Terrorismo por Computadora

JULIO TÉLLEZ VALDÉS
Doctor en Informática Jurídica y Derecho de la Informática
Miembro del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (UNAM).

Resumen

En estas breves, pero esperamos substanciosas líneas, resaltaremos la noción "Terrorismo por Computadora", la cual rebasa los elementos técnicos y económicos, convirtiendo en menester un estudio integral de carácter multidisciplinario, bajo una perspectiva eminentemente social (finalmente es un problema específico que atañe de manera cada vez más directa a la sociedad) tomando en cuenta, de igual forma los insoslayables factores políticos, étnicos, históricos, religiosos, etc. , a través de una reglamentación jurídica confiable.

Se alude de igual forma a los principales problemas provocados por dicho fenómeno tanto a nivel personal; material como inmaterial.

Es una cuestión directamente vinculada a aquella relativa a la seguridad informática y a los riesgos informáticos, tratándose de una formulación fundamentalmente enunciativa y no tanto propositiva, con un punto de vista breve, pero realista de dichas implicaciones, con el afán de recordarnos que, sin el

control necesario, el uso de las computadoras puede convertirse en un factor de autodestrucción en detrimento del desarrollo del hombre.

Introducción

El terrorismo, bajo cualquier forma u objetivo es condenable, y si bien debe prevalecer en todo momento el respeto a las ideas, antes que nada, y por una gradación jerárquica incuestionable, debe haber respeto a la integridad y a la dignidad de las personas y más aún si éstas no tienen relación alguna con los propósitos del atentado, desgraciadamente, el terrorismo como muchas manifestaciones del individuo, rebasan el "status convencional" para llegar a nuevos niveles más sofisticados y por ende más destructivos, permitiendo entrever el principio, pero nunca jamás el final...

Nuevas formas de Terrorismo

Infortunadamente, el terrorista con ese afán "incansable" de hacer cada ves más notorios sus atentados, no escatima en emplear nuevos métodos, que entre más estragos causen más fenómeno de recurrencia presentan. A este respecto que "mejor" que el avance científico y técnico para fortalecer la consecución más rápida y efectiva de esos tan "particulares" ideales (¿la Ciencia y la Tecnología al servicio del hombre?)

Así tenemos, a falta de recursos para el desarrollo de bombas atómicas, la acentuada proliferación de las llamadas armas químicas, o el empleo de armamento sofisticado por parte de los terroristas, que no conformes con ello han comenzado a dirigir su atención hacia las computadoras, como instrumentos de terror o en su caso a identificar aquellos objetivos informáticos para realizar sus atentados.

Principales Características

Desde luego que estos nuevos ilícitos dificultan la elaboración de un perfil completo de dichas manifestaciones, sin embargo, aprovechando los diversos estudios que respecto a los llamados "delitos informáticos" y el terrorismo en particular se han elaborado en fecha reciente, podemos decir que algunas de las características más significativas de esta forma de delincuencia son las siguientes:

a) Podemos considerarlos como delitos de "cuello blanco". Esto en cuanto al necesario conocimiento y manejo de elementos técnicos fundamentales que se requieren para poder cometer este tipo de ilícitos y que

desde luego (al menos en la actualidad) no cualquier persona domina. Cabe mencionar, que algunos doctrinarios consideran que la delincuencia de cuello blanco fundamentalmente es cometida por servidores públicos de alto rango, quienes valiéndose de su situación preponderante por el carácter de su puesto, obtienen "beneficios" sustanciosos que contrarían los intereses de la comunidad. Sobre esto, considero que es inadecuado el encuadramiento, y quienes deben estar considerados dentro de este singular tipo de delincuencia, son aquellos que por razones heurísticas, disponen del conocimiento y la experiencia científica y/o técnica suficiente para cometer el ilícito, no importando mucho el nivel o puesto que ocupen (la mayoría de las ocasiones, los terroristas son "desempleados").

b) Ofrecen facilidades de tiempo y espacio. Ya que como sabemos, en muchos de los casos se requieren sólo milésimas de segundo para su consumación y no necesariamente implican la presencia física del (los) autor(es) a menos de que se trate de una ocupación o apoderamiento de un centro neurálgico de información "in sito" por parte de los terroristas. Lo cierto es que merced a la versatilidad que ofrece la informática y las telecomunicaciones en aquello que se conoce como teleinformática, es muy factible de poder realizar un atentado terrorista a "control remoto" (digamos de un país a otro) lo que desde luego incrementa los problemas de identificación de los autores y su eventual captura. Imaginemos (como ya ha sucedido) que algún terrorista "decida" realizar movimientos en el control informático del sistema estratégico de defensa (misiles o antimisiles) de algún país poderoso, evidentemente que todo ello puede desencadenar una conflagración mundial. Afortunadamente parece que se ha empezado a tomar conciencia de esta problemática por lo que se han redoblado los dispositivos de seguridad, pero sobre todo, se le da un lugar especial a la decisión humana en detrimento de aquella emanada de la máquina.

c) Otra característica es que pueden provocar serias pérdidas personales y materiales. Decíamos que ese afán de "llamar la atención" por parte de los terroristas los puede orillar a realizar atentados cada vez más temerarios, en donde el "uso" de la computadora puede generar resultados catastróficos y desde luego, aunque lo ideal es que no se presenten este tipo de ilícitos, en un momento dado es preferible que se presenten pérdidas materiales y no tanto humanas que como bien sabemos son de carácter irreparable.

d) Usualmente son difíciles de probar. Aquí tenemos una de las más acentuadas complicaciones que el uso de la informática provoca en el ámbito jurídico: el aspecto probatorio. En el caso de atentados terroristas en que se emplee la computadora como instrumento, y en base a lo

que hemos señalado anteriormente, podemos deducir el alto grado de dificultad para probar fehacientemente la autoría material (quizás en lo intelectual, en virtud de la reivindicación del atentado se pueda saber que grupo lo realizó) del hecho.

e) Sumamente sofisticados. Esto lo constatamos fundamentalmente en el ambiente militar, pero habida cuenta de que algunos grupos terroristas actúan con disciplina férrea al estilo de los militares y que justamente los objetivos militares son de los más "preciados", en este tipo de atentados, y claro está, la habilidad de los terroristas, así tenemos una delincuencia "sui generis" que excede con creces aquellos límites de lo "convencional".

Evidentemente y dentro de una necesaria tipología de esta clase de delito; diríamos que el sujeto activo es el terrorista, el sujeto pasivo, la persona física o moral que sufre las consecuencias directas o indirectas del atentado y el bien jurídico tutelado, la vida o patrimonio de las personas (recordemos que en este caso la información como un verdadero bien de carácter intangible con un contenido económico intrínseco que radica en la destinación de que puede ser objeto, adquiere matices muy significativos).

Clasificación

A continuación y siguiendo uno de los esquemas más habituales en lo que concierne a la clasificación del terrorismo, diríamos bajo una perspectiva informática lo siguiente:

a) Terrorismo de Estado. Es el caso de aquellos gobernantes de un Estado en que para poder seguir ejerciendo un control político sobre sus gobernados recurren al uso de la computadora como un factor de opresión (recordemos que la información es poder, y quien detente esto, está tentado a usarlo en su beneficio). A este respecto debemos distinguir a aquellos gobernantes de un Estado totalitario y a aquellos otros que aún bajo un régimen de democracia, recurren a este tipo de "estrategias" para un mejor "control de la ciudadanía". Algunos tratadistas consideran que en estricto sentido, esto no se trata de un terrorismo sino un "exceso de poder", lo cierto es que se requiere un contrapeso adecuado para que no se susciten abusos contra los ciudadanos y que instituciones como la Oficina de inspección de Datos en Suecia, el Comisario Federal de Datos en la RFA o la Comisión Nacional de Informática y Libertades (CNIL) en Francia, constituyen aquello que yo consideraría un adecuado control sobre el control.

b) Terrorismo entre Estados. En este caso tenemos al llamado Flujo de Datos Transfronterizo (PDT) en el que la teleinformática al servicio de los intereses de un determinado Estado puede propiciar verdaderos atentados en contra de la Soberanía de otros Estados a través del conocimiento y empleo indebido de datos o informaciones de carácter estratégico y confidencial. En esta tesitura, también tenemos a las eventuales ocupaciones físicas o destrucción parcial o total, de centros de información, tal y como si se tratara de un cuartel militar, una central nuclear o química. Como ha sido el caso fundamentalmente en el Medio Oriente.

c) Terrorismo entre particulares. Aunque para muchos tampoco constituye esto, un terrorismo propiamente dicho, sino actos de criminalidad en sentido lato, motivados por cuestiones de orden personal, histórico, económico o religioso, yo considero (espero que en forma no demasiado "aventurada") que el surgimiento de los llamados "virus informáticos" constituyen en algunas ocasiones (siempre que exista esa intención dolosa de cometer un daño) verdaderos atentados terroristas en contra del soporte material y/o lógico de las computadoras con la consecuente pérdida de la información (y por ende de dinero) y sobretodo caracterizado por generar aún más perjuicios de los que originalmente se pretendían provocar (incluso, porque no, hasta pérdidas humanas) en aquello en que la doctrina penal ha tenido a bien en considerar como verdaderos delitos "praeterintencionales".

d) Terrorismo de particulares hacia el Estado. Sin lugar a dudas, que esta manifestación de terrorismo es la mas conocida en la actualidad realizada por grupos anárquicos de izquierda, de derecha, fanáticos religiosos, ecologistas, etc. y que generalmente provocan estragos a nivel de vidas humanas y pérdidas materiales. Pensemos en una intrusión física o automatizada a algún centro informático o la inserción de virus informáticos, la planeación o simulación de atentados a través de una computadora a fin de "perfeccionar" el "verdadero" ataque, el apoderamiento de información confidencial (cintas, discos magnéticos o toma de cualquier otro soporte material de información) o la comisión de robos o fraudes u la informática para obtención de fondos que "sufraguen" sus actividades, etc. ¿Qué acaso grupos tales como el ERI, ETA, Sendero Luminoso, Brigadas Rojas, Acción Directa, Ejército Rojo, Tamiles, Sijs, Kurdos, grupos neonazis, etc. si se les presenta la oportunidad de realizar cualquiera de estas conductas, no escatimarían en cometerlas! ¿Cuál puede ser entonces nuestro destino? En fin, solo el tiempo lo dirá.

Formas de Control

Aquí debemos distinguir a los elementos extrajurídicos y los jurídicos propiamente dichos:

a) Extrajurídicos: en este caso tenemos el reforzamiento de la seguridad informática en los centros de cómputo estatales y particulares; riguroso examen psicosométrico a personas que pretendan ocupar puestos estratégicos en el área de informática a fin de conocer si no se trata de potenciales terroristas o delincuentes, severo control en el acceso a centros informáticos o sistemas de cómputo (en este caso, a través de un continuo cambio en las claves de acceso "passwords") , en fin, no escatimar en recurrir a todo tipo de dispositivo técnico, administrativo, psicológico, ético o científico respetando siempre los derechos humanos) a fin de impedir o en su caso mitigar los efectos de cualquier eventual atentado terrorista.

b) Jurídicos: desde luego, la incorporación de nuevos tipos en la legislación penal no sólo a nivel nacional sino también a nivel internacional, introduciendo figuras como la de los "delitos informáticos" teniendo al terrorismo por computadora como una de sus modalidades ya que si seguimos recurriendo a figuras análogas (de por si prohibido en el ámbito penal) los efectos positivos a nivel preventivo y correctivo que puede propiciar una regulación jurídica específica, estarán al margen de una realidad cada vez más frecuente.

Es importante asimismo, desarrollar atingentemente una teoría del riesgo informático (desde luego ocupándose de los efectos provocados por el terrorismo). Todo ello a fin de emitir adecuadas pólizas de aseguramiento que brinden un marco de protección accesorio a la comisión de este tipo de ilícitos, aún con sus obvias limitantes como la imposibilidad evidente de restituir una vida humana.

Consideraciones finales

Es incuestionable el hecho de que el problema del terrorismo viene provocando cada vez más interés de parte de la mayoría de los paises de la comunidad internacional.

El destino o rumbo no está equivocado, sin embargo, el camino y celeridad conque se trabaja quizás no sea el más idóneo, los devastadores resultados que podemos esperar de un empleo inadecuado de los avances científicos y técnicos (aquí sólo hablamos de las computadoras) por parte de los grupos terroristas constituye (o debe constituir) un factor de honda preocupación, y en

este caso los juristas, sin ser desde luego la panacea, tenemos mucho por realizar ya que Convenciones Internacionales Antiterroristas como las de Viena, Ginebra, La Haya, Washington, Estrasburgo, Tokio, Montreal, etc. resultan infortunadamente insuficientes hoy en día, por lo que la actualización continua se convierte más que nunca en imperioso menester.