Reeditor.com
RED DE PUBLICACIÓN Y OPINIÓN PROFESIONAL

José Manuel López García
Profesor de Filosofía

Delincuencia electrónica

Ciudadanía, 23/04/2020

El trabajo telemático y la formación digital o a distancia han abierto ya desde hace años unas posibilidades realmente inmensas para el desarrollo de una vida cada vez más independiente de los condicionantes de espacio y tiempo. Lo presencial sigue siendo también fundamental, por razones obvias.

Las condiciones de seguridad digital tienen que ser más fuertes o potentes de modo general. Y las estrategias de encriptado o de cifrado también. Se puede poner un ejemplo, entre muchos. La seguridad de Twitter tiene que mejorar considerablemente. Debería haber números de teléfono de atención al cliente gratuitos o de muy bajo coste y que resuelvan de modo inmediato las actos de piratería en las cuentas y el robo de contraseñas, etc.

El hackeo o pirateo de cuentas es una actividad delictiva y una de las formas de pararla es poniendo a disposición de los usuarios de Twitter herramientas de resolución efectivas y sobre todo ágiles y rápidas, lo que no puede ser es una espera de meses para que se resuelvan los hackeos de cuentas de usuarios de Twitter y se descubra a los causantes. En los tiempos telemáticos que vivimos no es lógico. Los errores y la pérdida de datos personales en Internet han sucedido en determinadas compañías o redes sociales repetidas veces.

El aumento de los delitos informáticos o de los ciberdelitos se está notando debido, en buena medida, al aumento del número de personas con acceso a Internet. También es cierto que la inmensa mayoría de la gente realiza un uso adecuado de los dispositivos electrónicos y que son un medio de trabajo y de formación, comunicación y ocio excelente.

Los delincuentes han ampliado su campo de actividad y están incrementándose exponencialmente los delitos y las amenazas a la seguridad. Es cierto, por otra parte, que las fuerzas de seguridad se encargan también de investigar y perseguir a la ciberdelincuencia y se emplean a fondo, pero no debe ser tarea fácil aunque dispongan de los mejores medios.

Se producen delitos digitales contra la identidad, la propiedad y la seguridad de las personas, empresas e instituciones. Existe también una unidad de delitos telemáticos en España que lucha contra el ciberdelito. Pero existen más amenazas a la seguridad. Por ejemplo, en algunas aplicaciones de videollamadas los ciberdelincuentes intentan robar contraseñas para entrar en los datos personales. Los expertos aconsejan descargarlas desde fuentes oficiales y evitar Wi-Fis públicas para impedir intrusiones indeseadas en las videoconferencias. También recomiendan la utilización de las aplicaciones más seguras.

Lo que sucede es que, a mi juicio, existe el azar y una casuística extremadamente extensa y los riesgos pueden ser muy diversos y variados, si se parte de la base de que la seguridad absoluta no existe. Lo que está claro es que el refuerzo continuo de los elementos o mecanismos de seguridad en el entorno digital en el que se convive es algo absolutamente necesario.

Esperemos que con la llegada del 5G se pueda luchar con mucha mayor rapidez y efectividad contra este tipo de prácticas delictivas. Actualmente, la informatización de los bancos, por ejemplo, y sus sistemas de seguridad suelen ser muy fuertes, pero esto no quiere decir que sea imposible que pueda haber errores o delitos contra la propiedad o abusos y fraudes económicos. La delincuencia económica existe y se persigue por la policía y la magnitud de la tarea investigadora debe ser colosal.

El derecho a la privacidad y al honor y la buena imagen está amparado por los textos constitucionales y los derechos humanos,

pero ante el aumento increíble del número de aparatos digitales que ya es de miles de millones parece que se deben dedicar más medios económicos y más tecnología e investigadores para impedir la ciberdelincuencia y perseguirla.

Con el 5G puede ser que 75.000 millones de aparatos tecnológicos estén conectados a los móviles de los que viven en nuestro planeta en los próximos años. Los problemas de seguridad pueden ser aún mayores, pero se contará con los superordenadores cuánticos y con una latencia muy reducida del orden del milisegundo en los móviles. La latencia llegará con el 6G dentro de unos diez años a los 10 microsegundos o millonésimas de segundo. Esto proporcionará una potencia y una velocidad descomunal a todos los sistemas de conexión digital. De todas formas, está claro que las inmensas ventajas que ofrece el mundo digital en el que vivimos son incuestionables en todos los sentidos.