Resolución del Ararteko de 23 de mayo de 2013, por la que se concluye la actuación de oficio iniciada en relación con la supuesta difusión no consentida de fotos y vídeos íntimos a través de Internet.

Antecedentes

1. A través de informaciones y noticias aparecidas en medios de comunicación y redes sociales durante los días 28 y siguientes del mes de noviembre de 2012, el Ararteko tuvo conocimiento de la supuesta difusión, no consentida, de fotos y vídeos íntimos de varias personas, aparentemente relacionadas con la Universidad de Deusto. Por razones de respeto a estas personas y a los derechos que les asisten, no vamos a reproducir los contenidos de las informaciones reseñadas.

2. Entendiendo que estos hechos pudieran ser susceptibles de conculcar derechos fundamentales de las personas afectadas, tales como el derecho a la intimidad, la dignidad, la integridad moral y el libre desarrollo de la personalidad y, en su caso, a la protección de datos personales, se consideró conveniente la apertura de un expediente previo de investigación, al objeto de conocer los hechos y aclarar lo sucedido y, en su caso, recomendar las actuaciones oportunas en defensa de los derechos de las personas que hubieran podido verse afectadas.

   Dicho expediente se ha tramitado como Expediente de oficio núm. 66/2012/45O.

3. En el curso del expediente se ha recopilado toda la información existente y se ha solicitado información al Vicerrectorado de Comunicación de la Universidad de Deusto, no considerándose adecuado realizar otras actuaciones, atendido que ya la propia Universidad había adoptado las iniciativas oportunas ante la Ertzaintza.

   En primer lugar debemos dejar constancia de la gran confusión existente en torno a los hechos, las personas que hubieran podido verse afectadas, sus edades e, incluso, a la circunstancia de que se trate efectivamente de estudiantes de la Universidad de Deusto.

   En efecto, según informaciones publicadas, en el curso de la investigación desarrollada por la Ertzaintza no se ha acreditado que se haya producido ningún robo de información entre las personas que acceden a la red informática inalámbrica de la Universidad de Deusto, pudiendo concluirse que no se aprecia actuación irregular por parte de este centro académico.

   Según dicha universidad, en el eventual caso – insistimos, no confirmado-, de que mediante la red WIFI de uso público (una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día), alguien

hubiera accedido a la información contenida en un dispositivo electrónico, esta situación solo habría sido posible en el caso de que su propietario o propietaria no hubiera adoptado las mínimas medidas de seguridad para evitar el acceso a dicho terminal.

4. Aún cuando la actividad de una entidad privada como la Universidad de Deusto (cuya colaboración agradecemos) no está sometida al control de la institución del Ararteko, y a pesar de que se constató la ausencia de denuncia de cualquier persona que hubiera podido verse afectada, y de haberse producido un resultado negativo en la investigación de la Ertzaintza, desde esta Institución no se consideró oportuno el cierre del expediente.

   Al contrario, la constante preocupación del Ararteko por la cada vez más frecuente aparición de este tipo de situaciones, especialmente cuando potencialmente pueden afectar a niños, adolescentes y jóvenes, así como la trascendencia de los derechos en riesgo y la alarma social generada, han determinado la conveniencia de profundizar en torno a la problemática suscitada.

   En atención a todo ello, el Ararteko ha considerado procedente emitir la presente resolución, que encuentra su fundamento en las siguientes:

Consideraciones

1. El mundo virtual tiene sus propias especificidades, no es como el físico, es viral y hay que conocer sus riesgos, que no son mayores, sino distintos.

   Hace escasas semanas la Vicepresidenta de la Comisión Europea Viviane Reding y el Secretario General del Consejo de Europa Thorbjorn Jagland en un comunicado conjunto difundido en el Foro Económico Mundial de Davos (Suiza), ya alertaron sobre estos riesgos y sobre la necesidad de adoptar las oportunas medidas para proteger la información personal. Recordaron que la protección de datos es un derecho fundamental y que la hiperconectividad tiene que ir de la mano de la protección de la privacidad en la red. La información tecnológica ofrece un potencial económico y social enorme, que se aprovechará plenamente si los ciudadanos tienen confianza en que su información personal en internet está protegida. Hay una cantidad ingente de información privada que se procesa en la red, con un flujo instantáneo y sin barreras, lo que propicia algunos peligros. Insisten, asimismo, que se precisa una mayor transparencia para garantizar que las personas usuarias estén informadas sobre lo que ocurre con sus datos y que puedan consentir o no su tratamiento.

   Más recientemente, las autoridades europeas de protección de datos -el denominado Grupo de Trabajo del Artículo 29- han aprobado el primer dictamen conjunto sobre la privacidad en las aplicaciones móviles, en el que se

analizan la incidencia y los riesgos que plantean para la protección de datos. En el mismo recuerdan la necesidad de obtener el consentimiento informado y previo del usuario para recoger y tratar sus datos personales.

A este respecto, debemos insistir en el hecho de que los usuarios y usuarias de internet no somos plenamente conscientes de que nuestros datos están siendo recogidos y almacenados. Aún así, el 72% de los usuarios de Internet en Europa están preocupados ante la excesiva cantidad de datos personales que se les solicita en línea (Eurobarómetro especial 359: Actitudes frente a la protección de datos y a la identidad electrónica en la Unión Europea, junio de 2011).

Esta realidad provoca una sensación de haber perdido el control sobre los datos personales, puesto que no se recibe información adecuada respecto del destino de ellos, a quién se transmiten y con qué fines y, en una gran mayoría de casos, no saben cómo ejercer sus derechos en línea. Como ejemplo gráfico, basta observar que cuando realizamos en el correo personal intercambios de emails a través de algunas de las cuentas más usuales en internet, aún disponiendo de medidas de seguridad aplicadas en el equipo (antivirus), se aprecia claramente que los espacios del contorno del correo se llenan de anuncios relacionados con la conversación que se esté llevando a cabo, o respecto a las fotografías incluidas en los mismos; lo que evidencia que los buscadores automáticos de contenidos y de términos, tags o metadatos están haciendo su trabajo de indexación por debajo de la conversación que se está desarrollando.

Una coyuntura que se explica con un ejemplo esclarecedor: «Uno no necesita identificarse para pasear por una ciudad o para comprar en una farmacia pagando en efectivo; sin embargo, para conectarse a Internet se requiere, por lo pronto, un identificador como la IP que permite rastrearnos y analizarnos».

El problema reside en un entorno digital extraordinariamente intrusivo por su propia naturaleza técnica. Cualquier contenido publicado en una página abierta es susceptible de ser localizado, indexado, copiado y enlazado por Google.

Por tanto, de una desacertada actitud respecto a la protección de nuestra intimidad e identidad, o de la utilización que terceros legítima o ilegítimamente hagan de ella, pueden derivarse consecuencias no previstas, deseadas o admitidas para el presente o para el futuro, en un momento en el que, salvo que el legislador español o europeo lo remedie, la falta de información y la desprotección es grande y las posibles acciones para remediarla, prácticamente estériles.

2. Breve reseña de la normativa más directamente aplicable a esta materia:

El **Artículo 18 de la Constitución Española** *garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen,* estableciendo en el apartado

4 de dicho precepto la previsión de la limitación legal del *uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.* Estos derechos de la personalidad originarios, son absolutos, irrenunciables e intransferibles, y deben ser objeto de la máxima protección.

Asimismo, la Directiva de la UE 95/46/CE, y las legislaciones nacionales sobre protección de datos, constituyen la estructura jurídica en materia de protección de datos. El problema de esta legislación, especialmente la comunitaria, es evidente: se encuentra totalmente desfasada por ser anterior a la eclosión del fenómeno internet, por lo que no se configura como instrumento real de protección de dichos derechos. Es conocida la previsión de que la necesaria reforma y actualización de esta normativa europea se abordará durante el presente año 2013.

3. Si las consideraciones que anteceden pueden aplicarse a los usos en internet de las personas en general, y, sin perjuicio de que el asunto del expediente no afecte a menores de edad, merece la pena detenernos especialmente en lo que atañe a los niños, niñas y adolescentes, en los que confluyen dos elementos aparentemente antagónicos: su condición de nativos digitales (con unas habilidades innatas para relacionarse con cualquier tipo de tecnología) y su mayor vulnerabilidad.

   La preocupación por el empoderamiento de los más jóvenes en la protección de su propia información y su imagen ha estado muy presente en el Ararteko desde hace años, como lo demuestra la edición ya en 2008 de diversos materiales didácticos: Ventanas,"*Una aventura real en un mundo virtual. Disfrutar de internet si caer en la red*" y Ciberbullying, material didáctico para la prevención del acoso por medio de las nuevas tecnologías. Más recientemente, se ha creado un apartado específico sobre el uso responsable de los medios electrónicos en la web la Isla de los derechos.

   En este tiempo y por lo que la experiencia nos ha demostrado, podemos decir que nuestros niños y niñas no son ajenos al gran potencial de las nuevas Tecnologías de la Información y la Comunicación, de igual manera que no lo son a sus riesgos. Como bien concluía el Consejo de la infancia y la adolescencia del Ararteko con ocasión de la elaboración del Informe extraordinario sobre e-inclusión y e-participación, al que posteriormente se hará referencia, *debemos hacer un uso seguro de Internet y las redes sociales. Google lo sabe todo y Facebook se relaciona con todo, pero también hay peligros*.

   Así pues, si la necesidad de salvaguardar los derechos de los niños y las niñas está clara, si somos conscientes de los riesgos inherentes al entorno virtual, será tarea de todas las instituciones concernidas proveerles de instrumentos adecuados para su protección, creando las condiciones para un uso seguro y responsable de internet. Existen ya iniciativas interesantes y buenas prácticas

relacionadas con este objetivo, entre las que destacaremos, por distintos motivos, la campaña educativa Kontuzdatos, promovida por la Agencia Vasca de Protección de Datos en colaboración con el Departamento de Educación, Universidades e Investigación del Gobierno vasco, las iniciativas contempladas en el marco de la Agenda Digital Euskadi 2015 aprobada por el Gobierno Vasco en julio de 2012 y el Safer Internet Programme 2009-2013 de la Comisión Europea, cuyo principal objetivo es promover el uso seguro de Internet por parte de la población joven, creando centros de referencia en ciberseguridad infantil en todo el territorio UE que lleven a cabo acciones de sensibilización y lucha contra los contenidos ilegales y las conductas inapropiadas.

En suma, por la especial protección que ha de prestarse a los y las menores de edad, las instituciones han apostado por trabajar en la concienciación e información sobre el impacto del uso no responsable de estos medios. Sin duda, habrá de continuarse con esta tarea preventiva, de la que pueden extraerse algunos aprendizajes interesantes para ser trasladados a iniciativas de prevención dirigidas a las personas adultas, que han sido escasamente impulsadas hasta la fecha.

Todos estos aspectos constituyen elementos sobre los que seguir reflexionando, a fin de equilibrar la protección y el efectivo ejercicio de los derechos de cada persona, con la increíble capacidad de la web social y los dispositivos móviles para proveernos de información, para facilitar la transparencia y el conocimiento y facilitar nuestra vida y nuestro trabajo.

En esta línea, el Ararteko considera adecuado aportar sus propias conclusiones:

Conclusiones

Primera: A consecuencia de los hechos que dieron origen al inicio del expediente, tanto desde el ámbito educativo, como, específicamente, desde la propia Universidad de Deusto, se ha insistido en la necesidad de incidir en la información dirigida tanto a los y las estudiantes, como al conjunto de la sociedad en torno a la privacidad y las condiciones de seguridad de sus dispositivos electrónicos, y de forma complementaria, en la creación de cauces para la reflexión sobre el uso ético y responsable de las redes sociales, a fin de fomentar el análisis crítico de la información accesible por dichas vías.

Esta institución, en cuanto coincidente con estos posicionamientos, no puede sino insistir en la articulación de iniciativas que permitan avanzar hacia estos objetivos.

Segunda: Déficit de regulación y definición adecuada del entorno digital.

Ya nadie discute que hemos pasado a movernos en un entorno digital que tiene sus propias reglas y requerimientos. Pocas personas son capaces de ejercer un control efectivo sobre su información personal; ni siquiera los nativos digitales con grandes habilidades intuitivas en el uso de la tecnología y del mundo internet pero, probablemente, sin la adecuada información sobre algunos de sus riesgos-, son capaces de hacerlo eficientemente en muchos casos.

Una de las situaciones más habituales y características de las posibles vulneraciones producidas en el mundo digital es la aparente falta de asignación de responsabilidades en los supuestos de usos indebidos: la responsabilidad es muy confusa y puede resultar diluida. Es como si se advirtiera una dificultad extrema para saber donde están fijados los límites y las responsabilidades, como si estuviéramos frente a un espacio de impunidad, donde es más difícil ejercer el control y la defensa de derechos.

Para proteger estos derechos ciudadanos de nueva generación, es urgente disponer de un **marco jurídico actualizado** (que trasciende el ámbito del País vasco) que regule esas diferentes responsabilidades, que incremente el control de la ciudadanía sobre sus datos y que permita vencer la gran dificultad existente para cancelar los datos personales.

Por tanto, es preciso que la legislación específica sobre esta materia, permita:

- Regular el derecho a la información de los datos propios y el acceso a los mismos.
- Exigir a las empresas proveedoras de servicios en internet que realizan almacenamiento y tratamiento de datos que informen sobre las condiciones en que se realizarán tales operaciones de forma explícita y clara, y se solicite consentimiento para ello.
- Regular adecuadamente el derecho al olvido (entendido como el derecho a la desaparición de internet de los datos e información de una persona concreta), de forma que el ciudadano o ciudadana sepa dónde dirigirse para retirar su consentimiento (de forma análoga a como se prevén en la LOPD los derechos de acceso, rectificación y de cancelación de datos personales).

Esta última cuestión constituye una preocupación especial del Ararteko, que confía en que la anunciada Sentencia del Tribunal de Justicia de la Unión Europea ante la cuestión prejudicial planteada por la Audiencia Nacional (relativa al alcance de ciertas normas de la Directiva 95/46/CE sobre protección de datos personales) que afecta también al alcance de ese derecho al olvido en internet, resuelva varios de los déficits apuntados, configurando el marco de garantías que dichos derechos personalísimos, requieren en la actualidad.

Tercera: Actitud proactiva e impulso de iniciativas desde las administraciones para el uso responsable y seguro de las TIC.

En paralelo a las actuaciones que procuren un marco jurídico actualizado, **las administraciones han de adoptar un rol muy activo** para favorecer la información, la transparencia y el control. Esto supone avanzar en distintos ámbitos, entre los que destacamos:

1. Potenciar la prevención, educando para la madurez digital y evitando prácticas de riesgo.

Como ya señalábamos, nos encontramos en un nuevo y complejo entorno digital cambiante de forma permanente, por lo que únicamente los usuarios muy avanzados y los especialistas son capaces de "seguir la pista" a todos los canales que van surgiendo y hacer un diagnóstico certero de los problemas que, a nivel de seguridad, puedan presentarse.

Entre tanto esa situación se corrige, y mientras las organizaciones superan las actuales políticas de privacidad, prolijas y poco efectivas, la mejor herramienta para lograr un **uso seguro y responsable de las TIC** es aprender a utilizar el sentido común. Del mismo modo que en el mundo físico no dejaríamos la puerta de la vivienda u oficina abierta, o la cámara de fotos para su uso compartido de quien lo desease, el mismo sentido común cabe ser aplicado a las conductas en el mundo digital.

Los y las internautas tenemos la responsabilidad intransferible de evitar la intrusión en nuestra vida privada mediante el control de nuestras opiniones, imágenes y archivos en los dispositivos que usemos, o en las redes que utilicemos para las conexiones a internet. En suma, responsabilizarnos de los contenidos que editamos, huyendo del error frecuente de ignorar que una vez salen fuera del ámbito de protección, se pierde el control sobre ellos.

Contra las prácticas inadecuadas, el único instrumento preventivo real es la información, por lo que proponemos la realización de Campañas de sensibilización e información. Es innegable que son importantes, sin ser suficientes, las iniciativas adoptadas en la materia respecto a los y las menores de edad; pero son escasísimas las orientadas a las personas adultas, en las que se da frecuentemente la circunstancia de carecer de una falta de competencia tecnológica suficiente.

Instrumentos como la ya citada Agenda Digital Euskadi 2015, en la medida en que ha de propiciar una ciudadanía corresponsable, o las Agendas digitales locales podrían ser de gran utilidad si dedicaran parte de su potencial al objetivo de información y socialización en torno al uso seguro y responsable para alcanzar el máximo potencial de internet. Al tiempo, sería útil aprovechar la capilaridad que ofrecen los *KZ Gunea* y añadir a su catálogo de oferta formativa módulos específicos sobre todas estas cuestiones.

2. Insistir en la responsabilidad y cuidado individual en el uso de la red.

Es una realidad que cada vez se hace un uso menos intensivo de la lectura de las instrucciones de uso de los dispositivos que utilizamos (si acaso únicamente la de aquellos que tienen una función de transacción económica), pero no puede obviarse que esa es nuestra primera obligación como usuarios responsables: leer las políticas de privacidad, configurar en nuestros sistemas y aplicaciones los mecanismos de seguridad recomendados, conocer las condiciones de uso, y las consecuencias de las decisiones que se derivan de ellas (no pasarlas como si no fueran importantes), para, responsablemente, decidir si las aceptamos o no.

En este contexto, no podemos dejar de lado que el supuesto que dio origen al presente expediente del Ararteko aparece relacionado con el uso de las Redes WIFI públicas, por lo que es obligado hacer una mención expresa a las mismas. Sin obviar que constituyen un instrumento que contribuye al derecho universal a la banda ancha, nunca podemos olvidar que su uso exige la protección de los contenidos digitales en los smatphones, tablets y ordenadores, para evitar que una tercera persona pueda, a través de esa red pública, acceder a los archivos que no estén securizados. Por tanto, una red pública WIFI nunca debe ser utilizada para compartir o recibir contenidos confidenciales.

3. Imponer obligaciones a las empresas en materia de seguridad:

El conocimiento experto, pero poco común, que, en ocasiones, requieren las tecnologías que por su propia esencia cambian y avanzan de forma vertiginosa, determina, a la postre, una desigualdad real de las personas usuarias frente a las empresas que operan en internet, por lo que debería exigirse a las mismas que ofrezcan al usuario una información básica, comprensible, sencilla -ampliable a voluntad del mismo- sobre los riesgos de seguridad y la forma de activar los mecanismos de protección en la web social.

Como complemento de ello, debería activarse la exigencia de que la persona usuaria preste un consentimiento informado y específico sobre la información a la que accederá la aplicación que se esté instalando, pudiendo admitir unas funciones sí y otras no, no bastando una aceptación genérica, sino detallada y segmentada.

Igualmente, debería requerirse a los desarrolladores de aplicaciones que incorporen desde el diseño inicial de cualquier aplicación o sistema los requerimientos básicos en materia de privacidad y de información a la ciudadanía.

4. Observatorios: proactividad y vigilancia activa en la red:

Una dificultad añadida en este ámbito estriba en la velocidad de la innovación en esta materia; redes sociales emergentes aparecen continuamente y para cuando las agencias u organismos que tienen asignado el control reaccionan, la expansión

viral de aquellas hace que las actuaciones "a posteriori", por muy adecuadas que sean, devengan escasamente efectivas.

Por ello, se deben potenciar organismos u observatorios cuya principal función sea, precisamente, la de adelantarse a las tendencias y actuar como antena activa que alerte de posibles quiebras en materia de protección de datos o de peligros contra la intimidad, a fin de favorecer una enmienda de esas situaciones o prácticas de riesgo que propicien una reacción positiva por parte de las empresas u operadores. Existen ya iniciativas en este sentido, tanto en el ámbito estatal (véanse las estrategias y servicios relacionados con la e-Confianza desarrolladas por INTECO, Instituto Nacional de Tecnologías de la Comunicación), como internacional (informe conjunto de la Oficina del Alto Comisionado de Privacidad de Canadá (OPC) y la Oficina Holandesa de Protección de Datos en relación al WhatsApp, por ejemplo).

El proyecto de creación del Centro Vasco de Seguridad, previsto en la Agenda Digital Euskadi 2015, pretende contribuir a esta labor proactiva de fomento de la seguridad en la red.

Cuarta.- Máxima protección de estos derechos en el caso de los y las menores y adolescentes.

Por todas las razones ya conocidas, es prioritaria la actuación en el ámbito de los y las menores de edad. Es indudable que para la formación y concienciación de los menores es imprescindible una implicación y una coordinación entre los agentes sociales, progenitores, instituciones públicas -especialmente las educativas y las agencias especializadas- y sociedad civil. El marco idóneo que dibuja la Agenda digital Euskadi 2015, podría constituir un instrumento propicio para ello, con el valor añadido de la promoción y el impulso de las agendas digitales locales que incorpora.

En ese contexto, sería de interés que la Administración autonómica vasca adoptara iniciativas de corte similar a las contempladas en el Decreto 25/2007, de 6 de febrero, de la Junta de Andalucía por el que se establecen medidas para el fomento, prevención de riesgos y seguridad en el uso de internet, que, al tiempo que incorpora el derecho al uso y acceso a las TIC y sus beneficios por parte de los menores, incluye directrices sobre el buen uso.

La óptica de derechos que el Ararteko imprime a sus análisis nos lleva a defender que, en las actuaciones que relacionan TIC y menores de edad, el objetivo es facilitar el acceso de los y las menores a la sociedad de la información, posibilitando su crecimiento en la red en un contexto de seguridad. Así, en el curso de la elaboración del **Informe Extraordinario del Ararteko sobre e-inclusión** y la **participación** en las esferas social y pública de la ciudadanía a través de las TIC en Euskadi (de próxima publicación), y a pesar de no ser éste el objeto del Informe, se ha incorporado una recomendación **sobre el fomento de un uso seguro de Internet,** desde una visión global e integradora que avanzamos:

- Se propone trabajar tanto con menores, como con el resto de la comunidad educativa (profesorado, padres y madres) desde la difusión, la sensibilización y la formación.
- Se persigue el compromiso de la creación de una web más segura por parte de desarrolladores, creadores de contenidos, y otros perfiles, entidades y organismos que participan en el desarrollo de la web, tanto desde el plano público como privado. En base a ello, el Ararteko realiza diversas propuestas estratégicas ligadas a la promoción del uso seguro y responsable de las TIC por parte de menores y adolescentes.

De lo que se trata, **en definitiva**, es de encontrar el equilibrio entre la innovación y la extraordinaria potencialidad de las redes sociales, y la garantía de los derechos de las personas. Para ello resulta clave la información, la transparencia y el conocimiento eficiente. En suma, la madurez digital, para que todas las personas puedan utilizar el magnífico potencial de los dispositivos móviles, de internet y de la web social sin poner en riesgo su privacidad, su intimidad y su imagen, avanzando juntos en la construcción de una verdadera comunidad digital.