Universidad de Guadalajara
Derecho Global. Estudios sobre Derecho y Justicia
Año 2020. Vol. V. núm. 14, Marzo - Junio, pp.127-149, ISSN: 2448-5128 e-ISSN: 2448-5136
https://DOI.org/10.32870/dgedj.v5i14.250

Los delitos informáticos en el Código Penal Italiano

Computer crimes in the Italian Criminal Law

Leandro Ezequiel Fusco
Universidad de Buenos Aires, Argentina
leandrofusco@derecho.uba.ar

Recibido 11/06/19
Aceptado 14/10/19

Resumen: En el presente artículo se aborda una cuestión de derecho comparado, más precisamente de Italia, que hoy día resulta sumamente importante. Me refiero a los delitos informáticos. La importancia de su estudio excede la mera curiosidad intelectual o la habitual idea del estudio del derecho comparado; con las tecnologías actuales, muchos de los delitos informáticos pueden cometerse en un lugar y causar sus efectos en otro. De ese modo, se exponen aquí los tipos penales más importantes de la legislación italiana en la materia, que fueron incluidos en 1993 y reformados en 2008, para tener una perspectiva de sus estructuras, sanciones y modos de ejecución. Para finalizar, ya evaluadas las objeciones constitucionales que se presentan, se formula un análisis crítico de los institutos.

Palabras clave: Derecho penal italiano, delitos informáticos, reformas legislativas.

Abstract: In this paper, we are dealing with a comparative law subject, more precisely of Italy, which is extremely important at present times: computer crimes. The importance of their study exceeds the mere intellectual curiosity or the usual idea of the study of

comparative law, since with current technologies, many computer crimes can be committed in one place and cause its effects in another. Thus, the most important criminal types of the Italian legislation on the matter that were included in 1993 and reformed in 2008 are presented here to have a perspective of their structures, sanctions and methods of execution. To finalize, and already evaluated the constitutional objections that are presented, a critical analysis of the institutes is formulated.

Keywords: Italian criminal law. Cybercrime. Legislative reforms

Sumario: I. Introducción. II. La reforma. III. Los tipos penales introducidos por la ley y sus reformas. IV. Excursus, algunas particularidades del tema tratado. V. Conclusiones. Bibliografía.

I. Introducción

Las respuestas que el derecho podía dar al vertiginoso desarrollo de las tecnologías informáticas fue un tema que atrajo la atención de los países europeos –Italia, en particular–, mucho antes que el tema llegara a estas latitudes.

En efecto, la tradición codificadora de los países que receptaron el derecho continental evidenció numerosos inconvenientes al momento de resolver cuestiones relacionadas con la informática.

De más está decir que los viejos digestos normativos de ningún modo podían prever tecnologías como las que hoy tenemos al alcance. En lo particular, debe decirse que el Código Penal Italiano data del año 1931, y el Código Civil de 1942. Así pues, la ley no podía contemplar adecuadamente todas las posibles derivaciones de estas actividades.

A principios de los años noventa, la legislación italiana se preocupó por estas lagunas, y comenzó a sancionar leyes tendientes a darle completitud a su sistema jurídico.

Cabe señalar que los problemas fundamentales se situaban en torno al software y el conjunto de datos contenidos en un sistema, puesto que los casos relativos

a la tutela del hardware se subsanaban a través de los tipos penales tradicionales de daño y hurto.

Para los casos de software, o datos obrantes en un registro, en efecto, se tornaba difícil si no imposible afirmar el carácter de cosa física de éstos para adaptarlos a la figura prevista en el artículo 635 del C.P.,[1] que preveía el delito de daño en tanto la Constitución italiana veda la aplicación de la analogía en el derecho penal, como derivación del principio "*nulla crime nulla poena sine lege*" (artículo 25 de la Constitución italiana).

El derecho civil, a su vez, todavía ponía en duda que fuera correcta la aplicación analógica al software de los derechos de autor, regidos por la ley número 633 del año 1941.

Ante esta situación, el legislador se abocó a la solución del problema y mediante un decreto legislativo (el nro. 518/92) introdujo algunas modificaciones al concepto de derecho de autor en el ámbito civil para adaptarlo a las nuevas necesidades.

En el ámbito penal, por su parte, el parlamento dictó el día 23 de diciembre de 1993 la ley número 547, por la cual se penaban los delitos informáticos, subsanando, fundamentalmente, el obstáculo que traía el concepto de "inmaterialidad".[2]

A lo largo del presente artículo, se intentará brindar un resumen de lo que son los delitos informáticos en Italia a través de su regulación legal, y, en los casos en que sea pertinente, ver cómo la jurisprudencia los ha entendido, mediante la cita de antecedentes aplicables a cada caso.

---

[1] El artículo 635 del C.P.I. pena con reclusión de hasta un año o multa de 600.000 mil liras al que: "…*destruya, desvanezca, deteriore, o torne inservible en todo o en parte, a una cosa mueble o inmueble ajena*…".

[2] En Argentina ocurrió algo similar con el recordado resolutorio del Juez Sergio Torres sostuviera que "… *La violación del sistema de seguridad de una página Web, reemplazándola por otra -en el caso, un grupo de hackers alteró la página de inicio de la Corte Suprema de Justicia agregándole una alusiva al aniversario de la muerte de un periodista- no encuadra dentro de la figura penal del delito de daño prevista en el art. 183 y 184 inc. 5 del Cód. Penal, pues no es dable considerar a la citada página Web o a los datos o sistemas informáticos como "cosa" en los términos del art. 2311 del Cód. Civil, en tanto por su naturaleza no son objetos corpóreos ni pueden ser detectados materialmente….".* Juzgado Nacional de 1a Instancia en lo Criminal y Correccional Federal Nro. 12 • 20/03/2002 • Gornstein, Marcelo H. y otros • LA LEY 2002-C, 23. Vale resaltar que aquel fallo fue apelado por el Fiscal a cargo de la Fiscalía Nacional en lo Criminal y Correccional federal nro. 1 y luego confirmado por la Cámara Federal.

II. La reforma

Con la ley 547/93 se agregaron artículos y se modificaron conceptos en torno a los delitos informáticos.

La doctrina italiana comenzó entonces a hablar de los crímenes informáticos, entendiendo por estos cualquier delito o violación del código civil o penal en la que la tecnología informática haya sido un factor determinante para la concreción del acto.

Así, debemos distinguir entre delitos informáticos propiamente dichos y delitos que requieren la informática como medio comisivo. Son los primeros los que necesitaban urgentemente una legislación, pues los segundos podían subsanarse mediante las reglas generales obrantes en el Código Penal.

En virtud de la nueva ley, quedaban incluidos en las previsiones normativas los sistemas informáticos y de telemática,[3] el software y todo el patrimonio informático (incluye todo tipo de datos, imágenes, sonidos, etc.)

No obstante, la reforma fue criticada porque no se colocaban a los delitos informáticos de forma autónoma dentro de la legislación italiana; antes bien, se constituían a lo largo del Código como una simple adaptación dispersa a la realidad que se vivía.

Así pues, no se plasmaban en el Código las características de estos delitos, que por ello requieren un profundo análisis sobre el disvalor de la conducta del autor y el resultado producido.

Por eso, se considera que la reforma legislativa italiana obedeció no tanto a un sesudo proyecto de los parlamentarios, sino a la necesidad de dar cumplimiento a las directivas emanadas de la Comunidad Económica Europea a través del Consejo.

[3] Puede definirse como telemática la transmisión de datos a distancia entre y por medio de ordenadores. Si sustituimos el vocablo transmisión por el concepto de comunicación, comprendemos la palabra datos en un sentido amplísimo y sobreentendemos que tras los equipos informáticos hay personas, el concepto adquiere otro significado: la comunicación entre personas utilizando el ordenador como medio.

III. Los tipos penales introducidos por la ley y sus reformas

La antes mencionada reforma introdujo una gran cantidad de tipos penales en el Código. A continuación, trataré de agruparlos para una mejor exposición.

Atentado a instalaciones de utilidad pública.

El artículo 420 del Código Penal Italiano prevé en su figura genérica el atentado a las instalaciones de utilidad pública.

De este modo, sanciona con penas de uno a cuatro años al que, mediante la ejecución de una conducta, dañe o destruya instalaciones de utilidad pública, salvo que el hecho pueda encuadrar en una sanción más grave.

Con la reforma de 1993, se amplió el texto del artículo. Así, se incluyeron diversas actividades delictivas, como las conductas del que, mediante la ejecución de una conducta, dañe o destruya sistemas informáticos o telemáticos de utilidad pública, o bien datos, informaciones o programas contenidos o relacionados con ellos.

El artículo agrega que si del hecho derivase la destrucción o el daño a la instalación o del sistema, de la información o de los programas, o bien la interrupción –incluso parcial– del funcionamiento de la instalación o del sistema, la pena se eleva a una escala penal de tres a ocho años de reclusión (confr. artículo 2 de la ley 547/93).

Según la doctrina, el bien jurídico tutelado por este artículo es el orden público y los términos "datos", "información" y "programas" deben considerarse fungibles entre sí, en tanto el concepto técnico de "dato" es genérico y engloba sin duda los otros dos términos.

En el orden procesal debe decirse que el delito es perseguible de oficio, y que procede la detención en caso de flagrancia.

El tipo penal cuenta con un aspecto objetivo, constituido por la destrucción o el daño de instalaciones de utilidad pública o de investigación de elaboración de datos, o bien de sistemas informáticos o telemáticos de utilidad pública. Asimismo, se incluyen los datos, informaciones o programas contenidos en ellos.

La inserción de la palabra utilidad pública como elemento del tipo penal tiene efectos restrictivos sobre la aplicación de la figura, de modo que las instalaciones implicadas sean solo aquellas cuya desafectación pueda crear un peligro para el orden público.

De tal suerte, el concepto de utilidad pública se entiende en sentido funcional: esto es, en la estructura colectiva de su destino que excede la mera afectación al particular.

Sin embargo, la totalidad de las prescripciones introducidas en 1993, que acabo de reseñar, fueron dejadas sin efecto por la reforma del 18 de marzo de 2008.

Acceso indebido a un sistema informático y telemático

La figura está prevista por el artículo 615 ter del Código, y sanciona con penas de hasta tres años al que indebidamente se introduce en un sistema informático o telemático protegido por medidas de seguridad, o bien se mantiene contra la voluntad expresa o tácita de quien tiene el derecho de excluirlo. La pena sube de uno a cinco años si:

1) El hecho lo comete un oficial público o de un encargado de servicio público, quien abusando de sus facultades o violando los deberes inherentes a su función o servicio, o bien por quien ejercita también indebidamente la profesión de investigador privado o abusando de la calidad de operador del sistema.
2) Si el culpable del hecho usa violencia sobre las cosas o las personas, o bien lo concrete armado.
3) Si del hecho deriva la destrucción o el daño del sistema o interrupción total o parcial de su funcionamiento, o bien la destrucción o el daño de los datos, de las informaciones o de los programas contenidos en estos.

Por otro lado, si en los hechos previstos en los puntos uno y dos se tratan de sistemas informáticos o telemáticos de interés militar o relacionados con el orden público o a la seguridad o salud pública, a la protección civil o que de cualquier

modo revista interés público, la pena se eleva de uno a cinco años o de tres a ocho años, respectivamente.

Desde el aspecto procesal, el hecho previsto por el primer inciso es perseguible solo a instancia de acción privada, por la persona ofendida, en el resto de los casos, se procede de oficio (confr. art. 4 de la ley número 547/93.

Conviene advertir, respecto del bien jurídico tutelado, que el artículo fue introducido en el libro de los delitos contra las personas (II), en el marco de la tutela de la libertad individual, y más precisamente en lo que respecta a la inviolabilidad del domicilio (capítulo III).

Aquí debemos destacar que se trata del "domicilio informático" –el lugar en el que la persona desarrolla sus facultades intelectuales y expresa su forma de ser, con la consiguiente facultad de excluir a terceros– en tanto conforma un área de respeto a la privacidad, garantizado por el artículo 14 de la Constitución italiana y, en el ámbito penal, por la vieja redacción de los artículos 614 y 615 del Código Penal.

La jurisprudencia, por su parte, ha tenido oportunidad de expedirse precisando los alcances del tipo, al sostener que el acceso abusivo a un sistema informático o telemático se configura con la mera intrusión y que no exige que la conducta traiga aparejada una lesión de la reserva de los usuarios, ni tampoco que tal "invasión" se ejecute con el objetivo de violar su privacidad.[4]

La casación italiana también ha considerado que el delito previsto en el art. 615-ter c.p. se configura respecto del sujeto que, violando las disposiciones del titular regulador de los permisos de acceso, ingrese o se mantenga ilegítimamente en una base de datos o en un software de gestión.[5]

En esa sentencia también se sostuvo que, en el ámbito laboral y empresaria, tales parámetros se refieren a los límites de la autorización de acceso que pudiese tener el empleado, de modo que sea sancionable penalmente la conducta de acceso a un sistema informático producida en violación a las disposiciones o directivas impartidas en los casos en que el acceso a algunos datos sea materialmente impedido por contraseña o área reservada.

[4] Cámara de Casación Penal italiana, sentencia del 6 de febrero 2007, nro. 11689.
Cámara de Casación Penal, sentencia nro. 48895/2018.

Obtención o difusión indebida de códigos de acceso a sistemas informáticos o telemáticos

El artículo 615 quarter del CPI sanciona con prisión de hasta un año y multa de hasta diez millones de liras[6] al que, con el fin de obtener para sí o para otro un beneficio o provocar un daño al otro, indebidamente obtiene, reproduce, difunde, comunica o entrega códigos, contraseñas u otros medios idóneos para acceder a un sistema informático o telemático protegido por medidas de seguridad, o bien dicta indicaciones o instrucciones idóneas a dicho fin.

La pena de reclusión es de uno a dos años y la multa de diez a veinte millones de liras si concurre alguna de las circunstancias previstas en los números 1 y 2 del artículo 617 quarter párrafo cuarto, el cual veremos más adelante.

La norma bajo examen debe entenderse conglobante con los artículos siguientes y evidencia conductas netamente enunciativas que contienen todos los comportamientos que impliquen una efectiva amenaza para la seguridad de los sistemas.

La primera norma configura un delito de peligro, tendiente a prevenir el hecho dañoso. La jurisprudencia ha incluido en este tipo delitos como la clonación de celulares.[7]

Difusión de programas que tengan por fin dañar o interrumpir un sistema informático

El artículo 615 quinquies sanciona con pena de hasta dos años de prisión y con multa de hasta veinte millones de liras a quien difunde, comunica o entrega un programa informático confeccionado por él u otros que tenga por objeto o efecto el daño de un sistema informático o telemático de los datos, o de los programas en esos contenidos o relativos, o bien la interrupción total o parcial, o la alteración de su funcionamiento.

[6] 1 euro=2000 liras, aproximadamente.

[7] Cámara de Casación Penal italiana, sentencia del 17 de diciembre de 2004, nro. 5688.

La norma sanciona la conducta de quien introduce en el sistema un programa o un conjunto de datos dirigido únicamente a dañar el sistema en el que ingresa. En la norma se evidencian algunas hipótesis del daño que podría causarse y está destinado fundamentalmente a los virus informáticos.

En el marco de la jurisprudencia italiana, cobra especial relevancia el conocido como "caso Vierika", analizado por el tribunal de Bolonia en el que se condenó por este delito al difusor del virus conocido como Vierika.[8]

En primera instancia, se consideró que la propagación del virus alteraba el funcionamiento normal del Microsoft Outlook y del Internet Explorer, sin conocimiento del usuario. Asimismo, se agregó que debía encuadrase la conducta en el artículo 615 ter del Código Penal italiano, dado que el imputado había superado de modo abusivo los obstáculos predispuestos para proteger el acceso al sistema; es decir, el mero hecho de "bajar" la protección que tenía ya Internet Explorer podía considerarse como delito.

La sentencia fue apelada y la Corte de Apelaciones entendió que la creación del programa de auto reproducción y su lanzamiento en la web estaban unívocamente dirigidos a enviar e instalar de modo insidioso y fraudulento a una comunidad indiscriminada de usuarios que desconocía su origen usando sus datos personales de la firma de correo.

De tal suerte, explica el tribunal, la noción de "acceso abusivo" se ve configurada con el conocimiento indeseado de datos personales del domicilio informático que se identifica como el verdadero bien personalísimo protegido por la norma, y no tanto por el conocimiento o posibilidad de conocimiento de aquellos por parte del autor.

Daño de sistemas informáticos o de telemáticos

El artículo 635 bis prevé el daño a los sistemas informáticos o telemáticos, y sanciona con reclusión de seis meses a tres años a quien destruya, deteriore o torne inservibles, en todo o en parte, sistemas informáticos o telemáticos ajenos, o bien programas, informaciones o datos ajenos.

[8] Tribunal de Bolonia - Sentencia nro. 1823 del 21/07/2005.

El hecho se agrava si el responsable es operador del sistema, o bien concurre algunas de las agravantes de la figura genérica del artículo 635, a saber: ejercicio de violencia o amenazas contra la persona, si se trata de trabajadores en ocasión de un paro, sobre edificios públicos o destinados al ejercicio de un culto, de obras destinadas a la irrigación, etc.

El delito es perseguible de oficio. Con esta norma, el legislador ha intentado tutelar a los sistemas considerados en el marco de un patrimonio informático, y, por ello, considera agravante el hecho de que un operador del sistema cometa el delito.

La ubicación sistemática del delito –cerca del delito base de daño– busca proteger los componentes inmateriales del sistema, como datos y programas; pueden ser objeto de este delito todos los sistemas informáticos –total o parcialmente–, aun cuando el acceso se produzca de modo remoto.

Sobre el borrado, se considera que éste puede producirse por medio de una afectación al bien material (por ejemplo, desmagnetización), o por medio de la sustitución de datos con otros nuevos, o bien mediante el comando de borrado. Es de suma importancia aclarar que, aunque puedan recuperarse mediante algún programa de la especialidad, al vaciarse la papelera el delito se encuentra ya consumado.[9]

Ahora bien, con el objetivo de dar ejecución al Convenio sobre Cibercrimen del Consejo de Europa, en el año 2008, y a través de la sanción de la ley número 48, del 18 de marzo, se reformaron algunos aspectos de los delitos informáticos; y entre esas cuestiones, incorporó a este artículo una serie de agravantes a los tipos que he descripto.

Por caso, el art. 635-ter establece la figura del daño de información, datos y programas informáticos utilizados por el Estado o por otro ente público o de utilidad pública. En su redacción, sanciona con pena de uno a cuatro años a quien comete un hecho dirigido a destruir, deteriorar, eliminar, alterar o suprimir información, datos y programas informáticos utilizados por el Estado o por otro ente público o de utilidad pública.

[9] Así sostuvo la Cámara de Casación penal italiana en su sentencia de fecha 18/11/11 en causa seguida contra Spina, Roberto por el delito de daño informático.

Si del hecho se produce el resultado típico reseñado, la pena se fija entre tres y ocho años. Es decir, la norma sanciona la mera conducta de intentarlo, adelantando la punición, aun si el efecto deseado no se produce.

A partir de 2016, y por imperio del decreto legislativo número 7 del 15 de enero, se aumenta la pena si el hecho se comete con violencia contra la persona o amenaza al operador del sistema.

El artículo 635-quarter, por su parte, sanciona con penas de uno a cinco años a quien –mediante las conductas reseñadas en el artículo 635-bis, o bien a través de la introducción o transmisión de datos, informaciones o programas– destruye, daña o convierte en todo o en parte, inservible, sistemas informáticos ajenos u obstaculiza gravemente su funcionamiento. Asimismo, en 2016, mediante el decreto legislativo número 7 del 15 de enero, se aumentó la pena si el hecho se comete con violencia contra la persona o amenaza al operador del sistema.

Resta tratar en este acápite el delito de daño de sistemas informáticos de utilidad pública. En el art. 635-quinquies, se sanciona con reclusión de uno a cuatro años a quien comete el hecho previsto en el artículo 635 quarter contra sistemas de utilidad pública, y si logra el resultado, se aumenta la pena de tres a ocho años.

En todos los casos tratados, se extiende la punibilidad del delito de daño a programas o datos que antes eran imposibles de perseguir con la figura genérica caracterizada por la exigencia de la materialidad de la cosa.

De este modo, la doctrina ha entendido esto como el nacimiento de una nueva categoría de bien jurídico protegido, relacionado con la "integridad de los datos y los sistemas informáticos".

Fraude informático

El artículo Art. 640 ter sanciona al que –alterando de cualquier modo el funcionamiento de un sistema informático o telemático, o interviniendo ilegítimamente de cualquier manera sobre los datos, informaciones o programas contenidos en un sistema informático o telemático o relativo a éste– procure para sí o para otros un beneficio indebido con el daño ajeno. La sanción es de seis

meses a tres años de reclusión, y la multa es de cien mil a dos millones de liras. El delito es perseguible solo a instancia privada.

Asimismo, la pena se incrementa de uno a cinco años, y la multa de seiscientos mil a tres millones de liras, si el hecho se comete en perjuicio del Estado o de un ente público, o con el objetivo de hacer eximir a alguno del servicio militar (artículo 640, parte segunda, punto I). También se agrava la pena si el delito se comete abusando de la calidad de operador del sistema.

El delito es perseguible a instancia privada, salvo que concurra alguna de las agravantes. Este artículo ha sido bastante analizado por la doctrina italiana, en tanto abandona la vieja idea de la estafa cometida solo a través de un comportamiento humano y agrega la posibilidad de la intervención de una máquina en el ardid o engaño.

Por medio del tipo penal, se busca sancionar el incremento patrimonial indebido, obtenido a través del uso fraudulento de un sistema informático; es decir, debe existir una manipulación de un sistema en cualquier fase de su elaboración para lograr una ventaja patrimonial.

La ley 48 de 2008 introdujo la figura del fraude informático cometido por la persona que presta servicios de certificación de firma electrónica, estableciendo una pena de hasta tres años y multa de 51 a 1032 euros a quien, con el fin de procurar un beneficio indebido, o bien para generar un daño a otro, viola las obligaciones exigidas por la ley para la expedición de un certificado que exige calificación especial.

Ejercicio arbitrario de facultades propias con violencia sobre las cosas

La figura está regulada en el artículo 392 del Código, y ya estaba contemplada en el código originario que establecía una sanción de multa de hasta un millón de liras para aquel que, con el fin de hacer valer un derecho, y pudiendo recurrir al juez, de manera arbitraria lo ejecuta mediante violencia en las cosas.

Se agrega que se considera que hay violencia en la cosa aun si ésta termina dañada, transformada, o si muta su destino.

Sin embargo, para los fines de este trabajo, vale resaltar el párrafo siguiente, el cual agrega que se considera también violencia en las cosas cuando se afecta un sistema informático de modo que se lo altere, modifique o borre (total o parcialmente), o bien se impida o turbe el funcionamiento de un sistema informático o telemático (Confr. *art. 1, Ley 547/93).*

El delito es perseguible solo a instancia privada y, obviamente, no permite el arresto ni la prisión preventiva.

La importancia del artículo radica en que permite sancionar la violencia sobre las cosas que puedan configurarse en el caso de alteración de un programa informático: es decir, sobre un bien inmaterial. El legislador, entonces, ha querido tutelar nuevas modalidades de agresión que afectan tanto la vida cotidiana como las agresiones materiales.

La alteración al programa puede configurarse con la mera modificación de la esencia, como una manipulación total o parcial de las instrucciones que lo componen. La modificación del programa implica la intervención abusiva sobre este, a fin de transformarlo en otro distinto –sea en todo o en parte–, sin desnaturalizar sus funciones originarias. La supresión, en cambio, consiste en el borrado total o parcial de las instrucciones que lo componen.

La segunda de las hipótesis de violencia sobre las cosas tiene como objeto el funcionamiento de un sistema informático o telemático, por lo que quedarán incluidos los casos de molestias en el proceso de elaboración o de transmisión a distancia de datos que no consistan en una intervención directa sobre el programa.

Se configura el impedimento de funcionamiento del sistema, siempre que se desactiven las conexiones eléctricas o electrónicas de la computadora, haciendo que sea difícil para el usuario reiniciarlo o, al menos, individualizar la causa de la parálisis.

En cuanto a la turbación del funcionamiento del sistema, éste se configura por una acción de afectación del desenvolvimiento normal de las operaciones del elaborador, susceptibles de causar un perjuicio al legitimo usuario del sistema.

La jurisprudencia incluyó en la hipótesis del artículo 392, último inciso, la conducta de quien insertó en un programa gestor de maquinaria industrial una fecha de caducidad a partir de la cual se interrumpía la producción.[10]

Violación, sustracción y supresión de correspondencia

El artículo 616 del Código penal italiano sanciona con pena de hasta un año o con multa de seiscientos a un millón de liras a quien toma conocimiento del contenido de una correspondencia cerrada que no está dirigida a él, o bien sustrae o distrae, con el fin de que él u otro tome conocimiento de una correspondencia cerrada o abierta no dirigida a él, o bien en todo o en parte la destruye o suprime. Esto ocurre si el hecho no deriva en un delito más grave.

Si el culpable, sin causa justa, revela en todo o en parte, el contenido de la correspondencia, se sanciona, siempre que el hecho no deriva un prejuicio mayor, o el hecho mismo no constituye un delito más grave, con pena de reclusión de hasta tres años.

El delito es perseguible a instancia privada por la persona ofendida. A los efectos de las disposiciones de esta sección por "correspondencia", se entiende la epistolar, telegráfica, telefónica, o telemática, o bien efectuada con cualquier otra forma de comunicación a distancia (art. *5, 547/93).*

En el ámbito de las normas orientadas a reprimir los delitos contra la libertad individual, en la sección V, dedicada a la tutela de la inviolabilidad de los secretos, el legislador introdujo el IV parágrafo del artículo, equiparando formalmente el correo electrónico a la ordinaria, y superando el concepto de escritura en papel como único medio de documentación o comunicación de la voluntad de los sujetos trasmitida a distancia.

[10] Pretura di Torino (15 de mayo de 1996).

Interceptación, impedimento o interrupción ilegal de comunicaciones informáticas o telemática

El artículo 617-quater (incorporado mediante el artículo 6 de la ley 547/93) prevé genéricamente el delito de interceptación y sanciona con penas de seis meses a tres años a quien intercepta de manera fraudulenta comunicaciones relativas a un sistema informático o telemáticas o interconectado a más sistemas, o bien los impide o interrumpe.

Esta pena también se aplica a quien revela, por cualquier medio de información al público en todo o en parte, el contenido de las comunicaciones previstas en el primer párrafo, siempre que no constituya un ilícito mayor.

Desde el aspecto procesal debe decirse que los delitos previstos en los párrafos primero y segundo son perseguibles a instancia privada. Sin embargo, se procede de oficio, y la pena se eleva de uno a cinco años, si el hecho se comete:

1) dañando un sistema informático o telemáticas utilizado por el Estado o por otro ente público, o por una empresa que brinde servicios públicos o de necesidad pública;
2) por un oficial público o por un encargado de servicio público en abuso de los poderes, o con violación de los deberes inherentes a la función o al servicio, o bien con abuso de la calidad de operador del sistema;
3) por quien ejercita también indebidamente la función de investigador privado.

Al respecto, la Cámara de Casación Penal encuadró en la hipótesis del artículo 617-quater, inc. 2 del c.p. la conducta de quien difundió al público una transmisión de televisión transmitida de "punto a punto", es decir, fuera del espectro público a través de un canal reservado a comunicaciones de servicio, obtenida de modo fraudulento.[11]

[11] Cámara de Casación Italiana, sentencia nro. 4011 del 19 de mayo de 2005.

Instalación de instrumental apto para interceptar, impedir o interrumpir comunicaciones telemáticas o informáticas

El artículo 617 quinquies sanciona con penas de uno a cuatro años a quien fuera de los casos consentidos por la ley instala instrumental apto para interceptar, impedir o interrumpir comunicaciones relativas a un sistema informático o telemático o sistemas interconectados.

Se sanciona con reclusión de uno a cinco años los casos previstos en el punto cuarto del artículo 617-quater (ver *ut supra*).

El delito es perseguible de oficio y se admite el arresto en flagrancia.

La norma se dirige a penar la mera predisposición de aparatos aptos para interceptar, impedir o interrumpir comunicaciones telemáticas o informáticas. Bajo esta calificación legal, la jurisprudencia llevó a juicio a quien instaló en un cajero automático una ventanilla falsa y un sistema de video tendiente a capturar claves, siempre que no se haya logrado captar un código, por lo menos.

De tal suerte, la actividad ilícita prevista por el artículo se consuma con la mera aposición del mecanismo, siempre que sea idóneo para captar datos que, de otro modo, no hubiesen sido entregados.

Falsificación, alteración o supresión del contenido de comunicaciones informáticas o telemáticas.

El artículo 617 sexies sanciona a quien, con el fin de procurarse una ventaja, o bien atraer a otro un daño, confecciona falsamente, o bien altera o suprime en todo o en parte, el contenido, incluso si fuera interceptado ocasionalmente, de cualquiera de las comunicaciones relativas a un sistema informático o telemático o interrelacionados entre varios sistemas. Asimismo, se sanciona a quien haga uso de eso o deje que otros lo hagan. La pena va de uno a cuatro años, y se eleva el máximo a cinco en los casos previstos por el artículo 617 quarter.

La importancia de esta norma, que admite la persecución de oficio, es la de tutelar no solo el secreto, sino también la libertad informática. La protección a

la fe pública se ve con mayor evidencia, si se considera conjuntamente con el artículo 491 bis que se ubica en la parte pertinente a los documentos.

Al respecto, la norma mencionada más arriba establece que si algunas de las falsedades previstas en el capítulo respecto a un documento informático, público o privado, se aplican las disposiciones del capítulo y que conciernen a los documentos públicos y los instrumentos privados.

Finalmente, el artículo brinda la siguiente definición de documento informático: cualquier soporte informático que contenga datos o informaciones que tengan eficacia probatoria o programas destinados específicamente a elaborarlos. Este artículo fue agregado por el art. 3 de la ley 547/93.

La doctrina ha resaltado la importancia de este artículo, en tanto equipara sustancialmente los documentos informáticos a los de soporte de papel.

Mediante esta incorporación, el legislador ha superado la vieja dicotomía existente entre el documento informático y el de soporte en papel, ampliando la tutela legal a aquellos. De este modo, se refuerza la protección del bien jurídico de la fe pública, en tanto los documentos informáticos poseen idéntico carácter a los escritos.

Revelación del contenido de documentos secretos

El artículo 621 del digesto penal italiano sanciona con penas de hasta tres años o con multa de doscientos mil hasta un millón de liras a quien –habiendo tomado conocimiento indebido del contenido de un acto o documento ajeno, público o privado, que deba quedar en secreto, y que no constituya correspondencia– lo revela sin justa causa, o bien lo emplea a beneficio propio o de terceros, siempre que el hecho no derive en una afectación del documento.

A los efectos de la disposición de la primera parte del artículo se considera documento cualquier soporte informático que contenga datos, informaciones o programas.

Del aspecto procesal vale decir que el delito es perseguible a instancia privada iniciada por la persona ofendida.

La asimilación del documento informático a su análogo en papel es una consecuencia lógica del avance de la tecnología, puesto que la producción y almacenamiento intelectual se realiza, la mayoría de las veces, de manera virtual.

Tenencia de material pornográfico infantil

Si bien la doctrina italiana no ubica este delito dentro de los denominados crímenes informáticos, teniendo en cuenta la importancia del tópico y la alarma social que genera deberé referirme a la figura en la legislación italiana.

El artículo 600 ter, en su segundo párrafo, sanciona a quien, por cualquier medio, *incluso por vía telemática* (énfasis mío), distribuya, divulgue o publicite material pornográfico de menores de dieciocho años, o bien distribuya o divulgue noticias o informaciones que tengan por fin la apología o la explotación de menores de dieciocho años. La pena establecida es de uno a cinco años y multa de cinco a cien millones de liras.

Por su parte, la tenencia de material pornográfico infantil está penada por el artículo 600-quater, que sanciona a quien a sabiendas se procura o dispone de material pornográfico, producido mediante la explotación sexual de menores de dieciocho años. La sanción llega hasta los tres años de prisión o multa no inferior a tres millones de liras.

Estos delitos se ubican en el título correspondiente a los delitos contra la libertad individual, más precisamente, en la sección de delitos contra la personalidad.

Otras comunicaciones y conversaciones

Si bien no sanciona un delito en sí, la importancia del artículo 623 bis del código italiano radica en que equipara las comunicaciones y conversaciones telegráficas y telefónicas con las informáticas y telemáticas a cualquier otra transmisión a distancia de sonidos, imágenes o cualquier otro dato.

IV. *Excursus*. Algunas particularidades del tema tratado

La competencia

Al inicio de este trabajo, me referí a la importancia de los delitos informáticos para el derecho global, en virtud de la posibilidad de infringir la ley desde un lugar causando efectos en otro.

De este modo, uno de los tópicos más conflictivos respecto de los delitos informáticos es determinar la competencia territorial; es decir, qué juez debe intervenir según el código procesal.

La regla general aplicable en Italia es la del lugar donde se ha consumado el delito (artículo 8 inc. 1 c.p.p). En el marco de los delitos que hemos analizado, esto no resulta tan fácil de determinar, puesto que muchas veces resulta imposible llegar a ese "lugar" físico.

Así pues, en el marco del tratamiento de un caso de acceso abusivo a un sistema informático, la casación italiana en pleno consideró que el lugar de consumación es aquel en el cual se encuentra el sujeto que ejecuta la introducción abusiva o que la mantiene abusivamente, y no el lugar donde se encuentra el servidor que genera y controla las credenciales de autenticación provistas por el agente.[12]

La regla de la competencia con base en el lugar donde se encuentra el cliente no encuentra excepciones para la forma agravada del delito de introducción abusiva en un sistema informático. A idéntica conclusión se debe llegar respecto de las conductas del mantenimiento en el sistema informático contra la voluntad de quien tiene derecho a excluirlo (art. 615 del CP).

Me parece pertinente tratar en este acápite el papel de la denominada "Policía Postal" en la investigación de los delitos que estamos analizando. El deber de vigilar la internet le fue conferido por decreto del Ministerio del Interior del 31 de marzo de 1998, y le otorgó amplias facultades para que, desde su sede en Roma, lleve a cabo un seguimiento de los delitos de pornografía infantil, ciberterrorismo, copyright, *hacking* y apuestas en línea, entre muchos otros delitos.[13]

[12] Ver sentencia del 26 marzo 2015, n. 17325.

[13] https://www.cybersecurity360.it/cultura-cyber/reati-informatici-quali-sono-e-che-cosa-si-rischia/

La confiscación

En 2012, con ley número 12 del 15 de febrero, se agregó un inciso al artículo 240 del Código Penal, en el que se establece de modo imperativo para el juez ordenar la confiscación de los bienes y de los instrumentos informáticos que hayan sido utilizados en todo o en parte para la comisión de los delitos previstos por los artículos 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 635-quinquies, 640-ter y 640-quinquies.

Asimismo, ordena la confiscación de los bienes que se erigen como producido del delito, ya sean sumas de dinero, bienes u otras utilidades sobre las que el condenado tenga la disponibilidad por un valor equivalente a ese provecho, en caso de que no pueda confiscarse esa suma directamente.

La misma ley establece que las disposiciones de la primera parte del artículo reseñado deben también extenderse a los casos de condena o a la aplicación de la pena, a petición de parte en los términos del artículo 444 del Código procesal penal italiano[14] para aquellos delitos conexos con finalidades de terrorismo, subversión, producción o comercio de material pornográfico.

En estos casos, se dispone la confiscación de dinero, bienes y otras utilidades de las cuales el condenado no pueda justificar su procedencia y sobre las cuales, aun por interpósita persona física o jurídica, resulta ser titular o tener la disponibilidad a cualquier título en valores desproporcionados a su actividad declarada en el impuesto a las ganancias.

[14] Dice el artículo 444 del Código de procedimientos penales italiano que el imputado y el Ministerio Público pueden solicitar al juez conforme la especie y medida indicada, la aplicación de una sanción sustitutiva o de una pena pecuniaria disminuida hasta en un tercio, o bien de una pena restrictiva de la libertad cuando esta, teniendo en cuenta las circunstancia y disminuida hasta un tercio, no supere los cinco años, ya sea sola o junto a una pena pecuniaria. Así pues, el juez es quien dispone la imposición de la pena valorando los requisitos de procedencia de la solicitud impetrada. Es de advertir que el imputado no queda obligado al pago de costas, además de obtener como beneficio que los efectos penales se extinguen en la mitad del plazo contemplado por el Código de fondo.

V. Conclusiones

Uno de los objetivos del derecho comparado moderno es el de cotejar no solo legislaciones enteras o cuerpos normativos, sino problemas específicos que se suscitan en los distintos países y las respuestas que los ordenamientos legislativos dan a ellos.

En el presente artículo, se intentó dar un breve resumen de la legislación italiana, en relación a los delitos informáticos con el objeto de exhibir cómo en Italia se ha querido solucionar un problema que aqueja a toda la comunidad internacional.

La técnica legislativa intentó, en el marco del respeto al principio de legalidad, por un lado, actualizar ciertos tipos penales ya existentes para adaptarlos a la realidad de estas tecnologías, como puede ser el fraude mediante medios informáticos; y, por el otro, crear nuevos, como puede serlo el acceso indebido a sistemas o la divulgación de contraseñas.

Una particularidad que se presenta al observar los tipos penales incorporados en el marco de la ley 547/93 es la ausencia de tipos culposos que sí se presentan, por ejemplo, en la ley argentina número 26.388 –mediante la inclusión del segundo párrafo del artículo 255– y la faltante de tipos omisivos.[15]

Desde mi perspectiva, resulta necesaria la exhaustiva regulación de la figura de daño informático, con sus variantes y, sobre todo, mediante la separación de lo que son los datos de los sistemas, y estos a su vez del hardware.

En cuanto a la órbita procesal, se advierte que en el derecho italiano proliferan los delitos dependientes de acción privada en detrimento de la procedencia de oficio, la cual se verifica en los casos en que esté comprometido el orden público.

Asimismo, resulta relevante mencionar que se han instaurado respecto de este delito sanciones que exceden la pena de reclusión. A tales fines, como hemos

[15] ARTICULO 255. - Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500) **(**énfasis mío).

visto, el legislador ha aplicado con rigor la confiscación de bienes para esta clase de delitos.

En definitiva, si bien las respuestas que el derecho penal depende en gran parte del éxito de las investigaciones de los hechos delictivos, lo cierto es que una legislación que prevea las conductas específicas que pretende punir es siempre una buena noticia para la vigencia del principio de legalidad.

Bibliografía

Codice di procedura penale.

Costituzione italiana

Codice penale

Cordero, Franco (2000), *Procedimiento Penal,* Temis, Bogotá.

García Torres, María José (2004), *El Proceso Penal abreviado y el acuerdo el imputado. Legislación comparada y análisis constitucional,* Fabián J. Di Plácido Editores, Buenos Aires, 2004.

Salvadori, Ivan (2013). "La regulación de los daños informáticos en el código penal italiano". En: María José PIFARRÉ (coord.) "Internet y redes sociales: un nuevo contexto para el delito" [monográfico en línea]. IDP. *Revista de Internet, Derecho y Política*. Número 16, pág. 44-60. UOC.

Chiavario, Mario; *Commento al Codice di procedura penale (terzo aggiornamento)*; UTET, Torino, Italia, 1998.

Fiandaca, G.; Musco, E. (2007). *Diritto penale, Parte speciale.* Bolonia: Zanichelli. 5.ª ed. Vol. II, tomo II.

Fiandaca, G.; Musco, E. (2012). *Diritto penale, Parte generale.* Bolonia: Zanichelli. 6.ª ed.

Mantovani F. (2009). *Diritto penale, Parte speciale*. Padua: Cedam. 3.ª ed. Vol. II.

Pecorella, C. (2006a). “Commento all’art. 615-ter c.p.”. En: E. Dolcini, G. Marinucci (ed.). Codice penale commentato. Milán: Giuffrè. 2.ª ed. Pág. 4330 y sig.

Pecorella, C. (2006b). Il diritto penale dell’informatica. Padua: Cedam. 2.ª ed.

Pica, G. (1999). Diritto penale delle nuove technologie. Turín: Giappichelli.

Cómo citar el artículo: Fusco, L. (2020). Los delitos informáticos en el código penal italiano. *Derecho Global, Estudios sobre Derecho y Justicia,* V. (14) pp. 127-149 https://DOI.org/10.32870/dgedj.v5i14.250