Coloquio Preparatorio
24-27 abril 2013, Moscú (Rusia)
Sección II – Sociedad de la información y derecho penal

BRASIL*

Renato de Mello JORGE SILVEIRA - Eduardo SAAD-DINIZ*

Las prácticas legislativas y los conceptos jurídicos del "ciberdelito" aún necesitan de perfeccionamiento en el ámbito científico y en su manejo técnico. Sin embargo, la normativa penal brasileña en términos de los impactos regulatorios del desarrollo informático sigue siendo incipiente. En el Código Penal brasileño (en adelante CPbras) no hay referencias a títulos y el recurso a las TICs para la elaboración de tipos penales es algo novedoso en la legislación brasileña. Pero es posible evidenciar una tendencia a su adopción, lo que trae algunas dificultades en su aplicación y su adecuación al modelo de Estado de Derecho configurado en la Constitución Federal brasileña.

La Ley 11.829/2008 introdujo en el ordenamiento brasileño la idea de combate y prevención a la pornografía infantil por medio de sistemas informáticos o telemáticos. Y hace muy poco, en el 30.11.2012, fue promulgada la Ley 12.737/2012 (la así llamada "Ley Carolina Dieckmann"), que define los tipos penales informáticos con recurso a algunos de los términos de las TICs, agregándoles al CPbras.

Incluso sin una verificación empírica de la interpretación jurisprudencial brasileña, se puede afirmar que la Ley 12.737/2012 fue sancionada sin precedentes significativos en la práctica judiciaria.

La reforma legislativa advino, sin embargo, de algo que se hace cada vez más frecuente en el proceso legislativo criminal brasileño, manipulaciones políticas – los "gestores atípicos de la moral" – frente a apelaciones populares de criminalización de conductas.

Desde los propósitos de adecuación de las leyes penales frente a los cambios del desarrollo informático, las reformas penales que hacen referencia a las TICs lo hicieron con recurso a la refundición (*recasting*). La Ley 12.737/2012 incorporó al CPbras nuevos tipos penales, los arts. 154-A (invasión de dispositivo informático) e 266, § 1º e 2º (interrupción o perturbación de servicio telegráfico, telefónico, informático, telemático o de información de utilidad pública).

Otras referencias a las TICs fueron incorporadas en legislación especial, como la Ley 9.296/1996 (interceptación de comunicación telemática o informática); Ley 9.609/1998 (protección de la propiedad intelectual de los programas de computación); Ley 9.983/2000 (delitos relacionados al acceso indebido a sistemas informáticos de la Administración Pública); Ley 11.829/2008, que añadió la pornografía infantil en Internet al Estatuto del Niño y Adolescente (ECA); y Ley 12.034/2009, que regula el uso de Internet en el sistema electoral brasileño.

A su vez, la dogmática jurídico-penal hizo mención a elementos específicos de caracterización del tipo subjetivo. El tipo penal de invasión de dispositivo informático (154-A, CPbras) exige dolo específico de "obtener, adulterar o

---

* Atención: El texto que se publica constituye la última versión original del informe nacional enviado por el autor, sin revisión editorial por parte de la Revista.

* Profesor Catedrático Renato de Mello Jorge Silveira (USP). Prof. Dr. Eduardo Saad-Diniz (USP/FDRP).

destruir los datos o informaciones" e instalar vulnerabilidades "para obtener ventaja ilícita"[1]. Sin embargo, los recursos dogmáticos no alcanzaron las figuras imprudentes

No se permite observar en las leyes penales brasileñas una normativa específica con respecto al acceso ilegal e interceptación de trasmisiones, que manifiesten potencial ofensivo frente a la integridad y funcionalidad del sistema TI.

De todos modos, el CPbras a partir del art. 154-A prescribe la "invasión de dispositivo informático" con la siguiente descripción típica: *"invadir dispositivo informático ajeno, conectado o no a la red de computadoras, mediante violación indebida de mecanismo de seguridad y con el fin de obtener, adulterar o destruir datos o informaciones sin autorización expresa o tácita del titular del dispositivo o instalar vulnerabilidades para obtener ventaja ilícita. Pena - detención, de 3 (tres) meses a 1 (uno) año, y multa".*

La violación a la que hace referencia el art. 154-A del CPbras debe ser llevada a cabo con el uso indebido de mecanismo de seguridad, aunque su descripción no sea detallada. La descripción típica del art. 154-A alcanza también a la conducta de *"adulterar o destruir datos o informaciones sin autorización expresa o tácita del titular del dispositivo o instalar vulnerabilidades".* El art. 154-A, en su párrafo 3º prescribe pena de reclusión de 6 (seis) meses a 2 (dos) años, y multa, *"si de la invasión resultara la obtención de contenido de comunicaciones electrónicas privadas, secretos comerciales o industriales, informaciones en secreto, así definidas en ley, o el control remoto no autorizado del dispositivo invadido".* Y en su art. 4º la aumenta de uno a dos tercios en caso de divulgación, comercialización o transmisión a terceros, a cualquier título, de los datos o informaciones obtenidos"[2].

Desde el punto de vista conceptual, las referencias normativas recién promulgadas en Brasil no aportaron un concepto de "datos electrónicos y/o informáticos". Lo mismo aconteció con respecto a cualquiera de las herramientas con las que pueda ser instrumentalizada la infracción, sin que haya un catálogo o cualquier descripción adecuada.

Además de eso, la Ley 12.737/2012 introduce – añadiéndole al art. 298 del CPbras, que trata de la falsificación de documentos particulares – apenas la equiparación de las tarjetas de crédito y débito a documentos particulares, sin todavía alcanzar figuras de alteración, borrado o supresión no autorizadas de datos o información electrónica o informática que produzca la inautenticidad de los documentos.

La misma ley hizo sumar en el Art. 154-A del CPbras la criminalización genérica dela producción, ofrecimiento, distribución, venta o difusión de dispositivos o programas de computación que permitan la práctica de la invasión de

[1] "Invasão de dispositivo informático: Art. 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

[2] Art. 154-A: § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

dispositivo informático: *"§ 1º: en la misma pena incurre quien produce, ofrece, distribuye, vende o difunde dispositivo o programa de computación con el intuito de permitir la práctica de la conducta definida en el* caput*"*[3].

En su § 1º, el art. 154-A penaliza también la distribución, pero sin acceder a la figura de los delitos de posesión de cualquier instrumento que venga a ser utilizado en la infracción.

En cuanto a la tutela penal de la intimidad, no hay previsión específica de control "ex ante" de las informaciones sobre el consumidor. El Código brasileño de Defensa del Consumidor (CDC), en los arts. 43 y ss., regula genéricamente el manejo "ex post" de los registros. La Ley 12.414/2011 disciplina la formación y consulta a los bancos de datos con informaciones de adimplemento, de personas naturales o de personas jurídicas, para la formación del historial crediticio, protegiendo al consumidor solamente en el ámbito de responsabilidad civil. El CDC se concentra en la verificación de los abusos de relaciones de consumo (art. 37, § 2º, CDC), especialmente en relación a los *cookies* transmitidos sin autorización y conocimiento del cliente, derivando del principio constitucional de protección de la privacidad (art. 5º, X, CF) sanciones compensatorias (arts. 43, 59, 72, 73 del CDC, además del art. 129, Código Civil brasileño). Sin embargo, el ordenamiento jurídico brasileño deja de prever la debida información a los consumidores sobre la identidad y manejo de los datos personales. La misma omisión se percibe en relación a la ausencia de regulación de las políticas de privacidad o manejo de informaciones personales en *websites*.

En términos genéricos, el Código brasileño de Defensa del Consumidor (Ley 8.079/90 - CDC), en su art. 72, prescribe la conducta genérica de *"impedir o dificultar el acceso del consumidor a las informaciones que sobre él consten de 'cadastros'*[4]*, banco de datos, fichas y registros. Pena Detención de seis meses a un año o multa".* El art. 73, a su vez, también del CDC, prescribe: *"dejar de corregir inmediatamente información sobre consumidor constante de 'cadastro', banco de datos, fichas o registros que sabe o debería saber se inexacta. Pena Detención de seis meses a un año o multa".*

La transferencia y distribución ilegales de datos privados no es tipificada en las leyes penales brasileñas. En cuanto a esas conductas típicas, el CPbras penaliza los crímenes contra la inviolabilidad de correspondencia y los crímenes contra la inviolabilidad de secretos: 151, II (violación de comunicación telegráfica, radioeléctrica o telefónica), 152 (correspondencia comercial), 153 (divulgación de secreto), 154 (violación de secreto profesional) y el recién creado tipo penal de invasión de dispositivo informático, 154-A, § 1º.

La Ley complementaria 105/2001 regula el secreto de operaciones de instituciones financieras. En su art. 4º determina que la quiebra del secreto puede ser determinada en casos de verificación de un eventual ilícito, en cualquier fase procesal, especialmente cuando esté vinculado a delitos de terrorismo, tráfico de estupefacientes o armas, extorsión mediante secuestro, contra el sistema financiero nacional, contra la Administración Pública, el orden fiscal o la seguridad social, blanqueo de capitales o practicado por organizaciones criminales. La quiebra del secreto se orienta por la esencialidad de los datos para la investigación, además de la demonstración de urgencia para la obtención de informaciones.

---

[3] Art. 154-A: § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

[4] "Cadastro" = registro.

El art. 10 de la misma Ley criminaliza la quiebra fuera de las hipótesis legales, con pena de reclusión de uno a cuatro años, sin prejuicio de las otras sanciones penales. En su art. 11, la ley complementaria prescribe la responsabilidad personal de servidor público que haga uso indebido de esas informaciones.

En la interpretación de las leyes en Brasil, las libertades individuales no gozan de protección absoluta. La razonabilidad de la quiebra depende del potencial de peligro de la conducta, basando la decisión en las reglas de proporcionalidad y oportunidad procesal, además de su consecuente demonstración de su pertinencia a la investigación procesal. Las cortes supremas, en juzgados recientes, decidieron, p. ej., que meros indicios de prácticas de blanqueo de capitales en los informes de la Unidad de Inteligencia Financiera (el COAF) no bastarían para la aceptación de la denuncia.

En los supuestos de ejercicio profesional es presupuesto objetivo la percepción de justa causa, que en lo que toca a los abogados es establecido por el Tribunal de Ética y Disciplina del Consejo Brasileño de Abogados y reglado en el art. 25 de la Ley 8.906/1994, el Código de Ética y Disciplina, que establece que el secreto no ultrapasa eventuales amenazas que vaya a sufrir el abogado por parte de su cliente, ni incluso los límites de interés de la causa en cuestión.

En el ámbito de la regulación profesional, su actuación en Brasil está constitucionalmente protegida por el "secreto profesional". Tipifica el CPbras la violación de secreto profesional[5], en su art. 154, además del art. 207, del Código de Proceso Penal, que tutela la protección al secreto profesional por medio de la prohibición de deponer en juicio a las personas que deban mantener secreto en razón de su rol en cuanto profesional. Esos derechos son constitucionalmente asegurados en el art. 5º, incisos XIII e XIV – libertad de ejercicio profesional y protección del secreto de fuente de informaciones en razón del ejercicio profesional. Sin embargo, desde una perspectiva conceptual, hace solamente referencias genéricas a los vínculos entre el hecho delictivo y el ejercicio de la función profesional, sin mayores detalles o discriminación entre las distintas categorías. En términos generales, en Brasil aún sigue siendo válida la idea de que los ciberdelitos, en su mayoría, se consideran crímenes impropiamente informáticos, manejados en la dogmática jurídico-penal conforme a las normas del CPbras.

La protección de los datos se encuentra prevista en la legislación brasileña de forma genérica. El art. 154-A del CPbras penaliza la obtención (§ 3º) de datos y su eventual comercialización (§ 4º). El Estatuto del Niño y del Adolescente, abajo descripto, también prescribe semejantes conductas en su art. 241-B. Pero una vez más no hay previsiones direccionadas a determinadas categorías de personas.

El procesamiento ilegal de datos personales y privados no tiene recepción en nuestras leyes penales. En lo que toca al robo de identidad y sus formas y usos específicos, aunque el CPbras no traiga la caracterización de un delito específico, la conducta es punible como delito de naturaleza patrimonial, en sus formas tradicionales.

Ya en las figuras típicas de los arts. 240 y 241 del ECA[6] recibe la pornografía infantil previsión específica, discriminando la transmisión, la disposición, acceso intencional en Internet, pero sin previsión específica con

[5] *Violação do segredo profissional:* Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa.

[6] Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008). Pena – reclusão, de 4 (quatro) a 8 (oito) anos,

e multa. (Redação dada pela Lei nº 11.829, de 2008). § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena. (Redação dada pela Lei nº 11.829, de 2008). § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime: (Redação dada pela Lei nº 11.829, de 2008). I – no exercício de cargo ou função pública ou a pretexto de exercê-la; (Redação dada pela Lei nº 11.829, de 2008). II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou (Redação dada pela Lei nº 11.829, de 2008). III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento. (Incluído pela Lei nº 11.829, de 2008).

Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008). Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008).

Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008). Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008). § 1º Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008). I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008). II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.(Incluído pela Lei nº 11.829, de 2008). § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008). Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008). § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008). § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: (Incluído pela Lei nº 11.829, de 2008). I – agente público no exercício de suas funções; (Incluído pela Lei nº 11.829, de 2008). II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; (Incluído pela Lei nº 11.829, de 2008). III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (Incluído pela Lei nº 11.829, de 2008). § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido. (Incluído pela Lei nº 11.829, de 2008)

Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008). Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008). Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)

Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:(Incluído pela Lei nº 11.829, de 2008). Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008). Parágrafo único. Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008). I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;(Incluído pela Lei nº 11.829, de 2008). II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.(Incluído pela Lei nº 11.829, de 2008).

respecto a la exportación de los datos o cualquier posibilidad de orden judicial para que los jueces puedan ordenar que sean borrados los archivos o inclusivo embargados los instrumentos concernientes a la pornografía infantil colocada en sistemas informáticos.

En los delitos contra la autodeterminación sexual, hay figuras que protegen la condición del menor (criterio normativo: víctimas mayores de 14 años y menores de 18 años) desde su especial condición de "vulnerable".

Aunque no haga mención expresa a la pornografía virtual, la discusión más frecuente en Brasil se dedica a los límites entre la libertad de expresión artística y la caracterización de lo pornográfico, aunque haya el intento de definición en el art. 241-E: *"para efecto de los crímenes previstos en esta Ley, la expresión 'escena de sexo explícito o pornográfica' comprende cualquier situación que envuelva a un niño o adolescente en actividades sexuales explícitas, reales o simuladas, o exhibición de los órganos genitales de un niño o adolescente para fines primordialmente sexuales".* Las leyes penales brasileñas no hacen mención a la exclusión de responsabilidad en caso de personas que, sin advertencia previa, accedan a pornografía infantil en *websites*.

En general, la interpretación de la normativa sobre pornografía infantil y el ECA se evidencia de forma un tanto controvertida, una vez que se establece el primado de la protección integral solamente a personas menores de 14 (catorce) años, dejando de atribuir relevancia penal al *sexual intercourse* con consentimiento entre mayores de 14 años. A su vez, el ECA se orienta por la protección integral a menores de 18 (dieciocho) años, lo que puede llegar a ser interpretado como una confusión desde la aplicación de lo que sería pornografía infantil (habiendo consentimiento en la relación, pero no en la publicación de datos sobre personas de esta faja etaria). Esta interpretación trae dudas en la doctrina en lo que concierne a la legitimidad de delitos de pornografía virtual o simulada, considerándose que no habría, en semejantes situaciones, una víctima real.

Ni el anonimato en el envío en el manejo de material por las TIC, ni incluso el *cyber-bullying*, *cyber-stalking* o *cyber-grooming* llegan a tener previsión específica. Tampoco hay previsión específica para el espionaje industrial, criminalización de actos cometidos practicados en el mundo virtual. Los delitos de *non-compliance* e infracción del deber de colaboración siguen sin previsión en nuestro ordenamiento. La regulación penal de la recogida de datos no hace referencia al empleo de las TICs.

En lo que respecta a la violación de propiedad, la incriminación se da igualmente a partir de las formas tradicionales de defraudación, sin previsión específica cuanto al uso de las TICs. Nuestro ordenamiento lo hace por medio del art. 12 y párrafos de la Ley 9.609/1998: *"violar derecho de autor de programas de computación. Pena Detención de seis meses a dos años o multa. § 1º. Si de la violación consistiera reproducción, por cualquier medio, de programa de computación, total o parcialmente, para fines de comercio, sin autorización expresa del autor o de quien lo represente. Pena: Reclusión de uno a cuatro años y multa".*

Hay un *website* en el que se puede acceder a informaciones y análisis estadísticos más detallados: http://www.cert.br/stats/incidentes/, cuya manutención es de responsabilidad del CERT.br, Grupo de Respuesta a Incidentes de Seguridad para la Internet brasileña. Sin embargo, no hay estadísticas oficiales sobre semejantes denuncias. Hay solamente verificaciones no-oficiales.

Las encuestas no contemplan victimización en ciberdelitos.

Ni la Policía ni la Fiscalía disponen de unidad de delitos informáticos. Debe tenerse en cuenta, sin embargo, que la Policía Civil de São Paulo mantiene el DCS – Departamento de Comunicación Social, responsable por investigar

crímenes cometidos por medio de recursos informáticos, pero sin atribuciones administrativas oficiales, apenas basado en la aplicación del Código de Proceso Penal, en su art. 6º e incisos.

En las instituciones de enseñanza brasileñas no hay todavía cursos específicos sobre ciberdelito. Y, a pesar de no ser objeto de capacitación obligatoria, en la actualidad se están incrementando los cursos de capacitación y formación en materia de criminalidad informática.

En la Fiscalía Federal funciona el "Grupo de Trabajo para el Enfrentamiento de los Crímenes Cibernéticos", especialmente pornografía infantil y racismo cometido por medio de internet, que se orienta por algunas directrices básicas: especialización de los miembros de la Fiscalía, creación de núcleos regionales para el auxilio en las investigaciones de crímenes cibernéticos, implementación de una base nacional de datos sobre las denuncias, verificación de las dificultades encontradas por la Fiscalía en la persecución penal, proposición de nuevos modelos de actuación[7].

A pesar de eso, el robo de identidad *online* (incluido el *phishing* y el tráfico *online* de información sobre falsa identidad), Hacking (intrusión ilegal en sistemas informáticos), Código malicioso (gusanos, virus, *malware* y *spyware*), Interceptación ilegal de datos informáticos, Comisión *online* de delitos contra la propiedad intelectual, tráfico online de pornografía infantil y daño intencional de datos o sistemas informáticos ocurren con mucha frecuencia en Brasil.

[7] Fuente: http://2ccr.pgr.mpf.gov.br/coordenacao/grupos-de-trabalho/combate-crimes-cirberneticos/sobre