 2009 y se extenderá hasta junio de 2011.

En el marco del proyecto, el Consejo de Europa presta apoyo para la capacitación en materia de:

- Legislación sobre la ciberdelincuencia;

- Cooperación internacional policial y judicial;
- Cooperación entre los responsables del cumplimiento de la ley y los proveedores de servicios;
- Enjuiciamiento y fallo judicial en la esfera de la ciberdelincuencia;
- Adiestramiento de jueces en temas de ciberdelincuencia y pruebas electrónicas, incluido el abuso de menores en línea[51], actividad realizada en Egipto del 6 al 10 de diciembre de 2009.

Centro Internacional de Estudios sobre el Ciberdelito de la Universidad Simon Fraser (Canadá)

En el campus de esta Universidad en Surrey se ha establecido un nuevo Centro de estudios para la lucha contra la ciberdelincuencia, que cuenta con una subvención de 350.000 dólares aportada por el Gobierno provincial. El Centro es una iniciativa conjunta de la Universidad mencionada, las autoridades provinciales y la Sociedad Internacional para la Ordenación del Ciberespacio (POLCYB), organización sin ánimo de lucro con sede en Columbia Británica, cuyo objetivo es prevenir y combatir los delitos en Internet. El Centro de estudios para la lucha contra la ciberdelincuencia investigará las tendencias de los delitos informáticos y prestará asistencia para crear nuevas herramientas destinadas a actuar contra ellos. Uno de los proyectos iniciales que se propone realizar es el desarrollo de herramientas tipo escáner de virus para detectar material relacionado con la explotación infantil.

La Universidad Simon Fraser aportará al nuevo Centro experiencia en diversas disciplinas como la informática, la ingeniería y la criminología. Dado que, según se ha afirmado, no existe ninguna universidad en América del Norte de la que se sepa que imparta un programa de estudios expresamente dedicado a la ciberdelincuencia, se espera una enorme demanda a nivel de grado y de posgrado, así como de los cursos profesionales de formación continua debidamente acreditados.

Naciones Unidas

La Oficina de las Naciones Unidas contra la Droga y el Delito trabaja en la elaboración de un proyecto titulado “Establecimiento y fortalecimiento de marcos jurídicos y normativos para hacer frente a la ciberdelincuencia en los países en desarrollo”.

El plan propuesto, que se centrará en los países en desarrollo, es de gran alcance y tendrá como base los conocimientos especiales y la experiencia de los asociados que ya trabajan en ese terreno. Su objetivo es luchar contra los delitos informáticos de las siguientes maneras:

- Ayudando a los Estados Miembros a adoptar legislación adecuada que constituya una base sólida para la investigación y persecución de dichos delitos;

[51] www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (última consulta: 10 de enero de 2010).

- Fomentando los conocimientos técnicos y operativos de los jueces, fiscales y autoridades de aplicación de la ley sobre cuestiones relacionadas con el delito cibernético;
- Impartiendo capacitación a los profesionales judiciales para que utilicen con eficacia los mecanismos de cooperación internacional destinados a combatir la ciberdelincuencia;
- Intensificando la sensibilización de la sociedad civil y creando impulso entre las autoridades decisorias para que aúnen esfuerzos con el fin de prevenir y combatir los delitos cibernéticos.

El aspecto esencial a los efectos del presente estudio es el segundo objetivo, que refleja la labor desarrollada en otras iniciativas. La UNODC es miembro pleno del Grupo de trabajo de Europol para la armonización de la formación en investigación de la delincuencia cibernética, y resultará directamente beneficiada con la creación de la red de centros de excelencia que se ha propuesto.

La UNODC colabora asimismo con el Instituto Coreano de Criminología a fin de crear un foro virtual sobre ciberdelincuencia que ofrezca posibilidades de capacitación e investigación. El sector informático también participa como socio en este proyecto y aporta fondos para la infraestructura del foro.

Centro Internacional para Menores Desaparecidos y Explotados/Interpol/ Microsoft

El seminario de capacitación sobre delincuencia contra menores de edad facilitada por vía informática se organizó con el propósito de ofrecer a los responsables de aplicar la ley en todo el mundo herramientas y técnicas apropiadas para investigar los casos de explotación de menores a través de Internet. Esta iniciativa se puso en marcha en diciembre de 2003 en la sede de Interpol en Lyon (Francia). En noviembre de 2008, un total de 3.221 funcionarios policiales de 113 países habían participado en ella, en 36 centros regionales de capacitación en Francia, Costa Rica, Brasil, Sudáfrica, Croacia, RAE de Hong Kong, Rumania, España, Jordania, Argentina, Federación de Rusia, Nueva Zelandia, Tailandia, Turquía, Japón, Noruega, China, Bulgaria, Australia, Omán, India, Lituania, Marruecos, Qatar, Panamá, Filipinas, Polonia, Perú, República Checa, Grecia, Ucrania, República de Corea, Egipto, Brasil, Colombia e Italia.

El seminario de cuatro días de duración incluye los siguientes módulos:

- Explotación de menores facilitada por vía informática;
- Investigación del abuso de menores en línea;
- Organización de medidas policiales de respuesta a la delincuencia contra menores facilitada por vía informática;
- Actuación penal contra los delincuentes;
- Aspectos técnicos de la investigación;
- Recursos y ponentes invitados.

Se ofrece al patrocinador responsable de financiar la iniciativa la oportunidad de participar activamente en esta parte de la capacitación. Asimismo, se modifica el programa de estudios para adaptarlo a las necesidades (culturales, jurídicas, lingüísticas, en la esfera de aplicación de la ley, etc.) del país anfitrión.

Además, el Centro Internacional para Menores Desaparecidos y Explotados se encarga en la actualidad de la función operativa del Sistema de seguimiento de la explotación infantil creado por Microsoft como ayuda para las investigaciones sobre el delito cibernético.

El mencionado Centro participa también en la alianza financiera, en cuyo contexto trabaja con el sector de servicios financieros a fin de crear un mecanismo de denuncia de operaciones ilegales como la compra en línea de pornografía infantil, e impartir capacitación a las fuerzas policiales sobre este mecanismo.

Iniciativas del sector informático

Desde 2003 la Asociación francesa de proveedores de acceso y servicios de Internet viene participando en sesiones de capacitación sobre la cooperación entre esos proveedores y los responsables del cumplimiento de la ley, organizadas por investigadores especializados en delitos de alta tecnología (NTECH) y la Escuela Nacional Francesa de la Magistratura.

En agosto de 2006, Microsoft abrió un portal web destinado a los responsables de aplicar la ley de todo el mundo. El portal (www.microsoftlawportal.com) se diseñó de tal modo que proporcionara a dichos responsables fácil acceso a los materiales y recursos de capacitación relacionados con la ciberdelincuencia. Es una respuesta al creciente volumen y variedad de las solicitudes de entidades judiciales y policiales a Microsoft relativas a programas, juegos o servicios en línea de la empresa. Los materiales incluyen resúmenes sobre diversas amenazas en línea, entre ellas las referentes a seguridad infantil, peska, programas espía, correo basura y códigos maliciosos, e información sobre las organizaciones, asociaciones y otros recursos disponibles para ayudar a los defensores de la ley a entender, investigar, prevenir y enfrentar esas amenazas.

En diciembre de 2004, Microsoft anunció el establecimiento de Digital PhishNet (DPN), una alianza de entidades responsables de aplicar la ley y líderes de diversos sectores industriales como los de tecnología, banca, servicios financieros y subastas en línea. La finalidad de esta alianza es específicamente intercambiar información en tiempo real sobre los "peskadores" para facilitar su identificación, detención y procesamiento. La DPN es el primer grupo de este tipo centrado en la prestación de asistencia a los organismos de aplicación de la ley para detener y enjuiciar a los responsables de delitos de peska contra los consumidores.

Esta alianza sirve de foro para el debate imparcial, confidencial y con fines de colaboración entre los sectores público y privado, en el que es posible intercambiar información sobre los casos y tendencias en materia de peska y otras amenazas cibernéticas conexas en un ambiente de confianza, analizarla y transmitirla a los responsables de aplicar la ley y diversos servicios antipeska, de modo que se plasme en medidas enérgicas de protección y disuasión legal de futuros delitos en línea. La función rectora corre a cargo de National Cyber-Forensic & Training Alliance (NCFTA), organización público-privada sin ánimo de lucro de los Estados Unidos, que cuenta con personal perteneciente a entidades de

represión de la delincuencia y al sector informático. La NCFTA ofrece capacitación y apoyo a los defensores de la ley; asimismo, sirve como plataforma de contacto entre estos y los expertos del sector para la realización de análisis y actividades forenses. Es financiada y respaldada por sus miembros. La DPN organiza sesiones privadas del sector informático y los responsables de aplicar la ley para facilitar la cooperación. Tras las reuniones de Chicago en 2005 y Nueva Orleans en 2006, la DPN amplió su esfera de acción a Europa, con una reunión en Berlín en junio de 2007, y a Asia, con otra reunión en Singapur en enero de 2008. Volvió a reunirse en los Estados Unidos en San Diego, California, en septiembre de 2008.

Microsoft ha elaborado material para ayudar a los funcionarios judiciales y policiales a comprender la manera de utilizar la tecnología y los programas informáticos disponibles para investigar la ciberdelincuencia. Este material incluye información relativa a los detalles técnicos de los productos de Microsoft y orientaciones para llevar a cabo investigaciones en computadoras y otros aparatos utilizando programas de Microsoft.

En octubre de 2006 Microsoft dio acogida a la conferencia "LETech 2006" en su sede de Redmond, Washington. El objetivo de este acto, al que asistieron cerca de 300 autoridades judiciales y policiales provenientes de más de 45 países, fue presentarles las últimas iniciativas de Microsoft en ayuda de las investigaciones sobre el delito cibernético, entre ellas el Sistema de seguimiento de la explotación infantil, el nuevo portal de Microsoft para la aplicación de la ley y los programas Microsoft de apoyo a esa aplicación.

En enero de 2008, Microsoft, eBay, PayPal y Skype impartieron durante cinco días capacitación sobre programas maliciosos y redes infectadas a más de 40 investigadores experimentados en materia de delito informático de países de la Unión Europea. En junio de 2006, Microsoft organizó con Europol un curso de capacitación de cuatro días para 24 investigadores sobre delincuencia de alta tecnología de 15 países miembros y 12 personas más del Centro de delincuencia de alta tecnología y otras unidades especializadas de Europol. El curso abarcó las aplicaciones avanzadas de Windows XP Forensics, ampliamente superiores a las de las herramientas disponibles, metadatos y técnicas de ocultación MS Office, detección y análisis de redes infectadas y programas maliciosos, avance y demostración de Windows Vista Security, así como la respuesta del equipo del Instituto India-China a la amenaza de los programas maliciosos. Se concedió el acceso y también se analizó la aplicación de Microsoft Windows Vista BETA.

En lo que respecta a actividades de formación, Microsoft es patrocinador o anfitrión de ellas en todo el mundo en relación con diversas amenazas, el fomento de la capacidad y la protección de menores. Son ejemplos los siguientes:

- El grupo International Botnet Taskforce, que se inició en 2004 y celebra una reunión anual a la que asisten responsables del cumplimiento de la ley, interesados del sector informático, investigadores en temas de seguridad y empresas privadas, con objeto de analizar formas de colaboración en esta colectividad dirigidas a contrarrestar la amenaza de las redes infectadas. En esta serie de conferencias, considerada una de las primeras en su género, participan especialistas de la más alta reputación en sus respectivas esferas. La octava reunión tuvo lugar el 21 de octubre de 2008 en Arlington, Virginia (Estados Unidos).

Con representantes de cerca de 40 países y casi 200 asistentes, la reunión tuvo una de las mayores y más selectas concurrencias en los cuatro años de su historia, constituida por participantes que asistían por primera vez y miembros que ya habían estado presentes desde los comienzos.

- Law Enforcement Tech 2006 y 2008: esta actividad consistió en una capacitación intensiva durante tres días ideada para proporcionar a los responsables de aplicar la ley herramientas de la tecnología más avanzada e información para las investigaciones sobre la delincuencia cibernética. La conferencia se centró en los detalles y conocimientos especiales técnicos relativos a los productos y servicios de Microsoft más recientes.

Por medio de esa actividad y sesiones de formación similares, Microsoft ha colaborado en la capacitación de más de 6.000 funcionarios de órganos de aplicación de la ley de más de 110 países de todo el mundo (incluidos 1.500 funcionarios en los Estados Unidos) y tiene posibilidades de proporcionar las herramientas y aptitudes técnicas necesarias para identificar a delincuentes cibernéticos.

Entre las iniciativas de eBay figuran:

- El apoyo a la Comisión Nigeriana de Delitos Económicos y Financieros;
- Actividades de capacitación de 60 jueces y fiscales del ámbito penal organizadas por la Administración de Justicia de Berlín;
- Una conferencia/sesión de capacitación conjunta llevada a cabo por eBay, CBI e Interpol para 350 altos funcionarios de servicios de aplicación de la ley en la India;
- La capacitación de la mayoría de los detectives del Organismo contra la Delincuencia Organizada Grave del Reino Unido durante todo el año;
- Sesiones de "Formación de instructores" del Instituto Nacional de Magistrados de Bucarest (Rumania), para dos grupos de jueces y fiscales, mediante programas organizados en eBay, Reino Unido, o programas de acción exterior impartidos en sus redes u oficinas locales;
- La capacitación en 2009 de más de 1.700 funcionarios de servicios responsables del cumplimiento de la ley en el Reino Unido o países afines.

Estadísticas significativas de eBay

- 85 millones+ de usuarios activos en todo el mundo
- Volumen de negocios de 2.000 dólares por segundo
- 110 millones+ de listados activos en cualquier momento
- Venta diaria de 1.500 coches a través de eBay
- Venta diaria de 12.000 a 13.000 pares de zapatos

Estudio presentado por Tiberius Rusu, eBay Europa, en el Taller de expertos nacionales sobre un enfoque global de la seguridad cibernética, organizado por la OSCE los días 23 y 24 de noviembre de 2009.

La capacitación para la investigación del fraude impartida por eBay se centra en los siguientes temas:

- Presentación del equipo de eBay encargado de investigar el fraude;
- Comprensión de las prácticas de fraude;
- Estudio de casos de investigación del fraude;
- Interacción con el equipo de eBay encargado de investigar el fraude;
- Presentación de solicitudes conforme a la Ley de protección de datos;
- Solicitudes urgentes;
- Pruebas potencialmente disponibles y sugerencias sobre lo que interesa solicitar;
- Comprensión de las pruebas presentadas;
- Solicitud de declaraciones de testigos;
- Solicitud de testimonio ante un tribunal;
- Visión general de la página de eBay para la aplicación de la ley;
- Portal para la aplicación de la ley;
- Criterios de admisibilidad;
- Campos de búsquedas de usuarios;
- Limitaciones de la búsqueda;
- Realización de investigaciones encubiertas.

Otras iniciativas

Existe una serie de programas de capacitación sobre la ciberdelincuencia establecidos por organismos responsables de hacer cumplir la ley europeos, impartidos con frecuencia en centros nacionales y destinados principalmente a funcionarios de esos organismos. Además, hay programas que prevén la participación tanto de funcionarios responsables de aplicar la ley como de representantes del sector informático.

Varios de ellos están a cargo de organizaciones sin ánimo de lucro, tales como la Asociación de Investigadores de la Delincuencia de Alta Tecnología y la Asociación Internacional de Especialistas en Investigaciones Informáticas, ambas originarias de los Estados Unidos y con ramificaciones internacionales. Existen programas de capacitación prestigiosos que se ofrecen al sector informático y a los responsables de aplicar la ley. Quizá los más conocidos sean los del Instituto SANS de los Estados Unidos.

Actividades de capacitación existentes en la actualidad

Las actividades de capacitación en materia de informática forense e investigación de la ciberdelincuencia existentes actualmente para responsables del cumplimiento de la ley se dividen en las siguientes categorías:

- Programas nacionales y regionales como los ofrecidos en el Reino Unido, Bélgica, Alemania, el Canadá, los Estados Unidos y Francia, entre otros;
- Aportaciones de invitados internacionales a dichos programas;
- Talleres de formación celebrados en conferencias sobre el delito cibernético;
- Capacitación impartida por organizaciones internacionales de policía como Interpol y Europol;
- Iniciativas del sector informático en apoyo a las actividades de personal responsable del cumplimiento de la ley;
- Aportaciones de vendedores de programas y equipo físico informáticos;
- Iniciativas promovidas por autoridades nacionales y organizaciones internacionales;
- Labor de formación desarrollada por participantes en una o más de las iniciativas mencionadas;
- Capacitación ofrecida a consecuencia de iniciativas como los programas Falcone/Agis/ISEC financiados por la CE;
- Formación en materia de legislación sobre la ciberdelincuencia, promovida por el Consejo de Europa, el Departamento de Justicia de los Estados Unidos, la Organización de Estados Americanos y otros.

La capacitación se ha desarrollado tradicionalmente de manera aislada, con escasa colaboración. Por esa razón se creó el programa inicial FALCONE relativo al ciberdelito. Se constató que muchos países y organizaciones utilizaban módulos de formación casi idénticos. Esto se consideró un despilfarro de los escasos recursos disponibles y la idea motora del proyecto fue establecer un marco que permitiera desarrollar la capacitación por la vía de la colaboración e impartirla y ponerla gratuitamente a disposición de los responsables de aplicar la ley en todo el mundo.

En la actualidad existen siete cursos de ese tipo que han superado la fase experimental y están disponibles para los usuarios. Han sido traducidos a varios idiomas, incluidos en programas nacionales de capacitación y distribuidos en muchas partes del mundo. Sin embargo, no existe un organismo coordinador que garantice la permanencia de los estándares de calidad y que el material que se imparte esté actualizado y, cuando esté traducido, se haga llegar al mayor público posible. Actualmente la función de distribución de los materiales en Europa se encuentra a cargo de Europol, y para el resto del mundo, de Interpol. No existe una campaña para explotar comercialmente su disponibilidad.

En el pasado ha habido otras tentativas para coordinar las actividades de capacitación, tales como la del Grupo de Acción Internacional para la Formación sobre Ciberdelincuencia, una iniciativa de la Academia de Policía del Canadá emprendida con la participación de centros afines de una serie de países de habla inglesa. Esta iniciativa y otras similares no tuvieron éxito porque no había medios para encargarse continuamente de las actividades. He aquí otro ejemplo de la necesidad de que exista una red coordinadora para cualquier solución internacional.

VI. LÍMITES DE LA COOPERACIÓN

1. Limitaciones legales

Las colaboraciones entre el sector público y el privado son de efectividad limitada.

Legislación sobre protección de datos

Puesto que ninguna de las partes en la relación puede adoptar medidas contrarias a la ley, surgen dificultades importantes cuando el intercambio de información requiere modificar la legislación para que lo permita. Esto depende de la naturaleza de los datos en cuestión y del marco legislativo al que están sujetos tanto los datos como el intercambio.

Cuando investigan un fraude, las autoridades encargadas de hacer cumplir la ley necesitan con frecuencia tener acceso a grandes volúmenes de datos de clientes que podrían verse afectados o relacionados con una actividad delictiva en línea, especialmente en el caso de fraude de identidad y delincuencia económica. Estos datos son propiedad de un proveedor de servicios de Internet que puede tenerlos almacenados en el país donde se lleve a cabo la investigación o en un lugar diferente. Por ejemplo, eBay tiene un apéndice de normativa sobre privacidad—Intercambio de datos[52], donde se delimita claramente la información que se suministrará a terceros.

Tipo de información	Miembros titulares de derechos de propiedad (VeRO)	Proveedores de servicios internos	Vista pública	Usuarios en una operación	Organismos de aplicación de la ley y gubernamentales
Información de contacto					
Nombre completo	Sí	Sí		Sí	Sí
Identificación de usuario	Sí	Sí	Sí	Sí	Sí
Dirección de correo electrónico	Sí	Sí		Sí	Sí
Calle	Sí	Sí		Sí	Sí
Estado	Sí	Sí	Sí	Sí	Sí
Ciudad	Sí	Sí		Sí	Sí
Código postal	Sí	Sí		Sí	Sí

[52] http://pages.ebay.com/help/policies/privacy-appendix.html (última consulta: 10 de enero de 2010).

Tipo de información	Miembros titulares de derechos de propiedad (VeRO)	Proveedores de servicios internos	Vista pública	Usuarios en una operación	Organismos de aplicación de la ley y gubernamentales
Información de contacto					
Teléfono	Sí	Sí		Sí	Sí
País	Sí	Sí	Sí	Sí	Sí
Empresa	Sí	Sí		Sí	Sí
... 14 conceptos más en esta categoría					
Información financiera					
7 conceptos en esta categoría					
Información sobre la expedición					
5 conceptos en esta categoría					
Información sobre la operación					
7 conceptos en esta categoría					
Datos informáticos generados					
10 conceptos en esta categoría					
Varios					
3 conceptos en esta categoría					

Es digna de elogio la publicación transparente de esta relación detallada de datos almacenados. Vale la pena señalar que en el caso de eBay llega a 27 la lista de empresas de todo el mundo pertenecientes a la cadena de proveedores de servicios de Internet que tendrán acceso a todos los datos.

Leyes sobre la competencia

Las leyes sobre la competencia pueden ser un verdadero problema cuando todos los actores del sector informático colaboran estrechamente para crear una norma o una respuesta común a las condiciones específicas del mercado. Es necesario actuar con gran precaución para asegurarse de que todas las medidas que se adopten sean legal y económicamente viables para todos los actores en el mercado y que estos no podrán ser considerados como cartel comercial. Por ejemplo, durante las negociaciones sobre el Código de Práctica para el sector de Internet en Irlanda[53], hubo largas deliberaciones sobre cómo los proveedores de servicios de Internet deberían tratar a los clientes que abusaban de un proveedor y luego se cambiaban a otro. Las leyes sobre la protección de datos y la competencia imponían restricciones a las formas en que los proveedores de servicios de Internet podían intercambiar dicha información.

Las normativas sobre competencia de la Comisión Europea se estipulan en el Tratado de Roma, especialmente en los artículos 81 y 82[54].

[53] www.ispai.ie/docs per cent5Ccope.pdf (última consulta: 10 de enero de 2010).
[54] http://en.wikipedia.org/wiki/Treaties_of_Rome (última consulta: 10 de enero de 2010).

Artículo 81 (antiguo artículo 85)
El apartado 1 del artículo 81 prohíbe los acuerdos, prácticas concertadas y decisiones de empresas que puedan afectar al comercio entre los Estados miembros y tengan por objeto o efecto impedir, restringir o falsear el juego de la competencia. El apartado 2 del artículo 81 dispone que los acuerdos o decisiones prohibidos por el presente artículo sean nulos de pleno derecho. El apartado 3 del artículo 81 estipula que la Comisión (y únicamente la Comisión) podrá declarar inaplicable la prohibición del apartado 1 si se cumplen determinados requisitos.

Artículo 82 (antiguo artículo 86)
El artículo 82 prohíbe la explotación abusiva de una posición dominante en el mercado común o en una parte sustancial del mismo, en la medida en que pueda afectar al comercio entre los Estados miembros.

Artículo 86 (antiguo artículo 90)
El artículo 86 confirma que las actividades de las empresas públicas y aquellas empresas a las que los Estados concedan derechos especiales o exclusivos, también estarán sujetas a las normas del Tratado sobre competencia. El artículo también establece que no debe haber monopolios que gocen de protección estatal a menos que sean de interés público.

Derechos humanos

El intercambio de información y datos entre organismos gubernamentales y entidades responsables de aplicar la ley puede llegar a plantear dificultades en algunos países donde no siempre reinan el estado de derecho y los principios democráticos. Los derechos humanos son un aspecto esencial que tener en cuenta cuando, como resultado de la asociación entre el sector público y el privado, se forman lo que en el fondo son espacios de intercambio de información sensible cerrados y faltos de transparencia. Por lo tanto, es fundamental prestar atención en ellos a las cuestiones de transparencia y rendición de cuentas, tal vez mediante la presentación de informes periódicos o el establecimiento de un mecanismo de supervisión pública. Un consejo consultivo podría encargarse de supervisar y orientar la estrategia de esa asociación.

Relaciones sin roces

Cuando los principales interesados, es decir, las autoridades gubernamentales, los proveedores de servicios de Internet y los responsables de aplicar la ley, acuerdan intercambiar información y formular políticas con regularidad a fin de garantizar la eficacia en la investigación del delito, puede haber ocasiones en que esas iniciativas se perciban como algo falto de equilibrio y que, a la larga, no sirva a los intereses de una democracia transparente y consciente de su responsabilidad.

Reflejo de una reacción nacional a iniciativas de tal índole es un artículo aparecido el 25 de septiembre de 2009 en el *Irish Times* bajo el título "Alarmante memorando sobre retención de datos". La periodista Karlin Lillington escribía:

> Un acuerdo "privado" de retención de datos se basa en supuestos generales, no en artículos de la ley. Un memorando de entendimiento secreto entre organismos del Estado y el sector de las comunicaciones sobre la manera de aplicar la aún inexistente legislación gubernamental sobre retención de datos confirma las ya antiguas preocupaciones acerca de quién maneja los temas de la retención de datos y con qué propósito.
>
> En lo tocante a la retención de datos, parece que es la cola la que mueve al perro, en flagrante menosprecio del correcto proceso legislativo democrático. Los organismos que desean acceder a nuestros datos de llamadas y de Internet están esquivando la acción del Parlamento (Oireachtas) que al menos en teoría es la institución que elabora y aplica las leyes.
>
> Como me dijo un defensor de la privacidad alarmado: "esto es legislar por decreto". El "Memorando de entendimiento", visto por el *Irish Times*, es del 17 de agosto y fue redactado en colaboración "entre el sector de las comunicaciones y los órganos del Estado siguientes: Comisionado de la Policía Nacional (An Garda Síochána), Fuerzas de Defensa Permanente y Comisionados de Hacienda", como se indica en el párrafo inicial del memorando.

El artículo recibió varias respuestas en la edición del *Irish Times*[55] del 2 de octubre de 2009:

Rossa McMahon afirmó que:

> Cabe señalar, sin embargo, que su último informe, relativo a un acuerdo secreto entre organismos estatales y empresas de telecomunicaciones para intercambiar con el Estado más información que la prescrita por la ley, se relega a la sección de Economía (*Business This Week*, 25 de septiembre). Este acuerdo secreto no solo es alarmante, sino que es escandaloso, incluso aunque el secretismo del Estado en sus tratos ya no nos sorprende.

Ronan Lupton, Presidente de Operadores Alternativos en el Mercado de las Comunicaciones; Paul Durrant, Director General de la Asociación de Proveedores de Servicios de Internet de Irlanda; y Tommy McCabe, Director de la Federación de Telecomunicaciones e Internet, en representación del sector de las telecomunicaciones e Internet de Irlanda respondieron que:

> Este proyecto de memorando es muy conveniente porque también tiene como objetivo establecer el principio de un punto de contacto único, lo cual debería servir para minimizar errores y abusos. El memorando no tiene nada de "secreto", simplemente se encuentra todavía en la etapa de negociación y no es público.

Es esencial que toda asociación del sector público y el privado con el objetivo de combatir la delincuencia en la sociedad o en Internet cuente con la presencia de organizaciones diversas, en particular las responsables de la protección de datos, los derechos humanos, etc.

[55] www.irishtimes.com/newspaper/letters/2009/1002/1224255674433.html (última consulta: 10 de enero de 2010).

2. Restricciones en el plano internacional

A nivel internacional existe una variedad de restricciones que las asociaciones del sector público y privado no siempre tienen en cuenta. El intercambio transfronterizo de información sobre datos que tal vez tengan repercusiones en la seguridad nacional podría ser motivo para impedir o interrumpir dicho intercambio. Las investigaciones que requieren pruebas admisibles ante un tribunal han de realizarse en conformidad con las estrictas exigencias del "encadenamiento de material probatorio".

3. Limitaciones de la capacidad

La actuación de las diversas entidades puede verse limitada por una serie de razones.

Competencia entre las empresas

Muchos de los principales interesados del ámbito empresarial compiten entre sí. Se unen para abordar problemas que preocupan a la sociedad, pero también son temas que en un momento u otro se convierten en cuestiones importantes de competencia. Por ejemplo, algunas empresas se esfuerzan por proyectar una imagen familiar y amistosa a través de los servicios que ofrecen y de sus actividades de comercialización y publicidad. El mercado interno tiene una importancia fundamental y lo creen motivado por deseos de seguridad, protección y confianza. Cuando lo comprenden a fondo, tras unos gastos y tiempo considerables, y consiguen conocimientos únicos sobre cómo satisfacer ese mercado básico, una asociación público-privada cuyo objetivo es facilitar y hacer posible esa especialización para todo el mercado puede resultar una verdadera amenaza para este modelo de negocio.

Restricciones al intercambio de información en el plano jurídico

Muchos organismos responsables de aplicar la ley están sujetos a importantes restricciones institucionales o jurídicas en cuanto al intercambio de información con entidades de otros ámbitos, lo que posiblemente limitará la variedad de asociaciones y alianzas a las que se puedan adherir.

VII. CONCLUSIÓN

1. Medidas que funcionan

Las asociaciones entre los sectores público y privado para responder a la delincuencia, tanto en línea como por vías corrientes, son la medida más eficaz contra la compleja actividad delictiva actual, especialmente en la esfera del hurto de identidad y el delito económico.

Intercambio de conocimientos y especialización

Estas asociaciones aportan una variedad de conocimientos, aptitudes y experiencias de diversa procedencia, por ejemplo del sector informático, entidades gubernamentales, de derechos humanos, de aplicación de la ley y legislativas, lo que en general aumenta la efectividad global de la asociación, dado que las organizaciones que normalmente operan en solitario no pueden abarcar todas estas esferas. Cada organización participante posee información y conocimiento, los cuales, si se intercambian, pueden brindar una visión más completa de la actividad delictiva y, en algunos casos, aportar pruebas admisibles por los tribunales. La cooperación asegura una mínima duplicación de tareas, un intercambio e investigación de alta calidad, que se comparten con otros participantes en la red de manera que garantice la coherencia y las posibilidades de ampliación a escala respetando sensibilidades culturales y lingüísticas.

Coordinación independiente

La colaboración de los sectores público y privado hace necesaria una coordinación independiente. Si no se cuenta con ella, la coordinación entre instancias internacionales es limitada y depende de unas pocas personas que impulsen las actividades. Es necesaria una coordinación adecuada, organizada y plenamente dedicada a su fin, para estimular el intercambio, extender la cooperación a nuevas organizaciones y nuevos países cuando proceda, afianzar las relaciones externas con organismos y actividades transnacionales, así como promover la labor de la asociación. La financiación es con frecuencia un gran problema para esos centros coordinadores, que necesitan un amplio y prolongado apoyo financiero y de asesoramiento para ser sostenibles.

2. Medidas que no funcionan

Las asociaciones basadas en intercambios desiguales, niveles de poder dispares o no fundadas en la comprensión y el respeto mutuos encontrarán muchos obstáculos e inconvenientes a la hora de colaborar entre sí. En situaciones de crisis habrá divisiones y marginalización, a menos que se definan claramente los papeles y las relaciones. Es un error considerar que tales asociaciones público-privadas solucionarán por sí mismas todos los problemas relacionados con el hurto de identidad. Es necesaria una legislación actualizada, iniciativas internacionales, una coordinación internacional en la aplicación de la ley y una autorregulación y códigos de prácticas acordados del sector informático.

3. Perspectivas

- Las asociaciones entre el sector público y el privado necesitan apoyo y estímulo.
- La coordinación internacional sostenible de esas asociaciones es un problema de gran importancia.
- Las nuevas generaciones de programas maliciosos son cada vez más sofisticadas. Las redes infectadas son muy flexibles y se utilizan para fines múltiples como: obtener dinero (alquiler, extorsiones, espionaje industrial, etc.), robar datos personales o financieros, impulsar los ardides de "ingeniería social" (la peska y sus variedades), lanzar oleadas de correos basura, amenazar a víctimas y atacar infraestructuras de redes de información cruciales. El peligro acecha en todas partes y la prevención es una tarea difícil[56].

[56] *Sr. Nicole Dilone*, "European Alert Platform", Centro contra la delincuencia de alta tecnología, Europol, con ocasión del Diálogo público-privado para la lucha contra las actividades ilegales en línea, acogido por la Comisión Europea en Bruselas, 27 de noviembre de 2009.

GUÍA PRÁCTICA PARA LA COOPERACIÓN INTERNACIONAL PARA COMBATIR EL DELITO RELACIONADO CON LA IDENTIDAD*

Marco Gercke
Raluca Simion

* La presente Guía fue preparada por el Dr. Marco Gercke y el Dr. Raluca Simion en nombre de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), y de conformidad con las recomendaciones del grupo básico de expertos sobre el delito relacionado con la identidad, establecido por la UNODC para aunar experiencias, elaborar estrategias, facilitar la investigación y concertar las acciones prácticas de lucha contra el delito relacionado con la identidad. Para más información sobre la labor del grupo básico, visite el sitio web: http://www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside.

Índice

I. INTRODUCCIÓN

1. Propósito de la guía

Debido a la amplia dimensión transnacional que tiene el delito relacionado con la identidad, la cooperación internacional en materia penal es fundamental para el éxito de las investigaciones. Habida cuenta de que existen considerables diferencias entre las investigaciones que se realizan a nivel nacional y aquellas que requieren el uso de instrumentos de cooperación internacional, la presente guía tiene como objetivo brindar un panorama general de los aspectos relativos a la dimensión transnacional del delito relacionado con la identidad y los principios generales de la cooperación internacional. Con el fin de facilitar las tareas de investigación, esta guía también ofrece una reseña de algunos de los casos más relevantes. En vista de la complejidad del tema, la guía concentra información básica y directrices sobre la mejor manera de abordar las solicitudes de cooperación internacional en la esfera del delito relacionado con la identidad.

2. La expansión del delito relacionado con la identidad

Factores tales como la amplia difusión de los medios de comunicación[1], los resultados de diversas encuestas que analizan el alcance del hurto de identidad y las pérdidas que este ocasiona[2], así como varios análisis jurídicos y técnicos[3] publicados en los últimos años, podrían fácilmente llevarnos a la conclusión de que los delitos relacionados con la identidad son un fenómeno del siglo XXI[4]. Este no es precisamente el caso. Hace más de cien años que se tiene conocimiento de delitos tales como la suplantación de identidad, la falsificación y el uso indebido de documentos de identidad[5]. En la década de 1980 la prensa ya hacía referencia al uso indebido de la información de identidad[6].

---

[1] Véanse, por ejemplo, *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, disponible en: http://edition.cnn.com/2006/US/05/18/identity.theft; *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007, disponible en: http://www.iht.com/articles/2007/03/21/business/identity.php

[2] Véanse, por ejemplo, 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[3] Véanse, por ejemplo, *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, vol. 11, núm. 1, 2006; Peeters, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000.

[4] *Hoar*, Identity Theft: The Crime of the New Millennium, Oregon *Law Review*, vol. 80, 2001, página 1421 y ss.; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, 2008, página 8.

[5] Véase: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, página 5.

[6] Véase: *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003, página 1.

Sin embargo, la creciente utilización de la información digital ofreció a los delincuentes nuevas posibilidades para acceder a la información relacionada con la identidad[7]. El proceso de transformación que sufrieron los países industrializados hasta convertirse en sociedades de la información[8] ha tenido enormes consecuencias, particularmente en lo que respecta al surgimiento de los delitos relacionados con la identidad. A pesar del gran número de casos de delitos de hurto de identidad relacionados con Internet, la digitalización no ha modificado el delito típico sino que ha dado lugar en cambio a la aparición de nuevos objetivos y facilitado la creación de nuevas formas de delincuencia[9]. No obstante, a pesar de que existe una creciente tendencia orientada al delito de identidad en línea, los delitos tradicionales siguen teniendo mayor incidencia[10]. Las estafas en línea y las filtraciones de datos representaron menos del 20% de los delitos clasificados en 2007[11] en los Estados Unidos[12].

Habida cuenta de que la digitalización y la globalización de los servicios basados en redes llevaron a un aumento del uso digital de la información de identidad, resulta sorprendente la relevancia que siguen teniendo los delitos que no se cometen en línea. Las principales secciones de negocios y las operaciones federales dependen de sistemas automatizados para el procesamiento de sus datos[13].

La información relacionada con la identidad tiene una importancia creciente en la economía, así como en la interacción social. En el pasado, el "buen nombre" y las buenas relaciones interpersonales predominaban en los negocios y en las transacciones de la vida cotidiana[14]. Con el paso al comercio electrónico, la identificación en persona es poco frecuente y, como consecuencia, la información de identidad se ha vuelto cada vez más importante para la participación en las interacciones sociales y económicas[15]. El proceso de "instrumentalización"[16], a través del cual una identidad se traduce en información de identidad cuantificable, es de suma importancia, así como la distinción entre, por un lado, la identidad de una persona que se define[17] como el conjunto de características personales, y por el otro, la información relacionada con la identidad cuantificable que permite el reconocimiento de una persona.

---

[7] *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, *Crime, Law and Social Change*, vol. 46, página 270.

[8] Para más información sobre la sociedad de la información, véanse: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[9] *Clarke*, Technology, Criminology and Crime Science, *European Journal on Criminal Policy and Research*, vol. 10, 2004, página 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, Documento de la Oficina General de Contabilidad: GAO/GGD-98-100BR, página 51; Identity Fraud, Prevalence and Links to Alien Illegal Activities, GAO, 2002, GAO-02-830T, página 6, *Paget*, Identity Theft, McAfee White Paper, 2007, página 6; Para una reseña sobre las actividades de "peska" véase: *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, página 8 y ss.

[10] 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, página 5.

[11] El 35% del número total de casos.

[12] Informe sobre la encuesta del fraude de identidad de 2008, versión para el consumidor, Javelin Strategy & Research, página 6.

[13] Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, Documento de la Oficina General de Contabilidad: GAO-07_935T, página 4.

[14] *Elston/Stein*, International Cooperation in On-line Identity Theft Investigations: A Hopeful Future but a Frustrating Present, disponible en: http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

[15] Véase *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, página 555.

[16] *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, *Bulletin of Science* Technology Society, 2007, vol. 27, 2008, página 20.

[17] Véase: *Encyclopaedia Britannica,* 2007.

En la actualidad, la confianza y la seguridad son requisitos necesarios en las transacciones a distancia[18], no solo en el ámbito de los negocios de comercio electrónico sino también en la economía en general. Un ejemplo de ello son las tarjetas de pago con un número de identificación personal (PIN) para hacer compras en un comercio. Tener acceso a la información relacionada con la identidad permite a los infractores participar en muchas esferas de la vida social. Asimismo, el hecho de que la información no solo se procesa sino que se almacena en bases de datos hace que estas sean un blanco posible para los delincuentes.

3. Las consecuencias de la digitalización en el carácter transnacional del delito

El creciente número de casos relacionados con Internet repercute significativamente en las tareas de investigación debido al carácter transnacional del delito cibernético[19]. Internet se concibió inicialmente como una red para uso militar[20] basada en una arquitectura de red descentralizada. Debido a esta estructura básica y a la disponibilidad mundial de los servicios, el delito cibernético suele tener una dimensión internacional[21]. Los correos electrónicos con contenidos ilegales pueden atravesar fácilmente varios países en su recorrido de emisor a destinatario. Un caso podría tener una dimensión transnacional incluso si el remitente y el destinatario se encuentran en el mismo país. Basta solo con que uno de ellos utilice un servicio de correo electrónico de un proveedor situado en otro país. Teniendo en cuenta que algunos de los servicios gratuitos de correo electrónico cuentan con varios cientos de millones de usuarios, resulta evidente que el delito cibernético, por su propia naturaleza, tenga con frecuencia una dimensión transnacional[22].

La dimensión transnacional de los casos relacionados con Internet queda de manifiesto en las estadísticas sobre los lugares donde se almacenan los sitios web de "peska". En mayo de 2009, el Grupo de trabajo de lucha contra las estafas por Internet (AFWG) elaboró una lista que incluía a los siguientes países: Estados Unidos (68%), China (6%), Canadá (6%), Alemania (2%), Reino Unido (1%) y Suecia (1%)[23].

Las consecuencias de la investigación del delito cibernético son similares a las de otros delitos transnacionales: el principio fundamental de la soberanía nacional no permite llevar a cabo investigaciones dentro del territorio de países extranjeros sin el permiso de las

[18] *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, página 533.

[19] Respecto de la dimensión transnacional del delito cibernético, véanse: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, vol. 12, núm. 2, página 289; *Sofaer/Goodman*, Cyber Crime and Security—The Transnational Dimension, en *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, página 1 y ss.

[20] Para una breve historia de Internet, incluidos sus orígenes militares, véanse: *Leiner, Cerf, Clark, Kahn, Kleinrock*; *Lynch, Postel, Roberts, Wolff,* "A Brief History of the Internet", disponible en: http://www.isoc.org/internet/history/brief.shtml.

[21] Respecto a la dimensión transnacional del delito cibernético, véase: *Sofaer/Goodman*, Cyber Crime and Security, The Transnational Dimension, *supra* núm. 19, página 7.

[22] Con respecto al número de usuarios de servicios gratuitos de correo electrónico, véase *Graham*, E-mail Carriers Deliver Gifts of Ninety Features to Lure, Keep Users, *USA Today*, 16.04.2008. El artículo hace mención a que los cuatro principales proveedores de webmail cuentan con varios cientos de millones de usuarios: Microsoft (256 millones), Yahoo (254 millones), Google (91 millones) y AOL (48 millones). Respecto a la dimensión transnacional del delito cibernético, véase: *Keyser*, The Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, vol. 12, núm. 2, página 289; Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, capítulo 3.2.7.

[23] APWG Phishing Activity Trends Report, primer semestre de 2009, página 7.

autoridades locales[24]. Por tanto, es fundamental garantizar una estrecha colaboración entre los países involucrados para llevar a cabo las investigaciones de los casos de delitos cibernéticos[25].

En comparación con otras esferas del delito transnacional, una de las diferencias a destacar es que el tiempo del que se dispone para llevar a cabo las investigaciones es con frecuencia limitado. A diferencia del tráfico de drogas, el cual, según el medio de transporte, puede llevar semanas antes de que la mercadería llegue al destinatario, un correo electrónico puede recibirse en cuestión de segundos y, si se cuenta con una banda ancha adecuada, incluso se pueden descargar archivos de gran tamaño en cuestión de minutos.

Para asegurar el éxito de las investigaciones es necesario que exista una colaboración oportuna y eficaz entre las autoridades competentes de los distintos países. Existen dos razones para ello: en primer lugar, la velocidad de los procesos de transferencia, y en segundo, el hecho de que las pruebas que pudieran ser relevantes para la investigación con frecuencia se eliminan automáticamente en poco tiempo. La lentitud de los procedimientos formales puede obstaculizar seriamente las investigaciones.

Muchos de los acuerdos de asistencia judicial recíproca existentes aún se basan en procedimientos formales, complejos y a menudo prolongados[26]. Por consiguiente, resulta vital que se establezcan procedimientos para responder rápidamente a los incidentes y a las solicitudes de cooperación internacional[27].

4. Grado de participación de la delincuencia organizada

Como se detalla más adelante, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC) es un instrumento importante para la cooperación internacional. Su aplicación no se limita a los delitos tradicionales y puede incluir delitos relacionados con la identidad en los casos en que se trate de un delito organizado transnacional. De hecho, es muy importante que se determine si existe participación de un grupo delictivo organizado, tal como se estipula en el inciso 1) del artículo 3 de la UNTOC.

Sin embargo, el análisis de los vínculos que existen entre el delito relacionado con la identidad y el crimen organizado presenta dificultades. El principal obstáculo es la falta de una investigación científica sobre la materia que sea fiable. A diferencia de los aspectos técnicos del delito, en especial las estafas para obtener información relacionada con la

[24] Con relación al principio de la soberanía nacional, véanse Roth, State Sovereignty, International Legality, and Moral Disagreement, 2005, página 1, disponible en: http://www.law.uga.edu/intl/roth.pdf; *Martinez*, National Sovereignty and International Organizations, 1996; *Riegler*, Nation Building Between National Sovereignty and International Intervention, 2005.

[25] En lo que respecta a la necesidad de cooperación internacional en la lucha contra el delito cibernético, véanse: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, *supra* núm. 19, página 35 y ss.

[26] *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, capítulo 6.3.

[27] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, página 141.

identidad[28], el componente de crimen organizado que pueda tener el delito se estudia en menor profundidad. Otro de los obstáculos es la falta de una definición de hurto de identidad[29] y de terminología relacionada[30] que sean universalmente aceptadas. Esto no solo crea dificultades en la elaboración de leyes, sino que también tiene una influencia negativa en las investigaciones sobre el tema[31].

A nivel de las fuerzas del orden, las investigaciones de casos relacionados con el delito de identidad llevadas a cabo con éxito revelan la participación de grupos delictivos organizados que cumplen con los requisitos de la definición de delincuencia organizada que figura en el artículo 2, inciso *a)*, de la UNTOC. Como consecuencia, en esta esfera en particular no se cuestiona la participación del crimen organizado, si bien aún no se sabe con exactitud cuál es su grado de participación.

Con respecto a la definición de grupo delictivo organizado establecida en el artículo 2, inciso *a)*, de la UNTOC, se destacan dos elementos de interés: el requerimiento de que exista un grupo de tres o más personas y de que exista un beneficio financiero. El tercer elemento, concretamente, el carácter de los delitos de identidad como "delitos graves" se mencionará más adelante en el capítulo III, sección 3.

"Un grupo de tres o más personas"

La comisión de un delito relacionado con la identidad no requiere la ayuda de otras personas[32], ya que la tecnología se encuentra a disposición de los infractores para que puedan llevar a cabo el delito de forma individual. Sin embargo, las tareas de investigación pusieron de manifiesto la participación de varias bandas delictivas en casos de delitos relacionados con la identidad. El factor común en la mayoría de estos casos fue el hecho de que en la ejecución del delito participaban varios delincuentes. No obstante, la estructura de

[28] Respecto de los métodos utilizados, véanse: *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Prevention and Criminal Justice, 18th session, 2009, E/CN.15/2009/CRP.13; *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, *supra* núm. 26, páginas 59 y ss.

[29] Identity Crime, Final Report, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, 2008, página 7; Respecto de las definiciones, véanse: *Finklea*, Identity Theft: Trends and Issues, CRS, 2009, R40599, página 2; *Paget*, Identity Theft, McAfee White Paper, 2007, página 4.

[30] *Finklea*, Identity Theft: Trends and Issues, CRS, 2009, R40599, página 2. En el "estudio de las Naciones Unidas sobre el fraude y la falsificación de identidad", publicado en 2007, el término general de "delito relacionado con la identidad" se utilizó para abarcar toda clase de conducta ilícita relacionada con la identidad, incluidos el hurto de identidad y el fraude de identidad. La razón fue que los Estados Miembros presentes no se pusieron de acuerdo en las definiciones de estos términos, y la misma conducta llamada "hurto de identidad" en algunos países, es considerada en otros como "fraude de identidad". El término "hurto de identidad", en particular, incluía casos en que alguien se apodera de información relativa a la identidad (información básica de identificación u otra clase de información personal) de modo análogo que en el hurto o fraude, lo que abarca la sustracción de documentos tangibles y de información intangible y el hecho de persuadir con engaño a una persona para que entregue documentos o información a título voluntario. Por otro lado, la expresión "fraude de identidad" por lo general alude al uso subsiguiente de la información de identificación o de identidad con objeto de cometer otros delitos o de evitar ser descubierto o sometido a la justicia. Esto incluye el fraude contra entidades privadas (por ejemplo, el fraude de tarjetas de crédito) y el fraude contra el sector público (por ejemplo, obtener ilegalmente beneficios del seguro social o contratos de compra). Véase: Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos. Informe del Secretario General, 02.04.2007, E/CN.15/2007/8/Add. 3, página 4.

[31] Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos. Informe del Secretario General, 02.04.2007, E/CN.15/2007/8, página 6.

[32] Informe sobre el hurto de identidad, preparado para el Ministerio de Seguridad Pública del Canadá y para el Fiscal General de los Estados Unidos, Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2004; *Paget*, Identity Theft – McAfee White Paper, 2007, página 10.

esos grupos no es necesariamente comparable con la de los grupos del crimen organizado. Por ejemplo, los grupos dedicados al delito cibernético suelen tener una estructura más flexible[33]. Además, en comparación con los grupos tradicionales de delincuencia organizada el tamaño de los grupos es con frecuencia más reducido[34]. Internet facilita la estrecha colaboración y la coordinación de las actividades sin que exista un contacto cara a cara[35].

Es importante tener en cuenta que el término "delito relacionado con la identidad" no se utiliza para describir un único acto delictivo, sino una categoría de delito que con frecuencia combina diferentes acciones, incluidos los delitos que a menudo se describen como "fraude de identidad" y "hurto de identidad". El hecho de que varios delincuentes actúen juntos no significa necesariamente que exista una cooperación con otros en las diferentes etapas de la actividad delictiva. Un posible escenario sería, por ejemplo, cuando un delincuente envía correos electrónicos engañosos (peska) para obtener información de tarjetas de crédito. Este entrega la información por un precio fijo a un segundo delincuente, quien tiene un sitio web de venta de datos de tarjetas de crédito[36]. Por último, un tercer delincuente obtiene la información y la utiliza para realizar compras.

Otra posibilidad es que los delincuentes operen conjuntamente en grupos no estables creados especialmente para ese fin[37]. La cuestión de si los grupos reúnen los requisitos establecidos en el artículo 2, incisos *a)* y *c)*, de la UNTOC (definición de "grupo delictivo organizado" y "grupo estructurado", respectivamente) debería analizarse más en detalle caso por caso. Sin embargo, a los efectos de lograr una mayor clarificación y orientación sobre este asunto, cabría señalar que una nota interpretativa en el artículo 2, inciso *c)*, de la UNTOC especifica que el término "grupo estructurado" debe utilizarse en un sentido amplio para que incluya tanto a los grupos con jerarquías como los que tienen estructuras no jerarquizadas en los que no es necesario definir expresamente la función de sus miembros[38].

Beneficios económicos

Mientras que las preguntas respecto de la exactitud de las estadísticas sobre el perjuicio económico que causan los delitos de hurto de identidad continúan sin tener respuesta, es cierto que las pérdidas, así como las ganancias, son considerables. Con frecuencia sucede que las pérdidas económicas que sufren las víctimas se corresponden directamente con los beneficios financieros que obtienen los delincuentes. Un ejemplo de ello es el caso en el que el delincuente efectúa compras utilizando la información de la tarjeta de crédito de la víctima. No obstante, también se pueden obtener ganancias en etapas previas, por ejemplo, vendiendo información relacionada con la identidad obtenida de manera ilícita. Los precios varían según la categoría y la calidad de los datos, y en el caso de información de

[33] *Choo*, Trends in Organized Crime, 2008, página 273.
[34] *Brenner*, Organized Cybercrime, *North Carolina Journal of Law & Technology*, 2002, issue 4, página 27.
[35] Véase, por ejemplo: Convictions for internet rape plan, Great Britain Crown Prosecution Service, comunicado de prensa, 01.12.2006.
[36] Respecto de los precios de la información de tarjetas de crédito, véase: Symantec Internet Security Threat Report, vol. XIII, 2008.
[37] *Choo*, Trends in Organized Crime, *supra* núm. 34.
[38] Véanse los *Travaux Préparatoires* de las negociaciones para la elaboración de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos, Naciones Unidas, Nueva York 2006, parte 1, página 17.

cuentas bancarias[39], estos oscilan entre los 10 y los 1.000 dólares de los Estados Unidos, y entre 0,40 y 20 dólares de los Estados Unidos por información de tarjetas de crédito[40].

Además de los beneficios económicos directos, los delincuentes pueden utilizar la información relacionada con la identidad para obtener beneficios económicos indirectos. En particular, pueden utilizar el número de cuenta bancaria de la víctima para realizar operaciones de blanqueo de capitales. Existen varias medidas de lucha contra esta actividad que se basan en el principio de "conozca a su cliente" y, por tanto, dependen en gran medida de elementos de identidad o identificación. Para las estafas de blanqueo de capitales se utilizan las tecnologías de la información y de las comunicaciones comerciales, las cuales permiten a los delincuentes generar información de identificación falsa, lo que a su vez facilita aún más las transferencias a distancia para ocultar los bienes blanqueados[41]. Además, utilizando identidades robadas, los delincuentes pueden evitar ser identificados y evadir las medidas de prevención del terrorismo. El informe del Secretario General de las Naciones Unidas sobre las recomendaciones para una estrategia mundial de lucha contra el terrorismo destaca la importancia de diseñar mecanismos para abordar el problema del hurto de identidad en la lucha contra el terrorismo[42].

Sin embargo, en el estudio sobre el beneficio económico es importante considerar que los delitos relacionados con la identidad no tienen necesariamente un carácter económico o se cometen para obtener un beneficio financiero directo o indirecto. Los delincuentes pueden utilizar la información que obtienen para ocultar su verdadera identidad[43] y de ese modo dificultar las tareas de investigación. No obstante, estos delitos están comprendidos en el ámbito de la UNTOC cuando se vinculan a un grupo delictivo organizado que también está implicado en delitos económicos.

Además, el significado de la expresión "beneficio económico u otro beneficio de orden material" es relativamente amplio y comprende, por ejemplo, el tráfico de pornografía infantil con fines de gratificación sexual[44]. Por tanto, el delito de identidad abarca casos en que se trata a la información de identificación o de identidad sustraída o fabricada como mercancía ilícita, es decir, se la compra, vende o permuta, y casos en los que la información de identidad se utiliza indebidamente con miras a obtener beneficios personales o colectivos, incluidos beneficios que no fueran económicos, como el de poder entrar a otro país.

---

[39] *Ibid.*

[40] *Ibid.*

[41] Con respecto a la relación entre los delitos relacionados con la identidad y los delitos de blanqueo de capitales, véase: Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, Informe del Secretario General, E/CN.15/2007/8/Add. 3, página 12.

[42] Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo, 27.04.2006, A/60/825, página 13.

[43] Véase en este contexto, los Resultados de la segunda reunión del Grupo Intergubernamental de Expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos, *supra* núm. 42, página 10.

[44] Véanse los *Travaux Préparatoires* de las negociaciones para la elaboración de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos, *supra* núm. 39, parte 1, página 17.

II. ASPECTOS GENERALES DE LA COOPERACIÓN INTERNACIONAL EN LOS CASOS DE DELITOS RELACIONADOS CON LA IDENTIDAD

1. La importancia de la cooperación internacional en la lucha contra el delito relacionado con la identidad

En el pasado, los delitos en general tenían una dimensión nacional, y el delito transfronterizo era un fenómeno aislado. En la actualidad, el creciente uso de la tecnología ha permitido el surgimiento de nuevas formas de delito que han llevado a los académicos a hablar de la "desaparición de la territorialidad"[45]. Al tiempo que los delincuentes no parecen sentirse limitados por las fronteras, en la mayoría de los casos las normas del derecho penal todavía cumplen el principio tradicional de soberanía nacional, mientras que las normas de jurisdicción más estrictas sobre el delito penal se mantienen vigentes.

Dependiendo del tipo de delito de identidad que se haya cometido, la investigación, el procesamiento y la sentencia del delincuente podrían presuponer un elemento externo. En los casos de fraude telefónico[46] o fraude de servicios públicos, por ejemplo, el delito se comete dentro del territorio nacional de un determinado país, mientras que los delitos de identidad que se cometen a través de sistemas informáticos, tales como la peska (phishing) o la recolección de datos (pharming), con frecuencia abarcan a un gran número de víctimas en diversos países en distintos continentes. Lo mismo se aplica para el fraude de tarjetas de crédito, que puede tener un componente regional (que involucra a países en una determinada región), pero también puede tener un carácter internacional, especialmente si la información de la tarjeta de crédito se obtuvo o se transfirió a través del uso indebido de una computadora.

Tal como se mencionó anteriormente, un elemento transnacional presupone la necesidad de contar con la colaboración internacional entre los países, y debido a la naturaleza de los delitos, dicha cooperación debe llevarse a cabo bajo ciertas condiciones y, en muchas ocasiones, en un breve período. La necesidad de una respuesta rápida parece no estar en sintonía con la cooperación internacional tradicional, que con frecuencia se caracteriza por ser "lenta y engorrosa"[47]. La especificidad de la cooperación internacional en estos casos se ampliará en los capítulos correspondientes de la guía. Serían aplicables diversos tipos de solicitudes, pero las más relevantes son la de extradición (y su

[45] Véase, por ejemplo, *Guinchard*, Criminal Law in the 21st century: the demise of territoriality? Notes for the Critical Legal Conference on Walls, 16 de septiembre de 2007, Birkberk (Londres), disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1290049.

[46] Para los detalles de los tipos de fraude telefónico, véase: http://www.ftc.gov/phonefraud.

[47] Véase: *Nielsen*, From classical judicial cooperation to mutual recognition, in *Revue Internationale de Droit Penal*, 77e anée, nouvelle série, 1er et 2nd trimestres 2006, página 53 y ss.

versión simplificada, que se aplica dentro de la UE, a saber, la orden de detención europea) y la de asistencia judicial recíproca.

Dadas las particularidades de esta guía, se hará más hincapié en los aspectos de la asistencia judicial recíproca, ya que esta forma de cooperación internacional es parte de la labor diaria de jueces y fiscales que se ocupan de los delitos relacionados con la identidad. Este capítulo se limita a ofrecer una introducción a los principales instrumentos, los cuales se tratarán con más detalle en el capítulo III, y presenta los principales convenios aplicables en los casos de los delitos relacionados con la identidad. No solo abordará la función de jueces o fiscales que con frecuencia tratan temas relativos a la cooperación internacional, sino que también, y sobre todo, las necesidades de aquellos que carecen de experiencia previa en este sentido y buscan información general acerca de este tema.

2. Principales instrumentos en relación con la cooperación internacional para combatir el delito relacionado con la identidad

Extradición

Se sabe que la extradición cuenta con una larga historia, que surge en la antigüedad con la entrega de delincuentes políticos[48], hasta convertirse en lo que es hoy en día, concretamente, una institución que permite a un Estado (Estado requerido) prestar asistencia a otro (Estado requirente) en la entrega de un delincuente para que sea procesado o para que cumpla una condena.

Las reglas de extradición pueden aplicarse directamente sobre la base de un tratado que tenga fuerza de ley de acuerdo con la legislación interna del Estado requerido, o sobre la base de una ley nacional que aplique las disposiciones de un tratado. Otro posible escenario sería permitir la extradición sobre la base de acuerdos entre dos Estados especialmente concebidos para ese fin cuando no se encuentra en vigor ningún otro tratado bilateral o multilateral. Con frecuencia, este tipo de acuerdo se basa en el requisito de reciprocidad[49]. Algunos Estados conceden las solicitudes de extradición sobre la base de la reciprocidad (por ejemplo, Alemania, Suiza, Rumania), mientras que otros solamente actúan sobre la base de un tratado existente (por ejemplo, los Estados Unidos[50], Bélgica, el Reino Unido y los Países Bajos)[51].

[48] Al parecer, el primer tratado concerniente a la extradición se celebró entre Ramsés II de Egipto y el Príncipe hitita Hattushilish III. Para más detalles sobre la historia de la extradición, véase: *Gilbert*, Transnational Fugitive Offenders in International Law. Extradition and Other Mechanisms, *Kluwer Law International*, 1998, página 17 y ss.

[49] La ley de reciprocidad implica que un Estado que solicita la extradición de una persona buscada en el Estado requerido está obligado a considerar una solicitud de extradición de ese Estado en circunstancias similares.

[50] En lo que respecta a los Estados Unidos, el Manual del Abogado de los Estados Unidos establece que, en general, puede concederse la extradición únicamente en virtud de un tratado. Sin embargo, tras los cambios introducidos en 18 USC 3181 y 3184 en 1996, está permitido conceder la extradición de personas (siempre y cuando no sean ciudadanos, nacionales o residentes permanentes de los Estados Unidos) que hayan cometido delitos violentos contra ciudadanos de los Estados Unidos en países extranjeros donde no existe el tratado necesario. Para más detalles, véase: USAM Title 9-Chapter 9-15.000, disponible en: http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/15mcrm.htm

[51] Véase: *Radu*, Cooperare judiciară internațională și europeană în materie penală. Îndrumar pentru practicieni, Wolters Kluwer, Romania, 2009, página 25.

Todos los tratados de extradición, ya sean internacionales, regionales o bilaterales, comprenden principios similares, si bien cada derecho interno es diferente, teniendo en cuenta la especificidad de cada sistema jurídico. El siguiente capítulo presenta de manera breve los elementos más significativos que deben considerarse en relación con la extradición de delincuentes que cometen delitos relacionados con la identidad. Es fundamental reconocer a la extradición como un procedimiento que implica la participación tanto de las autoridades judiciales como del Poder Ejecutivo. Mientras que en algunos países la función del Ejecutivo tiene mayor prevalencia[52], en otros la tiene el Poder Judicial. Por tanto, es importante que las autoridades judiciales encargadas de preparar la documentación necesaria para llevar a cabo la extradición tengan en cuenta estos principios generales. Las particularidades de cada tratado se examinarán en las páginas siguientes.

Elementos importantes relacionados con el procedimiento de extradición

Las condiciones que se han de verificar al formular una solicitud de extradición se refieren al delito mismo y al delincuente. Dado que esta guía no está dedicada a la cooperación internacional en sí misma, la siguiente reseña se limita a tratar las características más relevantes que es necesario considerar cuando se formula una solicitud.

Gravedad del delito

La extradición de una persona en general se limita a delitos de cierta gravedad. Esto significa que este complicado procedimiento que requiere una movilización considerable de recursos no sería procedente en los casos de delitos menores. Algunos de los convenios establecen diferentes umbrales para el procesamiento de la condena o la ejecución de una orden de arresto[53], mientras que otros no hacen esa distinción.

Requisito de doble incriminación

El principio de doble incriminación es uno de los principales requisitos que surgen del principio de legalidad[54]. Teniendo en cuenta que los delitos relacionados con la identidad se encuentran dentro de la categoría de delitos que aún no están tipificados a nivel mundial, este principio tiene una importancia especial respecto del delito de identidad. Todos los tratados de extradición[55] incluyen la ausencia de la doble incriminación como motivo obligatorio para la denegación.

---

[52] Existen diferentes enfoques nacionales respecto a la toma de decisiones de un proceso de extradición. Por ejemplo, en los Estados Unidos la decisión final la toma el Secretario de Estado, mientras que en Rumania, la decisión de extraditar a una persona la toma la autoridad judicial.

[53] Véase, por ejemplo: el Convenio Europeo sobre Extradición, París 1957, disponible en: http://conventions.coe.int/Treaty/EN/Treaties/Html/024.htm.

[54] La doble incriminación existe si el delito se considera como tal en virtud de la legislación de los Estados Parte requerido y requirente. En lo que respecta al principio de la doble incriminación en las investigaciones internacionales, véanse *Manual de las Naciones Unidas sobre prevención y control de delitos informáticos*, Revista Internacional de Política Criminal, números 43 y 44: publicación de las Naciones Unidas, núm. de venta E.94.IV.5, página 269; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, que se presentó en la Reunión temática de la UIT sobre seguridad cibernética celebrada en Ginebra del 28 de junio al 1 de julio de 2005, página 5.

[55] Véanse, por ejemplo, el artículo 2 del Convenio europeo sobre extradición, París, 1957, el artículo 3 de la Convención Interamericana sobre Extradición, Caracas, 1981, etc.

En algunas ocasiones, en particular en el caso en que existen instrumentos bilaterales, la extradición solo puede concederse para una lista limitada de delitos previstos *expressis verbis* en el texto del tratado específico. Por ejemplo, mientras que el homicidio es un delito que típicamente figura en dicha lista, los delitos relacionados con la identidad son ejemplos típicos de los denominados delitos emergentes. En lo que respecta a estos delitos, existe el riesgo de que el Estado requerido no los reconozca en su derecho interno, o que el instrumento bilateral no los incluya en la lista de delitos, especialmente si en el momento de concluir el tratado bilateral[56] el delito relacionado con la identidad no estaba reconocido como un acto ilícito y no se acordaron enmiendas o actualizaciones de la lista de delitos.

Cabe señalar que en general los tratados de extradición contemporáneos, tanto bilaterales como multilaterales, han renunciado al criterio de esta "lista"[57], optando por el de "punibilidad" que, debido a su flexibilidad resulta más eficaz.

Teniendo en cuenta diversos enfoques para tipificar los delitos relacionados con la identidad[58], podría darse el caso de que el hurto de identidad no se considerase como un delito específico dentro del contexto de la cooperación internacional, pero sí algunas de sus diferentes etapas (la preparación, la obtención de la información, el proceso de transferencia, la utilización con fines delictivos)[59]. Por tanto, es importante que las autoridades competentes del Estado requirente faciliten información precisa de los delitos por los cuales se pide la extradición y de las disposiciones de su legislación pertinentes que establecen dichos delitos.

El carácter transnacional del delito relacionado con la identidad, que presenta desafíos al concepto mismo de territorialidad, puede acentuar los problemas con respecto a la interpretación del requisito de doble incriminación en el caso en que los Estados requirente y requerido se basen en diferentes tradiciones jurídicas[60].

Las tendencias y novedades recientes en materia de leyes de extradición apuntan a atenuar la aplicación estricta de determinados criterios para negar la extradición. En este contexto, se han intentado mitigar, por ejemplo, las dificultades relativas a la doble incriminación incluyendo disposiciones generales en los tratados, ya sea enumerando los actos y exigiendo únicamente que las leyes de ambos Estados los castiguen como delitos

[56] Este fue el caso de un antiguo tratado bilateral entre los Estados Unidos y el Reino Unido, según el cual la extradición desde el Reino Unido a los Estados Unidos dependía del hecho de que el delito hubiera sido parte de los delitos enumerados. En el Reino Unido esta lista quedó consagrada en la Ley de Extradición de 1870, la que obviamente no abarcó los delitos de fraude electrónico estipulados por el derecho penal de los Estados Unidos. En la legislación británica no existía un delito equivalente, sino un concepto similar (conspiración para cometer fraude), que tampoco figuraba en la lista de delitos de 1870. Esta resultó ser una situación bastante incómoda, que se solucionó mediante la concertación de un nuevo tratado que, en lugar de basarse en la lista, se basó en el criterio de la punibilidad. Véase: *Foshi*/*Gibbins*, Reform of the United Kingdom Extradition Law in United States Attorneys' Bulletin, septiembre de 2003, página 51 y ss., disponible en: http://www.justice.gov/usao/eousa/foia_reading_room/usab5105.pdf.

[57] Algunos textos consideran que el criterio de la lista presenta algunos inconvenientes en comparación con la tendencia impuesta por los tratados modernos de hacer referencia a un nivel mínimo del castigo. Para más detalles, véase: *Bantekas*/*Nash*, International Criminal Law, Routledge-Cavendish, 2007, página 296.

[58] Con respecto a los diferentes enfoques, véase: *Gercke*, Legal Approaches to Criminalize Identity Theft, *supra* núm. 28.

[59] *Ibid.*, página 38 y ss.

[60] En estos casos existen diferentes interpretaciones en los países donde se aplica el derecho civil, en comparación con los países de derecho consuetudinario, en el sentido de que, en general, los primeros juzgan con independencia el hecho de que el presunto delito se haya llevado a cabo parcial o totalmente fuera de su territorio, véase *Bantekas*/*Nash*, Interational criminal law, *supra* núm. 57, página 297.

o infracciones, o simplemente permitiendo la extradición por toda conducta tipificada y sujeta a determinado nivel de sanción en cada Estado. En vista de esto, se deberían tomar medidas a nivel regional encaminadas a la armonización de las leyes nacionales, cuando sea posible, en especial en relación con las disposiciones en materia de penalización establecidas en la Convención contra la Delincuencia Organizada y sus Protocolos, así como la Convención de las Naciones Unidas contra la Corrupción, para que el principio de la doble incriminación no obstaculice el desarrollo de arreglos más efectivos en materia de cooperación[61].

Ne bis in idem

Este tradicional principio, que se basa en consideraciones humanitarias y en la necesidad de garantizar una adecuada administración de justicia, exige que una persona no sea extraditada si ya ha sido juzgada en el Estado requerido por el mismo delito por el cual se solicita la extradición[62]. Esto constituiría un motivo de denegación obligatorio[63], aunque si la extradición se solicitase a efectos de procesar a esa persona, el principio *ne bis in idem* sería más bien un motivo opcional de denegación[64].

Aut dedere aut judicare ("extraditar o juzgar")

Según este principio, si un Estado no concede la extradición de la persona requerida, tendrá que hacerse cargo, a petición del Estado requirente, del proceso penal contra esa persona. La intención de este principio es impedir la creación de refugios para cometer delitos y está reconocido en todo tratado de extradición[65] o instrumento internacional contemporáneo que incluya disposiciones sobre extradición[66].

---

[61] Cabría señalar que el artículo 43, párrafo 2, de la Convención de las Naciones Unidas contra la Corrupción exige que, en cuestiones de cooperación internacional, cuando la doble incriminación sea un requisito, este se considerará cumplido si la conducta constitutiva del delito respecto del cual se solicita asistencia es delito con arreglo a la legislación de ambos Estados Parte, independientemente de si las leyes del Estado Parte requerido incluyen al delito en la misma categoría o lo denominan con la misma terminología que el Estado Parte requirente.

[62] Para más detalles, véanse: *Vervaele*, The transnational *ne bis in idem*. Principle in the European Union: Mutual Recognition and Equivalent Protection of Human Rights, *Utrecht Law Review*, vol. 1, núm. 2, págs. 100 a 118; Conway, *Ne bis in Idem* in International Law, International Criminal Law Review, vol. 3, núm.3, págs. 217 a 244; 2003, Informe explicativo del Convenio europeo sobre la ejecución en el extranjero de trámites procesales en materia penal, disponible en: http://conventions.coe.int/Treaty/en/Reports/Html/073.htm.

[63] Véase el artículo 9, primera sentencia del Convenio europeo sobre extradición, París, 1957, o el artículo 4, inciso *d)*, del Protocolo de Extradición de la Comunidad del África Meridional para el Desarrollo, 2002.

[64] Véase el artículo 9, segunda sentencia del Convenio europeo sobre extradición, *ibid.*, o el artículo 5, inciso *i)*, del Protocolo de Extradición de la Comunidad del África Meridional para el Desarrollo, *ibid*.

[65] Véase, por ejemplo, el artículo 8 de la Convención Interamericana sobre Extradición, disponible en: www.oas.org/juridico/english/treaties/b-47.html, que establece que "Cuando correspondiendo la extradición, un Estado no entregare a la persona reclamada, el Estado requerido queda obligado, cuando su legislación u otros tratados se lo permitan, a juzgarla por el delito que se le impute, de igual manera que si este hubiera sido cometido en su territorio, y deberá comunicar al Estado requirente la sentencia que se dicte".

[66] Véase el artículo 16, párrafo 12, de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, Palermo, 2000 (en adelante UNTOC) que dice: "Si la extradición solicitada con el propósito de que se cumpla una condena es denegada por el hecho de que la persona buscada es nacional del Estado Parte requerido, este, si su derecho interno lo permite y de conformidad con los requisitos de dicho derecho, considerará, previa solicitud del Estado Parte requirente, la posibilidad de hacer cumplir la condena impuesta o el resto pendiente de dicha condena con arreglo al derecho interno del Estado Parte requirente".

Caducidad

Se trata de otra condición que protege a una persona de ser extraditada, si esta no ha sido procesada o castigada por haber caducado el tiempo para ello. Algunos tratados de extradición más recientes han renunciado a la condición de verificar si la limitación estatutaria es aplicable en el Estado requerido, teniendo en cuenta que dicha solicitud dificulta la cooperación entre el Estado requirente y el requerido.

Principio de especialidad

En virtud del principio de especialidad, una vez una persona haya sido extraditada, no puede ser procesada, condenada o detenida por delitos cometidos con anterioridad a su entrega distintos de los que dio lugar a la solicitud de extradición. Por supuesto, existen limitadas excepciones a esta regla, como por ejemplo cuando el Estado requerido aprueba la extensión de la solicitud de extradición. Esta situación representa un escenario realista para los casos de los delitos relacionados con la identidad, donde los delitos que no se conocen en el momento de la presentación de la solicitud de extradición se detectan después de presentada la misma.

Otros principios

Uno de los principios tradicionales que gobiernan el procedimiento de extradición es el de la "no extradición de nacionales"[67]. Este principio está presente en la mayoría de los sistemas que aplican el derecho civil, si bien no es el caso de las jurisdicciones que se rigen por el derecho consuetudinario. Sin embargo, incluso en los sistemas de derecho civil podrían existir casos en los que se permite la extradición de nacionales con sujeción a determinadas condiciones[68].

Al parecer, muchos Estados se muestran cada vez menos renuentes a extraditar a sus nacionales. La Convención contra la Delincuencia Organizada incluye una disposición que refleja este avance: en el artículo 16, párrafo 11, se hace referencia a la posibilidad de conceder la entrega provisional del fugitivo a condición de que esa persona sea devuelta al Estado Parte requerido para cumplir la condena impuesta. Si el Estado requerido se niega a extraditar a un fugitivo argumentando que es su nacional, se suele considerar que el Estado tiene la obligación de juzgar a esa persona. Esto ilustra el principio de extraditar o juzgar (*aut dedere aut judicare*) antes mencionado. En los casos en que se solicita la extradición con el propósito de hacer cumplir una condena, el Estado requerido también puede hacer cumplir la condena impuesta de conformidad con las disposiciones de su legislación nacional.

Además, los motivos de la denegación de la extradición pueden basarse en consideraciones de derechos humanos, tales como la pena de muerte o la discriminación por motivos

[67] Este principio también tiene sus orígenes en la ley de la soberanía y ha sido consagrado en varias ocasiones incluso en las leyes fundamentales. Su aplicación depende de la interpretación que la legislación de cada país otorgue al término "nacional". Véase, por ejemplo, el caso de los Estados nórdicos, los cuales integran como nacionales a todos los residentes inscritos. Véase: *Bantekas/Nash*, International Criminal Law, *supra* núm. 57, página 308.

[68] Véase, por ejemplo, el artículo 26, párrafo 1, de la Constitución italiana, en la cual se establece que la extradición de un ciudadano se permite únicamente en los casos expresamente previstos en las convenciones internacionales.

de raza, religión, nacionalidad, origen étnico o pensamiento político[69]. En general, los tratados de extradición tradicionales[70] incluyen disposiciones que prohíben la extradición por delitos políticos o militares.

Otro principio importante que debe mencionarse brevemente es el de "no indagación". En términos generales, este principio estipula que las autoridades judiciales del Estado requerido no deberían preguntar por la buena fe o los motivos que llevaron a solicitar la extradición[71].

Requisitos prácticos y formales

El procedimiento de extradición es bastante formal. Existen varios aspectos prácticos que deben tenerse en cuenta al referirse a los documentos que acompañan a la solicitud de extradición. Esta consideración podría variar levemente dependiendo de los sistemas jurídicos de los Estados involucrados, si bien existen elementos comunes que no están relacionados con ningún sistema jurídico específico. La información que debe proporcionarse a las autoridades competentes del Estado requerido incluye, por ejemplo, los datos de la persona requerida, la orden de detención o condena penal dictada contra la persona que vaya a ser extraditada, el resumen de los hechos y las disposiciones legales aplicables. Los documentos relacionados deben estar certificados. Los requisitos de certificación pueden variar de un país a otro, pero en general la certificación es responsabilidad de la autoridad judicial que prepara la documentación. Los países que aplican el derecho consuetudinario tienen ciertas particularidades[72], especialmente en relación con los documentos anexos, los cuales deben presentarse en un formulario específico para que el Tribunal los admita[73]. Cuando se formula una solicitud, es importante que el Estado requirente tenga conocimiento de los requisitos formales especiales. Algunos Estados aceptan el envío de las solicitudes y los documentos adjuntos directamente de una autoridad central a otra, pero la mayoría de los Estados siguen utilizando la vía diplomática.

Es sabido que las diversas prácticas de enjuiciamiento, tanto en los sistemas que aplican el derecho consuetudinario como en los sistemas jurídicos continentales, dificultan la eficacia de la cooperación interregional e internacional. En la esfera de la extradición, estas

[69] La doctrina del delito político establece principalmente que la extradición podrá ser denegada si fue solicitada por delitos políticos en el país requirente. Para más detalles sobre este tema y sobre la evolución histórica, véase: *Cervasion*, Extradition and the International Criminal Court: The Future of the Political Offence Doctrine, issue núm. *Pace International Law Review*, vol. núm., 1999, página 419 y ss. Esta doctrina tiene menos importancia práctica desde la perspectiva del delito relacionado con la identidad.

[70] Véase el Convenio europeo sobre extradición, París 1957, el cual sigue siendo válido para los Estados miembros del Consejo de Europa que no son miembros de la Unión Europea o para los Estados miembros de la Unión Europea que hayan depositado declaraciones para la decisión marco sobre la orden de detención europea y los procedimientos de entrega de los Estados miembros, indicando que se seguirá aplicando el procedimiento de extradición bajo algunas condiciones estrictas (véase las declaraciones de Italia, Austria, Francia, República Checa y Luxemburgo). Para más detalles, véase el *European Handbook on How to Issue a European Arrest Warrant* en Instruments on Judicial Cooperation in Criminal Matters within the Third Pillar of the European Union and Other Essential International Instruments on Judicial Cooperation, Consilium, 2009, página 493 o disponible en línea en: www.gddc.pt/MDE/Manual_MDE_EN.pdf

[71] Para más detalles, véase: *Bantekas/Nash*, *supra* núm. 57, página 309. Respecto de una posible excepción parcial en aquellos casos en que se solicita la extradición para sentencias dictadas *in absentia*, véase *Pyle*, Extradition, Politics and Human Rights, Temple University Press, 2001, página 127.

[72] En estos países, la evidencia *prima facie* se encuentra entre los requisitos que deben cumplirse. Este es el caso del Canadá. Véase: http://laws.justice.gc.ca/eng/E-23.01/20100304/page-2.html?rp2=HOME&rp3=SI&rp1=extradition&rp4=all&rp9=cs&rp10=L&rp13=50; o incluso Israel en: http://www.coe.int/t/e/legal_affairs/legal_co-operation/transnational_criminal_justice/2_pc-oc/israel's%20prima%20facie%20evidence%20requirements.pdf.

[73] Por ejemplo, el Canadá tiene unos requisitos muy específicos en cuanto al formulario de solicitud de extradición, el cual debe ser presentado ante las autoridades, dependiendo del hecho de que la decisión haya sido dictada *in absentia* o no.

diferencias son aún mayores con respecto a los documentos que deben presentarse al Estado requerido y los requisitos pertinentes en cuanto a las pruebas necesarias para conceder una solicitud de extradición.

En la mayoría de los Estados donde se aplica el derecho continental, la extradición se percibe como un instrumento de cooperación internacional para someter a un fugitivo ante la justicia. El propósito del mecanismo de extradición es someter a la persona requerida a los procedimientos que se llevan a cabo en el extranjero. Según este concepto, los tribunales que se ocupan de los casos de extradición se abstienen de examinar las pruebas de culpabilidad contra la persona solicitada, ya que consideran que este análisis incumbe exclusivamente a las autoridades judiciales del Estado requirente. Para las autoridades del Estado requerido es suficiente el hecho de que exista una orden judicial de arresto válida basada en un delito motivo de extradición, que se cumplan los requisitos sustantivos y de procedimiento para la extradición, y que ninguno de los motivos de denegación de una solicitud de extradición estipulados contractual o estatutariamente sean aplicables al caso en cuestión.

Por el contrario, en muchos países que aplican el derecho consuetudinario, se exige que la iniciación del proceso de extradición cumpla con la normativa general necesaria para iniciar un procedimiento penal. Por consiguiente, la investigación va más allá de un control formal de las condiciones de extradición y la autoridad judicial competente examina si la solicitud tienen motivos razonables o causa probable para creer que la persona requerida cometió el delito que se le imputó o si la solicitud proporciona una prueba de culpabilidad *prima facie* que sería suficiente para justificar que el acusado sea procesado en el Estado requerido[74]. En vista de que la prueba *prima facie* ha demostrado ser en la práctica un impedimento considerable para la extradición, no solo entre los sistemas de tradiciones jurídicas diferentes, sino también entre países con las mismas tradiciones pero con distintas normas relativas a las pruebas, y dado que varios Estados de tradición jurídica consuetudinaria ya no aplican este requisito en ciertas circunstancias prescritas, se recomienda que los Estados Miembros reduzcan al mínimo la carga de la prueba en los procedimientos de extradición y consideren en sus relaciones de extradición la necesidad de simplificar los requisitos probatorios (véanse también el artículo 16, párrafo 8, de la Convención contra la Delincuencia Organizada y el artículo 44, párrafo 9, de la Convención de las Naciones Unidas contra la Corrupción).

La orden de detención europea

Aunque este mecanismo se utiliza únicamente dentro de la Unión Europea, es importante tenerlo en cuenta como una herramienta para la cooperación internacional[75], ya que la cantidad de casos tratados en la Unión Europea hasta el momento pone de manifiesto su

[74] Véase, entre otros, el Manual revisado sobre el Tratado modelo de extradición, Comisión de Prevención del Delito y Justicia Penal, 13º período de sesiones (Viena, 11 a 20 de mayo de 2004), E/CN.15/2004/CRP.11, páginas 32 y 33, párrafo 108.

[75] Para una presentación detallada del instrumento, véase: *Kreijzer/Van Sliedregt*, The European Arrest Warrant in Practice, T.M.C Asser Press, 2009.

eficacia para hacer frente al fraude de tarjetas de crédito y a las actividades de peska[76]. Este tipo de cooperación fue introducida por la Decisión Marco 2002/584/JAI, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros[77] de acuerdo con las principales políticas penales que el Consejo Europeo introdujo en el ámbito de la Unión Europea en el marco del programa de Tempere[78]. El proceso de la orden de detención europea (ODE) ha sido valorado por unos y criticado por otros, ha ocasionado problemas constitucionales en algunos Estados miembros[79] y se encuentra en proceso continuo de evaluación[80].

Si se lo compara con los procedimientos de extradición anteriores, el proceso de la ODE presenta los siguientes cambios:

Procedimientos expeditivos: la decisión final sobre la ejecución de la orden de detención europea debería tomarse dentro de un plazo máximo de 90 días tras la detención de la persona requerida. Si dicha persona decidiera entregarse, la decisión se tomaría dentro de los 10 días siguientes (artículo 17).

Abolición del requisito de doble incriminación en los casos prescritos: el principio de doble incriminación, profundamente arraigado en la ley de extradición tradicional, no se comprobará en la lista de los 32 delitos, lo cual, de acuerdo con el artículo 2, párrafo 2, de la Decisión Marco, debería ser sancionable en el Estado miembro emisor por un período máximo de al menos 3 años de prisión y definido por la ley en ese Estado miembro. Estos delitos incluyen, entre otras cosas, la participación en una organización delictiva, el terrorismo, el tráfico de personas, la explotación sexual de menores y la pornografía infantil, el tráfico ilícito de estupefacientes y sustancias sicotrópicas, el tráfico ilícito de armas, municiones y explosivos, la corrupción, el fraude, incluido el que afecte los intereses financieros de las comunidades europeas, el blanqueo de capitales producto de actividades delictivas, los delitos informáticos, los delitos medioambientales, la facilitación de la entrada y residencia no autorizada, el asesinato y agresión con lesiones graves, la violación, el racismo y la xenofobia, el tráfico de vehículos robados, la falsificación de dinero, etc. Respecto de los delitos que no están incluidos en esta lista, o no entran en el umbral de los 3 años, sigue siendo aplicable el principio de doble incriminación (artículo 2, párrafo 4).

[76] Véase, por ejemplo, los informes de Eurojust de 2007 y 2008, donde se mencionan acciones conjuntas respecto a la ejecución de la orden de detención europea emitida para los casos de peska y *skimming*, disponible en: http://www.eurojust.europa.eu/.

[77] Publicado en el Diario Oficial L 190, 18.07.2002, páginas 1 a 20.

[78] Es por todos sabido que el consenso de los Estados miembros y la idea detrás de esta decisión marco surgió tras los ataques terroristas del 11 de septiembre, los que determinaron una respuesta clara y rápida de la Unión Europea a través de la creación de un instrumento que habría facilitado la lucha contra el terrorismo y los delitos graves.

[79] Alemania, Polonia y Chipre fueron tres de los Estados miembros donde los Tribunales Constitucionales presentaron decisiones en contra de la constitucionalidad de las leyes nacionales de transposición de la decisión marco. Para más detalles, véase European Handbook on How to Issue a European Arrest Warrant in Instruments on Judicial Cooperation in Criminal Matters within the Third Pillar of the European Union and other Essential International Instruments on Judicial Cooperation, Consilium July 2009, página 490 y ss. Las primeras dos decisiones se encuentran disponibles en inglés, como sigue: el juicio de 27 de abril de 2005 del Tribunal Constitucional polaco, P 1/05 en: http://www.trybunal.gov.pl/eng/summaries/summaries_assets/documents/P_1_05_full_GB.pdf, el juicio de 18 de julio de 2005, 2 BvR 2236/04 del Tribunal Constitucional Federal alemán, en: http://www.bundesverfassungsgericht.de/en/decisions/rs20050718_2bvr223604en.html.

[80] Se llevaron a cabo varias rondas de evaluación desde que se introdujo la orden de detención europea en los sistemas jurídicos de los Estados miembros de la UE: las evaluaciones más recientes en el marco de la Cuarta Ronda de Evaluación Recíproca tuvieron lugar a finales de 2008 y se referían a Bulgaria y Rumania.

"Judicialización" de la entrega: el nuevo procedimiento de entrega basado en la ODE se transfiere del poder ejecutivo al judicial. Tanto la autoridad emisora como la ejecutora son consideradas las autoridades judiciales competentes para expedir o ejecutar una orden de detención europea en virtud de la legislación del Estado miembro emisor o ejecutor (artículo 6). En consecuencia, dado que el procedimiento para la ejecución de una orden de detención europea es principalmente judicial, la fase administrativa inherente a los procedimientos de extradición, es decir, la competencia de la autoridad ejecutiva para dictar la decisión final respecto de la entrega de una persona que reclama el Estado requirente, queda derogada.

Entrega de nacionales: los Estados miembros de la Unión Europea ya no pueden negarse a entregar a sus nacionales. En la Decisión Marco no se contempla la nacionalidad como motivo obligatorio ni facultativo para la no ejecución. Además, en el artículo 5, párrafo 3, se dispone la opción de condicionar la ejecución de la orden a una garantía de que la persona, tras haber declarado, sea devuelta a su país para cumplir la pena.

Abolición de la excepción del delito político: la excepción del delito político no se enumera como motivo obligatorio o facultativo para la no ejecución de una orden de detención europea. El único elemento restante de esta excepción se limita a los considerandos del preámbulo de la Decisión Marco (considerando 12) y adopta la forma de versión actualizada de una cláusula de no discriminación.

Desviación adicional de la norma de especialidad: en el artículo 27, párrafo 1, de la Decisión Marco se permite a los Estados miembros notificar a la Secretaría General del Consejo que, en sus relaciones con otros Estados miembros que han presentado la misma notificación, se presume que se dio consentimiento para el procesamiento, condena o detención con vistas a llevar a cabo una pena privativa de libertad u orden de detención por un delito que se cometió antes de la entrega distinto de aquel para el cual se entregó la persona en cuestión.

Canales y medios de comunicación

Este constituye otro elemento importante que diferencia a la orden de extradición europea del sistema tradicional de extradición, en el sentido de que promueve el contacto directo entre las autoridades judiciales, requeridas o requirentes, lo que elimina intermediarios tales como los canales diplomáticos o las autoridades centrales. Estas últimas continúan funcionando cuando el sistema legal así lo permite, siendo responsables de la transmisión y recepción administrativas de la orden de detención europea[81]. Para la transmisión de la orden de detención, la Decisión Marco permite el uso del fax o del correo electrónico[82]. El contacto directo y el uso de medios de comunicación expeditivos representan una ventaja significativa en la lucha contra el delito relacionado con la identidad al cual debe darse un tratamiento adecuado.

[81] Algunos Estados miembros como Italia, el Reino Unido e Irlanda, utilizan esta disposición en todos los casos para que las órdenes de detención europeas sean recibidas y transmitidas únicamente a través de los Ministerios de Justicia.

[82] En el artículo 10, párrafo 4, de la Decisión Marco se establece que "la autoridad judicial emisora podrá transmitir la orden de detención europea por cualesquiera medios fiables que puedan dejar constancia escrita en condiciones que permitan al Estado miembro establecer su autenticidad". Algunos Estados miembros condicionan la entrega del delincuente a la presentación de los documentos originales que emanan de la autoridad judicial requirente.

La orden de detención de CARICOM

Otro instrumento regional similar a la orden de detención europea es la orden de detención de CARICOM, que fue establecida por los Estados de la región del Caribe por conducto del Tratado de la orden de detención de CARICOM[83]. Fue adoptada en 2008 y, debido a que facilita el contacto de las autoridades judiciales de los Estados requirente y requerido, promueve un procedimiento de extradición simplificado[84].

De acuerdo con la definición prevista en el artículo I, "la orden de detención de CARICOM es una orden de arresto expedida por la autoridad judicial emisora de un Estado Parte [...] con miras a detener y entregar a la persona solicitada por la autoridad judicial de otro Estado Parte a fin de llevar a cabo un proceso judicial o ejecutar una pena privativa de libertad". Al igual que la orden de detención europea, el instrumento menciona la celeridad[85] y también utiliza el término "entrega".

La transmisión y recepción de la orden de arresto de CARICOM se efectúa por conducto de las autoridades centrales, si bien la decisión de emitir o ejecutar una orden de arresto corresponde a las autoridades judiciales: el instrumento permite el uso de medios de comunicación expeditivos[86].

Asistencia judicial recíproca y particularidades que surgen de los delitos relacionados con la identidad

Las solicitudes de asistencia judicial recíproca (AJR) son fundamentales para la resolución de casos transnacionales. Es imposible abordar los delitos relacionados con la identidad de manera eficaz si no se cuenta con una colaboración inmediata y eficaz de parte de las autoridades policiales y judiciales de todo el mundo. Mientras que los enfoques regionales pueden resultar suficientes en los casos típicos de AJR, no lo son en los casos de los delitos relacionados con la identidad. Una solicitud de asistencia judicial típica implica la participación de un Estado requirente y un Estado requerido. Esto no siempre sucede en el caso de los delitos relacionados con la identidad. En muchas ocasiones es necesario transmitir las solicitudes a más de un país, incluso existen situaciones en las que las solicitudes se envían a tres continentes, en particular en los casos de fraude y falsificación informáticos. Este es un ejemplo del carácter transnacional de los delitos relacionados con la identidad.

La mayoría de las solicitudes de asistencia judicial recíproca se emiten durante la fase previa al juicio, teniendo en cuenta que en muchos casos la acusación se basa en pruebas o información obtenidas en el extranjero. Asimismo existen solicitudes que se formulan durante las actuaciones judiciales, como la citación de las partes afectadas, las audiencias o las solicitudes de información tales como los antecedentes penales de posibles delincuentes.

---

[83] CARICOM es la abreviación de Comunidad del Caribe. Para obtener una lista de los Estados miembros y miembros asociados, véase: http://www.caricomlaw.org.

[84] El texto del Tratado se encuentra disponible en: www.caricom.org/jsp/secretariat/legal_instruments/caricom_arrest_warrant_treaty.pdf

[85] Véase el artículo X del Tratado: en el caso en que la persona acepte ser entregada, la decisión de la autoridad judicial debe tener lugar dentro de las 48 horas siguientes de haberse dado el consentimiento.

[86] Véase el artículo VII del Tratado.

Antes de analizar los desafíos que plantea el carácter transnacional de los delitos relacionados con la identidad, cabe destacar que, en general, los principios que se presentan en la sección de extradición siguen siendo, hasta cierto punto, válidos y aplicables con respecto a la asistencia judicial recíproca (por ejemplo, los principios de la doble criminalidad, *ne bis in idem*, consideraciones de derechos humanos y la reciprocidad en ausencia de un tratado aplicable).

Existen varios tipos de solicitudes de asistencia judicial recíproca: la carta rogatoria (peticiones de diversa índole), los testimonios o declaraciones de los sospechosos, víctimas y testigos, en ocasiones, a través de videoconferencia, la presentación de documentos judiciales, el embargo con carácter preventivo o la confiscación de activos. En lo que respecta a las solicitudes de asistencia judicial recíproca en los casos del delito de identidad con carácter transnacional, también resultan relevantes los equipos conjuntos de investigación o los puntos de contacto permanente (redes 24/7) establecidos para prestar asistencia inmediata en los casos de delitos cibernéticos.

Además, existen nuevas formas de asistencia recíproca que resultan de gran utilidad para este tipo de delitos. En la actualidad, estas nuevas formas de asistencia introducidas por el Convenio del Consejo de Europa sobre el delito cibernético se utilizan con más frecuencia en los casos de delitos relacionados con la identidad. Su propósito es garantizar una respuesta rápida de los Estados requeridos a través de la conservación inmediata de los datos informáticos almacenados, la asistencia recíproca respecto del acceso a dichos datos, la asistencia judicial recíproca en la recopilación de información del tránsito en tiempo real o la asistencia judicial recíproca con respecto a la intercepción de datos de contenido (véanse, los artículos 29 a 34 del Convenio del Consejo de Europa sobre el delito cibernético, el cual se presentará en las secciones pertinentes de esta guía).

A continuación se presenta un breve resumen de las dificultades que plantearon los casos de delitos relacionados con la identidad en los que se solicitó asistencia judicial recíproca.

Variedad de instrumentos jurídicos aplicables

En el momento de formular una única solicitud, podría haber más de un instrumento jurídico internacional por considerar. Por tanto, la autoridad judicial que formula la solicitud necesita saber si existe algún instrumento jurídico que tenga preeminencia sobre otro, en el caso en que hubiese varios Estados requeridos, y cuál es el convenio que se aplica en cada uno de ellos. Esto resulta de suma importancia para determinar el instrumento jurídico apropiado, ya que muchos Estados todavía cuentan con requisitos formales muy estrictos y podrían negarse a ejecutar la solicitud si la asistencia se solicita sobre la base de un tratado de no aplicación. En uno de los subcapítulos a continuación se presenta una reseña sobre los tratados regionales e internacionales que son o podrían ser utilizados con respecto a los delitos relacionados con la identidad. Cabe destacar que si bien algunos tratados aceptan la utilización de nuevos medios de comunicación que favorecen la rapidez, otros siguen requiriendo que la transmisión de solicitudes se realice a través de la vía diplomática[87].

[87] Por ejemplo, la legislación coreana en este ámbito establece una regla para la asistencia judicial recíproca, exigiendo que se transmita o reciba una solicitud únicamente a través de la vía diplomática. Sin embargo, en los casos urgentes, se permite el uso del fax y del correo electrónico. Para más detalles, véase: *Knoops/Brenner*, Cybercrime and Jurisdiction, A Global Survey, Asser Press 2006, página 271.

Volatilidad de los datos

Como se mencionó en la introducción, esta guía hace hincapié en los casos de delitos relacionados con la identidad, ya se cometan en línea o a través de las tecnologías de la información, dado que es más probable que estos casos tengan una dimensión transnacional. Mientras que los procesos de transferencia utilizando la tecnología de redes se pueden completar en cuestión de segundos, la prestación de servicios de asistencia judicial recíproca es lenta cuando se utilizan los canales o medios de comunicación "convencionales". Existen ocasiones en que es fundamental que las solicitudes relacionadas con las direcciones IP o el envío de archivos de registro sean tratados con prontitud para poder continuar con la investigación. Sin embargo, el tipo y precisión de la respuesta dependen del tiempo que se necesita para enviar la solicitud de asistencia judicial a la autoridad ejecutora[88]. En los casos de "skimming", si la solicitud no se formula y ejecuta de manera oportuna, la cinta de vídeo de un cajero automático situado en otro país podría no conservarse, ya que los bancos en muchos países guardan las cintas de vídeo por períodos cortos. Este tipo de peticiones deben ser tratadas con urgencia, utilizando medios de comunicación expeditivos, tales como el fax o el correo electrónico.

Requisito de doble incriminación

Como se mencionó anteriormente, la doble incriminación es uno de los principales principios de la cooperación internacional. Este se deriva de la soberanía y los principios de legalidad y, dependiendo del instrumento jurídico en vigor, también es aplicable en lo que respecta a las solicitudes de asistencia recíproca[89]. Cabe destacar que la convergencia de disposiciones jurídicas sustantivas con respecto a los delitos relacionados con la identidad podría ayudar a superar los obstáculos o dificultades que plantea esta exigencia.

Sin embargo, en vista de que muchos de los motivos para denegar una solicitud de asistencia judicial recíproca contemplados actualmente en los instrumentos bilaterales, regionales o multilaterales constituyen el remanente de tratados, leyes y prácticas de extradición en los que la vida o la libertad de la persona requerida se encuentran directa e inmediatamente en juego[90], los Estados deberían considerar si es necesario mantener estos motivos de denegación o reducirlos al mínimo y utilizarlos ocasionalmente. Asimismo, debería considerarse si se conserva o no el requisito de la doble incriminación en los programas de asistencia judicial recíproca en su conjunto.

Una manera posible de superar los problemas que plantea el requisito de "etiquetas jurídicas idénticas" es garantizar que en la determinación de la aplicación de la doble incriminación, la conducta constitutiva del delito se tome en cuenta independientemente de la denominación o categorización del delito en virtud de las leyes de los Estados requerido y requirente[91].

---

[88] Para acceder a algunos ejemplos prácticos sobre la lentitud de la asistencia recíproca tradicional y los impedimentos que surgen a causa de un proceso tan lento, véase: *Elston/Scott*, International Cooperation in On-line Identity Theft Investigations: A Hopeful Future but a Frustrating Present, disponible en http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

[89] Véase el artículo 18, párrafo 9, de la UNTOC, el cual estipula que "Los Estados Parte podrán negarse a prestar la asistencia judicial recíproca con arreglo al presente artículo invocando la ausencia de doble incriminación".

[90] Véase el informe de la UNODC "Expert Working Group on Mutual Legal Assistance Casework Best Practice" (Viena, 3 a 7 de diciembre de 2001), página 11. El informe se encuentra disponible en: http://www.unodc.org/pdf/lap_mlaeg_report_final.pdf.

[91] Véase, en particular, el artículo 43, párrafo 2, de la Convención de las Naciones Unidas contra la Corrupción.

Conflictos positivos de jurisdicción

El problema de la jurisdicción[92] es una de las principales cuestiones que se plantean en el debate sobre la delincuencia transnacional. Como destacan los profesionales, cuando se trata de abordar los delitos cibernéticos y relacionados con la identidad, con frecuencia es difícil determinar si se ha cometido un delito y cuál es el Estado que tiene derecho a someter a los delincuentes a la justicia. Las reivindicaciones relativas a la jurisdicción planteadas por varios Estados llevaron a que surgieran los conflictos de jurisdicción positivos. Esto sucede a menudo en los casos de fraude informático, falsificación o clonación de tarjetas de crédito, ya que ambos Estados, donde se encuentran la víctima y el delincuente, llevan a cabo investigaciones paralelas.

Existe gran controversia en los textos especializados respecto a cuál de los Estados tiene más derecho a tener prioridad y hasta qué punto se puede aplicar la jurisdicción extraterritorial en los casos relacionados con Internet[93]. Las disposiciones relativas al intercambio espontáneo de información o al principio *aut dedere aut judicare* podrían mejorar parcialmente una situación general. En ausencia de un marco jurídico adaptado a este contexto, la cooperación continua y los contactos entre las autoridades policiales en tiempo real son clave en la prevención de la aparición de estos conflictos de jurisdicción.

Ejecución de las solicitudes de asistencia judicial recíproca en un Estado extranjero

Una de las mayores dificultades respecto de la prestación de asistencia judicial recíproca es la necesidad de utilizar un formulario admisible en el sistema jurídico del Estado requirente en el momento de preparar la solicitud. En vista de las diferencias existentes entre los sistemas jurídicos de los Estados miembros, el Estado requerido podría tener requisitos específicos, por ejemplo, para la obtención de una orden judicial o para tomar declaración a las personas desconocidas para el Estado requirente, todo lo cual genera atrasos, gastos innecesarios y frustración. Por tanto, es importante que los marcos jurídicos de los Estados miembros sean lo suficientemente flexibles y adaptables para asistir a una variedad de países y sistemas jurídicos diferentes. Por ejemplo, en el artículo 18, párrafo 17, de la UNTOC se establece que se dará cumplimiento a toda solicitud con arreglo al derecho interno del Estado Parte requerido y en la medida en que ello no lo contravenga y sea factible, de conformidad con los procedimientos especificados en la solicitud. Del mismo modo, en el Tratado modelo de asistencia recíproca en asuntos penales[94] se prevé el

[92] El problema de la jurisdicción en Internet se examina exhaustivamente en *Koops/Brenner*, "Cybercrime and Jurisdiction, A Global Survey", Asser Press 2006; *Kohl*, "Jurisdiction and the Internet, A Regulatory Competence over Online Activity, Cambridge University Press, 2007; o *Kaspersen*, "Cybercrime and Internet Jurisdiction, A Discussion Paper prepared under the Council of Europe Project on Cybercrime", 5 de marzo de 2009, disponible en: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf

[93] Véanse, por ejemplo, *Koops*, "Cybercrime Jurisdiction: Introduction, in *Koops/Brenner*, Cybercrime and Jurisdiction", *supra* núm. 87, página 6; Brenner, "The Next Step: Prioritizing Jurisdiction", *Ibid.*, página 327 y ss. *Goldsmith*, "The Internet and the Legitimacy of Remote-Cross-border Searches", 1 University of Chicago Legal Forum 103 (2001), disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732; *Seitz*, Transborder Search, A New Perspective?, *7 Yale Journal of Law and Technology* 23, 2004-2005.

[94] Aprobado por la resolución 45/117 de la Asamblea General, de 14 de diciembre de 1990, y posteriormente enmendado según la resolución 53/112 de la Asamblea General, de 9 de diciembre de 1998.

cumplimiento de la solicitud en la forma que haya indicado el Estado requirente "en la medida que sea compatible con sus leyes y prácticas" (artículo 6)[95].

Para superar las dificultades antes mencionadas, los Estados miembros podrían considerar alternativas tales como la designación de personas de enlace[96] en las autoridades centrales de países de la misma región o en países clave dentro de una región o continente en los que la magnitud o la utilidad de la cooperación justifiquen tal medida. Dicha iniciativa podría resultar muy efectiva y dar resultados satisfactorios, particularmente en los casos complejos y urgentes, dado que los oficiales de enlace facilitan la manera en que se realizan y ejecutan las solicitudes. Asimismo, podría disminuir considerablemente la cantidad de papel que se utiliza y las demoras inevitables en toda gestión de documentos, como sucede con frecuencia, cuando las solicitudes no cumplen con las leyes o los procedimientos del Estado requerido[97]. La utilización de redes regionales también podría ser de gran utilidad en el cumplimiento de esta tarea.

Cooperación informal[98]

Los delitos relacionados con la identidad que se cometen en línea con frecuencia se llevan a cabo en un período muy corto de tiempo y es necesario que las investigaciones sean rápidas para asegurar que no se destruye la información relevante mientras tanto. En vista de esto, las herramientas tradicionales de asistencia judicial recíproca deben adaptarse en consecuencia para ser eficientes y eficaces. En algunas ocasiones, la información que se recopila mediante la cooperación informal puede utilizarse para reunir la información necesaria para acelerar el proceso formal. Por tanto, la cooperación policial que se lleva a cabo en el marco de instituciones tales como Interpol o Europol reviste gran importancia. Esta información puede, por ejemplo, ser utilizada para recoger datos iniciales de identificación de posibles delincuentes, una cuestión preliminar en la investigación y procesamiento del delito relacionado con la identidad. Sin embargo, este tipo de cooperación interpolicial o entre las fuerzas del orden no se refiere a la recolección de las pruebas para los procedimientos judiciales, siempre que tal actividad requiera en general una solicitud formal. En general, la cooperación informal está intrínsicamente vinculada a los datos a disposición del público. Por regla general, los instrumentos internacionales, regionales y bilaterales contienen disposiciones que tratan este tipo de cooperación bajo títulos, tales como "La cooperación de las fuerzas del orden"[99]. Otros métodos de cooperación informal incluyen el intercambio de memorandos de entendimiento y acuerdos administrativos recíprocos[100].

[95] Véase el Manual revisado sobre el Tratado modelo de asistencia recíproca en asuntos penales, Comisión de Prevención del Delito y Justicia Penal, 13º período de sesiones (Viena, 11 a 20 de mayo de 2004), E/CN.15/2004/CRP.11, página 96 y ss.

[96] Un subcapítulo separado de la guía hará referencia a la institución del magistrado de enlace.

[97] Véase el Grupo de trabajo oficioso de expertos sobre las mejores prácticas de extradición, Viena, 2004, página 14. El informe se encuentra disponible en: http://www.unodc.org/unodc/en/legal-tools/training-tools-and-guidelines.html.

[98] Las ventajas de la cooperación informal y las condiciones bajo las cuales esta cooperación puede llevarse a cabo pueden consultarse en el informe del Grupo de trabajo oficioso especializado en prácticas óptimas de asistencia judicial recíproca, Viena, 2001, página 9, *supra* núm. 90.

[99] Véase, por ejemplo, el artículo 27 de la UNTOC.

[100] Véase *Bantekas/Nash*, "International Criminal Law", *supra* núm. 57, página 405.

Equipos conjuntos de investigación

Los equipos conjuntos de investigación constituyen otra importante forma de cooperación internacional. La idea detrás de esta modalidad de cooperación es facilitar la asistencia judicial recíproca en los casos transnacionales donde las cuestiones que sean objeto de investigación, procesamiento o actuación judicial involucren a más de un Estado. Por tanto, delitos tales como el tráfico de drogas, el tráfico de personas y los relacionados con la identidad, que revisten un carácter transnacional, también se pueden abordar a través de los equipos conjuntos de investigación.

En algunas ocasiones la legislación interna de muchos países permite iniciativas de colaboración y cooperación y prácticas de investigación conjuntas. Sin embargo, la experiencia apunta a que todavía existen dificultades jurídicas y de otro tipo para el establecimiento de investigaciones conjuntas eficaces.

Así, su base jurídica se puede encontrar en la legislación (legislación sobre asistencia judicial recíproca, sobre cooperación internacional, incluido el uso transfronterizo de técnicas de investigación tales como la vigilancia, las operaciones encubiertas, el código de procedimiento penal, la legislación específica sobre investigaciones conjuntas), o directrices administrativas, procedimientos de funcionamiento, prácticas de cooperación duraderas y acuerdos en función de cada caso.

El alcance de la legislación necesaria depende del modelo de investigación conjunta utilizado. En la práctica, se han elaborado dos modelos de investigación conjunta: el primero consiste en investigaciones paralelas y coordinadas, que se llevan a cabo en distintos lugares pero persiguen un objetivo común y cuentan con la cooperación de las fuerzas del orden y del proceso formal de asistencia judicial recíproca. Los funcionarios involucrados no comparten el mismo espacio físico y están habilitados para trabajar conjuntamente sobre la base de las prácticas de cooperación duradera o de la legislación de asistencia judicial recíproca vigente, o ambas, dependiendo de la naturaleza de los sistemas jurídicos que intervienen.

El segundo modelo es un modelo integrado que puede además caracterizarse por ser pasivo o activo, dependiendo del alcance de los poderes de las fuerzas del orden disponible para los agentes participantes. Un ejemplo de un equipo integrado pasivo podría ser una situación en la que un oficial extranjero encargado de hacer cumplir la ley coopera con oficiales del país anfitrión en el desempeño de tareas de asesoramiento o consultoría o en calidad de asistente técnico en el país de acogida. Un equipo integrado activo podría incluir funcionarios de al menos dos jurisdicciones que tengan la capacidad de ejercer las competencias operativas en el marco del control del Estado anfitrión en un territorio o jurisdicción determinado.

Los problemas particulares relacionados con el establecimiento de investigaciones conjuntas en áreas específicas de la actividad delictiva incluyen, entre otras cosas, lo siguiente: la falta de puntos de contacto para las investigaciones conjuntas; la falta de claridad en la selección de funcionarios competentes para autorizar las investigaciones conjuntas; la necesidad de que exista un ambiente de confianza, un compromiso y objetivos comunes; la necesidad de que se disponga de recursos y una planificación operativa que incluya estructuras de gestión; la necesidad de garantizar la seguridad de la información operativa; y la falta de una capacitación adecuada para los funcionarios de justicia penal.

Con respecto a los instrumentos internacionales que se encargan de los equipos conjuntos de investigación, en el artículo 19 de la UNTOC se alienta a los Estados, aunque no se les obliga, a que establezcan acuerdos o arreglos para crear órganos mixtos de investigación respecto de los asuntos que son objeto de investigaciones, procesos o procedimientos en más de un Estado. Asimismo, a falta de dichos acuerdos, se alienta a los Estados a que establezcan una base jurídica para la cooperación en función de cada caso, sujeto a la soberanía nacional del Estado anfitrión donde se realiza la investigación conjunta. La UNCAC también contiene una disposición similar (artículo 49).

En el ámbito de la Unión Europea, se hizo referencia a una investigación conjunta, por ejemplo, en el Tratado de Amsterdam[101] y se trató con más detalle durante la reunión extraordinaria del Consejo de Europa en Tampere[102].

A nivel de la UE existe en la actualidad un marco jurídico dual respecto de los equipos conjuntos de investigación. La mayoría de los Estados miembros de la UE[103] promulgaron leyes en todas las esferas pertinentes, de conformidad con el artículo 13 del Convenio europeo de asistencia judicial en materia penal de 2000, que proporciona un marco integral para el establecimiento de los equipos conjuntos de investigación[104]. Debido a que el proceso de ratificación de la Convención de la UE era demasiado lento, se incorporaron los artículos 13, 15 y 16 que hacen referencia a los equipos conjuntos de investigación en una decisión marco del Consejo separada, la cual fue adoptada en 2002. Era necesario incorporar la decisión marco en la legislación de los Estados miembros de la UE y en 2003 se complementó con la recomendación del Consejo sobre un modelo de acuerdo (véase *infra*). La aplicación de la decisión cesará cuando el Convenio de 2000 entre en vigor para todos los Estados miembros[105]. En el artículo 20 del Segundo Protocolo Adicional del Convenio Europeo de Asistencia Recíproca del Consejo de Europa de 1959 se puede encontrar un enfoque casi idéntico respecto de los equipos conjuntos de investigación.

Debido a su carácter y objetivos, Eurojust cuenta con una visión general de las investigaciones conjuntas de la UE, así como con acuerdos relevantes de investigaciones conjuntas (operacionales). Además, Eurojust como organización, o a través de sus miembros nacionales, puede pedir a los Estados miembros de la UE que establezcan un equipo conjunto de investigación o que participen en dicho equipo, o ambas cosas. Eurojust está capacitada para identificar los casos potenciales idóneos para los equipos conjuntos de investigación, para facilitar los contactos entre la UE y los Estados miembros, y está habilitada para organizar reuniones de coordinación a fin de estudiar la formación de los equipos conjuntos de investigación. Además, puede proporcionar apoyo para superar las barreras lingüísticas brindando servicios de interpretación, y puede asimismo cooperar con diversos países no miembros de la UE a través de puntos de contacto y acuerdos. En 2005, bajo los

[101] Para una evolución histórica de los equipos conjuntos de investigación, véase: *Rijken*, Joint Investigation Teams: principles, practice and problems. Lessons learnt from the first efforts to establish a JIT in *Utrecht Law Review*, vol. 2, Tomo 2, página 99 y ss.

[102] A este respecto, véase la Conclusión núm. 43 del Consejo de Europa en Tampere, cuyo texto se encuentra disponible en: http://www.europarl.europa.eu/summits/tam_en.htm#c.

[103] A junio de 2009, Italia y Grecia no habían ratificado el Convenio de la UE de 2000. Véase, al respecto, el Manual de los equipos conjuntos de investigación, disponible en todos los idiomas de la UE en: http://www.eurojust.europa.eu/jit_manual.htm.

[104] Más adelante se presenta información adicional sobre el marco dentro de la Unión Europea en el contexto del Convenio de 2000.

[105] Véase el Manual de los equipos conjuntos de investigación, disponible en todos los idiomas de la UE en: http://www.eurojust.europa.eu/jit_manual.htm, página 4.

auspicios de Eurojust, se creó la red de expertos en equipos conjuntos de investigación, la cual se reúne periódicamente para intercambiar información y prácticas óptimas con el fin de mejorar el funcionamiento de los equipos a nivel de la UE[106].

Dentro del contexto de la Unión Europea, se utilizó como punto de partida para las negociaciones entre las autoridades nacionales pertinentes de los Estados miembros un acuerdo tipo elaborado por recomendación del Consejo de la UE de 8 de mayo de 2003, que se basa en las disposiciones de la Convención de la UE de 2000. Teniendo en cuenta la necesidad que manifestaron los profesionales de disponer de un modelo actualizado, también reconocida en el Programa de Estocolmo[107], el acuerdo tipo fue recientemente reemplazado de conformidad con la resolución del Consejo de 26 de febrero de 2010, sobre un acuerdo tipo para la creación de un equipo conjunto de investigación (2010/C 70/01)[108]. Este modelo hace una distinción entre las condiciones generales y las especiales. Los prerrequisitos generales son: las partes de la investigación conjunta (organismos encargados de hacer cumplir la ley, autoridades judiciales), el propósito de la investigación conjunta, los plazos (y fechas de revisión), la designación de los Estados miembros en los cuales funcionarán los equipos conjuntos de investigación, el (los) Estado(s) desde donde se llevarán a cabo las operaciones del equipo conjunto, así como cualquier disposición específica del acuerdo. Respecto de este último punto, las condiciones especiales podrían incluir, entre otras cosas, lo siguiente: las condiciones bajo las cuales se permite a los miembros en comisión de servicio participar o ser excluidos de las tareas de investigación o las circunstancias específicas en las que un miembro en comisión de servicio podría solicitar a su propia autoridad nacional que tome las medidas que el equipo solicite sin tener que presentar una carta formal solicitando asistencia judicial recíproca.

A pesar de que en el ámbito de la UE el funcionamiento de los equipos conjuntos de investigación fue bastante lento[109] y aún tiene cosas para mejorar, las tendencias recientes muestran que los Estados miembros de la UE han comenzado a considerar la importancia de esta forma de cooperación, dado el rápido aumento de la delincuencia transnacional. Asimismo, los aspectos jurídicos y prácticos relativos a los equipos conjuntos de investigación han logrado ocupar un lugar destacado en foros pertinentes de las Naciones Unidas[110].

[106] Para una lista de las conclusiones adoptadas por el grupo de expertos, véase http://www.eurojust.europa.eu/jit_meetings.htm.

[107] A este respecto, véase el punto 4.3.1 del Programa de Estocolmo, disponible en: http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf.

[108] El texto de la resolución del Consejo se encuentra disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:070:0001:0012:Es:PDF.

[109] A 15 de mayo de 2007, se habían establecido únicamente 18 equipos conjuntos de investigación. Véase "Implementation of the European Arrest Warrant and Joint Investigation Teams at EU and National Level", página 33, disponible en línea en: http://www.statewatch.org/news/2009/feb/ep-study-european-arrest-warrant.pdf.

[110] Véanse el informe del 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, párrafo 233 (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V05/844/09/PDF/V0584409.pdf?OpenElement), y el informe del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, párrafo 188 (http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf).

III. CONVENIOS APLICABLES EN LOS CASOS DE COOPERACIÓN JUDICIAL INTERNACIONAL DE LUCHA CONTRA EL DELITO RELACIONADO CON LA IDENTIDAD Y LOS ASUNTOS PRÁCTICOS QUE SURGEN DE SU APLICACIÓN

1. La importancia de identificar el instrumento aplicable

Cuando se aborda un caso práctico de un delito relacionado con la identidad, ya se trate de una solicitud de extradición o de asistencia judicial recíproca, es fundamental seguir ciertos pasos para asegurarse de que el Estado requerido ejecutará correctamente dicha solicitud. El primer elemento importante para la ejecución de la solicitud es identificar el instrumento jurídico aplicable para el caso en cuestión.

Esto ayudará a que el Estado requirente identifique la información necesaria relacionada con el procedimiento. En el caso de una extradición, el Estado requirente, por ejemplo, sobre la base de la convención o el tratado bilateral aplicable, identificará:

- El período de tiempo dentro del cual deberán presentarse la solicitud y la documentación complementaria, en caso de que la persona haya sido detenida de manera provisoria con fines de extradición;
- Los documentos anexos que deben adjuntarse y otros requerimientos de procedimiento que deben cumplirse;
- Los canales y medios de comunicación;
- La relación con otros instrumentos internacionales pertinentes. En particular, en los casos en que estén en vigor y sean aplicables un tratado de extradición bilateral y otro multilateral, la autoridad judicial del Estado requirente deberá saber cuál aplicar[111];
- El idioma en el cual se deberá presentar la solicitud. Normalmente, se utiliza el idioma oficial del Estado requerido. Si el Estado tiene más de un idioma oficial, solo puede utilizarse uno de ellos. Algunos países también pueden aceptar idiomas distintos del suyo[112].

[111] Por ejemplo, el Convenio europeo sobre extradición de 1957 estipula en su artículo 28 que "el Convenio abroga, en lo que concierne a los territorios en los cuales se aplica, las disposiciones de los Tratados, Convenios o Acuerdos bilaterales que regulen la materia de la extradición entre las Partes contratantes", mientras que otros convenios, como el Convenio del Consejo de Europa sobre el delito cibernético, en su artículo 39, párrafo 2, confiere preeminencia a instrumentos ya existentes.

[112] Esta disposición resulta muy útil (en particular en los casos urgentes), y es promovida normalmente por aquellos países que tienen idiomas poco comunes. Por tanto, permitir que el Estado requirente cuente con un traductor de un idioma popular en Europa como son el inglés o el francés es relativamente más fácil. Por lo general, cada Estado hace una declaración al instrumento jurídico aplicable indicando los idiomas que está dispuesto a aceptar.

Esto mismo se aplica para las solicitudes de asistencia judicial recíproca. Es fundamental identificar el tratado aplicable para definir las medidas que deben adoptarse para la transmisión de la solicitud. Si el tratado permite un determinado tipo de solicitud de asistencia judicial, el próximo paso será formular la solicitud, seleccionando los canales y medios de comunicación, idiomas y plazos[113]. En los casos del delito relacionado con la identidad que sean de carácter transnacional, podrían aplicarse varios instrumentos internacionales y regionales[114].

Teniendo esto en cuenta, se presenta a continuación un resumen de los instrumentos jurídicos que tienen aplicación a nivel regional o internacional. Este resumen no constituye una lista exhaustiva, sino una mera ejemplificación de las herramientas legales que se pueden utilizar en los casos de cooperación internacional relativos a los delitos relacionados con la identidad. Algunos de estos instrumentos se centran en un campo específico de la cooperación (por ejemplo, la extradición o la asistencia judicial recíproca), mientras que otros, tales como la UNTOC o el Convenio del Consejo de Europa sobre el delito cibernético[115], contienen disposiciones relativas a la cooperación internacional en materia penal. Además, existen diversos tratados bilaterales, que por razones prácticas no se examinan en detalle en esta guía.

2. Convenios aplicables respecto del procedimiento de extradición

A continuación se presenta un breve resumen de los instrumentos regionales en materia de extradición, así como de los instrumentos multilaterales que contienen disposiciones sobre extradición que son de relevancia en los casos de delitos relacionados con la identidad, indicando los recursos en línea donde se pueden encontrar y destacando su relevancia. La guía ofrece más información analítica sobre la UNTOC y el Convenio del Consejo de Europa sobre el delito cibernético.

[113] A modo de ejemplo, se podría ofrecer el caso de citación de un acusado que debe estar presente en el juicio. Algunos países exigen que la solicitud sea transmitida con suficiente tiempo antes del plazo establecido para el juicio, a fin de poder enviar los documentos a esa persona antes del plazo especificado. A nivel europeo, muchos países han hecho declaraciones al artículo 7, párrafo 3, del Convenio del Consejo de Europa de asistencia judicial en materia penal de 1959, el cual permite a las partes establecer un plazo dentro del cual el Estado emisor debería transmitir los documentos necesarios: dicho plazo no deberá exceder los 50 días. Según el informe explicativo del Convenio, esta disposición era un compromiso de los sistemas jurídicos existentes a nivel europeo, algunos de los cuales no permiten que un juicio se celebre *in absentia*.

[114] Véase, por ejemplo, los casos prácticos que ofrece Rumania como respuesta al Cuestionario distribuido por el PC-OC sobre asistencia judicial recíproca en los casos informáticos, PC-OC (2008) 08, disponible en: http://www.coe.int/tcj (con referencia a la multitud de acuerdos que se necesitan para citar a las partes perjudicadas que se encuentran en diferentes países y continentes).

[115] Convenio del Consejo de Europa sobre el delito cibernético (STCE núm. 185), disponible en: http://conventions.coe.int. Para más detalles, véanse: *Sofaer*, Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, página 225, disponible en: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, página 140 y ss.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, página 7 y ss.; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, núm. 1, disponible en: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, *Themes and Critiques*, 2005, disponible en: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in *Policing: An International Journal of Police Strategies and Management*, 29(2), 2006, página 408 y ss.

Instrumentos regionales de extradición

Convenio europeo sobre extradición de 1957 y sus protocolos adicionales

El Convenio y sus dos protocolos adicionales (1975 y 1978) representan una herramienta de gran utilidad para abordar este tema entre los Estados miembros del Consejo de Europa, pese a que el Convenio "original" se remonta a 1957.

En el artículo 2 del Convenio se estipula que los delitos motivo de extradición serán aquellos sancionables con privación de libertad o bajo una orden de detención por un período máximo de al menos un año, tanto por el derecho del Estado requirente como por el Estado requerido. En el caso en que ya se haya pronunciado la sentencia, la sanción dispuesta debe ser de por lo menos 4 meses. La extradición será denegada si los delitos son de carácter militar o político, o si existen razones fundadas para creer que la persona requerida fue objeto de discriminación[116]. Por otro lado, los delitos fiscales pueden convertirse en delitos extraditables si las partes dan su consentimiento (por tanto es necesario un acuerdo previo). Asimismo, se puede denegar la extradición de nacionales cuando la nacionalidad se determina en el momento de tomar la decisión relativa a la extradición[117]. En el caso en que la parte requerida no extradite a sus nacionales, el Convenio establece la obligación del Estado requerido de hacerse cargo del procedimiento. En el artículo 9 se aborda el problema de *ne bis in idem* en relación con las sentencias finales. El Protocolo adicional al Convenio europeo sobre extradición aprobado en 1975 introdujo algunos cambios a este artículo. El Protocolo lo complementa aplicando el principio de extradición de una persona contra la cual se ha dictado una sentencia definitiva en un tercer Estado.

Como regla general, la comunicación de los documentos debe realizarse a través de la vía diplomática[118]. La duración de la detención provisional (período en el cual debe enviarse la solicitud de extradición) es de 18 días y en ningún caso puede exceder los 40 días[119]. Las disposiciones del Convenio sustituyen cualesquiera otros tratados, convenios o acuerdos bilaterales ya existentes entre dos partes. Sin embargo, las partes pueden concertar nuevos acuerdos bilaterales o multilaterales con el fin de complementar las disposiciones de la Convención o para facilitar la aplicación de sus principios[120].

El Segundo Protocolo Adicional, adoptado en 1978, introduce cambios en el artículo 5 relativo a los delitos fiscales, y también complementa al artículo 3 al introducir el concepto de sentencias dictadas *in absentia* para que se corresponda con situaciones prácticas. El artículo 12 también presenta cambios importantes, que permiten a los Ministerios de Justicia de los respectivos Estados Parte establecer contacto directo entre ellos para propósitos de extradición. Una vez más, se permite la transmisión a través de la vía diplomática.

En la práctica, muchos países aceptan la transmisión de documentos por fax, con la posterior confirmación formal enviada a través del servicio postal (si se permite el contacto directo entre los ministerios de justicia), o a través de la vía diplomática.

---

[116] Véanse los artículos 3 y 4 del Convenio.
[117] Véase el artículo 6, *idem*.
[118] Véase el artículo 12, *idem*.
[119] Algunos países requieren que la presentación de los documentos se realice dentro de los 18 días, otros aceptan la prórroga de los 40 días.
[120] Véase el artículo 28 del Convenio.

Convención Interamericana sobre Extradición de 1981[121]

La Convención fue creada bajo los auspicios de la OEA y constituye el actual convenio regional en este ámbito. Esta concede prioridad a los tratados bilaterales o multilaterales que los Estados Parte hayan celebrado anteriormente, a menos que las partes decidan lo contrario[122]. La Convención contiene todas las disposiciones pertinentes relativas al procedimiento de extradición, las cuales se abordan en las páginas siguientes.

Cabe señalar que los casos de extradición deben ser sancionables tanto en el derecho del Estado requirente como en el requerido con al menos dos años de prisión, y cuando la extradición se solicita para cumplir una condena, el tiempo restante para completar la pena deberá ser de al menos seis meses (nótese que los umbrales son mayores que en el caso del Convenio del Consejo de Europa). Otro elemento importante es el hecho de que no podrá recurrirse a la nacionalidad de la persona requerida para denegar la extradición, salvo cuando las leyes del Estado ejecutor dispongan otra cosa. En el artículo 4 se mencionan los motivos de denegación. Aunque por regla general la transmisión de la solicitud de extradición se haga a través de la vía diplomática, no se excluye una transmisión de gobierno a gobierno si tal procedimiento fue acordado por las partes interesadas.

El Plan de Londres para la extradición dentro de los países del Commonwealth[123]

Este Plan incluye las enmiendas que fueron introducidas en Kingston en noviembre de 2002, y contiene las disposiciones específicas para los países del Commonwealth y los principios generales que se encuentran en cualquier acuerdo de extradición. Como tal, presenta una definición de los delitos motivo de extradición y brinda una interpretación amplia de la verificación de la doble incriminación[124]. Los delitos fiscales y los delitos cometidos fuera del territorio del Estado requirente se incluyen en la lista de casos de extradición (cláusula 2). El Plan también contiene referencias a las órdenes provisionales, y la audiencia del caso que se llevará a cabo como si la persona hubiera sido acusada de un delito en el Estado requerido. Los detalles con respecto a las pruebas que deben presentarse ante el tribunal, incluidas aquellas que pudieran establecer un caso *prima facie*, se encuentran en las cláusulas 5 (diligencias de procesamiento) y 6 (diligencias de procesamiento alternativas opcionales).

Respecto de los motivos de denegación, la cláusula 12 (excepción del delito político) establece como regla general la negativa a ejecutar las solicitudes de extradición

---

[121] La Convención y la lista de Estados Parte se encuentran disponibles en: http://www.oas.org/juridico/treaties/b-47.html.

[122] El artículo 33 de la Convención titulado Relación con otras Convenciones sobre Extradición dice lo siguiente: "La presente Convención regirá entre los Estados Parte que la ratifiquen o adhieran a ella y no dejará sin efecto los tratados multilaterales o bilaterales vigentes o concluidos anteriormente, salvo que medie, respectivamente, declaración expresa de voluntad de los Estados Parte o acuerdo de estos en contrario. Los Estados Parte podrán decidir el mantenimiento de la vigencia de los tratados anteriores en forma supletoria". Esto podría conducir a la aplicación de la Convención de Montevideo sobre la Extradición de 1933, que fue la iniciativa regional anterior. Para más detalles respecto de los instrumentos pertinentes en la región, véase: *Gilbert*, Transnational Fugitive Offenders in International Law. Extradition and other Mechanisms, *supra* núm. 49.

[123] El texto del Plan se encuentra en línea en: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7B56F55E5D-1882-4421-9CC1634DF17331%7D_London_Scheme.pdf. Los orígenes de la cooperación entre los países del Commonwealth se remontan a 1843, cuando se estableció el primer estatuto referente a la rendición de fugitivos. Para más detalles, véase: *Bassiouni*, International Extraditionúm. *United States Law and Practice*, 5th Ed, Oceana, 2007, páginas 21 a 71.

[124] Véase cláusula 2, Delitos extraditables y la ley de doble incriminación, párrafo 3, incisos *a)* y *b)*, *ibid*.

relacionadas con delitos de carácter político. Existen casos en los que esto no se cumple, como aquellos en que los convenios internacionales obligan a los Estados Parte a extraditar o juzgar, o cuando el motivo de denegación del delito político no es aplicable en virtud del derecho internacional. Otros motivos obligatorios de denegación incluyen la discriminación *ne bis in idem*, o el carácter trivial del caso (para más detalles, véanse las cláusulas 12 y 13).

Entre los motivos de denegación opcionales, se encuentran los siguientes: sentencias dictadas *in absentia* en el Estado requirente, inmunidad procesal penal por caducidad o amnistía, el carácter militar del delito, la extraterritorialidad, la pena de muerte y la nacionalidad (véanse las cláusulas 14 y 15). También son aplicables medidas alternativas cuando se deniega la extradición para garantizar que los Estados Parte no se utilizan como refugios para cometer delitos (cláusula 16).

Las autoridades competentes están compuestas por una autoridad judicial encargada de escuchar a la persona sujeta a extradición y por una autoridad ejecutora responsable de las solicitudes de extradición. En la cláusula 20 se establece el principio de especialidad.

El Protocolo de Extradición de la Comunidad del África Meridional para el Desarrollo de 2002[125]

El Protocolo contiene disposiciones relativas a los delitos que dan lugar a la extradición, la detención provisoria, el principio de especialidad y el procedimiento simplificado de extradición. En lo que respecta a los casos de extradición, según se estipula en el artículo 3 del Protocolo, podría solicitarse la extradición para los casos de delitos sancionables tanto por el derecho del Estado requirente como del requerido con al menos un año de prisión. En los casos en que se solicita la extradición para cumplir una condena, el tiempo restante para completar la pena deberá ser de al menos seis meses. Entre los motivos obligatorios de denegación que se mencionan en el artículo 4 se encuentran los relacionados con los delitos de carácter político y militar, la discriminación, el principio *ne bis in idem* y la inmunidad (incluida la caducidad y la amnistía). En la lista de los motivos opcionales de denegación, el Protocolo incluye la nacionalidad de la persona requerida (si esa persona es nacional del Estado requerido) y la pena de muerte (si en el Estado requirente el delito por el cual se solicita la extradición se castiga con la pena de muerte). Las solicitudes de extradición deben transmitirse a los Ministerios de Justicia u otras autoridades designadas por los Estados Parte a través de la vía diplomática. El plazo máximo para la detención provisional es de 30 días.

El Acuerdo de Extradición de la Liga Árabe de 1952/Acuerdo árabe de cooperación judicial de Riad de 1983

Este Convenio fue aprobado por la Liga de Estados Árabes en 1952, si bien lo han ratificado únicamente Egipto, Jordania y Arabia Saudita[126].

[125] El Protocolo se encuentra disponible en: http://www.sadc.int/index/browse/page/148.
[126] Véase: *Bassiouni*, International Extradition. United States Law and Practice, *supra* núm. 123 *in fine*, página 20.

La lista de ratificaciones y adhesiones se amplió con posterioridad[127]. El Convenio, al igual que otros instrumentos similares en la materia, contiene disposiciones que permiten la continuidad de la aplicación de los tratados bilaterales preexistentes[128] entre los Estados Parte y, en caso de conflicto, prevalecerá el instrumento que facilite la extradición de la persona requerida.

El Convenio no incluye una lista de delitos motivo de extradición, pero aplica los criterios de castigo. El delito tiene que ser sancionable con una pena de prisión de al menos un año, o si la extradición se solicita para cumplir una condena, la pena de prisión impuesta tiene que ser de al menos dos meses.

Los impedimentos para la extradición de conformidad con el Acuerdo incluyen los delitos de carácter político, la ley de prescripción con aplicación en el Estado requirente y la no extradición de nacionales (aunque en este caso el Estado requerido está obligado a iniciar el proceso interno en lugar del de extradición).

Otro instrumento importante en este contexto geográfico es el Acuerdo árabe de Riad de cooperación judicial (1983), el cual se emplea en un mayor número de Estados Árabes, por lo que tiene una aplicabilidad geográfica más amplia[129].

Como lo indica su título, el Convenio tiene un campo de aplicación más extenso, y aborda temas de cooperación internacional en materia penal en general, y, en este contexto, trata el tema de la extradición en la Parte VI que se titula "La Extradición de personas acusadas o condenadas"[130].

El umbral de la pena es de por lo menos un año. El artículo 41 establece los motivos de denegación (delitos políticos, militares, principio *ne bis in idem*, la amnistía, si el delito por el cual se solicita la extradición se cometió en el territorio del Estado requerido, etc.). La nacionalidad es un motivo de denegación opcional. En el artículo 42 figuran los requisitos formales para la presentación de la solicitud de extradición. El instrumento regional permite una detención provisional a la espera de la solicitud de extradición. El período durante el cual la persona puede permanecer detenida provisionalmente hasta que se reciban los documentos es de 30 días. Otras disposiciones se refieren a la información complementaria, las solicitudes múltiples, el principio de especialidad, etc.

Cabe asimismo mencionar que los Estados de la Liga Árabe concertaron otros acuerdos regionales y bilaterales, que también podrían tener relevancia en el ámbito de la cooperación internacional en materia penal[131].

---

[127] Para más detalles, véase: *Gilbert*, Responding to International Crime, Koninklijke Brill NV, 2006, página 32.

[128] Para más detalles de la Convención, véase: *Shearer*, Extradition in International Law, Manchester University Press, 1971, páginas 52 y 53.

[129] Para más información sobre la aplicabilidad de este Convenio, véase: *Gilbert*, Responding to International Crime, *supra* núm. 127.

[130] El texto del Convenio se encuentra disponible en inglés en: http://www.unhcr.org/refworld/type.MULTILATERALTREATY.ARAB.3ae6b38d8.0.html

[131] Para una lista de instrumentos pertinentes, véase: *Ibrahim*/*Siam*, An Overview of the Arab Guiding Law on International Cooperation in Criminal Matters, Revue Internationale de Droit Pénal, vol. 76, 2005, páginas 105 y 106.

Otros convenios de relevancia

Existen otros convenios regionales referentes a la extradición que deberían tenerse en cuenta. Entre ellos se encuentra el Plan de los Países Nórdicos, que entró en vigor a través de la aprobación de la Ley de extradición por delitos penales para Dinamarca, Finlandia, Islandia y Noruega en 1962[132], el Convenio de Benelux de extradición y asistencia judicial en materia penal (1962)[133] y el Convenio de la CEDEAO[134] sobre extradición adoptado en 1994[135].

En el ámbito de la UE, previo a la adopción del sistema de orden de detención europea, se adoptaron otros dos instrumentos con el propósito de facilitar el proceso de extradición entre los Estados miembros de la Unión Europea: el Convenio relativo al procedimiento simplificado de extradición entre los Estados miembros de la Unión Europea (1995)[136] y el Convenio relativo a la extradición entre los Estados miembros de la Unión Europea (1996)[137].

Instrumentos internacionales y regionales que se ocupan, entre otras cosas, de la extradición

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 2000 (UNTOC)

En el artículo 16 de la Convención[138] figuran las disposiciones pertinentes relativas a la extradición, y representan una herramienta valiosa para los países de diferentes partes del mundo que no hayan concertado convenios o acuerdos bilaterales en materia de extradición.

Ámbito de aplicación

En el artículo 16, párrafo 1, de la UNTOC se define el alcance de la obligación de los Estados Parte de cumplir con la extradición estableciendo que la solicitud de extradición se concede, sin perjuicio de la exigencia de la doble incriminación, con respecto a "los delitos comprendidos en la presente Convención o a los casos en que un delito al que se hace referencia en los apartados *a)* o *b)* del párrafo 1 del artículo 3 entrañe la participación de un grupo delictivo organizado y que la persona objeto de la solicitud

[132] Véase: *Bassiouni*, International Extradition, United States Law and Practice, *supra* núm. 126, página 23.

[133] El Convenio de Benelux fue concertado en 1962 entre Bélgica, Holanda y Luxemburgo, cuando ninguno de los mencionados Estados había ratificado el Convenio Europeo de Extradición de 1957. Véase: *Mathisen*, Nordic Cooperation and the European Arrest Warrant: Intra-Nordic Extradition, the Nordic Arrest Warrant: Intra-Nordic Extradition, the Nordic Arrest Warrant and Beyond, in *Nordic Journal of International Law*, 79 (2010), página 4.

[134] CEDEAO es la abreviación de la Comunidad Económica de los Estados del África Occidental.

[135] *Bassiouni*, International Extradition, *supra* núm. 126, página 24.

[136] El Convenio se publicó en el Diario Oficial de las Comunidades Europeas, C078, de 30 de marzo de 1995, y tiene como objetivo facilitar la extradición entre los Estados miembros complementando la aplicación del Convenio sobre extradición del Consejo de Europa de 1957, evitando de esta manera los procedimientos formales de extradición y los retrasos. Para más información sobre su aplicabilidad, véase: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/l14015a_en.htm; véase también *Bantekas/Nash*, International Criminal Law, *supra* núm. 58, páginas 314 y 315.

[137] El Convenio se publicó en el Diario Oficial de las Comunidades Europeas, C313, de 23 de octubre de 1996. Para más información sobre su aplicabilidad véase: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/l14015b_en.htm; véase también *Bantekas/Nash*, *supra* núm. 57, página 315 y ss.

[138] El estado de ratificación de la UNTOC y sus protocolos complementarios pueden encontrarse en: http://www.unodc.org/unodc/en/treaties/CTOC/signatures.html.

de extradición se encuentre en el territorio del Estado Parte requerido [...]". En consecuencia, la obligación de extradición se aplica inicialmente a los delitos de la Convención, los delitos graves que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena mayor, así como a los delitos del Protocolo (véase el artículo 1, párrafo 2) de cada uno de los Protocolos complementarios, siempre que los delitos sean de carácter transnacional y entrañen la participación de un grupo delictivo organizado[139]. Sin embargo, y siempre con sujeción al requisito de doble incriminación, la obligación de extradición también se aplica en los casos en que estos delitos involucren a un grupo delictivo organizado, y la persona que es objeto de la solicitud de extradición se encuentre en el territorio del Estado Parte requerido, sin que sea necesario establecer la transnacionalidad de la conducta delictiva. En este sentido, el ámbito de aplicación del artículo 16 de la UNTOC es más amplio que el de la propia Convención, ya que esta disposición también podría ser aplicable en los casos en que el delincuente es aprehendido en el territorio de otro Estado Parte[140].

Bases jurídicas para la extradición

Como se mencionó anteriormente, la Convención permite a aquellos Estados Parte que supeditan la extradición a la existencia de un tratado o no hayan concertado ningún acuerdo de extradición, que consideren la Convención como base jurídica de la extradición. Los países que ya aplican tratados bilaterales vigentes basados en "la lista" de criterios también pueden utilizar la Convención. En estos casos, los Estados Parte podrían aplicar la Convención en lugar de los acuerdos bilaterales, lo que demuestra su utilidad[141]. Cualquiera que sea el caso, la extradición estará sujeta a las condiciones exigidas por la legislación del Estado requerido o por los tratados de extradición aplicables, incluido el requisito de una pena mínima o los motivos de denegación[142].

Disposiciones específicas

En el artículo 16, párrafo 9, se sientan las bases para la detención provisional con miras a la extradición. Además, la UNTOC ofrece garantías para la persona requerida[143] y prohíbe la denegación de la extradición por delitos fiscales[144].

Algunas disposiciones del artículo 16 reflejan el hecho de que muchos Estados se muestran menos renuentes a extraditar a sus propios nacionales. Si el Estado requerido se niega a extraditar a un fugitivo argumentando que es su nacional, se considera que ese Estado tiene la obligación de juzgar a esa persona. Esto ilustra el principio de extraditar o juzgar (*aut dedere aut judicare*)[145]. La disposición hace referencia a la posibilidad de conceder la entrega provisional del fugitivo a condición de que esa persona sea devuelta al Estado Parte requerido para cumplir la condena impuesta[146]. En los casos en que se solicita la extradición con el propósito de hacer cumplir una condena,

[139] Véase: Legislative Guide for the United Nations Convention against Transnational Organized Crime, página 197 y ss., disponible en: http://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html#_Full_Version_1.

[140] En este sentido, véase el párrafo 5 del Informe de la Presidenta de la Reunión del Grupo de Trabajo de composición abierta de expertos gubernamentales sobre cooperación internacional celebrada en Viena, del 8 al 10 de octubre de 2008, CTOC/COP/2008/18, disponible en: http://www.unodc.org/documents/treaties/organized_crime/Report_of_the_Chair_English.pdf.

[141] Párrafo 5, *ibid*.

[142] Véase el artículo 16, párrafo 7.

[143] Véase el artículo 16, párrafos 13 y 14, *ibid*.

[144] Párrafo 15, *idem*.

[145] Véase el artículo 16, párrafo 10.

[146] Véase el artículo 16, párrafo 11.

el Estado requerido también puede hacer cumplir la condena impuesta de conformidad con las disposiciones de su derecho interno[147].

Con respecto a los derechos humanos en los procedimientos de extradición, la Convención impone ciertas normas para garantizar el derecho a un juicio justo y que no se discrimine a la persona por motivo de sexo, raza, religión, nacionalidad, origen étnico u opinión política. El Grupo de trabajo sobre cooperación internacional, establecido por la Conferencia de las Partes en la UNTOC[148], reconoció que en la actualidad existen diferentes prácticas sobre las garantías aplicables entre los Estados, pero pese a los diferentes enfoques, las garantías que ofrecen los organismos autorizados deberían considerarse válidas y fiables[149].

Se debería estudiar detenidamente la cuestión de las sentencias dictadas *in absentia* en el Estado requirente. En estos casos, debería presentarse al Estado requerido, de la manera más detallada posible, las circunstancias en que se dictó dicha sentencia y las posibles garantías de celebrar un nuevo juicio[150].

Respecto a los delitos fiscales, como se mencionó anteriormente, no se les permite a los Estados Parte denegar la extradición por ese motivo, y están obligados a garantizar que ese motivo de denegación no está incluido en sus leyes o tratados. Esto podría requerir la adopción de nuevos instrumentos o la modificación de la legislación nacional para tal efecto[151].

Por último, aunque no por eso menos importante, la Convención insta a que antes de denegar una solicitud de extradición se celebren consultas entre los Estados requerido y requirente. Esta medida permite a este último presentar información suplementaria y opiniones de expertos que podrían apoyar la solicitud de extradición[152]. Esto representa una garantía adicional que aumenta las posibilidades de que realmente se ejecute una solicitud de extradición.

La Convención de las Naciones Unidas contra la Corrupción de 2003 (UNCAC)

La presente Convención[153] podría ser relevante si los delitos relacionados con la identidad están vinculados a delitos de corrupción establecidos de conformidad con este instrumento[154]. Debido al hecho de que su aplicación podría ser únicamente incidental, se presentará brevemente con el fin de destacar su conexión con otros instrumentos de extradición pertinentes.

---

[147] Véase el artículo 16, párrafo 12.

[148] Para conocer la labor de este Grupo, véase: http://www.unodc.org/unodc/en/treaties/working-group-on-international-cooperation.html.

[149] Véase en este sentido, el párrafo 18 del documento CTOC/COP/2008/18, *supra* núm. 140.

[150] Párrafo 17, *ibid*.

[151] Véase la Guía Legislativa, página 224, *supra* núm. 139.

[152] Véase el artículo 16, párrafo 16.

[153] El estado de ratificación de la UNCAC se encuentra disponible en: http://www.unodc.org/unodc/en/treaties/CAC/signatories.html.

[154] Los delitos consagrados en la Convención se encuentran en los artículos 15 y 25 (soborno de funcionarios públicos nacionales, soborno de funcionarios públicos extranjeros y funcionarios de organizaciones internacionales públicas, malversación, apropiación indebida u otras formas de desviación de bienes por un funcionario público, tráfico de influencias, abuso de funciones, enriquecimiento ilícito, soborno en el sector privado, malversación de bienes en el sector privado, blanqueo del producto del delito, ocultación y obstrucción de la justicia).

En el artículo 44 figuran las disposiciones que se refieren a la extradición, en las que se prevén requisitos similares a los del artículo 16 de la UNTOC. De conformidad con dicha disposición, los Estados Parte deben tratar de ampliar su red de tratados de extradición o ajustar su legislación pertinente, o ambas cosas, garantizando así la existencia de marcos jurídicos adecuados que faciliten la extradición. La UNCAC intenta establecer una norma de extradición mínima básica y exige a los Estados Parte que supeditan la extradición a la existencia de un tratado, que indiquen si la Convención se utilizará como base jurídica de la extradición y, de no ser así, que celebren tratados de extradición con otros Estados a fin de aplicar el artículo 44 de la Convención relativo a la extradición (artículo 44, párrafo 6, inciso *b)*), así como convenios o acuerdos bilaterales y multilaterales para aumentar la eficacia de la extradición (artículo 44, párrafo 18).

Si los Estados Parte no supeditan la extradición a la existencia de un tratado, la Convención les obliga a utilizar legislación relativa a extradición como base jurídica para la entrega de fugitivos y a que reconozcan los delitos que estén dentro del alcance de la Convención como causa de extradición entre ellos (artículo 44, párrafo 7).

Pese a que entre las condiciones para solicitar una extradición se impone el principio de doble incriminación como regla general (véase el artículo 44, párrafo 1, de la UNCAC), la Convención también permite que dicho principio quede sin efecto estipulando que un Estado Parte cuya legislación lo permita podrá conceder la extradición de una persona por cualesquiera de los delitos comprendidos en la presente Convención que no sean sancionables en virtud de su derecho interno (véase el artículo 44, párrafo 2). Esto representa una medida progresista que no está dispuesta en la UNTOC.

Para los procedimientos urgentes, la Convención permite la simplificación de los requerimientos en materia de pruebas y cambios legislativos, si fuere necesario, para corresponder a las normas de la Convención. Además, incluye el principio *aut dedere aut judicare*, de entrega temporal y de hacerse cargo de la ejecución de la condena como alternativas en los casos en que la extradición sea denegada por motivos de nacionalidad[155].

En general, las disposiciones de extradición están diseñadas para asegurar que la Convención apoye y complemente los acuerdos existentes de extradición y para que no se aparte de ellos.

El Convenio del Consejo de Europa sobre el delito cibernético de 2001

El artículo 24 del Convenio del Consejo de Europa sobre el delito cibernético rige los principios relativos a la extradición[156]. En este artículo se establece que se aplicará la extradición en los casos de las infracciones que se definen en los artículos 2 a 11 del presente Convenio, siempre que estas resulten sancionables en la legislación de los dos Estados implicados y

[155] Para más detalles sobre la aplicación de la UNCAC, véase: Guía legislativa para la aplicación de la Convención de las Naciones Unidas contra la Corrupción, página 178 y ss., disponible en: http://www.unodc.org/documents/treaties/UNCAC/Publications/LegislativeGuide/06-53440_Ebook.pdf.

[156] Convenio del Consejo de Europa sobre el delito cibernético, *supra* núm. 117. Para más detalles, véanse: Sofaer, Toward an International Convention on Cyber Security, *ibid.*; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, *ibid.*, página 140 y ss.; *Gercke*, National, Regional and International Approaches, *ibid.*; *Aldesco*, The Demise of Anonymity …, *ibid.*; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, *ibid.*; *Broadhurst*, Development in the global law enforcement of cybercrime, *ibid.*

tengan prevista una pena privativa de libertad de al menos un año. Reiterando lo dispuesto en el artículo 23, el Convenio confiere preeminencia a otros instrumentos con respecto a la cuantía de la pena, si esos convenios o tratados bilaterales son aplicables entre el Estado requirente y el requerido. En lo que respecta a los Estados miembros del Consejo de Europa podría tener prioridad el Convenio europeo sobre extradición.

El Convenio sobre el delito cibernético permite que los Estados Parte lo consideren como la base jurídica de la extradición respecto de cualquier delito tipificado con arreglo al Convenio, si dichos Estados Parte supeditan la extradición a la existencia de un tratado. Los Estados Parte que no supediten la extradición a la existencia de un tratado reconocerán los delitos establecidos por el Convenio como casos de extradición entre ellos. En general, la extradición está subordinada a las condiciones previstas por el derecho del Estado Parte requerido o por los tratados de extradición aplicables, incluidos los motivos que dicho Estado Parte pudiera alegar para denegar la extradición.

En el artículo 24, párrafo 6, se prevé la aplicación del principio *aut dedere aut judicare* a fin de permitir la iniciación de los procedimientos internos en el Estado requerido, en lugar de la extradición de un nacional de ese Estado. Es importante recordar que el Convenio exige que el Estado requirente solicite específicamente al Estado requerido que se haga cargo de las actuaciones[157].

Por último, el artículo 24 obliga a las Partes a designar a una autoridad competente para enviar y recibir solicitudes de extradición o de arrestos provisionales con miras a la extradición en caso de ausencia de un tratado.

3. Convenios aplicables con respecto a las formas tradicionales de asistencia judicial recíproca

Con respecto a la asistencia judicial recíproca, el Convenio sobre el delito cibernético introdujo nuevas formas de colaboración en relación con los delitos cibernéticos, que permiten a los Estados miembros cooperar en tiempo real. La presentación de las disposiciones relevantes que hacen referencia a la asistencia recíproca se concentrará, en primer lugar y en gran medida, en las formas tradicionales de asistencia judicial recíproca, y las formas específicas de cooperación propuestas en el Convenio del Consejo de Europa sobre el delito cibernético se presentarán en un subcapítulo separado.

Pese a que la mayoría de los convenios que se presentaron son de carácter regional, la enumeración de sus principales mecanismos podría proporcionar a los profesionales de otras regiones del mundo una visión general de los elementos necesarios para formular una solicitud en un país en particular. Las siguientes subsecciones no se destinarán a proporcionar una lista exhaustiva de los convenios ni un detalle de sus disposiciones, sino que más bien ofrece una visión de algunos de sus instrumentos relativos a la asistencia judicial recíproca en los casos de delitos relacionados con la identidad.

[157] Véase el informe explicativo del Convenio del Consejo de Europa sobre el delito cibernético, párrafo 251, disponible en: http://conventions.coe.int/treaty/en/reports/html/185.htm.

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 2000 (UNTOC)

El artículo 18 de la UNTOC constituye la principal disposición relativa a la asistencia judicial recíproca, si bien existen otras disposiciones relevantes (véase, por ejemplo, el artículo 13 de la UNTOC sobre las disposiciones relativas a la cooperación internacional con fines de decomiso, el artículo 19 sobre investigaciones conjuntas y el artículo 20 sobre técnicas de investigación especiales).

Ámbito de aplicación

El alcance de la aplicación del artículo 18 de la UNTOC, que rige la asistencia judicial recíproca es más amplio que el alcance de aplicación de la Convención misma. Según lo previsto en el párrafo 1 de este artículo, los Estados Parte deben prestarse "la más amplia asistencia judicial recíproca respecto de investigaciones, procesos y actuaciones judiciales relacionados con los delitos comprendidos en la Convención". Además, los Estados Parte tienen la obligación de prestarse asistencia de esa índole cuando el Estado Parte requirente tenga "motivos razonables para sospechar" que uno o más de estos delitos son de carácter transnacional y que las víctimas, los testigos, el producto, los instrumentos o las pruebas de esos delitos se encuentran en el Estado Parte requerido y que el delito entraña la participación de un grupo delictivo organizado.

Es evidente que en comparación con el artículo 3 de la UNTOC, el artículo 18 establece requisitos probatorios menos exigentes respecto al alcance de aplicación, al requerir únicamente la posibilidad razonable y no pruebas fehacientes respecto del carácter transnacional y la participación de un grupo delictivo organizado. Este umbral probatorio más bajo procura simplificar las solicitudes de asistencia judicial recíproca con el fin de determinar si el carácter transnacional y los elementos de delincuencia organizada están presentes en un caso determinado y luego evaluar si es necesaria y puede solicitarse la cooperación internacional para posteriores medidas de investigación, proceso o extradición.

Los delitos a los que se refiere la solicitud de asistencia judicial recíproca estarían comprendidos en los artículos 5, 6, 8 y 23 de la UNTOC o deberían constituir un delito grave[158] con la condición de que el delito por el que se solicita asistencia es de carácter transnacional[159] y entraña la participación de un grupo delictivo organizado[160].

---

[158] Según el artículo 2, inciso *b)*, de la UNTOC, "Por 'delito grave' se entenderá la conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave".

[159] Según el artículo 3, párrafo 2, de la UNTOC, se considera un delito transnacional si:

a) se comete en más de un Estado;

b) se comete dentro de un solo Estado, pero una parte sustancial de su preparación, planificación, dirección o control se realiza en otro Estado;

c) se comete dentro de un solo Estado, pero entraña la participación de un grupo delictivo organizado que realiza actividades delictivas en más de un Estado; o

d) se comete en un solo Estado, pero tiene efectos sustanciales en otro Estado.

[160] Véase el artículo 3, párrafo 1, inciso *b)*, de la UNTOC. Para una definición de grupo delictivo organizado véase también el artículo 2, inciso *a)*, según el cual "'por grupo delictivo organizado' se entenderá un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material".

Con respecto a los delitos relacionados con la identidad, en general se aplica la UNTOC únicamente si se considera que el delito es grave, que podría ser el caso dependiendo de las circunstancias del mismo[161]. En lo que respecta a la dimensión transnacional, es necesario reiterar que este requisito se suprime parcialmente en el artículo 18 de la Convención en el caso de que las víctimas, los testigos, los procedimientos, instrumentos o pruebas se encuentren en el Estado requerido[162]. Con el fin de cumplir con la solicitud del Estado requirente, algunos países podrían remitirse al principio de la doble incriminación. Esta es una condición opcional y no impide al Estado requirente brindar asistencia independientemente de ello[163]. Las disposiciones de la UNTOC relativas a la asistencia judicial recíproca también se pueden aplicar en relación con los delitos tipificados en los tres protocolos adicionales[164].

Motivos de denegación

Con referencia a los motivos de denegación de asistencia, el secreto bancario no podrá citarse como uno de ellos[165]. Aparte del requisito de doble incriminación, existen otros motivos de denegación opcionales que se mencionan en el párrafo 21: la falta de conformidad con lo dispuesto en la UNTOC; la discrepancia con las disposiciones del sistema jurídico del Estado Parte requerido, la soberanía, el orden público, la seguridad, otros intereses fundamentales o impedimentos para ejecutar determinada acción que surjan del derecho interno del Estado requerido y que se pudieran aplicar a un delito análogo si este hubiera sido objeto de actuaciones judiciales en el ejercicio en su propia jurisdicción. La Convención establece que cualquier negativa de brindar asistencia judicial recíproca deberá ser razonable y[166], en todo caso, antes de denegar una solicitud, los Estados requirente y requerido deberán celebrar consultas para considerar la posibilidad de brindar la asistencia que se solicita supeditándola a las condiciones que se estimen necesarias[167].

Tipos de asistencia judicial recíproca autorizados por la Convención

La Convención permite una amplia gama de solicitudes de asistencia judicial recíproca, entre ellas recoger pruebas o tomar declaración a personas, presentar documentos judiciales, efectuar inspecciones e incautaciones y embargos preventivos o facilitar información a cualquier tipo de asistencia que no contravenga el derecho interno del Estado requerido[168].

---

[161] Véase el Informe de la Segunda Reunión del grupo básico de expertos sobre el delito relacionado con la identidad, celebrada en Viena, el 2 y 3 de junio de 2008, en el que se señaló que "el delito relacionado con la identidad en sí mismo no se mencionó expresamente en el texto de la Convención, pero dos delitos estrechamente relacionados, la participación en un grupo delictivo organizado y el blanqueo de capitales, fueron establecidos específicamente por dicho instrumento. Además, otros delitos como el hurto de identidad, el fraude de identidad, el tráfico de información de identidad o de documentos y el fraude económico convencional entrarían en su ámbito de aplicación a los fines de investigación y procesamiento si se tipifican como "delitos graves" de conformidad con el sentido del artículo 2". E/CN.15/2009/CRP.11.

[162] Véase el Catálogo de ejemplos de casos de extradición, asistencia judicial recíproca y otras formas de cooperación jurídica internacional sobre la base de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, 17 de septiembre de 2008, CTOC/COP/2008/CRP.2, página 2.

[163] Véase el del artículo 18, párrafo 9, de la UNTOC.

[164] Para una interpretación del alcance, véase la Guía legislativa, *supra* núm. 139, página 220 y ss.

[165] Véase el artículo 18, párrafo 8.

[166] Véase el artículo 18, párrafo 23.

[167] Véase el artículo 18, párrafo 26.

[168] Véase el artículo 18, párrafo 3.

Contenido de la solicitud y otros requisitos formales

En el artículo 18, párrafo 15, se estipula claramente el contenido de la solicitud. Dentro de los elementos necesarios se incluyen la identidad de la autoridad que realiza la solicitud, el objeto de la misma, el resumen de los hechos pertinentes, la descripción de la asistencia solicitada, la identidad de la persona interesada y, si fuera posible, su paradero. Se deberá dar cumplimiento a la solicitud con arreglo a las disposiciones internas del Estado requerido. Sin embargo, en ese artículo se establece también que, en la medida en que ello no lo contravenga y siempre que sea posible, se dará cumplimiento a la solicitud de conformidad con los procedimientos especificados en ella (artículo 18, párrafo 17). La UNTOC alienta a que se establezca un contacto directo y se celebren consultas a fin de asegurar un mayor grado de admisibilidad por parte del Estado requirente de las pruebas reunidas en el Estado requerido. Se deberá prestar especial atención a los requisitos de confidencialidad[169].

Canales y medios de comunicación

En lo que respecta a los canales de comunicación, la UNTOC exige que las solicitudes de asistencia judicial recíproca se transmitan de una autoridad central a otra[170], haciendo énfasis en la importancia de una ejecución rápida y adecuada. La función de las autoridades centrales puede variar de un país a otro, en algunos podrían participar directamente en la entrega de la solicitud, en otros podrían únicamente enviarla. La Convención permite a los Estados decidir si prefieren que la solicitud se transmita por vía diplomática. Con respecto a la celeridad de la cooperación internacional, resulta desafortunado que muchos países sigan empleando este método. Como consecuencia de ello, las respuestas de las autoridades competentes no llegan a tiempo, dado que recibir una respuesta podría demorar más de seis meses. En los casos en que es necesario actuar con urgencia, está permitido recurrir a la Organización Internacional de Policía Criminal (Interpol) cuando los Estados Parte así lo acuerdan. Las peticiones verbales se permiten únicamente en circunstancias urgentes y tras lo cual debe presentarse una solicitud por escrito. Se recomienda recurrir al directorio de autoridades competentes de las Naciones Unidas, disponible en línea o en versión impresa, a fin de identificar los canales y medios de comunicación que utiliza un determinado Estado.

Los informes de los Estados Parte sobre la aplicación de la Convención demuestran que, mientras que la mayoría de los Estados cuentan con legislaciones que obligan a que la solicitud de asistencia judicial recíproca se formule por escrito, solo unos pocos mencionaron la transmisión por adelantado de solicitudes temporales a través del correo electrónico[171].

Transmisión espontánea de información

El artículo 18, párrafos 4 y 5, proporciona una base legal para que un Estado Parte transmita información o pruebas a otro Estado Parte si cree que esa información podría ayudar a combatir los delitos comprendidos en la Convención y el Protocolo, cuando el otro Estado Parte no haya solicitado su colaboración y pueda tener un desconocimiento absoluto de la existencia de dicha información o pruebas. El

[169] Véase CTOC/COP/2008/18, *supra* núm. 140, párrafos 33 y 34.
[170] Véase el artículo 18, párrafo 13.
[171] Véase CTOC/COP/2008/18, *supra* núm. 140, párrafo 27.

objetivo de estas disposiciones es fomentar (no se impone ninguna obligación) el intercambio de información entre los Estados Parte sobre asuntos penales independientemente de si existe o no una solicitud previa. El Estado receptor también podrá utilizar la información con posterioridad a fin de presentar una solicitud de asistencia formal. La única obligación general impuesta por el Estado receptor, que es similar a la restricción que se aplica cuando se envía una solicitud de asistencia, es que se respete el carácter confidencial de la información y que se impongan restricciones respecto de su utilización, a menos que la información recibida sea exculpatoria de la persona acusada. En este caso, el Estado receptor puede divulgar esta información en actuaciones internas. En cuanto a la necesidad de mantener el carácter confidencial de la información y el derecho del acusado a probar su inocencia, la Convención otorga prioridad a esto último.

Relación con otros instrumentos

A fin de formular una solicitud de asistencia judicial recíproca por un delito relacionado con la identidad basado en la UNTOC, existen varias consideraciones que deberán tenerse en cuenta, entre ellas, determinar si es aplicable algún otro instrumento jurídico entre los Estados requirente y requerido. En el artículo 18, párrafo 6, se establece que la UNTOC no afectará a las obligaciones dimanantes de otros tratados bilaterales o multilaterales vigentes o futuros que rijan, total o parcialmente, la asistencia judicial recíproca. En el párrafo 7 del mismo artículo se permite a los Estados Parte aplicar las solicitudes que se formulen con arreglo al presente artículo siempre que no medie entre los Estados Parte interesados un tratado de asistencia judicial recíproca. Así, el artículo 18, párrafos 9 a 29, es aplicable para los Estados que no han concertado ningún tratado o acuerdo previos. Si entre los Estados Parte interesados ya existe un tratado en vigor, se aplicarán las disposiciones correspondientes de dicho tratado, salvo que los Estados Parte convengan en aplicar, en su lugar, los párrafos 9 a 29 del presente artículo. Se insta encarecidamente a los Estados Parte, aunque no se les obliga, a que apliquen estos párrafos si los mismos facilitan la cooperación[172].

Cabe destacar que en el artículo 18, párrafo 30, se otorga a los Estados Parte la posibilidad de celebrar acuerdos o arreglos bilaterales o multilaterales que sirvan a los fines del presente artículo.

Síntesis

La UNTOC es una herramienta de suma importancia y utilidad, y cuya aplicación es mundial. Normalmente la cooperación internacional tiene, de hecho, carácter regional y se promueve dentro de una esfera específica en determinados países que mantienen vínculos económicos y culturales sólidos. En este aspecto, el delito transnacional presenta desafíos, ya que los instrumentos regionales no son suficientes para abarcar la magnitud del problema. El delito relacionado con la identidad es un buen ejemplo de ello. La UNTOC ya ha probado ser valiosa como base jurídica para la cooperación internacional entre países de diferentes continentes[173]. Por tanto, si un Estado

[172] Para esta explicación, véase CTOC/COP/2008/18, *supra* núm. 140, párrafos 25 y 26.

[173] Véase la recopilación de ejemplos de casos de extradición, asistencia judicial recíproca y otras formas de cooperación judicial internacional sobre la base de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, CTOC/COP/2010/CRP.5/Corr.1.

necesita transmitir una solicitud a otro con el que no está obligado por un tratado regional o bilateral, lo primero que deberá hacer es comprobar si el delito relacionado con la identidad específico por el cual se solicita asistencia tiene un carácter transnacional y, en segundo lugar, si el Estado requerido es Parte de la UNTOC.

Al presentar la solicitud sobre la base de la UNTOC, es importante consultar el directorio de autoridades nacionales competentes en línea o su versión impresa, la cual contiene información sobre la autoridad central del Estado requerido, los canales de comunicación y otra información pertinente[174]. A fin de garantizar la adecuada preparación de la solicitud, se recomienda encarecidamente que la autoridad competente del Estado requerido utilice el manual de redacción de solicitudes de asistencia judicial recíproca de la UNODC[175]. En el caso en que la solicitud sea de carácter urgente, es importante evaluar con exactitud, sobre la base de la información disponible en el directorio en línea, los canales de comunicación a seguir[176].

La Convención de las Naciones Unidas contra la Corrupción de 2003 (UNCAC)

La Convención de las Naciones Unidas contra la Corrupción contiene disposiciones detalladas sobre la cooperación internacional en cuestiones penales, incluida la asistencia judicial recíproca (artículo 46). Estas disposiciones se basan generalmente en la UNTOC, y en ocasiones van más allá de esta.

En general, la Convención busca la manera de facilitar y mejorar la asistencia judicial recíproca, alentando a los Estados Parte a participar en la celebración de nuevos acuerdos o arreglos y mejorando la eficiencia de la asistencia judicial recíproca. En todo caso, en el artículo 46, párrafo 1, se exige a los Estados Parte que se presten la más amplia asistencia judicial recíproca tal como se menciona en el párrafo 3 del mismo artículo, respecto de investigaciones, procesos y actuaciones judiciales[177] relacionados con los delitos comprendidos en la presente Convención. Si el marco legal relativo a la asistencia judicial recíproca de un Estado Parte no es lo suficientemente amplio como para abarcar todos los delitos comprendidos en la Convención, podría ser necesario enmendar la legislación.

En el artículo 46, párrafo 2, se obliga a los Estados Parte a que presten asistencia judicial recíproca con respecto a investigaciones, procesos y actuaciones judiciales en los que una persona jurídica pueda ser considerada responsable (véase también el artículo 26 de la presente Convención).

---

[174] El directorio da a conocer la autoridad central encargada de recibir la solicitud de asistencia judicial, los idiomas aceptados, los canales de comunicación, los puntos de contacto, los números de fax y las direcciones de correo electrónico, las peticiones específicas de los Estados receptores y, a veces, incluso extractos de la legislación nacional del Estado.

[175] El software se encuentra disponible para su descarga en: http://www.unodc.org/mla/index.html.

[176] Un ejemplo al azar del directorio es el siguiente: si el país A tiene que presentar una solicitud de asistencia judicial recíproca a Belarús, la autoridad competente encargada de recibir dicha solicitud sería la Oficina del Fiscal General en Minsk, los idiomas aceptados son el bielorruso y el ruso, la solicitud debe ser transmitida a través de la vía diplomática pero se acepta que se envíe por adelantado a través de cualesquiera medios que proporcionen una constancia escrita, siempre y cuando se envíen los originales a través de la vía diplomática y, en caso de urgencia, se acepta la transmisión a través de canales de comunicación expeditivos, seguida de una confirmación formal.

[177] Los Estados Parte tienen el poder discrecional de determinar la medida en que prestarán asistencia en tales procesos. No obstante, la asistencia debería estar disponible por lo menos en relación con las partes del proceso penal que en determinados Estados pueden no constituir el juicio propiamente dicho, tales como los procesos previos al juicio, de pena y de fianza.

Tipos de asistencia judicial recíproca autorizados por la Convención

En el artículo 46, párrafo 3, se presenta una lista de los tipos de asistencia que otorga la UNCAC. A fin de garantizar el cumplimiento de esta disposición, los Estados Parte necesitarían llevar a cabo una revisión exhaustiva de su marco jurídico en lo tocante a la asistencia judicial recíproca y evaluar si dicho marco es lo suficientemente amplio como para abarcar todas las formas de cooperación que se mencionan en el párrafo 3. Los Estados Parte que hayan ratificado la UNTOC normalmente cumplirían con esta disposición y, además, deben contar con los mecanismos vigentes apropiados para brindar asistencia en los casos de identificación, embargo con carácter preventivo y localización del producto del delito y recuperación de bienes (véanse el artículo 46, párrafo 3, incisos *j)* y *k)*).

En ausencia de un tratado de asistencia judicial recíproca aplicable, y de conformidad con el artículo 46, párrafos 7 y 9, la UNCAC proporciona un mecanismo para la transmisión y ejecución de solicitudes respecto de los tipos de asistencia antes mencionados. Si entre los Estados Parte interesados existe un tratado en vigor, este se aplicará en su lugar, a menos que los Estados Parte acuerden aplicar los párrafos 9 a 29. En cualquier caso, se alienta a los Estados Parte a que apliquen esos párrafos para facilitar la cooperación. En algunas jurisdicciones podría ser necesario contar con legislación adicional para dar pleno efecto a estas disposiciones.

Secreto bancario

En el artículo 46, párrafo 8, se dispone que los Estados Parte se abstengan de citar al secreto bancario como motivo de denegación de la asistencia judicial recíproca. Es significativo el hecho de que este párrafo no está incluido entre los párrafos que se aplican únicamente en ausencia de un tratado de asistencia judicial recíproca. Los Estados Parte están obligados, en cambio, a garantizar que ese motivo de denegación sea citado de conformidad con su régimen jurídico, incluido el Código Penal, el Código de Procedimiento Penal o las leyes o reglamentos bancarios (véanse también el artículo 31, párrafo 7, y los artículos 55 y 57). Así, cuando la legislación de un Estado Parte permita invocar este motivo de denegación, será necesario hacer enmiendas en la legislación.

Doble incriminación

En el artículo 46, párrafo 9, se exige a los Estados Parte que al dar respuesta a una solicitud de asistencia en ausencia del principio de doble incriminación, tengan en cuenta la finalidad y espíritu de la presente Convención (artículo 1). Si bien los Estados Parte podrán negarse a prestar asistencia con arreglo al presente artículo invocando la ausencia de este principio (párrafo 9, inciso *b)*), se les alienta además a que obren con discreción y consideren la adopción de medidas necesarias que le permitan prestar una asistencia más amplia, incluso en ausencia de este requisito (párrafo 9, inciso *c)*).

No obstante, siempre que esté en consonancia con los conceptos básicos de sus ordenamientos jurídicos, los Estados Parte prestarán asistencia que no entrañe medidas coercitivas en el entendimiento de que no suponga asuntos de naturaleza *de minimis* o que no pueda proporcionarse en virtud de otras disposiciones de la Convención (párrafo 9, inciso *b)*).

Designación de autoridades centrales

La Convención también exige que cada Estado Parte designe un autoridad central (véanse los párrafos 13 y 14) encargada de recibir solicitudes de asistencia judicial recíproca y facultada para darles cumplimiento o para transmitirlas a las autoridades internas competentes para su ejecución, proporcionando así una alternativa a la vía diplomática. Las autoridades judiciales del Estado requirente pueden comunicarse directamente con la autoridad central. En la actualidad se utilizan cada vez más los canales directos, a través de los cuales un funcionario del Estado requirente puede enviar la solicitud directamente al funcionario correspondiente del otro Estado.

Transmisión espontánea de información

El artículo 46, párrafos 4 y 5, proporciona una base legal para que un Estado Parte transmita información o pruebas a otro Estado Parte si cree que esa información podría ayudar a combatir los delitos comprendidos en la UNCAC que se encuentran en una fase temprana, aún cuando el otro Estado Parte no lo haya solicitado y pueda tener un desconocimiento absoluto de la existencia de dicha información o pruebas. El objetivo de estas disposiciones es fomentar el intercambio de información entre los Estados Parte de manera voluntaria y proactiva. El Estado receptor también podrá utilizar la información con posterioridad a fin de presentar una solicitud de asistencia formal. La única obligación general impuesta por el Estado receptor, que es similar a la restricción que se aplica cuando se envía una solicitud de asistencia, es que se respete el carácter confidencial de la información y que se impongan restricciones respecto de su utilización, a menos que dicha información sea exculpatoria de la persona acusada. En ese caso, el Estado receptor puede divulgar esta información en actuaciones internas.

Diferencias respecto de las disposiciones de la UNTOC

Puesto que la UNTOC contiene una disposición similar sobre asistencia judicial recíproca (artículo 18), los Estados Parte de la Convención deberían, en general, estar en condiciones de cumplir con los requisitos correspondientes que derivan del artículo 46 de la UNCAC. Sin embargo, existen diferencias significativas entre los dos instrumentos.

En primer lugar, de conformidad con la UNCAC, la asistencia judicial recíproca se extiende también a la recuperación de activos, un principio fundamental de la presente Convención (véanse el artículo 1 y el artículo 46, párrafo 3, incisos *j)* y *k)*), así como el capítulo V de la Convención.

En segundo lugar, en ausencia del principio de doble incriminación, los Estados Parte están obligados a prestar asistencia que no entrañe medidas coercitivas, siempre que sea compatible con su ordenamiento jurídico y que el delito no sea de carácter trivial. Esta disposición no está incorporada en la UNTOC.

Además, cuando la doble incriminación constituye un requisito a los efectos de la cooperación internacional en materia penal, la UNCAC establece una norma de interpretación adicional para su aplicación, la cual no está contemplada en la UNTOC. La norma propone que el criterio de doble incriminación se considerará cumplido independientemente de si las leyes del Estado Parte requerido incluyen el delito en la misma categoría o lo denominan con la misma terminología que el Estado Parte

requirente, si la conducta constitutiva del delito respecto del cual se solicita asistencia es considerado como tal con arreglo a la legislación de ambos Estados Parte (el artículo 43, párrafo 2). Además, la Convención permite que los Estados Parte no se limiten a la cooperación en materia penal, sino que también colaboren entre ellos en las investigaciones y procedimientos correspondientes a cuestiones civiles y administrativas relacionadas con la corrupción cuando proceda y esté en consonancia con su ordenamiento jurídico interno (artículo 43, párrafo 1).

Convenio del Consejo de Europa sobre el delito cibernético de 2001

El Convenio contiene varios artículos sobre asistencia judicial recíproca, si bien el capítulo que sigue a continuación se centrará únicamente en los artículos 25 y 27[178]. Estos artículos hacen referencia a los principios generales relativos a la asistencia judicial recíproca en ausencia de acuerdos internacionales aplicables.

Condiciones

En el artículo 23 del Convenio sobre el delito cibernético titulado "Principios generales relativos a la cooperación internacional" se dispone que el capítulo sobre cooperación internacional se aplicará en los casos que entrañen infracciones penales relacionadas con sistemas y datos informáticos, así como para recoger pruebas electrónicas de un delito penal. Aunque en el Convenio sobre el delito cibernético, el delito relacionado con la identidad no figura como un delito separado[179], son aplicables las disposiciones relativas a la cooperación internacional.

En el artículo 25, párrafo 4, se menciona claramente que las solicitudes de asistencia judicial recíproca estarán sujetas a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de asistencia recíproca aplicables. Esto incluye los motivos de denegación, proporcionando así una garantía para los derechos de la persona que se encuentre en el Estado requerido, especialmente cuando se trata de medidas intrusivas[180].

Tipos de asistencia judicial recíproca permitida y contenido de la solicitud

No existen disposiciones especiales respecto de los tipos de asistencia judicial recíproca y sus contenidos, aunque sobre la base de las disposiciones generales, seguirán siendo aplicables los tipos de asistencia permitida en virtud de acuerdos previos y sus requisitos respecto del contenido de la solicitud.

Canales y medios de comunicación

En ausencia de acuerdos internacionales aplicables entre las partes, el Convenio exige la comunicación directa entre las autoridades centrales designadas como tales por los Estados Parte. Sin embargo, en los casos urgentes, se permite el contacto directo

[178] Para más detalles, véase: *Gercke*, Understanding Cybercrime…, *supra* núm. 26, página 207 y ss.

[179] En este contexto, véase: *Gercke*, Internet-related Identity Theft, Documento de debate del Consejo de Europa, 2007, disponible en: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf.

[180] Véase el informe explicativo de la Convención sobre el delito cibernético, párrafo 159, *supra* núm. 159.

entre las autoridades judiciales de los dos Estados cooperantes[181]. En cualquier caso, el Convenio también requiere el envío de una copia de la solicitud a la autoridad central del Estado requerido. En el caso de una solicitud urgente, y de conformidad con el Convenio, también podría recurrirse a la Interpol.

En el artículo 27, párrafo 9, se autoriza a los Estados Parte a que informen al Secretario General del Consejo de Europa de que continuarán transmitiendo las solicitudes urgentes a través de las autoridades centrales por razones de eficacia. No obstante, se mantiene un contacto directo, que desde el punto de vista práctico es la mejor manera de gestionar las solicitudes urgentes, siempre que la autoridad judicial requirente conozca la información de contacto de la otra autoridad judicial competente.

En lo que respecta a los medios de comunicación, el Convenio[182] responde a los requerimientos prácticos con respecto a los delitos relacionados con la identidad estipulando el uso de medios de comunicación expeditivos, tales como el fax o el correo electrónico, que deberán ir seguidos de una confirmación formal si el Estado requerido así lo solicita. En estos casos urgentes, la respuesta debe ser transmitida a través de los mismos medios de comunicación.

Transmisión espontánea de información

El Convenio permite la transmisión espontánea de información[183] a la parte receptora aún cuando no exista una solicitud de asistencia judicial recíproca previa, a fin de colaborar con ese Estado para iniciar o llevar a cabo investigaciones o procedimientos penales relacionados con los delitos estipulados en el Convenio o, si el Estado emisor considera que esto podría dar lugar a una nueva solicitud de asistencia de parte del Estado receptor. Esta regulación es similar a las disposiciones pertinentes de la UNTOC y la UNCAC, incluido el requisito de confidencialidad con respecto a la información sensible proporcionada por el Estado emisor.

Investigaciones conjuntas

El Convenio no hace ninguna referencia especial a esta forma de cooperación. Sin embargo, sí se refiere a su relación con otros instrumentos. En vista de esto, es posible que esta forma de colaboración esté permitida en virtud de otros instrumentos aplicables en determinados casos y de conformidad con las disposiciones pertinentes del derecho interno de los países involucrados.

Relación con otros instrumentos

En el artículo 39 se define la preeminencia de otros acuerdos internacionales existentes, ya que el Convenio no afecta los derechos y compromisos que se derivan de convenciones internacionales multilaterales existentes. El Convenio también permite

[181] En el artículo 27, párrafo 2, incisos *a)* y *b)*, se estipula lo siguiente:

a) Las Partes designarán una o varias autoridades centrales encargadas de tramitar las demandas de colaboración, de ejecutarlas o de transferirlas a las autoridades competentes para que estas las ejecuten.

b) Las autoridades centrales se comunicarán directamente las unas con las otras.

[182] El artículo 25 es el que trata este tema.

[183] El artículo 26 del Convenio sobre el delito cibernético es de relevancia. El informe explicativo indica que la fuente de dicha disposición reside en instrumentos previos adoptados por el Consejo de Europa, a saber, el artículo 10 del Convenio del Consejo de Europa relativo al blanqueo, seguimiento, embargo y decomiso de los productos del delito, STE núm. 141, 1990, y el artículo 28 del Convenio de derecho penal sobre la corrupción, STE núm. 173, 1999. Véase el párrafo 260 del informe explicativo del Convenio, *supra* núm. 157.

la celebración de acuerdos bilaterales sobre los temas tratados en el mismo. No obstante, cuando las partes establecen sus relaciones respecto de los temas que abarca el Convenio a través de otros acuerdos, deben hacerlo de manera que no contradigan los objetivos y principios del Convenio.

La Convención Interamericana sobre Asistencia Mutua en Materia Penal de 1992[184]

En el artículo 7 de la Convención titulado "Ámbito de aplicación" se establece que la asistencia prevista en esta Convención comprenderá lo siguiente: notificar resoluciones y sentencias; escuchar testimonios y tomar declaraciones; notificar a los testigos y peritos a fin de que rindan testimonio; embargar y secuestrar bienes, inmovilizar activos y prestar asistencia en procedimientos relativos al decomiso; efectuar registros o decomisos; examinar objetos y lugares; remitir documentos, informes, información y elementos de prueba; trasladar a las personas detenidas y finalmente "cualquier otro acto siempre que hubiere acuerdo entre el Estado requirente y el Estado requerido". Cabe destacar que el alcance de la Convención es más amplio que el de una Convención regional similar adoptada a nivel europeo, ya que incluye otros temas relativos a la cooperación internacional en asuntos penales que en el contexto europeo se abordan en tratados separados (por ejemplo, la transferencia de personas condenadas).

Condiciones

En general, la formalización de una solicitud no se basa en el requisito de doble incriminación (artículo 5, párrafo 1, de la Convención), aunque existen excepciones a esta regla: si la solicitud se refiere a casos de embargo, secuestro, inspecciones, incautaciones o registros domiciliarios, entonces el Estado *requerido* podría negarse a ejecutar la solicitud de asistencia judicial recíproca (por tanto, la falta de requisito de doble incriminación es un motivo opcional de denegación). En el artículo 9 se mencionan los motivos de denegación, los cuales son opcionales (*ne bis in idem*, discriminación, delitos de carácter político, solicitud emitida a pedido de un tribunal concebido especialmente para ese fin, orden público, soberanía, seguridad y solicitud por delitos fiscales).

La solicitud se ejecutará de conformidad con el derecho interno del Estado requerido y, en la medida de lo posible, de la manera expresada por el Estado requirente, siempre que no contravenga la legislación del Estado requerido (artículo 10 de la Convención).

Contenido de la solicitud y otros requisitos formales

El contenido de la solicitud se especifica en el artículo 26 de la Convención, el cual hace referencia al delito por el cual se solicita la asistencia, los hechos pertinentes, los procedimientos que dan lugar a la solicitud y la descripción detallada de la asistencia requerida[185].

---

[184] La Convención se encuentra disponible en: http://www.oas.org/juridico/english/treaties/a-55.html. El estado de ratificación se puede consultar en la misma página.

[185] En el artículo 26 de la Convención se estipula lo siguiente: "Las solicitudes de asistencia deberán contener las siguientes indicaciones:

a) delito a que se refiere el procedimiento y descripción sumaria de los hechos constitutivos del mismo, investigación o juicio penal de que se trate y descripción de los hechos a que se refiere la solicitud;

b) acto que origina la solicitud de asistencia con una descripción precisa del mismo;

c) cuando sea pertinente, la descripción de cualquier procedimiento u otros requisitos especiales del Estado requirente;

d) descripción precisa de la asistencia que se solicita y toda la información necesaria pare el cumplimiento de la solicitud".

Canales de comunicación

De conformidad con lo dispuesto en el artículo 3 de la Convención, la transmisión y recepción de las solicitudes deberá realizarse a través de las autoridades centrales. Sobre la base de las prácticas óptimas[186] elaboradas durante la Tercera Reunión de Autoridades Centrales y Otros Expertos en Asistencia Mutua en Materia Penal y Extradición, celebrada en Bogotá en 2007, antes de enviar la solicitud formal se anima a que se establezca un contacto directo entre las autoridades competentes de los Estados requirente y requerido.

Relación con otros instrumentos

El artículo 36 de la Convención establece la preeminencia de otros instrumentos internacionales, regionales o bilaterales que ya se encuentren en vigor, en referencia a cualquiera de los posibles objetos de la solicitud regulados por la Convención y a aquellos instrumentos que contengan medidas más favorables que las que establece la Convención.

Protocolo Facultativo relativo a la Convención Interamericana sobre Asistencia Mutua en Materia Penal de 1993

El Protocolo Facultativo hace referencia a los delitos tributarios y proporciona modificaciones respecto de la aplicación práctica del artículo 9 *f)* de la Convención relativo a los motivos de denegación, así como al artículo 5 que trata sobre la doble incriminación. En este sentido, no se puede rechazar una solicitud de asistencia judicial recíproca por el mero hecho de que la infracción forme parte de los delitos tributarios. Con respecto a la doble incriminación, los Estados Parte en el Protocolo, cuando actúen como un Estado requerido en virtud de la Convención, no denegarán asistencia si el hecho que se especifica en la solicitud corresponde a un delito tributario de la misma naturaleza según las leyes del Estado requerido[187].

Plan del Commonwealth para la Asistencia Mutua en Materia Penal (Plan de Harare), modificado por última vez en 2005[188]

El Plan establece que el Estado requerido debe informar cuanto antes al Estado requirente si la solicitud no cumple con los requisitos específicos del Plan, y si existen motivos de denegación en virtud del mismo o razones de demora[189], mientras que la formalización de

[186] Prácticas óptimas propuestas respecto de la recogida de declaraciones, documentos y pruebas físicas, con respecto a la asistencia judicial recíproca en relación con la localización, los embargos preventivos y confiscación de bienes producto o instrumento del delito y los formularios sobre asistencia judicial recíproca en materia penal, adoptadas en Bogotá, 12 a 14 de septiembre de 2007, disponibles en: http://www.oas.org/juridico/MLA/en/model_law.pdf.

[187] El texto del Protocolo Opcional puede consultarse en: http://www.oas.org/juridico/english/treaties/a-59.html, y la lista de los Estados Parte del instrumento en: http://www.oas.org/juridico/english/Sigs/a-59.html.

[188] La forma actual del Plan de Harare incluye los cambios introducidos en abril de 1990, noviembre de 2002 y octubre de 2005, se aplica a los 22 Estados miembros del Commonwealth y puede consultarse en línea en: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/2C167ECF-0FDE-481B-B552-E9BA23857CE3_HARARESCHEMERELATINGTOMUTUALASSISTANCE2005.pdf.

[189] Véase el artículo 7, párrafo 3.

la solicitud podría depender de que se cumplan algunas condiciones[190]. Además de estas condiciones, existen motivos opcionales de denegación. Es importante destacar que bajo este Plan, los motivos de denegación son opcionales y no obligatorios (artículo 8). Entre ellos se cuentan el de doble incriminación, el principio *ne bis in idem*, los delitos de carácter político o militar, la discriminación, el orden público y la soberanía[191].

Tipos de asistencia judicial recíproca permitida

Los tipos de asistencia judicial recíproca que pueden solicitarse en virtud del Plan[192] son los siguientes: identificación y localización de personas, expedición de documentos; interrogatorio de testigos; registro y confiscación; obtención de pruebas; traslado temporal de personas; obtención de expedientes judiciales u oficiales; localización, decomiso y confiscación de productos o medios del delito y conservación de datos informáticos.

Cabe destacar que a diferencia de otros instrumentos, el Plan también contiene disposiciones relativas a la conservación de datos informáticos, que es un tipo específico de asistencia judicial recíproca que tiene gran relevancia en el caso de los delitos relacionados con la identidad. En particular, en el artículo 15 del Plan se abordan específicamente las solicitudes de preservación de datos informáticos. En virtud de este artículo dicha información deberá preservarse por 120 días (ciento veinte días) de conformidad con la solicitud, hasta que el país requirente presente la solicitud de asistencia para obtener los datos informáticos. Una vez recibida la solicitud, los datos se conservarán hasta la resolución de dicha solicitud y, si es aprobada, hasta que los datos se hayan obtenido de conformidad con la solicitud de asistencia. Si el Estado requerido considera que la preservación de los datos informáticos en virtud de una solicitud formulada conforme al presente artículo no garantiza la disponibilidad futura de los datos, o pone en peligro la confidencialidad o perjudica las tareas de investigación en el país requirente, lo comunicará de manera inmediata a este a fin de que determine si la solicitud, no obstante, debe ejecutarse. Pese a los motivos de denegación generales contenidos en el artículo 8 del Plan, podría negarse una solicitud de conservación de datos informáticos en virtud de este artículo únicamente cuando el país requerido considere que su cumplimiento estaría contraviniendo las leyes o la constitución de ese país, o perjudicando la seguridad, las relaciones internacionales u otros intereses públicos esenciales en el mismo.

El hecho de que en general el Plan concede gran importancia a la cooperación internacional en materia de delitos cibernéticos se refleja no solo en la inserción del artículo *supra*, sino también en el extenso espacio dedicado a las definiciones de términos, tales como la información de los suscriptores, los datos informáticos y el tráfico de datos.

---

[190] Véase el artículo 7, párrafo 4, que reza como sigue: "El Estado requerido podrá supeditar la prestación de asistencia a condición de que el país requirente se comprometa a:

a) no utilizar las pruebas aportadas directa o indirectamente en relación con la investigación o juicio de una persona determinada; o

b) que un tribunal en el país requirente determine si el material está sujeto a privilegio".

[191] Véase el artículo 8 relativo a la denegación de asistencia.

[192] Véase el artículo 1, párrafo 3, relativo al objetivo y alcance.

Contenido de la solicitud y otros requisitos formales

En el artículo 14 se hace referencia a los requisitos del contenido de la solicitud de asistencia judicial recíproca (con exclusión de la preservación de los datos, que se menciona en disposiciones especiales). Los requisitos generales establecidos en el presente artículo hacen referencia al carácter de la asistencia que se solicita, el plazo para su cumplimiento, los datos de identificación de un organismo o autoridad emisores de la solicitud, la naturaleza de la materia penal y el hecho de si se ha iniciado el proceso penal. Si este fuera el caso, deberán aplicarse los requisitos especiales previstos al respecto. Si aún no se ha iniciado el proceso penal, la autoridad central del Estado requirente deberá especificar la naturaleza del delito y presentar un resumen de los hechos conocidos. En los casos urgentes, la solicitud se puede hacer de manera verbal (seguida de una confirmación por escrito).

Canales de comunicación

Según el artículo 5 del Plan, las solicitudes deberán transmitirse y recibirse a través de las autoridades centrales. El Plan establece claramente las competencias de los Estados requirente y requerido[193].

Relación con otros instrumentos

Como ya se ha puesto en evidencia en su parte introductoria[194], el objetivo del Plan es mejorar "el nivel y alcance de la asistencia prestada entre dos gobiernos de la Commonwealth en materia penal", y que, en este sentido, no se hará en detrimento de las prácticas de cooperación existentes, ya sean formales o informales.

Tratado del Caribe sobre Asistencia Judicial Recíproca en Asuntos Penales de 2005[195]

Como lo indica el título, este Tratado es aplicable en los casos de delitos graves (delitos sancionables con al menos doce meses de prisión, incluidos los delitos tributarios). El Tratado introduce una serie de motivos de denegación opcionales, entre ellos, de orden público, el principio *ne bis in idem*, de discriminación y los delitos de carácter político o militar[196]. La doble incriminación o el secreto bancario no constituyen un requisito previo para formalizar la solicitud[197]. Existe una disposición especial para cada tipo de asistencia judicial recíproca permitida por el Convenio con detalles más específicos que deben considerarse en el momento de enviar la solicitud pertinente. Para los propósitos de esta guía, dos de los artículos que revisten especial importancia son el artículo 12 sobre "Entrega de documentos" y el artículo 13 sobre "Asistencia para la recolección de pruebas".

Tipos de asistencia judicial recíproca permitida

En el artículo 2, párrafo 3, se estipula que, siempre y cuando lo permita la legislación del Estado requerido, se llevarán a cabo, sobre la base del Tratado, los siguientes tipos de asistencia judicial recíproca: identificar y localizar personas y objetos; recoger

[193] Véanse los artículos 6 y 7 del Plan.
[194] Véase el artículo 1, párrafo 1, titulado "Objetivo y alcance".
[195] El texto del Tratado se encuentra disponible en línea en: http://www.caricomlaw.org/doc.php?id=554.
[196] Para más detalles, véase el artículo 7, párrafo 1, del Tratado.
[197] Véase el artículo 7, párrafos 3 y 4.

testimonio o declaraciones de personas; obtener documentos judiciales o de otra índole; presentar documentos judiciales; analizar objetos, locales e instalaciones; suministrar información, originales o copias certificadas de documentos y expedientes, facilitar la comparecencia de testigos; transferir temporalmente a las personas en custodia; llevar a cabo inspecciones o incautaciones, localizar, embargar con carácter preventivo y confiscar el producto del delito.

Contenido de la solicitud y otros requisitos formales

De conformidad con el artículo 5 del Tratado, la solicitud debe incluir el nombre de la autoridad competente, el propósito de la solicitud, una descripción de la asistencia que se solicita, un resumen de los hechos, las disposiciones legales aplicables, los datos de identificación de la persona en cuestión (cuando se trata de la entrega de documentos), detalles sobre determinados procedimientos a seguir por el Estado requerido y las razones por las cuales el Estado requirente solicita tal información, así como detalles sobre el bien que debe localizarse o embargarse con carácter preventivo, la declaración del Estado requirente respecto de la confidencialidad y las razones por las cuales se le solicita al Estado requerido, y cualquier otra información pertinente.

Canales de comunicación

En el artículo 4 se hace efectiva la comunicación de la asistencia judicial recíproca a través de las autoridades centrales encargadas de recibir la solicitud y facultadas para darles cumplimiento o para transmitirlas a las autoridades competentes para su ejecución. En el artículo 6 se establece la obligación del Estado requerido para que actúe "tan rápido como sea posible" respecto de las solicitudes de asistencia.

Relación con otros instrumentos

De conformidad con el artículo 24 titulado "Otros acuerdos", se establece que los Estados Parte podrán celebrar otro tratado bilateral o multilateral para complementar o reforzar la aplicación del Tratado de asistencia judicial recíproca de CARICOM.

Tratado de asistencia recíproca en asuntos penales entre países miembros de la ASEAN de 2004[198]

El Tratado pide que exista una cooperación lo más amplia posible entre los Estados Parte en el ámbito de la asistencia judicial recíproca[199]. Sin embargo, existen limitaciones respecto de la concesión de asistencia[200], incluidos, entre otros, la denegación en caso de que el delito sea de carácter político o militar, la discriminación por motivos de raza, religión, sexo, etc., el principio *ne bis in idem*, la doble incriminación, el orden público, la soberanía y la incapacidad de actuar sobre la base de la reciprocidad.

Tipos de asistencia judicial recíproca permitida

El propósito de este Tratado se describe claramente en el primer artículo: facilitar ciertos tipos de asistencia, entre ellos, recibir testimonio, preparativos para que las

[198] El Tratado, que fue firmado en Kuala Lumpur por los Estados miembros de la ASEAN, puede consultarse en: http://www.aseansec.org/.
[199] Véase el artículo 1, párrafo 1, del Tratado.
[200] Véase el artículo 3, *ibid.*

personas presten testimonio o asistencia en materia penal; expedir documentos judiciales; efectuar inspecciones e incautaciones; examinar objetos y lugares; entregar originales o copias certificadas de los documentos pertinentes; identificar y embargar bienes con carácter preventivo; localizar e identificar testigos y sospechosos; y cualquier otro tipo de asistencia que pudiera acordarse de conformidad con el Tratado y la legislación del Estado requerido.

Contenido de la solicitud y otros requisitos formales
En lo que respecta al contenido de la solicitud, el artículo 6 del Tratado comprende requisitos obligatorios y opcionales.

Entre los elementos obligatorios que deberían estar presentes en la solicitud se cuentan los siguientes: el propósito de la solicitud y el carácter de la asistencia que se solicita; una declaración con respecto al resumen de los hechos; una descripción de los hechos y una copia de los textos jurídicos aplicables; una descripción de las pruebas, información sobre la asistencia que se solicita; una indicación de si es necesario seguir un determinado procedimiento o requisito y las razones para ello; una especificación de los plazos (si los hubiere); y la indicación de si es necesario mantener la confidencialidad o cualquier otra información específica requerida en la legislación del Estado requerido.

Con respecto a los requisitos opcionales, dependiendo del tipo de solicitud, su contenido podría incluir, entre otras cosas: la nacionalidad y la ubicación de la persona o personas objeto de la investigación o de quien se buscan pruebas o a quien es necesario entregar los documentos; información sobre el paradero de la persona; una lista de preguntas para los testigos; una descripción de los bienes, activos o artículo a los que se refiere la solicitud; y una descripción sobre la manera en que debe tomarse o documentarse un testimonio o declaración.

Canales de comunicación
El Tratado establece no solo un contacto directo entre las autoridades centrales, sino que también permite la posibilidad de utilizar los canales diplomáticos abiertos a la discreción de los Estados Parte[201]. Las disposiciones del Tratado brindan la oportunidad de utilizar los medios de comunicación expeditivos, cuando sea necesario y, en lo que respecta a los canales de comunicación, en casos de urgencia, es posible la transmisión a través de Interpol o Aseanpol[202].

Relación con otros instrumentos
En el artículo 23 del Tratado se da prioridad a otros tratados y acuerdos sobre asistencia judicial recíproca existentes entre los Estados Parte.

[201] Véase, a este respecto, el artículo 4 del Tratado.
[202] Véase el artículo 6 del Tratado.

Protocolo de Asistencia judicial Mutua en Asuntos Penales del SADC de 2002[203]

El Protocolo exige a los Estados Parte que se presten la asistencia recíproca más amplia posible[204]. Es importante tener en cuenta que el principio de doble incriminación no es una condición previa para la concesión de ayuda: la "asistencia se prestará sin considerar si la conducta objeto de la investigación, procesamiento o actuación en el Estado requirente constituiría un delito con arreglo a la legislación del Estado requerido". La solicitud debe ejecutarse de conformidad con la legislación del Estado requerido y con las disposiciones del Protocolo[205]. En el artículo 4 se estipula que el Estado requerido debería hacer todos los arreglos necesarios para permitir que el Estado requirente sea representado en cualquier procedimiento que surja de una solicitud de asistencia.

En el artículo 6 del Protocolo se estipulan algunos motivos de denegación opcionales. Estos hacen referencia a los delitos de carácter militar y político, de soberanía, seguridad y orden público, así como los de no conformidad con las disposiciones del Protocolo.

Tipos de asistencia judicial recíproca permitida
En el artículo 2 del Protocolo se mencionan, entre los tipos de asistencia a otorgarse en virtud del mismo, los de localizar o identificar personas, facilitar información y documentos, presentar documentos, efectuar inspecciones e incautaciones, obtener pruebas y facilitar la comparecencia de testigos.

Contenido de la solicitud y otros requisitos formales
En el artículo 5 se establece el contenido de la solicitud, el cual estipula los requisitos generales y específicos, dependiendo del tipo de asistencia judicial recíproca que se haya solicitado. Los requisitos generales se refieren al nombre de la autoridad competente del Estado requirente, el carácter de la investigación o procedimientos, el resumen de los hechos, el suministro de una copia de las disposiciones legales aplicables, la identificación del propósito de la solicitud, la naturaleza de la asistencia que se solicita y el grado de confidencialidad que se requiere.

Canales de comunicación
El Protocolo exige que las autoridades centrales tengan la competencia para formular y recibir solicitudes de asistencia judicial recíproca y que establezcan contacto directo unas con otras. Sin embargo, en el artículo 3 se disponen alternativas tales como el uso de la vía diplomática o de Interpol.

Relación con otros instrumentos
En el artículo 23 titulado "Relación con otros instrumentos", se estipula que la disposición de cualquier tratado o acuerdo bilateral aplicable entre cualesquiera dos Estados Parte deberá complementar al Protocolo y se deberá aplicar de conformidad con las disposiciones del mismo. En caso en que existan inconsistencias entre el Protocolo y otros instrumentos, prevalecerán las disposiciones del primero.

[203] El Protocolo, que fue adoptado por la Comunidad del África Meridional para el Desarrollo, puede consultarse en línea en: http://www.sadc.int/index/browse/page/156.
[204] Véase el artículo 2 del Protocolo, relativo al alcance de la aplicación y la obligación de proporcionar asistencia judicial recíproca.
[205] Véase el artículo 4 del Protocolo.

Convenio europeo sobre cooperación judicial en materia penal de 1959[206]

Condiciones

El Convenio exige que los Estados Parte se presten la asistencia recíproca más amplia posible en los procedimientos relativos a delitos cuyo castigo está comprendido dentro de la jurisdicción de las autoridades judiciales de la Parte requirente[207]. Los motivos de denegación opcionales que se mencionan en el artículo 2 hacen referencia a los delitos de carácter político y fiscal (en este último caso, nótense los cambios introducidos por el Primer Protocolo Adicional al Convenio), así como a los de soberanía, orden público, seguridad u otros intereses esenciales de la Parte requerida. Respecto de las cartas rogatorias, existen requisitos específicos que se mencionan en el artículo 5 del Convenio, tal como figura a continuación:

- Que la infracción que motiva la carta rogatoria sea sancionable en la legislación tanto de la Parte requirente como de la requerida;
- Que el delito que motiva la carta rogatoria sea extraditable en el país requerido; y
- Que el cumplimiento de la carta rogatoria sea compatible con la legislación de la Parte requerida.

Estos motivos de denegación no son obligatorios sino que opcionales, lo que permite a las Partes del Convenio presentar una declaración en este sentido.

Tipos de asistencia judicial recíproca permitida

El Convenio permite varias formas de cooperación, pero para los propósitos de esta guía y teniendo en cuenta el carácter de la mayoría de las solicitudes, los más relevantes son las cartas rogatorias y la expedición de documentos.

En los artículos 3, 4 y 5 del Convenio se hace referencia a las cartas rogatorias, que en general se cumplirán de conformidad con la legislación del Estado requerido. El Convenio permite la transmisión de copias certificadas o copias fotostáticas de los documentos requeridos a menos que el Estado requirente exija el envío de originales.

En el artículo 7 se establece como regla principal que la presentación de documentos se realice a través de una transmisión simple del documento a la persona interesada. Si el Estado requirente solicita que la expedición de documentos se realice de la manera prevista en su legislación, el Estado requerido deberá actuar en consecuencia[208]. La prueba de la entrega será un recibo fechado y firmado por el destinatario del documento, o bien una declaración en la que el Estado requerido manifieste que se ha hecho entrega del documento que indique el modo y la fecha en que se haya realizado.

---

[206] La decisión de elaborar un Convenio relativo a la asistencia judicial en materia penal se tomó durante la cuadragésima primera reunión de Ministros adjuntos celebrada en septiembre de 1956, donde se decidió encomendar a los expertos la preparación de un borrador del Convenio sobre asistencia recíproca en materia penal. Véase el informe explicativo en: http://conventions.coe.int/Treaty/en/Reports/Html/030.htm.

[207] Véase el artículo 1 del Convenio.

[208] Véase el artículo 7, párrafo 1, del Convenio.

La entrega de documentos a los acusados deberá hacerse con suficiente antelación al plazo real establecido para el juicio. A tal efecto, el Convenio permite a los Estados Parte hacer declaraciones solicitando que la entrega de la convocatoria a un acusado se envíe a sus autoridades dentro de un determinado plazo antes de la fecha establecida para la comparecencia. Este plazo debería especificarse en la declaración, pero no puede exceder los 50 días[209].

Contenido de la solicitud y otros requisitos formales
En el artículo 14, párrafo 1, se establecen los requisitos generales respecto del contenido de la solicitud, la cual deberá incluir el nombre de la autoridad que formula la solicitud, el objeto, la razón de la misma, la identidad y nacionalidad de la persona interesada, si es posible, el nombre y dirección de la persona en cuestión en el caso de que se necesite presentar documentos. Además de esto, existen requisitos específicos en relación con las cartas rogatorias. En tales casos, se deberá mencionar también el delito y presentar un resumen de los hechos.

Canales de comunicación
En el artículo 15 del Convenio se incluyen las disposiciones pertinentes al tema. La norma es que se establezca un contacto entre los Ministerios de Justicia de los Estados requirente y requerido, y en lo que concierte a la carta rogatoria, podría establecerse un contacto directo entre las autoridades judiciales únicamente en caso de urgencia (sin embargo, los documentos se remitirían a través de las autoridades centrales). En el artículo 13, párrafo 1, se establece otra situación en la que se permite un contacto directo (en los extractos y la información relativa a los expedientes judiciales). En los casos en que se permite la transmisión directa, la misma puede hacerse incluso a través de Interpol (esta disposición fue ligeramente modificada conforme al Segundo Protocolo Adicional).

Otro aspecto importante a destacar es que el Convenio otorga preferencia a otros acuerdos o arreglos bilaterales que ya se encuentren en vigor entre las partes, lo que permite una transmisión directa de solicitudes de asistencia judicial recíproca[210].

Relación con otros instrumentos
El artículo 26 del Convenio aborda este tema. Según lo dispuesto en el párrafo primero, el Convenio de 1959 sustituirá a los demás tratados, convenios o acuerdos bilaterales que rijan las solicitudes de asistencia judicial recíproca entre las partes, excepto las disposiciones relativas al envío directo de las solicitudes y la traducción de las mismas y los documentos adjuntos, que seguirán siendo regidos por tratados, arreglos, etc., anteriores[211].

Sin embargo, el Convenio no afecta a las obligaciones específicas respecto de la asistencia judicial recíproca en una esfera determinada por razón de instrumentos bilaterales o multilaterales anteriores.

En cuanto a los futuros acuerdos bilaterales o multilaterales, podrían celebrarse a fin de complementar las disposiciones del Convenio o para facilitar su aplicación.

[209] Véase el artículo 7, párrafo 3, *ibid*.
[210] Véase el artículo 15, párrafo 7, *ibid*.
[211] Véase el artículo 26, párrafo 1, del Convenio, así como el informe explicativo en: http://conventions.coe.int/Treaty/en/Reports/Html/030.htm.

Primer Protocolo Adicional de 1978 al Convenio de 1959[212]

El Primer Protocolo Adicional incluye las normas que introducen las enmiendas del texto del Convenio con respecto a los delitos fiscales, la entrega de documentos relativos al cumplimiento de una sentencia, el reembolso de una multa (véase el artículo 3 del Protocolo), así como las modificaciones al artículo 22 del Convenio sobre el intercambio de información de expedientes judiciales (véase el artículo 4 del Protocolo).

Cabe mencionar que el Protocolo confiere preeminencia a las "regulaciones más amplias en los acuerdos bilaterales y multilaterales celebrados entre las Partes contratantes", en aplicación del artículo 26, párrafo 3, del Convenio (el cual permite a los Estados Parte celebrar otros acuerdos o instrumentos para complementar las disposiciones del Convenio o para facilitar su aplicación).

Segundo Protocolo Adicional de 2001 al Convenio de 1959[213]

Para los propósitos de esta guía, el Segundo Protocolo Adicional de 2001, que introdujo cambios en lo relativo a los canales de comunicación (artículo 4 del Protocolo), así como nuevas formas de cooperación, es el que tiene mayor relevancia. Los cambios incluyen el uso de la videoconferencia o la conferencia telefónica para llevar a cabo la audiencia, los comentarios transfronterizos, la entrega vigilada y las investigaciones encubiertas, así como los equipos conjuntos de investigación. Muchas de estas disposiciones se encuentran en el Convenio de la UE de 2000 (véase *infra*). Debido a las restricciones de espacio, pero también en vista de que esta guía ofrece una orientación general, se hará referencia únicamente a algunas de las disposiciones del Protocolo, a saber, las que se refieren a los canales de comunicación, a la transmisión espontánea de información y a los equipos conjuntos de investigación.

Canales de comunicación

En el artículo 4 se establece como regla general que las solicitudes se canalicen a través de los Ministerios de Justicia de los Estados cooperantes. Este artículo también permite el contacto directo entre las autoridades judiciales de los Estados requirente y requerido. Este mismo contacto directo puede aplicarse con respecto a las entregas vigiladas y las investigaciones encubiertas, así como a las cartas rogatorias en general, aunque existen algunas solicitudes de asistencia judicial recíproca que continuarán siendo enviadas y recibidas a través de las autoridades centrales (por ejemplo, las solicitudes de traslado temporal de testigos o detenidos al Estado requerido). El contacto directo también es posible con referencia al envío de copias de condenas e información relacionada con expedientes judiciales[214].

En caso de urgencia se pueden utilizar los servicios de Interpol. Cabe destacar que en el artículo 4, párrafo 7, del Segundo Protocolo Adicional se permite recurrir a la Interpol únicamente en los casos urgentes, mientras que en el párrafo 5 del

[212] El texto del Protocolo Adicional y el informe explicativo pueden consultarse en: http://www.asser.nl/default.aspx?site_id=8&level1=10785&level2=10861.

[213] El texto del Segundo Protocolo Adicional al Convenio europeo sobre cooperación judicial en materia penal, STE núm. 182, se encuentra disponible en: http://conventions.coe.int/treaty/en/Treaties/word/182.doc.

[214] Véase el artículo 4, párrafos 5 y 6, del Segundo Protocolo Adicional, *ibid*.

artículo 15 del Convenio se autoriza su utilización en general cuando está permitido el contacto directo.

El Protocolo permite que los Estados Parte decidan si desean transmitir copias de la solicitud a las autoridades centrales, incluso en casos urgentes, o enviar algunas de las solicitudes a través de otros canales (incluida la vía diplomática).

Cabría destacar que en el artículo 16 se permite a un Estado Parte efectuar la notificación o el envío de documentos procesales y judiciales directamente a las personas que se encuentren en el territorio de otro Estado Parte a través del correo postal[215]. Este mismo artículo también presenta cambios respecto de los medios de comunicación, que son de suma importancia cuando se trata de datos vulnerables tal como se da generalmente en los casos de delitos informáticos o relacionados con la identidad. En el artículo 4, párrafo 9, se especifica que las solicitudes pueden ser enviadas a través de medios electrónicos u otro medio de comunicación, siempre y cuando también se formule una solicitud por escrito.

Transmisión espontánea de la información
En el artículo 11 del Protocolo se permite a las autoridades competentes de una de las partes transmitir a las autoridades competentes de la otra parte la información obtenida en el curso de su propia investigación, si creen que dicha información podría ayudar al país receptor a iniciar o llevar a cabo tareas de investigación[216].

Equipos conjuntos de investigación
En el artículo 20 del Protocolo se sientan las bases para la creación de los equipos conjuntos de investigación entre los Estados miembros del Consejo de Europa, y guarda muchas similitudes con el artículo 13 de la Convención de la UE de 2000 relativa a la asistencia judicial recíproca.

Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea de 2000[217]

De conformidad con este Convenio, la asistencia judicial recíproca se prestará de acuerdo con los requisitos del Estado requirente, a menos que los trámites y procedimientos contravengan los principios del derecho interno del Estado requerido. Esta disposición se aparta de la práctica tradicional en la que la solicitud debe ejecutarse de conformidad con las disposiciones del derecho interno del Estado requerido.

Tipos de asistencia judicial recíproca permitida
El Convenio complementa a los llamados convenios de base en este ámbito, incluidos el Convenio del Consejo de Europa de 1959 y su Protocolo Adicional de 1978, así como las disposiciones sobre asistencia judicial recíproca del Acuerdo de Schengen de 1990. De conformidad con el Convenio de 2000, se regularon formas específicas

[215] Para más detalles, véase el artículo 16, *idem*.
[216] Véase el artículo 11, *idem*, así como el informe explicativo al Segundo Protocolo Adicional, disponible en: http://conventions.coe.int/treaty/en/Reports/Html/182.htm.
[217] El texto del Convenio, del Protocolo Adicional y de los informes explicativos pueden consultarse en: http://ec.europa.eu/justice_home/doc_centre/criminal/acquis/doc_criminal_acquis_en.htm.

de asistencia recíproca, tales como la videoconferencia (artículo 10), la conferencia telefónica (artículo 11), las entregas vigiladas (artículo 12), los equipos conjuntos de investigación (artículo 13) y las investigaciones encubiertas (artículo 14). Asimismo, existen disposiciones importantes relacionadas con la intercepción de comunicaciones telefónicas (artículos 17 a 22). Para los propósitos de esta guía se hará especial referencia a los artículos 5, 6, 7 y 13.

Contenido de la solicitud
Respecto de este tema, se aplicarán los requisitos generales establecidos en los convenios de base.

Canales y medios de comunicación
Las solicitudes deberán hacerse por escrito, por cualquier medio capaz de reproducir un documento escrito. En el artículo 6, párrafo 1, del Convenio se establece como norma que exista un contacto directo entre las autoridades judiciales de emisión y ejecución. Sin embargo, este requisito no impide que el envío se realice entre autoridades centrales o entre la autoridad judicial de un Estado Parte y la autoridad central de otro. Existen algunos tipos de solicitudes (por ejemplo, la transferencia temporal de personas en custodia) que aún deberían llevarse a cabo en todos los casos a través de las autoridades centrales[218].

Respecto de la notificación de documentos procesales, el Convenio es bastante innovador con relación a los instrumentos anteriores (las disposiciones se adoptarán también en el Segundo Protocolo Adicional al Convenio del Consejo de Europa de 1959), ya que establece, como regla general, que los documentos se envíen directamente al destinatario en el otro Estado miembro de la UE a través del correo postal.

Los documentos procesales podrían enviarse a través de las autoridades competentes del Estado miembro requerido únicamente si:

- Se desconoce o no se sabe con exactitud la dirección de la persona a la que se destina el documento; o
- El derecho procesal pertinente del Estado miembro requirente exige una prueba de que el documento fue entregado al destinatario distinta de la que se puede obtener del servicio postal; o
- No se ha podido enviar el documento por correo; o
- El Estado miembro requirente tiene razones justificadas para considerar que el envío por correo podría resultar ineficaz o inadecuado[219].

Intercambio espontáneo de la información
En el artículo 17 se permite a los Estados Parte, dentro de los límites de sus leyes nacionales, intercambiar, sin que exista una solicitud previa, información relativa a los delitos penales o infracciones de las normas de derecho de los que tendrían que ocuparse las autoridades receptoras.

[218] Véase el artículo 6, párrafo 8, del Convenio.
[219] Véase el artículo 5, párrafo 2, incisos *a)* a *d)*, *ibid.*

Equipos conjuntos de investigación

Como se mencionó anteriormente, el concepto de los equipos conjuntos de investigación está cobrando cada vez mayor importancia a causa del aumento de la delincuencia transnacional. Debido a que el proceso de ratificación del Convenio ha sido lento, las mismas disposiciones se incluyeron en una Decisión Marco del Consejo sobre equipos conjuntos de investigación adoptada el 13 de junio de 2002, que los Estados miembros deberían haber puesto en funcionamiento en 2003[220].

Los equipos conjuntos de investigación pueden establecerse con un propósito específico y por un período de tiempo limitado con el fin de realizar investigaciones en uno o más de los Estados miembros que los crearon. Esto se lleva a cabo a través de acuerdos recíprocos[221].

Los equipos conjuntos de investigación se forman cuando las investigaciones en un Estado miembro plantean dificultades y dependen de investigaciones posteriores en otros Estados miembros, o cuando varios Estados llevan a cabo investigaciones que requieren de acciones coordinadas y concertadas. Un equipo conjunto de investigación opera en el territorio del Estado miembro encargado de formar ese equipo, bajo la condición de que las operaciones se realicen de conformidad con la legislación del Estado donde opera, y que el jefe del equipo sea de ese Estado.

En lo que respecta a los miembros del equipo, aquellos que no sean originarios del Estado donde opera el equipo serán llamados miembros asignados en comisión de servicio. En el artículo 13, párrafos 5 y 10, del Convenio se establece claramente la competencia de estos y el uso que pueden hacer de la información que se obtenga durante la investigación.

Relación con otros instrumentos

A diferencia de otros instrumentos que incluyen los artículos pertinentes al final, el artículo 1 del Convenio establece estos aspectos desde el principio (Relación con otros convenios sobre asistencia recíproca), estipulando que el Convenio de la UE de 2000 complementa y facilita la aplicación de las disposiciones del Convenio del Consejo de Europa de 1959 relativo a la de asistencia judicial en materia penal y su Protocolo Adicional de 1978, así como las disposiciones del Acuerdo de Schengen, de 19 de junio de 1990, y el capítulo 2 del Tratado de Benelux. Debido a estas disposiciones, se considera que al formular una solicitud de asistencia judicial no se puede recurrir únicamente a la Convención, sino que siempre deberá citarse conjuntamente con el Convenio de base que complementa. En caso de que existan disposiciones contradictorias entre los dos, prevalecerá el Convenio de la UE de 2000[222].

---

[220] Para más detalles, véase el Manual de los equipos conjuntos de investigación adoptado por Europol y Eurojust, así como la implementación de la orden de detención europea y los equipos conjuntos de investigación a nivel nacional y de la UE (estudio), enero de 2009, publicado por el Directorate General Internal Policies, Policy Department C, Citizens' Right and Constitutional Affairs, disponible en: http://www.ecba.org/cms/index.php?option=com_content&task=view&id=259&Itemid=21.

[221] Por recomendación del Consejo de 8 de mayo de 2003, se propuso un Modelo de Acuerdo para la creación de un equipo conjunto de investigaciónúm. Actualmente el tema está siendo objeto de debate a nivel de la UE en su versión actualizada.

[222] Véase el informe explicativo del Convenio, disponible en: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229(02)&model=guichett.

Protocolo de 2001 del Convenio de 2000

El Protocolo es especialmente relevante para las disposiciones relativas a la información sobre cuentas y transacciones bancarias, lo que podría resultar de utilidad en el contexto de los delitos relacionados con la identidad y su conexión con actividades de blanqueo de capitales[223].

Conclusiones

A pesar del hecho de que todos estos instrumentos han sido adoptados en diferentes contextos regionales y que son muy diferentes entre sí, existen varios elementos que permanecen constantes. Como autoridad judicial emisora o de ejecución, es fundamental seguir algunos pasos a fin de optimizar la cooperación en los casos de delitos relacionados con la identidad, sobre la base de los instrumentos existentes.

Antes de proceder al envío de una solicitud formal, sería oportuno recurrir a las fuerzas policiales o del orden ya que estas podrían hacer aportaciones valiosas. También podría resultar de utilidad celebrar consultas previas con el Estado de ejecución.

En la mayoría de los casos, la comunicación de los documentos se realiza a través de las autoridades centrales, incluidas las situaciones en las que el envío se realiza por vía diplomática. Se trata de un procedimiento demasiado largo, por lo que la autoridad judicial requirente o requerida debería ser capaz de utilizar un procedimiento más eficaz para obtener una respuesta rápida. En la mayoría de los casos, esto significaría establecer un contacto directo o, si el tratado en vigor no lo permite, recurrir a las redes disponibles en las que los contactos personales entre los puntos de contacto son de suma importancia (este aspecto se abordará al final del presente capítulo). Las respuestas que se reciben con prontitud dependen con frecuencia de la forma en que se completó la solicitud y si se siguieron los procedimientos que se especifican en el Tratado aplicable o las necesidades especiales del derecho interno del Estado de ejecución.

En los casos de los delitos relacionados con la identidad, los problemas y desafíos revisten un carácter transnacional[224]. Como se muestra en la sección donde exponen los estudios de casos, esto implicaría la participación de múltiples jurisdicciones y diversos sistemas jurídicos. En estas situaciones, la coordinación es esencial para obtener los resultados que se esperan. Una de las mejores soluciones en estas circunstancias sería recurrir a los equipos conjuntos de investigación.

A fin de mejorar los resultados de los casos que se presentan a diario, es necesario tener en cuenta aspectos tales como el establecimiento de prácticas óptimas[225] en la materia y la

[223] Para una interpretación de sus disposiciones, véase el informe explicativo en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:257:0001:0009:ES:PDF.

[224] La información detallada sobre la cooperación internacional en los casos de delitos relacionados con la identidad puede consultarse en el Informe del Secretario General titulado: Cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad, E/CN.15/2009/2, Viena, 16 a 24 de abril de 2009.

[225] Véase el Informe del Grupo de trabajo especializado en prácticas óptimas de asistencia judicial recíproca, disponible en: http://www.unodc.org/pdf/lap_mlaeg_report_final.pdf, que también incluye en la última parte modelos de listas de comprobación y formularios.

continua capacitación de las personas encargadas de tramitar las solicitudes de asistencia judicial recíproca. Entre los factores clave para lograr una mayor cooperación con respecto a este tipo de delincuencia, se cuentan el diálogo permanente, la utilización de las herramientas y la capacitación que proporcionan las organizaciones internacionales.

4. Formas específicas de asistencia judicial recíproca que pueden ser relevantes para el delito relacionado con la identidad previstas en el Convenio del Consejo de Europa sobre el delito cibernético y en el Plan de Harare

Como se mencionó con anterioridad, el Convenio del Consejo de Europa sobre el delito cibernético introdujo algunas formas específicas de asistencia recíproca[226], las cuales fueron diseñadas para abordar las particularidades de los delitos cibernéticos y de los delitos que se cometen en línea. Es importante saber que los Estados Parte en el Convenio cuentan con estas disposiciones en sus legislaciones nacionales. Aunque algunos países no han firmado o ratificado el Convenio, podrían haber introducido tales medidas en su legislación nacional. Además, también se hará especial referencia al artículo sobre la conservación de datos y al artículo en el Plan de Harare de asistencia judicial recíproca, que se mencionó brevemente en las páginas sobre el instrumento del Commonwealth[227].

Los artículos 29 a 33 del Convenio representan el "equivalente de la asistencia judicial recíproca" para el conjunto de disposiciones que establecen instrumentos de procedimiento específicos[228], los cuales están diseñados para optimizar las investigaciones en los Estados Parte[229]. Con respecto al principio de la soberanía nacional, estos instrumentos solo pueden utilizarse para las investigaciones llevadas a cabo a nivel nacional[230]. Si los investigadores se percatan de que las pruebas deben reunirse fuera de su territorio, necesitarán solicitar asistencia judicial recíproca. Cada uno de los instrumentos establecidos en los artículos 16 a 21 tienen una disposición correspondiente en los artículos 29 a 33, lo que permite a los organismos encargados de hacer cumplir la ley aplicar los instrumentos de procedimiento a la solicitud de un organismo extranjero encargado de hacer cumplir la ley.

---

[226] Para un análisis detallado de la asistencia judicial recíproca centrada en las medidas provisionales en virtud del Convenio del Consejo de Europa sobre delito cibernético, véase *Cybercrime Training for Judges (Training Manual)*, cuarta versión, marzo de 2009, elaborado por *Gercke*, página 84 y ss., disponible en: http//:www.coe.int/cybercrime.

[227] Véase *supra*, en la sección relativa al Plan de Harare.

[228] Véase *Gercke*, "Understanding Cybercrime ...", *supra* núm. 26, capítulo 6.2.

[229] Los instrumentos de procedimiento más importantes que establece el Convenio sobre el delito cibernético son: Conservación inmediata de datos informáticos almacenados (artículo 16), Conservación y divulgación inmediata de los datos de tráfico (artículo 17), Mandato de comunicación (artículo18), Registro y decomiso de datos informáticos almacenados (artículo 19), Recogida en tiempo real de datos informáticos (artículo 20) e Interceptación de datos relativos al contenido (artículo 21).

[230] El artículo 32 del Convenio es una excepción. Respecto de este instrumento, véase el Informe de la 2a reunión del Comité del Convenio sobre el delito cibernético, T-CY (2007) 03, página 2: "[...] la Federación de Rusia (tenía una actitud positiva hacia el Convenio, pero debería conceder mayor consideración al inciso *b)* del artículo 32 en particular, a la luz de la experiencia adquirida del empleo de este artículo).

Conservación inmediata de los datos informáticos almacenados: artículo 29 del Convenio del Consejo de Europa sobre el delito cibernético

Esta disposición reviste especial importancia para la investigación de delitos informáticos en general, y para el delito relacionado con la identidad en particular. La misma permite que el Estado requirente solicite al Estado requerido que conserve los datos almacenados, ganando así tiempo adicional antes de presentar la solicitud formal de asistencia judicial recíproca. Esta última incluye el registro, el decomiso o la divulgación de los datos. Se trata de una medida lógica, habida cuenta de la volatilidad que tienen los datos en el ciberespacio, ya que impide que un delincuente los elimine, altere o extraiga. En el artículo 29 se establece un mecanismo a nivel internacional equivalente al previsto en el artículo 16 para uso a nivel nacional[231]. En el artículo 29, párrafo 2, se establece el contenido de la solicitud para la conservación de datos, se especifica la autoridad solicitante, el delito objeto de investigación, una breve exposición de los hechos vinculados al mismo, los datos informáticos almacenados que deben conservarse, la información del responsable de los datos informáticos almacenados, la necesidad de conservación y la acreditación de que el Estado requirente está dispuesto a formular una solicitud de asistencia judicial recíproca[232]. El principio de la doble incriminación constituye un motivo de denegación únicamente si el delito en cuestión es distinto a los que se establecen en los artículos 2 a 11 del Convenio sobre el delito cibernético, y aún así representa un motivo de denegación opcional. Una solicitud también podría ser denegada si el Estado requerido estima que de acceder a la misma pondría en peligro su soberanía y el orden público, o si considera que se trata de delitos de carácter político[233]. Los datos pueden conservarse por un período de al menos 60 días, para permitir al Estado requirente formular una solicitud formal de asistencia judicial recíproca.

Solicitudes de conservación de datos informáticos en virtud del Plan de Harare de asistencia judicial recíproca

De conformidad con este instrumento, la solicitud de conservación de datos en general no varía en términos de contenido respecto de los requisitos mencionados en el Convenio del Consejo de Europa sobre delitos cibernéticos[234]. La principal diferencia es el límite de tiempo, que en este caso es de 120 días. La solicitud podría ser denegada únicamente si "el Estado requerido estima que de acceder a la demanda estaría actuando contrario a sus leyes o su constitución o se pondría en peligro su seguridad, sus relaciones internacionales u otro interés público esencial de su país".

Comunicación inmediata de los datos de tráfico conservados: artículo 30 del Convenio del Consejo de Europa sobre el delito cibernético

En el artículo 30 se dispone el equivalente internacional del poder establecido en el artículo 17 para el uso interno. Con frecuencia, a solicitud del Estado Parte donde se cometió el delito, la parte requerida conservará los datos de tráfico relativos a una transmisión que se ha realizado a través de sus computadoras, a fin de rastrear el

[231] Véase el informe explicativo del Convenio del Consejo de Europa sobre el delito cibernético, *supra* núm. 157, párrafo 282.

[232] Para la lista de comprobación propuesta para las solicitudes de conservación inmediata, véase The functioning of the 24/7 points of contact for cybercrime, documento de debate disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20DataPreservationChecklists_en.pdf.

[233] Véase el artículo 29, párrafo 5.

[234] Véase el artículo 15, párrafo 2, del Plan.

origen de la misma y poder identificar al autor del delito o localizar pruebas de importancia crítica. Así, la Parte requerida podría identificar si los datos de tráfico en su territorio revelan que la transmisión ha sido enviada desde un proveedor de servicios en un tercer Estado, o desde un proveedor en el propio Estado requirente. En tales casos, el Estado requerido deberá, con carácter urgente, proporcionar a la parte requirente suficientes datos de tráfico para permitir la identificación del proveedor de servicios y la ruta de comunicación en el otro Estado. Si la transmisión proviene de un tercer Estado, la información permitirá a la parte requirente formular una solicitud de conservación de datos y de asistencia recíproca inmediata a ese otro Estado a fin de seguir el rastro de la transmisión hasta su fuente última. Si la transmisión regresase al Estado requirente, este será capaz de conservar y divulgar datos de tráfico adicionales a través de procesos internos[235].

La parte requerida podría negarse a divulgar los datos de tráfico únicamente si considera que podría menoscabar su soberanía, su seguridad, su orden público u otros intereses fundamentales, o cuando considere que se refiere a un delito de carácter político o relacionado con un delito político. Al igual que en el artículo 29 (Conservación inmediata de datos informáticos almacenados), debido a que este tipo de información reviste especial importancia para identificar a aquellos que cometieron delitos que entran en el ámbito de aplicación de este Convenio, o para localizar pruebas de importancia crítica, los motivos de denegación deben de ser estrictamente limitados y quedan excluidos cualesquiera otros motivos de denegación de asistencia.

Asistencia judicial recíproca concerniente al acceso a datos informáticos almacenados: artículo 31 del Convenio del Consejo de Europa sobre el delito cibernético
Una vez más, este artículo corresponde a una medida similar dispuesta a nivel interno, como se estipula en el artículo 19 del Convenio, titulado "Registro y decomiso de datos informáticos almacenados". El Estado requerido debe ejecutar la solicitud de conformidad con los instrumentos y acuerdos internacionales celebrados con el Estado requirente que ya se encuentren en vigor (en este sentido, se hace especial referencia al artículo 23 del Convenio) y si fuera necesario, de manera expeditiva[236].

Asistencia recíproca para la recogida en tiempo real de datos relativos al contenido: artículo 33 del Convenio del Consejo de Europa sobre el delito cibernético
En el artículo se establecen las bases de la cooperación internacional para la recogida de datos de tráfico en tiempo real, y se da preeminencia a los tratados y acuerdos existentes que permitan este tipo de colaboración[237].

Asistencia judicial recíproca en materia de interceptación de datos relativos al contenido: artículo 34 del Convenio del Consejo de Europa sobre el delito cibernético
Debido al alto grado de intrusión que supone la interceptación de datos de contenido, se restringe la obligación de proporcionar asistencia judicial recíproca para realizar dicha interceptación. La asistencia se proporcionará en la medida en que los tratados

[235] Para más información con respecto a la interpretación de este artículo, véase el informe explicativo, *supra* núm. 157, párrafos 290 y 291.
[236] Véase el artículo 31, párrafo 3, incisos *a)* y *b)*.
[237] Véase el informe explicativo, *supra* núm. 157, párrafos 295 y 296.

vigentes o las leyes internas de los Estados Parte lo permitan. Dado que la disposición sobre cooperación para la interceptación de datos de contenido es un ámbito nuevo dentro de la práctica de asistencia judicial recíproca, se resolvió adherirse a los regímenes de asistencia judicial recíproca y a las leyes nacionales existentes relativos al alcance y las limitaciones de la obligación de prestar asistencia[238].

5. La función de las redes para dar respuesta a las solicitudes de asistencia judicial recíproca

Para obtener respuestas rápidas es fundamental tener acceso a las diferentes redes e instituciones que facilitan las interconexiones. Existen diferentes redes regionales que pueden demostrar su funcionalidad a nivel regional, así como instituciones que funcionan a nivel bilateral, tales como los magistrados de enlace. En la era de la globalización resulta más importante que nunca que las redes regionales trabajen en colaboración como una red mundial. La presentación de un marco jurídico relativo a la cooperación internacional en los casos de delitos relacionados con la identidad no puede ignorar este aspecto, ya que en muchas ocasiones el uso de las redes nacionales arroja resultados más rápidos y satisfactorios. A pesar de que estas redes tienen un carácter principalmente informal, los puntos de contacto pueden ofrecer información valiosa sobre los sistemas jurídicos e información de contacto de las autoridades competentes, todo lo cual facilita la transmisión de solicitudes de asistencia judicial recíproca.

Las redes 24/7

Existen varias redes que operan de manera ininterrumpida, durante las 24 horas, siete días de la semana, incluida la red diseñada en el marco del G8, y la red desarrollada por los Estados Parte del Convenio del Consejo de Europa sobre el delito cibernético. La función que cumplen las redes 24/7 es asegurar la disponibilidad de los puntos de contacto a toda hora, de modo que puedan atenderse cuanto antes las medidas provisionales que deben tomarse respecto de los delitos informáticos (incluidas las formas de delitos relacionados con la identidad cometidos en línea).

Las investigaciones sobre los delitos cibernéticos con frecuencia requieren una reacción inmediata[239]. Para incrementar la velocidad de las investigaciones internacionales, el artículo 25 del Convenio Europeo sobre el delito cibernético destaca la importancia de permitir el uso de medios de comunicación expeditivos. Con el fin de mejorar aún más la eficiencia de las solicitudes de asistencia recíproca, el Convenio exige que los Estados

[238] Véase el informe explicativo, *ibid.*, párrafo 297.

[239] En el informe explicativo se indica la necesidad de acelerar el proceso de cooperación internacional: "Los datos informáticos son muy volátiles. Al pulsar unas pocas teclas o mediante la operación de programas automáticos, estos pueden ser eliminados, haciendo imposible seguir la pista de un delito hasta su autor o destruyendo pruebas esenciales de su culpabilidad. Algunas formas de datos informáticos están almacenados solo por cortos períodos de tiempo antes de ser eliminados. En otros casos, se puede causar un daño significativo a personas o bienes si las pruebas no se reúnen con rapidez. En esos casos urgentes, no solo la solicitud, sino también la respuesta deben hacerse de una manera acelerada. El objetivo del párrafo 3 es, por tanto, facilitar la aceleración del proceso de obtención de asistencia mutua de manera tal que la información o las pruebas esenciales no se pierdan debido a que han sido eliminadas antes de que pudiera prepararse, transmitirse y dar respuesta".

Parte designen un punto de contacto para las solicitudes de asistencia judicial recíproca, y que estos puntos estén disponibles a toda hora[240]. Los encargados de redactar el texto del Convenio pusieron de relieve que el establecimiento de los puntos de contacto es una de las medidas más importantes previstas en este instrumento[241].

Según lo dispuesto en el artículo 35 del Convenio sobre el delito cibernético, los puntos de contacto tienen la responsabilidad de ofrecer servicios de asesoramiento técnico, conservar los datos de conformidad con los artículos 29 y 30 del Convenio, reunir pruebas, localizar sospechosos o brindar información jurídica. Los Estados Parte han hecho declaraciones para identificar a sus órganos internos a cargo de estas tareas. En el sitio web del Consejo de Europa se puede encontrar una lista de los puntos de contacto[242]. En el documento de debate titulado "El funcionamiento de los puntos de contacto 24/7 para el delito cibernético", que se encuentra en el mismo sitio web, se destacan otros elementos importantes.

La Red Judicial Europea (RJE) y EUROJUST dentro de la UE

La RJE

La Red Judicial Europea se estableció en 1998 en virtud de la Acción Conjunta 98/428/JAI, y cuenta con puntos de contacto entre las autoridades centrales y judiciales de los Estados miembros de la Comisión Europea. El instrumento actual que trata con la Red Judicial Europea data de 2008[243]. De conformidad con el artículo 4 de la Acción Conjunta, los puntos de contacto hacen las partes de intermediarios activos destinados a facilitar la cooperación judicial entre los Estados miembros, en particular para combatir los delitos graves (la delincuencia organizada, la corrupción, el tráfico de drogas y el terrorismo). Asimismo proporcionan información jurídica y práctica de utilidad para las autoridades judiciales locales de sus propios países, así como para los puntos de contacto y las autoridades judiciales locales de otros países a fin de que puedan preparar de manera eficaz una solicitud de asistencia judicial o para mejorar la cooperación judicial en general. Además, su función es coordinar de manera eficiente la cooperación judicial en los casos en que las solicitudes de las autoridades judiciales de un Estado miembro requieran una acción coordinada en otro Estado miembro.

Los puntos de contacto tienen acceso a un sistema de telecomunicaciones seguro. La Red Judicial Europea posee una lista de contraseñas de los recursos protegidos, si bien algunos materiales, formularios e información también se encuentran disponibles en el sitio público de la web[244]. El mismo componente público abarca el Atlas Judicial Europeo en relación con la orden de detención europea y con la asistencia judicial recíproca.

---

[240] La disponibilidad las 24 horas del día, los 7 días de la semana es especialmente importante con respecto a la dimensión internacional del delito cibernético, ya que las solicitudes pueden provenir de regiones del mundo con diferentes husos horarios. En cuando a la dimensión internacional del delito cibernético y las dificultades relacionadas véase: *Gercke*, Understanding Cybercrime…, *supra* núm. 27, capítulo 3.2.6.

[241] Véase el informe explicativo, *supra* núm. 157.

[242] Esta lista puede consultarse en: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp.

[243] Decisión del Consejo 2008/976/JAI, de 16 de diciembre de 2008, sobre la Red Judicial Europea.

[244] A este respecto véase: http://www.ejn-crimjust.europa.eu/.

La Unidad de Cooperación Judicial de la Unión Europea (EUROJUST)

Eurojust es un organismo compuesto de 27 miembros nacionales con sede en La Haya. Este organismo se estableció en 2002 por decisión del Consejo de Europa[245] y fue modificado en 2003 y en 2009. Eurojust tiene como objetivo estimular y mejorar la coordinación de las investigaciones y procesos en los Estados miembros, mejorar la cooperación entre las autoridades competentes de los mismos, en particular facilitando la ejecución de la asistencia judicial recíproca y la tramitación de las solicitudes de extradición, y prestar otro tipo de apoyo a las autoridades competentes de los Estados miembros a fin de que las investigaciones y procesos sean más eficaces (artículo 3 de la decisión del Consejo). Consta de un miembro nacional designado por cada Estado miembro en su capacidad como fiscal, juez u oficial de policía de competencias equivalentes (artículo 2 de la decisión del Consejo).

Eurojust puede concertar acuerdos con terceros países y organizaciones internacionales. Cada año se publica un informe sobre sus actividades de cooperación, y los últimos informes ponen de manifiesto la manera eficiente en que este organismo ha abordado los delitos relacionados con la identidad[246].

Puntos de contacto PC-OC

Se trata de una red de expertos creada en el marco del Comité de Expertos sobre el Funcionamiento de los convenios europeos sobre la cooperación en materia penal (PC-OC)[247], y se constituye a partir de puntos de contacto de los Estados miembros del Consejo de Europa. Estos puntos de contacto tienen acceso a un sitio web restringido y su labor es la misma que la que cumplen los puntos de contacto de la Red Judicial Europea. En muchos casos, la misma persona ocupa el cargo de punto de contacto en la Red Judicial Europea y en el PC-OC.

La Red de Personas de Contacto del Commonwealth (CNCP)

Esta Red fue creada en 2007 y está formada por 53 representantes de Estados miembros procedentes de diversas regiones (permite que los Estados miembros también formen parte de otras redes regionales). El objetivo de establecer una red con características tan informales era facilitar la cooperación judicial internacional en materia penal en lo que respecta a la extradición y la asistencia judicial recíproca, y ofrecer asesoramiento jurídico y práctico sobre la aplicación de los principales instrumentos en la materia[248]. Para acceder a esta red se necesita una contraseña y se realiza a través de un sitio web seguro.

---

[245] Véase la Decisión del Consejo 2002/187/JAI, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (la versión consolidada derivó de las enmiendas introducidas por las decisiones 2003/659/JAI y 2009/426/JAI).

[246] Los informes anuales y otros materiales pertinentes pueden consultarse en: http://www.eurojust.europa.eu/.

[247] Para detalles e información jurídica respecto de los Estados miembros en temas diversos, incluidos la extradición y la asistencia judicial recíproca, véase: http://www.coe.int/t/e/legal_affairs/legal_co-operation/Transnational_criminal_justice/.

[248] Para más información véase el Marco del CNCP, disponible en: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/1D0DC9F4-815A-4B0E-8B9D-718209E46D77_COMMONWEALTHNETWORKOFCONTACTPERSONS(CNCP).pdf.

La Red Iberoamericana de Cooperación Jurídica Internacional—IberRed

La Red Iberoamericana se estableció en 2004[249] y actualmente cuenta con 21 miembros procedentes de América Latina y 2 miembros europeos (España y Portugal). Esta Red cuenta con puntos de contacto establecidos entre las autoridades centrales de los Estados miembros. Para acceder a la lista de puntos de contacto es necesaria una contraseña. Por otro lado, el sitio web de la Red también ofrece al público información sobre la legislación interna de cada uno de sus países[250].

En la actualidad se está elaborando un memorando de entendimiento entre IberRed y la Red Judicial Europea[251], que podría considerarse un paso importante para facilitar futuras solicitudes de asistencia.

La Red Hemisférica de Intercambio de Información para la Asistencia Mutua en Materia Penal y Extradición de la Organización de los Estados Americanos[252]

Se trata de una red regional creada en el año 2000 por la Organización de los Estados Americanos (OEA) en virtud de la decisión adoptada en la Tercera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA). El objetivo de esta Red es mejorar la cooperación recíproca entre los Estados miembros. Para ello, fue diseñada sobre la base de un componente de tres niveles: un sitio público (una biblioteca en línea que contiene información sobre el sistema jurídico de cada Estado miembro); un sitio web privado, que contiene la información de contacto de los representantes de cada país; y un sistema de comunicación electrónica seguro que incluye un foro en línea para llevar a cabo debates.

Directorio en línea de Autoridades Nacionales Competentes de la UNODC[253]

El Directorio en línea de Autoridades Nacionales Competentes de la UNODC facilita el acceso a la información de contacto de las autoridades nacionales competentes designadas en virtud de la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas de 1988 y la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. El Directorio contiene información de contacto de casi 600 autoridades nacionales competentes autorizadas a recibir, responder y tramitar solicitudes de extradición, el traslado de personas condenadas, la asistencia judicial recíproca, el tráfico ilícito de narcóticos por mar, el tráfico de inmigrantes por mar y el tráfico de armas de fuego.

[249] Para más detalles, véase: http://www.iberred.org/presentacion/.
[250] Disponible en: http://www.iberred.org/legislaciones/.
[251] El texto del Memorando se puede consultar en: http://www.iberred.org/assets/Uploads/Memorandum-de- Entendimiento-IberRed-Eurojust.pdf.
[252] Para más información acerca de la historia de la Red, véase: http://www.oas.org/juridico/MLA/en/index.html.
[253] Véase: http://www.unodc.org/compauth/en/index.html.

A fin de facilitar la comunicación y la resolución de problemas entre las autoridades competentes a nivel interregional, el Directorio contiene información básica sobre:

- Los Estados que pertenecen a redes nacionales existentes;
- Los requisitos legales y de procedimiento para la concesión de las solicitudes;
- Los casos en que es posible valerse de la UNTOC como base jurídica de las solicitudes;
- Los enlaces a leyes nacionales y páginas web; y
- La indicación de las solicitudes que se pueden tramitar a través de Interpol.

El Directorio en línea se encuentra a disposición de las autoridades competentes y de los organismos gubernamentales que se hayan registrado como usuarios. Aquellos que lo hayan hecho también reciben una publicación actualizada del Directorio dos veces al año y pueden descargarlo en los formatos pdf y rtf.

Magistrados de enlace

La función de los oficiales de enlace en la aplicación de la ley ya se mencionó con anterioridad. En este contexto, cabe destacar que los magistrados de enlace desempeñan un papel de igual importancia en los temas de asistencia recíproca en materia penal. Con frecuencia, los magistrados de enlace facilitan el contacto entre las autoridades centrales pertinentes o el contacto directo entre las autoridades judiciales de los dos países interesados. Los magistrados de enlace participan directamente en la transmisión de cartas rogatorias y otras solicitudes de asistencia judicial recíproca, incluidas las relativas al fraude de identidad. También pueden participar en el intercambio de información sobre los sistemas jurídicos y datos estadísticos. Asimismo, pueden intervenir como intermediarios en los casos de extradiciones cuando el Estado requerido solicita información complementaria, pero también pueden facilitar otras solicitudes de extradición. Normalmente, los magistrados de enlace se intercambian entre los países sobre la base de acuerdos bilaterales. A nivel europeo, el instrumento de referencia está representado por la acción común 96/277/JAI, de 22 de abril de 1996, para la creación de un marco de intercambio de magistrados de enlace que permita mejorar la cooperación judicial entre los Estados miembros de la Unión Europea[254].

[254] Para más información, véase: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEX numdoc&lg=EN&numdoc=31996F0277&model=guichett.

V. CASOS

Este capítulo ofrece una visión general de los casos típicos de delitos relacionados con la identidad. Siguiendo con el propósito de esta guía de ofrecer acceso al tema en cuestión, especialmente para los expertos que investigan dichos delitos, cada caso brinda información estratégica y orientación práctica.

1. Primer caso: clonación de tarjetas de crédito

Enfoque del caso: carta rogatoria formulada durante la fase del juicio. Uso de tarjetas de crédito clonadas.

Los hechos del caso

Un ciudadano de un país A utiliza tarjetas de crédito clonadas en un país B. Ambos países son miembros de la Unión Europea. El citado ciudadano se encuentra bajo proceso judicial en el país B.

Antecedentes

La clonación de tarjetas de crédito es el acto de duplicar una tarjeta de crédito existente[255]. Esto puede llevarse a cabo, por ejemplo, a través de dispositivos que leen la información de la banda magnética y la transfieren a una tarjeta magnética virgen[256]. Con frecuencia la información de la tarjeta de crédito se obtiene a partir de procesos de pago legítimos, por ejemplo, cuando el titular paga con su tarjeta de crédito en una estación de servicio o restaurante[257]. A menudo, la clonación de tarjetas de crédito se realiza después de haberse llevado a cabo la técnica delictiva conocida como "skimming", término que se utiliza para describir un delito en el cual el delincuente manipula un cajero automático a fin de obtener información de tarjetas de crédito y números de identificación personal[258]. La información obtenida de los cajeros que fueron manipulados[259] se utiliza posteriormente para clonar las tarjetas originales y utilizarlas con fines delictivos. Las pérdidas estimadas que estas actividades

[255] Con respecto al fenómeno de la clonación en conexión con el delito relacionado con la identidad, véase: *Wall*, Cybercrime: The Transformation of Crime in the Information Age (Crime and Society), Polity Press, 2007, página 80.
[256] *Green*, Encyclopedia of Police Science, Rotlegde, 2006, 2ª edición., página 646.
[257] *Wall*, Cybercrime: The Transformation of Crime in the Information Age, *supra* núm. 255.
[258] Respecto al delito, véanse: *Grabosky*, The Internet, Technology, and Organized Crime, *Asian Journal of Criminology*, 2007, vol. 2, página 148; *Robertson*, Identity Theft Investigations, Kaplan Publishing, 2008, página 43.
[259] Comunicado de prensa del Departamento de Justicia, Distrito de Georgia del Norte, titulado "Indictment handed down in major ATM skimming operation", de 17 de febrero de 2009.

suponen para la economía podrían ascender a varios miles de millones de dólares de los Estados Unidos anuales[260]. Existen varias conexiones con grupos delictivos organizados[261].

Propósito de la solicitud

A fin de que el juez competente del país B tenga un conocimiento cabal del delincuente y pueda dictar la sentencia, necesita conocer sus antecedentes penales. Por tanto, el juez tiene que transmitir una solicitud al país A para averiguar si el delincuente tiene o no antecedentes penales y, en caso afirmativo, pedir que se le envíen las copias de las condenas. El fiscal competente del país B no ha solicitado esta información con anterioridad.

Estrategia

Identificación de los instrumentos aplicables

Lo primero es identificar el convenio que tiene aplicación. En este caso, dado que ambos países son miembros de la UE, tiene pertinencia el Convenio de 29 de mayo de 2000 relativo a la asistencia judicial en materia penal entre los Estados miembros[262], en particular el artículo 6, párrafo 8, inciso *b)*, tesis segunda. En el artículo 6, párrafo 8, se estipula que:

> Las solicitudes y comunicaciones siguientes se cursarán a través de las autoridades centrales:
>
> [...]
>
> *b)* las comunicaciones relativas a la información sobre condenas judiciales contempladas en el artículo 22 del Convenio europeo de asistencia judicial y en el artículo 43 del Tratado Benelux. No obstante, las solicitudes de copias de las condenas y medidas previstas en el artículo 4 del Protocolo Adicional del Convenio europeo de asistencia judicial[263] podrán dirigirse directamente a las autoridades competentes[264].

---

[260] Final Report of the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, 2006, capítulo 3, página 1, disponible en: www.scag.gov.au/.../SCAG/...scag...Final_Report.../MCLOC_ MCC_Chapter_3_Identity_Crime_-_Final_Report_-_PDF.pdf.

[261] *Montaque*, Fraud Prevention Techniques for Credit Card Fraud, Victoria, 2006, página 62; *Choo*/*Smith*, Criminal Exploitation of Online Systems by Organized Crime Groups, *Asian Journal of Criminology*, 2008, vol. 3, página 41; *Choo*, Organized crimes groups in Cyberspace: A typology, Trends in Organized Crime, *Asian Journal of Criminology*, 2008, vol. 11, página 277; Final Report of the Model Criminal Code Officers' Committee, *supra* núm. 260.

[262] Para más detalles, véase el informe explicativo del Convenio en: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229(02)&model=guichett. El texto del Convenio se puede consultar en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0712(01):EN:HTML.

[263] El Segundo Protocolo Adicional al Convenio Europeo sobre Cooperación Judicial en materia Penal de 2001, junto con el informe explicativo y la lista de ratificaciones y declaraciones pueden consultarse en línea en: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=07/03/2010&CL=ENG.

[264] El artículo 4 del Protocolo Adicional al Convenio del Consejo de Europa sometido a debate se refiere principalmente a la solicitud de antecedentes penales para los casos individuales. Esta situación es aplicable al presente caso. El artículo 4 modificó al artículo 22 del Convenio europeo sobre cooperación judicial en materia penal de 1959, el cual se puede consultar en línea en: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CM=8&DF=07/03/2010&CL=ENG. Recientemente, se adoptó la Decisión Marco del Consejo 2009/315/JAI, de 26 de febrero de 2009, relativa a la organización y el intercambio de información del registro de antecedentes penales entre los Estados miembros, la cual establece en el párrafo 10 de su preámbulo que las disposiciones de la presente Decisión Marco no deben afectar a la posibilidad de que disponen las autoridades judiciales de solicitarse y transmitirse directamente información del registro de antecedentes penales, de conformidad con los instrumentos anteriores aplicables.

Canales de comunicación

El segundo aspecto que es necesario considerar es el canal de comunicación a utilizar. En los casos de urgencia, la mejor solución disponible es el contacto directo entre la autoridad emisora del país B y la autoridad ejecutora del país A. En este sentido, puede recurrirse al Atlas Judicial Europeo en materia penal, el cual se encuentra disponible en línea[265]. Se recomienda seguir los pasos que allí se mencionan. Sin embargo, cabe destacar que este contacto directo no es obligatorio, y que la norma es que la transmisión se haga a través de los Ministerios de Justicia. Si no es posible establecer un contacto directo, existen canales alternativos que ayudarán al juez responsable a saber exactamente cómo actuar a fin de obtener la información que se necesita.

Si el juez competente en el país B no logra identificar a la autoridad judicial ejecutora en el país A y desea recurrir a la norma tradicional, la solicitud puede transmitirse al Ministerio de Justicia del país B, el cual la transmitirá al Ministerio de Justicia del país A.

Elegir entre la vía directa o a través de los Ministerios de Justicia u otra autoridad central pertinente depende también en la legislación interna de los Estados A y B y de la manera en que fueron aplicadas las disposiciones del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros, de 29 de mayo de 2000. En este sentido, se puede utilizar otra aplicación creada a nivel de la UE, concretamente la *Fiche Belge*, que contiene referencias a la legislación de los Estados miembros sobre antecedentes penales[266].

Como último recurso, en caso de que el juez competente no logre identificar a la autoridad judicial ejecutora, pero aún así desea recurrir al contacto directo y tiene dificultades con el manejo de herramientas electrónicas, puede transmitir la solicitud a uno de los puntos de contacto de la Red Judicial Europea (RJE)[267]. A través de esta Red, el juez competente puede incluso solicitar información sobre el sistema judicial del Estado ejecutante, como por ejemplo si este acepta el contacto directo entre las autoridades judiciales.

Medios de comunicación

Respecto de los medios de comunicación, si la solicitud es de carácter urgente se recomienda el uso de medios expeditivos tales como el fax o el correo electrónico. En caso de que no sea posible, es necesario hacer una evaluación clara al respecto y, en caso en que el nivel de prioridad de la solicitud sea normal, también se aceptará el envío por correo postal. Es probable que la autoridad judicial emisora necesite recurrir a medios de comunicación expeditivos cuando una solicitud sea formulada durante el juicio.

Recomendación práctica

En el momento de formularse una solicitud, es necesario incluir específicamente un resumen de los hechos y una justificación de la solicitud, así como las disposiciones legales aplicables en el país B.

[265] Consultar: http://www.ejn-crimjust.europa.eu/atlas_advanced.aspx.
[266] Véase: http://www.ejcrimjust.europa.eu/fiches_belges_result.aspx?measure=405&lang=AT&other.
[267] Para obtener información acerca de la Red Judicial Europea, véase: http://www.ejn-crimjust.europa.eu/.

2. Segundo caso: las actividades de "peska"

Enfoque del caso: carta rogatoria formulada durante la fase previa al juicio, delincuencia transnacional organizada.

Los hechos del caso

Un grupo delictivo organizado de un país A envía correos electrónicos a clientes de la plataforma de subastas de eBay con el propósito de obtener datos de las tarjetas de crédito de nacionales de diversos países. Los datos obtenidos se utilizan posteriormente para comprar o alquilar nombres de dominios de Internet y promover sitios web de servicios de envío a domicilio inexistentes. Durante este proceso, se alentó a los clientes a que utilizaran estos sitios web falsos que ofrecían mayor autenticidad a las transacciones realizadas a través de eBay. En la práctica, nunca se llegó a concretar la entrega de los productos que los clientes en los países A, B, C y D habían adquirido.

Los países A y B están ubicados en distintos continentes. No existe ningún tratado bilateral vigente entre los dos países. Ambos países son parte de la UNTOC.

Propósito de la solicitud

El fiscal del país A debe enviar solicitudes similares a los países cuyos ciudadanos fueron víctimas, incluido el país B. La solicitud al país B hace referencia a la identificación de posibles víctimas. El fiscal también solicita al país B que pregunte a las posibles víctimas si desean presentar una denuncia y, en caso afirmativo, que le sea enviada, así como la información que pudieran tener acerca de los delincuentes.

Estrategia

Identificar el convenio aplicable

El primer paso para la elaboración de la solicitud de asistencia judicial recíproca es identificar el instrumento jurídico que se aplica. En este caso, debido a que no existe ni un tratado bilateral entre los dos Estados ni ningún otro instrumento bilateral en vigor, la UNTOC resulta pertinente.

> **Artículo 18, párrafo 7, de la UNTOC**
>
> Los párrafos 9 a 29 del presente artículo se aplicarán a las solicitudes que se formulen con arreglo al presente artículo siempre que no medie entre los Estados Parte interesados un tratado de asistencia judicial recíproca. Cuando esos Estados Parte estén vinculados por un tratado de esa índole se aplicarán las disposiciones correspondientes de dicho tratado, salvo que los Estados Parte convengan en aplicar, en su lugar, los párrafos 9 a 29 del presente artículo. Se insta encarecidamente a los Estados Parte a que apliquen estos párrafos si facilitan la cooperación.

En este sentido, antes de formular la solicitud es preciso verificar si las condiciones que se estipulan en el artículo 18, párrafo 1, se cumplen en el país A. Más específicamente, es especialmente necesario verificar si el fraude o falsificación informáticos se consideran delitos graves en virtud de la legislación interna del país A[268].

Canales de comunicación

Se recomienda consultar los directorios de los que se dispone (directorios en línea o su versión impresa) a fin de poder determinar cuál es el canal de comunicación aplicable y si es posible establecer un contacto directo a través de los ministerios de justicia (u otras autoridades centrales, por ejemplo, la oficina del fiscal). Si el país B no permite un contacto directo con su autoridad central, el fiscal del país A necesitará enviar la solicitud a través de la vía diplomática.

Medios de comunicación

En general, la UNTOC permite el uso de cualquier medio de comunicación, incluidos los medios expeditivos. Por tanto, se recomienda que el envío se realice por fax si la solicitud es de carácter urgente y si el país requerido lo permite. De no ser así, se recurrirá al envío tradicional a través del correo postal.

El contenido de la solicitud

En el momento de preparar la solicitud se recomienda utilizar el Programa para Redactar Solicitudes de Asistencia Judicial Recíproca[269] y, si esto no fuera posible o si la autoridad judicial emisora decidiera otra cosa, se deberá tomar en consideración el artículo 18, párrafo 15, de la UNTOC.

Artículo 18, párrafo 15, de la UNTOC

Toda solicitud de asistencia judicial recíproca contendrá lo siguiente:

a) La identidad de la autoridad que hace la solicitud;

b) El objeto y la índole de las investigaciones, los procesos o las actuaciones judiciales a que se refiere la solicitud y el nombre y las funciones de la autoridad encargada de efectuar dichas investigaciones, procesos o actuaciones;

c) Un resumen de los hechos pertinentes, salvo cuando se trate de solicitudes de presentación de documentos judiciales;

d) Una descripción de la asistencia solicitada y pormenores sobre cualquier procedimiento particular que el Estado Parte requirente desee que se aplique;

e) De ser posible, la identidad, ubicación y nacionalidad de toda persona interesada; y

f) La finalidad para la que se solicita la prueba, información o actuación.

[268] Para una interpretación del artículo 18, párrafo 1, véase: Legislative Guides: United Nations Convention Against Transnational Organized Crime, *supra* núm. 139, página 230 y ss. Las decisiones que se tomaron en la reunión del Grupo de trabajo sobre cooperación internacional se encuentran disponibles en: http://www.unodc.org/unodc/en/treaties/working-group-on-international-cooperation.html.

[269] La información sobre esta herramienta y su versión para descargar se encuentran disponibles en: http://www.unodc.org/mla/.

Recomendación práctica

A fin de destacar el carácter transnacional y lograr una respuesta más rápida del Estado ejecutante, es importante poner de relieve el hecho de que existen posibles víctimas en más de un país, nombrar a esos países, revelar el número aproximado de víctimas y mencionar el total estimado del daño ocasionado (esto último podría ser relevante para el país B, principalmente si representa el sistema de derecho común que se guía por el principio de proporcionalidad).

Otro aspecto importante es el idioma en el cual ha de transmitirse la solicitud. La autoridad judicial emisora necesita comprobar la declaración que el país B hizo al respecto y, en este sentido, sería de gran utilidad recurrir al directorio de autoridades nacionales competentes en línea o en versión impresa.

3. Tercer caso: fraude en las plataformas de subastas

Enfoque del caso: carta rogatoria formulada durante la fase previa al juicio, delito no organizado, no existe un acuerdo de asistencia recíproca en vigor.

Los hechos del caso

Dos delincuentes que operan en el país A crean un sitio web que se asemeja al sitio web de una conocida plataforma de subastas en línea. Además, los delincuentes envían correos electrónicos que contienen un documento adjunto con un código corrupto que instala software malicioso en la computadora de la víctima en el país B en el momento en que esta abre el adjunto. Los delincuentes utilizan la información bancaria que obtuvieron de la computadora en el país B para iniciar una subasta en la que ofrecen productos que no existen. Clientes en el país C compran estos productos y transfieren el dinero a través de pagos electrónicos. Las actividades delictivas se llevan a cabo desde direcciones IP que se originaron en el país A.

Los países A, B y C están ubicados en distintos continentes. No existe ningún tratado bilateral vigente entre los países. Todos ellos son parte de la UNTOC, pero no del Convenio sobre el delito cibernético.

Antecedentes

Las subastas en línea son en la actualidad uno de los servicios de comercio electrónico más populares. En 2006, se vendieron en eBay, el mercado de subastas en línea más grande del mundo, productos por un valor de más de 20.000 millones de dólares de los Estados Unidos[270]. Los compradores pueden acceder a productos variados o exclusivos desde cualquier parte del mundo. Los vendedores gozan de un público a nivel mundial, una demanda estimulante y un impulso de los precios. Los delincuentes se aprovechan de la ausencia del

[270] Véase: http://www.ebay.com.

contacto personal entre vendedores y compradores[271]. La dificultad para distinguir entre los usuarios auténticos y los que no lo son ha situado al fraude de subasta entre los delitos cibernéticos más populares[272]. Los dos timos más comunes incluyen[273]:

- Ofrecer a la venta productos que no existen y pedir a los compradores que paguen antes de la entrega[274];
- Comprar productos y solicitar servicio de entrega, sin intención de pagar por ello.

En respuesta a esto, los proveedores de servicios de subasta crearon mecanismos de protección tales como el sistema para recoger observaciones y comentarios. Después de cada transacción, los compradores y vendedores dan a conocer sus opiniones que puede que sean utilizadas por otros usuarios[275] como información neutra acerca de la fiabilidad de vendedores o compradores. Sin embargo, los delincuentes han burlado esta protección utilizando cuentas de terceros[276]. A través del timo llamado "apropiación de una cuenta"[277], los delincuentes tratan de obtener nombres y contraseñas de usuarios auténticos para comprar o vender productos fraudulentos, lo que hace que su identificación sea más difícil.

Propósito de la solicitud

Con frecuencia los proveedores de Internet, tales como los proveedores de correo electrónico, tiendas en línea y plataformas de subastas, conservan registros de acceso a sus servicios en los llamados archivos de registro. Para poder identificar a los delincuentes que actúan en el país A, el fiscal en el país C necesita pedir el envío de los archivos de registro del país B a fin de identificar el usuario de Internet que utilizó la dirección IP para acceder a la cuenta de la plataforma de subastas. Es necesario considerar medidas provisionales para garantizar que no se eliminen las pruebas antes de ejecutar la solicitud.

Recomendación práctica

En la actualidad, el delito relacionado con la identidad entraña en gran medida pruebas digitales. Reunir dichas pruebas presenta desafíos únicos. Uno de los más importantes es el hecho de que los datos que pudieran ser relevantes para una investigación podrían eliminarse automáticamente en el plazo de unos días si no resulta relevante para los fines de facturación. Por tanto, es prioritario brindar una respuesta inmediata y pedir que se tomen medidas provisionales.

---

[271] Véase: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, vol. 6, issue 1.

[272] El Centro de denuncias de delitos en Internet de los Estados Unidos (IC3) (una alianza entre el FBI y el Centro nacional contra la delincuencia de guante blanco) informó de que alrededor del 45% de las denuncias hacían referencia al fraude de subastas. Véase: "IC3 Internet Crime Report 2006", disponible en: http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

[273] "Law Enforcement Efforts to combat Internet Auction Fraud", Federal Trade Commission, 2000, página 1, disponible en: http://www.ftc.gov/bcp/reports/int-auction.pdf.

[274] Véase: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on Aging, 2004, página 7, disponible en: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[275] Para más información, véase, por ejemplo: http://pages.ebay.com/help/feedback/feedback.html.

[276] Respecto a la sanción para los apropiadores de una cuenta, véase: *Gercke*, Multimedia und Recht 2004, issue 5, página XIV.

[277] Véase: Putting an End to Account-Hijacking Identity Theft", Federal Deposit Insurance Corporation, 2004, disponible en: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

Estrategia e identificación de otros instrumentos aplicables

El primer paso es identificar los instrumentos aplicables para la asistencia recíproca. Aunque los países B y C son parte de la UNTOC y esta Convención ofrece un amplio rango de formas de cooperación internacional, la misma no tiene aplicación en el caso en cuestión. Sobre la base de lo dispuesto en el artículo 3, párrafo 1, las disposiciones de la Convención se aplican si el delito entraña la participación de un grupo delictivo organizado. El artículo 2 define "grupo delictivo organizado" como un grupo estructurado de tres o más personas, lo cual no se aplica al caso mencionado.

> **Artículo 2 de la UNTOC**
>
> *Definiciones*
>
> Para los fines de la presente Convención:
>
> *a)* Por "grupo delictivo organizado" se entenderá un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material;

> **Artículo 3 de la UNTOC**
>
> *Ámbito de aplicación*
>
> 1. A menos que contenga una disposición en contrario, la presente Convención se aplicará a la prevención, la investigación y el enjuiciamiento de:
>
> *a)* Los delitos tipificados con arreglo a los artículos 5, 6, 8 y 23 de la presente Convención; y
>
> *b)* Los delitos graves que se definen en el artículo 2 de la presente Convención;

Debido a la ausencia de convenciones internacionales aplicables, y a la falta de acuerdos de asistencia recíproca, es necesario transmitir la solicitud utilizando las normas de cortesía internacional, y sobre la base del principio de reciprocidad[278].

Canales y medios de comunicación

Basado en las normas de cortesía internacional, el Estado requirente debe enviar una solicitud al Estado ejecutor a través de la vía diplomática. En la práctica esto significa que una autoridad judicial en el país C deberá enviar una carta rogatoria a su Ministerio de Justicia, el cual transmitirá la solicitud al Ministerio de Asuntos Exteriores en dicho país. Posteriormente, traspasará la solicitud al Ministerio de Asuntos Exteriores del país B, el cual la enviará a su Ministerio de Justicia. Finalmente, este último transmitirá la carta rogatoria a la autoridad competente para que ejecute la solicitud.

[278] Véanse: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, *AGORA International Journal of Juridical Science*, 2008, página 160 y ss.; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, página 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, página 119.

Recomendación práctica

En comparación con el contacto o contactos directos a través de las autoridades centrales, la transmisión de las solicitudes a través de la vía diplomática lleva mucho tiempo y podría causar grandes dificultades para las tareas de investigación, en particular en lo que respecta a los casos urgentes. Por tanto, es probable que las solicitudes de medidas provisionales no sean tan eficaces como podrían serlo a través de otros canales.

Por consiguiente, la autoridad requirente debería comprobar si el país B es parte de la UNTOC, si se han presentado solicitudes previas en ese país y si normalmente acepta que se utilicen medios de comunicación expeditivos. En ese caso, se podría enviar una solicitud informal al punto de contacto responsable de las solicitudes para averiguar si las solicitudes transmitidas utilizando las normas de cortesía internacional basadas en la reciprocidad pueden enviarse por anticipado por correo electrónico o fax junto con los documentos originales certificados, seguido del envío por la vía diplomática. Algunos países aceptan este procedimiento.

Contenido de la solicitud

Es necesario que la solicitud enviada al país B incluya cierta información clave. Dado que tanto el Estado requirente como el ejecutor son parte de la UNTOC, la normativa relativa en la Convención (artículo 18) puede, a pesar del hecho de que la Convención no es aplicable, ser utilizada como guía.

Artículo 18, párrafo 15, de la UNTOC

Toda solicitud de asistencia judicial recíproca contendrá lo siguiente:

a) La identidad de la autoridad que hace la solicitud;

b) El objeto y la índole de las investigaciones, los procesos o las actuaciones judiciales a que se refiere la solicitud y el nombre y las funciones de la autoridad encargada de efectuar dichas investigaciones, procesos o actuaciones;

c) Un resumen de los hechos pertinentes, salvo cuando se trate de solicitudes de presentación de documentos judiciales;

d) Una descripción de la asistencia solicitada y pormenores sobre cualquier procedimiento particular que el Estado Parte requirente desee que se aplique;

e) De ser posible, la identidad, ubicación y nacionalidad de toda persona interesada; y

f) La finalidad para la que se solicita la prueba, información o actuación.

Seguir los procedimientos de la UNTOC garantizará que la solicitud coincida con los procedimientos que ya fueron aplicados a la legislación interna del país A y llevados a la práctica por las autoridades competentes.

Recomendación práctica

En caso de duda respecto de los procedimientos a seguir, podría ser útil ponerse en contacto con el Estado ejecutor previo al envío de la solicitud formal, o averiguar si existen requisitos específicos que es necesario considerar. En este sentido, el directorio en línea de las autoridades competentes nacionales podría ser de gran ayuda.

Seguimiento

Una vez el país B presenta la información, las autoridades del país C necesitan llevar a cabo gestiones adicionales para identificar a los delincuentes. Sobre la base de la información de la dirección IP y de los archivos de registro proporcionada por el país B, es necesario presentar otra solicitud, en esta ocasión al país A.

4. Caso cuarto: apropiación de una cuenta

Enfoque del caso: carta rogatoria formulada durante la fase previa al juicio, delito no organizado.

Los hechos del caso

La víctima se encuentra en el país A y tiene una cuenta de correo electrónico con una empresa ubicada en el país B. Un delincuente accede ilegalmente al servidor de la víctima y se apropia de su cuenta de correo electrónico con el objetivo de enviar correos haciéndose pasar por ella. Los países A y B están ubicados en distintos continentes. Los países no son parte del Convenio del Consejo de Europa sobre el delito cibernético[279]. En su lugar se aplica un tratado bilateral.

Antecedentes

La apropiación de una cuenta es una expresión que se utiliza para describir el uso indebido de la cuenta de otra persona[280]. Se lo considera uno de los típicos delitos de identidad[281]. Los delincuentes tienen como objetivo las cuentas de ahorro y de correo electrónico, si bien también utilizan cuentas para operar en plataformas y redes sociales[282]. Mediante la apropiación de una cuenta, los delincuentes pueden utilizar la identidad de la víctima, por ejemplo, enviando correos electrónicas desde su cuenta o haciendo transferencias de dinero desde su cuenta bancaria. Los delincuentes que operan de esta manera se valen del hecho de que el acceso a la cuenta proporciona legitimidad a la transacción. Asimismo, pueden utilizar la apropiación de cuentas a fin de evadir las medidas de protección de los proveedores para impedir el uso fraudulento de servicios. Un ejemplo es la ejecución de sistemas para recoger observaciones y comentarios en las plataformas de subastas. Para evitar que los usuarios abusen del servicio, algunas plataformas de subastas permiten a los clientes realizar una evaluación de sus homólogos. Después de cada transacción,

[279] Para más detalles sobre el Convenio, véanse: *Sofaer*, Toward an International Convention on Cybercrime, in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, disponible en: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, página 140 y ss.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, *ibid.*, página 7 y ss.; *Jones*, The Council of Europe Convention on Cybercrime; *Broadhurst*, Development in the global law enforcement of cyber-crime, página 408 y ss.

[280] *Biegelman*, Identity Theft Handbook, Detection, Prevention and Security, John Wiley & Sons. Inc, 2009, página 29.

[281] *Hoofnagle*, Identity Theft: Making the Known Unknowns Known, *Harvard Journal of Law & Technology*, 2007, página 103.

[282] *Ferretti*, The Law and Consumer Credit Information in the European Community, The Regulation of Credit Information Systems, página 26. *Hoofnagle*, Identity Theft, *supra*.

compradores y vendedores hacen públicos sus comentarios para que otros usuarios puedan enterarse[283] de la fiabilidad de los vendedores o compradores. Esto dificulta que los delincuentes utilicen plataformas de subastas para cometer delitos. Sin embargo, pueden eludir esta protección utilizando cuentas de terceros[284]. Mediante la apropiación de una cuenta[285], los delincuentes tratan de obtener nombres y contraseñas de usuarios legítimos para realizar compras o ventas fraudulentas de bienes, lo que hace que su identificación sea más difícil.

Propósito de la solicitud

Una vez la víctima denuncia la apropiación de su cuenta, las autoridades locales del país A necesitan acceder a las pruebas que les permitan localizar al delincuente. En este contexto, la información de acceso del proveedor de correo electrónico es particularmente importante. Los proveedores con frecuencia conservan los registros de las direcciones IP que los clientes utilizan para acceder a sus cuentas. Obtener la dirección IP permitiría a las autoridades locales en el país A identificar al delincuente. En lo que respecta al hecho de que el principio fundamental de la soberanía nacional no permite llevar a cabo investigaciones dentro del territorio de otro país sin el permiso de las autoridades locales[286], los investigadores en el país A no pueden simplemente recoger pruebas a distancia. El hecho de que muchos servicios de Internet, como las cuentas de correo electrónico o las redes sociales, se ofrecen a nivel mundial, pone de relieve la importancia de que exista una estrecha cooperación entre los países que participan en la investigación[287].

Estrategia

En primer lugar es necesario identificar los instrumentos aplicables. Debido a que no existe ninguna indicación acerca de cuántos delincuentes participaron en el delito, la UNTOC no sería aplicable ya que la definición de delincuencia organizada que figura en el inciso *a)* del artículo 2 requiere la participación de un grupo de tres o más personas. Como el delito se comete utilizando tecnologías de la información y requieren el acceso ilegal a un sistema informático, podría considerarse en general la aplicación de los instrumentos contenidos en el Convenio del Consejo de Europa sobre el delito cibernético[288]. En el presente caso, dado que los países A y B no son parte de dicho Convenio tampoco son aplicables los medios de cooperación internacional mencionados en el mismo.

---

[283] Para más información, véase: http://pages.ebay.com/help/feedback/feedback.html.

[284] Respecto a la sanción para los apropiadores de una cuenta, véase: *Gercke*, *supra* núm. 276, página XIV.

[285] Véase: "Putting an End to Account-Hijacking Identity Theft", *supra* núm. 277.

[286] Con respecto al principio de soberanía nacional, véanse: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, *supra* núm. 25; *Martinez*, National Sovereignty and International Organizations, 1996; *Riegler*, Nation Building Between National Sovereignty and International Intervention, 2005.

[287] En lo que respecta a la necesidad de cooperación internacional en la lucha contra el delito cibernético, véase: *Putnam/Elliott*, "International Responses to Cyber Crime", *supra* núm. 25, página 35 y ss.

[288] Para más detalles sobre el Convenio, véanse: *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, página 140 y ss.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, página 7 y ss.; *Jones*, The Council of Europe Convention on Cybercrime; *Broadhurst*, Development in the global law enforcement…, página 408 y ss.

Tratado bilateral[289]

En las investigaciones de este tipo, la atención se centrará en la conservación de las pruebas. A diferencia del Convenio sobre el delito cibernético, que permite la asistencia recíproca respecto de las medidas provisionales[290], los acuerdos de asistencia recíproca tales como los que se consideran en el Tratado modelo de asistencia recíproca en asuntos penales, no abarcan tales medidas provisionales[291]. Existen varios acuerdos recientes que contienen medidas provisionales además de las tradicionales.

La solicitud debe ser transmitida al punto de contacto designado. Siguiendo las disposiciones establecidas en el artículo 3 del Tratado modelo de asistencia recíproca en asuntos penales, la solicitud debe enviarse a la autoridad central, a menos que los países consideren la comunicación directa. Es necesario que la solicitud incluya la información tal como se especifica en el acuerdo (véase, por ejemplo, el artículo 5 del Tratado modelo de asistencia recíproca en asuntos penales).

Artículo 5 del Tratado modelo de asistencia recíproca en asuntos penales

Contenido de la solicitud

1. En la solicitud de asistencia deberán constar:

   a) La identidad del órgano que formula la solicitud y de la autoridad competente que está incoando la investigación o las actuaciones judiciales relacionadas con la solicitud;

   b) El objetivo de la solicitud y una somera explicación de la asistencia que se pide;

   c) Una descripción de los hechos presuntamente constitutivos de delito y una relación o un texto de las leyes pertinentes, salvo en el caso de que se solicite la entrega de documentos;

   d) El nombre y la dirección del destinatario, cuando así proceda;

   e) Los fundamentos y pormenores de todo procedimiento o trámite concreto que el Estado requirente desee que se siga, con indicación de si se exigen declaraciones o testimonios jurados o solemnes;

   f) Indicación del plazo deseado para dar cumplimiento a la solicitud;

   g) Cualquier otra información necesaria para que se dé curso adecuado a la solicitud.

Los medios de comunicación dependen de lo que se especifique en el acuerdo. Si no se menciona explícitamente la utilización de medios expeditivos, se considerarán en general los métodos de transmisión tradicionales. Asimismo, se deberá prestar especial atención a los requisitos relacionados con el idioma de la solicitud[292].

[289] La sección que sigue a continuación se basa en el Tratado modelo de asistencia recíproca en asuntos penales, aprobado por la resolución 45/117 de la Asamblea General, y posteriormente modificado por la resolución 53/112 de la Asamblea General.

[290] Véase el artículo 29 del Convenio sobre el delito cibernético, *supra* núm. 117.

[291] Véase el artículo 1 del Tratado modelo de asistencia recíproca en asuntos penales.

[292] Véase, por ejemplo, el artículo 5, párrafo 3, del Tratado modelo de asistencia recíproca en asuntos penales.

5. Quinto caso: skimming

Enfoque del caso: grupo delictivo organizado transnacional, carta rogatoria formulada durante la fase previa al juicio, instrumentos de la UNTOC, la Unión Europea y el Consejo de Europa.

Los hechos del caso

Un grupo delictivo organizado del país A instala dispositivos para llevar a cabo actividades de skimming en cajeros automáticos ubicados en los países B y C. Los delincuentes manipulan los teclados y las ranuras donde se insertan las tarjetas e instalan cámaras microscópicas para obtener información de tarjetas de crédito y números de identificación personal (PIN). Posteriormente, con los datos obtenidos realizan clonaciones de las tarjetas de crédito y las utilizan en transacciones fraudulentas.

Los países A, B y C son europeos. Todos ellos son parte de la UNTOC y los países A y B son miembros de la Unión Europea. El país A y el C son miembros del Consejo de Europa.

Antecedentes

En general, el término "skimming" se emplea para describir un delito en el que los delincuentes manipulan un cajero automático a fin de obtener información de tarjetas de crédito y números de identificación personal[293]. Se trata de un delito que se lleva a cabo en dos etapas. En la primera, los delincuentes se hacen con la información de la tarjeta de crédito instalando dispositivos en el cajero automático. Por lo general, los dispositivos se esconden dentro de la ranura donde se introduce la tarjeta en el cajero automático, y están diseñados para que parezcan que son parte del mismo[294]. El dispositivo graba y almacena los datos de todas las tarjetas que se insertan. Para obtener el número de identificación personal, los delincuentes alteran el teclado o instalan una cámara de microorificio para grabar a las víctimas cuando ingresan su número PIN[295]. En la segunda etapa, los delincuentes utilizan la información que obtuvieron para clonar tarjetas de crédito y luego usarlas. Se calcula que esta actividad ocasiona pérdidas económicas anuales que ascienden a varios miles de millones de dólares de los Estados Unidos.[296]. Existen varias conexiones con grupos delictivos organizados[297].

[293] Con respecto a este delito, véase: *Grabosky*, The Internet, Technology, and Organized Crime, *supra* núm. 261, página 43.

[294] Comunicado de prensa del Departamento de Justicia, Distrito de Georgia del Norte, titulado "Indictment handed down in major ATM skimming operation", de 17 de febrero de 2009.

[295] ATM Crime, ENISA (Agencia Europea de Seguridad de las Redes y de la Información), 2009, página 14, disponible en: http://www.scribd.com/doc/19636432/Enisa-Atm-Crime.

[296] Final Report of the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, *supra* núm. 260.

[297] *Montaque*, Fraud Prevention Techniques for Credit Card Fraud, supra núm. 261, página 62; *Choo*/*Smith*, Criminal Exploitation of Online Systems by Organized Crime Groups, página 41; *Choo*, Organized crimes groups in Cyberspace…, *supra* núm. 261, página 277; Final Report of the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, *supra* núm. 260.

Recomendación práctica

La participación de un grupo delictivo organizado reviste particular importancia para que se pueda aplicar la UNTOC.

Propósito de la solicitud

El fiscal en el país A solicita la siguiente información: los nombres de los bancos emisores de las tarjetas de crédito que fueron clonadas, los nombres de los titulares de las tarjetas de crédito y la cantidad total a que se eleva el daño causado a las víctimas. El fiscal envía la solicitud con propósitos similares a los países B y C a fin de obtener información.

Estrategia

Lo primero que se debe hacer es identificar los instrumentos internacionales aplicables. Dado que este caso presenta elementos de crimen organizado, es necesario considerar a la UNTOC. Sin embargo, en relación con el artículo 18, párrafos 6 y 7, es necesario investigar en primer lugar si son aplicables otros tratados que rigen la asistencia judicial recíproca. Para los propósitos de esta investigación, dichos tratados son particularmente pertinentes dado que los tres países se encuentran en la misma región.

Artículo 18 de la UNTOC

Asistencia judicial recíproca

[…]

6. Lo dispuesto en el presente artículo no afectará a las obligaciones dimanantes de otros tratados bilaterales o multilaterales vigentes o futuros que rijan, total o parcialmente, la asistencia judicial recíproca.

7. Los párrafos 9 a 29 del presente artículo se aplicarán a las solicitudes que se formulen con arreglo al presente artículo siempre que no medie entre los Estados Parte interesados un tratado de asistencia judicial recíproca. Cuando esos Estados Parte estén vinculados por un tratado de esa índole se aplicarán las disposiciones correspondientes de dicho tratado, salvo que los Estados Parte convengan en aplicar, en su lugar, los párrafos 9 a 29 del presente artículo. Se insta encarecidamente a los Estados Parte a que apliquen estos párrafos si facilitan la cooperación.

Identificación de otros instrumentos aplicables

Como los países A y B son miembros de la Unión Europea, resulta pertinente el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (2000)[298], a menos que uno de los países involucrados aún no lo haya ratificado[299].

[298] Convenio celebrado por el Consejo de conformidad con el artículo 34 del Tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, Diario Oficial 197 de 12 de julio de 2000, páginas 3 a 23.

[299] Para una reseña general del Convenio, véase: *Bantekas/Nash*, International Criminal Law, *supra* núm. 57, página 237 y ss.

Tras cuatro años de intensas negociaciones[300], el Convenio se finalizó en 2000 y entró en vigor en 2005, reemplazando a la Decisión Marco sobre los equipos conjuntos de investigación[301] y complementando a los instrumentos del Consejo de Europa[302].

En lo que respecta al país C, debe tenerse en cuenta que tanto el país A como el C son miembros del Consejo de Europa. En consecuencia, es aplicable el Convenio europeo sobre cooperación judicial en materia penal de 1959[303], que fue ratificado por 47 Estados miembros del Consejo de Europa e Israel en su calidad de Estado no miembro[304]. En lo que respecta a los medios de comunicación, es importante corroborar si los países A y C también son parte del Segundo Protocolo Adicional al Convenio Europeo sobre Cooperación Judicial en materia Penal de 2001[305]. El Protocolo, que a diciembre de 2009 había sido ratificado por 19 países, contiene una normativa especial respecto de los canales de comunicación[306].

Recomendación práctica

La fase de ratificación de los instrumentos del Consejo de Europa, el texto de los instrumentos y los informes explicativos se encuentran disponibles en línea en: http://conventions.coe.int.

Canales de comunicación

La elección de los canales de comunicación reviste especial importancia para establecer un contacto inicial. Dependiendo de cual sea el instrumento aplicable, los canales de comunicación que utilice el país A para comunicarse con los países B y C podrían ser diferentes.

Respecto de la comunicación entre los países A y B, la misma podría llevarse a cabo a través del contacto directo entre las oficinas de los fiscales en los dos países, de conformidad con el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea[307].

El contacto a través de otras autoridades podría resultar necesario si uno de los países ha declarado que continuará empleando la comunicación por medio de la autoridad central. En los casos urgentes, el Convenio también permite que las transmisiones se hagan por intermedio de Interpol[308]. Dado que el Convenio únicamente complementa instrumentos tales como los del Consejo de Europa[309], podrían ser pertinentes otros instrumentos jurídicos para aquellos Estados miembros de la UE que no hayan ratificado el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea.

---

[300] *Maklu-Uitgevers in De Ruyver/Bermeulen/Vander Beken*, Combating Transnational Organized Crime, 2002, página 224.
[301] Decisión Marco 2002/465/JAI.
[302] *Kronenberger/Kapteyn* (ed.), The European Union and the International Legal Order—Discord or Harmony, Asociación Europea de Libre Intercambio, 2001, página 547.
[303] Convenio europeo sobre cooperación judicial en materia penal (STE 30).
[304] El estado de ratificación del Convenio del Consejo de Europa se encuentra disponible en: http://conventions.coe.int.
[305] Segundo Protocolo Adicional al Convenio europeo sobre cooperación judicial en materia penal (STE 182).
[306] Véase, en particular, el artículo 4.
[307] Véase el artículo 6 para más detalles.
[308] *Ibid*.
[309] *Kronenberger/Kapteyn* (*ed*.), The European Union and the International Legal Order—Discord or Harmony, European Free Trade Association, 2001.

Artículo 6 del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea de 2000

Transmisión de solicitudes de asistencia judicial

1. Las solicitudes de asistencia judicial, así como los intercambios espontáneos de información a los que se hace referencia en el artículo 7, se efectuarán por escrito, o por cualesquiera medios que puedan dejar constancia escrita en condiciones que permitan al Estado miembro receptor establecer su autenticidad. Dichas solicitudes se efectuarán directamente entre las autoridades judiciales que tengan competencia jurisdiccional para formularlas y ejecutarlas, y se responderán del mismo modo, salvo que en el presente artículo se disponga lo contrario. Toda denuncia cursada por un Estado miembro cuyo objeto sea incoar un proceso ante los tribunales de otro Estado miembro con arreglo a lo dispuesto en el artículo 21 del Convenio europeo de asistencia judicial y en el artículo 42 del Tratado Benelux podrá transmitirse mediante comunicación directa entre las autoridades judiciales competentes.

2. El apartado 1 se entiende sin perjuicio de la facultad de envío de las solicitudes y de las respuestas en casos particulares:

a) de una autoridad central de un Estado miembro a una autoridad central de otro Estado miembro;

b) de una autoridad judicial de un Estado miembro a una autoridad central de otro Estado miembro.

[...]

4. En caso de urgencia, las solicitudes de asistencia judicial podrán transmitirse por conducto de la Organización Internacional de Policía Criminal (INTERPOL) o de cualquier órgano competente según las disposiciones adoptadas en virtud del Tratado de la Unión Europea.

[...]

Recomendación práctica

No existe ninguna aplicación en línea que pueda utilizarse para identificar la autoridad competente en los países europeos[310].

El Convenio arriba mencionado no puede utilizarse para escoger los canales de comunicación entre los países A y C ya que no son miembros de la Unión Europea. Sin embargo, dado que ambos países son miembros del Consejo de Europa, los canales de comunicación se identificarán teniendo en cuenta el Convenio europeo del Consejo de Europa sobre cooperación judicial en materia penal (1959). De conformidad con el artículo 15 del Convenio, la solicitud debe ser transmitida a la autoridad central designada, en este caso, el Ministerio de Justicia. El contacto directo con la autoridad judicial en el país C será posible únicamente en los casos que revistan urgencia. No obstante, incluso en esos casos, la respuesta aún deberá provenir de la autoridad central.

[310] Véase en: http://www.ejn-crimjust.europa.eu/atlas_advanced.aspx.

Artículo 15 de la Convención sobre asistencia judicial recíproca de 1959

Las comisiones rogatorias mencionadas en los artículos 3, 4 y 5, así como las solicitudes a que hace referencia el artículo 11, serán cursadas por el Ministerio de Justicia de la Parte requirente al Ministerio de Justicia de la Parte requerida y devueltas por la misma vía. En caso de urgencia, las citadas comisiones rogatorias podrán cursarse directamente por las autoridades judiciales de la Parte requirente a las autoridades judiciales de la Parte requerida. Serán devueltas acompañadas de los documentos relativos a la ejecución por la vía estipulada en el párrafo 1 del presente artículo.

El contacto directo entre las autoridades judiciales en los casos que no son urgentes es posible únicamente si ambos países son parte del Segundo Protocolo Adicional al Convenio del Consejo de Europa. En este caso, los documentos sobre el cumplimiento de la solicitud se devolverán a través de la misma vía[311]. Esta disposición se aplicará, a menos que uno de los países haya declarado que continuará realizando la transmisión a través de las autoridades centrales.

Recomendación práctica

Los ejemplos indican que la elección de los canales de comunicación incluso dentro de una región (Europa) puede presentar dificultades debido a la existencia de diferentes marcos jurídicos vigentes. La aplicación en línea es una herramienta útil para identificar a las autoridades competentes adecuadas. Las investigaciones de los casos de skimming revelan que los grupos delictivos con frecuencia no actúan únicamente en un país, sino en varios. En consecuencia, los procedimientos relacionados con la cooperación internacional y especialmente la selección de los canales para la transmisión de la solicitud revisten una gran importancia práctica. Si el contacto directo es posible, debería utilizarse ya que en general acelera el proceso.

Medios de comunicación

Los aspectos formales de las actuaciones presentan tantas dificultades como la elección de los canales de comunicación. En virtud del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, los medios de comunicación disponibles entre los países A y B incluyen desde el envío por correo postal, fax o correo electrónico y, además de los medios de comunicación tradicionales, el Convenio también incluye medios de comunicación expeditivos[312].

Sobre la base del Convenio del Consejo de Europa relativo a la asistencia judicial en materia penal, la comunicación entre los países A y C se limita a los medios de comunicación regulares, es decir, el envío por correo postal, ya que el texto del Convenio no menciona explícitamente los medios de comunicación expeditivos. Sin embargo, el Segundo Protocolo Adicional sí hace mención de estos medios.

[311] Artículo 4, párrafo 1, del Segundo Protocolo Adicional al Convenio del Consejo de Europa de 1959.
[312] Para más detalles, véase el informe explicativo del Convenio, disponible en: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229(02)&model=guichett.

Segundo Protocolo Adicional al Convenio del Consejo de Europa relativo a asistencia judicial en materia penal

Artículo 4. Canales de comunicación

[...]

9. Las solicitudes de asistencia recíproca y cualesquiera otras comunicaciones en virtud de este Convenio o sus Protocolos deberá ser transmitida a través de cualquier medio de comunicación electrónico o de otro medio de telecomunicación a condición de que la Parte requirente esté dispuesta, previa solicitud, a producir en cualquier momento un registro escrito y la solicitud original. Sin embargo, cualquier Estado contratante, mediante una declaración dirigida en cualquier momento al Secretario General del Consejo de Europa, podría establecer las condiciones en virtud de las cuales estaría dispuesto a aceptar y cumplir las solicitudes que le fueron enviadas por medios de comunicación electrónicos o de otro tipo.

[...]

Pese a ello, como se menciona en el artículo 4, el Estado contratante podría establecer determinadas condiciones en relación con el uso de medios de comunicación electrónicos o de otro tipo.

Recomendación práctica

Como consecuencia de la capacidad de los Estados miembros de limitar los medios de comunicación expeditivos, es necesario comprobar las posibles salvedades que pudieran tener los Estados requeridos antes de utilizar medios de comunicación electrónicos. Las declaraciones transmitidas se encuentran disponibles en: http://conventions.coe.int.

Contenido de la solicitud

Es necesario que la solicitud que se envía a los países A y B incluya determinada información clave. Con mucha frecuencia, las autoridades competentes que se encargan de dichas solicitudes cuentan con una serie de formularios tipo que cumplen con los requisitos del Estado requerido. Como los requisitos de cada Estado son distintos, resulta difícil proporcionar un formulario que sirva como modelo para todos los posibles destinatarios, si bien existen varios temas que en general deberían considerarse:

- En general, la solicitud debe incluir información básica, tal como el nombre de la autoridad que formula la solicitud, el propósito y motivo de la misma, la identidad y nacionalidad de la persona involucrada;
- Con el fin de garantizar que el Estado requerido sea capaz de cumplir la solicitud de manera oportuna, deberá destacarse el carácter transnacional del delito;
- Es necesario que se proporcionen todos los detalles pertinentes. Esto es especialmente importante para los casos de delitos relacionados con la identidad, ya

que dichos casos son con frecuencia muy complejos. Se debería preparar un resumen de todos los hechos relevantes para que el Estado requerido entienda los antecedentes de la solicitud;

- Es imprescindible que se mencionen las disposiciones jurídicas nacionales aplicables. Esto es particularmente importante en los casos en que la Parte requerida aplica el principio de doble incriminación[313]. Este principio podría ser una de las condiciones para cumplir con la solicitud. En este caso, el envío de una copia de la legislación local podría resultar de gran utilidad para facilitar el proceso de evaluación de la doble incriminación.

6. Sexto caso: skimming II

Enfoque del caso: carta rogatoria formulada durante la fase previa al juicio. La asistencia judicial recíproca precede a la solicitud de extradición. Elemento constitutivo de la delincuencia organizada transnacional.

Los hechos del caso

Un delincuente en el país B participa en un grupo delictivo organizado que supuestamente cometió fraude y falsificación informáticos, además de delitos de clonación de tarjetas de crédito en los países A, C, D y E. Estos hechos han ocasionado daños a varias víctimas en los países mencionados. La solicitud de asistencia judicial recíproca se origina en el país A y se envía al país B. Ambos países son parte de la UNTOC. No existe ningún otro tratado multilateral o bilateral aplicable entre los dos países.

Antecedentes

En general, el término "skimming" se emplea para describir un delito en el que los delincuentes manipulan un cajero automático a fin de obtener información de tarjetas de crédito y números de identificación personal[314]. Se trata de un delito que se lleva a cabo en dos etapas. En la primera, los delincuentes se hacen con la información de la tarjeta de crédito instalando dispositivos en el cajero automático. Por lo general, los dispositivos se esconden dentro de la ranura donde se introduce la tarjeta en el cajero automático, y están diseñados para que parezcan que son parte del mismo[315]. El dispositivo graba y almacena los detalles de todas las tarjetas que se insertan. Para obtener el número de identificación

[313] La doble incriminación se da en el caso en que el delito es considerado como tal en la legislación de las Partes requerida y requirente. Las dificultades que la doble incriminación puede plantear para las investigaciones internacionales es un tema que se trata en varios convenios y tratados internacionales. Algunos ejemplos incluyen el artículo 2 de la Decisión Marco de la UE, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (2002/584/JAI). Con respecto al principio de doble incriminación en las investigaciones internacionales, véase: *Manual de las Naciones Unidas sobre prevención y control de delitos informáticos*, 269, disponible en: http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, página 5, disponible en: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[314] Respecto al delito, véase: *Grabosky*, The Internet, Technology, and Organized Crime, *supra* núm. 261, página 43.

[315] Comunicado de prensa del Departamento de Justicia, Distrito de Georgia del Norte, titulado "Indictment handed down in major ATM skimming operation", de 17 de febrero de 2009.

personal, los delincuentes alteran el teclado o instalan una cámara de microorificio para grabar a las víctimas cuando ingresan su número PIN[316]. En la segunda etapa, los delincuentes utilizan la información que obtuvieron para clonar tarjetas de crédito y usarlas. Se calcula que esta actividad ocasiona pérdidas económicas anuales que ascienden a varios miles de millones de dólares de los Estados Unidos[317]. Existen varias conexiones con grupos delictivos organizados[318].

En la actualidad al fraude se lo relaciona normalmente con el delito cibernético, ya que las tecnologías de la información brindan amplias oportunidades para que se cometa. El fraude de tarjetas de crédito[319], las estafas de pago por adelantado[320], el fraude a través de Internet y al por menor y las estafas en las plataformas de subastas[321] son solo algunos ejemplos de delitos informáticos.

Recomendación práctica

La participación de un grupo delictivo organizado es particularmente importante para la aplicación de la UNTOC.

Propósito de la solicitud

Las autoridades del país A poseen información que lleva a pensar que el delincuente, que se encuentra en el país B, tiene intenciones de huir de ese país. Deben asegurarse de que se conserven las pruebas incriminatorias que se cree que posee el delincuente y, si esto se confirmase, como segunda medida, deberían solicitar su arresto provisional. Esto les permitiría presentar una solicitud de extradición. Por tanto, las autoridades necesitan solicitar a las autoridades judiciales en el país B que lleven a cabo un registro domiciliario y de la computadora del delincuente. Debido a que existe el temor de que el delincuente pueda abandonar el país B y huir de la justicia, la solicitud de asistencia judicial recíproca es de carácter urgente.

---

[316] ATM Crime, ENISA, *supra* núm. 298, página 14.

[317] Final Report of the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, *supra* núm. 260.

[318] *Montaque*, Fraud Prevention Techniques for Credit Card Fraud, *supra* núm. 261, página 62; *Choo*/*Smith*, Criminal Exploitation of Online Systems by Organized Crime Groups, Asian Criminology, 2008, vol. 3, página 41; *Choo*, Organized crimes groups in Cyberspace…, página 277; Final Report of the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, *supra* núm. 260.

[319] Con respecto al alcance del fraude de tarjetas de crédito, véase Consumer Fraud and Identity Theft Complain Data, January–December 2005, Federal Trade Commission, 2006, página 3, disponible en: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[320] El término "estafa de pago por adelantado" se refiere a los delitos en los que los delincuentes tratan de obtener de las víctimas pequeñas sumas de dinero por adelantado con la esperanza de recibir más adelante una suma mucho mayor. Para más información, véase: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, página 1; *Smith*/*Holmes*/*Kaufmann*, Nigerian Advance Fee Fraud, "Trends & Issues in Crime and Criminal Justice", núm. 121, disponible en: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response", *Computer Law & Security Report*, vol. 21, issue 3, página 237; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on Aging, *supra* núm. 273, página 7.

[321] El término "estafa en las plataformas de subastas" se refiere a las actividades fraudulentas en las plataformas de subastas electrónicas a través de Internet. Con respecto a este tipo de delito, véase: *Bywell*/*Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), página 265 y ss., disponible en: http://www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, *Federal Communications Law Journal*, 52 (2), página 453 y ss.; *Chau*/*Falooutsos*, Fraud Detection in Electronic Auction, disponible en: http://www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf; *Dolan*, Internet Auction Fraud: The Silent Victims, *Journal of Economic Crime Management*, vol. 2, issue 1, disponible en: https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

Estrategia

Ambos países son parte de la UNTOC y, como se mencionó anteriormente, no existe ningún otro tratado multilateral o bilateral aplicable entre los dos países. Por consiguiente, la solicitud se formulará de acuerdo con lo estipulado en la UNTOC. La solicitud reviste carácter urgente debido a que existen claros indicios que llevan a pensar que el delincuente podría huir del país B.

> **Artículo 18, párrafo 13, de la UNTOC**
>
> 13. Las solicitudes de asistencia judicial recíproca y cualquier otra comunicación pertinente serán transmitidas a las autoridades centrales designadas por los Estados Parte. La presente disposición no afectará al derecho de cualquiera de los Estados Parte a exigir que estas solicitudes y comunicaciones le sean enviadas por vía diplomática y, en circunstancias urgentes, cuando los Estados Parte convengan en ello, por conducto de la Organización Internacional de Policía Criminal, de ser posible.

Transmisión de la solicitud

Las autoridades judiciales del país A deben verificar en primer lugar si desean transmitir la solicitud a través de Interpol. Si el país B permite este tipo de transmisiones, el directorio de autoridades nacionales competentes es de vital importancia. No debe asumirse que todos los países parte de la UNTOC aceptan la transmisión a través de Interpol. Algunos de ellos mencionan de manera explícita que, en los casos urgentes, no aceptan la transmisión a través de Interpol, por tanto es necesario realizar una verificación como medida necesaria.

Un segundo aspecto a considerar es que la decisión de elegir estos canales de comunicación le corresponde a la autoridad judicial. Un poderoso incentivo para hacerlo sería si el Estado requerido aceptase que la solicitud se transmitiera a través de la vía diplomática, lo cual, dadas las circunstancias del caso, no sería la manera más apropiada de proceder. La transmisión por intermedio de Interpol normalmente facilitaría el contacto entre la autoridad judicial en el país A y la autoridad ejecutora del país B.

Cumplimiento de la solicitud

La oficina nacional de Interpol en el Estado requerido debería en consecuencia transmitir la solicitud directamente a la autoridad judicial competente, la cual deberá formalizarla y evitar, en la medida de lo posible, establecer un contacto adicional transmitiendo la solicitud a la autoridad central del Estado requerido (a menos que existan disposiciones nacionales específicas que así lo estipulen).

Seguimiento

Una vez se da cumplimiento a la solicitud, la autoridad judicial ejecutora deberá transmitir la respuesta directamente a la autoridad judicial requirente a través de medios de

comunicación expeditivos o, en el caso en que el contacto directo no sea posible, se realizará a través de Interpol. Sobre la base de las pruebas recogidas, el país A podría posteriormente transmitir una solicitud de extradición.

Recomendación práctica

En el artículo 18, párrafo 17, de la UNTOC se establece que se dará cumplimiento a toda solicitud con arreglo al derecho interno del Estado Parte requerido y en la medida en que ello no lo contravenga y sea factible, de conformidad con los procedimientos especificados en la solicitud. Por consiguiente, se mantiene el hecho de que Interpol es únicamente un canal de comunicación y de que los requisitos formales para transmitir y formalizar una solicitud siguen siendo válidos.

7. Séptimo caso: tráfico ilícito de migrantes

Enfoque del caso: carta rogatoria formulada durante la fase previa al juicio. Elemento constitutivo de la delincuencia organizada transnacional.

Los hechos del caso

Varios delincuentes del país A participan en un grupo delictivo organizado que se dedica al tráfico de migrantes originarios del país C. El tráfico se realiza desde el país A al país B. A fin de garantizar que las personas ingresen en el país de destino, se utilizan identidades sintéticas[322], aunque en algunas ocasiones también se utilizan identidades verdaderas que se obtienen alterando tarjetas de identificación legítimas. Los países A y B son limítrofes. El país C se encuentra en otro continente. Los tres países son parte de la UNTOC y del Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire, que complementa a la UNTOC. Entre los países A y B se encuentra en vigor además un tratado bilateral respecto de la cooperación judicial internacional en materia penal.

Propósito de la solicitud

Las autoridades del país B a cargo de la investigación necesitan saber lo siguiente: en lo que respecta al país A, necesitan recibir datos sobre el grupo delictivo organizado y su forma de operar, haciendo especial hincapié en las actividades delictivas o convicciones previas (si procede); en relación con el país C, las autoridades necesitan obtener los datos de identificación reales de los migrantes que fueron víctimas del tráfico ilícito, dado que los documentos presentados ante las autoridades del país B no se corresponden con sus verdaderas identidades.

[322] Una identidad sintética se obtiene combinando datos verdaderos con datos falsos, o utilizando exclusivamente datos falsos. Para más información respecto de las identidades sintéticas, véase: *McFadden*, Detecting synthetic identity fraud, disponible en: http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp; véase además: *Gercke*, Legal Approaches to Criminalize Identity Theft, *supra* núm. 28, página 39.

Estrategia

La solicitud formal surge como consecuencia de una cooperación informal que se lleva a cabo previamente entre las fuerzas del orden, tal como está previsto en los artículos 27 y 28 de la UNTOC y en el artículo 10 del Protocolo contra el tráfico ilícito de migrantes, y que normalmente también contemplan los tratados bilaterales contemporáneos. Como se mencionó anteriormente en el capítulo II, este tipo de cooperación, ya sea entre fuerzas policiales o entre los organismos encargados de hacer cumplir la ley en general, es de suma importancia para obtener las primeras aportaciones en las investigaciones delictivas, las cuales constituyen los principales elementos que permiten la posterior elaboración de una solicitud formal de asistencia judicial recíproca.

Artículo 10 del Protocolo contra el tráfico ilícito de migrantes

Información

1. Sin perjuicio de lo dispuesto en los artículos 27 y 28 de la Convención y con miras a lograr los objetivos del presente Protocolo, los Estados Parte, en particular los que tengan fronteras comunes o estén situados en las rutas de tráfico ilícito de migrantes, intercambiarán, de conformidad con sus respectivos ordenamientos jurídicos y administrativos internos, información pertinente sobre asuntos como:

a) Los lugares de embarque y de destino, así como las rutas, los transportistas y los medios de transporte a los que, según se sepa o se sospeche, recurren los grupos delictivos organizados involucrados en las conductas enunciadas en el artículo 6 del presente Protocolo;

b) La identidad y los métodos de las organizaciones o los grupos delictivos organizados involucrados o sospechosos de estar involucrados en las conductas enunciadas en el artículo 6 del presente Protocolo;

c) La autenticidad y la debida forma de los documentos de viaje expedidos por los Estados Parte, así como todo robo o concomitante utilización ilegítima de documentos de viaje o de identidad en blanco;

d) Los medios y métodos utilizados para la ocultación y el transporte de personas, la alteración, reproducción o adquisición ilícitas o cualquier otra utilización indebida de los documentos de viaje o de identidad empleados en las conductas enunciadas en el artículo 6 del presente Protocolo, así como las formas de detectarlos;

[…]

Canales y medios de comunicación

A fin de hacer posible la cooperación formal, el país B deberá observar con referencia al país A las disposiciones del tratado bilateral, teniendo en cuenta el artículo 18, párrafo 7, el cual confiere, tal como se ha mencionado anteriormente, preferencia a los tratados bilaterales ya existentes. Para más detalles sobre los tratados bilaterales, véase el cuarto caso mencionado *supra*.

En lo que respecta a la solicitud que presenta el país B al país C, resultan relevantes la UNTOC y el Protocolo contra el tráfico ilícito de migrantes y deberían citarse conjuntamente. Se recomienda que se observen las normas previstas en el artículo 18 relativas a los canales de comunicación y demás requisitos formales (para más detalles, véanse los casos anteriores).

Tal como se mencionó anteriormente, en el artículo 18, párrafo 9, se establece que los Estados Parte podrán negarse a prestar la asistencia judicial recíproca con arreglo al presente artículo invocando la ausencia de doble incriminación. Sin embargo, en el presente caso, este motivo no es suficiente para rechazar la solicitud en circunstancias normales, ya que tanto el país B como el C son parte del Protocolo contra el tráfico ilícito de migrantes. Esto significa que ambos han puesto en práctica en su legislación nacional el artículo 6 del Protocolo, el cual penaliza no solo el tráfico ilícito de migrantes, sino también la creación, facilitación o suministro de un documento de viaje o de identidad falso con el fin de posibilitar el tráfico ilícito de migrantes. El buen resultado de la solicitud depende también de la implementación parcial o total del derecho penal sustantivo en el Estado requerido.

Contenido de la solicitud

En cuanto al contenido de la solicitud, deberán observarse las condiciones previstas en el artículo 18, párrafo 15, así como los requisitos específicos del Estado requerido, si se los conoce (debería utilizarse información de experiencias pasadas con ese Estado y los datos obtenidos a través de la cooperación informal). Este ejemplo pone de relieve, desde un punto de vista práctico, la interrelación que existe entre las disposiciones de cooperación sustantivas, procesales e internacionales de la UNTOC y sus Protocolos, así como la importancia de la aplicación de la legislación de cada uno de los Estados cooperantes.

8. Octavo caso: falsificación

Enfoque del caso: solicitud de asistencia judicial recíproca formulada durante la fase del juicio. Elemento constitutivo de la delincuencia Organizada Transnacional.

Los hechos del caso

Un grupo delictivo organizado del país A lleva a cabo delitos informáticos y de falsificación, causando perjuicios a personas que se encuentran en los países B, C, D, E, F y G. Los países A, B y C se encuentran en Europa, los países D y E en América del Sur, el país F en América del Norte y el país G en Australia. Los países A y B son parte del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (2000) y los países A y C son parte del Convenio del Consejo de Europa de 1959. Todos los países involucrados son parte de la UNTOC. Existe un tratado bilateral aplicable entre los países A y F. Los países A, B y F son parte del Convenio sobre el delito cibernético de 2001.

Propósito de la solicitud

El juez del país A necesita expedir los documentos a los países B, C, D, E, F y G. Esta solicitud formulada durante la etapa del juicio es el último eslabón en la cadena de cooperación, que comienza con las denuncias presentadas por las víctimas ante sus autoridades nacionales o directamente ante las autoridades del país A, la cooperación policial y las solicitudes formales transmitidas durante la etapa previa al juicio en la cual se envían cartas rogatorias a los países B, C, D, E, F y G a fin de determinar la identidad de las víctimas y obtener su declaración y cualesquiera otros documentos recogidos como prueba para preparar la imputación contra los individuos parte del grupo delictivo organizado. Durante el juicio, es necesario informar a las partes afectadas sobre la duración del juicio y que pueden estar presentes en el juzgado, si así lo desean.

Estrategia: consideraciones sobre la aplicabilidad de los instrumentos pertinentes

En este caso en particular, debido a que la solicitud debe transmitirse simultáneamente a varios países o continentes, deben considerarse algunos aspectos comunes.

El primer asunto importante es identificar el tratado aplicable en cada caso y observar sus disposiciones con respecto a la asistencia judicial recíproca en general y la expedición de documentos en particular. En la mayoría de los casos, las citaciones no pueden enviarse directamente a las víctimas y, en consecuencia, es necesario formular una solicitud de asistencia judicial recíproca. En el momento de preparar la solicitud, se deberá tener presente que las citaciones deben transmitirse a la autoridad judicial ejecutora con suficiente antelación al plazo establecido para el juicio. Además, se debe saber exactamente si la autoridad requerida solicita el envío de los documentos de notificación dentro de un determinado período y si tiene declaraciones especiales en este sentido. Como no se puede asumir que la legislación nacional de cada Estado prevé plazos idénticos, el plazo final establecido para el juicio debe tener en cuenta todas las condiciones y plazos previstos por la legislación de los Estados requeridos (algunos podrían prever períodos más cortos y permitir el uso de medios de comunicación expeditivos, otros podrían no hacerlo). Por tanto, es muy probable que se establezca un período más largo.

Otro asunto a considerar guarda relación con el contenido de la solicitud. Si algunos países contemplan requisitos específicos respecto de dicho contenido, la solicitud que se envía a estos países deberá estar respaldada por información relevante. Por ejemplo, en el caso de los países que aplican el derecho consuetudinario, sería necesario calcular el valor del daño, así como proporcionar una descripción detallada de los hechos del caso y una clara justificación de la solicitud.

Un último asunto que debe tenerse en cuenta desde el primer momento es el de los idiomas requeridos para las citaciones. En este caso, las víctimas se encuentran en diferentes países y hablan distintos idiomas. Las citaciones deberían traducirse a esos idiomas para que las víctimas en los Estados requeridos puedan entenderlas.

En el caso de los países A y B, se aplica el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (2000). Pese a que ambos Estados son parte del Convenio del Consejo de Europa sobre el delito cibernético, este último no es pertinente, ya que sus disposiciones confieren principalmente prioridad a otros tratados o acuerdos bilaterales vigentes entre los Estados miembros (véase el artículo 27, párrafo 1, del Convenio sobre el delito cibernético), en este caso en particular, al Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea de 2000.

Artículo 5, párrafo 2, del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea

El envío de documentos procesales podrá efectuarse por mediación de las autoridades competentes del Estado miembro requerido únicamente en caso de que:

a) el domicilio de la persona a la que va dirigido un documento sea desconocido o incierto;

b) el Derecho procesal pertinente del Estado miembro requirente exija una prueba de que el documento ha sido notificado al destinatario distinta de la que pueda obtenerse por correo;

c) no haya resultado posible entregar el documento por correo;

d) el Estado miembro requirente tenga razones justificadas para estimar que el envío por correo resultará ineficaz o inadecuado.

[…]

En la situación que se menciona en el artículo 5, párrafo 2, debido a que la solicitud no se transmite directamente al destinatario, es necesario enviar una solicitud de asistencia judicial recíproca a las autoridades del Estado requerido, las cuales se pueden identificar a través del Atlas Judicial Europeo, disponible en: http://www.ejn-crimjust.europa.eu/atlas_advanced.aspx (dependiendo del Estado requerido, podría tratarse de una autoridad judicial o central). Las notificaciones se deberán traducir a los idiomas oficiales del país B (véase el artículo 5, párrafo 3).

Entre los países A y C se aplica el Convenio del Consejo de Europa sobre cooperación judicial en materia penal (1959). En este caso, la transmisión se realiza a través de las autoridades centrales. Los documentos que es necesario expedir van acompañados por una solicitud de asistencia judicial recíproca. En el momento de enviar la solicitud, muchos países se aseguran de utilizar los formularios que exigen los requisitos generales de una solicitud de asistencia judicial recíproca de conformidad con el artículo 14 del Convenio de 1959, que fuera mencionado en casos anteriores. La autoridad central del Estado requerido (en este caso, del país C) enviará los documentos a las autoridades judiciales competentes. La expedición de los documentos puede llevarse a cabo a través de un simple envío o de la manera prevista o compatible con la legislación del Estado requirente.

Artículo 7, párrafo 1, del Convenio del Consejo de Europa sobre cooperación judicial en materia penal de 1959

[...]

La notificación podrá efectuarse mediante la simple entrega al destinatario del documento o resolución. Si la Parte requirente lo solicita expresamente, la Parte requerida efectuará la notificación en una de las formas previstas por su legislación para notificaciones análogas o en alguna forma especial que sea compatible con dicha legislación.

Asimismo, es importante comprobar si los dos países son Parte del Segundo Protocolo Adicional de 2001, cuyo artículo 16 menciona que la expedición de documentos podría realizarse directamente desde la autoridad judicial emisora al destinatario a través del correo postal (dicha disposición es similar a la estipulada en el Convenio sobre cooperación judicial en materia penal entre los Estados miembros de la Unión Europea de 2000).

Segundo Protocolo Adicional de 8 de noviembre de 2001 al Convenio Europeo de Asistencia Recíproca del Consejo de Europa de 1959

Artículo 16: notificación por correo

1. Las autoridades judiciales competentes de cualquier Parte podrían enviar directamente por correo documentos procesales y decisiones judiciales a las personas que se encuentren en el territorio de cualquier otro Estado Parte.

Es necesario que se traduzcan las notificaciones al idioma del Estado ejecutante, teniendo en cuenta de este modo la nacionalidad de las víctimas.

En el caso de los países A y D, y E, A y G se aplica la UNTOC. La expedición de documentos se menciona expresamente en el artículo 18, párrafo 3, inciso *b)*, de la UNTOC bajo el título "presentación de documentos judiciales". Tal como se mencionó anteriormente con respecto al Convenio del Consejo de Europa de 1959, es necesario que la citación vaya acompañada de la solicitud de asistencia judicial recíproca. Por consiguiente, serán relevantes todos los temas principales que fueron abordados en relación con la aplicación de la UNTOC en ocasiones anteriores, incluidas las disposiciones del artículo 18, párrafo 15. Con respecto a los canales de comunicación, el contacto directo con la víctima por correo postal, tal como está previsto en los Convenios europeos, no sería apropiado. Como regla general, el contacto deberá establecerse a través de las autoridades centrales.

El directorio de autoridades nacionales competentes resulta muy práctico para realizar la transmisión a través de las autoridades centrales o por la vía diplomática. Algunos de los países implicados podrían incluso aceptar el empleo de medios de comunicación expeditivos, tales como el fax o el correo electrónico. En este sentido, en caso de que no hubiera contactos anteriores, también podría ser de suma utilidad llevar un control de la información que se suministra a través del directorio en línea.

En cuanto a las posibilidades de que el país A establezca contacto con los países ubicados en América del Sur, debería considerarse la opción que ofrece la Red judicial europea (RJE)[323]. El país A, al ser Estado miembro de la UE y tener puntos de contacto dentro de la RJE, puede pedir apoyo a la Red para contactar[324] a los puntos de contacto de IberRed[325] (con la condición de que los países situados en América del Sur sean parte de IberRed). Esta forma de proceder podría resultar extremadamente eficaz cuando la solicitud de notificar a las víctimas tiene carácter urgente.

Entre los países A y F, existe un tratado bilateral aplicable que ya se encuentra en vigor. El Convenio del Consejo de Europa sobre el delito cibernético no tendría preeminencia de acuerdo a lo mencionado *supra* (en la descripción de la solicitud transmitida del país A al B). El Convenio podría citarse junto con el instrumento bilateral si la transmisión de documentos es de carácter urgente y cuando sea necesario el empleo de medios de comunicación expeditivos previstos en el artículo 25 del Convenio, o si se tiene en cuenta la asistencia recíproca respecto de medidas provisionales tales como la conservación de datos únicamente (lo cual no es el caso, habida cuenta del hecho de que se está hablando de una solicitud tradicional de expedición de documentos). Las citaciones se pueden transmitir a través de la vía diplomática entre los ministerios de justicia. Habitualmente, en el caso de que hubiera un tratado bilateral reciente, esta última hipótesis sería razonable. Cabe reiterar que el uso del fax o del correo electrónico debería estar permitido como regla general.

9. Noveno caso: falsificación de documentos y tráfico de personas

Enfoque del caso: carta rogatoria formulada durante la fase previa al juicio. Elemento constitutivo de la delincuencia organizada transnacional.

Los hechos del caso

Varios delincuentes del país B participan en un grupo delictivo organizado que se dedica al tráfico de menores con fines de explotación sexual. El tráfico se realiza del país A al país C, utilizando el país B como zona de tránsito. A fin de garantizar que los menores viajen al país de destino, se fabrican documentos falsos en los que se modifica la edad de los menores para que puedan figurar como adultos. Los países B y C son parte de la Convención Interamericana sobre Asistencia Mutua en Materia Penal[326] (Nassau, 1992), pero también son parte de la UNTOC y del Protocolo contra la trata de personas (Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la UNTOC), mientras que los países A y C son únicamente parte de la UNTOC y del Protocolo contra la trata de personas. No existe ningún tratado bilateral con respecto a la cooperación internacional entre los países C y B y entre los países C y A que sea aplicable.

[323] Para información sobre la Red judicial europea, véase: http://www.ejn-crimjust.europa.eu/.

[324] La RJE y la IberRed están asociadas y cada una de estas redes regionales puede facilitar el contacto con un miembro de la otra. El Memorando de Entendimiento de las dos redes puede consultarse en: http://www.ejn-crimjust.europa.eu/my_news/documents/MoU_EN.pdf.

[325] IberRed es la abreviación de Red Iberoamericana de Cooperación Jurídica Internacional, véase *supra*, página 93. Para más información sobre la Red y los puntos de contacto, véase: http://www.iberred.org/presentacion/.

[326] La Convención se encuentra disponible en línea en: http://www.oas.org/juridico/english/Treaties/a-55.html.

Propósito de la solicitud

El fiscal del país C debe transmitir la solicitud a los países A y B como sigue:

- La solicitud que se transmite al país B hace referencia a los datos de la actividad criminal de las personas que forman parte del grupo delictivo y, en el caso en que los delincuentes hayan participado en actividades delictivas anteriores, los datos sobre los mismos. Además, en las situaciones en que existan informes, el fiscal del país C pedirá el envío de cualquier tipo de información o pruebas de las que ya dispongan las autoridades judiciales del país B.

- La solicitud que se transmite al país A consiste principalmente en tomar declaración a diversas personas que se encontraban próximas a la víctima en el país A. Una segunda solicitud se refiere a los documentos falsificados, es decir, si existía algún vínculo conocido entre la organización delictiva sujeto de investigación y un grupo delictivo organizado en el país A especializado en la falsificación de documentos de identidad, así como otros elementos importantes que pudieran ayudar a la investigación en el país C. Estos datos podrían encontrarse en posesión de las autoridades judiciales del país A.

Estrategia

Contactos informales: transmisión de la solicitud

Con respecto a la solicitud del país C al país B, es necesario hacer hincapié en que antes de transmitir la solicitud formal, se deberán utilizar los contactos informales a través de los canales policiales, a fin de obtener algunos datos iniciales sobre el grupo delictivo organizado y la información que poseen las autoridades del país B respecto de su funcionamiento. La Organización de los Estados Americanos (OEA), de la cual son parte ambos países, recomienda el uso de medios de cooperación alternativos o colaterales, debido a la urgencia que reviste este tipo de cooperación:

> Se recomienda que los Estados miembros reconozcan la importancia vital de otros métodos de asistencia menos formales, incluida la cooperación entre las fuerzas policiales de los respectivos Estados miembros, y de que se prevea la preservación y el fomento de dicha cooperación directa en la mayor medida posible[327].

La solicitud formal con el objeto mencionado anteriormente se transmitirá de acuerdo con la Convención Interamericana sobre Asistencia Mutua en Materia Penal (A-55), por

[327] Véanse, a este respecto las Propuestas de guías de mejores prácticas con respecto a la recopilación de declaraciones, documentos y pruebas físicas, así como con respecto a la asistencia mutua en relación con la investigación, congelación y confiscación de activos que sean producto o instrumento de delitos y formularios sobre cooperación jurídica en materia penal adoptados en la Tercera Reunión de autoridades centrales y otros expertos en asistencia mutua en materia penal y extradición, celebrada en Bogotá, Colombia, los días 12, 13 y 14 de septiembre de 2007, disponible en: http://www.oas.org/juridico/MLA/sp/mejores_pract_sp.pdf.

tanto, la transmisión deberá realizarse desde una autoridad central a otra[328]. Otra posibilidad sería utilizar la Red Hemisférica de Intercambio de Información para la Asistencia Mutua en Materia Penal y Extradición[329] (la transmisión de la solicitud de asistencia judicial recíproca a través de autoridades centrales no impide a las autoridades judiciales de ambos países que inicien contactos directos si se conocen los detalles de contacto de la autoridad judicial ejecutora del país C).

El principio de la doble incriminación no es una condición previa para ejecutar la solicitud aunque existen, con algunas excepciones, tal como se establece en el artículo 5, párrafo 2:

> **Artículo 5, párrafo 2, de la Convención Interamericana sobre Asistencia Mutua en Materia Penal**
>
> Cuando la solicitud de asistencia se refiera a las siguientes medidas: *a)* embargo y secuestro de bienes; y *b)* inspecciones e incautaciones, incluidos registros domiciliarios y allanamientos, el Estado requerido podrá no prestar la asistencia si el hecho que origina la solicitud no fuera punible conforme a su ley.

Para el envío de la solicitud, también podrían utilizarse los formularios mencionados anteriormente en las propuestas de guías de prácticas óptimas.

Con referencia a la solicitud que el país C necesita transmitir al país A, como se mencionó con anterioridad, son aplicables la UNTOC y el Protocolo contra la trata de personas[330], los cuales deben citarse conjuntamente.

La solicitud formal, en particular en lo que respecta a la falsificación de documentos, podría ir precedida de la cooperación informal entre los organismos encargados de hacer cumplir la ley, con arreglo a los artículos 27 y 28 de la UNTOC y al artículo 10 del Protocolo contra la trata de personas.

Deben tenerse en cuenta los comentarios que se realizaron en los casos anteriores respecto de las disposiciones del artículo 18 de la UNTOC relativas a los canales de comunicación, el uso del directorio de autoridades competentes en línea o su versión impresa y el contenido de las solicitudes. Respecto del contenido, deberían cumplirse los requisitos previstos en el artículo 18, párrafo 15.

[328] Véase, al respecto, el artículo 3 de la Convención Interamericana sobre Asistencia Mutua en Materia Penal.
[329] Para más información sobre la Red, véase: http://www.oas.org/juridico/mla/sp/index.html.
[330] El Protocolo contra la trata de personas puede consultarse, junto con la UNTOC en: http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf y la Guía legislativa en: http://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html#traffickig.

Artículo 10 del Protocolo contra la trata de personas

Intercambio de información y capacitación

1. Las autoridades de los Estados Parte encargadas de hacer cumplir la ley, así como las autoridades de inmigración u otras autoridades competentes, cooperarán entre sí, según proceda, intercambiando información, de conformidad con su derecho interno, a fin de poder determinar:

a) Si ciertas personas que cruzan o intentan cruzar una frontera internacional con documentos de viaje pertenecientes a terceros o sin documentos de viaje son autores o víctimas de la trata de personas;

b) Los tipos de documento de viaje que ciertas personas han utilizado o intentado utilizar para cruzar una frontera internacional con fines de trata de personas; y

c) Los medios y métodos utilizados por grupos delictivos organizados para los fines de la trata de personas, incluidos la captación y el transporte, las rutas y los vínculos entre personas y grupos involucrados en dicha trata, así como posibles medidas para detectarlos.

[...]

3. El Estado Parte receptor de dicha información dará cumplimiento a toda solicitud del Estado Parte que la haya facilitado en el sentido de imponer restricciones a su utilización.

Cumplimiento de la solicitud

Se dará cumplimiento a la solicitud de conformidad con el derecho interno del Estado requerido. Sin embargo, en la medida en que ello no lo contravenga y sea factible, se dará cumplimiento a la solicitud de conformidad con los procedimientos que en ella se especifican (artículo 18, párrafo 7, de la UNTOC). Teniendo en cuenta que una de las solicitudes hace referencia a la toma de declaraciones a personas que conocían a las víctimas, el Estado requirente deberá preparar una serie de preguntas y pautas claras que deberá enviar al Estado requerido para garantizar el cumplimiento del procedimiento y permitir a las autoridades del país C utilizar con posterioridad las pruebas en el tribunal.

El hecho de que ambos países son parte del Protocolo contra la trata de personas permite no solo la cooperación informal (véase, por ejemplo, el artículo 10 mencionado anteriormente), sino también el cumplimiento de la solicitud en la mayor medida posible (a este respecto, véase el caso séptimo relativo al tráfico ilícito de migrantes y la referencia que se hace a las sanciones penales).

10. Décimo caso: equipo conjunto de investigación y tráfico de personas

Enfoque del caso: equipo conjunto de investigación formulado durante la fase previa al juicio. Tienen aplicación los tratados bilaterales, multilaterales y sobre el crimen organizado.

Los hechos del caso

Un grupo delictivo organizado, cuyas actividades se desarrollan en el país A, está involucrado en el tráfico de chicas jóvenes (nacionales del país A) hacia el país B. Dentro de este contexto, el grupo delictivo utiliza documentos de identidad falsificados que hacen pasar a las víctimas como mayores de edad. Posteriormente, se lleva a cabo el tráfico de estas personas con el fin de explotarlas sexualmente en el país B.

Los países A y B se encuentran en continentes distintos. En este caso son aplicables un tratado bilateral de asistencia judicial recíproca en materia penal y la UNTOC.

Estrategia

A fin de llevar a cabo el examen del caso, los organismos de investigación del país B podrían constituir un equipo conjunto de investigación (ECI) con las autoridades del país A. Los indicadores para recurrir a dicha estrategia son la complejidad del caso y su dimensión transnacional. El equipo conjunto se establecerá en el país B. El país A apoya este proceso enviando expertos nacionales al país B. El objetivo del equipo conjunto de investigación es identificar a las víctimas, tomarles declaración y reunir información sobre la trama de la red delictiva con base en el país A.

La primera medida es identificar los instrumentos aplicables. El tratado bilateral referente a la asistencia judicial recíproca debería citarse conjuntamente con la UNTOC, el cual contiene una disposición sobre investigaciones conjuntas (artículo 19). Antes de iniciar negociaciones para el establecimiento de un ECI, por lo general se recomienda que primero se envie una solicitud de asistencia judicial recíproca pidiendo un acuerdo preliminar respecto de la creación de un equipo conjunto.

Artículo 19 de la UNTOC

Los Estados Parte considerarán la posibilidad de celebrar acuerdos o arreglos bilaterales o multilaterales en virtud de los cuales, en relación con cuestiones que son objeto de investigaciones, procesos o actuaciones judiciales en uno o más Estados, las autoridades competentes puedan establecer órganos mixtos de investigación. A falta de acuerdos o arreglos de esa índole, las investigaciones conjuntas podrán llevarse a cabo mediante acuerdos concertados caso por caso. Los Estados Parte participantes velarán por que la soberanía del Estado Parte en cuyo territorio haya de efectuarse la investigación sea plenamente respetada.

Una vez se alcanza el acuerdo preliminar, es necesario establecer un arreglo entre los países A y B respecto del equipo conjunto de investigación. Como ya se mencionó, se recomienda establecer un modelo integrado activo[331] condicionado a los hechos del caso.

[331] Para las categorías, véase: Report of the Informal Expert Group on Joint Investigations, Conclusions and Recommendations, 2 a 4 de septiembre de 2008, Viena.

En este sentido, es necesario considerar varios aspectos. Los asuntos más importantes serán tratados aquí teniendo en cuenta los modelos propuestos por el Grupo de trabajo oficioso de expertos sobre las investigaciones conjuntas[332], así como la versión revisada del Modelo de Acuerdo para establecer un equipo conjunto de investigación, aprobado recientemente[333].

Los acuerdos de los equipos conjuntos de investigación deben comprender, entre otras cosas, las partes del acuerdo, el propósito del equipo y el período que se abarca, el líder del equipo y la competencia de los miembros y las disposiciones de organización.

- En lo que respecta a las partes del acuerdo, los países A y B deberán contar con autoridades competentes dentro de la oficina del fiscal o de la policía, o ambos. El acuerdo necesita definir las autoridades competentes involucradas.

- El propósito del equipo conjunto de investigación debe estar bien definido. Para este caso en particular, el equipo se establece a fin de desbaratar una red delictiva que se dedica al tráfico de seres humanos (TSH), identificando y tomando declaración a las víctimas. El equipo necesita iniciar medidas de investigación para identificar a las víctimas y desvelar información acerca de los delincuentes. La participación de expertos nacionales del país A que tengan la misma nacionalidad que las víctimas podría ser una gran ventaja.

- Es importante definir el período durante el cual el equipo conjunto de investigación estará operativo. Si la investigación tiene que hacer frente a dificultades no previstas, se podría evaluar la necesidad de prolongar su período de funcionamiento durante la etapa de seguimiento.

- El líder del equipo deberá escogerse entre los representantes del país B (el país anfitrión) teniendo en cuenta el hecho de que el tipo de equipo conjunto de investigación establecido es un modelo integrado activo.

- Con respecto a las competencias de los participantes del equipo, podrían surgir algunas dificultades con los expertos nacionales en comisión de servicio. Es necesario que se los defina claramente en el acuerdo considerando el hecho de que los expertos nacionales en comisión de servicio no tendrán una simple función consultiva, sino que participarán en la investigación. En este marco, el líder del equipo conjunto de investigación u otro miembro del mismo necesitarán capacitar al experto para garantizar que, por ejemplo, las pruebas se recojan de conformidad con las normas y procedimientos del país anfitrión (país B). Esto es especialmente importante en los casos en los que participan representantes de un país que posee un sistema jurídico diferente (derecho civil, derecho consuetudinario).

- En relación con las disposiciones de organización, se recomienda tener en cuenta la cobertura de los gastos de personal (por ejemplo, los gastos de viajes, dietas

[332] *Ibid.*

[333] El Modelo de Acuerdo fue aprobado por resolución del Consejo de 26 de febrero de 2010 (2010/C70/01), y se encuentra disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:070:0001:0012:Es:PDF.

diarias para las personas en comisión de servicio), así como los gastos de las medidas de investigación (con frecuencia el país anfitrión se encarga de ello). El acuerdo del equipo conjunto de investigación podría también incluir normativas en relación con la confidencialidad, así como con la participación de redes nacionales y organizaciones (a nivel de la UE, en particular podrían estar incluidas Eurojust y EUROPOL).

- También deberán definirse claramente la principal competencia y obligaciones de los representantes en comisión de servicio. En lo que respecta a las condiciones del acuerdo, en el artículo 13, párrafo 3, del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (2000) se presenta un buen ejemplo de posibles condiciones.

Artículo 13 del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea de 2000

3. El equipo conjunto de investigación actuará en el territorio de los Estados miembros que lo hayan creado, con arreglo a las condiciones generales siguientes:

a) Dirigirá el equipo un representante de la autoridad competente que participe en la investigación penal del Estado miembro en el que actúe el equipo. El jefe del equipo actuará dentro de los límites de las competencias que tenga atribuidas con arreglo a la legislación nacional;

b) El equipo actuará de conformidad con la legislación del Estado miembro en el que esté llevando a cabo sus investigaciones. Los miembros del equipo llevarán a cabo su labor bajo la dirección de la persona a que se refiere la anterior letra *a)*, teniendo en cuenta las condiciones establecidas por sus propias autoridades en el acuerdo de constitución del equipo;

c) El Estado miembro en el que actúe el equipo tomará las disposiciones organizativas necesarias para que el equipo pueda actuar.

11. Décimo primer caso: delito relacionado con Internet

Enfoque del caso: aplicación de instrumentos de investigación específicos de Internet.

Los hechos del caso

Un delincuente en un país A crea un sitio web falso con una apariencia similar al sitio web de una institución financiera legítima que está registrado y opera desde un país B. El sitio está alojado en un proveedor de Internet en el país A. Varios usuarios de Internet en el país B tienen acceso al sitio y hacen públicos sus datos de identidad. Esta información se utiliza más tarde para acceder a las cuentas bancarias de las víctimas y hacer transferencias. Los países A y B han ratificado el Convenio del Consejo de Europa sobre el delito cibernético.

Antecedentes

Los delitos relacionados con la identidad que se cometen utilizando las tecnologías de redes son objeto de creciente preocupación. Las actividades de "peska" y de apropiación de cuenta son solo dos términos utilizados para describir fenómenos típicos relacionados con Internet. En general, la principal preocupación en este sentido no es la falta de penalización de los delitos relacionados con la identidad, sino los desafíos que presentan para las tareas de investigación. La identificación de un delincuente que comete un delito cibernético podría requerir el examen de datos de tráfico[334]. Con frecuencia la información que podría ser de relevancia para la identificación se elimina cuando ya no se necesita para el procesamiento de transferencia de datos[335]. Una respuesta expeditiva por parte de las autoridades investigadoras resulta crucial para el éxito de la investigación. Si no se cuenta con una legislación e instrumentos adecuados que permitan a los investigadores actuar de manera inmediata y evitar que los datos sean eliminados, es imposible luchar eficazmente contra el delito cibernético[336].

Estrategia

Incluso si se utilizan medios de comunicación expeditivos, la cooperación internacional es en general un proceso que lleva tiempo. Esto tiene especial relevancia cuando se lo compara con la velocidad de la transferencia de datos y los procesos de eliminación automática. Por tanto, la estrategia debe centrarse en la conservación de los datos. En este caso revisten especial interés los archivos de registro que fueron generados por el proveedor de alojamiento. Debido a que ambos países han ratificado[337] el Convenio del Consejo de Europa sobre el delito cibernético, se encuentra disponible a nivel nacional un instrumento de procedimiento que permite a las fuerzas del orden solicitar la conservación expeditiva de los datos informáticos.

[334] Determinar la fuente o destino de las comunicaciones pasadas puede ayudar a identificar la identidad de los autores. Para rastrear estas comunicaciones a fin de determinar su origen y destino, es necesario contar con los datos de tráfico respecto de las mismas, véase: Explanatory Report to the Council of Europe Convention on Cybercrime núm. 155, *supra* núm. 159; Con respecto a la identificación de los sospechosos mediante investigaciones basadas en IP, véase: *Gercke*, Preservation of User Data, Datenschutz und Datensicherheit, 2002, página 577 y ss.

[335] *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, 2002, disponible en: http://www.citeulike.org/user/alexbdigital/article/80546.

[336] Respecto de los instrumentos necesarios, véanse: *Gercke*, Understanding Cybercrime…, *supra* núm. 26, capítulo 6.2. La conservación de datos es una de las soluciones que más se examina. En cuanto a las posibilidades y los riesgos que entraña la conservación de datos, véase: *Allitsch*, Data Retention on the Internet–A measure with one foot offside?, *Computer Law Review International 2002*, página 161 y ss.

[337] Una lista completa de los países que han firmado y ratificado el Convenio del Consejo de Europa sobre el delito cibernético (STE 185) se encuentra disponible en: http://www.conventions.coe.int.

Artículo 16 del Convenio del Consejo de Europa sobre el delito cibernético de 2001

Conservación inmediata de datos informáticos almacenados

1) Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

2) Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos –que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente- durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3) Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4) Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Como el principio fundamental de la soberanía nacional limita la capacidad de llevar a cabo investigaciones fuera del territorio, el país B no puede utilizar este instrumento para obligar al proveedor del alojamiento a conservar los datos informáticos.

Recomendación práctica

La única disposición del Convenio que permitiría una interacción directa entre las autoridades encargadas de hacer cumplir la ley en el país B y el proveedor de servicio registrado que opera en el país A es el artículo 32, inciso *b)*, del Convenio sobre el delito cibernético. Este permite a las fuerzas del orden acceder a los datos informáticos almacenados fuera de su territorio (tal como la información de los archivos de registro), si los investigadores han obtenido el consentimiento legítimo y voluntario de la persona que tiene autoridad legal para revelar esos datos. Esta autorización es muy criticada[338]. Existen buenos argumentos en contra de esta norma. El más destacado es el hecho de que al establecer la segunda exención, los redactores del Convenio contravienen la estructura dogmática del régimen de asistencia judicial recíproca en el Convenio[339].

En cambio, es necesario que el país B haga referencia a los procedimientos definidos en el artículo 29 del Convenio sobre el delito cibernético.

[338] Informe de la Segunda reunión del Comité del Convenio sobre el delito cibernético, T-CY (2007) 03, página 2, disponible en: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2007)%2003%20E.pdf.

[339] Para más detalles, véase: Gercke, Understanding Cybercrime…, *supra* núm. 26, capítulo 6.3.

Artículo 29 – Conservación inmediata de datos informáticos almacenados

1. Las Partes podrán ordenar o imponer de otro modo la conservación inmediata de datos almacenados en sistemas informáticos que se encuentren en su territorio, en relación a los cuales el Estado requirente tiene intención de presentar una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

2. Una demanda de conservación formulada en aplicación del párrafo 1 deberá contener:

a) la identificación de la autoridad que solicita la conservación;

b) la infracción objeto de investigación con una breve exposición de los hechos vinculados a la misma;

c) los datos informáticos almacenados que deben conservarse y su vinculación con la infracción;

d) todas aquellas informaciones disponibles que permitan identificar al responsable de los datos informáticos almacenados o el emplazamiento de los sistemas informáticos;

e) justificación de la necesidad de conservación; y

f) la acreditación de que el Estado requirente está dispuesto a formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

3. Después de recibir la demanda, el Estado requerido deberá adoptar las medidas necesarias para proceder sin dilaciones a la conservación de los datos solicitados, conforme a su derecho interno. Para hacer efectiva la demanda de conservación no resultará condición indispensable la doble incriminación.

[…]

Recomendación práctica

En vista de la urgencia de la solicitud, debería considerarse la utilización de la red 24/7 que opera de manera ininterrumpida. A fin de mejorar la eficacia de las solicitudes de asistencia recíproca, el Convenio obliga a los Estados Parte a que designen un punto de contacto para que se encargue de las solicitudes y que se encuentre disponible de manera permanente[340]. Este contacto es necesario dado que los dos países en este caso firmaron y ratificaron el Convenio. Los encargados de preparar un borrador del Convenio hicieron hincapié en que el establecimiento de puntos de contacto era uno de los instrumentos más importantes previstos en el Convenio sobre el delito cibernético[341]. El documento de debate titulado "The Functioning of 24/7 Points of Contact for Cybercrime" del Consejo de Europa de 2009 incluye una lista de comprobación de solicitudes para la conservación expedita de datos informáticos, el cual puede verse en: http://www.coe.int/cybercrime/.

En el artículo 29 se prevé un mecanismo a nivel internacional equivalente al que se estipula en el artículo 16 de aplicación a nivel nacional. Este mecanismo, al tiempo de ser más rápido que la práctica común de asistencia recíproca, resulta también menos intrusivo. Los

[340] La disponibilidad las 24 horas del día y los 7 días de la semana es especialmente importante con respecto a la dimensión internacional del delito cibernético, ya que las solicitudes pueden provenir de regiones del mundo con diferentes husos horarios.

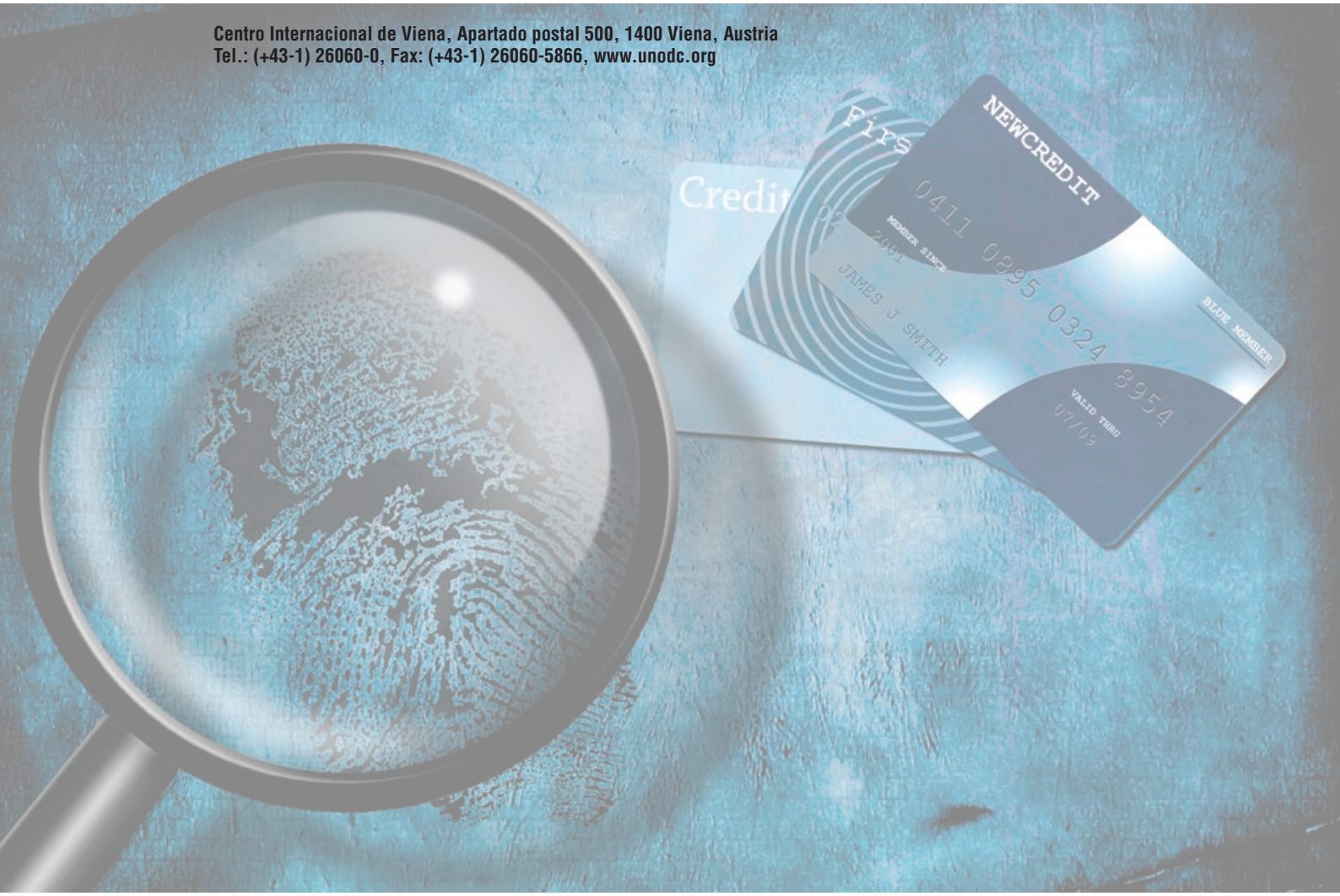
[341] Véase el informe explicativo del Convenio sobre el delito cibernético, *supra* núm. 157, párrafo 298.

funcionarios de asistencia recíproca de la Parte requerida no están obligados a obtener los datos de su custodio. Se da preferencia al procedimiento para que la Parte requerida garantice que el custodio (con frecuencia se trata de un proveedor de servicio o un tercero) conserve (es decir, que no elimine) los datos a la espera de que se inicie el proceso que requiere que sean entregados a los funcionarios encargados de hacer cumplir la ley en una etapa posterior. La ventaja de este procedimiento es que es rápido y protege la intimidad de la persona a quien pertenecen los datos, ya que estos no serán revelados o sometidos a análisis por parte de ningún funcionario hasta que los criterios para su divulgación, de conformidad con los regímenes normales de asistencia recíproca, se hayan cumplido. Al mismo tiempo, se permite a la Parte requerida el empleo de otros procedimientos para garantizar la conservación rápida de datos, incluida la emisión expeditiva y la ejecución de una orden de producción o de registro de los datos. Para evitar la pérdida irreversible de los datos es requisito fundamental contar con un proceso extremadamente rápido que se encuentre en vigor[342].

[342] *Ibid.*, párrafo 283.

UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

Centro Internacional de Viena, Apartado postal 500, 1400 Viena, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org



V.13-83700—Noviembre de 2013