PRIVACIDAD Y RIESGOS TECNOLÓGICOS DERIVADOS DE LA TRANSFORMACIÓN DIGITAL. DESAFÍOS PARA EL DERECHO PÚBLICO

Juan Francisco Rodríguez Ayuso, Profesor Contratado Doctor de Derecho Administrativo y Coordinador Académico del Máster Universitario en Protección de Datos de la Universidad Internacional de La Rioja (UNIR)

I. BREVE INTRODUCCIÓN AL PROBLEMA

Parece adecuado partir analizando qué se entiende por riesgo. De un modo general, el riesgo viene a traducirse como la probabilidad de que se materialice una amenaza y el impacto que tendría en caso de que se materializara, entendiendo por amenaza cualquier factor de riesgo susceptible de provocar un daño o perjuicio a los interesados cuyos datos personales son objeto de tratamiento. Como podemos deducir fácilmente, el riesgo siempre estará presente y condicionará cualquier tipo de decisión que debamos tomar, lo que determina la necesidad de identificar dicho riesgo y proceder a su evaluación para, de este modo, poder minorarlo[1]. En materia de protección de datos, el riesgo consistiría en la probabilidad de que suceda un daño para el interesado como resultado de la realización de operaciones de tratamiento sobre sus datos personales.

Hacemos referencia, de este modo, al riesgo que puede conllevar la realización de operaciones de tratamiento sobre los datos personales

[1] LLANEZA GONZÁLEZ, P., «Nuevo marco de cumplimiento en las obligaciones de protección de datos: la gestión de la privacidad desde la mitigación del riesgo», *Revista de privacidad y Derecho digital*, núm. 4, 2016, pág. 146.

propiedad del interesado en relación con sus derechos y libertades fundamentales, en especial el derecho fundamental a la protección de sus datos personales. De este modo, es fundamental tener en cuenta el riesgo que implica cualquier tratamiento de datos personales, así como cualquier otro riesgo que pueda derivarse de situaciones tales como violaciones de seguridad, que pueden acarrear daños y perjuicios físicos, materiales o inmateriales para las personas físicas, tales como pérdida de control sobre sus datos personales o limitaciones de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daños para la reputación, pérdida de confidencialidad de datos personales sometidos al secreto profesional o cualquier otro perjuicio de carácter económico o social relevante para el interesado.

No se proporciona una definición de qué ha de entenderse por riesgo elevado o, más comúnmente, alto riesgo, siendo aconsejable que sea el Comité Europeo de Protección de Datos, tal y como establece el considerando 77 RGPD[2], el que emita aquellas directrices relativas a las operaciones de tratamiento que se considere improbable que supongan un alto riesgo para los derechos y libertades de los titulares de los datos, indicando, de igual modo, qué medidas pueden ser suficientes, en estos casos, para hacer frente al riesgo.

En cambio, la nueva normativa en materia de protección de datos personales sí que proporciona determinados criterios para entender en qué consiste este riesgo elevado, tales como la sensibilidad de los datos personales y las consecuencias que puede conllevar para el interesado el hecho de que se traten sus datos, lo que implica que el responsable del tratamiento habrá de efectuar una evaluación de impacto y, en su caso, una consulta previa a la autoridad de control.

---

[2] Diario Oficial de la Unión Europea L 119/1, de 04 de mayo de 2016.

En el ámbito concreto de la protección de datos, como ya se indicado, la aproximación basada en el riesgo no constituye una novedad, ya que se incorporaba ya a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[3] derogada, lo que pone de relieve la importancia de esta concepción, hasta el punto de erigirse, en la actualidad, en elemento nuclear del principio de responsabilidad proactiva. En este sentido, la aproximación basada en el riesgo está interconectada con otros principios, tales como el principio de privacidad desde el diseño y por defecto, y con obligaciones que recaen sobre el responsable el tratamiento, como aquella que establece el deber de elaborar y llevar un registro de las actividades de tratamiento. Ahora bien, podemos afirmar que el concepto de aproximación basado en el riesgo adquiere, dentro de la nueva regulación en materia de protección de datos, su más alto exponente.

En un contexto internacional, este reconocimiento tiene lugar también en instrumentos internacionales en materia de protección de datos. Más específicamente, la versión revisada y actualizada de las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales del año 2013 incorpora, de manera específica, la evaluación del riesgo entre los principios de aplicación, aludiendo concretamente a la relevancia que tiene en el desarrollo de políticas y salvaguardas para garantizar la privacidad. Esta evaluación del riesgo constituye uno de los pilares esenciales para el desarrollo de salvaguardas apropiadas que sean objeto de programas de gestión de la privacidad, de modo que la evaluación de impacto constituye la medida que va a posibilitar, en su caso, identificar, analizar y evaluar el riesgo.

---

[3] Diario Oficial de las Comunidades Europeas L 281/31, de 23 de noviembre de 1995.

II. ORIENTACIONES PARA UN AJUSTE ADECUADO A LAS EXIGENCIAS DERIVADAS DE LA TRANSFORMACIÓN DIGITAL POR PARTE DEL DERECHO PÚBLICO DEL ESTADO

El surgimiento de la crisis actual de emergencia sanitaria derivada del COVID-19 ha supuesto, entre otras cosas, una limitación de la libertad de circulación de las personas físicas. Esto ha tenido un efecto inmediato en el ámbito profesional, como ha sido la decisión, por parte de las organizaciones, de que todas o parte de las actividades realizadas se lleven a cabo en situaciones de teletrabajo, habiendo, dada la urgencia de la situación, de implementarlas con carácter provisional y sin una previa planificación.

En estos casos, resulta imprescindible, paralelamente a la implementación de esta modalidad de trabajo, reflexionar sobre la resiliencia de la organización a la adaptación y la continuidad de los procesos de negocio. Todo ello manteniendo los derechos y libertades de los interesados.

Por este motivo, el responsable del tratamiento y el personal que interviene en los tratamientos deben tener en consideración las recomendaciones técnicas básicas que a continuación se siguen[4]:

1. Seguridad en el seno de las organizaciones

Desde el momento en el que el responsable del tratamiento opte por adecuar su objeto de negocio a esta modalidad de teletrabajo, deberá implementar, al menos, los siguientes controles:

---

[4] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo, 2020.

1.1. Políticas básicas

Dentro de esta política general, deberá incluirse, como parte integrante, una política concreta que regule la movilidad en situaciones, como esta, ciertamente excepcionales y que establezca las necesidades específicas y los riesgos singulares que se deriven del acceso que tendrá que producirse a los recursos de la organización desde espacios que escapan del control de esta. Entre estas necesidades específicas, se deberán incluir las modalidades de acceso remoto permitidas, los dispositivos que pueden ser empleados para cada modalidad y el nivel de acceso permitido dependiendo de cada perfil de movilidad que se haya definido; a su vez, se tendrán que definir el conjunto de obligaciones y responsabilidades a asumir por los empleados de la organización que trabajen bajo esta modalidad.

Además de lo anterior, también será preciso elaborar y remitir a las personas afectadas las guías funcionales que se hayan adaptado para formarles, que se deriven de tales políticas y que deberán recoger, como mínimo, las recomendaciones dirigidas a los empleados que, específicamente, participen en operaciones de tratamiento de datos personales, los cuales deberán respetar también el resto de normas y procedimientos que las desarrollen, especialmente en lo concerniente al deber de confidencialidad en relación con los datos personales a los que tuvieran acceso en el desempeño de sus funciones laborales.

1.2. Terceros encargados del tratamiento

Para el cumplimiento de esta medida, será necesario emplear aplicaciones y soluciones de teletrabajo que proporcionen garantías adecuadas y que eviten la exposición de la información personal de los

interesados y servicios corporativos del responsable del tratamiento, en especial, en lo que se refiere a los servicios de correo electrónico y de mensajería.

Junto a lo anterior, y merced al principio de responsabilidad proactiva que debe presidir permanentemente la actuación del responsable del tratamiento, este sólo podrá acudir a prestadores de servicios que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas (artículo 28.1 RGPD) antes de proceder a la necesaria celebración del contrato o acto jurídico equivalente que describa el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Por ende, deberán proporcionar soluciones seguras que, entre otras cosas, eviten la exposición de los datos personales del interesado y de información confidencial de la organización tratados por el encargado del tratamiento.

1.3. Acceso supervisado a los datos

En este caso, los perfiles o niveles de acceso a la información y, más concretamente, a los datos personales ha de estar configurada de tal modo que atienda al rol de cada empleado. Lo lógico será, además, que esta configuración sea más restrictiva cuando el trabajo se desempeña desde una red externa, como sucede con la modalidad del teletrabajo.

De igual modo, la organización tendrá que implementar limitaciones de acceso complementarias dependiendo de la modalidad de dispositivo (equipos portátiles corporativos securizados, equipos personales externos y dispositivos móviles, como smartphones o tablets) por medio del cual se produzca el acceso a los datos personales y del lugar desde el que se produzca dicho acceso.

1.4. Control regular de equipos y sistemas de información

Los servidores a través de los cuales se acceda remotamente a la información tendrán que ser objeto de revisión regular y de adecuada actualización y configuración con el fin de asegurar la satisfacción de la política de protección de datos y de seguridad de la información en un contexto de teletrabajo. También se tendrán que controlar los perfiles de acceso que se hayan definido.

En concreto, los equipos de la organización que se utilicen como clientes tendrán que estar actualizados a nivel de aplicación y sistema operativo, tener deshabilitados los servicios que no sean necesarios, contar con una configuración por defecto de mínimos privilegios definida por los servicios TIC que no pueda ser desactivada ni modificada por el empleado, instalar únicamente las aplicaciones autorizadas por la organización, contar con software antivirus actualizado, disponer de un cortafuegos local activado, tener activados sólo las comunicaciones (WiFi, bluetooth, etc.) y puertos (USB u otros) necesarios para llevar a cabo las tareas encomendadas e incorporar mecanismos de cifrado de la información.

1.5. Control de accesos telemáticos

Parece obvio que, en aras de dotar de seguridad a los accesos que se produzcan desde fuera de la organización por parte de los empleados, el monitoreo será fundamental para la identificación de patrones anormales de comportamiento en el tráfico de red cursado en el contexto de la solución de acceso remoto para evitar la propagación de programas malignos por la red corporativa y el acceso y uso no autorizado de recursos.

A tal efecto, como veremos, las violaciones de seguridad de los datos personales deberán ser notificadas a la autoridad de control y, además, en determinados supuestos, comunicadas a los interesados (artículos 33 y 34 RGPD) para garantizar un entorno de teletrabajo resiliente. Esto deberá ir precedido de la comunicación a los empleados, dentro de la política de protección de datos y de seguridad de la información, de la existencia y alcance de estas actuaciones encaminadas a monitorizar su actividad remota; no obstante, si las actuaciones de control y supervisión por parte del responsable del tratamiento se extendieran a la verificación del cumplimiento de las obligaciones laborales de los empleados, aquel tendrá que proporcionar oportuna y previa información, y habrá de hacerlo de forma clara, expresa y concisa, incardinándose esta actividad proactiva dentro de las medidas adoptadas en el contexto de las funciones de control contempladas y del respeto a los derechos digitales previstos en la LOPDGDD (en especial, el derecho a la intimidad y al uso de dispositivos digitales y el derecho a la desconexión digital en el ámbito laboral -artículo 87-), ejercidas dentro de su marco legal y con los límites inherentes al mismo.

1.6. Uso seguro de dispositivos corporativos y externos

Los empleados que, por medio de los dispositivos corporativos de la organización que actúe como responsable del tratamiento, accedan a información personal de los interesados, tendrán que configurar y emplear contraseñas de acceso robustas y distintas a las utilizadas para el acceso a cuentas de correo electrónico personales, redes sociales o cualquier otro tipo de aplicaciones utilizadas en el ámbito de su vida personal.

Además, queda prohibida la descarga o instalación de aplicaciones o software que no hayan sido autorizados previamente por el responsable del tratamiento, habiendo de ser una recomendación de la organización que se

eviten aquellas conexiones de dispositivos a la red de la organización producidas en lugares públicos o a través de redes WiFi que sean abiertas no seguras.

Fundamental será también el mantenimiento de mecanismos de autenticación previamente definidos (certificados, contraseñas, tokens, sistemas de doble factor, etc.) que sirvan para la validación de los sistemas de control de acceso remoto a información de la organización. Asimismo, si los empleados disponen de dispositivos corporativos, estos no deberán ser utilizados para finalidades personales, a fin de evitar accesos a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como a otros sitios que puedan contener virus o favorecer la ejecución de código dañino; en cambio, si los dispositivos empleados para el acceso remoto pertenecen al propio empleado, será preciso evitar la simultaneidad en el desarrollo de actividades personales y de tareas profesionales, definiendo, igualmente, perfiles separados e independientes para el desarrollo de cada una de ellas.

1.7. Integridad, disponibilidad y confidencialidad como principio rector del tratamiento

Cuando se esté teletrabajando, será precisa la adopción de precauciones adecuadas que garanticen que la información a la que se esté accediendo se mantiene confidencial.

Cuando se trabaje con documentos en formato físico, será necesario reducir al mínimo la entrada y salida de estos, extremando las salvaguardas que impidan accesos no autorizados por parte de terceros, y evitar desecharlos sin estar seguros de que son adecuadamente destruidos. A ello, deberemos sumar la prohibición de arrojar papeles enteros o en trozos en

papeleras de hoteles, lugares públicos o en la basura doméstica a los que alguien pudiera acceder y recuperar información personal.

1.8. Conservación adecuada de la información

Deberá estar prohibido el almacenamiento local de la información personal de los interesados, siendo necesario que la misma se encuentre archivada en espacios compartidos, o en la nube, suministrados por el responsable del tratamiento. Al respecto, si los dispositivos empleados son personales, no se podrán utilizar aplicaciones no autorizadas en la política de la entidad para compartir información.

También será imprescindible impedir el cumplimiento de la política de copia de seguridad corporativa definida para cada dispositivo por la organización, amén de proceder a la revisión y supresión periódica de la información residual que pueda quedar archivada en el dispositivo, como archivos temporales del navegador o descargas de documentos.

2. Gestión de las violaciones de seguridad de la información

2.1. Detección de la brecha y notificación a la autoridad pública de control y supervisión

El artículo 33 RGPD dispone que, en el caso de que tenga lugar una brecha de seguridad, el responsable del tratamiento tendrá el deber de notificarla a la autoridad de control que resulte competente, de acuerdo con lo que establece el artículo 55 RGPD. Y deberá hacerlo sin dilación indebida, en concreto, en las setenta y dos horas siguientes a que se haya tenido conocimiento de la misma; de no efectuarse dentro del período descrito,

tendrán que acompañarse las razones que lo impidieron, exponiéndolas de forma motivada.

Empero, esta obligación de notificación no será necesaria en el supuesto de que exista escasa probabilidad de que tal incidencia en materia de seguridad suponga un riesgo para los derechos y las libertades de los interesados.

Amén de lo anterior, el responsable del tratamiento tendrá que dejar constancia documental de toda brecha seguridad de los datos, incluyendo los hechos que se relacionen con la misma, qué impacto ha ocasionado y cuáles han sido las medidas correctoras, de cualquier naturaleza, implementadas. Esta documentación permitirá que la autoridad de control pueda verificar la satisfacción de tales exigencias normativas.

2.2. Comunicación a los interesados

Junto a lo anterior, el artículo 34 RGPD dispone que, cuando haya probabilidad de que la brecha de seguridad suponga y determine un riesgo alto para los derechos y libertades de los interesados, el responsable del tratamiento deberá efectuar una comunicación a los titulares de los datos personales afectados, y deberá hacerlo igualmente sin dilación indebida. Esta comunicación deberá consistir en una descripción, en un lenguaje claro y sencillo, de la naturaleza del incidente de seguridad y habrá de incluir, al menos, la información descrita en las letras b), c) y d) del precepto inmediatamente anterior.