

## Derecho y nuevas tecnologías (I)

**Por Gustavo Sain**  
@grsain

Con la incursión de la informática en la vida cotidiana de las personas, el Derecho tuvo que adaptar su teoría no sólo para la protección de la información y los dispositivos sino para el mejoramiento de procesos jurídico-administrativos. Para este último caso se creó una nueva área, la *informática jurídica*, donde la tecnología es puesta al servicio del Derecho. La misma se divide en Informática Jurídica Documental, orientada a la compilación y búsqueda de documentos jurídicos; Informática Jurídica Administrativa o de Gestión, concebida como ayuda a los procesos jurídico-administrativos tradicionales; y la Informática Jurídica Decisiva, que busca suplantar decisiones humanas mediante el uso de programas automatizados de software. En cuanto a la informática como objeto de estudio, es a través del *Derecho Informático* o *Derecho de Alta Tecnología* es donde se aplica las reglas jurídicas con los problemas vinculados con la tecnología. Dentro de este campo existe un área relacionada con el derecho penal, que consiste en el estudio de aquellos delitos donde la informática desempeña un papel condicionante, tanto como medio para la comisión de un ilícito. Así, estos tipos de ilícitos son entendidos como delitos informáticos, delitos de alta tecnología o delitos cibernéticos, entre otros.

Desde la incorporación de mecanismos electrónicos en la vida cotidiana, muchos países comenzaron a modernizar su legislación de acuerdo a las nuevas modalidades ilícitas. Algunos países incorporaron los delitos informáticos a su normativa mediante la promulgación de leyes específicas en el área, mientras que otros modificaron su legislación para incorporar nuevas figuras que incluyan a la información como un bien

jurídico a proteger. Otros, sin embargo, trataron de aplicar los tipos penales convencionales para la protección de la misma, como por ejemplo los delitos contra la propiedad, cuando el bien afectado eran las computadoras personales; o los delitos contra la intimidad, para el caso de la interceptación del correo electrónico como correspondencia personal. En este caso se presenta el problema de que a medida que evoluciona la tecnología, las figuras penales tradicionales de los antiguos códigos no alcanzan para ser cubiertas por las mismas. En este caso, resulta fundamental realizar un estudio particular sobre el tipo de bien o interés lesionado para adecuar la normativa o promulgar una nueva legislación específica.

Cabe señalar, resulta apropiado que las leyes penales establezcan diferenciaciones conceptuales de las expresiones “uso abusivo de computadoras”, “uso indebido de computadoras” y “delitos informáticos”, aunque en algunos documentos de referencia se los utilice como sinónimos. Existen usos abusivos de dispositivos informáticos que se producen en forma accidental, negligente y en forma deliberada y/o no autorizada, que en este último caso implica un uso indebido. De la misma manera se debe hacer una distinción de lo que no es ético y no es legal, es decir, la diferenciación entre una conducta vinculada con cuestiones reñidas con la moral pero lícita; y otras que constituye una conducta lisa y llanamente ilegal. Por último, el establecimiento de medidas sancionatorias -sean de tipo penal, administrativa, civil o comercial- debe ser proporcional al hecho que se ha cometido.

Los delitos en los que intervienen dispositivos informáticos -sea como blanco del delito o como fin para cometerlos- presentan algunas características diferenciales en relación a otros delitos. En primer lugar la *transnacionalidad*, a partir de la posibilidad de su comisión a distancia desde cualquier parte del mundo si el mismo involucra a la

red Internet; las *dificultades probatorias* en función de la fragilidad de la evidencia digital y volatilidad de los rastros del crimen; su *atemporalidad*, ante la posibilidad de programar su ejecución automática para determinada fecha y hora –para el caso de los virus-, el *anonimato* que permite determinados entornos virtuales a partir de la construcción de identidades ficticias en la red; y la *inadecuación legal* de determinadas conductas ilícitas a las normas penales vigentes, entre otros. A su vez, el delito informático tiene una importante *cifra oculta* en cuanto –salvo excepciones- no son conductas que llegan a la justicia habitualmente. Asimismo de la cantidad de hechos denunciados un porcentaje muy ínfimo tiene resolución penal en términos de identificación de los responsables. Existen varios factores que explican este fenómeno: *la velocidad y complejidad* de funcionamiento de las tecnologías modernas hacen que sean difíciles de descubrir, los investigadores *carecen de pericia suficiente* para encarar el proceso de examen y por último *el desconocimiento* de las víctimas de que fueron víctima de un delito informático, entre otros factores.

Para el jurista alemán Ulrich Sieber, el proceso de reformas legislativas en materia de delitos informáticos se inicia a partir la década del 70 en Occidente, con el objeto de proteger la privacidad de los datos a partir de las nuevas formas de recogida, almacenamiento y transmisión de los mismos a través de sistemas informáticos. Países como Suecia en 1973, Estados Unidos en 1974 y Alemania en 1977 incorporaron figuras en sus normativas orientadas en este sentido. La segunda oleada comienza en los 80s con la protección que establecen los países europeos de bienes inmateriales frente a la aparición de dinero electrónico, proceso que iniciado por los Estados Unidos en 1978. El tercer campo de reformas se relaciona con la protección de la propiedad intelectual, donde diversos países establecieron reformas a las leyes de patentes promulgadas durante los años 70s para evitar la reproducción y venta no autorizada de obras digitales. En este sentido, países como Estados Unidos (1984),

Japón (1985) y Suecia (1986), entre otros, establecieron legislaciones específicas para la protección de obras en semiconductores y chips. La cuarta tendencia reformista se relaciona con los contenidos ilícitos y nocivos tales como la difusión de pornografía infantil, la llamada incitación al odio o la difamación. Mediante la adaptación de las leyes tradicionales a las nuevas tecnologías, Gran Bretaña en 1994 y Alemania en 1997 iniciaron el proceso, tanto así como el establecimiento de responsabilidad de los proveedores de servicio y acceso a Internet sobre el material publicado, en Estados Unidos 1996 y Alemania 1997. La última oleada de reforma se dio en materia de derecho procesal penal iniciado en Australia en 1971. Gran Bretaña en 1984, Dinamarca en 1985 y Estados Unidos 1986, entre otros.