“Claves para la comunicación de la protección de datos y cómo incrementar su eficacia”

Orígenes de esta iniciativa

Esta declaración es producto del discurso pronunciado por Alex Türk, Presidente de la Autoridad Francesa para la Protección de Datos, con motivo de la conferencia organizada en Varsovia en mayo de 2006 por el Inspector General para la Protección de los Datos en Polonia con el título “Seguridad pública y privacidad”. Alex Türk compartió su profunda preocupación sobre los desafíos a los que se enfrentan las autoridades para la protección de los datos (DPA) en la actualidad. Destacó la necesidad imperiosa de que estas autoridades adapten urgentemente sus medidas para afrontar los mismos, ante el temor de que la filosofía subyacente a la reglamentación para la protección de los datos se vea rápidamente desprovista de fundamentos.

Tras la celebración de esta conferencia, el EDPS invitó al CNIL a establecer una iniciativa conjunta para exponer la necesidad de esta acción urgente ante la conferencia de Londres. El Comisario de información británico ofreció de inmediato su apoyo pleno a esta iniciativa. Esta declaración ha sido redactada gracias a la estrecha colaboración de esas tres autoridades.

Mediante su adhesión a esta iniciativa, las autoridades para la protección de datos participantes se comprometen a coordinar sus acciones para alcanzar los siguientes objetivos:

- Desarrollar actividades de comunicación fundamentadas en ideas comunes, algunas de las cuales se exponen en los anexos adjuntos;
- Adaptar sus prácticas y métodos mediante una evaluación minuciosa de su eficacia y efectividad, y el reforzamiento de sus capacidades de conocimientos técnicos, la anticipación de tendencias y la intervención en el campo tecnológico;
- Contribuir al reconocimiento institucional de las Autoridades para la Protección de los Datos a nivel internacional y fomentar la participación de otras partes interesadas apropiadas, nacional e internacionalmente.

En la actualidad, las siguientes DPA han expresado en principio su apoyo a esta iniciativa:

- Commission nationale de l’informatique et des libertés, CNIL (Francia)
- Supervisor Europeo de Protección de Datos, EDPS (Unión Europea);
- Information Commissioner (Reino Unido);
- Privacy Commissioner of Canada (Canadá);
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Alemania);
- Agencia Española de Protección de Datos (España);
- Garante per la Protezione dei Dati Personali (Italia);
- College Bescherming Persoonsgegevens (Países Bajos);
- Privacy Commissioner (Nueva Zelanda)
- Préposé fédéral à la protection des données et à la transparence (Suisse) / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Switzerland).

Esta iniciativa conjunta se presentará durante la sesión a puerta cerrada de la Conferencia de Comisarios para la Protección de los Datos y la Privacidad en Londres los días 2 y 3 de noviembre. No

será redactada a modo de resolución sino que se presentará como una iniciativa conjunta de CNIL, EDPS y el Comisario de Información del Reino Unido, a quienes las DPA arriba mencionadas ofrecen su apoyo y, en consecuencia, su compromiso de adaptar sus medidas para tomarla en consideración. Se invitará a las restantes DPA representadas en la conferencia a expresar su apoyo e incluso quizás a unirse a esta iniciativa, si así lo desean. No obstante, no se les exigirá la adopción formal de este documento.

Tras hacer una recapitulación de los motivos por los que la protección de datos es indispensable en nuestras sociedades (I), este texto analiza en profundidad los riesgos a los que se enfrentan actualmente las libertades individuales y la protección de los datos en todo el mundo y que plantean tantos desafíos a las autoridades supervisoras (II). De esta declaración se derivan diversas propuestas para la adopción de medidas e iniciativas coordinadas (III), así como para el desarrollo de una nueva estrategia de comunicación común (IV).

I – LA PROTECCIÓN DE DATOS ES INDISPENSABLE PARA LA SOCIEDAD

1. La protección de los datos personales de los ciudadanos es vital para cualquier sociedad, en el mismo grado que la libertad de prensa o de movimientos. A medida que nuestras sociedades dependen cada vez más del uso de las tecnologías de la información y los datos personales se recaban y se generan a escalas cada vez mayores, resulta más importante que nunca que las libertades individuales y otros intereses legítimos de los ciudadanos se respeten adecuadamente en las prácticas informativas relevantes.

2. La protección de los datos no es y no debe considerarse una materia abstracta, teórica y, mucho menos aún, "teológica". Las normas para la protección de los *datos* consisten en la protección de los *individuos*. Su objetivo es la defensa de la dignidad humana y la capacitación de los individuos para ejercer sus derechos y proteger sus intereses legítimos.

3. La protección de los datos sólo puede convertirse en una realidad, si en la práctica se cumplen las normas establecidas a ese fin. Las autoridades para la protección de datos desempeñan un papel fundamental en asegurar su cumplimiento, pero sólo podrán lograr su objetivo si son eficaces a la hora de comunicar los mensajes para la protección de datos así como de implicar a las partes interesadas correspondientes y, de ser necesario, de aplicar sus competencias de investigación y aplicación.

II – DOS OLEADAS; TRES DESAFÍOS

4. Las libertades individuales y las propias autoridades para la protección de los datos están expuestas a riesgos sin precedentes. Dos oleadas amenazan con abrumarlas, al tiempo que se enfrentan a un tercer desafío.

A –El primer desafío se deriva de numerosos factores diversos asociados con el ritmo de los cambios tecnológicos.

5. **Aceleración**: Internet, RFID, nanotecnologías, etc. Las DPA no son hostiles a la innovación ni al progreso tecnológico, pero el periodo de tiempo que media entre el descubrimiento de un fenómeno hasta su aplicación técnica, desde una innovación a otra, desde el desarrollo de un prototipo hasta su aplicación industrial, se reduce cada vez más. Cada vez resulta más difícil lograr que los intentos de adaptación legal o construcción coincidan con la evolución tecnológica. El ritmo tecnológico continúa acelerándose mientras que el ritmo legal se

mantiene particularmente lento, puesto que va sincronizado con aquel impuesto por los procedimientos democráticos.

6. **Globalización:** la reubicación del procesamiento de datos se encuentra en su punto álgido. Sin lugar a dudas, resulta extremadamente difícil controlar las transferencias de datos internacionales. Esta tendencia hacia la globalización se encuentra en conflicto con una de las características principales del imperio de la ley, que es el ámbito geográfico limitado de su aplicación.

7. **Ambivalencia:** la innovación tecnológica conlleva por igual avances y peligros. Es posible que los individuos se sientan considerablemente tentados por las ventajas y la comodidad que la tecnología proporciona, aunque es posible que del mismo modo no tengan consciencia plena de sus riesgos hasta que ellos u otros sufran perjuicios o hasta que sea demasiado tarde. A muchos no les preocupa que se les siga el rastro ni la vigilancia potencial de todos sus movimientos, comportamientos o relaciones. Resulta difícil reconciliar esta ambivalencia hacia la tecnología con el imperio de la ley que, por definición, busca proporcionar respuestas en "blanco y negro".

8. **Impredecibilidad:** los usos tecnológicos a menudo se desarrollan de un modo que inicialmente resultaba impredecible, incluso por los propios diseñadores de la tecnología. En consecuencia, es posible que resulte difícil regular estos usos imprevistos, especialmente cuando discrepan totalmente de aquellos para los que inicialmente se diseñó la tecnología y para los que originalmente la ley parecía fácilmente aplicable.

9. **Invisibilidad (invisibilidad virtual/invisibilidad física)**: el procesamiento de la información cada vez resulta más invisible e intangible, y cada vez menos controlable. La tecnología tiende a hacerse invisible, en primer lugar, porque gran parte del procesamiento de los datos lo realizan los individuos sin ser conscientes de su existencia (por ejemplo, seguimiento del rastro en el uso del transporte público, de la navegación por Internet, de las comunicaciones electrónicas y telefónicas, etc.). En estos casos se puede hablar de invisibilidad virtual, puesto que los procesos son invisibles; pero la tecnología también resulta invisible como resultado de su miniaturización excesiva: en estos casos se puede hablar entonces de invisibilidad real. Dentro de unos cuantos años, el desarrollo de las nanotecnologías hará que resulte imposible ver a simple vista qué tipo de tecnología está presente en un objeto determinado. ¿Cómo será posible controlar el desarrollo de las operaciones de procesamiento realizadas por tecnologías invisibles?

10. **Irreversibilidad**: los avances tecnológicos son irreversibles: ya nunca podremos volver a vivir en un mundo sin ordenadores, Internet, teléfonos móviles, identificación biométrica, geolocalización, CCTV. Puesto que estas tecnologías convergen y cada vez se encuentran más entrelazadas, su combinación puede presentar riesgos reales para nuestras sociedades.

B – El segundo desafío es de naturaleza legal, especialmente en relación con el desarrollo de nueva legislación contra el terrorismo

11. El desarrollo de leyes contra el terrorismo presenta un desafío a las autoridades para la protección de datos que, en este contexto, deben evitar caer en trampas, denunciar fantasías y luchar contra los mitos.

12. **La necesidad de equilibrio**: aunque no poseen calidad de legisladores, ni de tribunales, ni de activistas, las autoridades independientes para la protección de datos desempeñan, sin embargo, una función muy específica. Raramente les resulta posible resolver cuestiones bajo el principio del "blanco y negro". Así pues, todas las autoridades para la protección de los

datos reconocen la legitimidad de las políticas antiterroristas que se han venido desarrollando en los últimos años. No obstante, en concordancia con la misión que la ley les ha otorgado y en nombre del conjunto de la sociedad, es su deber el buscar constantemente el equilibro adecuado entre los imperativos de la necesidad de la seguridad pública, por un lado, y los imperativos de la protección de los datos y de la privacidad, por otro. Deben continuar desempeñando esta función con independencia plena y resistir las inaceptables acusaciones de irresponsabilidad que ocasionalmente se pronuncian en su contra.

13. **El peligro de quedar atrapado en un sistema en espiral:** este riesgo (un tipo de "desviación del uso", conocido en inglés como *"function creep"*) es tal como se describe a continuación. En un momento determinado, bajo circunstancias determinadas, se crea legalmente una base de datos. La autoridad supervisora participa en su desarrollo. Posteriormente, su ámbito se extiende (por ejemplo, al ampliar primero las categorías de las personas implicadas, a continuación los motivos para registrarlas, y, finalmente, otra vez las categorías de las personas con derecho a acceder a la base de datos). En esas fases posteriores, la autoridad se enfrenta al argumento de que no puede oponerse a una simple ampliación, ya que acató el principio para la creación de la base de datos inicial y demás si fuese necesario. No obstante, entre la primera y la última fase en el desarrollo de ese sistema, su ámbito inicialmente aceptable se habrá desplazado tanto que habrá evolucionado hasta convertirse en inaceptable.

14. **La fantasía del carácter ejemplar de los precedentes extranjeros:** con frecuencia, los gobiernos nacionales hacen uso del argumento de que determinados países ya han puesto en marcha un sistema para atacar a sus autoridades nacionales responsables de la protección de datos a causa de su renuencia a aceptar el mismo sistema sin someterlo a un proceso de debate. Esto origina serios problemas de armonización y obliga a las DPA a reflexionar conjuntamente sobre la creación de denominadores comunes.

15. **El espejismo de la base de datos como una cura milagrosa**: las DPA deben recordar constantemente al público y a los gobiernos que crear bases de datos cada vez con más información personal no es la solución a todos los problemas. El aura sagrada del supuestamente infalible archivo informático debe representarse con frecuencia como una vana ilusión. Además, a medida que se procesa cada vez más información personal, aumenta el riesgo de concordancias falsas, información desfasada y otros errores. Estos pueden causar verdaderos perjuicios a las oportunidades en la vida, la salud, la prosperidad e incluso la libertad de los individuos.

16. **El mito del archivo infalible (la cuestión de la "mayoría/minoría")**: con mucha frecuencia se supone (sin fundamento alguno) que todos los individuos se registran en una base de datos por un motivo válido. En consecuencia, las personas que se han inscrito innecesariamente o incorrectamente en tales bases de datos ("la minoría") a veces se encuentran en situaciones imposibles, ya que todo el mundo cree que es virtualmente imposible aparecer mencionado en un sistema tan eficiente sin una justificación. Por lo tanto, resulta esencial desde un punto de vista ético continuar afirmando que la tecnología es falible, así como prohibir la toma automática de decisiones, especialmente en campos como la seguridad y la justicia.

C – El tercer desafío concierne a la reputación

17. En algunos países al menos, la protección de los datos y las DPA no disfrutan de la reputación positiva que merecen. Las normas pueden llegar a percibirse como complejas y difíciles de aplicar en la práctica de forma sistemática, previsible y realista. Algunos critican la regulación en la protección de datos por excesiva, abstracta e insuficientemente enfocada hacia los perjuicios reales o potenciales que pueden surgir (tanto para los individuos como para la sociedad en su conjunto) como resultado del incumplimiento de las reglas. Otros critican el modo en que estas normas se aplican y hacen respetar, lo que resulta en una falta de incentivos

positivos o negativos para cumplir las mismas o para invertir en un cumplimiento adecuado. Políticos, administradores, empresas, medios de comunicación y, en ocasiones, individuos particulares sostienen percepciones negativas como éstas. Es necesario atacarlas y demostrar la importancia práctica de la protección de datos, convirtiendo en realidad el lenguaje de los derechos y libertades fundamentales así como la reconsideración de las prácticas actuales, cuando resulte oportuno.

III – LÍNEAS DE ACTUACIÓN E INICIATIVAS PARA LAS DPA

18. Debido a su gravedad, las DPA deben tomar medidas urgentes para concienciar a los ciudadanos y hacerles comprender los riesgos que depara la amenaza a las libertades individuales en sus respectivos países. Asimismo, deben evaluar sus métodos de trabajo y mejorar su eficacia y efectividad.

A – Las DPA deben trabajar conjuntamente para llevar a cabo cambios y estrategias coordinadas de modo que resulte posible actuar de maneras nuevas, más efectivas y relevantes

19. **Fortalecimiento de las capacidades de conocimiento, estudios avanzados e intervención en el ámbito tecnológico:** actualmente la protección de datos sufre debido a su imagen excesivamente "jurídica"; sin embargo, la credibilidad de nuestras instituciones depende, y cada vez lo hará más, de nuestra capacidad para comprender, analizar y anticipar los avances tecnológicos.

20. Para analizar estas nuevas tendencias, las DPA deben elaborar estrategias para compartir actividades entre ellas según las cuestiones del caso que se esté tratando, sus respectivas experiencias y responsabilidades y sus medidas prácticas de actuación.

21. Deben reflexionar sobre las relaciones que desean establecer con los investigadores y la industria en el campo de las nuevas tecnologías, así como hacer hincapié en las ventajas de una buena protección de datos para las propias empresas y entidades públicas.

22. **Evaluación de nuestra efectividad y cambios en nuestras prácticas:** es absolutamente necesario realizar una evaluación meticulosa y honesta de la efectividad de cada autoridad. ¿Están logrando todas y cada una de las autoridades obtener un impacto real y cambiar las cosas verdaderamente en la práctica? ¿Se traducen las palabras en acciones? Este tipo de evaluaciones nos permitirá aprender lecciones sobre cómo mejorar nuestros resultados.

23. La evaluación de la eficacia de cada autoridad ciertamente llevará a algunas de ellas a exigir de los legisladores el otorgamiento de suficientes poderes y recursos. Es posible que también presente cuestiones sobre algunas prácticas de determinadas autoridades. Todos debemos establecer prioridades, particularmente en lo referente a la gravedad y probabilidad de perjuicios. Debemos concentrarnos principalmente en los principales riesgos a los que las personas individuales se enfrentan en la actualidad y poner cuidado de no ser excesivamente rígidos o puristas en cuestiones que no lo requieren. Debemos estar preparados para un mayor pragmatismo y una mayor flexibilidad.

B – Las DPA deben reflexionar conjuntamente sobre cómo obtener un mejor reconocimiento institucional de sus acciones a nivel internacional y cómo implicar a las partes interesadas

24. **Una reestructuración necesaria de la conferencia internacional:** los desafíos globales requieren soluciones globales. La Conferencia Internacional de Comisarios para la Protección de Datos y de la Privacidad debe actuar como la vanguardia de nuestras acciones a nivel internacional. Debemos asegurarnos de su viabilidad, mejorar su funcionamiento, incrementar su visibilidad y eficacia, y elaborar un plan de acción y un programa de comunicación. Esto puede implicar el considerar la creación de un secretariado permanente para la Conferencia. La Conferencia debe convertirse en el interlocutor inevitable en todas las iniciativas internacionales que tengan repercusión sobre la protección de datos. Debe ofrecer un espacio para el debate y permitir que surjan sugerencias específicas para poder realizar un mejor seguimiento de las iniciativas internacionales, armonizar prácticas y adoptar posiciones comunes.

25. **Elaboración de una Convención Internacional y otros instrumentos globales:** en la Declaración de Montreux (2005), los Comisarios para la Protección de los Datos y la Privacidad hicieron un llamamiento para el desarrollo de una Convención universal para la protección de los datos. Esta iniciativa debe recibir el apoyo de las DPA mediante las instituciones competentes, manteniendo el respeto debido a su posición institucional y a los prerrequisitos necesarios para su coordinación nacional, si fuesen aplicables. Dentro de este marco, las DPA deberán poner todo su empeño para fomentar esta iniciativa en sus respectivas áreas de influencia, en particular dentro de las organizaciones regionales o zonas lingüísticas a las que pertenecen. La necesidad de soluciones globales para el respeto de la privacidad y la protección de datos puede surgir en sectores específicos (por ejemplo: gobierno de Internet, transacciones financieras, transporte aéreo) y en consecuencia las DPA deberán afrontarla con todos los medios apropiados.

26. **Participación de otras partes interesadas (sociedad civil, ONG, etc.)**: existen otras partes interesadas en la protección de los datos y de la privacidad activas en la actualidad, tanto nacional como internacionalmente, a diferentes niveles y en diversos sectores. Estas organizaciones pueden actuar como socios estratégicos y contribuir de modo sustancial para que las DPA logren una mayor eficacia. Por lo tanto, deberá fomentarse la cooperación con otras partes interesadas apropiadas o incluso desarrollarse de forma activa.

IV – HACIA UNA NUEVA ESTRATEGIA COMUNICATIVA

27. La comunicación es una condición clave para lograr una protección de los datos más eficaz. Un mensaje no recibido y no comprendido es como si no existiese. Una opinión o decisión que no es accesible tendrá un impacto limitado y es posible que los esfuerzos invertidos en su desarrollo no merezcan la pena.

A – Necesitamos desarrollar y aplicar urgentemente una nueva estrategia comunicativa, tanto a nivel nacional como internacional

28. **La comunicación como objetivo.** El objetivo impulsor de todas las DPA debe ser una mejor comunicación con el público. No es aceptable que en algunos países donde el derecho a la protección de los datos es un derecho constitucional, al igual que lo son la libertad de movimientos o de prensa, la inmensa mayoría de los ciudadanos no tengan el más mínimo conocimiento de tales derechos o de su importancia. Son aún menos aceptables aquellos casos en los que incluso existen actitudes negativas hacia la protección de los datos.

29. Debemos iniciar campañas de concienciación robustas y a largo plazo cuyo objetivo sea informar a las personas de la existencia y los contenidos de sus derechos. Deberá realizarse una medición de los efectos de estas acciones. Se debería centrar la atención en dos grupos específicos:

    - Representantes electos regionales y nacionales (la mayoría de ellos no están mucho mejor informados que el ciudadano medio).
    - Los jóvenes, los cuales muestran poco interés en estas cuestiones puesto que están muy acostumbrados a usar las nuevas tecnologías. Debemos tomar medidas en el campo educativo lo antes posible.

30. **La comunicación como un poderoso resorte**. Es importante y urgente que se otorguen a nuestras DPA mejores medios de acción y que se les asegure un reconocimiento a nivel internacional. La confianza y el apoyo público son absolutamente esenciales. La protección de datos debe ser una cuestión mucho más concreta. Son únicamente aquellas organizaciones que se comunican, generalmente a través de los medios y de modo **coherente, accesible y relevante**, con el público general las que obtendrán el poder necesario para influir sobre la opinión pública y, consecuentemente, para ser escuchadas y tomadas en serio por los estados y la comunidad internacional. El cumplimiento de esta condición es necesaria para obtener los medios de actuación indispensables.

31. Ello implica que todos debemos usar profesionales de la comunicación en nuestras autoridades y que los mensajes comunicativos sean lo más sistemáticos posible en todas las PDA.

B – Un mensaje comunicativo interesante sería el establecer paralelos entre la preservación de las libertades individuales y la preservación del medioambiente

32. En cuestiones medioambientales las acciones particulares no resultan impunes. Del mismo modo, debemos actuar con extremada cautela en el ámbito de la protección de los datos ante cualquier evolución tecnológica incontrolada o cualquier ley que pueda aplicarse sin una visión clara de los peligros en juego. Adicionalmente, corremos el riesgo de que nuestro "capital" en términos de libertades y de identidad se reduzca o incluso resulte destruido. Y éste no se renovará, precisamente porque la innovación tecnológica es irreversible.

33. La protección de los datos y de la privacidad puede resultar, de hecho, tan preciosa como el aire que respiramos. Ambos son invisibles, pero la ausencia de cualquiera de ellos puede tener consecuencias igualmente desastrosas.

V - PROGRAMA DE ACTIVIDADES DE SEGUIMIENTO

34. El debate de esta iniciativa en la sesión a puerta cerrada de la Conferencia Internacional de Comisarios para la Protección de Datos y de la Privacidad en Londres deberá entenderse como un primer paso hacia un consenso creciente sobre la necesidad de actuar y de desarrollar medios para comunicarse mejor y lograr una protección de los datos más efectiva.

35. Las DPA que apoyen esta iniciativa se comprometen a desarrollar en mayor profundidad y, cuando resulte necesario, a responsabilizarse de la realización de una serie de actividades conjuntas sobre las que se informará y se realizará un seguimiento en la siguiente conferencia en Montreal, como por ejemplo:
    - Taller sobre aspectos estratégicos: condiciones para lograr una mayor eficacia de las DPA; posible desarrollo de los "principios de buena supervisión" para la protección

de datos; información sobre buenas prácticas (comisarios y personal estratégico); reflexión sobre el desarrollo de una convención internacional;

- Taller sobre comunicación: conocimientos disponibles acerca de la comunicación de la protección de datos (por ejemplo, campañas, investigación de opiniones); desarrollo de un mensaje conjunto y herramientas efectivas para su divulgación (profesionales de la comunicación);
- Taller sobre la aplicación: conocimientos disponibles para realizar un seguimiento y asegurar el cumplimiento; medios eficaces para la inspección (incluidas auditorías) e intervención (comisarios y personal de aplicación);
- Taller sobre organización interna: experiencias recientes acerca de cambios organizativos; proyectos para mejorar la eficiencia y eficacia (comisarios y personal de la organización);
- Cualquier otra actividad considerada relevante para esta iniciativa.