LA TRANSPOSICIÓN DEL CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA EN LA LEGISLACIÓN FRANCESA EN LA PRÁCTICA

Cynthia SOLÍS*
Vincent LEMOINE**

SUMARIO: I. *Introducción*. II. *La Convención sobre cibercriminalidad*. III. *El problema de la aplicación práctica de la Convención de Budapest en Francia*. IV. *El problema de la modificación de los datos*. V. *El problema del lugar de almacenamiento de los datos*. VI. *Bibliografía*.

I. INTRODUCCIÓN

El uso de las nuevas tecnologías de información y la comunicación en los asuntos judiciales, han llevado a los jueces y en especial a los investigadores a cuestionar las modalidades de aplicación del Código de Procedimientos Penales. Sin lugar a dudas, existe un gran incremento en los actos ilícitos resultantes del uso de estos vastos sistemas de comunicación, que ahora simbolizan el estandarte de una sociedad inmersa en la red.

De hecho, las nuevas tecnologías pueden permitir o facilitar la comisión de un delito, como el uso de un teléfono para informar a los delincuentes en un acto específico o permitir la comisión del delito directamente usando una computadora para realizar una intrusión en un sistema remoto.

En los últimos años, estos sistemas han cambiado profundamente la naturaleza de las relaciones sociales y las relaciones entre los individuos, en particular en cuanto a sus orientaciones. Este tipo de herramientas no

* Investigadora adscrita al Centro de Estudios e Investigación en derecho inmaterial de las universidades Panthéon Sorbonne y Paris Sud; y maestra en derecho de la innovación técnica.

** Perito en forense informática, profesor investigador de la Universidad Paris Sud y doctor en derecho.

sólo se utilizan para fines privados (correo electrónico, *chat*, búsquedas en la web), sino también para el uso profesional, y en general en todos los actos de la vida (medios de pago, transferencias electrónicas, transporte). De hecho, ¿Existen herramientas utilizadas hoy en día, que no incluyan algún tipo de tecnología? ¿Quién no ha hecho uso del comercio electrónico para hacer una compra?

Con el desarrollo del acceso a través de la banda ancha a partir de 2001, las nuevas tecnologías se han convertido en una parte esencial de la economía (compras, gestión, publicidad, etcétera). Ellos están en constante crecimiento, y el número de personas que los utilizan no ha dejado de crecer.

En quince años, hemos pasado de simple "*pager*" para recibir un mensaje de texto, a Internet a través del teléfono móvil para recibir la radio de banda ancha, la televisión, y el progreso no se detiene allí. Una encuesta realizada por el sitio web de Silicon[1] en septiembre de 2010, puso de relieve que Francia tenía 21.4 millones de suscriptores de Internet y 62.6 millones de teléfonos móviles.

En paralelo, los actos delictivos relacionados con las nuevas tecnologías o cometidos por ellos, también están en aumento. No es raro ver cada semana en las noticias un caso de pedofilia, intrusión, fraude o abuso a través de sitios web.

Desde 1978, el legislador tuvo la intención de prevenir esta situación a través de la Ley de Protección de Datos,[2] mejor conocida como la Ley de Informática y Libertades, con respecto a la creación de bases de datos. Esta legislación es más conocida bajo el acrónimo de la comisión encargada de supervisar este tipo de delitos, es decir, la "CNIL",[3] Comisión Nacional de Informática y Libertades, la cual es fruto del proyecto que nació muerto llamado Safari.

En 1988, la Ley Godfrain[4] creó nuevos tipos penales, orientados a criminalizar ciertas conductas relacionadas con el procesamiento automatizado de datos. Las nuevas tecnologías, en general, se pueden utilizar directamente para atacar, permitir o facilitar la comisión de los mismos.

---

1 *Les abonnements Internet se tassent en Francs*, por Christophe Lagane en http://www.silicon.fr/les-abonnements-internet-se-tassent-en-france-43682.html, consultado el 20 de octubre de 2014.

2 http://www.cil.cnrs.fr/CIL/spip.php?rubrique281, consultado el 20 de octubre de 2014.

3 *Atteinte aux systèmes d'informations*, por Alain Bensoussan, en www.alain-bensoussan.com, consultado el 20 de octubre de 2014.

4 *Panorama de la cybercriminalité en 2010*, en el sitio de CLUSIF, http://www.clusif.asso.fr., consultado el 20 de octubre de 2014.

La definición más apropiada para describir la nueva tecnología es "cualquier medio para comunicar, procesar, almacenar datos, así como la gestión de los sistemas informáticos o incluso mecánicos". El alcance de estas nuevas tecnologías es relativamente grande.

El legislador francés, a través del artículo L.32 de la Ley de Telecomunicaciones Electrónicas, define con mucha precisión la terminología, tomando en cuenta diversos aspectos técnicos y jurídicos, citados a continuación:

1. *Comunicaciones electrónicas*. Se entiende por comunicaciones electrónicas a las emisiones, transmisiones o recepciones de signos, señales, escritos, imágenes o sonidos, enviados por vía electromagnética.
2. *Red de comunicaciones electrónicas*. Se entiende por red de comunicación electrónica, toda instalación o conjunto de instalaciones para el transporte o la difusión y, en su caso, otros medios de garantizar la entrega de las comunicaciones electrónicas, incluidos los de conmutación y enrutamiento. Se consideran como redes de comunicación electrónica: las redes satelitales, redes terrestres, así como los sistemas que utilizan dichas redes, siempre y cuando se utilicen para el suministro de redes de comunicaciones electrónicas y asegurar la difusión o las utilizadas para la distribución de servicios la comunicación audiovisual.

Pero, ¿qué es en sí un dato informático?

A nivel de la Unión Europea. En términos del artículo primero de la Convención Europea en materia de la lucha contra la cibercriminalidad del 21 de noviembre de 2001, mejor conocida como la Convención de Budapest,[5] esta expresión "Datos informáticos", se define como: "Toda representación de hechos, de información o de conceptos en formato idóneo para ser tratada a través de medios informáticos, incluido el propio sistema de tratamiento".

Una de sus principales características es la de ser intangible, es decir, palpables como cualquier otro documento en papel. Únicamente el soporte material que contiene los datos, por ejemplo, un disco duro, un CD-Rom, una memoria flash o incluso una terminal móvil, pueden ser percibidas físicamente; es por ello que la propia explicación de motivos de la Convención

[5] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF, consultado el 19 de octubre de 2014.

proporciona una serie de definiciones importantes, utilizadas a lo largo de su redacción.

Los datos informáticos pueden constituir un recurso para un sistema o una red informática. Por sistema informático es importante comprender todo dispositivo que, por sí mismo o en su conjunto, aseguran a través de la ejecución de un programa, un tratamiento automatizado de datos. Es entonces el conjunto de elementos que participan en la administración, almacenamiento, tratamiento, transporte y difusión de la información en el seno de una organización, en conjunto con el propio medio informático como una computadora, un servidor o cualquier sistema de explotación donde se encuentre presente.

A nivel Francia. El legislador reagrupa las diferentes definiciones jurídicas en un código único, el citado anteriormente de la Ley de Comunicaciones Electrónicas, en su artículo L.32, en el que se dispone lo siguiente:

> 1. *Comunicaciones electrónicas*. Se entiende por comunicaciones electrónicas a las emisiones, transmisiones o recepciones de signos, señales, imágenes o sonidos por vía electromagnética.
>
> 2. *Redes de comunicaciones electrónicas*. Se entiende por red de comunicaciones electrónicas, toda instalación o conjunto de instalaciones de transporte o difusión, y en su caso, otros medios que aseguren el encaminado de comunicaciones electrónicas, en particular aquellos de conmutación y enrutamiento.
>
> Se consideran como redes de comunicaciones electrónicas: las redes satelitales, redes terrestres, sistemas que utilicen la red eléctrica para garantizar el encaminado de las comunicaciones electrónicas y aquellas que aseguren la difusión o distribución de servicios de comunicación audiovisual.
>
> 3. *Red abierta al público*. Se entiende por red abierta al público toda red de comunicaciones electrónicas establecidas o utilizadas para proveer al público de servicios de comunicación electrónicas o servicios de comunicación al público por vía electrónica.

Hoy en día es muy difícil que alguien no cuente con un teléfono celular o acceso a Internet, sobre todo en países desarrollados como los europeos, en México, incluso miles de personas cuentan con este tipo de dispositivos tales como: computadoras portátiles, tabletas, GPS (*Global Positioning System*) y teléfonos inteligentes, ya sean propios o de sus lugares de trabajo; todos ellos conectados a Internet.

La industria poco a poco ha automatizado procesos sustituyendo el trabajo humano por el de las máquinas; en la obra intitulada *Las TIC en los desarrollos habitacionales de México*, editada por INFOTEC, se demuestra la

importancia que tienen las nuevas tecnologías en la vida diaria de nuestros connacionales.

Desgraciadamente, si el legislador francés hubiese previsto en aquella época reprimir ciertas acciones a través de las citadas leyes, no hubiera necesitado modificar el Código de Procedimientos Penales para crear nuevas disposiciones para facilitar la ejecución de las investigaciones judiciales. Desde hace diez años, al fin ha puesto en marcha la creación de numerosas reformas en la materia.

En paralelo, en un ámbito puramente civil la firma electrónica en Francia no fue reconocida como válida hasta el año 2000 por la Ley núm. 2000-230 del 13 de marzo de 2000 la cual incluyó la adaptación del derecho de la prueba a través de tecnologías de la información relativa a la firma electrónica y su decreto 2001-272[6] del 30 de marzo de 2001. Esta ley se dio con motivo de la transposición de la directiva comunitaria del 13 de diciembre de 1999,[7] estableciendo un esquema comunitario para las firmas electrónicas.

En materia de procedimiento penal especial en materia de nuevas tecnologías, fija las reglas aplicables a los diferentes actores de la justicia: magistrados, policías, gendarmes, incluyendo aquellos actos y procedimientos que permitiesen realizar requisiciones de informáticas, intervención de equipos y sistemas de cómputo e interceptar correspondencia electrónica.

II. La Convención sobre Cibercriminalidad

En realidad no fue hasta 2001, que las primeras disposiciones a nivel de la Unión Europea vieron la luz a través de la Convención del 23 de noviembre de 2001 de Budapest. De hecho era imperativo que el derecho penal pudiera seguir el ritmo de las evoluciones tecnológicas, las cuales, además de ofrecer beneficios inigualables, también abren un universo de posibilidades para los delincuentes.

En la exposición de motivos de dicha Convención, el Consejo Europeo hace énfasis en ello.

La recomendación núm. R(89) 9 del Consejo de Europa,[8] ciertamente ha permitido acercarse a las concepciones nacionales que tocan al uso

[6] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796, consultado el 10 de octubre de 2014.

[7] http://www.dnielectronico.es/marco_legal/directiva_1999_93_CE.html, consultado el 20 de octubre de 2014.

[8] Véase el índice cronológico y referencias en http://www.mjusticia.gob.es/cs/Satellite/1292344070605?blobheader=application%2Fpdf&blobheadername1=Co

abusivo de las computadoras. Únicamente un instrumento jurídico internacional puede tener la eficacia necesaria contra estos nuevos fenómenos, un instrumento que permitiese la cooperación internacional y, además de ello, tratar cuestiones de derecho sustantivo y adjetivo. Uno de los grandes avances es incluir la posibilidad y legitimidad jurídica de combatir el crimen a través de los mismos medios informáticos, es decir, que el remedio y la enfermedad se encuentren al mismo nivel de competencia.

Sin pretender colocar a la convención en un pedestal ni tomarla como la panacea en el tema, es cierto que es la piedra angular de los avances en materia de cibercriminalidad, no solamente para la Unión Europea sino para los demás Estados firmantes, dentro de los cuales, según las predicciones, se encontrará nuestro país.

La Convención ha ido perfeccionando sus preceptos, por ejemplo, con el protocolo adicional relativo a la incriminación de actos de racismo y xenofobia a través de sistemas informáticos del 28 de enero de 2003 en Estrasburgo, así como la de Lanzarote del 25 de octubre de 2007 en materia de explotación y abuso sexual infantil.

Ahora bien, aterrizando en la realidad actual, no basta con las buenas intenciones, ya que muchos de los Estados firmantes han tardado demasiado en ratificar, además de que existe una gran paradoja, ya que la Convención de Schengen[9] de 1990, puesta en marcha en 1995, instauró la apertura de las fronteras entre los Estados firmantes, así como la libre circulación de personas y bienes.

El Tratado de Lisboa, del 13 de diciembre de 2007, vino a completar las reglas jurídicas de la zona Schengen, reforzando la noción de "espacio de libertad, seguridad y justicia", por lo cual, ya se encontraba sobreentendida la obligación de cooperación policial y judicial entre los Estados para garantizar estas premisas.

Luego entonces, no es fácil explicar cómo es que países como España y Bélgica siguen negándose a cooperar en la materia sin ratificar la Convención de Budapest, lo cual complica en la práctica la persecución de delitos informáticos desde Francia, haciendo obligatoria la exigencia de una requisición internacional para acceder a cooperar.

---

ntent-Disposition&blobheadername2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1991_1599.pdf&blobheadervalue2=1288777592356, consultado el 20 de octubre de 2014.

[9] http://europa.eu/legislation_summaries/glossary/schengen_agreement_es.htm, consultado el 20 de octubre de 2014.

Lo anterior implica un proceso bastante complejo y pesado que desde luego se convierte en una incoherencia con la manifestación de buenas intenciones de cooperación en la materia.

El principal mensaje de la décimo segunda edición del Congreso de las Naciones Unidas de 2010 para la prevención del crimen y la justicia penal, fue justamente la puesta en marcha de instrumentos jurídicos eficaces, en particular la Convención de Budapest, como representación del mejor medio para ayudar a los países para ayudar a luchar contra la cibercriminalidad en todo el mundo.

Canadá, por ejemplo, recibió con singular interés el mensaje redundando en la creación de sus dos proyectos de Ley, el C.51[10] y el C.52,[11] en materia de investigaciones informáticas y prevención del ciberdelito.

Por lo tanto, una de las principales inquietudes de los servicios policiacos a nivel Unión Europea, que se ven obligados a reflexionar acerca de las dificultades en cuanto a las investigaciones, la uniformidad de las legislaciones, y principalmente por parte del Colegio Europeo de Policía (CEPOL). Este organismo se ha dedicado a organizar regularmente seminarios a lo largo de todos los países de la Unión Europea destinado a la capacitación de policías y gendarmes, el último de ellos llevado a cabo en Atenas en 2010.

Entrando a detalle, la Convención de Budapest permite definir conceptos unificados a fin de que los Estados puedan utilizar la misma terminología al momento de adaptar su legislación local, así como tomar las medidas pertinentes para su puesta en marcha, misión que no es nada sencilla al interior de cada país.

Los temas que se abordan son extensos e incluyen desde los lógicamente aplicables como intrusiones ilícitas a sistemas, falsificaciones y fraudes informáticos, hasta aquellos relativos a la protección de la propiedad intelectual, pornografía infantil y abuso sexual de menores.

Otra de las innovaciones que presenta es la de permitir las nociones de tentativa y complicidad en las infracciones evocadas en sus artículos 2o. al 8o., así como la responsabilidad de las empresas, recordando que puede ser penal, civil o administrativa, según el caso.

Ahora bien, para algunos países como Francia, este tipo de disposiciones no representan ninguna novedad ya que se encontraban incluidas desde 1978 y 1988 respectivamente; sin embargo, es imposible negar que a nivel

[10] http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c51-f.pdf, consultado el 20 de octubre de 2014.

[11] http://www.ledevoir.com/politique/canada/332857/projet-de-loi-c-52-l-intimite-numerique-des-canadiens-pourrait-etre-menacee, consultado el 15 de octubre de 2014.

de procedimientos penales, sí representa un gran avance, sobre todo en la parte que toca a la obtención de evidencias informáticas.

Por ejemplo, el artículo 16 de la Convención de Budapest[12] impone a las partes, la adopción de medidas legislativas que permitan a sus autoridades competentes el ordenar la conservación rápida de evidencias informáticas específicas, tales como datos de tráfico o almacenamiento en un sistema informático y, sobre todo, cuando son volátiles, es decir, susceptibles de pérdida o modificación.

Concretamente en los hechos, los servicios de investigación se vuelven lentos y se contraponen con lo establecido si tomamos en cuenta que existe la obligación de recurrir mediante una demanda por escrito a la Sección Central de Cooperación Operativa de la Policía, mediante la cual se pueda garantizar que los datos queden "congelados" durante 90 días y cuando así se requiera otros 90 días más; tiempo en el que el magistrado revisará si procede la emisión de una carta rogatoria internacional al país que aloje la información.

III. El problema de la aplicación práctica de la Convención de Budapest en Francia

La mayor parte de intercambios realizados cotidianamente por los internautas, en términos de correos electrónicos, mensajería instantánea, redes sociales y almacenamiento de información en la nube, pasan por servidores o prestadores de servicios radicados en Estados Unidos, por ejemplo: Hotmail, Yahoo, Gmail, Twitter, Facebook, etcétera. Aun cuando este país es firmante de la convención desde 2006, la realidad es que tanto investigadores como magistrados parecen desconocer a detalle las disposiciones relativas al acceso de dichos datos.

El artículo 57-1 del Código Francés de Procedimientos Penales, inspirado en el artículo 19 de la Convención de Budapest, permite realizar intervenciones a distancia, si bien es cierto que los redactores de la Convención comprendían los diferentes servicios judiciales como la policía y la gendarmería francesas, el artículo 57-1, únicamente permite estas intervenciones en el territorio francés.

Sin embargo, en términos del artículo 31 de la Convención, sobrevive la posibilidad de requerir directamente al Estado miembro su cooperación a través de una demanda de cooperación judicial formulada por las autori-

[12] *Ibidem*, p. 4.

dades francesas. Por lo que compete a Estados Unidos, lo más frecuente en materia de investigaciones de este tipo es adherirse al decreto 2001-1122,[13] el cual establece la cooperación entre Estados Unidos y Francia, y conviene mucho más a los intereses de la investigación.

Si bien es cierto que el proceso es largo y pesado, es más sencillo que seguir el procedimiento establecido en la Convención, lo cual retrasaría mucho más la investigación sin contar el hecho de la desaparición de las pruebas.

IV. El problema de la modificación de los datos

El primer problema al que se enfrentan los investigadores especialistas, como el coautor de la obra, Vincent Lemoine, implica utilizar la computadora de la persona investigada y con ello modificar los eventuales datos alojados en ella, ya sea agregando o modificando los datos existentes al momento de actualizarlos.

Este problema radica en la propia arquitectura de los sistemas y del propio tiempo. Es un hecho que al momento de que un investigador o el mismo usuario de una computadora interactúa con ella, desde luego que será modificada la información, lo anterior como resultado de la propia actualización de los sistemas, de los antivirus, descarga de correos electrónicos, etcétera.

El conjunto de los procesos anteriormente descritos se cargan en la memoria viva de la computadora, mejor conocida como memoria RAM (*Random Access Memory*), así como en los archivos temporales que se guardan en los diferentes espacios del disco duro. Particularmente la información que se encuentra en archivos de paginación del sistema operativo (*pagefile.sys*) o el archivo de hibernación (*hyberfile.sys*).

Estos archivos, cuyo tamaño es bastante significativo, también almacenan todos los archivos abiertos y las operaciones realizadas a través del sistema operativo, por lo tanto, todas las modificaciones serán efectuadas cuando el sistema esté en funcionamiento y serán multiplicadas si el investigador las utiliza para expatriar los datos.

Por ejemplo, desde que una computadora se conecta a Internet, la información es transmitida permanentemente a través de paquetes basados en el protocolo TCP/IP, lo que permite una conexión a distancia entre dos

[13] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000393833, consultado el 10 de octubre de 2014.

sistemas que se encuentran o pueden encontrarse completamente lejanos uno de otro.

Del otro lado, nos enfrentamos al hecho de que la operación tiene que ser realizada desde el sistema inicial, es decir, el domicilio de la persona donde tuvo lugar la investigación, lo que necesita un mínimo de conocimientos técnicos por parte del grupo de investigadores y, en la práctica, muy pocos oficiales cuentan con dichos conocimientos; tratándose de investigaciones realizadas en empresas el asunto puede volverse aún más complejo; por ejemplo, un Centro de Datos que normalmente se encuentran en el extranjero.

Antes de proceder a la investigación es indispensable identificar el lugar preciso donde reside la información a analizar, realizando un inventario completo de la configuración del *hardware* y del *software*, pero sobre todo el nivel de seguridad, el cual seguramente deberá de ser bastante alto; y si a eso le agregamos el hecho de que muchas empresas cuentan con funcionalidades de "puerta trasera" mediante las que pueden respaldar y restaurar su información, es necesario saber si están implementadas para que el investigador las desactive e impida la alteración de la evidencia, lo cual la mayoría de los investigadores desconoce y pasa por alto. El artículo 57-1 del Código Francés de Procedimientos Penales prescribe a los agentes de la policía judicial a realizar una investigación directamente a partir de un sistema en funcionamiento, luego entonces, se contrapone directamente con el principio fundamental de la criminalística que impide alterar los indicios.

De hecho, el principio dictado por Edmon Locard,[14] se aplica perfectamente desde el momento que una computadora se encuentra funcionando sobre una red informática y es por ello, que esta disposición, si bien es legal, es raramente utilizada por los investigadores.

Estos últimos prefieren realizar sus peritajes *a posteriori*, por técnico especialista en la tecnología de la que se trate, lo cual no se encuentra previsto en las disposiciones del Código de Procedimientos Penales.

Hay que recordar que el espíritu del proceso no se limita a la investigación policial, pero es un hecho que marca la diferencia en cuanto al seguimiento del mismo. Ya sea que se trate de la fase de instrucción preparatoria o del juicio o en ambos casos, un peritaje puede ser exigido ya sea por el juez o por el ministerio público, o incluso por las partes, para aclarar algún punto preciso.

[14] Referencia al principio de Intercambio de Locard, http://inza.wordpress.com/2006/03/05/edmond-locard/, consultado el 20 de octubre de 2014.

En este caso, cuando el perito sea llamado a presentar su informe, se enfrentará al problema de evidenciar todas aquellas manipulaciones efectuadas en el sistema a analizar, por lo tanto, se constatará que la evidencia ha sido alterada y debe precisarlo correctamente al momento de presentar verbalmente las conclusiones de su informe.

En efecto, uno de los principios esenciales en materia criminalística, tal como se evoca en la obra de Harlan Carvey, llamada *Herramientas de análisis forense en Windows*, es indispensable describir cada acción y mencionar fecha y hora de las misma, así como las personas que han sido autorizadas para tal efecto en el expediente, lo que conocemos en México, como la cadena de custodia. En el caso de descargas de información remota, únicamente se habla de los datos visibles y no aquellos ocultos o borrados, la recuperación de éstos puede llevarse a cabo, pero el costo es exponencial.

Para poder realizar este tipo de análisis, se requiere de programas especializados llamados "e-discovery". Algunas compañías, como *Guidance Software*, trabajan arduamente en ingresar al mercado sobre todo de los investigadores y posicionar este tipo de herramientas.

El principio de la alteración de un indicio fue retomado en el capítulo IV relativo a las barreras u obstáculos en cuanto a la presentación de pruebas en justicia, en el artículo 434-4[15] del Código Penal francés, el cual dispone:

> Se castigará con tres años de prisión y 45 000 euros de multa, cualquier acto que obstaculice o manipule la manifestación de la verdad, como lo es:
>
> 1o. Modificar el lugar de los hechos de un crimen o delito, a través de la alteración, la falsificación, el borrado de rastros o indicios, ya sea aportando, moviendo o suprimiendo objetos,
>
> 2o. Destruir, sustraer, ocultar o alterar un documento público o privado o un objeto susceptible de facilitar el descubrimiento de un crimen o un delito, la búsqueda de pruebas o la condena de los culpables.
>
> En caso de que los hechos previstos en el presente artículo sean cometidos por una persona que ya sea por sus funciones, es llamada a coadyuvar a manifestar la verdad de los hechos, la pena aumentará a cinco años de prisión y 75 000 euros de multa.[16]

[15] http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418608&cidTexte=LEGITEXT000006070719, consultado el 26 de octubre de 2014.

[16] *Idem*.

Estamos en presencia de un agravante en razón de la cualidad del sujeto, en este caso, el investigador, un técnico o un perito en la materia, ya que todas estas personas son llamadas a coadyuvar en la impartición de justicia a través de la manifestación de la verdad. Es conveniente recordar que los datos informáticos son extremadamente volátiles y que todo acceso a distancia tendrá el impacto que ya se ha mencionado.

La única solución legalmente admisible podría ser el proceder en dos tiempos, es decir: en un primer tiempo realizar una copia bit a bit del disco duro de la computadora y después colocar el disco duro original sellado. Una copia bit a bit es una copia idéntica de un disco. De hecho, contrariamente a ciertas pruebas biológicas de que no es posible la clonación, un soporte digital puede ser clonado en numerosas ocasiones sin límite.

En una segunda etapa es necesario colocar la copia bit a bit del disco duro clon, en la computadora y en ese momento comenzar las investigaciones, de esta manera, la prueba no será alterada y por lo tanto y las pruebas obtenidas a distancia serán copiadas en el clon y no en el original.

Si esta operación, que es jurídica y técnicamente admisible, puesto que la copia de datos informáticos se encuentra prevista por el artículo 56 del Código de Procedimientos Penales, la realidad es que no puede llevarse a cabo de forma tan sencilla dada la creciente capacidad de los nuevos discos duros, ya que esto implica un tiempo de copia bastante importante a través de sistemas para los cuales se debe contar aproximadamente un minuto por cada gigabyte.

Por otra parte, esta copia debe realizarse en presencia de la persona que será investigada, esto impacta desde luego el proceso ya que este periodo puede ser superior a las 24 horas en caso de grandes volúmenes de datos o de demasiados soportes a copiar. La copia no puede interrumpirse y esto reduce los tiempos de retención legal del objeto a analizar.

De hecho, el estándar actual en la capacidad del disco duro en un equipo es de aproximadamente 320 gigabytes lo cual significa que en el mejor de los casos necesitaremos al menos tres horas. Podrían obtenerse mejores tiempos de copia, sin embargo, tendría que llevarse a cabo a través de una copia física cuyos costos son mucho más altos.

La solución mejor adaptada a los investigadores para no perder tiempos procesales importantes es una técnica comúnmente utilizada en el caso de las investigaciones llevadas a cabo en las empresas, las cuales permiten realizar simultáneamente los peritajes tanto en los documentos como en los sistemas informáticos.

Otra opción, en ausencia de un tercero auxiliando la investigación, sería realizar una búsqueda utilizando un CD en vivo que protege el disco

duro de la computadora contra cualquier cambio. Por lo general, es una distribución, a menudo GNU / Linux en CD-ROM que se carga en la memoria RAM y permite analizar los datos de la computadora de una persona sospechosa, sin hacer cambios, y también recuperar datos remotos para ser copiados en un medio extraíble.

V. El problema del lugar de almacenamiento de los datos

El segundo problema deviene directamente de la naturaleza misma del funcionamiento de las redes y de la noción de territorialidad de los datos. De hecho, numerosos prestadores de servicios de Internet como Google, MSN o Yahoo, proponen aplicaciones de mensajería en la nube o lo que se conoce comúnmente como *Cloud Computing* por su nombre en inglés.

Las direcciones creadas por un internauta poseen una extensión con un nombre de dominio .fr, lo cual presume que al ser un servicio que se ofrece en el territorio francés, es la legislación francesa la que debería aplicarse, desgraciadamente no es así. En efecto, es el derecho del Estado donde los datos residen, el que se aplica, aun cuando sea un servicio en lengua francesa, con un nombre de dominio de la región y destinado principalmente a usuarios de la misma.[17]

Esta circunstancia complica enormemente el trabajo del investigador, desde que simplemente consulta una bandeja de entrada de correo electrónico, ya que nunca sabe en qué país realmente está alojada la información. La sola indicación de la dirección IP del país donde se encuentra almacenada la información, es ya una advertencia a la vista, antes de bajar o abrir un correo en los servicios que así lo permiten, como Yahoo o Hotmail. Por el contrario, para Gmail, no existe ningún indicador de la implantación del servidor de descarga.

De hecho, para los Webmails Yahoo y Hotmail, una vez que el investigador desee acceder a la información contenida en la mensajería de un tercero en su presencia, en el marco de una medida precautoria, él obtendrá información relativa a la dirección IP del servidor, pero únicamente del archivo adjunto.

Esta información no está disponible en simple lectura del correo, por lo tanto, es necesario recurrir a una investigación del tipo "rastreo de ruta"

[17] Para conocer las reglas aplicables a los derechos sobre un nombre de dominio .fr, http://www.afnic.fr/medias/documents/Presentation_AFNIC_atelier_18_octobre_2011.pdf, consultado el 15 de octubre de 2014.

para intentar localizar el sitio de implantación geográfica del servidor en cuestión y verificar los eventuales criterios de competencia en cuanto a la territorialidad y, sobre todo, la aplicación de la Convención de Budapest.

Por lo tanto, podríamos pensar que esta cuestión regulada en la propia convención, en su artículo 32, relativo al acceso transfronterizo de datos almacenados, ya sea con consentimiento o cuando son accesibles al público, dispone:

> Que una parte, puede sin la autorización de la otra:
>
> a) Acceder a los datos accesibles al público (fuente pública), sin importar la localización geográfica de los datos; o
> b) Acceder o recibir a través de un sistema informático, situado en su territorio, datos informáticos almacenados o situados en algún otro Estado, si la parte obtiene el consentimiento legal y voluntario de la persona legalmente autorizada a divulgar estos datos por ese medio.

Sin embargo, en el primer caso se puede dar el valor de una declaración por parte del experto; en el segundo caso, ya que el hecho de que el acceso a los datos de un correo electrónico no provienen de una fuente abierta, sino de un entorno privado, por lo tanto requiere, como se estipula en el artículo 32 de la Convención, "el consentimiento legal y voluntario de la persona".

En el caso de una investigación preliminar, es necesario recabar el consentimiento expreso y por escrito en la forma prevista por la ley. La única manera de acceder a los datos sin este consentimiento es obtener una autorización expedida por el juez. Sin embargo, esta disposición sólo es aplicable a los delitos punibles con más de cinco años de prisión.[18]

La redacción de este acuerdo tiene su base desde hace más de cien años en el artículo 127 del Decreto Orgánico del 20 de mayo 1903 por el que se establecen normas relativas a la organización y el servicio de la policía. Aunque este decreto fue derogado por la Ley núm. 2009-971,[19] del 3 de agosto de 2009, su formulación es una práctica o un uso y costumbre, ya que no aparece textualmente en ninguno de los artículos del Código de Procedimientos Penales. Está formulado de la siguiente manera: "Sabiendo que me puedo oponer a la perquisición, consiento expresamente que se lleve

[18] *Ibidem*, p. 4.

[19] Referencia retomada de forma no textual en la Ley 2009-971, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020954146&dateTexte=&categorieLien=id, consultado el 20 de octubre de 2014.

a cabo, así como la incautación que considere de utilidad para la investigación".

Anteriormente, este consentimiento únicamente aplicaba a bienes inmobiliarios, ya que su campo de aplicación se precisaba en el mismo artículo de la siguiente manera: "Ninguna investigación, visita o decomiso, podrá hacerse sin el consentimiento libre, expreso y en conocimiento de causa, de la persona en cuestión".

Esto se ha adaptado en función de las circunstancias para ser admisible en una gran cantidad de situaciones. Se trata simplemente de poner en evidencia que la persona implicada puede oponerse a dichas operaciones, únicamente precisando la causa de la investigación. Podrá ser reformulada siempre y cuando no se viole su esencia.

A este efecto, según las reglas procesales, generalmente debe precisarse el domicilio, en el cuerpo de un proceso verbal. Cada descubrimiento de evidencia debe ser objeto de una mención precisa acerca de sus características y del lugar donde fue encontrado; esto implica que en el caso de un peritaje informático debe mencionarse, entre otras cosas, la dirección de correo electrónico de la que se trate, el espacio o lugar donde se encuentra alojado, precisar la dirección IP ligada a los elementos descargables para verificar la ley aplicable.

Los datos no tangibles no pueden ser percibidos físicamente, pero al ser extraídos del servidor, gracias a la interface del correo electrónico en el que se encuentran en vista de ser copiados en un soporte extraíble, el cual será objeto de una copia de seguridad cifrada, podremos convertir al soporte en un bien tangible.

La manifestación del consentimiento expreso, la identidad de la persona propietaria de la dirección de correo, la dirección incriminada, así como el del servidor, deberán adjuntarse.

Ahora bien, la segunda dificultad es la limitación de los poderes coercitivos del oficial de policía, quien, en el caso de una indagación realizada en un domicilio, se encuentra facultado para llevarla a cabo sin necesidad de consentimiento expreso; no es así en el de la búsqueda de evidencia a distancia, la cual opera desde un Estado firmante de la convención Budapest, es obligatorio obtener el consentimiento expreso de la persona titular del sistema informático, únicamente los datos que residan en Francia se encuentran exonerados.

La particularidad de este proceso es que el investigador realiza la perquisición y luego solicita la autorización para acceder a los datos, luego

entonces, esta disposición se encuentra en clara contradicción del derecho francés[20] en sí mismo.

En todo caso, la redacción de un proceso verbal de investigación debe ser lo más precisa posible, sobre todo en materia de datos informáticos, para constatar que el conjunto de obligaciones legales impuestas por el artículo 57-1 del Código de Procedimientos Penales han sido respetadas y, desde luego, los acuerdos internacionales.

VI. Bibliografía

ARPAGIAN, Nicolas, *La cybersecurité*, París, PUF, 2010.

BENSOUSSAN, Alain, *Atteinte aux systèmes d'informations*, recuperado de www.alain-bensoussan.com, 20 de octubre de 2014.

FILIOL, E. y RICHARD, F., *Cybercriminalité*, París, Dunod, 2006.

GIROT, Jean-Luc, *Le harcèlement numérique*, París, Dalloz, 2005.

LAGANE, Christophe, *Les abonnements Internet se tassent en France*, recuperado de www.silicon.fr, 20 de octubre de 2014.

LIRA, Óscar, *Cibercriminalidad, fundamentos de investigación en México*, México, Inacipe, 2010.

Panorama de la cybercriminalité XE "cybercriminalité", en 2010, recuperado de CLUSIF, http://www.clusif.asso.fr, 20 de octubre de 2014.

[20] En el marco de los fundamentos y principios del derecho francés, entre ellos, el de presunción de inocencia en un proceso penal, http://www.justice.gouv.fr/organisation-de-la-justice-10031/les-fondements-et-principes-10032/le-droit-a-un-proces-equitable-10027.html, consultado el 20 de octubre de 2014.