Página inicial: 61 Página final: 78

LA LUCHA CONTRA EL HURTO DE IDENTIDAD:

LAS DIFERENTESPERSPECTIVAS LEGISLATIVAS*

Por: Dr. Iván Salvadori, LL. M.**

Resumen:

El presente artículo busca hacer un estudio sobre la definición del delito de hurto de identidad así como sobre las diversas conductas que componen este delito para posteriormente analizar los diferentes enfoques legislativos que se le han dado este problema en algunos ordenamientos jurídicos.***

Palabras Clave:

Delitos Informáticos; Hurto de Identidad; Tipicidad; Obtención Ilícita de Datos.

Abstract:

This article offers a study on the definition of identity theft as well as on the various behaviors that integrate this crime to further analyze the different legislative approaches given to this problem in several legal systems.

Key Words:

Cybercrime; Identity Theft; Typification; Unlawful Acquisition of Data.

Sumario:

*Artículo presentado para una investigación llevada conjuntamente por la Agencia de Protección de Datos, la Sociedad Internacional de Derecho Penal y el Instituto de Derecho Penal Europeo e Internacional de la Universidad de Castilla la Mancha, publicado previamente en el libro "Robo de Identidad y Protección de Datos", Cizur Menor: Aranzadi, (2010).

**Licenciado en Derecho por la Università di Trento (Italia), Magíster en Derecho Penal y Ciencias Penales de la Universidad de Barcelona y de la Universidad Pompeu Fabra (España), Doctor en Derecho y Economía de la Empresa de la Università di Verona (Italia). Profesor e investigador en derecho penal informático de la Università de Verona. Página de internet: www.ivansalvadori.net. E-Mail: ivan.salvadori@univr.it

***Resumen agregado por la editora.

I. Introducción.

Tal como ponen de manifiesto recientes estudios realizados por destacados centros de investigación, el hurto de identidad representa actualmente un fenómeno de masas en continua expansión, no sólo en los Estados Unidos de América sino también en Europa.[1] Según la Federal Trade Commission cerca de diez millones de ciudadanos americanos cada año son víctimas de un hurto de identidad.[2] Se calcula que los ID-crime causan anualmente a las empresas y a los consumidores americanos daños por un valor de alrededor de cincuenta billones de dólares.[3] El hurto de identidad también representa una seria amenaza para la economía inglesa. Según los datos suministrados por Home Office Identity Fraud Steering Committee las pérdidas económicas debidas al identity theft superan cada año el billón de libras esterlinas.[4]

Resultan también notables los costes directos para los consumidores.[5] Un estudio reciente ha calculado que las víctimas pierden de media cincuenta y ocho horas para resolver los problemas causados por el identity theft.[6] El hurto de identidad ocasiona igualmente daños considerables a las empresas y comercios en términos de «consumer confidence»,[7] obligándolas a instalar sofisticados software para proteger los propios sistemas informáticos y telemáticos y adoptar medidas preventivas técnico-organizativas idóneas. Estas medidas son necesarias no sólo para reducir los

[1] FTC, 2006 Identity theft Survey Report, disponible en http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf; ITU, Understanding Cyber-crime: A Guide for Developing Countries, Draft, April 2009, 160, disponible en http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf. En relación a la situación en Europa v. VAN DER MEULEN, N., The Spread of Identity Theft: Developments and Initiatives within the European Union, 2007, en http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1190&issue_id=52007.Para la Federal Trade Commission (FTC) el hurto de identidad cuesta a los consumidores y a las empresas 50 billones de dólares al año; al respecto vd. Putting an End to Account-Hijacking Identity theft, disponible al sitio http://www.ftc.gov.

[2] FTC, Identity Theft Focus of National Consumer Protection Week, 2005, disponible en http://www.ftc.gov/opa/2005/02/ncpw05.shtm. Sustancialmente análogos son los datos ofrecidos por JAVELIN STRATEGY & RESEARCH, 2006, Identity Fraud Survey Report,January, 2006, 4, aunque este instituto de investigación, en contradicción con la mayor parte de los estudios sobre el hurto de identidad, afirma que en los últimos años el fenómeno está en disminución.

[3] DEPT OF JUSTICE, A National Strategy to Combat Identity Theft, 2006, 1 ss., disponible en http://www.cops.usdoj.gov/files/ric/Publications/e03062303.pdf

[4] HOME OFFICE IDENTITY FRAUD STEERING COMMITTE: Identity theft, Don 't become a victim, disponible en http://www.identitytheft.org

[5] MITCHISON, N.; WILIKENS, M.; BREITENBACH, L.; URRY R; PORTESI, S., Identity Theft. A Discussion Paper; 2004, 9, disponible en https://www.prime-project.eu/community/furtherreading/ studies/IDTheftFIN.pdf

[6] ITRC, Identity theft: the Aftermath 2008, disponible en http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf

[7] MITCHISON, N.; WILIKENS, M.; BREITENBACH, L.; URRY R; PORTESI, S., Identity Theft. A Discussion Paper; 2004, 5, disponible en la página https://www.prime-project.eu/community/furtherreading/ studies/IDTheftFIN.pdf

ataques procedentes del exterior, los llamados «outsiders» (hacker, cracker, delincuentes informáticos, terroristas, etc.), sino también los ataques cometidos por los llamados «insider», es decir, de empleados, colaboradores, y dirigentes deshonestos, que muy a menudo acceden de manera abusiva a los sistemas informáticos de las empresas para sustraer datos de diferente naturaleza (personales, sensibles, secretos).[8]

Pese a que la «cifra oscura» continúa siendo muy elevada, cada vez hay más denuncias de usuarios víctimas de hurto de identidad.[9] Según los datos de la Federal Trade Commission, las denuncias relativas a los episodios de fraude han sido de ochocientas mil durante 2007.[10] De éstos, el 32% han sido concernientes a casos de ID-crimes.

Aunque los estudios estadísticos y criminológicos están en constante aumento, no existe aún una definición generalmente aceptada del identity theft.[11] No se trata de una simple cuestión nominal. De la determinación precisa de las conductas de identity theft depende, sobre todo, la decisión acerca de si resulta preciso introducir en los ordenamientos jurídicos nuevas y específicas figuras delictivas. Igualmente delimitar este concepto resulta un presupuesto necesario no sólo para establecer las dimensiones reales del fenómeno sino también para estimar su relevancia económica.

Dados los límites de este trabajo, a continuación se analizarán las principales definiciones de hurto de identidad elaboradas en diversos centros de investigación y organismos internacionales, y las contenidas en algunos ordenamientos jurídicos nacionales (par. 2). Después se estudiarán individualizadamente las diversas fases a través de las cuales puede ser cometido un hurto de identidad en el espacio cibernético (par. 3), a partir de estos resultados analizaré si, de jure condito, las ordenamientos nacionales contemplan ya esta nueva amenaza. En particular, se mostrará en este punto el diferente enfoque legislativo adoptado para atajar este problema que existe entre los Estados Unidos de América, tanto a nivel federal como estatal (par. 3.1), y en Europa (par. 3.2.). A la luz de los resultados de este análisis comparado se formularán de jure condendo, algunas breves consideraciones finales (par. 4).

II. La Definición de Hurto de Identidad.

Los organismos internacionales que se ocupan del fenómeno del hurto de identidad rara vez han definido el concepto de identity theft. Su definición también varía notablemente entre sistemas de common law y civil law. Si en la mayor parte de los Estados Unidos de América la gran mayoría de la literatura utiliza «identity theft», en Gran Bretaña se emplea con más frecuencia el término de «identity fraud».[12] En los países francófonos en lugar de identity theft se utiliza la expresión de «vol

[8]Sobre este tema vid. los datos ofrecidos por CSI, Computer Crime & Security Survey, 2008, según el cual, si bien en el 2008 los abusos cometidos por los insider se han disminuido de manera notable, respecto del año anterior, siguen siendo la segunda amenaza para la seguridad de las empresas después de la difusión de los programas de virus.

[9]V. OECD, Online Identity theft, 2009, 34-35, disponible en la página http://www.oecd.org. Sobre las causas principales de la llamada «cifra negra» v. NEWMAN, C. R; McNALLY, M. M., Identity Thejt Literatwti Review, 2005, 7, disponible en la página http://www.ncjrs.gov/pdffilesl/nij/grants/210459.pdf

[10]FTC, Consumer Fraud and Identity Theft Complaint Data, January-December 2007, 3.

[11]V. MITCHISON, N., WILIKENS, M., BREITENBACH, L., URRY, R., PORTESl, S., Identity Theft, cit., 22; Cfr. Koops, B.J., LEENES, R., «Identity theft, Identity fraud and/or Identity related crime», DuD, núm. 30, 2006, 9, 553-556, que partiendo de la dificultad de definir el concepto de identity theft, prefiere hablar, de manera más general, de identity-related crime.

[12]En referencia a los diferentes enfoques utilizados a nivel nacional para definir el concepto de identity theft v. PAGET, Identity theft- McAffe White Paper, 2007, pg. 15.

d'identitè» o «usurpation d'identitè». Muy a menudo se nos refiere el fenómeno del hurto de identidad utilizando de manera indiferente expresiones tales como «phishing»[13] o «account takeover».

Según la definición aportada por Home Office Identity Fraud Steering Committee del Reino Unido, el hurto de identidad consiste en la recogida de información relativa a la identidad de una persona con el fin de cometer un fraude de identidad (identity fraud), prescindiendo del hecho de que la víctima sea una persona viva o fallecida.[14] La identity theft consiste por tanto en la apropiación indebida («misappropriation») de la identidad o de cualesquiera otros datos personales (por ej., fecha de nacimiento, dirección de casa, etc.)[15] sin el consentimiento del interesado. Esta definición es substancialmente similar a la aportada por el CIFAS, organismo asentado en Inglaterra que se ocupa de la lucha por el fraude de identidad. Según esta definición, el hurto de identidad consiste en la apropiación de la identidad de una persona sin su consentimiento con el fin de obtener ventajas y servicios.[16] Ambas definiciones resultan muy limitadas, en cuanto que sólo toman en consideración la obtención no autorizada de datos e información relativa a otra persona con el fin de cometer un fraude o de conseguir de manera indebida una ventaja o un servicio, pero dejan de lado las conductas de apropiación de datos personales ajenos realizados con el fin de cometer otros delitos o ilícitos diversos (p. ej., revelaciones de secretos, falsificaciones de datos, difusión de spam, malware, etc.).

Son pocas las legislaciones nacionales que en la actualidad definen expresamente el hurto de identidad.[17] De acuerdo con § 15 U.S.C. 1681 a (q) (3) de los Estados Unidos de América, el identity theft consiste en la utilización sin autorización de informaciones relativas a la identidad de otra persona para cometer un fraude.[18] Al igual que ocurre con las definiciones anteriores, ésta puede resultar demasiado limitada desde el momento que cubre sólo aquellos comportamientos instrumentales para la comisión del fraude. Mucho más precisa es la definición aportada, también en Estados Unidos, por la Identity Theft and Assumption Deterrence Act (Identity Theft Act).[19] De acuerdo con el § 18 USC 1028 (a) (7) comete hurto de identidad «quien transfiere, posee o utiliza, sin autorización, datos identificativos de otra persona con la intención de cometer; intentar o favorecer cualquier actividad

[13]Sobre la relevancia del phishing en la experiencia jurídica italiana v. FLOR, R., «Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente», in Riv. it. dír. proc. pen., 2007, 899 y ss, y sus referencias bibliográficas.

[14]HOME OFFICE IDENTITY FRAUD STEERING COMMITTEE, «Identity Theft occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead».

[15]El concepto de datos personales se utiliza normalmente, en un sentido amplio, con el fin de abarcar cualquier información concerniente a una persona física identificada o identificable. En este sentido véase la noción de dato personal que se encuentra en el art. 2 (a) de la Directiva 95/46/CE, relativa a la tutela de las personas físicas referidas al tratamiento de los datos personales así como a la libre circulación de los mismos.

[16]CIFAS: «Identity Theft - (also known as impersonation fraud) is the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name», disponible en la página http://www.cifas.org.uk/default.asp?ediUd=561-56.

[17]OECD; Online Identity Theft, cit. 47.

[18]§ 15 USC 1681a (q) (3): «The term "identity theft" means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation».

[19]Identity Theft and Assumption Deterrence Act, as amended by Public Law 105-318, 112 Stat. 3007 (oct. 30, 1998), disponible en la página http://www.ftc.gov/os/statutes/itada/itadact.htm.

ilícita que constituya una violación del derecho federal o que constituye un delito de acuerdo a las leyes estatales o de derecho federal».[20] Sustancialmente análoga resulta la definición elaborada recientemente por los expertos de la OECD, según la cual existe hurto de identidad cuando un sujeto sin autorización obtiene, transfiere, posee o utiliza datos personales de una persona física o jurídica con el fin de cometer, o en conexión con, un fraude u otro delito.[21]

III. Las Tres Fases del Hurto de Identidad.

Tal como se deriva de este breve análisis, de las definiciones principales de hurto de identidad, no existe consenso alguno sobre su concepto. Algunas hacen coincidir el hurto de identidad con la obtención o la apropiación ilícita de datos e informaciones personales ajenas. Más si el hurto de identidad se circunscribiera a un mero comportamiento de empoderamiento no autorizado de informaciones ajenas mediante instrumentos informáticos no existiría necesidad alguna de introducir una norma ad hoc para reprimir este fenómeno.[22] De hecho, podría ser subsumido por el tipo penal de espionaje de datos, conducta que se sanciona penalmente en algunos ordenamientos nacionales.[23] Resulta paradigmático en este sentido el veterano tipo penal de espionaje de datos («Ausspähen von Daten»), introducido por el legislador alemán en el código penal a través de la Ley Segunda para la lucha contra la criminalidad económica (2. WiKG) del 1986.[24] El § 202a StGB, recientemente modificado por la 41 Ley de reforma del Código Penal[25] de 2007, castiga con pena de reclusión de hasta tres años o con la multa a «quien sin autorización se procura datos, no dirigidos a él y que están especialmente protegidos frente a un acceso indebido, superando las barreras de acceso».[26] Las otras definiciones de hurto de identidad se focalizan, en cambio, en la utilización ilícita, por parte del delincuente informático, de las informaciones personales ajenas para cometer un fraude u otra actividad ilícita. En estos casos, el hurto de identidad no asume una relevancia penal autónoma, configurándose como una conducta instrumental para la comisión de un fraude o de otros delitos. Tal como ha indicado la doctrina, los actos ilícitos realizados en la fase siguiente a la de obtención de datos e informaciones relativas a la identidad de otra persona, pueden ser abarcados en diferentes tipos de delitos (por ej. fraude informático, revelación de secretos, etc.).[27]

---

[20] § 18 USC 1028 (a) (7): «knowingly transfers or uses, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law».

[21] OECD, Online Identity Theft, cit., 16: «ID theft occurs when a party acquires, transfers, possess or uses personal information of a natural or legal person in an unauthorized manner with the intent to commit, or in connection with, fraud or other crimes».

[22] En este sentido véase GERCKE M., Internet-related identity-theft, cit., 13. en referencia a las principales técnicas de espionaje de los datos vid. ITU, Understanding Cyber crillle: A Guide for Developing Countries, Draft, april 2009, 23 y ss., disponible en la página http://www.itu.org.

[23] Sobre este tema vid. ITU, Understanding Cyber crime, cit., 118 – 120.

[24] Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), 15.5.1986.

[25] Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (41. StrÄndG), 11.08.2007

[26] § 202a, comma 1, StGB: "Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft". Para un comentario § 202a StGB v. HILGENDORF, E., FRANK, T., VALERIUS, B., Computer und Internetstrafrecht, Berlín, Heidelberg, 2005.

[27] En este sentido véase GERCKE M., Internet-related identity-theft, cit., 13.

Mucho más amplio es el enfoque seguido por el legislador federal estadounidense, que incluye en el hurto de identidad una serie de conductas «intermedias», ubicadas tras la primera fase de obtención de los datos personales ajenos, y la última de utilización de los mismos para cometer un fraude u otra actividad ilícita Il § 18 USC 1028(a)(7). El legislador norteamericano criminaliza, de hecho, no sólo la utilización de los datos de identificación de otra persona con el fin de cometer un delito sino también la transferencia y la mera posesión de los mismos datos.

De las definiciones mencionadas se deriva que el hurto de identidad coincide substancialmente con una o más de las siguientes fases: obtención de informaciones personales (primera fase); posesión y/o la venta de información (segunda fase); utilización de información para cometer actividades ilícitas (tercera fase).[28]

Las modalidades a través de las cuales un delincuente informático puede procurarse de manera ilícita datos e información que conciernen a la identidad de otra persona resultan muy diversas.[29] Tal como demostró la encuesta realizada por el Computer Security Institute (CSI) uno de los métodos más tradicionales para la obtención de datos personales es el hurto de un ordenador o de soportes de almacenamientos ajenos (USB, CD-ROM, DVD, etc.).[30] Otra técnica muy utilizada es el denominado «trashing» («dumpster diving» o «bin raiding»), consistente en buscar dentro de la papelera documentos (como, por ejemplo, tickets de compra, extractos de la cuenta corriente, recibos emitidos por los correos electrónicos, etc.) que permiten directa o indirectamente obtener datos personales y sensibles de otra persona.

La delincuencia informática está a la vanguardia de las nuevas tecnologías para procurarse informaciones personales ajenas en el ciberespacio. Paradigmáticas en este punto son las técnicas de «search engines» (como p. ej. «googlehacking» o el «googledork»), consistentes en la utilización de la enorme potencia de los motores de búsqueda para recoger información (datos personales, dirección de mail, número de la tarjeta de crédito, password, códigos de acceso, etc.), contenida normalmente en páginas web, chat-room, blog e social networks (como p. ej. Facebook, Twitter, Myspace, etc.).[31] Cada vez es más frecuente también la utilización de sofisticadas técnicas de social engineering (como p. ej. el phishing, el pharming, el smishing, el vishing, etc.).[32]

[28]En la doctrina, véase por todos GERCKE M., lnternet-related identity-theft, cit., 13, según el cual «the only consistent element of the identity theft definitions is therefore the fact, that the conduct is related to one or more of the fol1owing phases: act of obtaining identity-related information; act of possessing or transferring the identity related information; act of using the identity-re1ated information for criminal purposes»; ITU, Understanding Cyber-crime, cit., 161. Análogamente v. SEGER, A., Identity theft and the Convention on Cybercrime, in UN-ISPAC, Conference on the Evolving Challenge of identity-related Crime (Atti del Convegno di Courmayer, 30.11-2-12 2007). Parcialmente similar es la tripartición del identity theft propuesta por NEWMAN, C. R., McNALLY, M. M., Identity Theft, cit., 6, que distinguen entre «Acquisition», «Use» e «Discovery». Consideran que el hurto de identidad pueda ser descompuesto en cuatro fases (fishing for data; misappropriation; misuse y criminal action) MITCHISON, N., WILIKENS M., BREITENBACH L., URRY R., PORTESI S., Identity Theft, cit., 21.

[29]Sobre este tema véase VICTOR, G. M., Identity theft, its environment and proposals for change, 18 Loy. Consumer L. Rev., 2006, 276; TOWLE, H. K., Identity theft: myths, methods, and new law, 30 Rutgers Computer & Tech. L.J., 2004, 247 y ss.

[30]CSI, Computer Crime & Security Survey, 2008, 16; v. tambien McAFFE, Identity Theft, White Paper 2007, 5.

[31]Sobre los peligros para la identidad de los internautas que pueden derivar de un uso incorrecto de las redes sociales v. GARANTE PRIVACY, Social networks: attenzione agli effetti collaterali, disponible en la página http://www.garanteprivacy.it/garante/docJsp?ID=1614258.

[32]Acerca de las principales técnicas de social engineering empleadas por la delincuencia informática con el fin de obtener ilícitamente datos de otro v. OECD, Online Identity Theft, cit., 22-28; McAFFE, Identity theft, cit., 7.

Otra modalidad empleada por los cracker con el fin de obtener datos de diversa índole (personales, secretos, etc.) es introducirse de manera abusiva en los sistemas informáticos y en las redes telemáticas ajenas o de difundir en red programas malware y spyware, que una vez instalados en el computer por parte de los usuarios más descuidados permiten a los ciber-delincuentes obtener el control remoto de las máquinas «infectadas».

Una vez obtenidos los datos y las informaciones relativos a la identidad ajenas los cyber criminals pueden transferirlos o venderlos a otros posibles infractores u organizaciones criminales o bien utilizarlos directamente para cometer otros delitos, para adquirir mercancías, productos o servicios, para difundir en la red programas de malware (virus, worm, etc.) o spam,[33] o para crear nuevas cuentas de correo electrónico etc. En este momento se trata de evaluar si, de jure condito, en los ordenamientos jurídicos nacionales existen ya normas idóneas para castigar en todo o en parte los comportamientos reconducibles a alguna de las tres fases en las que se articula el hurto de identidad, es decir, la obtención, la transferencia y posesión, y la utilización de informaciones personales de terceros con el fin de realizar un comportamiento ilícito.

IV. La Lucha Contra el Hurto de Identidad. Aspectos de Derecho Comparado.

a. La Experiencia Jurídica en Los Estados Unidos.

Los Estados Unidos han sido el primer país del mundo en introducir una norma penal ad hoc con el fin de castigar el hurto de identidad. En 1988 el Congreso aprobó la Identity Theft and Assumption Deterrence Act (Identity Theft Act) con el objetivo de modificar el Título 18 del US Criminal Code relativo a los fraudes y otras actividades conexas con los documentos de identificación y la información. En concreto la Identity Theft Act ha modificado el § 18 USC 1028 (a)(7), castiga «a quien transfiere, posee o utiliza sin autorización, medios de identificación de otra persona con la intención de cometer, intentar o favorecer cualquier actividad ilícita que constituye una violación de un derecho federal o que constituye un delito de acuerdo con las leyes estatales o federales».[34] Con la Identity Theft Penalty Enhancement Act de 2004[35] el legislador federal estadounidense introdujo en el § 18 USC 1028 (a)(1) un tipo penal agravado de identity theft que castiga «a quien durante y en relación con uno de los delitos graves previstos en la subsección c), de forma intencional transfiera, posea o utilice, sin autorización, medios de identificación de otra persona».[36]

La totalidad de los cincuenta estados americanos tienen hoy una legislación penal ad hoc para sancionar el identity theft,[37] con una formulación típica similar. Las ID-theft State law sancionan principalmente las conductas de obtención, adquisición, transferencia, posesión y utilización de

[33]En relación a la relevancia penal de la difusión de malware y spam en la red en la experiencia italiana v. SALVADORI, I., «Hacking, cracking e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive de jure condendo», en Cyberspazio e diritto, núm. 3, 2008, 329 y ss.

[34]§ 18 USC 1028 (a)(7): «knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law».

[35]Identity Theft Penalty Enhancement Act, Public Law 108-275, 15 June 2004.

[36]§ 18 USC 1028A (a) (1): «Whoever, during and in relation to any felony violation enumerated in subsection (e), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years».

[37]The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, 2007, 53, disponible en la página http://www.identitytheft.gov/reports/StrategicPlan.pdf. Un elenco detallado de los ID Theft State laws está disponible en http://www.ncsl.org/?tabid=12535.

informaciones personales para cometer o intentar cometer un fraude u otra actividad ilícita. A este respecto resulta paradigmático el § 530.5 (a) del Código penal el Estado de California, que castiga a quien «de forma intencional obtiene informaciones personales relativas a otra persona y la utiliza para cualquier actividad ilícita o para obtener o intentar obtener bienes, servicios, ventajas económicas o informaciones médicas sin el consentimiento del interesado».[38] El § 530.5 (c) (1) castiga además la conducta de quien con el fin de defraudar adquiere, transfiere o posee datos e informaciones relativas a otra persona.[39]

El § 530.55 (a) ofrece una definición muy amplia de «datos de identificación personal» (personal identifying information) que abarca, por ejemplo, número PIN, passwords, números de teléfono, dirección, número de las tarjetas de crédito, fecha de nacimiento, número del pasaporte, etc.

[38] § 530.5 (a) California Penal Code: «every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person».

[39] § 530.5 (e) (1) California Penal Code: «Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information of another person, and who has previously been convicted of a violation of this section upon conviction therefore shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison». Para un comentario de la legislación de California sobre identity theft v. DAVIS, L. M., With or without authorization, it's still identity theft, 33, McGeorge L. Rev., 2002, 231y ss.

[40] § 530.55 (a) California Penal Code: "For purposes of this chapter, "personal identifying information" means any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person, or an equivalent form of identification».

[41] § 13-2008 (a) Ariz. Rev. Stat.: «A person commits taking the identity of another person or entity if the person knowingly takes, purchases, manufactures, records, possesses or uses any personal identifying information or entity identifying information of another person or entity, including a real or fictitious person or entity, without the consent of that other person or entity, with the intent to obtain or use the other person's or entity's identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense, or with the intent to obtain or continue employment». El legislador de Arizona fue el primero en introducir una legislación estatal ad hoc en materia identity theft. Al respecto v. PASTRIKOS, C., Identity Theft Statutes: Which will Protect Americans the Most?, 67, Alb. L. Rev., 2004, 1138. Un comentario de la legislación del Estado de Arizona puede verse en v. GONZÁLEZ, E. M., The new Arizona Data Security Breach Law: a Step in the Right Direction, but Unlikely to Prevent Identity Theft: or Compensate Consumers, 40 Niz. St. LJ., 2008, 1349 y ss.

[42] § 817.568 Fla. Stat. Ann.: «Any person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent, commits the offense of fraudulent use of personal identification information, which is a felony of the third degree».

[43] § 32.51 (b) Texas Penal Code: «a person commits an offense if the person, with intent to harm or defraud another, obtains, possesses, transfers, or uses identifying information of: (1) another person without the other person's consent; or (2) a child younger than 18 years of age».

Muy similares son las formulaciones legislativas de los tipos penales de identity theft previstas en Arizona,[41] Florida[42] y Texas.[43]

La elección político criminal de introducir una norma ad hoc en materia de hurto de identidad resulta acertada en cuanto que abarca todos los actos reconducibles a las tres fases mencionadas mediante las que se realiza el hurto de identidad tanto en el mundo real, como en el virtual.[44]

La división entre las conductas típicas de transferencia de datos y de otras informaciones permite castigar gran parte de los comportamientos reconducibles a la primera fase del hurto de identidad.[45] Con todo no se incluyen en el área penalmente relevante aquellas hipótesis en las que la transferencia de la información se realiza por obra de la propia víctima, como ocurre por ejemplo en la utilización de técnicas sofisticadas de social engineering que permite al delincuente informático obtener directamente del usuario sus datos personales.[46] Igualmente todos los actos que conforman la segunda fase del hurto de identidad son penalmente relevantes, al poder ser subsumidos en la conducta típica de la posesión de información personal relativa a otra persona. El castigo, finalmente, de la utilización de datos e información personal para realizar un delito, permite sancionar las conductas que se incluyen en la tercera fase del hurto de identidad [§ 18 USC 1028 (a) (7)].

b. La Aproximación Legislativa Europea.

La aproximación legislativa efectuada por la mayoría de los países europeos en la lucha contra el fraude de identidad es diversa a la de los Estados Unidos. En Europa ningún ordenamiento jurídico nacional contiene una norma penal ad hoc para castigar el identity theft.[47] Igualmente el Convenio sobre cybercrime del Consejo de Europa, que ha sido tomado como modelo por numerosos Estados miembros (como por ejemplo, Alemania, Austria, Italia, Bélgica, Francia, Rumania, etc.) para implementar las normas penales nacionales relativas a la criminalidad informática, no contiene un tipo penal específico de hurto de identidad, y lo mismo cabe indicar de la Decisión marco de la UE 2005/222/JAI sobre ataques a sistemas de información.[48]

Esta carencia de normas no significa sin embargo que el hurto de identidad no sea penalmente relevante en Europa. La mayor parte de los ordenamientos jurídicos contienen normas penales que permiten sancionar casi todos los comportamientos incluidos en alguna de las tres fases en las que se articula el hurto de identidad cometido mediante la utilización de tecnología informática.[49]

---

[44]GERCKE M., Internet-related identity-theft, cit., 20; ITU, Understanding Cyber Crime, cit., 161.

[45]En este sentido v. GERCKE M., Internet-related identity-theft, cit., 21.

[46]Sobre las principales técnicas de social engineering empleadas por la delincuencia informática con el fin de obtener datos personas de terceros v. OECD, Online Identity theft, cit., 22-28.

[47]MITCHISON N., WILIKENS M., BREITENBACH L., URRY R., PORTESI S., Identity Theft, cit., 23; OECD, Online Identity Theft, cit., 47.

[48]Un análisis comparativo de la Convención cybercrime y la Decision marco 2005/222/JAH v. DE HERT P., GONZALES G.F., KOOPS, B.J., «Fighting Cyber-crime in the two Europes: the Added Value of the EU Framework Decision and the Council of Europe Convention», International Review of Penal Law, 77 (3-4), 2007, 503 y ss.

[49]MITCHISON N., WILIKENS M., BREITENBACH L., URRY R., PORTESI S., Identity Theft, cit., 24.

[50]En la doctrina vid. por todos GERCKE M., Internet-related identity-theft, cit., 22-25, quien considera que parte de los comportamientos reconducibles a la primera fase del hurto de identidad pueden ser subsumidos también en el tipo de data interference o de system inteference.

En relación a la primera fase, la obtención ilícita de datos e informaciones personales de un tercero, resultan de aplicación los tipos penales de acceso abusivo a sistemas informáticos y de interceptación de datos de información.[50] Puede servir como ejemplo la conducta del cracker que, después de introducirse abusivamente en un sistema informático, obtiene datos memorizándolos o la conducta de invito domino a través de la que se instalan en el sistema informático de un tercero programas, por ejemplo, de Spyware (como por ejemplo Trojan Horse, Keylogger; Sniffer, etc.) con el fin de interceptar las comunicaciones electrónicas y apoderarse ilícitamente de datos (personales, sensibles, secretos) pertenecientes a una tercera persona.

Al día de hoy son numerosos los legisladores nacionales europeos, que con el fin de cumplir con obligaciones supranacionales, en particular las del Convenio sobre cybercrime del Consejo de Europa, han introducido normas ad hoc que castigan el acceso abusivo a sistemas informáticos y la interceptación de datos informáticos.[51] En este sentido resulta paradigmática la reciente reforma alemana, mediante la 41 Ley de reforma del Código Penal de 2007 que además de modificar el § 202 a del StGB con el objeto de sancionar a quien obtiene sin autorización y violando las medidas de seguridad, el acceso a datos de los que no es el destinatario y que están protegidos específicamente contra el acceso, al que no tiene derecho, ha introducido en el 202b un nuevo tipo penal ad hoc para sancionar la interceptación de datos informáticos. El nuevo § 202b StGB castiga a «quien sin autorización se procura datos, no dirigidos a él y que están especialmente protegidos frente a un acceso indebido, superando las barreras de acceso».[52]

Los comportamientos que se incluyen en la tercera fase del hurto de identidad, es decir, la utilización de datos y de la información para cometer un fraude u otra actividad ilícita no presentan especiales problemas en el terreno práctico. En estos casos, se puede aplicar, sin duda alguna, el tipo de fraude informático, de difusión de programas de software malicioso etc., eventualmente en la forma de tentativa.[53] Sin embargo, mayores problemas se presentan en relación a la incriminación de los actos (intermedios) de transferencia, detención y posesión ilícita de datos y de información personal de terceros. En estos supuestos, el ámbito de aplicación del tipo penal de mala utilización de dispositivos o (misuse of device) resulta demasiado exiguo para englobarlos a todos.

La mayor parte de los legisladores penales europeos que han implementado el artículo 6 del Convenio sobre Cibecrimen (CoC) relativo a actos de misuse of device amparándose en la reserva del

[51]En relación a las diversas técnicas de implementación del tipo de acceso abusivo interceptación de datos previstos respectivamente en los arts. 2 y 3 del Convenio cybercrime del Consejo de Europa por parte de las legislaciones nacionales v. PICOTTI, L., SALVADORI, I., «National legislation implementing the Convention on Cybercrime», Working paper disponible en la pagina http://www.coe.int.

[52]§ 202b StGB: «Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist». Un primer comentario de los nuevos tipos penales introducidos en el CP Alemán por la 41 Ley de reforma puede verse en SCHUMANN, K. H., Das 41. «StrÄndG zur Bekampfung der Computerkriminalität», in NStZ, 2007, 67; ERNST, S., «Das neue Computerstrafrecht», NJW, núm. 37, 2007, 2661 y ss.; GRÖSELING, N., HÖFINGER, F. M., Hacking und Computerspionage. Auswirkungen des 41. «StrÄndG zur Bekampfung der Computerkriminalität», MMR núm. 9, 2007, 549 y ss.

[53]En este sentido, GERCKE M., Intemet-Related identity-theft, cit., 26-27.

[54]En argumento v. PICOTTI, L., SALVADORI, I., National legislation, cit.

artículo 6, no han mantenido la sanción penal de la mera posesión de contraseñas, códigos de acceso u otros datos análogos que permitan acceder a un sistema informático.[54] Las normas nacionales castigan generalmente sólo la venta, la puesta a disposición y la difusión de dichos datos con la finalidad de cometer un delito CIA, esto es, un delito contra la privacidad, integridad y disponibilidad de los datos y del sistema informático (acceso ilícito, interceptación de datos informáticos, daños a los datos y a los sistemas informáticos). Estas normas resultan por tanto demasiado limitadas desde el punto de vista del elemento objetivo (al no hacer referencia a datos personales sino sólo a los códigos de acceso) y del elemento subjetivo (no estando previsto el fin de cometer un fraude informático sino sólo un delito CIA), para poder castigar la mera posesión de datos personales para cometer un fraude u otra actividad ilícita.

La transferencia, captura, posesión, recolección y más en general, el tratamiento no autorizado de datos e información relativa a la identidad de otra persona puede, no obstante, constituir una infracción a la normativa en materia de tutela de datos personales.[55] Ya con la Directiva 95/46/CE el legislador comunitario había establecido que para proceder de modo lícito a la recolección, conservación, en una palabra, al tratamiento de los datos personales era necesario obtener previamente el consentimiento de su titular [art. 7, letra. a)]. El artículo 2 (a) de la Directiva define de forma amplia el concepto de datos personales comprendiendo cualquier información relativa a una persona física identificada o identificable.[56] Tal definición resulta por tanto idónea para cubrir muchas de las informaciones y datos relativos a otros usuarios que los delincuentes informáticos pueden encontrar ilícitamente en la web (como, por ejemplo, direcciones e-mail, códigos fiscales, números telefónicos, fecha de nacimiento, número de tarjeta de crédito, etc.). La conducta del delincuente informático que procede a la recogida, conservación, elaboración o, en síntesis, el tratamiento de datos personales sin el consentimiento expreso del titular a cuyos datos se refieren, viola por tanto la normativa en materia de privacy. Resulta ilustrativa, en este sentido, la legislación italiana. El arto 167, inciso 1, del Decreto Legislativo 196/2003 relativo al Código en materia de protección de datos personales castiga con la pena de reclusión de 6 a 18 meses «a quien con el fin de obtener para sí o para otro un beneficio, u ocasionar un daño a un tercero, lleva a cabo el procesamiento de datos personales en violación de lo dispuesto en los artículos 23, 130 (...) si del hecho se deriva el perjuicio».[57] Por consiguiente, cuando el consentimiento del interesado no se ha rechazado previamente, el tratamiento de datos personales de otra persona, que se han obtenido en Internet, puede incluirse en el delito de tratamiento ilícito de datos personales del art. 167 del Decreto Legislativo 169/2003.[58]

---

[55]Sobre la legislación de los Estados miembros de la Unión Europea en materia de intimidad v. http://ec.europa.eu/ justice_home/fsj/privacy/.

[56]Art. 2 letra a.) «A los efectos de la presente Directiva, se entenderá por: "datos personales" toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

[57]Para un comentario al art. 167 del DLeg 196/2003, V. MANNA, A., «Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento di dati personali», en Dir. Inf. Inf., 2003, 745 y ss.; en el mismo sentido SALVADORI, I., «Il trattamento senza consenso di dati personali altrui reperibili su Internet costituisce reato?», en Dir.pen. proc., núm. 4, 2006, 458 y ss.

[58]Sobre este punto, acudimos a SALVADORI, I., «Il trattamento senza consenso di dati personali altrui», cit., 468 y ss.

[59]Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber-crime, COM (2007), 267.

V. Consideraciones Finales y Perspectivas de Jure Condendo.

En su reciente comunicación «Hacia una política general en la lucha contra la criminalidad informática», la Comisión Europea evidenció la necesidad de introducir a nivel europeo una normativa ad hoc para sancionar el hurto de identidad.[59] Del análisis de la aproximación legislativa que se ha adoptado en Europa en la lucha contra el hurto de identidad se deriva que, aunque existen muchas normas que pueden ser aplicadas para contrarrestar este fenómeno (como por ejemplo, el acceso abusivo a un sistema informático, la interceptación de datos informáticos, el abuso de dispositivos, el hurto informático, etcétera), éstas no resultan idóneas para cubrir todos los actos reconducibles a las tres fases sobre las que se sustancian los delitos ID.

Para colmar esta laguna y favorecer la cooperación entre autoridades enfrentadas sería deseable que los legisladores nacionales europeos introdujeran en sus respectivos ordenamientos una norma ad hoc para castigar el hurto de identidad.[60] A tal fin, se puede tomar como modelo el precepto de hurto de identidad del Código Federal estadounidense, al que antes hicimos mención [§ 18 USC 1028 (a) (7)]. Una previsión normativa como ésta, facilitaría la represión de las cada vez más frecuentes conductas de identity theft que se cometen no sólo en el mundo virtual o cyberspace, sino también en el mundo real.

No obstante, la elección por el legislador estadounidense de castigar también la mera posesión de datos e informes relativos a la identidad de otra persona produce una gran perplejidad. Según la doctrina más autorizada, la mera tenencia no constituye un comportamiento humano, ni positivo ni negativo, sino más bien, simplemente, «una situación individual que por sí misma no constituye una infracción de ningún precepto o prohibición penal, y que sólo resulta incriminada por las sospechas que levanta.[61]

Aunque se pueda sostener que tales críticas carecen de fundamento dada la existencia en este tipo de previsiones de una conducta exterior (en la forma de comisión y/o omisiva)[62] subsisten importantes dudas sobre la conformidad de una técnica de formulación normativa como ésta, con el principio de lesividad,[63] por anticipar de forma excesiva la consumación del delito, a una fase muy anterior a la verificación del resultado lesivo. La penalización de la mera posesión de los datos identificativos personales de una tercera persona representa una suerte de delito de peligro eventual

[60]En este sentido, v. también Communication from the Commission, COM (2007), 267.

[61]MANZINI, V., Trattato di Dir. Pen. It., vol. 1, V edición puesta al día (a cargo de P. NUVOLONE y G. D. PISAPIA), 1986, 460; v. también MARINUCCI, G., Il reato come azione, Milano, 1971, 167 y ss. En un sentido sustancialmente análogo, v., en la doctrina alemana, STRUENSEE, E., «Besitzdelikte», en SAMSON, E., DENCKNER, F., FRISCH, P., FRISTER, H., REIB, W. (Hrsg), Festschrift für Gerard Grünwald zum siebzigsten Geburstag, Baden-Baden, 1999, 713 y ss. Mantiene que el delito de posesión es inconstitucional ya que no incrimina ningún comportamiento humano LACODNY, O., Strafrecht vor den Schranken der Grundrechte, Tübingen, 1996, 323, ed. especialmente, nota 32.

[62]GALLO, M., voce «Dolo», en Enc. Dir., XIII, Milano, 1964, 754-755. Sostiene que los delitos de posesión sean reconducidos a la hipótesis de la omisión propia e impropia. PASTOR MUÑOZ, N., Los delitos de posesión y los delitos de estatus: Una aproximación político-criminal y dogmática, Barcelona, 2005, 41-43. En contra STRUENSEE, E., «Besitzdelikte» cit., 719.

[63]Sobre el principio de lesividad, v. más en general, MANES, V., Il principio di offensività nel diritto penale, Torino, 2005, con una referencia bibliográfica exhaustiva también a la doctrina extranjera.

[64]Respecto a la distinción entre delitos de peligro necesariamente indirectos y delitos de peligro eventualmente indirectos, v. MARINUCCI, G., DOLCINI, E., Corso di diritto penale, III ed., Milano, 2001, 595.

indirecto.[64] La tenencia crea, de hecho, no sólo el peligro directo de la utilización por parte del criminal de los datos y las informaciones personales de otros para cometer una actividad (continuada) criminal (fraude informático, difusión de programas de software malicioso o correos basura, etc.), sino también el peligro indirecto de la cesión a terceros de la información que a su vez podrán usarla o cederla posteriormente a otros sujetos malintencionados. La incriminación de tales actos sería una manifestación de un derecho penal meramente preventivo dirigido a castigar actos en sí mismos equívocos que podrían desembocar en otros actos delictivos (fraude, difusión de software malicioso, correo basura, etc.), pero de hecho privados de relevancia penal alguna.[65]

También suscita bastantes interrogantes, la utilización de un delito de dolo específico, que contendría un elemento subjetivo del injusto, con el fin de incriminar la «conducta» de poseer datos personales ajenos con la finalidad de cometer un fraude u otra actividad ilícita nos deja en un estado de perplejidad.[66] De hecho, no resulta fácil probar en juicio que el criminal poseía los datos identificativos ajenos con el claro fin de cometer un fraude u otra actividad ilícita. Estas dificultades podrían llevar a incentivar el recurso a deducciones argumentativas o a presunciones legales de dudosa legitimidad constitucional que de forma automática deducen del hecho material también su finalidad. La finalidad criminal debe establecerse sobre la base de indicios objetivos e «indicios reveladores» posteriores en relación mera tenencia de los datos personales de terceros.[67] Para tal fin se debe tomar en consideración no sólo de la cantidad de datos personales en poder del criminal, sino también la especial relevancia que tiene para la comisión de determinados delitos (como, por ejemplo, número de tarjeta de crédito, códigos fiscales, contraseñas para acceder a los sistemas informáticos, etc.). La finalidad de cometer un fraude u otro delito debe ser por tanto, excluida en aquellas ocasiones en las que el sujeto activo posea un número muy reducido de datos personales «comunes» de fácil localización también en Internet (como, por ejemplo, direcciones de correo electrónico, número de teléfono, señas del domicilio, etcétera).

La posesión de datos personales pertenecientes a otra persona constituye un simple acto preparatorio para la comisión de un hurto de identidad.[68] La tipificación de los actos meramente preparatorios es legítima al menos de manera excepcional y en presencia de requisitos bien delimitados.[69] Está justificado en aquellos supuestos en los que los actos preparatorios sean instrumentales en la comisión de otros graves hechos delictivos que representen una puesta en peligro de bienes jurídicos primarios y fundamentales.[70]

---

[65] MANTOVANI, F., Dir. pen., part. gen., Padova, 2007, 216.

[66] Sobre la estructura del tipo con dolo específico v. sobre todo, PICOTTI, L., Il dolo specifico. Un'indagine sugli «elementi finalistici» delle fattispecie penali, Milano, 1993. En la obra manualística v. MARINUCCI, G., DOLCINI, E., Corso, cit., 572 y ss.

[67] En este sentido, v. PICOTTI, L., Il dolo specifico, cit., 504 y ss.

[68] Con respecto a la naturaleza de la hipótesis de posesión de objetos no peligrosos con el objeto de cometer un delito, v. PASTOR MUÑOZ, N., Los delitos de posesión, cit., 57.

[69] En tal sentido, véase, la resolución de la AIDP, The expanding forms of preparation and anticipation, adoptada en Estambul con ocasión del congreso de la Asociación internacional de Derecho Penal el pasado 27 de septiembre de 2009, disponible al sitio http://www.aidpitalia.org/. Sobre formas de anticipación de la tutela penal véase más en general también PICOTTI, L., «The expanding forms of preparation and participation, General report", en Revue international de droit pénal, vol. 3-4, 2006, 623 y ss.

[70] Sobre este argumento v. MARINUCCI, G., DOLCINI, E., Corso, cit., 602. En el mismo sentido, también AIDP, The expanding forms of preparation and anticipation, cit.; ANGIONI, F., Contenuto e funzioni del concetto di bene giuridico, Milano, 1983, 176.

[71] Así ANGIONI, F., Contenuto e funzioni del concetto di bene giuridico, Milano, 1983, 176.

[72] MARINUCCI, G., DOLCINI, E., Corso, cit., 602.

Como ha puesto de manifiesto la doctrina más autorizada, entre el grado de anticipación de la tutela penal y la importancia del bien jurídico tutelado debe existir una proporcionalidad: «cuanto más importante (...) sea el bien lesionado por el delito, será igual de legítimo anticipar su tutela y viceversa».[71] La incriminación de la mera posesión de los datos personales ajenos no resulta de conformidad con el principio de proporcionalidad, en cuanto que atiende a prevenir la comisión de un delito (como, por ejemplo, el fraude, la revelación de secretos, la difusión de programas maliciosos) que no lesionan bienes jurídicos primarios y fundamentales (como el bienestar público, la seguridad del Estado, etcétera).[72]

En conclusión, para evitar una excesiva expansión del campo penalmente relevante, se podría limitar la incriminación a aquellas conductas reconducibles a la primera y tercera etapa del hurto de identidad (véase, supra, párr. 3), esto es, aquellas que consisten en procurarse ilícitamente los datos personales ajenos y utilizarlos para una finalidad ilícita. Por cuanto a la mera posesión de datos identificativos ajenos, en cambio, se podría prever el recurso a una sanción de tipo administrativa o civil, como está prevista en numerosos ordenamientos en relación a la cuestión del tratamiento no autorizado de datos personales.

Bibliografía

AIDP, "The expanding forms of preparation and anticipation", disponible en: ‹http://www.aidpitalia.org/›

ANGIONI, F., "Contenuto e funzioni del concetto di bene giuridico", Milano, 1983; p. 176.

ARIZONA REVISED STATUTES, disponible en: ‹http://www.azleg.state.az.us/ArizonaRevisedStatutes.asp›

CALIFORNIA PENAL CODE, disponible en: ‹http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=pen&codebody=&hits=20›

CIFAS, "Identity Fraud", disponible en: ‹http://www.cifas.org.uk/default.asp?ediUd=561-56›

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS TOWARDS A GENERAL POLICY ON THE FIGHT AGAINST CYBER-CRIME, COM (2007), disponible en: ‹http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14560_en.htm›

CSI, "Computer Crime & Security Survey" (2008), disponible en: ‹http//www.gocsi.com›

DAVIS, L. M., "With or without authorization, it's still identity theft". En: McGeorge Law Review, No. 33, (2002); p. 231y ss.

DE HERT P., GONZALES G.F., KOOPS, B.J., "Fighting Cyber-crime in the two Europes: the Added Value of the EU Framework Decision and the Council of Europe Convention". International Review of Penal Law, Vol. 77 (3-4), (2006); p. 503 y ss.

ERNST, S., "Das neue Computerstrafrecht". En: Neue Juristiche Wochenschrift, No. 37, (2007); p. 2661 y ss.

FDIC, "Putting an End to Account-Hijacking Identity theft" (2004), disponible en: ‹http://www.ftc.gov›

FLOR, R., "Phishing, Identity Theft e Identity Abuse. Le Prospettive Applicative del Diritto Penale Vigente". En: Rivista Italiana Di Diritto E Procedura Penale, (2007); p. 899.

FLORIDA STATUTES ANNOTATIONS, disponible en: ‹http://www.flsenate.gov/Statutes/index.cfm?Tab=statutes&submenu=-1&CFID=239344567&CFTOKEN=60039921›

FTC, "Identity Theft Focus of National Consumer Protection Week" (2005), disponible en: ‹http://www.ftc.gov/opa/2005/02/ncpw05.shtm›

FTC, "Identity theft Survey Report" (2006), disponible en: ‹http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf›

FTC, "Consumer Fraud and Identity Theft Complaint Data" (2007), disponible en: ‹http://www.ftc.gov/opa/2008/02/fraud.pdf›

GALLO, M., voce «Dolo», en Enc. Dir., XIII, Milano, 1964, 754-755.

GARANTE PRIVACY, "Social networks: attenzione agli effetti collaterali" (2009), disponible en: ‹http://www.garanteprivacy.it/garante/docJsp?ID=1614258.›

GERCKE M., "Internet-Related Identity-Theft: a Discussion Paper" (2007), disponible en: ‹http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf›

GONZÁLEZ, E. M., The new Arizona Data Security Breach Law: a Step in the Right Direction, but Unlikely to Prevent Identity Theft: or Compensate Consumers, 40 Niz. St. LJ., 2008, 1349 y ss.

GRÖSELING, N., HÖFINGER, F. M., "Hacking und Computerspionage. Auswirkungen des 41. StrÄndG zur Bekampfung der Computerkriminalität". En: Multimedia und Recht, No. 9, 2007; p. 549 y ss.

HILGENDORF, E., FRANK, T., VALERIUS, B. Computer und Internetstrafrecht. Berlín-Heidelberg: Springer, 2005.

HOME OFFICE IDENTITY FRAUD STEERING COMMITTEE, "Identity theft, Don't become a victim" disponible en: ‹http://www.identitytheft.org›

ITRC, "Identity theft: the Aftermath" (2008), disponible en: ‹http://www.idtheftcenter.org/artman2/uploads/l/Aftermath_2008_20090520.pdf›

ITU, "Understanding Cyber-crime: A Guide for Developing Countries" (2009), disponible en: ‹http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf›

JAVELIN STRATEGY & RESEARCH, 2006, "Identity Fraud Survey Report" (2006), disponible en: ‹http://www.javelinstrategy.com›

KOOPS, B.J., LEENES, R., "Identity Theft, Identity Fraud and/or Identity Related Crime". En: Datenschutz und Datensicherheit, No. 30 - 9, (2006); p. 553-556.

LACODNY, O., Strafrecht vor den Schranken der Grundrechte, Tübingen, (1996); p. 323.

MARINUCCI, G. Il reato come azione. Milano, 1971, 167 y ss.

MARINUCCI, G., DOLCINI, E., Corso di diritto penale, III ed., Milano, 2001; p. 595.

MANNA, A., "Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento di dati personali". En: Rivista dell' Informazione e dell'Informatica, No. 4, (2003); p. 745 y ss.

MANES, V., "Il principio di offensività nel diritto penale", Torino, 2005.

MANTOVANI, F., Diritto penale parte generale, Padova, 2007; p. 216.

MANZINI, V. Trattato di Diritto Penale Italiano. Vol. 1, 5° edición puesta al día (a cargo de P. NUVOLONE y G. D. PISAPIA), 1986; p. 460.

MITCHISON, N.; WILIKENS, M.; BREITENBACH, L.; URRY R; PORTESI, S., "Identity Theft. A Discussion Paper" (2004), disponible en:
‹http://www.prime-project.eu/community/furtherreading/ studies/IDTheftFIN.pdf›

NEWMAN, C. R; McNALLY, M. M., "Identity Theft Literature Review" (2005), disponible en: ‹http://www.ncjrs.gov/pdffilesl/nij/grants/210459.pdf›

OECD, "Online Identity theft" (2009), disponible en: ‹http://www.oecd.org›

PAGET, F., "Identity Theft - McAfee White Paper" (2007), disponible en: ‹http://www.mcafee.com›

PASTOR MUÑOZ, N., "Los delitos de posesión y los delitos de estatus: Una aproximación político-criminal y dogmática", Barcelona, 2005; p. 41-43.

PASTRIKOS, C., "Identity Theft Statutes: Which will Protect Americans the Most?" En: Albany Law Review, Vol. 67, (2004).

PICOTTI, L., "Il dolo specifico. Un'indagine sugli «elementi finalistici» delle fattispecie penali", Milano, 1993.

PICOTTI, L., "The expanding forms of preparation and participation, General report", en Revue international de droit pénal, vol. 3-4, (2006); p. 623 y ss.

PICOTTI, L., SALVADORI, I., "National legislation implementing the Convention on Cybercrime". Working paper disponible en: http://www.coe.int.

_____"Il trattamento senza consenso di dati personali altrui reperibili su Internet costituisce reato?" En: Rivista Italiana Di Diritto E Procedura Penale, No. 4, (2006); p. 458 y ss.

SALVADORI, I., "Hacking, cracking e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive de jure condendo". En: Cyberspazio e diritto, No. 3, (2008); p. 329 y ss.

SEGER, A., "Identity Theft and the Convention on Cybercrime". En: UN-ISPAC, Conference on the Evolving Challenge of identity-related Crime (Atti del Convegno di Courmayer, 30.11-2-12 2007), disponible en: http://www.idfraudconference-pt2007.org/ebook/ebook.php

SCHUMANN, K. H., "Das 41. StrÄndG zur Bekampfung der Computerkriminalität". En: Die Neue Zeitschrift für Strafrecht, No. 67, (2007).

STRAFGESETZBUCH, disponible en: ‹http://www.gesetze-im-internet.de/stgb/›

STRAFRECHTSÄNDERUNGSGESETZES ZUR BEKÄMPFUNG DER COMPUTERKRIMINALITÄT (41. StrÄndG), 11.08.2007

STRUENSEE, E., "Besitzdelikte". En: SAMSON, E., DENCKNER, F., FRISCH, P., FRISTER, H., REIB, W. (Hrsg), Festschrift für Gerard Grünwald zum siebzigsten Geburstag, Baden-Baden, (1999); p. 713 y ss.

TEXAS PENAL CODE, disponible en: ‹http://law.justia.com/texas/codes/2005/pe.html›

UNITED STATES CODE, disponible en: ‹http://uscode.house.gov/›

UNITED STATES DEPARTMENT OF JUSTICE, "A National Strategy to Combat Identity Theft" (2006), disponible en: ‹http://www.cops.usdoj.gov/files/ric/Publications/e03062303.pdf›

UNITED STATES IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT, disponible en: ‹http://www.ftc.gov/os/statutes/itada/itadact.htm›

UNITED STATES IDENTITY THEFT PENALTY ENHANCEMENT ACT, Public Law 108-275, 15 June 2004.

THE PRESIDENT'S IDENTITY THEFT TASK FORCE, "Combating Identity Theft: A Strategic Plan" (2007), disponible en: ‹http://www.identitytheft.gov/reports/StrategicPlan.pdf›

TOWLE, H. K., Identity theft: myths, methods, and new law. En: Rutgers Computer & Tech. L.J., No. 30, (2004): p. 247 y ss.

VAN DER MEULEN, N., "The Spread of Identity Theft: Developments and Initiatives within the European Union" (2007), disponible en: ‹http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1190&issue_id=52007›

VICTOR, G. M., "Identity theft, its Environment and Proposals for Change". En: Loyola Consumer Law Review, No. 18, (2006); p. 256.

ZWEITES GESETZ ZUR BEKÄMPFUNG DER WIRTSCHAFTSKRIMINALITÄT (2. WiKG), disponible en: ‹http://openlibrary.org/books/OL1917177M/Zweites_Gesetz_zur_Beka%CC%88mpfung_der_Wirtschaftskriminalita%CC%88t_(2._WiKG)›