Protección penal de la privacidad en la "sociedad de la información"

Análisis de la ley 26.388 y algunas consideraciones preliminares en torno al Anteproyecto de Código Penal de la Nación

por **HORACIO SANTIAGO NAGER**[1]

1 | Introducción

El presente trabajo tiene por objeto analizar el impacto que han significado las nuevas tecnologías de la información en un bien jurídico fundamental: la intimidad o privacidad de las personas, y en pos de cumplir con el objetivo trazado, nos centraremos especialmente en las figuras legales modificadas y/o introducidas por la Ley de Delitos Informáticos 26.388.

Asimismo, dedicaremos algunos breves párrafos a conductas, cuya tipificación fue discutida en los recintos legislativos, pero que finalmente no merecieron recepción positiva.

(1) Especialista en Derecho Penal (UBA). Auxiliar docente del Departamento de Derecho Penal y Criminología de la Facultad de Derecho (UBA), en la asignatura Elementos de Derecho Penal y Procesal Penal, cátedra del Prof. Alejandro Alagia. Prosecretario Letrado de la Defensoría General de la Nación.

Finalmente, procuraremos realizar un breve análisis sobre las reformas que el reciente Anteproyecto de Código Penal de la Nación propone en la temática.

2 | Bien jurídico protegido

A raíz de la sanción de la Ley de Delitos Informáticos (ley 26.388) modificó el epígrafe del Capítulo III, del Título V del Código Penal, definiendo el legislador los contornos materiales del bien jurídico tutelado por las figuras penales allí previstas.

Tradicionalmente, la doctrina jurídico penal criticó la formulación del texto derogado, pues parecía circunscribir la protección legal a información y/o documentos cuyo contenido resultara secreto; sin embargo, esta impresión inicial, se revelaba errónea al reparar en las conductas allí tipificadas, ya que en aquel elenco penal se punían acciones lesivas de la intimidad de las personas. De esta forma, se ha corregido un error histórico, porque la correspondencia y los papeles privados no constituyen necesariamente cosas secretas.(2)

Ahora bien, con respecto al término escogido en la ley 26.388, cabe advertir que lo privado puede no ser lo íntimo, de manera que el legislador optó por la fórmula más amplia a la hora de receptar posibles actos lesivos al núcleo ético social protegido. Esta elección terminológica se encuentra muy posiblemente inspirada en el derecho anglosajón donde, desde antiguo, se ha definido a la privacidad como el derecho a estar libre de injerencias indebidas o arbitrarias, sea que éstas provengan de terceros o del Estado. Por cierto, en el *common law* norteamericano esta garantía material, bajo el rótulo de *right of privacy,* ha sido definida como el derecho que cada individuo tiene a permanecer aislado, solo, dentro de una esfera de reserva o exclusión de la injerencia de otros individuos o del Estado; o sea, "como el derecho de vivir sin interferencias no deseadas por el público, sobre asuntos que no están necesariamente relacionados con éste".(3)

(2) Molinario, Alfredo J., *Los Delitos*, (preparado y actualizado por Eduardo Aguirre Obarrio) Bs. As., TEA, 1996, t. II, p. 108.

(3) *Enciclopedia Jurídica Omeba* (versión digital), voz "*intimidad (derecho a la)*", tema desarrollado por el Dr. Mateo Goudstein.

Sin perjuicio de ello, a los fines de este trabajo, y en lo que respecta al tratamiento dogmático de los delitos que integran este capítulo, usaremos en forma indistinta los términos "intimidad" y "privacidad".

No está demás puntualizar, siguiendo a Moeremans que:

> "... sobre la intimidad se han pronunciado infinidad de definiciones y teorías. Pero al ser éste un elemento vivo, que responde a las circunstancias, que debe adaptarse a cada momento y tiempo social, sus manifestaciones se encuentran debatidas. Siguiendo la teoría de las Esferas podemos distinguir en: La esfera íntima: es lo intangible de la persona, sus atributos, pensamientos, que de modo alguno influyen en la sociedad. La esfera privada: se compone por las ideas compartidas con familiares, amigos, por las acciones que se realizan sin menoscabo de derechos de terceros. La esfera social: son las acciones que entran en la interacción social…".(4)

Una breve referencia histórica sobre el bien jurídico, en tanto constituye una de las manifestaciones de la libertad humana, resultará ilustrativa al objeto de comprender el enorme desafío que plantea la sociedad ultra tecnificada del siglo XXI.

La libertad de intimidad es un derecho de base ilustrada que surgió en los albores del Estado Moderno como una reacción contra el sistema monárquico y absolutista del Antiguo Régimen, cuya piedra fundacional reside en el reconocimiento del principio de dignidad y autodeterminación ética de la persona humana. En dicho marco histórico, el acceso al conocimiento por parte del ciudadano encontró directa vinculación con los valores revolucionarios de libertad e igualdad, que se erigió en una pieza fundamental para el avance del humanismo y la ciencia, en contraposición con el oscurantismo medieval. Sin dudas, los cambios fueron progresivos, y la evolución jurídica no fue siempre acompañada por la consecución concreta de estos derechos, devenidos también en garantías.

(4) Moeremans, Daniel E., "Protección del e-mail como extensión del derecho a la intimidad", en *Revista Jurídica La Ley*, 2007-E, p. 740.

Sin embargo, resulta innegable que el derecho a la privacidad constituye un límite racional y concreto al poder público y a terceros. Los Estados autoritarios tienden a difuminar sus límites permitiendo injerencias arbitrarias en la esfera de reserva de las personas, mientras que el Estado de derecho tiene la obligación de proteger este espacio donde el individuo tiene "derecho a estar solo", como una de las manifestaciones más importantes de la libertad personal.

Ya inmersos en el siglo XX, la protección de la intimidad se intensificó al finalizar la segunda guerra mundial, a raíz de la preocupación de la comunidad internacional por las prácticas de espionaje, tal como quedara expuesto en la Declaración Universal de Derechos del Humanos (art. 12).[5]

Como hemos visto, en el pasado el monopolio de la información y la censura implicaba la principal manifestación de poder; actualmente dicho poder no reside solamente en el acceso o la supresión de los datos,[6] sino también en las posibilidades que ofrece su tratamiento, y en la capacidad de discernir entre la información confiable de aquella que no posee tales características. Por otro lado, las conductas susceptibles de afectar este bien jurídico se han incrementado sensiblemente en términos de intensidad e inmediatez de la mano del fenómeno de la globalización.

Por último, debemos recordar que la intimidad constituye un derecho personalísimo, y como tal, es inherente al ser humano por su sola condición de tal.

3 | Los desafíos que plantea la protección de la privacidad en la "sociedad de la información"

En relación con lo expuesto anteriormente, resulta innegable que en las últimas décadas, y de manera cada vez más acelerada, se han producido

(5) Adoptada y proclamada por la Asamblea General en su Resolución 217 A (III), del 10/12/1948.

(6) Sobre el acceso igualitario y libre a la información almacenada en Internet se recomienda ver Tomeo, Fernando, "La neutralidad en Internet", en *Revista Jurídica La Ley*, 2011-E, 1367.

importantes avances tecnológicos en materia de comunicaciones; lo que constituye uno de los datos sociológicos por excelencia de este siglo, a punto tal que frecuentemente, escuchamos decir que vivimos en la "sociedad de la información".

Como manifestación negativa del incesante desarrollo de estas herramientas técnicas, se advierte que el ámbito de reserva o privacidad del individuo nunca ha sido tan vulnerable, y que se ha quebrado, al menos en parte, aquel vínculo ilustrado entre libertad de acceso a la información y libertad individual. En este sentido, basta detenerse unos instantes en la conexión que existe (al menos en el plano discusivo) entre la "sociedad de la información" y la "sociedad del riesgo", con sus súbitas y controvertidas emergencias.(7) Todo lo cual, repercute a la hora de recortar progresivamente el ámbito de reserva personal, permitiendo una mayor injerencia del Estado en la vida privada.

(7) Por ejemplo, la invocación de la lucha contra el terrorismo internacional y guerra preventiva como fundamento de la existencia de sistemas de espionaje global como *Carnivore* (FBI) y *Echelon* (NSA). El primero de estos sistemas de vigilancia a distancia de origen estatal es "… un software usado por el FBI que (…) se instala en los proveedores de acceso a Internet y, tras una petición proveniente de una instancia judicial, rastrea todo lo que un usuario hace durante su conexión a Internet (Ver [en línea] http://www.wikipedia.org). Sus críticos "… advierten que su poder es ilimitado (…) tiene la capacidad de filtrar en busca de determinadas palabras clave millones de mensajes de correo electrónico que viajan por la Red y sin saber que son vigilados. El programa tiene unas claves, que el FBI mantiene en secreto, que permiten descubrir la información que la agencia policial busca. Estas claves pueden ser palabras, nombres de políticos, de ciudades, y terminología que levante sospechas entre los investigadores del FBI. Cuando uno de estos mensajes es localizado, el programa se introduce en el disco duro del internauta 'capturado' y archiva toda su información confidencial, a la espera de que los investigadores determinen si ha cometido algún delito. Incluso antes de un juez les dé permiso para hacerlo."; no obstante, en el año 2005, el gobierno estadounidense, anunció el cese del uso de este programa especial de vigilancia por Internet, al tiempo que requirió a los servidores de servicios de Internet que vigilen a sus clientes (ver [en línea] http://www.elmundo.es). Por su parte, Echelon "... es considerada la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia. Controlada por la comunidad UKUSA (Estados Unidos, Reino Unido, Canadá, Australia, y Nueva Zelanda) (…) puede capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y e-mails en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones. Se estima que Echelon intercepta más de tres mil millones de comunicaciones cada día". (ver [en línea] http://www.wikipedia.org). Precisamente, este poder de control y espionaje masivo ha sido desde el año 2009 el eje de un escándalo internacional generado a partir de la revelación de documentos clasificados pertenecientes al gobierno de los EEUU, gracias al incidente conocido como "WikiLeaks" y el aporte posterior del ex analista de la CIA Edward Snowden. Escándalo que culminó en la modificación de la ley de inteligencia de ese país del Norte.

Precisamente, una de las notas características de las sociedades postmodernas es el aumento de los riesgos humanos de la mano de la evolución tecnológica, como un efecto colateral de las grandes ventajas que este desarrollo provee a la vida social. Por ello, el nexo que une a conceptualizaciones sociológicas como la "sociedad de la información" y la "sociedad del riesgo" es el auge técnico (muchas veces de origen militar) que se ha incrementado exponencial e incesantemente desde la invención de la máquina de vapor. Criminológicamente, este binomio también se complementa y retroalimenta, pues la sociedad del riesgo requiere nuevas técnicas de control social, dentro de las cuales, el monitoreo de personas, el control y tratamiento del tráfico de datos privados, el "espionaje" y otras tecnologías son presentadas como herramientas eficaces y útiles, que posibilitan nuevos mecanismos de control justificados en criterios utilitaristas y modelos de gestión de riesgos que bien podrían significar una vuelta del viejo peligrosismo. Así, diversos ensayistas refieren que vivimos bajo una **libertad vigilada** o en una **casa de cristal**; mientras otros, señalan una contraposición dialéctica entre dos modelos bien diferenciados: por un lado, la concentración y control de la información en manos de unos pocos ("*Big Brother*"), y por el otro, el acceso irrestricto a la información como una suerte oráculo al alcance de todos. A esta altura, la mención de las distopías del siglo XX de Aldous Huxley[8] y Eric Blair —mejor conocido como George Orwell—[9] resulta inevitable.

En sintonía con lo anterior, Zygmunt Bauman entiende que vivimos en los tiempos del modelo post-panóptico, sujetos al control de vigilantes que ya no tienen la necesidad de atarse al espacio para cumplir con su tarea, ni de encerrar al sujeto a observar en instituciones totales. En otras palabras, el control (electrónico) se ejerce en tiempo real y a distancia, con un grado de eficiencia aún mayor. No olvidemos que por diversas razones (por ejemplo, seguridad pública, control del tránsito, cuidado de plazas, etcétera) nuestros movimientos quedan registrados, día a día, en sistemas de cámara de video instalados en espacios públicos.[10] Este fenómeno debe ser advertido, aunque resulta obvio que la tecnología no es más que

(8) Huxley, Aldous, *Un mundo feliz*, Bs. As., Sudamericana, 1958.

(9) Orwell, George, *1984*, Madrid, Salvat, Editores S. A., 1971.

(10) Merece mencionase la resolución 415/2004 del Ministerio de Justicia, Seguridad y Derechos Humanos, en virtud de la cual se creó el registro de huellas digitales genéticas, en el ámbito de la Policía Federal Argentina, la existencia de sitios de Internet como "23andMe", etcétera.

una herramienta, en sí misma "neutral"; por lo que corresponde centrar el debate en la forma y los fines con que se la emplee en el caso concreto.

No podemos dejar de mencionar en estos párrafos introductorios, la proliferación de herramientas de uso civil como "Google" y sus distintas aplicaciones,[11] *Facebook*[12] *You Tube, Fotolog, Twitter,* etcétera, en las cuales se perciben importantes cambios culturales en torno a la distinción entre lo público y lo privado, con fuerte impacto en el sustrato material del bien jurídico en trato. Esta cuestión, sin perjuicio de que su debido abordaje corresponde a la sociología, deviene palpable, y en esa dirección se ha dicho, por ejemplo, que:

> "... la intimidad se mira como un valor retrógrado, represivo, puritano (…) De ahí el auge, a veces desmedido de los *reality shows*, donde la vida transcurre en vivo y a la vista de audiencias multitudinarias; de facebooks y sitios similares donde cada uno muestra sus fotos, sus preferencias, sus conversaciones, sus amigos, su humor, sus datos de contacto; de blogs que lo cuentan todo. No hay filtros, o siquiera los menos posibles, para no traicionar el ideal de total transparencia…"[13]

Asimismo, se sostiene que *Twitters, Facebooks* y demás "bellezas informáticas" han logrado meterse en la vida privada de todos los que, muchas veces involuntariamente y sin ningún tipo de aviso previo, son sometidos a vejámenes, indiscreciones y bochornos y que:

> "… de nada se vale que uno se resguarde evitando pertenecer a red social alguna. Nada importa. Puede haber 'otros yo' que con tu nombre digan lo que les dé la gana y hablen por uno dando opiniones que nada tienen que ver con nuestra ideología

(11) Sobre este tema se recomienda la lectura del siguiente trabajo: Palazzi, Pablo A., "Google y el Derecho a la Privacidad sobre las búsquedas realizadas en Internet", *RCE* n° 74, 2006, pp. 31/40.

(12) Se ha destacado que "Lo extraordinario de Facebook respecto de Google es que no hacen falta algoritmos para conocer las preferencias del público. Las personas ceden esta información por voluntad propia". Ver Torres, Ariel, "¿Es Facebook el próximo Google?", en diario *La Nación*, Bs. As., edición impresa 09/01/2011, p. 2.

(13) Batallanez, Teresa,"La intimidad al desnudo", en revista *La Nación*, Bs. As., 09/01/2011, p. 74.

> de vida (…) Casi todas las constituciones democráticas, incluida la argentina, resguardan el derecho a la intimidad, y en casi todas las sociedades es negada, burlada y ofendida (…) hoy en día no sólo se trata del espionaje político para detectar enemigos opositores, sino de pura y dura violación del sagrado derecho a ser quien uno quiera ser sin la obligación de compartirlo con desconocidos".(14)

Al mismo tiempo, resulta paradojal que la mayoría de los usuarios de Internet no confíen en la seguridad de la red, más no adopten recaudo alguno a fin de utilizarla de modo seguro —por ejemplo: *firewalls*, claves seguras, cifrado y borrado seguro de datos, antivirus y anti-*spywares* actualizados, navegación anónima, etcétera—. En este punto, lejos de propiciar la incursión en políticas paternalistas o perfeccionistas, creemos que los Estados debieran incluir programas públicos destinados a fomentar el uso responsable e informado de estas nuevas tecnologías, lo que entendemos hallaría asidero y armonía con el carácter de *ultima ratio* del sistema penal. De lo contrario, antes de implementar medidas de prevención, seguramente más idóneas, seguiremos recurriendo al derecho penal en su función preponderantemente simbólica, si tenemos en cuenta el alto porcentaje —"cifra negra"—, que caracteriza a estos delitos y las dificultades que éstos presentan de cara al dictado de una eventual sentencia de condena.(15)

De esta manera, para dotar de racionalidad y proporcionalidad a la potestad punitiva del Estado no debería perderse de vista cuáles son los contornos actuales del bien jurídico "privacidad" a la luz de las nuevas prácticas y costumbres sociales, deteniéndonos unos instantes, en el rol de la víctima, en función de su "autopuesta" en peligro —consciente o no— como elemento de recorte de la tipicidad objetiva o, en su defecto, como pauta mensurativa de la pena. Con esto, no buscamos relativizar la trascendencia del bien jurídico sino evitar una aplicación de las normas mecánica y ajena de la realidad, que se base en una visión idealizada de

(14) Pinti, Enrique, "*1984 es el pasado*", en revista *La Nación*, 26/12/2010, p. 18.

(15) Así se ha informado que: "... las encuestas indican que cada cuatro delitos informáticos, sólo uno es denunciado. La conducta que con mayor frecuencia se reporta es el robo de contraseñas o claves de acceso. En los tribunales de la Capital Federal ya se registraron 8425 denuncias por "ciberdelitos" durante los últimos cuatro años y medio" (fuente: Profesional.com del 28/06/2010).

la sociedad que sólo persiga una finalidad preventivo general, en su faz positiva. En otras palabras, la conducta del usuario es imprescindible en la búsqueda de la seguridad informática, y por lo tanto, el Estado debe asumir la obligación de concientizar a la población acerca de los riesgos que conlleva el uso desaprensivo de estas herramientas tecnológicas, pues sólo así cada individuo será realmente libre a la hora de ejercer su derecho a la privacidad en el espacio virtual.

Asimismo, cabe apuntar que en este mundo globalizado las desigualdades sociales se manifiestan también en torno al acceso y manejo de estos nuevos instrumentos, verificándose una ostensible "brecha digital",(16) dentro de las fronteras de un país, e incluso entre los diferentes Estados Nación; circunstancia que no sólo parece otorgar razón a quienes endilgan al proceso de mundialización —fuertemente favorecido por las nuevas tecnologías de la información— un carácter unidireccional, sino que también plantea serias dificultades a los sistemas de administración de justicia locales, si se tiene en cuenta que el ciberespacio no se ve limitado por reglamentaciones de derecho interno. Sobre este tópico, en los debates parlamentarios se dijo que debía brindarse:

> "... la mayor libertad posible en el uso de los ordenadores, de la red y de las comunicaciones, porque es la única forma en que se podrá aumentar la posibilidad de que el usuario —en el caso de la Internet— se apropie de una tecnología que no sea de dominio exclusivo de grupos o países (…) Después de la escritura y de la imprenta aparece lo que hoy se denomina la hipermedia, el hipertexto, la red o el ordenador. Al igual que la escritura y la imprenta va a modificar no solamente las formas del desarrollo que el ser humano tiene en cuanto a la comunicación, sino que también modificará la relaciones de producción (…) la tecnología no es buena ni mala, ni neutral, está ahí, construye las sociedades y la cultura, se mete en la dinámica social y modifica las relaciones sociales".(17)

(16) Ver al respecto, el contenido de la *Declaración del Milenio* aprobada por la Asamblea General de las Naciones Unidas, [en línea] http://www.un.org/spanish/milenio/ares552.pdf.

(17) Nemirovsci, Osvaldo M., Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión - 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

En razón de lo expuesto, las posibilidades que brinda la tecnología para vulnerar el bien jurídico privacidad conlleva serios riesgos para la vigencia real del Estado de derecho, correspondiendo a sus distintas agencias —especialmente, las ejecutivas— no sólo abstenerse de espiar indebidamente a los individuos, sino también asumir la obligación y el desafío de idear e implementar políticas públicas que resguarden esta manifestación de la libertad individual. La vigencia práctica de los derechos constitucionales y las garantías del justiciable reclama más que nunca el respeto de los límites formales y materiales que racionalizan y humanizan el ejercicio de la potestad punitiva. En esta convicción, rechazamos los intentos de flexibilización de garantías procesales y sustantivas a través de la aceptación de un nuevo estándar procesal que ha recibido en la doctrina la denominación de "Derecho Procesal Penal del Enemigo",[18] que bajo el argumento de combatir nuevas y más peligrosas formas de delincuencia transnacional, se propone reformular o "modernizar" las bases del derecho penal liberal.

Por último, y sin perjuicio de exceder el objeto de este trabajo en función del bien jurídico que nos ocupa, baste mencionar que la informática en general, representa riesgos para los Estados Nación, y tanto más, a medida que avanza la automatización de servicios públicos o el denominado *e-goverment*.

4 | Marco normativo convencional, constitucional y legal

La **privacidad** halla recepción positiva en diversos instrumentos normativos de naturaleza convencional, constitucional y legal. Así, nuestra Carta Magna en sus arts. 18 y 19 establece que "el domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación" y que "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los

(18) Sobre este tema, ver Muñoz Conde, Francisco, "De las prohibiciones probatorias al Derecho procesal penal del enemigo", *Claves del Derecho Penal*, Bs. As., Hammurabi, 2008..

magistrados". Por otro lado, la reforma constitucional de 1994 influyó en la protección jurídica de este derecho/garantía, en su faz de libertad de autodeterminación informativa, ya que estableció en el art. 43 que toda persona podrá interponer acción de amparo "… para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística". A su vez, mediante la cláusula contenida en el art. 75, inc. 22 CN incorporó con jerarquía constitucional los tratados internacionales de Derechos Humanos, destacándose en lo que a la libertad de intimidad o privacidad se refiere, el art. 11 (incs. 2 y 3) de la Convención Americana de Derechos Humanos, el art. 17 del Pacto Internacional de Derechos Civiles y Políticos, el art. 12 de la Declaración Universal de Derechos Humanos, y el art. 11 de la Declaración Americana de Derechos y Deberes del Hombre.

No puede pasarse por alto la opinión de un sector de la doctrina, en cuanto se refiere a la irrupción de un nuevo bien jurídico: "la protección de los datos personales". De esta manera, en relación a los tipos penales previstos en los arts. 117 *bis* y 157 *bis* del Código Penal, se ha dicho que:

> "… no protegen los bienes jurídicos tradicionales como la fe pública, la confidencialidad o la privacidad, sino uno nuevo que es la protección de los datos personales (…) La incolumidad de la información almacenada en bases de datos debe preservarse porque sobre esos datos se toman decisiones y ellas pueden perjudicar y afectar a individuos y titulares de datos personales".(19)

Creemos que el reconocimiento de este nuevo bien jurídico, distinto de aquél previsto en el epígrafe del Capítulo III, Título V, Libro II del Código Penal, si bien posee atendibles fundamentos, resulta opinable desde la perspectiva que imponen los principios jurídicos reductores del ámbito de intervención del derecho penal, pues se corre el riesgo de ampliar la potestad punitiva en desmedro del justiciable; máxime, cuando estamos

(19) Palazzi, Pablo A., *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388*, Bs. As., Abeledo-Perrot, 2009, p.142.

ante delitos de acción privada, pues la tesitura antedicha podría incidir en adjudicar legitimación procesal para querellar, a quien de otra manera, carecería de tal derecho. Además, sin soslayar la existencia de nuevos derechos y garantías, téngase presente que durante la Convención Constituyente, al analizar el texto del art. 43 CN, se dijo que:

> "... el tercer párrafo alude a un ámbito de derechos personales en el marco de una realidad donde la acumulación de información y su manipulación han generado amenazas y daños tremendos a las personas y a sus derechos. Estamos en presencia de una acción destinada a proteger el derecho a la privacidad, a la intimidad, derecho contemplado en el art. 19 de la CN. Con ello se incorpora una protección efectiva ante el avance de un fenómeno nuevo y poderoso que puede exceder el ámbito de las garantías y defensas clásicas (…) Esta incorporación (…) es por demás relevante, máxime considerando las aciagas épocas del autoritarismo, en donde la inclusión de datos de personas en determinados registros podía implicar desde la incorporación en las llamadas "listas negras" con discriminaciones y atropellos consiguientes, hasta la pérdida de la libertad o la vida".[(20)]

En esta inteligencia, en la hermenéutica de la norma penal, el bien jurídico es la privacidad, y la protección de datos personales es una manifestación del primero, y no constituye un concepto jurídico autónomo, encontrando un claro referente o sustrato material en dicho atributo de la personalidad.

A nivel interno, el derecho a la privacidad se encuentra contenido en las constituciones locales,[(21)] como también en los códigos sustantivos, diversas leyes especiales y los digestos de forma. Así, a título meramente ilustrativo, podemos mencionar los arts. 1071 CC; 153 a 157 *bis* CP; 235 y 236 CPPN y las leyes 24.766, 25.326, 25.520 y 25.873; etcétera.

(20) Debate del dictamen de la Comisión de Redacción en los despachos en mayoría y minoría originados en la Comisión de Nuevos Derechos y Garantías (Orden del Día Nº 11), Sesión 3ª, reunión 31ª, 16/08/1994, p. 4284, Solicitada de la Sra. Convencional Arellano, [en línea] http://www.infoleg.gov.ar.

(21) Ver arts. 12 inc. 3, 13 inc. 8 y 16 de la Constitución de la CABA; arts. 12 incs. 3, 4, 5 y 20 inc. 3 de la Constitución de la provincia de Buenos Aires, etc.

5 | Análisis dogmáticos de los tipos penales previstos en la ley 26.388

5.1 | Artículo 153 del Código Penal

La sanción de la ley 26.388 obedeció a la necesidad de actualizar la legislación penal a las demandas de la "sociedad de la información", en la que a la par de observarse el decrecimiento del uso del correo epistolar, se produjo la irrupción de nuevas formas de comunicación, tales como el *e-mail,* el *chat* (palabra del idioma inglés que significa "charla" o "charlar"), las redes sociales, el SMS *(Short Message Service)*, etcétera.

En este sentido, resultan ilustrativas las palabras del diputado Nemirovsci:

> "Obviamente, al redactar el Código Penal el legislador no podía prever en 1921 —tampoco en ninguna de las 800 modificaciones que se han introducido desde entonces— la comisión de delitos a través de la informática y de las nuevas tecnologías. Por eso hoy le damos la bienvenida a toda iniciativa que venga a llenar ese vacío legal (…) no estamos sancionando una ley de delitos informáticos que crea nuevas figuras penales. Simplemente estamos adaptando los tipos penales a las nuevas modalidades delictivas".[22]

A su vez, el proceso legislativo —iniciado en el año 1996 con el proyecto de Leonor E. Tolomeo— se aceleró al hacerse público en el año 2006 un caso de intrusismo informático sobre correos electrónicos pertenecientes a políticos, jueces y periodistas, de reconocida trayectoria.[23]

(22) Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión – 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

(23) A fin de conocer los antecedentes históricos de la Ley 26.388, publicada en el BO el 25/06/2008, puede consultarse el siguiente trabajo: Fillia, Leonardo C.; Monteleone, Romina *et al.*, "*Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación*", *La Ley* Suplemento Penal, agosto 2008, p. 15. Asimismo, en relación a los hechos de público conocimiento que aceleraron el *iter* legislativo, resulta pertinente citar las siguientes expresiones de la diputada Norma Elena Morandini: "Se moderniza el espionaje, que ahora es electrónico, pero no se erradica la vieja práctica del chantaje. Los datos jaqueados, como demostró la denuncia que inspiró los proyectos en que se basa el dictamen de comisión,

Este episodio colocó nuevamente en la escena pública la discusión sobre la interpretación del derogado art. 153 del Código Penal a la luz del principio de legalidad. Antes de la sanción de la ley 26.388, un sector de la doctrina proponía una interpretación extensiva, teleológica, progresiva o dinámica de las leyes por imperio histórico. Así, por ejemplo, el constitucionalista Gregorio Badeni opinaba que "frente a tales adelantos es necesaria una razonable interpretación dinámica de las leyes para que, sin necesidad de acudir a su reforma, se pueda evitar que queden a la zaga de la realidad social" y Creus —en sintonía— afirmaba que "salvo casos de conceptualizaciones terminantemente limitativas de su sentido, acompañar las transformaciones técnicas ampliando, para comprenderlas, el significado de las acciones típicas respecto del que poseían en tiempos pretéritos de la evolución técnica no es hacer analogía sino interpretar".(24) Otro segmento de la academia, rechazaba esta exégesis de la ley, acusándola de constituir una forma solapada de extensión analógica del tipo penal, vedada al intérprete por imperio del principio de legalidad, en su función de *lex stricta*. La jurisprudencia no era uniforme sobre el tópico, se establecieron, como habitualmente sucede, dos posturas. La Sala VI de la Cámara Nacional en lo Criminal y Correccional —integrada por los Dres. Ameghino Escobar, Elbert y González—, en el caso "Lanata, Jorge s/ desestimación", de fecha 04/03/1999, sostuvo que :

> "Nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada. En tal sentido la correspondencia y todo lo que por su conducto

se utilizaron para controlar los movimientos de un periodista, un funcionario o un juez, para mapear sus relaciones y hacerles sentir (insisto con esta idea) que están siendo controlados. De alguna manera todos tenemos naturalizado que algunas cuestiones no se pueden hablar por teléfono…". (Ver Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión - 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

(24) Creus, Carlos, "El miedo a la analogía y la creación de vacíos de punibilidad en la legislación penal (intercepción de comunicaciones telefónicas y apropiaciones de e-mail)", *JA*, 1999-IV-869. Este autor, pese a estar a favor de la interpretación dinámica de la ley penal, sostenía que considerar como objeto del delito de violación de correspondencia al correo electrónico era hacer analogía, ya que sus textos podían ser leídos en la pantalla tal como le han sido remitidos al destinatario. Nada se "abre", pues nada está cerrado. Sin embargo, opinaba que eso no sucedía, si se consideraba objeto material de los delitos previstos en el art. 153 (segunda figura) y 155 del Código Penal al correo electrónico, ya que en estos casos la acción típica no es la de "abrir" sino la de "apoderarse" y "publicar respectivamente".

> pueda ser transmitido o receptado, goza de la misma protección que quiso darle el legislador al incluir los arts. 153 a 155 del CP, en la época de su redacción, cuando aún no existían estos avances tecnológicos".

Sin embargo, algunos tribunales adoptaron la postura contraria, como el Juzgado Nacional en lo Correccional N° 9, que en la causa "Gálvez, Esteban", del 11/04/2007, rechazó la asimilación del correo electrónico a la correspondencia privada, señalando que:

> "... el principio de máxima taxatividad legal e interpretativa se manifiesta mediante la prohibición absoluta de la analogía 'in malam partem', lo que se verificaría si en la especie se intentara forzar la interpretación que inveteradamente se ha dado no sólo en lo concerniente al objeto de protección de la norma del art. 153 del código sustantivo, sino a sus quehaceres típicos, por lo que resulta inaceptable dar cabida a la presente querella desde la norma escogida por la querella como la infringida por los intrusos, que accedieron a su correo del servidor Yahoo de Argentina SRL".

Esta discusión se encuentra zanjada a partir a partir de la entrada en vigencia de la ley 26.388, cuyo texto reza lo siguiente en su art. 4:

> "Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida".

En primer término, es necesario advertir que el correo electrónico es un medio de comunicación inseguro que circula por la red a través de millones de nódulos y *routers*, pudiendo ser captado en cualquiera de estas fases. A su vez, el 50% del tráfico mundial de Internet pasa siempre por

el Estado de Virginia, EEUU, tal como lo revela Bárbara Cassin.[25] Como hemos anticipado, estas comunicaciones electrónicas pueden ser objeto de accesos ilegítimos o legítimos. No olvidemos que los ISP y los motores de búsqueda pueden registrar los datos de tráfico en servidores, o que empresas tales como *Hotmail, Gmail o Yahoo* —generalmente a través de rutinas automatizadas— pueden filtrar nuestras comunicaciones electrónicas a fin de optimizar el servicio (por ejemplo: eliminación o bloqueo de amenazas lógico informáticas, desvío de correo no deseado, etcétera). Así, es claro que más allá de que una finalidad legítima en su origen pueda mutar su naturaleza (transformándose en ilegítima), estas herramientas de comunicación moderna presentan no pocas vulnerabilidades desde el punto de vista técnico.

Núñez, definió a la correspondencia como "la comunicación por carta, pliego o despacho telegráfico, fonográfico o de otra naturaleza, enviada por un remitente a un destinatario", en la que se establece un diálogo.[26] Por papeles privados se entiende cualquier expresión de ideas escrita comprendida dentro del ámbito de reserva de una persona, y a su vez, a partir de la redacción típica del delito de "apoderamiento indebido de correspondencia u otro papel privado" parece englobarse dentro del género "papeles privados" a cartas, pliegos y despachos. Antes de la reforma, se decía que resultaba esencial que el papel escrito "se encuentre dispuesto en forma tal que no baste su simple desdoblamiento para que el texto se ofrezca a la vista" y que su contenido revista el carácter de íntimo o personal, no siendo aptas para configurar el tipo, por ejemplo, una simple nota o publicidad comercial.[27]

La ley 26.388 incluyó dentro del concepto amplio de **correspondencia** las comunicaciones electrónicas, apelando a un término susceptible de adaptarse, sin necesidad de una nueva reforma legal, a las incesantes innovaciones que deparan los avances tecnológicos a estas formas de

(25) Cassin, Bárbara, *Googléame. La segunda misión de los Estados Unidos*, trad. de Víctor Goldstein, Bs.As., Fondo de Cultura Económica, 2008, p. 25.

(26) Nuñez, Ricardo C., *Manual de Derecho Penal. Parte especial*, 2° ed. actualizada por Víctor F. Reinaldi, Córdoba, Marcos Lerner, 1999, p. 175.

(27) Ossorio y Florit, Manuel, *Código Penal de la República Argentina. Comentarios. Jurisprudencia. Doctrina. Legislación complementaria*, Bs. As., Universidad, 1979, p. 237.

comunicación.[28] Si bien la opción del codificador resulta adecuada, será tarea de la jurisprudencia delinear los precisos alcances de este elemento del tipo penal recurriendo a la función reductora del bien jurídico y a los mandatos del principio de legalidad. Por ello, y a título meramente enunciativo, pensamos que la inclusión legal no modifica las exigencias tradicionales de que la comunicación electrónica se encuentre dirigida a una persona —incluso podría tratarse del propio remitente que se envía un mensaje a sí mismo, por ejemplo, a modo de borrador o para acceder desde cualquier lugar al documento, si atendemos al concepto detrás del género papeles privados— y que su contenido revista carácter privado, no siendo accesible a simple vista. Esta aclaración viene al caso, pues en la Red existen numerosas operaciones automatizadas, donde difícilmente pueda afirmarse que se ha procurado entablar un diálogo con un interlocutor frente a la ausencia de un componente volitivo en dicho proceso comunicacional. Por su supuesto, la cuestión es compleja, pues estas funciones siempre son precedidas de una tarea de programación, por lo que a los fines de evitar una ampliación ilegítima del tipo penal, deberá establecerse en primer lugar a la naturaleza del contenido de la comunicación electrónica. Al respeco, Palazzi se pregunta si debe haber al menos un emisor o destinatario humano, respondiendo que de entenderlo así quedaran fuera de protección penal numerosas situaciones, ya que "hoy en día la relación con numerosas empresas y sistemas está automatizada a través de ordenadores, y con ellos también hay comunicación".[29] No estamos de acuerdo con este razonamiento porque la interpretación histórica del art. 153 del CP, el significado del término "comunicación"[30] y la naturaleza del bien jurídico, creemos que exigen, al menos, que interactúe un ser humano en alguna de las fases del proceso: emisor - mensaje - destinatario.

(28) Nótese que en una reciente nota titulada "El correo electrónico le deja su lugar a las redes sociales y al chat", se advierte que el uso extensivo de los mensajes de texto y las recientes modificaciones que realizó Facebook en su servicio de mensajería replantean el uso del e-mail en determinados entornos. Así se ha dicho, por ejemplo, que "el futuro de los mensajes es más en tiempo real, más dialogado y más informal (…) el medio no es el mensaje. El mensaje es el mensaje", ver [en línea], *lanación.com,* 26/12/2010.

(29) Palazzi, Pablo A., *op. cit.*, p. 75.

(30) Según el Diccionario de la Real Academia de Lengua Española: 1) Acción y efecto de comunicar o comunicarse; 2) Trato, correspondencia entre dos o más personas; y 3) Transmisión de señales mediante un código común al emisor y al receptor.

Volviendo al tratamiento dogmático de las figuras penales previstas en el art. 153 del CP, desde la perspectiva de los delitos informáticos, es menester señalar que esta disposición legal, en primer término, sanciona al que abriere o accediere indebidamente a una comunicación electrónica que no le esté dirigida.

En opinión de Arruvito:

> "... las comunicaciones electrónicas —que son el objeto protegido en la figura— se encuentran guardados, alojados, archivados, etc. en una cuenta de correo electrónico. O sea que para violentar la intimidad de la víctima, previamente debe tenerse acceso a la cuenta de ***e-mail.*** Recién una vez allí, el agresor podrá abrir, acceder, apoderarse, suprimir, desviar, interceptar o captar una comunicación electrónica".(31)

Vale aclarar que si bien esto puede suceder cuando se trata de correos electrónicos que funcionan bajo un protocolo SMTP,(32) existen otras comunicaciones electrónicas distintas del *e-mail* que no requieren, por así decirlo, de este paso previo.

Cabe señalar que **abre** quién descubre o hace patente aquello que está oculto, removiendo los obstáculos que lo cierran o protegen, a fin de impedir a terceros imponerse de su contenido; **accede** quien entra, ingresa u obtiene el objeto de protección legal. En este punto, corresponde hacer una distinción desde el sentido semántico de estos verbos típicos, pues bien podría decirse que un *e-mail* puede ser accedido aun cuando ya se encontrare abierto. Sin embargo, partiendo de la aclaración efectuada por el legislador respecto de la figura de "apoderamiento indebido de comunicaciones electrónicas" (**aunque no esté cerrado**) es posible sostener la interpretación contraria. Es decir, que en el acceso se requiere que las comunicaciones electrónicas estén cerradas;(33) no sería típica la conducta de

(31) Arruvito, Pedro A., "Ley 26.388. Violación del e-mail o comunicación electrónica", *Doctrina Judicial*, Bs. As., La Ley, 18/02/2009, p. 403.

(32) No así con el protocolo POP3, que funciona con programas como el Outlook, *Incredimail, Thunderbird, Windows Mail,* etc.

(33) Entiéndase por "cerradas", que para acceder, sea necesario iniciar una sesión y consecuentemente ingresar un nombre de usuario y contraseña.

la persona que se imponga del contenido de un correo electrónico o de un mensaje de texto, que ha quedado expuesto a la vista de terceros por un descuido de su titular.[34] Desde otro enfoque, se refiere que no queda en claro en qué se distinguen los verbos típicos abrir y acceder, y que respecto de este último podría decirse que el sujeto activo "… si bien llega a conocimiento del mail accedido, ello fue logrado sin haberlo abierto (puede ser porque no haya sido necesario 'abrir' el mail porque ya se encontraba abierto, o porque otra persona —la que sí lo abrió— se lo reenvió ya 'abierto')".[35] En síntesis, nos parece que la redacción legal no es clara, debiendo primar el criterio restrictivo por imperio del principio de legalidad. Por otro lado, bien podría afirmarse que un correo electrónico puede abrirse muchas veces porque las condiciones de seguridad que resguardan su contenido de la mirada de terceros (nombre de usuario, clave o contraseña, etc.), a diferencia del correo epistolar, carecen de soporte físico.[36]

Ahora bien, la apertura o el acceso de las comunicaciones electrónicas, debe realizarse **indebidamente**, es decir, sin derecho o autorización del titular. Según lo expresaba Molinario

> "... la voz indebidamente tiene más de un papel (…) Uno es recalcar que el dolo debe ser directo (…) Otro, que evidentemente no exista derecho a ejecutar esa acción. En primer lugar, por supuesto, tienen tal derecho las personas autorizadas por el destinatario. En general, los tribunales se han referido a este segundo aspecto tomando en cuenta diversos casos. Entre ellos, el de autorizaciones que diversas leyes[37] dan a ciertos funcionarios en casos determinados (hay autorizaciones administrativas, y por otro lado, judiciales) o el ejercicio de la patria potestad o de la tutela o curatela (…) o cuando entran en juego razones humanitarias…".[38]

(34) En contra de esta interpretación: Palazzi, Pablo A., *op. cit.*, p. 76/77.

(35) Arruvito, Pedro A., *op. cit.*

(36) A favor de la tesis según la cual la comunicación electrónica debe estar cerrada. Ver Ghersi, Sebastián, "Violación de secretos y privacidad. Los documentos electrónicos", en *Revista Jurídica La Ley*, 2008-F, p. 731.

(37) Por ejemplo: ley 25.520, ley 25.873, art. 236 CPPN, etc.

(38) Molinario, Alfredo J., *op. cit.*, p. 113.

En el mismo sentido, se pronuncia Palazzi quien entiende que la inclusión el término "indebidamente" tiene incidencia principalmente en la órbita del tipo subjetivo. De igual manera, se ha señalado que "con respecto al elemento subjetivo del tipo, la norma indica que el autor debe obrar a sabiendas o ilegítimamente, lo que significa saber claramente lo que hace o no hace y que ese hacer o no hacer es contrario a derecho. Estamos hablando de un dolo directo, no de uno indirecto o eventual".[39]

Sin embargo, creemos que esto se produce como un reflejo o consecuencia del juicio de tipicidad objetiva —función conglobante— en tanto el dolo exige el conocimiento y la voluntad de realización del tipo objetivo.[40] De esta manera, la exigencia típica opera por lógica sistemática al momento de analizar la eventual tipicidad objetiva de la conducta; es decir, este adverbio alude a la antinormatividad de la conducta, la que no se verificaría, por ejemplo, en caso de haber mediado el consentimiento del titular por ausencia de lesividad. Por lo demás, así como se ha criticado la voz "ilegítimamente" en el hurto (art. 162 del CP) por superflua, idéntica observación podría realizarse en este caso, aunque cabe aclarar que la inclusión del término obedeció principalmente al reclamo proveniente de empresarios del sector de la informática y las comunicaciones. Posiblemente hubiera sido preferible reemplazar el término en cuestión por la frase "violando sistemas de seguridad mínimos", siguiendo la línea ya trazada en el art. 1 inc. c) de la ley 24.766, respecto de la información confidencial, donde se requiere para su protección legal que dichos datos sean secretos, tengan valor comercial en función de la característica anterior y hayan sido objeto de medidas razonables, en las circunstancias, para mantenerlos así.

Finalmente, debe tratarse de una comunicación electrónica **que no le esté dirigida** al sujeto activo; dicho en otros términos, el autor de este delito no debe ser el destinatario de la comunicación electrónica, lo que en todo caso, se complementa con la exigencia de actuar en forma ilegítima.

(39) Romero, Rosario Margarita, Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión – 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

(40) Esto según el finalismo y las teorías que resultan tributarias a esta escuela dogmática.

Párrafo aparte, merece la discusión que plantea el monitoreo de correos electrónicos en el ámbito laboral, donde las comunicaciones electrónicas se han transformado en un recurso casi indispensable en la mayoría de las actividades. En estos supuestos, coincidimos con la doctrina mayoritaria de que el usuario no tiene un derecho a la privacidad sobre estas comunicaciones, en tanto constituyen herramientas de trabajo; sin perjuicio de ello, sería conveniente que el empleador notifique a cada usuario (empleado) los términos y condiciones que rigen el uso de tales elementos en el ámbito estrictamente laboral, evitando así la generación de eventuales conflictos futuros. Siguiendo este criterio, se ha proyectado la incorporación del art. 86 *bis* a la ley 20.744 (LCT), proponiéndose el siguiente texto:

> "Cuando el correo electrónico sea provisto por el empleador al trabajador en función o con motivo de una relación laboral, se entenderá que la titularidad del mismo corresponde al empleador (…) El empleador se encuentra facultado para acceder y controlar toda la información que circule por dicho correo electrónico laboral, como asimismo a prohibir su uso para fines personales. El empleador no podrá prohibir el uso de las direcciones de correo electrónico que pudiera tener el trabajador que sean de carácter personal o privado, aunque los mismos sean abiertos desde el lugar de trabajo. El empleador deberá asimismo, notificar fehacientemente al empleado su política respecto del acceso y uso de correo electrónico personal en el lugar de trabajo, así como las condiciones de uso y acceso al correo electrónico laboral al momento de poner a su disposición el mismo…".(41)

La segunda conducta receptada en el primer párrafo del art. 153 del CP consiste en **apoderarse** indebidamente de una comunicación electrónica **aunque no esté cerrada**. Se apodera de un correo electrónico quién lo pone bajo su poder, se lo apropia o lo retiene en su ámbito de dominio. Compartimos con Palazzi que el término "apoderarse" no requiere aquí los requisitos típicos del hurto, pues cuando es aplicado a elementos digitales el sujeto activo puede realizar la conducta sin necesidad de des-

(41) Ver [En línea] http://www.iprofesional.com/notas/70004-Proyecto-de-ley.html. Nos parece que el art. 1 de este proyecto no regula con claridad el uso del correo electrónico de carácter personal o privado, como acontecía en el art. 4 de un proyecto de la Diputada Bisutti de fecha anterior (expte. 2032-D-06).

apoderar al damnificado, tal como ocurría con la copia o el reenvío de un e-mail. En estos casos habría apoderamiento, más no desapoderamiento en sentido estricto, dado que la comunicación original permanecería en la bandeja de entrada del correo electrónico del usuario.(42) A su vez, el sujeto activo podría apoderarse del correo electrónico mediante su impresión, en cuyo caso, se apropiaría de su contenido, afectando el derecho a la privacidad del sujeto pasivo, con la salvedad de que obtendría para sí una copia en soporte material del mismo, lo que entendemos no obsta a la configuración del delito. En sentido coincidente, en la Cámara de Diputados, en relación al texto legal se expuso que "el término apoderamiento debe entenderse en un doble sentido. Apoderarse de una comunicación electrónica puede ser copiarla o apoderarse físicamente de una copia".(43)

Por último, el párrafo bajo análisis, prevé una tercera y última figura básica: la supresión o el desvío indebido de comunicaciones electrónicas que no estén dirigidas al sujeto activo. **Suprime** quién hace desaparecer, destruye u oculta, impidiendo la circulación; mientras **desvía**, el que le da a la comunicación electrónica un curso distinto al estipulado por el remitente. En ambos supuestos, el sujeto activo altera el destino del *e-mail*, SMS, MMS, etcétera.

Como en el caso anterior, para la configuración del delito es requisito, por un lado, que la conducta sea realizada sin derecho (indebidamente), y por el otro, la ajenidad del correo electrónico. La intención del legislador ha sido dejar fuera del espectro de conductas incriminadas las prácticas de filtrado automático de comunicaciones electrónicas que realizan los ISP y las empresas proveedoras del servicio de correo electrónico, en pos de optimizar su rendimiento, eliminado SPAM, virus, etcétera. La Senadora Vilma Ibarra enfatizó que:

> "… hay que dejar en claro para la interpretación ulterior de los jueces en materia de interpretación auténtica a efectos de que no queden dudas a quienes interpretan la ley de que la finalidad debe ser dolosa; o sea, debe existir un dolo específico del

(42) Palazzi, Pablo A., *op. cit.*, p. 78.

(43) Romero, Rosario Margarita, Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 35ª Reunión - 26ª Sesión Ordinaria, 25/10/2006 (versión taquigráfica).

> autor del delito (…) Muchas veces las empresas colocan filtros y desvían el spam, y esto no constituye la vocación dolosa de suprimirlo para causarle un daño al otro. Entonces, esto lo dejamos claramente especificado (…) la expresión indebidamente excluye, desde ya, la actividad empresarial para el desvío de spam".(44)

Debe distinguirse esta figura del denominado *sniffing* —derivado de la palabra *sniff*, que en inglés significa olfatear— donde no hay desvío de los paquetes de datos sino una triangulación entre ordenadores conectados a una misma red, a través de la cual es posible captar o acceder a esa información sin que emisor y destinatario lo adviertan. De esta forma, es posible apropiarse de claves, *e-mails*, y cualquier tipo de información, ya sea de carácter público o privado.

Justamente, el segundo párrafo del dispositivo legal en estudio castiga con prisión de quince días a seis meses al "… que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido".

Nuestra Constitución Nacional consagra expresamente la inviolabilidad de la correspondencia epistolar, pero por razones obvias, nada dice sobre la privacidad de las telecomunicaciones. En efecto, se ha señalado que "...la letra de la Constitución Nacional menciona solamente la privacidad de las comunicaciones epistolares: no pudo referirse a las comunicaciones telefónicas; pero es evidente que analógicamente cabe extender a estas la inviolabilidad prevista para aquellas…",(45) a lo que cabe agregar que "... ha sido voluntad de la ley 19.798 de telecomunicaciones que no sólo el intercambio epistolar quede en secreto, sino además la palabra transmitida por el cable telefónico (...) La ley 19.798 de telecomunicaciones se ha propuesto tutelar la personalidad integral del hombre a la luz del precepto constitucional del art. 18 …".(46)

(44) Ibarra, Vilma, Cámara de Senadores de la Nación, 18° Reunión (14° Sesión Ordinaria) 28 de noviembre de 2007, Versión Taquigráfica.

(45) Cám. Nac. Com., Sala D, mayo 18-1989, La Ley 1989-D-329.

(46) Cám. Nac. Crim. y Corr. , Sala VI, 04/11/1980, "Landeira de Ferradás, Josefina E.", La Ley 1981-B-193; JA 1981-II-333 y ED, 92-828.

En el derecho público provincial, hay disposiciones que expresamente protegen la privacidad de las comunicaciones telefónicas; tal es el caso, por ejemplo, de la Constitución de la provincia de San Luis.[47] Por su parte, nuestro Código Penal hasta la entrada en vigencia de la ley 26.388 no contenía disposición alguna que sancione la violación de las telecomunicaciones.[48]

En el plano normativo nacional, la ley 19.798 define el término **telecomunicaciones** como toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos (art. 2). Si bien esta ley no contiene disposiciones penales, establece que la correspondencia de telecomunicaciones es inviolable, procediendo su interceptación sólo a requerimiento de juez competente (art. 18) y que esta inviolabilidad importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos (art. 19).

Debe tenerse presente, además, la sanción de la ley 25.873 (BO 09/02/2004) en cuyo marco se ha establecido que todo prestador de servicios de telecomunicaciones:

> "… deberá disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. Los prestadores de servicios de telecomuni-

(47) Art. 33: "Los papeles particulares, la correspondencia epistolar, las comunicaciones telegráficas, telefónicas, teletipeado o de cualquier otra especie o por cualquier otro medio de comunicación, son inviolables y nunca puede hacerse registro de las mismas, examen o intercepción sino conforme a las leyes que se establecen para casos limitados y concretos. Los que son sustraídos, recogidos u obtenidos en contra de las disposiciones de dichas leyes, no pueden ser utilizados en procesos judiciales o administrativos".

(48) Creus, Carlos, "El miedo a la analogía...", *op. cit.* Antes de producirse el auge de la tecnología inalámbrica, sostenía que era aconsejable pero no imprescindible una reforma, ya que una conversación telefónica era confiada al cerramiento de un cable que valía (en cuanto a la tipicidad penal) como el sobre de una carta; de manera que quien penetraba aquél cerramiento lo "abría" y si lo hacía fuera de los supuestos autorizados lo hacía "indebidamente".

> caciones deberán soportar los costos derivados de dicha obligación y dar inmediato cumplimiento a la misma a toda hora y todos los días del año. El Poder Ejecutivo nacional reglamentará las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o el Ministerio Público" (art. 45 *bis*).

Asimismos éstos:

> "…deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. La información referida en el presente deberá ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años" (art. 45 *ter*).

Además, en el art. 45 *quater* se introduce una cláusula de naturaleza resarcitoria mediante la cual el Estado Nacional asume responsabilidad por los eventuales daños y perjuicios que pudieran derivarse para terceros.

Posteriormente, desde la óptica de la protección del derecho constitucional a la intimidad y a la vida privada, la situación se vio agravada a raíz del dictado del decreto reglamentario 1563/2004 —suspendido por el decreto PEN 357/2005—, finalmente declarado inconstitucional por el Máximo Tribunal de la República, en el caso "Halabi, Ernesto c/PEN ley 25.873 dto. 1563/04 s/ amparo ley 16.986", del 24/02/2009. En este pronunciamiento, la Corte definió y precisó los alcances de los derechos de incidencia colectiva referentes a intereses individuales homogéneos,[49] y

(49) Estos derechos surgen del segundo párrafo del art. 43 de nuestra Carta Magna. En particular se dijo que: "... en estos casos no hay un bien colectivo, ya que se afectan derechos individuales enteramente divisibles. Sin embargo, hay un hecho, único o continuado, que provoca la lesión a todos ellos y por lo tanto es identificable una causa fáctica homogénea. Ese dato tiene relevancia jurídica porque en tales casos, la demostración de los presupuestos de la pretensión es común a todos esos intereses, excepto en lo que concierne al daño que individualmente se sufre. Hay una homogeneidad fáctica y normativa que lleva a considerar

señaló a las **acciones de clase** como el medio o carril procesal idóneo para canalizar jurisdiccionalmente la defensa de estos intereses. Al mismo tiempo, y en relación a la cuestión de fondo, destacó que: "… el Tribunal Constitucional de España, mediante su sentencia del 5 de abril de 1999 (STC 49/1999), con cita del Tribunal Europeo de Derechos Humanos (TEDH), ha sostenido que 'si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones (...) quedaría materialmente vacío de contenido…"; y que:

> "... es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos. Se añade, a ello, la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales. En suma (…) resulta inadmisible que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la Administración quede en manos de la más libre discreción de estos últimos, afirmación que adquiere primordial relevancia si se advierte que desde 1992 es la Dirección de Observaciones Judiciales de la SIDE, que actúa bajo la órbita del poder político, la que debe cumplir con los requerimientos que formule el Poder Judicial en orden a la interceptación de comunicaciones telefónicas u otros medios de transmisión que se efectúen por esos circuitos".[50]

razonable la realización de un solo juicio con efectos expansivos de la cosa juzgada que en él se dicte, salvo en lo que hace a la prueba del daño" (consid. 12 del voto de la mayoría).

(50) Consids. 24 y 26 del voto de la mayoría, suscripto por los Ministros Lorenzetti, Higthon de Nolasco, Maqueda y Zaffaroni.

Luego de esta introducción, daremos paso al análisis de los requisitos típicos de esta figura. Incurre en este delito quien sin autorización **intercepta** (se apodera, detiene, obstruye, o interrumpe una vía de comunicación) o **capta** (percibe, obtiene, recoge) comunicaciones electrónicas o telecomunicaciones de carácter privado o de acceso restringido. La técnica legislativa empleada es criticable, pues no resultará tarea sencilla distinguir (si es que esa fue la intención del codificador penal) entre, por un lado, comunicaciones electrónicas y telecomunicaciones, y por el otro, sistema de carácter privado y sistema de acceso restringido. En primer término, porque el art. 77 del CP no establece una definición de "comunicación electrónica" y atento la amplitud otorgada al término "telecomunicación" en la ley 19.798, este último concepto parece abarcar al primero. Así, en el Informe Preliminar de la Comisión de Estudio de Correo Electrónico, elaborado en el ámbito de la Secretaría de Comunicaciones, dependiente del Ministerio de Infraestructura y Vivienda, de fecha 07/08/2001, se explicaba que:

> "... el diccionario general de la lengua española define el termino correo electrónico como correspondencia que se transmite por un ordenador a un usuario concreto. Es esta la acepción que receptamos en el presente anteproyecto de ley que sometemos a consideración, haciendo especial referencia a que solo se considera correo electrónico al que se transmite por medio de una red de interconexión entre computadoras, excluyendo del ámbito de esta ley a cualquier otra modalidad de mensaje transmitido por medios electrónicos, como por ejemplo los emitidos a través del servicio de radiocomunicaciones para ser receptados por un móvil portátil (pager) o los recibidos a través del servicio de audio texto".(51)

No obstante, esa distinción no se aplica al término "comunicación electrónica", que claramente incluye, como ya hemos visto, SMS, MMS, logs de chat, mensajes de voz por redes IP, etc.(52) Y en segundo término, no se

(51) [En línea] www.zendo.com.ar/documentos/Informe_Preliminar.doc

(52) En relación a las vulnerabilidades que presentan las redes de telefonía celular, como las prácticas más usuales de escuchas, puede consultarse: Kanto, Damián, "Privacidad en peligro. Para escuchar conversaciones usan celulares como micrófono", Clarin.com, 22/04/1998. En este artículo, entre otras cosas, se explica que "… existen distintas maneras de acceder a

aprecian con facilidad las diferencias existentes entre sistemas privados o de acceso restringido, y en todo caso, ello da lugar a distintas interpretaciones. De nuestra parte, coincidimos con Palazzi que será de acceso restringido en cuanto tenga alguna medida de seguridad que impida el libre acceso.(53) Resulta innegable que "... no son objeto del delito las de carácter público, no en el sentido de servicio público, sino en el de que la comunicación no es privada sino abierta, tales como un mensaje subido a un blog que puede leer cualquiera…".(54) Entonces, deben tratarse de sistemas cerrados, resultando la información que allí circula de carácter privado (personal), o bien, no destinada a ser conocida por terceros. También podría tratarse de información confidencial por aplicación de la ley 24.766 (arts. 1, 2 y 12).

Cabe aclarar que en esta figura el objeto de protección son "sistemas informáticos privados o de acceso restringido", resultando excluidos los pertenecientes a un banco o archivo de datos personales (art. 157 *bis* del CP), cuyas características particulares están prefijadas en la ley 25.326. En otras palabras, puede tratarse de una PC o de una red compuesta por varios dispositivos electrónicos. A su vez, es fácil de imaginar la posibilidad

conversaciones ajenas (…) las modalidades dependen de varios factores: el tipo de aparato celular, el tipo de escucha que se pretende y la distancia del individuo que posee la terminal. Para entender cómo se realizan estas acciones, es preciso saber —aunque sea de manera superficial— cómo funciona la red de telefonía celular. La red tiene un complejo tramado de antenas. Cada una funciona como receptor y transmisor de señal de voz. Las antenas reciben el nombre de celda o célula (de ahí la denominación celular) y tienen un alcance de aproximadamente 20 manzanas. Este es el radio de alcance, aunque depende de la zona en que esté instalada. Cuando un usuario tiene encendido su aparato telefónico se vincula con la celda más cercana enviando dos códigos que tiene el celular: el ESN (*Electronic Serial Number*, que es una clave interna del aparato) y el MIN (*Movil Identification Number*) que es el número telefónico asignado por la prestadora del servicio. Esto permite al sistema informático de la empresa, ubicar al usuario y saber su posición. El sistema celular funciona a través de frecuencias de radio. Cuando se mantiene una conversación, la señal se envía a determinada frecuencia. El que dispone de esa información y tiene el equipo adecuado para interferirla, puede escucharla. Para detectarla se valen de unos aparatos llamados escáner que localizan la frecuencia de la víctima (…) Un espía que tiene los códigos, la frecuencia y la tecnología para efectuar la pinchadura, tiene que estar sí o sí en la misma celda o antena que el blanco. (…) Sin embargo, las modalidades de pinchaduras más difundidas en el mundo y en la Argentina no se limitan al ejemplo anterior. El más llamativo es el que permite usar un aparato celular de un usuario como si fuera un micrófono ambiente".

(53) Palazzi, Pablo A., *op. cit.*, p. 102.

(54) *Ibid.*, p. 82.

de un concurso ideal con el delito previsto en el artículo en el art. 153 *bis* del digesto punitivo.

En el plano subjetivo, estamos aquí también ante un delito doloso (directo), que admite la tentativa. Sobre el particular, nos remitidos a las consideraciones efectuadas al analizar los tipos penales de violación, apoderamiento, supresión y desvío de la correspondencia y los papeles privados.

Por último, la ley 26.388 omitió toda regulación legal de las cámaras ocultas, frecuentemente utilizadas en investigaciones periodísticas, con el argumento de que, de lo contrario, era posible afectar la libertad de expresión, optándose entonces por diferir su tratamiento para otra ocasión, lo que hasta el presente no ha ocurrido.(55) En la Cámara Alta también se sostuvo que esta cuestión no tenía que ver específicamente con los Delitos Informáticos.

Ahora bien, el art. 153 del CP agrava las penas previstas para las figuras básicas en dos casos:

a. "…si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica" la pena será de prisión de un (1) mes a un (1) año".

Comunicar es transmitir, hacer saber o dar a conocer a un tercero o terceros, distintos del destinatario, mientras publicar, es revelar, hacer notorio o difundir a un número indeterminado de personas el contenido de la comunicación electrónica.(56)

En general como lo ha destacado la doctrina este delito se configura en dos actos, pues presupone la existencia previa de alguno de los delitos previstos en los párrafos anteriores (apertura o acceso; apoderamiento;

(55) Se discutió la incorporación al Código Penal del art. 153 *ter*, bajo la siguiente redacción: "Será reprimido con prisión de un mes a dos años, el que ilegítimamente y para vulnerar la privacidad de otro, utilizando mecanismos de escucha, intercepción, transmisión, grabación o reproducción de voces, sonidos o imágenes, obtuviere, difundiere, revelare o cediere a terceros los datos o hechos descubiertos o las imágenes captadas" (Cámara de Diputados de la Nación, OD Nº 1227, 26/10/2006).

(56) Ver, Navarro, Guillermo R.; Báez, Julio C.; Aguirre, Guido J., "*Violación de Secretos y de la Privacidad*", en David Baigún y Eugenio Raúl Zaffaroni (dir), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, Bs. As., Hammurabi, 2008, p. 724.

supresión o desvío; interceptación o captación de comunicaciones electrónicas). Para Grasso: "... la forma agravada remite a las manifestaciones típicas expuestas, con la sola excepción del desvío de correspondencia. La exclusión responde al principio que proscribe la doble valoración de los elementos del tipo penal, pues el desvío implica ya el conocimiento del contenido a manos de un falso destinatario".(57)

b. "... si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

Por el término "funcionario público" o "empleado público" se designa a todo el que participa accidental o permanentemente del ejercicio de funciones públicas, sea por elección popular o por nombramiento de autoridad competente (art. 77 del CP).(58) Asimismo, la función de la cual se abusa debe dar ocasión o favorecer en modo alguno la realización de cualquiera de las conductas precisadas en las figuras básicas.

Si el funcionario público perteneciere al Sistema de Inteligencia de la Nación rige la ley 25.520, que en su art. 5°, establece que:

> "... las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario".

Consecuentemente, en los arts. 42 y 43 prevé disposiciones penales para aquellos agentes de la Secretaría de Inteligencia del Estado (SIDE) que se aparten de sus obligaciones funcionales. Así, incurrirá en delito, la persona que participando en forma permanente o transitoria de las tareas reguladas en dicha ley, indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier

(57) Grasso, Mariana, "Violación de Secretos", en Luis Niño y Stella Maris Martínez, (coords.) *Delitos contra la Libertad*, 2° ed., Bs. As., Ad-Hoc, 2010, p. 358.

(58) Ver también la Ley 25.188 de Ética de la Función Pública.

otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos. Finalmente, también sanciona con pena de prisión e inhabilitación especial al que con orden judicial y estando obligado a hacerlo, omitiere destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones.

5.2 | Artículo 153 *bis* del Código Penal

La ley 26.388 incorporó al catálogo punitivo el tipo penal que, a continuación, se transcribe:

> "Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
>
> La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

Se trata de una figura de aplicación subsidiaria, y por lo tanto, será desplazada si la conducta imputada recayera en un delito más severamente penado.

Mucho se ha dicho alrededor de los reparos que presenta este tipo penal a la luz de los principios de mínima intervención, subsidiariedad del derecho penal, exclusiva protección de bienes jurídicos y *ultima ratio*. Su construcción político criminal responde a los estándares del denominado proceso de Modernización del Derecho Penal, en el cual la función y los límites del "viejo" derecho penal liberal parecen debilitarse. En efecto, esta tendencia político criminal punitivista o neopunitivista ha sido denominada Derecho Penal de Segunda Velocidad (Silva Sánchez) o Derecho

de Intervención (Hassemer), y por su intermedio, se pretende replantear las bases filosóficas y políticas del derecho penal liberal.[59] Conforme a esta nueva orientación, el **derecho penal de riesgos**"[60] requiere de instrumentos jurídico-penales flexibles, que reemplacen los rígidos principios del sistema de garantías de la Ilustración, pues así el Estado será capaz de proteger a la sociedad de los múltiples y novedosos riesgos humanos que la acechan a la luz del auge tecnológico y la complejización de la vida en comunidad. Ejemplo paradigmático de esta clase de legislaciones, es el Código Penal Español de 1995, siendo aún más intenso el declive de garantías en la legislación antiterrorista y el derecho penal internacional (Derecho Penal de Cuarta Velocidad). En este marco, se alude, por ejemplo, a un concepto formal de **bien jurídico** o a la anticipación de la tutela penal en virtud de exigencias o consideraciones político-criminales de corte preventivo. El fundamento detrás de la incriminación de estas conductas reside en su consideración como actos previos o antesala de delitos más graves, como defraudaciones y estafas, ofensas al honor, y otros. En este sentido, la prestigiosa doctrina afirma que estas conductas carecen de entidad suficiente en términos de lesividad para legitimar la intervención del derecho penal, resultando preferible la vía contravencional, o en todo caso, su incriminación bajo la amenaza de imposición con penas distintas a la privativa de libertad, como multa, inhabilitación especial o alternativas reparatorias.[61] Por otro lado, se ha referido con justeza que "resulta inaceptable suplantar las deficiencias procesales del sistema mediante la inclusión de un tipo penal que prevé esta conducta como delito autónomo justamente por no poder acreditar ultra finalidad

(59) A modo de ejemplo, los Códigos Penales de la primera mitad del siglo pasado, apenas tenían un par de delitos de peligro, dejando las conductas sin resultado concreto como delitos tentados, con la consiguiente reducción de la escala penal. Hoy día, en cambio, los delitos de peligro y los tipos de omisión impropia se multiplican y justifican mediante la invocación de necesidades político-criminales.

(60) La "Escuela de Frankfurt", iniciada por los profesores Wolfang Naucke, Klaus Lüderssen y Winfried Hassemer, se ha constituido en la principal usina crítica al cambio de dirección del derecho penal orientado principalmente a las consecuencias. Muy ilustrativo sobre este tema resulta el libro de AAVV, *Crítica y Justificación del Derecho Penal en el Cambio de Siglo. El análisis crítico de la Escuela de Frankfurt*, Cuenca, Colección Estudios, Ediciones de la Universidad de Castilla - La Mancha, 2003.

(61) Riquert, Marcelo A., *Delincuencia Informática. En Argentina y el Mercosur*, Bs. As., Ediar, 2009, p. 182.

o como adelantamiento de la barrera punitiva y por ende disminuyendo el ámbito de libertad de las personas".(62)

Sujeto activo de este delito puede ser cualquier persona, y ésta debe **acceder** (entrar, ingresar u obtener) al objeto de protección legal conforme las modalidades típicas que veremos a continuación. A fin de llevar adelante la finalidad ilícita el autor puede realizar el **acceso por cualquier medio,** es decir, el ingreso u obtención de un sistema o dato informático, puede efectuarse en forma directa o remota. Así, existen diversos recursos para procurar este cometido, basta mencionar sólo algunos de ellos: a) *malware*, que tiene como objetivo infiltrarse en una computadora a través de virus, gusanos, troyanos, bombas de tiempo o lógicas, *rootkits*, *keyloggers*, y otros software maliciosos; b) *cookies*, es decir, fragmentos de información que se almacenan en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, resultando posible conseguir información sobre los hábitos del usuario; c) *spyware*, es decir, programas espías cuya finalidad es hurgar en la información de un ordenador, en búsqueda de algún dato privado; d) ingeniería social, consistente en la obtención de información confidencial de manos del propio usuario, a través de técnicas de manipulación o engaño, etcétera.

La ley 25.326 define **datos informatizados** como los datos personales —información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables— sometidos al tratamiento o procesamiento electrónico o automatizado. Compartimos que, a los efectos de la interpretación de los alcances del art. 153 *bis*, "no debe tratarse necesariamente de un dato personal".(63) No obstante, reafirmamos que es necesario delimitar el ámbito de aplicación del tipo en función del bien jurídico tutelado, de forma tal que el dato, amén de ser de acceso restrin-

(62) Rosende, Eduardo, "El intrusismo informático. Reflexiones sobre su inclusión al código penal", Ponencia presentada en el VII Encuentro de la AAPDP realizado en la Facultad de Derecho de la Universidad de Buenos Aires, los días 7, 8 y 9 de noviembre de 2007. De este autor, véase también, *Derecho Penal e Informática. Especial referencia a las amenazas lógico informáticas*, Bs. As., Fabián Di Plácido, 2007.

(63) Palazzi, Pablo A., *op. cit.*, p. 103.

gido, debe revestir el carácter de secreto o privado.[64] En otras palabras, no cualquier dato reúne las características típicas, aunque lógicamente pueda configurarse el delito —con independencia de las cualidades del dato— desde el momento en que se acceda al sistema informático de acceso restringido (sin autorización) que eventualmente lo contenga. Nuevamente aquí, debe tenerse presente lo establecido en el art. 12 de la ley 24.766 respecto de la confidencialidad de la información comercial.[65]

Por su parte, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, instrumento jurídico tenido en cuenta por el legislador nacional como importante antecedente de derecho internacional, define al "sistema informático", como todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa (art. 1, letra a). Asimismo, al tratarse de un sistema informático o dato de acceso restringido se requiere que el usuario o el administrador de la Red hayan adoptado alguna medida de seguridad, por mínima que sea. Principalmente, y por sentido inverso, no debe poder accederse al objeto de protección legal en forma libre o irrestricta; en otras palabras, por su disposición no debe estar destinado a ser accedidos por terceros no autorizados. Al respecto, se ha señalado que:

> "... el término restringido no es muy feliz y hubiera sido mejor que el legislador describiera la situación en que debían encontrarse el sistema o dato informáticos (por ejemplo, porque tiene medidas de seguridad que lo amparan) (…) no debe entenderse como un elemento fáctico, sino como uno normativo del tipo penal (…) está orientado a resaltar la obligación de no ingresar en un ordenador extraño".[66]

(64) Amans, Carla V. y Nager, Horacio S., *Manual de Derecho Penal. Parte Especial*, Bs. As., Ad-Hoc, 2009, p. 214.

(65) Con mayor claridad, el art. 197 del Código Penal Español establece que: "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses…".

(66) Palazzi, Pablo A., *op. cit.*, p. 103.

Es de destacar, en relación con lo anterior, que al no exigirse un umbral o nivel mínimo de seguridad informática, cualquier sistema o dato informático de acceso restringido, aún el más vulnerable, sería típico.(67) En todo caso, será tarea de la jurisprudencia analizar, en el caso concreto, la entidad de la conducta y la incidencia del comportamiento de la víctima, en el estrato analítico de la tipicidad o en la determinación judicial de la pena.

Antes de la sanción de la Ley de Delitos Informáticos, mucho se discutió acerca de las diferencias entre el intrusismo informático blanco o ético, de aquel que no lo es. Así se explicaba que el primero procura poner a prueba la seguridad de un sistema informático para descubrir sus vulnerabilidades, sin otra intención subyacente que la optimización del mismo. En cambio, el *hacking* no ético es realizado con una ultrafinalidad delictiva. Atento a la redacción típica, el mero intrusismo informático sería típico; no obstante, debe tenerse especialmente en cuenta al bien jurídico protegido para evitar caer en procesos de criminalización irrazonables (arts. 19 y 28 CN).(68) Claro está, que el problema del *ethical hacking* se presenta cuando el intruso actúa sin el consentimiento o la autorización del titular del sistema o dato informático explorado.

El sujeto activo debe realizar la conducta "a sabiendas", lo que conduce a la exigencia de un dolo directo. Riquert señala que "se trata de un delito doloso, que por este condicionamiento subjetivo es sólo compatible con el dolo directo, excluyendo el eventual, dejando por fuera la punición de todo acceso fortuito, casual o imprudente".(69) Además, se debe actuar

(67) El Convenio sobre la Ciberdelincuencia del Consejo de Europa Budapest - 2001 establece que cada Estado Parte tipificará como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático, pudiendo exigir que este delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

(68) Tal sería el caso de un proceso penal, de alta exposición mediática, sustanciado en EEUU a principios de la década de 1990, que culminó en la condena de integrantes de un grupo de *hackers* denominado LOD (*Legión of Doom*) por realizar actividades supuestamente peligrosas, como haber ingresado a un servidor privado y apoderarse de un documento cuyo nombre era "E91", que en realidad contenía información respecto del sistema de emergencias de la empresa AT&T, de conocimiento público (ver Rosende, Eduardo, "*El intrusismo informático. Reflexiones sobre su inclusión al código penal*", Ponencia presentada en el VII Encuentro de la AAPDP realizado en la Facultad de Derecho de la Universidad de Buenos Aires, los días 7, 8 y 9 de noviembre de 2007.

(69) Riquert, Marcelo A., *Delincuencia Informática, op. cit.* p. 181.

"sin la debida autorización o excediendo la que se posea", lo que equivale, en pocas palabras, a hacerlo sin derecho o indebidamente. Esto se daría, por ejemplo, "en los casos del personal de una institución autorizado para acceder sólo a determinados datos o archivos y que violando directivas internas, accede a sistemas, datos o archivos a los cuales no tiene acceso autorizado".(70) Por supuesto, que si el titular del sistema o dato informático permite el acceso, no estaremos ante un delito, no requiriendo dicha autorización formalidad alguna, más allá de que por razones de índole probatoria sea recomendable tomar recaudos al respecto.

La pena se agrava cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal —ANSES, AFIP, BCRA, IGJ, Dirección Nacional de Migraciones, Registro Nacional de Reincidencia y Estadística Criminal, etcétera— o de un proveedor de servicios públicos o de servicios financieros —Colegio Público de Abogados de la Capital Federal, Colegio de Escribanos de la Ciudad de Buenos Aires, Bancos y Entidades Financieras, Registro de la Propiedad Inmueble de la Ciudad de Buenos Aires, etcétera—. Puede tratarse de entes de derecho público centralizados o descentralizados, autárquicos o autónomos, y también de personas de existencia ideal de carácter privado que suministren o proveen un servicio público, tales como empresas concesionarias, bancos y demás entidades financieras, etcétera. La razón de la agravante reside en la naturaleza pública del sistema o dato informático accedido. En este punto, cabe aclarar que el acceso recaerá sobre el sistema informático perteneciente a cualquiera de estos entes jurídicos, más el dato allí contenido, si se refiere a condiciones inherentes a un usuario en particular: —vulnerará también un interés subjetivo individual—.

Si nos atenemos a la letra de la ley, es un delito de acción privada por imperio de lo establecido en el art. 73 inc. 2 del CP, lo que presenta algunas dudas, especialmente en lo referente a la figura calificada. Parte de la doctrina sostiene que esto obedece a un olvido legislativo; mientras otro sector, entiende que la exclusión es correcta, ya que los titulares de esos datos privados, confidenciales o secretos, son personas físicas o jurídicas puntualmente damnificadas.

(70) Arruvito, Pedro A., *op. cit.*

5.3 | Artículo 155 del Código Penal

La disposición legal reprime con multa (de pesos un mil quinientos a pesos cien mil) a la persona que "hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros"; especificando, en un segundo párrafo, que "está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".

Para la consumación del delito no es suficiente la simple comunicación del contenido a un tercero o terceros determinados, tal como lo admite la redacción del art. 153 del CP; este tipo penal exige que la comunicación electrónica sea publicada, es decir, que sea puesta en conocimiento del público en general, expuesta a un número indeterminado de personas. Resultan indiferentes los medios comisivos, pudiendo el autor realizar la publicación por sí mismo o a través de un tercero (editor, director de un periódico, blogger).

Además, el sujeto activo debe hallarse en posesión de la comunicación electrónica —sea porque se trate del destinatario o por cualquier otra razón— en forma lícita, ya que de lo contrario, resultaría de aplicación la agravante prevista en el art. 153 del CP. En otros términos, no se requiere ninguna cualidad especial para ser autor, pero la posesión de la comunicación electrónica debe haberse adquirido en forma legítima, resultando desvalorada aquí la conducta de hacer público su contenido cuando la misma no estaba destinada a trascender a un número indeterminado de individuos.

No es un delito de resultado, por lo que basta la existencia de un perjuicio potencial, el que puede asumir cualquier naturaleza —material, moral, patrimonial, etcétera—, pero este debe ser consecuencia directa del hecho de la publicación abusiva.[71] El comportamiento debe llevarse adelante con conocimiento y voluntad de realización del tipo objetivo,

(71) Fontán Balestra, *Derecho Penal. Parte Especial*, actualizado por Guillermo A. C. Ledesma, 16° ed., Bs. As., Lexis-Nexis - Abeledo-Perrot, 2002, p. 372. En igual sentido ver Navarro, Guillermo R.; Báez, Julio C. y Aguirre, Guido J., *op. cit.*, p. 760.

por lo que se requiere obrar con dolo (directo). Admite la tentativa. Finalmente, la ley 26.388, exime de responsabilidad a quien obre con el propósito inequívoco de proteger un interés público.

5.4 | Artículo 157 del Código Penal

El art. 157 del CP reprime, con penas de prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, al "funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos".

Se trata del delito de violación de Secreto Oficial, no habiendo la ley 26.388 de Delitos Informáticos introducido modificaciones sustanciales, dado que el legislador se limitó a actualizar el texto legal mediante la incorporación de la voz "datos", que debe entenderse en sentido amplio, conforme fuera desarrollado precedentemente al analizar la estructura típica del delito de intrusismo informático (art. 153 *bis* del CP).

El sujeto activo debe presentar una cualidad específica: ser funcionario público (art. 77 del CP), y en virtud de esta condición especial, debe recaer en su persona la obligación legal de guardar secreto sobre los datos que hubiere conocido en ejercicio o en ocasión de sus funciones. La obligación de guardar el secreto debe ser impuesta por la ley (art. 51 del CP), de manera que el funcionario, al quebrantarlo, no sólo vulnera un deber genérico de confianza y privacidad, sino que su acción deviene antinormativa, al contradecir una disposición legal que expresamente lo obliga a guardar silencio.

Esta figura será desplazada en caso de concurrir, en el supuesto de hecho, los requisitos típicos contemplados en los arts. 222 y 223 del CP, o en los arts. 2 y 3 de la ley 13.985, también conocida como Ley Antiespionaje. A su vez, compartimos que "en caso de que un funcionario público revelare ilegítimamente un secreto oficial que fuera a su vez información personal registrada en un banco de datos personales, el tipo penal del art. 157 del CP —que releva que el secreto concierna a las esferas de actuación del Estado— será el que prevalezca".[72]

(72) Seco Pon, Juan Carlos, "Violación de datos personales (art. 157 bis, CP) y revelación de secretos oficiales (art. 157, CP)", en Niño, Luis y Martinez, Stella Maris (coords.), *op. cit.*, p. 570.

El delito se consuma cuando el secreto es revelado, lo que equivale a su comunicación a un sujeto que no está autorizado a conocerlo; quien incluso pude también revestir la calidad de funcionario público. El delito es doloso, discutiéndose en la doctrina si basta con el dolo eventual, o si éste debe ser directo.(73) Admite la tentativa.

Por encontrarse en juego un interés público, parece razonable su inclusión en el catálogo de delitos perseguibles de oficio (arts. 71 y 73 inc. 2 del CP).

5.5 | Artículo 157 *bis* del Código Penal

Los datos personales no son una novedad, más lo que provoca alarma en la actualidad es su facilidad de obtención, almacenamiento, tratamiento y divulgación. A diferencia de lo que acontecía con el viejo fichero, la capacidad de almacenamiento y tratamiento de información hoy es inmensa, su consulta es sumamente sencilla, y no está sujeta a las restricciones o limitaciones temporales y espaciales tradicionales. El resultado del procesamiento de estos datos se obtiene en forma casi inmediata, constituyendo una herramienta de enorme utilidad, y a la vez económica, por el ahorro de energía y de recursos humanos que posibilita. Sin embargo, este inconmensurable caudal de información, puesto a disposición del gobierno o de particulares, presenta un grave riesgo a la esfera de intimidad de las personas. Es que en la "sociedad de la información", más que nunca, es necesario responder al interrogante relativo a qué se debe guardar y qué no, con qué fines y por cuánto tiempo.

Consideramos que el análisis de esta disposición debe ser precedido por una breve remisión al contenido de la ley 25.326 de *Hábeas Data* (BO 02/11/2000), reglamentaria del instituto previsto en la Ley Fundamental.(74) Este cuerpo legal establece que su objeto es la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al

(73) Navarro, Guillermo R.; Báez, Julio C. y Aguirre, Guido J., *op. cit.*, p. 802.

(74) Esto, sin desconocer que "las garantías constitucionales existen y protegen a los individuos por el solo hecho de estar en la Constitución e independientemente de sus leyes reglamentarias, cuyas limitaciones no pueden constituir obstáculo para la vigencia efectiva de dichas garantías" (Fallos: 239:459; 241:291 y 315:1492).

honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el art. 43, párr. tercero de la Constitución Nacional. Y agrega, que sus disposiciones también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal, y que en ningún caso, se podrán afectar la base de datos ni las fuentes de información periodísticas (art. 1).

En el art. 2, se definen diversos términos, lo que contribuye a una correcta hermenéutica del texto legal. De esta manera, se precisa qué debe entenderse por datos personales; datos sensibles; archivo, registro, base o banco de datos; tratamiento de datos; responsable de archivo, registro, base o banco de datos; datos informatizados; titular de los datos; usuario de datos; y disociación de datos. Particular importancia reviste la distinción entre **datos personales** —o sea, información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables—y **datos sensibles** —es decir, datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual—.

Por su parte, en el art. 5, se establece que el tratamiento de datos personales, sólo será lícito cuando el titular lo consintiera en forma libre, expresa e informada, documentándose por escrito, o por otro medio que se le equipare. Así, la regla es que debe solicitarse el consentimiento del titular de los datos, admitiendo las siguientes excepciones: a) datos obtenidos de fuentes de acceso público irrestricto; b) datos que se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) datos que deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) operaciones que realicen las entidades financieras e informaciones que reciban de sus clientes, conforme las disposiciones del art. 39 de la ley 21.526.

La Dirección Nacional de Protección de Datos Personales es el órgano de control creado en el ámbito Nacional para la efectiva protección de los datos personales, que tiene a su cargo el Registro de las Bases de Datos,

debiendo asesorar y brindar asistencia a los titulares de datos personales ante denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos, por violación de los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos.

Ahora bien, el art. 157 *bis* reprime con pena de prisión de un mes a dos años a la persona que realice cualquiera de estas conductas: 1) Acceso ilegítimo a un banco de datos personales; 2) Revelación de secretos registrados en un banco de datos personales; 3) Inserción de datos en un banco de datos personales. A continuación, veremos cada una de ellas.

En el inc. 1 se reprime a la persona que "a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales".

Sujeto activo del delito es quien accede a un banco de datos personales "a sabiendas e ilegítimamente" o "violando sistemas de confidencialidad y seguridad de datos", pudiendo servirse de cualquier medio para alcanzar la concreción del plan delictual. Ciertamente, la generalidad de la primera fórmula, en cuanto alude a un ingreso ilegítimo, torna sobreabundante la referencia a la violación de sistemas de confidencialidad y seguridad de datos, y más aún, cuando posteriormente se establece que el acceso puede concretarse "de cualquier forma". Por ello, la técnica legislativa luce deficiente, debiendo tratarse, en definitiva, de un acceso sin autorización del titular o de la ley.

Debe tenerse presente que la Ley de *Hábeas Data,* en su art. 9, obliga al responsable o usuario de un archivo de datos a adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, prohibiendo la registración de éstos en bancos que no reúnan condiciones técnicas de integridad y seguridad. El objeto de protección penal son los archivos de datos personales, o sea, el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera fuere la modalidad de su formación, almacenamiento, organización o acceso (art. 2, ley 25.326). Técnicamente, un archivo, registro, base o banco de datos es "un conjunto no redundante de datos organizados e interrelacionados de acuerdo con ciertos atributos comunes en función de los po-

sibles requerimientos de distinta aplicación",[75] que por mandato legal debe estar destinado a dar informes (art. 1, ley 25.326).

Compartimos que desde el punto de vista subjetivo, no sólo el autor debe saber lo que hace —a sabiendas—, sino que debe conocer que accede en forma ilegítima, sin autorización legal o consentimiento del titular de la información personal. Por ello, "… se está castigando un actuar doloso solo compatible con el denominado dolo directo, excluyéndose de tal modo el dolo eventual".[76] Si bien es admisible la tentativa, no debe olvidarse que, tal como acontece con la conducta descrita en el art. 153 *bis* del Código Penal, estamos ante la criminalización de un acto preparatorio punible por una decisión de política criminal.

Se discute si se trata de un delito de acción pública o privada; sin embargo, el segundo incido del art. 73 del Código Penal prevé que la violación de secretos, a excepción de los casos de los arts. 154 y 157, son delitos de acción privada, por lo que, más allá de la tesis del olvido legislativo y de la opinión de parte de la doctrina,[77] una interpretación contraria a la norma, vulneraría el principio de legalidad en perjuicio del eventual inculpado.

La descripción típica se diferencia del art. 153 *bis*, en función de que estas disposiciones poseen un objeto de protección distinto: en este caso, la conducta debe dirigirse contra un banco de datos personales; mientras que en aquel supuesto, el objeto de protección es un sistema o dato informático de acceso restringido.

Por su parte, el inc. 2 prevé la imposición de pena prisión a quién "ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley".

Esta figura no presenta mayores novedades, pues estamos en presencia de una modalidad especial del convencional delito violación de secretos

(75) Cesario, Roberto, *Hábeas Data. Ley 25.326*, Bs. As., Universidad, 2001, p. 27.

(76) Tazza, Alejandro y Carreras, Eduardo, "La protección del banco de datos personales y otros objetos de tutela penal", Bs. As., La Ley 2008-E, p. 869.

(77) Tazza, y Carreras, *Ibid.*

(arts. 156 y 157 CP), generada por los avances tecnológicos. La Ley de Protección de Datos Personales coloca en cabeza del titular de una base de datos y de todas aquellas personas que intervengan en cualquier fase del tratamiento de la información, la obligación de guardar el secreto profesional, inclusive aún después de finalizada la relación laboral (art. 10, ley 25.326). Asimismo, la obligación de guardar secreto o preservar la confidencialidad de la información, está prevista en leyes específicas (por ejemplo: leyes 11.683, 21.526, 24.766, y otras).

El delito es doloso (admite la modalidad eventual), resultando posible la tentativa.

El obligado al secreto sólo podrá revelarlo, sin incurrir en delito, previa autorización judicial, o ante la existencia de razones fundadas en motivos de seguridad pública, defensa nacional o salud pública.

A su vez, el inc. 3 reprime a quién "ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales". Esta conducta, se encontraba prevista en el inc. 1 del art. 117 *bis* del Código Penal —derogado por la ley 26.388—, dentro de los delitos que afectan el honor de las personas. Por esta razón, la figura derogada sancionaba la inserción de **datos falsos**; en cambio, la redacción actual sólo requiere que el autor inserte o haga insertar **datos** en un archivo de datos personales. No obstante, creemos que la simple conducta de insertar cualquier dato no es suficiente para configurar el injusto penal, se requiere que éste tenga virtualidad suficiente para producir la lesión del bien jurídico. Tazza y Carreras expresan que "la información que se inserta en tales registros puede ser verdadera o falsa, y en este último caso —de ser falsa—, la misma conducta podría configurar, a la vez, el delito de falsedad documental ideológica (arts. 77 y 293 del CP) cuando se trata de instrumento público, o el de injurias o calumnias (arts. 109 y 110 del CP), cuando ello pudiera afectar el honor del perjudicado";[78] sin embargo, la fórmula del art. 77 sólo parece aceptar la existencia de instrumentos privados digitales, excluyendo a los efectos de la ley penal la posibilidad de documentos digitales de naturaleza pública.

Para traer aún más confusión en torno al carácter público o privado de la acción penal que deriva de la comisión de este delito, es interesante

(78) Tazza, Alejandro y Carreras, Eduardo, *op. cit.*

señalar que en su versión anterior (ver el texto del art. 117 *bis*) era de acción pública.

Por último, en cualquiera de los tres supuestos, cuando el autor sea funcionario público (art. 77 CP) sufrirá también pena de inhabilitación especial de uno a cuatro años.

6 | Consideraciones preliminares sobre el Anteproyecto de Código Penal de la Nación (decreto 678/2012)

En primer término, se propone un cambio de rúbrica al capítulo correspondiente del catálogo punitivo, reemplazando el de "violación de secretos y de la privacidad" por el de "violación de comunicaciones y de la privacidad", pese a que se encuentran incluidas entre estas disposiciones aquellas referidas al secreto profesional y funcional.

Las conductas actualmente previstas en el art. 153 del CP son ordenadas en el art. 119 (violación de comunicaciones) y se aumentan los montos punitivos, previéndose la pena de prisión de seis meses a dos años y multa de diez a ciento cincuenta días. Si bien el artículo prevé la pena de multa en forma conjunta atento usar la conjunción "y", debe tenerse en cuenta la alternativa prevista para supuestos de escasa lesividad o significancia jurídico penal consiste en la imposición alternativa de una multa reparatoria o la determinación de una pena judicial por debajo del mínimo legal (arts. 3 inc. a y 22 inc. g).

Las conductas típicas en términos generales se mantiene inalterables, pero son organizadas en cuatro incisos, correspondiendo destacar que se incluye expresamente a las comunicaciones telefónicas y se reemplaza la voz "u otro papel privado" por "un papel privado", lo que nos parece de mejor técnica legislativa, atento las razones enunciadas al analizar ut supra el art. 153 del CP. Asimismo, en el inc. d) se mantiene la expresión "cualquier sistema de carácter privado o acceso restringido", respecto de la cual ya hemos señalado que no se aprecian con facilidad las diferencias

existentes entre sistemas privados o de acceso restringido, y en todo caso, ello seguirá dando lugar a distintas interpretaciones. No obstante, es claro que la norma no sería de aplicación si el sistema es abierto, accesible a una generalidad de individuos.

A su vez, las agravantes de la figura básica están previstas en el inc. 2 del art. 120 del Anteproyecto. Se mantiene el incremento punitivo cuando la conducta es ejecutada por un funcionario público abusando de su condición e incorpora también el abuso de oficio o profesión del agente, aun cuando no se tratare de un funcionario público.

El citado art. 120 proyecta en su inc. 1 la siguiente figura delictiva: "Será reprimido con prisión de seis (6) meses a dos (2) años y multa de diez a ciento cincuenta días, el que vulnerare la privacidad de otro, mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o se hiciere de registros no destinados a la publicidad". Con esta inclusión se propone subsanar la omisión en la que incurrió la Ley de Delitos Informáticos. Recordemos que la ley 26.388 no reguló el uso de las cámaras ocultas, frecuentemente utilizadas en investigaciones periodísticas, con el argumento de que era posible afectar la libertad de expresión, y optó por postergar su tratamiento.[79] El texto del Anteproyecto es similar al del fallido art. 153 *ter* del Código Penal: "Será reprimido con prisión de un mes a dos años, el que ilegítimamente y para vulnerar la privacidad de otro, utilizando mecanismos de escucha, intercepción, transmisión, grabación o reproducción de voces, sonidos o imágenes, obtuviere, difundiere, revelare o cediere a terceros los datos o hechos descubiertos o las imágenes captadas".

En los arts. 119 y 120 si bien se agrava la pena cuando interviene un funcionario público abusando de su condición, no se prevé en forma conjunta la pena de inhabilitación. En ambos casos, sí se prevé la pena conjunta de multa y se agrava la pena de prisión con un mínimo de un año y un máximo de cuatro.

En el art. 121 del Anteproyecto se castiga la comunicación o publicación indebida de los instrumentos, registros o contenidos a los que se refieren los artículos precedentes —a saber: una comunicación electrónica,

(79) Cámara de Diputados de la Nación, OD Nº 1227, 26/10/2006.

telefónica, una carta, un pliego cerrado, un papel privado, un despacho telegráfico o telefónico o de otra naturaleza o registros obtenidos mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen—. En el inc. 1 se reprime con prisión de seis meses a tres años, multa de diez a ciento cincuenta días e inhabilitación de uno a cuatro años, al que hallándose en posesión de estos instrumentos, registros o contenidos, los comunicare, publicare o los hiciere publicar, indebidamente. De seguido, el inc. 2 prevé igual pena para quien los hiciere publicar, siempre que no estuvieren destinados a la publicidad —aunque le fueren dirigidos— si el hecho causare o pudiere causar perjuicios. En la parte Exposición de Motivos se aclara que en este inciso se pune la conducta de quien posee el objeto de protección penal "debidamente", por lo que entendemos que el injusto radica en el hecho darlo a conocer a un número indeterminado de personas —aunque le estuviere dirigido— cuando su destino no era la publicidad y con ello se pueda causar un perjuicio (daño potencial). A *contrario sensu* puede afirmarse entonces que la conducta prevista en el primer inciso de la norma abarca aquellos supuestos en los que el autor ha entrado en posesión del material en forma indebida a través de cualquiera de las formas enunciadas en los arts. 119 y 120 del Anteproyecto.[80] Sin embargo, por su ubicación y función gramatical el adverbio "indebidamente" se halla vinculado a los verbos típicos y no a la posesión previa de los materiales, por lo que sería recomendable dotar de mayor claridad a la fórmula legal propuesta. Finalmente, la norma proyectada exime de responsabilidad penal a quien hubiere obrado con el propósito inequívoco de proteger un interés público actual. En síntesis, se ordenan bajo una misma disposición legal las conductas que actualmente se encuentran previstas en los arts. 153, 3 párr. y 155 del CP, lo cual nos parece de buena técnica legislativa.

Se suprime el art. 154 del CP y en el art. 122 del Anteproyecto se reproducen en dos incisos los vigentes arts. 156 y 157, ocupándose en forma conjunta del secreto profesional y funcional. Como dato relevante, en este caso se prevé la pena de multa en forma alternativa utilizando la conjunción disyuntiva "o". Asimismo, en la Exposición de Motivos se aclara que si bien con mayor frecuencia el sujeto pasivo del secreto funcional es la Administración o el Estado, ello no es una regla, "pues

(80) Al igual que en el art. 153 del CP, donde se utiliza la fórmula "si el autor además comunicare a otro o publicare...".

la conducta tipificada —al menos en buen número de casos— resulta pluriofensiva: el funcionario que revela los datos de la ficha de salud de una persona reservada en una oficina de personal, no sólo lesiona a la administración".

Finalmente, en el art. 123 se prevé el delito de "acceso ilegítimo a información". En el inc. 1° se reproduce el texto del art. 153 *bis* del CP, se elimina la mención expresa al carácter subsidiario de la figura y se sustituye la pena de prisión por la de multa de diez a cien días. La previsión de una pena más benigna responde al reclamo de un importante sector de la doctrina que entiende que esta conducta, como antesala de delitos más graves (por ejemplo: otros atentados contra la intimidad, sabotaje, espionaje o defraudaciones), no posee relevancia penal o debe ser considerada una contravención.[81] Si bien se mantuvo el carácter de delito se suprimió como dijimos la pena privativa de libertad. El acceso —al igual que en el actual art. 153 *bis* del catálogo punitivo— puede ser a un "sistema" o a un "dato" informático, lo cual entendemos nos es superfluo. Veamos, si la acción del denominado *hacker* simple consiste en acceder a un sistema informático, sin que dicho acceso importe al mismo tiempo conocer datos informáticos de carácter confidencial o privado, nos parece que la conducta no posee relevancia penal o, en todo caso, la misma sería mínima. Por ello, la sustitución de la pena de prisión por la de multa con un mínimo de diez días nos parece adecuada. Ahora bien, si el autor mediante el acceso ilegítimo a datos informáticos obtuvo información confidencial o privada —que no constituya, a su vez, una comunicación electrónica o un registro obtenido a través de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, lo que podría ser abarcado por otras disposiciones— se advierte cierta desproporción con las penas previstas para los delitos de "violación de comunicaciones" y "violación de la privacidad" (arts. 119 y 120 del Anteproyecto), pues ante similar afectación del bien jurídico se prevé una reacción estatal de distinta entidad.

(81) En este sentido José Saez Capel y Claudia Velciov sostienen que: "... tales conductas carecen de entidad suficiente para merecer la intervención del Derecho penal; o bien se materializan en otro hecho más grave, o caso contrario, resultan inofensivas, y su incriminación atenta contra el principio de lesividad e intervención mínima..."(Saez Capel, José y Velciov, Claudia, "Artículo 153 bis", en Eugenio Zaffaroni y David Baigún (dirs.), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, Bs. As., Hammurabi, 2008, tomo V, p. 743).

Por su parte, en el inc. 2 se prevé una pena de prisión de seis meses a dos años para los mismos casos descriptos en el segundo párrafo del actual art. 153 *bis* del CP, incorporándose al tipo penal la mención de los servicios de salud.[82] Finalmente, como novedad, si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional, se proyecta elevar el máximo de la pena de prisión a cuatro años.

Los tres primeros apartados del inciso tercero del art. 123 del Anteproyecto reproducen en términos generales los tres incisos del art. 157 *bis* del CP, proponiendo algunas modificaciones a la redacción típica que redundan en una mejor técnica legislativa. Se suprimen en los delitos de acceso no autorizado a un banco de datos personales y revelación de información registrada en un banco de datos personales el adverbio "ilegítimamente", que fuera criticado por toda la doctrina por sobreabundante. Asimismo se simplifica y clarifica la descripción de la conducta prevista actualmente en el inc. 1 del art. 157 *bis* del CP a través de la siguiente fórmula: "será penado (...) el que a sabiendas y violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales".[83] El apartado d) se complementa con el apartado a), sancionando la obtención de datos personales, financieros o confidenciales mediante cualquier ardid o engaño, por lo que se requiere que el sujeto pasivo sea una persona física.

En lo referente a los apartados e) y f), dado su carácter novedoso, es importante transcribir las consideraciones efectuadas en la Exposición de Motivos:

> "El apartado e) tipifica la conducta no sólo de quien provea los instrumentos para la comisión de los delitos previamente tipificados, sino que se incluye también su tenencia cuando sean inequívocamente destinados a su comisión. Se trata de a tipificación de un acto preparatorio, como el tradicional referido a la falsificación. Si el hecho se tentare, esta tipicidad desaparece en función de las reglas del concurso aparente. El apart. f) pro-

(82) Compartimos con Saez Capel y Velciov que debería establecerse con precisión el alcance del concepto "servicio público" (Saez Capel, y Velciov, *op. cit.*, p. 747).

(83) Ver las críticas efectuadas en forma precedente al art. 157 ***bis*** del CP.

> puesto, tipifica una conducta frecuente y altamente peligrosa en la comunicación. Si bien no está referida a datos personales, se trata de una grave suposición de identidad, perjudicial para el buen nombre del real portador del nombre y con capacidad para producir serios daños".

En el primer caso basta con la tenencia de los materiales siempre y cuando surja en forma inequívoca su finalidad ilícita. Es decir, estamos frente a un delito de peligro abstracto, no obstante lo cual, entendemos se requiere establecer una vinculación entre el bien jurídico y la acción del autor, pues la descripción típica no puede ser concebida como un delito formal. En otras palabras, es necesario que la conducta resulte riesgosa aunque no se traduzca en un peligro concreto. En consecuencia, en nuestra opinión, si por algún motivo los artificios técnicos resultan absolutamente inidóneos para el fin para el cual fueron concebidos no puede considerarse típica su tenencia. La utilización del término "inequívocamente" es correcta en este caso —a diferencia de lo que sucede en el segundo párr. del art. 14 de la ley 23.737—,[(84)] ya que la carga de la prueba recae en la parte acusadora.

En el segundo supuesto, se propone legislar el delito de usurpación de identidad, respondiendo a un reclamo social. En este sentido, cabe mencionar que en nuestro país se creó un Centro de Asistencia a las Víctimas de Robo de Identidad, y además, la Dirección Nacional de Protección de Datos Personales dispuso la creación de un Registro de Víctimas de Robo de Identidad. Por otro lado, y más allá de su acierto o no a la luz de los principios de *ultima ratio* y carácter subsidiario del derecho penal, existían otras iniciativas legislativas para tipificar el robo de identidad digital, como el proyecto de la diputada Natalia Gambaro, quién propició la incorporación al Código Penal del art. 139 *ter:*

> "Será reprimido con prisión de 6 meses a 3 años el que adoptare, creare, apropiare o utilizare, a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca. La pena será de 2 a 6 años de prisión cuando el autor asumiera la identidad

(84) Véase el fallo de la CSJN, "Vega Giménez, Claudio Esteban s/ Tenencia Simple de Estupefacientes", V. 1283, causa N° 660, 27/12/2006.

de un menor de edad o tuviese contacto con una persona menor de dieciséis años, aunque mediare su consentimiento o sea funcionario público en ejercicio de sus funciones".

Afortunadamente, en el Anteproyecto se requiere que el agente actúe con el propósito de causar un perjuicio.

Mención aparte, consideramos que esta última conducta podría haber sido incluidas en el mismo artículo como inc. 4 ya que no guarda relación con el art. 157 *bis* del Código sustantivo.

Finalmente, el inc. 4, cuando el sujeto activo fuere funcionario público, repite la fórmula prevista en el último párrafo del art. 157 *bis*, mantiene la pena conjunta de inhabilitación, pero aumenta su máximo a cinco años.

7 | Palabras finales

Hemos visto a lo largo de este trabajo las dificultades y desafíos que presenta la protección de la privacidad en la "sociedad de la información", en la que los recursos técnicos reducen cada vez más la posibilidad real de que los individuos gocen de un ámbito de dominio exclusivo, donde se encuentren solos, exentos de la injerencia arbitraria o ilegal de terceros o del Estado. De esta manera, somos testigos de una importante transformación, fáctica y cultural, del bien jurídico, que el derecho necesariamente debe contemplar y regular. En este contexto, resultó razonable la sanción de la ley 26.388 de Delitos Informáticos, y más aún, su inclusión en el catálogo punitivo, evitando así la proliferación de leyes especiales que conducen inexorablemente a la ruptura del sistema de código.

No obstante, creemos corresponde ser cautos a la hora de generar expectativas en punto a la efectiva protección del bien jurídico a través del derecho penal en materia de delitos cometidos mediante el uso de las nuevas tecnologías, por cuanto la herramienta punitiva no sólo actúa cuando la lesión material se ha concretado, sino que en esta temática específica surge en forma particularmente manifiesta la mayor idoneidad de las medidas extra-penales, principalmente sustentadas en el suministro de información al usuario como política pública sobre el uso seguro y responsable de estos dispositivos electrónicos.

Asimismo, nos hemos ocupado del estudio dogmático de los "delitos informáticos" contemplados en nuestro Código Penal, a fin de exponer nuestro punto de vista sobre los alcances y requisitos típicos de estas figuras penales en el marco de un Estado de Derecho, siempre desde una hermenéutica reductora del poder punitivo.

Por último, hemos realizado un análisis preliminar del Anteproyecto de Código Penal de la Nación elaborado por la comisión *ad hoc* encabezada por el Dr. Raúl E. Zaffaroni, e integrada por los Dres. León Arslanian, Ricardo Gil Lavedra, María Elena Barbagelata y Federico Pinedo,[85] el que, como bien se ha dicho, constituye "...un plan admirable que tiene las mejores cartas para lograr (re)construir un Código Penal que resulte adecuado al modelo liberal y humanista impuesto en la materia por los textos políticos fundamentales de nuestro Estado constitucional y democrático de derecho", que implica la continuidad de la reforma penal emprendida en 2004 y que debiera extenderse al régimen procesal penal.[86]

(85) Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (Decreto 678/12).

(86) Pastor, Daniel R., "La recodificación penal en marcha. Una iniciativa ideal para la racionalización legislativa", en *Revista Pensar en Derecho*, Bs. As., Eudeba, 2012, p. 37.