## GLOSARIO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD): Ente público independiente cuya finalidad principal es velar por el cumplimiento de la legislación española sobre protección de datos personales.

ALESSANDRO ACQUISTI: economista especializado en privacidad, se ha dedicado al estudio de las redes sociales y al comportamiento del consumidor. Para ello, utiliza como marco teórico la economía conductual. A través de experimentos es capaz de llegar a algunas conclusiones interesantes acerca de la actitud del consumidor hacia la privacidad.

AUTODETERMINACIÓN INFORMATIVA: es la facultad de toda persona a ejercer el control sobre sus datos personales. Piensa por ejemplo en la información que tiene Facebook sobre ti y que puede que ya está fuera de tu control. En España, eso se garantiza a través de la Ley Orgánica de Protección de Datos de carácter personal (LOPD) y la Agencia Española de Protección de Datos es el organismo que vela porque se garanticen tus derechos en esta materia.

DATO PERSONAL: es cualquier información que puede ser vinculada a una persona concreta. Un ejemplo es el nombre, la fecha de nacimiento, la religión. El cambio tecnológico y las avanzadas técnicas de big data pueden hacer posible que incluso con la ropa que llevamos puesta demos indicios sobre nuestra vida privada por eso el concepto de dato personal no es estático.

BIG DATA: son datos que cumplen tres características —las llamadas tres Vs—. Por un lado, hablamos de grandes Volúmenes de información. Por otro, de Velocidad, el ritmo al que generamos información es apabullante, piensa en la cantidad de datos que subimos a las redes sociales. Y, por último, debemos destacar la Variedad. Hablamos, de fotos, de tweets, correos electrónicos, mensajes de voz, de texto. Procesar todo esto y obtener una historia creíble es tarea del big data. La privacidad es justamente una de los grandes desafíos que tiene que enfrentar.

DERECHO AL ACCESO: permite al ciudadano conocer qué datos tienen de él las instituciones tanto públicas como privadas. Para ejercerlo hay que ir primero a la empresa u organismo que el ciudadano considere y si en un plazo de un mes no obtiene respuesta puede reclamar la tutela de derechos por parte de AEPD, que será la encargada de ejercer ese derecho en nombre del ciudadano.

DERECHO DE CANCELACIÓN: El derecho de cancelación es uno de los derechos de la Ley Orgánica de Protección de Datos de carácter personal (LOPD) y permite que nuestros datos se supriman de ficheros cuando resulten inadecuados o excesivos. Como todo derecho ARCO, debe ejercerse en primer lugar en el organismo correspondiente y si en diez días no hay respuesta se podrá pedir la tutela de derechos a la AEPD. Recuerda, aunque el organismo no tenga datos tuyos, tiene obligación de responder.

DERECHO A LA INFORMACIÓN: Es uno de los derechos básicos y principales contenidos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Si van a recopilar tus datos personales, te tienen que avisar con carácter previo de forma clara y precisa, así de como los medios por los que lo harán.

DERECHOS ARCO: son el conjunto de derechos que permite a los ciudadanos controlar sus datos personales. Estos derechos (acceso, rectificación, cancelación y oposición) constituyen una herramienta a través de los cuales la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (Lopd) se ocupa de garantizar que podamos controlar nuestros datos.

DERECHO AL OLVIDO: es el derecho de cancelación y oposición aplicado a Internet. Es decir, que si hay información tuya, que aunque sea verídica, se haya quedado obsoleta, puedes pedir que la quiten. Debes ejercer tu derecho directamente al motor de búsqueda y en caso de que no te hagan caso, puedes acudir a la AEPD para que tutele tu derecho.

DERECHO DE OPOSICIÓN: es el derecho que tienen los ciudadanos a que no se recopilen sus datos personales. Es uno de los derechos de la Ley Orgánica de Protección de Datos de carácter personal. Como todo derecho ARCO, debe ejercerse en primer lugar en el organismo correspondiente y si en diez días no hay respuesta se podrá pedir la tutela de derechos a la AEPD. Recuerda, aunque el organismo no tenga datos tuyos, tiene obligación de responder.

FISHING: es un fraude que consiste en enviar de forma masiva correos electrónicos o SMS pidiendo claves o información confidencial para supuestamente confirmar datos. Sin embargo, el propósito es obtener claves de acceso para acceder a las cuentas de los usuarios.

HAPPY SLAPPING: la práctica surge en el Reino Unido entre adolescentes. Es el ataque físico o verbal sobre una persona mientras otro lo graba, normalmente con un teléfono móvil. En este caso, la difusión de las imágenes (y la consiguiente violación de su intimidad) es un medio más para hacer daño.

INFORMACIÓN ASIMÉTRICA: es una característica específica de algunos mercados, como puede ser el de los datos personales. Vendedores y compradores no tienen la misma información acerca de un bien, en este caso el dato personal. Los vendedores de datos personales no saben cuánto vale su información ni adónde va a parar. Esto provoca grandes desequilibrios y consecuencias inesperadas para el vendedor.

INFORMATIONAL PRIVACY: ver autodeterminación informativa.

LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: es la ley que recoge una serie de derechos fundamentales en relación a la protección de datos. Entre ellos los llamados derechos ARCO.

ONLINE CHILD GROOMING: es la conducta que realiza un adulto para acercarse y ganarse la confianza del menor para luego exigir, normalmente, favores sexuales. La falta de cultura en el control de los propios datos puede llevar a un niño a dar más información de la que debiera.

PRIVACIDAD: según la RAE es el ámbito de la vida privada que se tiene derecho a proteger. La extensión de ese ámbito ha cambiado a lo largo de los años conforme lo ha hecho el cambio tecnológico. Un estudio más sistemático del asunto se hizo a raíz del surgimiento del término “informational privacy” de la mano de Warren y Brandeis.

RANSONWARE: es un delito que consiste en el robo de tus archivos. Los ciberdelincuentes secuestran la información que tienes en tu ordenador y piden un rescate.

SEXTING: es el envío de imágenes de contenido sexual entre jóvenes. Esta práctica conlleva numerosos riegos, en especial, cuando se no se tiene control sobre la difusión que tendrán esas imágenes. En España, aunque hayas dado consentimiento para enviar esa imagen a tu destinatario eso no le da derecho a difundirla sin tu aprobación, si lo hace, estará cometiendo un delito contra la intimidad (revelación de secretos).

TECNOLOGÍA DE LA INFORMACIÓN: hace referencia a sistemas avanzados para procesar y almacenar grandes volúmenes de información. La capacidad de esta tecnología se ha acrecentado rápidamente en las últimas décadas haciendo posible de forma rápida y barata el acceso a grandes cantidades de información que, en muchos casos, contienen datos personales. Esto plantea nuevos desafíos en términos de privacidad y puede suponer nuevos peligros. Piensa en la posibilidad que tiene alguien a quien no le caes muy bien de que te encuentre gracias a Internet.

TUTELA DE DERECHO: es lo que hace la AEPD cuando un organismo no ha respondido un pedido de un ciudadano en lo que a ejercicio de los derechos ARCO se refiere. La Agencia reclama en nombre del ciudadano pero éste debe acudir primero al organismo y una vez que no haya respuesta puede dirigirse a la Agencia.

VIGILANCIA: puede ser entendida como la atención sistemática, rutinaria y enfocada en los detalles personales de alguien concreto. El big data intensifica esta práctica y resulta crucial al brindar herramientas tecnológicas que facilitan el control de determinados individuos. En parte, gracias a Edward Snowden hemos sabido que las empresas tecnológicas facilitan información a los gobiernos para controlar a los usuarios. Los usuarios de empresas como Google supieron en 2006 que había facilitado información a la Administración de Bush. Aunque parezca que tu información es inocua y que no tienes nada que esconder nunca sabes quién va a analizar esa información y con qué propósito. Puede ser que estés investigando el mercado de la marihuana en tu país y que alguien llegue a la conclusión de que, por tu historial de Internet, te dedicas a la venta de maría. Por otra parte, el control masivo por parte de gobiernos puede hacer que sus ciudadanos dejen de sentirse cómodos a la hora de expresarse. ¿Realmente criticarías al gobierno de turno si supieras que hay alguien viendo tus correos o sabiendo que tus opiniones pueden influir a la hora de, por ejemplo, encontrar un trabajo?

WARREN Y BRANDEIS: autores del célebre paper “The right to privacy”(1890) considerado el ensayo fundacional sobre el derecho a la privacidad. El articulo pone de manifiesto, entre otras cosas, cómo el cambio tecnológico, en este caso la aparición de la cámara fotográfica, posibilitó nuevas formas de invasión a la privacidad hasta el momento inexistentes.

## Fuentes consultadas y que puedes consultar tú para ampliar esta información

Amnistía Internacional <https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/>

AEPD <https://www.agpd.es/portalwebAGPD/index-ides-idphp.php>

No more ransom <https://www.nomoreransom.org/>

Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/privacy/>

Juan, I. M. (2016). Cibercriminalidad social juvenil: la cifra negra. *IDP. Revista de Internet, Derecho y Política*, (22).

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 2053951714541861.