TRANSFORMACIÓN DIGITAL Y DISEÑO ORIENTADO A LA PRIVACIDAD EN LA UNIVERSIDAD

DIGITAL TRANSFORMATION AND PRIVACY-ORIENTED DESIGN AT THE UNIVERSITY[1]

Autor:

Ricard Martínez Martínez. Universitat de València. Cátedra de privacidad y Transformación Digital Microsoft - Universitat de València. IRTIC (Instituto de Robótica y Tecnologías de la Información y las Comunicaciones). ricard.martinez@uv.es

Resumen:

En este artículo se consideran los requerimientos de cumplimiento normativo vinculados a la transformación digital. A partir de la experiencia del autor se reflexiona sobre como la digitalización impacta en el derecho fundamental a la protección de datos. Es necesario considerar los proyectos de transformación desde un enfoque basado en privacidad. Y este enfoque no debe responder a la necesidad de cumplir con la norma. La protección de datos desde el diseño y por defecto contribuye significativamente a la mejora de procesos, a la calidad y confiabilidad de la información, y a la seguridad. La privacidad no es un coste sino una inversión. Y, además, un imperativo ético para la institución universitaria.

Abstract:

This article studies the regulatory compliance requirements related to the digital transformation. From the author's experience, the workpaper reflects on how digitisation impacts on the fundamental right to data protection. It is necessary to consider transformation projects from a privacy-based approach. And this approach should not respond to the need to comply with the Law. Data

[1] El presente trabajo se enriquece y contribuye al debate en sendos proyectos de investigación sobre la reforma del sistema europeo de protección de datos financiados por el Ministerio de Economía y Competitividad (DER2012- 34764) y por la Universitat Jaume I (P1-2012-12).

protection by design and by default contributes significantly to process improvement, information quality and reliability, and security. Privacy is not a cost but an investment. And it is also an ethical imperative for the university institution.

Palabras clave:
Transformación digital; privacidad; protección de datos
Keywords:
Digital transformation; privacy; data protection

Abordar el proceso de transformación digital de la institución universitaria requiere de un esfuerzo considerable que debe tener en cuenta todo tipo de factores. Este trabajo se centrará en un ámbito muy específico: el cumplimiento de las previsiones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).

Sin embargo, desde el punto de vista del autor, el trabajo se vería seriamente menoscabado si no se tienen en cuenta elementos de experiencia vinculados al conocimiento de la realidad material de la institución universitaria. Como suele decirse coloquialmente el papel es muy sufrido, lo aguanta todo. Y esta capacidad de aguante podría traducirse en un ejercicio barroco y preciosista sobre “cómo hay que hacer las cosas”, muy alejado de la realidad, de “cómo son las cosas”. Y, para un profesional e investigador de la protección de datos no habría peor negligencia, que desconocer los hechos. El Reglamento General de Protección de Datos, no es una norma que admita aproximaciones de sillón, obliga al jurista a trabajar a pie de obra, a ensuciarse las manos en procesos que implican una profunda transformación organizativa y técnica.

1. La transformación digital: un deber ineludible para la Universidad

La naturaleza jurídica de las universidades en España presenta peculiaridades cuyo influjo en materia de transformación digital no resulta en absoluto desdeñable. Todas las universidades, con independencia de su naturaleza pública y privada se ordenan a realizar el servicio público de la educación superior mediante la investigación, la docencia y el estudio, conforme a la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y lo hacen protegidas por una garantía institucional-constitucional, la autonomía universitaria.

La institución universitaria esta llamada a jugar un papel determinante en la transformación digital en España, podría casi decirse que la Universidad está éticamente obligada a transformarse digitalmente para transformar nuestro país. En ello inciden razones tan sobradamente conocidas que no necesitan ni siquiera de una evidencia empírica para ser compartidas por cualquier lector.

Cada universidad constituye un pilar fundamental en el desarrollo de su entorno territorial. Y no me refiero con esto exclusivamente a la incidencia de la población de estudiantes y profesores universitarios en la economía local, -a través de alquileres, consumos, transportes etc.-, sino al potencial transformador de estos centros educativos. Es un hecho bien conocido que la transformación digital va a cambiar profundamente las necesidades de formación y cualificación. En este sentido, la digitalización creará nuevos puestos de trabajo, modificará el modo de hacer las cosas en sectores enteros, y afectará profundamente a una parte significativa del mercado laboral haciendo innecesarias actividades repetitivas susceptibles de ser sustituidas por la robotización y la inteligencia artificial.

En la universidad residen el conocimiento y las capacidades investigadoras necesarias para hacer viable ese cambio y también para humanizarlo. Basta con mirar la historia reciente para verificar como fueron las universidades españolas casi las primeras en utilizar la informática para la investigación científica, -no en vano los centros de proceso se llamaron en muchas universidades se llamaron “centros de cálculo-, en contribuir al nacimiento de la Internet Española, o en impulsar la supercomputación.

Corresponde a la universidad soportar el esfuerzo de formación cambio e innovación que requerirá la transformación digital española. Mientras se escriben estas líneas miles de estudiantes universitarios finalizan sus estudios de grado, máster o doctorado. Y muchos de ellos redactan trabajos finales que sustentan investigaciones, ideas innovadoras, y emprendimiento directamente relacionados con la materia objeto de este trabajo. Y esta oportunidad no sólo se presenta en los máster sobre "*big data*", es una oportunidad transversal a todas y cada una de las disciplinas universitarias. El adjetivo "digital", acompaña a la escuela, la medicina, la economía, el derecho, la administración pública, la biblioteconomía, la biología, la informática, la sociología… y sitúa a la Universidad en un lugar central

Además, en el desarrollo de la actividad investigadora y en la transferencia de conocimiento la universidad juega un papel crucial en la generación de redes. La Sociedad Red que ha hecho posible la transformación digital define ecosistemas de innovación en el doble contexto de la ciudad, -en el que nacen y viven las universidades-, y en una sociedad hiperconectada y basada en datos.

Bastan estos factores para entender que en las universidades la transformación digital debería concebirse como algo más que una apuesta o decisión política. La Universidad, y los universitarios, han moldeado nuestra sociedad desde la Ilustración. Y lo han hecho desde la libertad, y la autonomía, desde la ciencia y el humanismo. Asumiendo un liderazgo social, y a veces político, determinante en cada sociedad. El "*Sapere Aude*" kantiano es un imperativo categórico irrenunciable también en el contexto de la Cuarta Revolución. No podemos sustentar una nueva era de evolución tecnológica deshumanizada, regida por puros principios de eficiencia y beneficio.

La Universidad tiene la ineludible necesidad de comprometerse con la transformación digital desde el compromiso con los valores de la dignidad y los derechos humanos para la sociedad en la que se integra. Pero para ello, debe transformarse a sí misma. Debe asumir que es momento de cambiar de modo radical sus estructuras y modos de hacer. Debe digitalizarse para contribuir a la

digitalización. No es una cuestión de elección, es un deber inexcusable. La Universidad debe emprender el camino del cambio si no quiere traicionarse a sí misma, traicionando con ello a la entera comunidad.

2. La resistencia al cambio o la Universidad como Administración

El mapa universitario español incluye hasta 52 universidades públicas integradas en lo que la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, define como sector público institucional. Esto posee profundas implicaciones estructurales e incide de modo muy particular en las condiciones del cumplimiento normativo en materia de protección de datos.

Administración y burocracia se han usado como conceptos sinónimos en el lenguaje coloquial de un modo probablemente acertado. Incluso los entornos universitarios de naturaleza privada no escapan en muchas ocasiones a la burocratización ante la complejidad de un modelo de gestión que, tras las reformas de Bolonia, no para de complicarse trámite a trámite.

Desde un punto de vista práctico, para el universitario medio es evidente hasta qué punto es una realidad cotidiana ese modo de entender una administración que se sirve de las personas en lugar de estar a su servicio. La burocracia universitaria consume horas y horas de estudiantes, de profesores e investigadores, y del propio personal de administración, en una vorágine de trámites imposibles e incomprensibles. Alimentamos a la bestia con toneladas de papel, con comisiones y reuniones interminables. Y sacrificamos en el altar del procedimiento lo que mejor sabemos hacer: generar y transferir conocimiento.

La Universidad ha asistido a distintas reformas normativas que deberían haber impulsado la digitalización de la administración universitaria, que probablemente han generado más forma que sustancia. Me refiero al menos a las siguientes normas, aplicables o no, a la institución universitaria. Así han sido directamente aplicables:

- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y normas autonómicas de desarrollo.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Pudieron haber sido inspiradoras al menos:

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

Todas estas normas poseen elementos comunes muy relevantes desde el punto de vista del propósito de este trabajo y del desarrollo de la transformación digital:

1. Se vinculan directa o indirectamente al procesado de información personal en el mundo digital.

2. Obligan a una reingeniería de procesos.

No es posible la correcta implementación de las exigencias de estas normas sin un análisis profundo de la organización universitaria. Cada una de las normas ha supuesto una oportunidad, quien sabe si perdida, de auditar la organización universitaria, y de diseñar nuevos procesos funcionales no sólo al cumplimiento normativo, sino también a la mejora en el funcionamiento operativo de la institución.

3. Favorecen y obligan a procesos de simplificación administrativa.

4. Obligan a un rediseño de los procedimientos orientado al usuario, que debería poner a cada perfil de la comunidad universitaria en el centro de atención de la organización.

5. Implican un esfuerzo constante y reiterado de formación y adaptación del personal.

6. Suponen nuevas formas de gestionar las plantillas y determinan un enfoque basado en los datos que apueste por el conocimiento y la creatividad.

La alta especialización de las áreas de gestión universitaria, unida a la limitación de efectivos en las plantillas convierte la movilidad funcionarial tradicional en algo paralizante. El impacto de la transformación digital debería implicar un nuevo modelo centrado en la creatividad y calidad en el desempeño.

7. Obligan a adoptar decisiones estratégicas y a alinear al conjunto de la organización. Apuntan a la transversalidad y a la ruptura de los modelos verticales y los de taifas.

8. Favorecen la rentabilidad en términos de mejora y calidad del servicio, de la mano de la eficiencia en los nuevos procesos que se diseñen.

9. Deberían impulsar procesos de innovación, transferibles al resto de la administración y de la sociedad.

10. Podrían haber generado entornos de open data altamente creativos.

11. Cambian por completo el rol de los servicios responsables de las tecnologías de la información. La informática constituye el sistema nervioso al completo de la organización universitaria, es su infraestructura básica. Y no puede ser concebida por mucho más tiempo como algo auxiliar y subordinado.

Sin embargo, no parecen haber sido estos los resultados generalmente alcanzados. Podría decirse, por ejemplo, aunque se trata de una afirmación conscientemente exagerada, que la administración electrónica pasó por la Universidad, pero más de una no subió a ese autobús.

Así por ejemplo, la administración electrónica que debería haber supuesto una profunda revolución que simplificase y mejorase los procesos, parece haber consistido en la mayoría de los casos en una mera "digitalización" de los procedimientos. Y cuando se "sube" a la sede electrónica un mal procedimiento no tenemos una mejora, sino un empeoramiento. Del mismo modo, no hay conversación más habitual entre el profesorado que la relativa a su cansancio con la exagerada "*comisionitis*", y la asunción constante y en progresión aritmética de la carga burocrática de tareas.

En España contamos con más de una decena de universidades que reúnen estos requisitos: a) ser de tamaño medio-alto; b) contar con estudios relacionados con la informática, las telecomunicaciones o la ingeniería; c) tener un alto grado de interacción con empresa y administración en la transferencia de conocimiento; d) disponer de recursos adecuados en materia informática; e) disponer de algún tipo de campus orientado a la promoción de la innovación y el emprendimiento, susceptible de ser vivero de *spin off* y *start ups*; f) disponer de una masa crítica adecuada de investigadores y de futuros egresados competentes en la transformación digital.

Y, si esta visión es correcta, ¿cómo es posible que la Universidad española no haya liderado la transformación digital de las administraciones públicas? Para que el lector entienda esta cuestión basta plantear un ejemplo muy sencillo. El artículo 27.6 de la derogada Ley de administración electrónica disponía:

> *"6. Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos."*

Los colectivos habituales relacionados con la administración universitaria suelen haber terminado sus estudios secundarios, disponen de un ordenador en el puesto o en el aula, suelen ser propietarios como mínimo de un Smartphone, un ordenador portátil y/o una tableta, y disponen de conectividad gratuita 9 meses al año en sus puestos, en aulas informáticas, o inalámbrica con Eduroam. ¿Cuántas universidades conoce el lector cuyo Reglamento de Administración Electrónica haya aprovechado para apostar por las notificaciones exclusivamente electrónicas? ¿Cuántas universidades españolas han implantado en sus procedimientos una política de papel cero? ¿No deberíamos rendir cuentas por no haber respondido a lo que debería esperarse de nosotros? ¿Es posible que pasado un decenio no lideremos todavía este campo? ¿Es posible que existiendo normativa de protección de datos desde 1992 no seamos capaces de cumplirla adecuadamente?

Curiosamente la respuesta a este aparente estado de cosas podría residir en el hecho de que la estructura universitaria se haya comportado exactamente tal y como se esperaría de una administración tradicional. Es muy probable que la resistencia al cambio haya modulado en gran medida la situación de hecho. Si se examinan con detalle las leyes 39 y 40/2015, veremos que el legislador, viene a sugerir que la universidad pública es algo distinto. Que, a pesar de su naturaleza jurídica no debería comportarse como un ayuntamiento, sencillamente porque no lo es.

La Universidad significa y aporta investigación, innovación, creatividad, conocimiento. No puede permitirse el lujo de comportarse de manera conservadora y reactiva. El liderazgo en su gobierno no puede tolerar comportamientos reluctantes al cambio, debe incentivar la transformación y ponerla en valor desde un punto de vista positivo. Existen tres elementos comunes en los modelos de gestión del cambio: la creación de un sentido de urgencia, buscar pequeños logros a corto plazo, ser capaces de gestar alianzas para la transformación. Cada una de las normas citadas, debería haber sido el acicate para alcanzar esos pequeños éxitos. Las leyes 39 y 40/2015, y el Reglamento General de Protección de Datos nos presentan una nueva oportunidad.

Sin embargo, el proceso de cambio y transformación digital se acelera hasta el punto de que prácticamente vivimos en un contexto de disrupción estructural. La urgencia es máxima, no es ni siquiera necesario crear un sentido de ella, sencillamente está ahí frente a nosotros. No es ni posible, ni admisible, que en una misma institución universitaria convivan de espaldas quienes diseñan inteligencia artificial o computación cuántica, y quienes gestionan la administración con hábitos del Siglo XIX. No es razonable que en el mundo de *HR Analytics*, la analítica del desempeño siga resolviéndose con informes y evaluaciones personales o de comisiones. No es viable que, en la sociedad de la *customización*, -en ese mundo de Amazon en el que lo que hace el cliente y lo que interesa al cliente es ley para el proveedor-, el estudiante o el personal deba orbitar la Universidad, deba comportarse a su servicio y no a la inversa.

Cada segundo, el proceso de transformación digital se acelera, y las oportunidades pasan de largo. La Universidad española se enfrenta de alguna manera al reto de decidir que desea si formar parte de los pioneros o de los regazados, si ser productor o consumidor de innovación, si liderar el cambio o simplemente cumplir la ley a regañadientes. Y esta no es una cuestión individual. Nadie duda que en nuestras universidades se encuentra el talento, están las mujeres y los hombres que desde la ciencia y la tecnología transformarán digitalmente este país. Pero esto no basta. Lo que debemos

decidir, es si nos basta con eso, o apostamos por una Universidad transformadora que lidere el proceso colectivamente como institución.

3. Transformación digital y Derecho

La transformación digital debe ser un proceso regido por el Derecho. En el anterior epígrafe se señalaron distintas normas que han ido incidiendo profundamente en esta materia desde diversos ámbitos. La tecnología debe tener en cuenta el ineludible valor que representa la dignidad humana y el respeto de los derechos fundamentales. En este sentido, en demasiadas ocasiones se nos dice que "*no cabe poner puertas al campo*", o que el legislador siempre va por detrás de la tecnología. Estos argumentos han sustentado en más de una ocasión una suerte de falacia de la inevitabilidad tecnológica, a la que se une otra, que vendría a afirmar que el Derecho opera como un freno a la ciencia y a la innovación.

La historia muestra en demasiadas ocasiones lo ilusorio de creer que el avance tecnológico sólo puede ser positivo y no causar daño. Europa despertó de la *Belle Époque*, culminación de un sueño de crecimiento económico y tecnológico, con la pesadilla de la Primera Guerra Mundial. El siglo XX, acreditó como nunca antes en la historia el potencial negativo de la innovación tecnológica al servicio de la destrucción de la entera humanidad. Incluso ahora que la transformación digital sirve también para poner en cuestión un modelo insostenible depredador de recursos, la resistencia al cambio se apoya en la tecnología buscando el siguiente salto en esa productividad malentendida.

Es radicalmente falso que el Derecho paralice la innovación. Desde el Derecho no podemos someter la innovación a un corsé que la asfixie. Pero tampoco podemos renunciar a un modelo democrático que pone en su centro la dignidad y la libre autodeterminación de las personas. Desde este punto de partida, no todo vale, no todo es posible, no todo es admisible. Existen reglas, algunas muy antiguas y la más elemental fue formulada por Ulpiano entre los siglos II y III: "*alterum non laedere*". No hacer el daño, actuar de buena fe, proteger a las personas. Son reglas sencillas y fáciles de entender. Sin embargo, en sociedades complejas esas reglas se traducen en ocasiones en regulaciones

que obligan a un cierto esfuerzo y que, obviamente, imponen costes de distinta naturaleza.

Esto sucede sin duda con el marco europeo de garantía de la privacidad. La Unión Europea ha diseñado un modelo altamente tuitivo que pivota sobre el derecho a la privacidad y el derecho fundamental a la protección de datos. La reciente jurisprudencia en los asuntos sobre el derecho al olvido (Google-Costeja), Schrems (Safe Harbour), Digital Rights Ireland y Comisión contra Hungría así lo demuestra. En nuestro contexto, se concibe claramente la privacidad como un espacio al servicio de los derechos de la personalidad que juega un papel central en el mundo digital como garantía instrumental de nuestro sistema de derechos y libertades.

De la llamada autodeterminación informativa, entendida con la capacidad de ejercer un control efectivo sobre nuestra información personal, y de sus principios y facultades dependen nuestros derechos. La digitalización de la sociedad conferirá a cada persona una identidad digital que crecerá y se desarrollará paralela a la del mundo físico. Procesos cada vez más intensivos en el manejo de información personal, y cada vez más automatizados gobernarán nuestras vidas. Hoy, debería ser tecnológicamente viable resolver una solicitud de ayuda al estudio de modo simultáneo al trámite de matrícula. Cada uno de los datos, de los parámetros necesarios, se encuentra disponible y los criterios de decisión responden a parámetros objetivables y programables. Sin embargo, el más leve error, una baja calidad de la información, produciría injusticias cercenando de raíz el derecho fundamental a la educación de una persona.

El ejemplo, anterior es relativamente banal. Los procesos de gestión o selección de personal mediante tecnologías analíticas, la evaluación del riesgo en el crédito o en el aseguramiento, la gestión de la circulación en vías urbanas, son ejemplos cotidianos de impacto de las tecnologías de la información en nuestras vidas. El reciente caso, Cambridge Analytica ha confirmado las peores expectativas sobre el llamado filtro burbuja y las capacidades de manipulación de la voluntad política de sociedades enteras.

Por ello, parece plenamente justificada la apuesta de la Unión Europea por una garantía fuerte del derecho fundamental a la protección de datos mediante una norma que regula los procesos de tratamiento de la información desde su diseño hasta su final, insertando en su ADN el respeto de los derechos fundamentales. Se trata además de un sistema que refuerza su modelo de garantías mediante las autoridades de protección de datos a las que confiere elevados poderes de "*enforcement*", y un marco sancionador altamente exigente.

Y ello nos obliga de una vez a desterrar una concepción formal de la protección de los datos personales. No "protegemos datos", no aplicamos lo que parece concebirse por algunos como una burocracia insufrible. Protegemos "personas", garantizamos sus derechos, aseguramos el pleno desarrollo de su personalidad en el contexto de una transformación digital acelerada.

4. La protección de datos desde el diseño y por defecto elemento fundamental de la transformación digital

El RGPD contiene tres principios nucleares. El primero de ellos se formula de modo muy breve en el inciso final del artículo 5 RGPD sobre principios aplicables a los tratamientos: somos responsables del cumplimiento de estos principios y debemos ser capaces de demostrarlo. Esto significa, la adopción de un nuevo enfoque, la responsabilidad proactiva, en la que la definición de los procesos de cumplimiento normativo, su documentación y mantenimiento resulta esencial.

A la Universidad ya no le basta con inscribir unos cuantos ficheros, y redactar políticas de privacidad. El enfoque ya no puede seguir siendo formal ni un minuto más. El derecho fundamental a la protección de datos es un derecho de naturaleza prestacional. En términos coloquiales, es un derecho que obliga a "hacer cosas", y desde luego no de cualquier manera. Obliga a hacer las cosas bien, poniendo los derechos de las personas en el centro del diseño. Y esto determina una apertura del conjunto de la organización universitaria al cumplimiento normativo en este ámbito.

En segundo lugar, el Reglamento General de Protección de Datos, obliga a un enfoque basado en el riesgo. La proactividad se encuentra al servicio de un derecho fundamental sometido a distintas presiones y susceptible de generar riesgos que afecten a la vida de las personas. Y aunque pueda parecer algo muy lejano a la actividad universitaria, resulta esclarecedor como errores banales pueden afectar significativamente a la vida de una persona. ¿Qué sucede si no se rectifica una nota a tiempo? ¿Es posible que una persona no pueda opositar? ¿Qué podría ocurrir si identificamos con nombres, apellidos y fotografías a los menores que participan en actividades de divulgación de la Universidad? ¿Qué sucederá si perdemos o revelamos datos de salud de personas que participan en un ensayo clínico o de trabajadoras víctimas de violencia de género? Una carpeta abierta a internet que contenga documentos de una preinscripción con datos de identificación como domicilios, DNI o cuentas bancarias, ¿podría facilitar suplantaciones de identidad?

Los ejemplos anteriores podrían ampliarse *ad infinitum* con escenarios mucho más graves. Como se señalaba anteriormente, protegemos personas. Y esas personas nos confían su bien más valioso: su información personal, sus esperanzas de futuro. De ahí, que el RGPD aporte un enfoque muy valioso a la gestión universitaria y que debe ser tenido rigurosamente en cuenta en todos nuestros esfuerzos.

Finalmente, estos principios cristalizan en un valor y una directriz estratégica esencial: la protección de datos desde el diseño y por defecto. Indica el Reglamento (UE) 2016/679:

> *"(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento*

de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

El artículo 25 RGPD concreta las estrategias básicas a adoptar por el responsable:

"Artículo 25. Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."

La teoría de la protección de datos desde el diseño y por defecto fue desarrollada en su día por la autoridad de Ontario Bajo la dirección de Ann Cavoukian y se articula a partir de 7 principios básicos:

1. Proactivo, no Reactivo; Preventivo no Correctivo

El enfoque de Privacidad por Diseño (PbD por sus siglas en inglés) está caracterizado por medidas proactivas, en vez de reactivas. Anticipa y previene eventos de invasión de privacidad antes de que estos ocurran. PbD no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron – su finalidad es prevenir que ocurran. En resumen, Privacidad por Diseño llega antes del suceso, no después.

2. Privacidad como la Configuración Predeterminada

Todos podemos estar seguros de una cosa – ¡Lo predeterminado es lo que manda! La Privacidad por Diseño busca entregar el máximo grado de privacidad asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier práctica de negocios. Si una la persona no toma una acción, aun así, la privacidad se mantiene intacta. No se requiere acción alguna de parte de la persona para proteger la privacidad – está interconstruida en el sistema, como una configuración predeterminada.

3. Privacidad Incrustada en el Diseño

La Privacidad por Diseño está incrustada en el diseño y la arquitectura de los sistemas de Tecnologías de Información y en las prácticas de negocios. No está colgada como un suplemento, después del suceso. El resultado es que la privacidad se convierte

en un componente esencial de la funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad.

4. Funcionalidad Total – "Todos ganan", no "Si alguien gana, otro pierde"

Privacidad por Diseño busca acomodar todos los intereses y objetivos legítimos de una forma "ganar-ganar", no a través de un método anticuado de "si alguien gana, otro pierde", donde se realizan concesiones innecesarias. Privacidad por Diseño evita la hipocresía de las falsas dualidades, tales como privacidad versus seguridad, demostrando que sí es posible tener ambas al mismo tiempo.

5. Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo

Habiendo sido incrustada en el sistema antes de que el primer elemento de información haya sido recolectado, la Privacidad por Diseño se extiende con seguridad a través del ciclo de vida completo de los datos involucrados – las medidas de seguridad robustas son esenciales para la privacidad, de inicio a fin. Esto garantiza que todos los datos son retenidos con seguridad, y luego destruidos con seguridad al final del proceso, sin demoras. Por lo tanto, la Privacidad por Diseño garantiza una administración segura del ciclo de vida de la información, desde la cuna hasta la tumba, desde un extremo hacia el otro.

6. Visibilidad y Transparencia – Mantenerlo Abierto

Privacidad por Diseño busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, esta en realidad esté operando de acuerdo a las promesas y objetivos declarados, sujeta a verificación independiente. Sus partes

componentes y operaciones permanecen visibles y transparentes, a usuarios y a proveedores. Recuerde, confíe pero verifique.

7. Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario

Por encima de todo, la Privacidad por Diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada, y facultando opciones amigables para el usuario. Hay que mantener al usuario en el centro de las prioridades.

Acreditar la aplicación de políticas de diseño basado en la privacidad constituye una exigencia normativa ineludible cuyo objetivo es doble. Primariamente permitirá probar "que se cumple". Sin embargo, lo esencial es asegurar que todos nuestros procesos se ordenan a garantizar los derechos fundamentales de los afectados cuya información tratamos. El mandato de aplicar la protección de datos desde el diseño y por defecto debe ir unido a la seguridad inserta desde el principio en el diseño.

Desde un punto de vista de orden práctico debemos tener en cuenta que el Reglamento General de Protección de Datos condiciona la adopción de distintas decisiones, -como por ejemplo ciertas políticas relacionadas con los menores de edad o las garantías del derecho la portabilidad-, con el Estado de la técnica la naturaleza del tratamiento y el coste de aplicación de la prescripción normativa en un contexto determinado. Adicionalmente tenemos que considerar de modo muy preciso la naturaleza del tratamiento a la hora de tomar decisiones estratégicas. La experiencia nos muestra que no es lo mismo tratar el porcentaje de discapacidad para conceder el beneficio de una matrícula gratuita, que gestionar la historia clínica completa de una persona con discapacidad para adoptar decisiones en materia de integración y de adaptación curricular.

Por otra parte, es fundamental destacar que el punto de vista de la protección de datos desde el diseño y por defecto implica un enfoque centrado en el riesgo para los derechos y libertades de las personas físicas, que además es contextualizado. Es decir, debemos tener en cuenta la naturaleza, el contexto y el ámbito de los fines del tratamiento a la hora de tomar decisiones. Además, es una decisión temporalmente acotada o temporalizada en el sentido de que no puede adoptarse en cualquier momento, sino que generalmente se tomará con carácter previo al menos en dos fases. La primera, la más inicial, en el proceso de diseño del procedimiento en virtud del cual trataremos los datos y de modo muy específico en el momento de determinar los medios del tratamiento. Después desplegaremos el principio de protección de datos desde el diseño y por defecto a partir del momento del desarrollo del propio tratamiento acompañándolo hasta su finalización, hasta la extinción o eliminación de los datos.

Este principio debe ser definido y concretado. No se trata únicamente de un cumplimiento epidérmico o meramente formal de la normativa, exige la adopción de medidas técnicas y organizativas apropiadas. Las decisiones en esta materia son funcionales. En primer lugar, suponen aplicar de forma efectiva los principios de protección de datos y tomar decisiones significativas entre las que destaca una: la minimización de los datos. El Reglamento General de Protección de Datos que obliga a acotar de modo muy preciso las categorías de datos y su volumen. De otro lado, es necesario integrar a lo largo de todo el tratamiento las garantías que nos permitirán cumplir con los requisitos del Reglamento. Y todo ello desde una filosofía funcionalmente ordenada a entender que ante todo protegemos personas, protegemos los derechos de las personas, no sólo sus datos personales.

5. Sin privacidad la transformación digital de la universidad no es viable

Llegados a este punto es necesario entender que la transformación digital requerirá de procesos altamente intensivos en el tratamiento de información personal. Y esta afirmación no solo debe leerse de modo lineal o literal. Alguna de las posibilidades que nos ofrecen la analítica de datos, el internet de los

objetos o la inteligencia artificial, implicará repercusiones inesperadas en la esfera de la personalidad y la vida privada de las personas. Cada terminal, cada objeto, conectado es una puerta abierta que hay que securizar. Cada dato por muy ajeno que sea a una persona si se contextualiza adquiere un valor material relevante. El código postal es un dato irrelevante. Sin embargo, si se vincula al análisis de los datos de contaminación de los últimos diez años, a los estudios epidemiológicos sobre incidencia de determinadas enfermedades, y se correlaciona con los hábitos de ejercicio de una persona, resulta un dato valiosísimo para el cálculo de la prima de un seguro de vida.

Desde este punto de vista, cumplir con el Reglamento (UE) 2016/679 resulta esencial para la institución universitaria en al menos tres niveles: gestión, investigación y transferencia.

▪ La gestión universitaria será digital o no será.

Y ello implica un rediseño estratégico multinivel. En primer lugar, los procesos de administración sin papel deben conducir a entornos altamente tecnificados para los que la protección de datos y la seguridad desde el diseño y por defecto constituyen un prerrequisito. Y ciertas metodologías preexistentes en el enfoque de estos proyectos no resultan sostenibles.

En más de una ocasión, los procesos de administración electrónica se han abordado desde un enfoque aristocrático, con visión de túnel. Ni se han tenido en cuenta las aspiraciones de los administrados, ni se han abordado desde un enfoque institucional global y transversal, ni se han tenido en cuenta las capacidades y requerimientos de los equipos internos de tecnologías de la información, y se ha buscado el soporte jurídico y de cumplimiento en protección de datos al final del proceso. Cuando un proyecto de digitalización incluye alguno, parte o todos estos errores, produce graves disfunciones. Y no es la menor la relativa a las objeciones que inevitablemente se plantearán en protección de datos y que podrían paralizar un proyecto completamente.

Por otra parte, no podemos abordar estos procesos desde una concepción administrativa decimonónica. Y no solo porque las formas de esa vieja

administración autoritaria deben cambiar, sino también, porque las universidades son algo más que una administración. Ofrecen una enorme diversidad de servicios y prestaciones en las que no se ejercen potestades públicas, y en las que el respeto de la autonomía y de los derechos de sus usuarios es fundamental. No es admisible que el mayor *spammer* para un o una estudiante sea su propia universidad. La actividad cultural y promocional de la universidad debe fidelizar y comprometer, y esto en protección de datos tiene un nombre: consentimiento explícito mediante una clara acción afirmativa.

▪ En la investigación debe garantizar el cumplimiento del Reglamento (UE) 2016/679.

El volumen de investigación sujeto a las previsiones del Reglamento General de Protección de Datos es mayor de lo que usualmente se cree. No se trata exclusivamente de los estudios de caso en el área de Ciencias de la Salud. El impacto puede ser muy significativo para cualquier estudio poblacional en sociología, economía, marketing, biología… Ni siquiera escaparían ámbitos como el de las matemáticas ya que "la transparencia del algoritmo" resulta jurídicamente relevante.

Y este impacto se está traduciendo en la realidad. La mayor parte, si no todas, las convocatorias de investigación de la Comisión Europea, incorporan un paquete de privacidad, junto al tradicional bloque de ética en la investigación. Y ello supone que se exigen condiciones que aseguren que o los datos son completamente anónimos, o que han sido recabados y tratados conforme al RGPD, y en determinados casos se exige una evaluación de impacto relativa a la protección de datos. Este compromiso con la privacidad se extiende a las más prestigiosas revistas científicas que requieren acreditar condiciones de cumplimiento normativo en esta materia e incluso su revisión y confirmación por un comité de ética.

▪ La transferencia, el desarrollo de productos y aplicaciones, debe cumplir con la norma.

No es inusual que la transferencia científica cristalice en productos y aplicaciones que se ponen a disposición de la comunidad. Y tampoco lo ha sido históricamente que la privacidad no haya sido tenida en cuenta en su diseño y desarrollo. Ello implica, cuando existe un proceso de validación y autorización por la universidad, la imposibilidad de autorizar el producto del que se trate. Baste un sencillo ejemplo: una aplicación móvil que no se haya desarrollado cumpliendo con las especificaciones a las que obligue el principio de protección de datos y la seguridad desde el diseño y por defecto, la normativa que regula el uso de *fingerprints* como las cookies, y los permisos de acceso al terminal que impone la Directiva 2002/58/CE, no debería estar disponible en Google Play o Apple Store avalada por la marca de la universidad de la que se trate. Lo contrario, supondría que institucionalmente se aprueba y avala un dispositivo que vulnera derechos fundamentales, amén de asumir la condición de "responsable" en términos de RGPD.

▪ La privacidad en riesgo.

La conclusión a la que cabe llegar es bien sencilla: la privacidad es sin duda una inversión que va a producir retornos y debe proyectarse sobre todos los procesos. No es posible concebir el cumplimiento del Reglamento (UE) 2016/679 como una cuestión puramente accesoria, incluso como una materia ciertamente antipática y generadora de resistencia al cambio.

Y esta inversión no sólo alcanza a los procesos sino también a la inversión en recursos humanos. Desgraciadamente es probable que la protección de datos haya sido desatendida. En un número significativo de universidades no existen perfiles profesionales directamente vinculados a esta materia, y allí donde existen no siempre cuentan con el respaldo del liderazgo en el gobierno de la institución. Y en el horizonte del 25 de mayo de 2018, el número de delegados de protección de datos nombrados es muy bajo, y es altamente probable que se produzca un gran número de externalizaciones.

En este ámbito, y como conocedor de la materia, desde la autoría de este trabajo, debe cumplirse con el ineludible compromiso ético de alertar y enumerar ciertos peligros:

▪ Es fundamental reducir la resistencia al cambio de los cuadros directivos. Ni la protección de datos, ni sus profesionales, amenazan sus tareas, ni van a alterar significativamente sus procesos. Ni protección de datos, ni seguridad de la información son el enemigo, aunque a veces se les trate como si lo fueran. Aportarán al contrario seguridad, calidad y confianza.

▪ Es esencial iniciar procesos formativos que empoderen al conjunto de la comunidad universitaria tanto en lo relativo a la privacidad como a la seguridad. Aun a costa de exagerar, esta es una precondición para tener éxito en la transformación digital.

▪ La externalización no puede dejarse en manos de empresas que desconozcan la enorme complejidad jurídica y técnica de una universidad. Todos no sirven, y la Universidad no puede caer en las mismas trampas que las PYME de nuestro país y optar por asesoramientos de baja calidad a bajo coste. Ello les permitirá sencillamente proporcionar una apariencia de cumplimiento, no cumplir.

▪ Es fundamental implementar políticas de seguridad verdaderamente eficientes y que comprometan al conjunto de la organización de modo efectivo.

▪ En el caso de las universidades públicas debe compensarse la carencia de estímulo sancionador con políticas proactivas de compromiso y empoderamiento para el cumplimiento de la normativa sobre privacidad.

La Universidad, es una institución singular en cuyo espejo se ha mirado históricamente la sociedad. La institución universitaria a lo largo de los siglos ha sido catalizadora de ideas y pensamiento, crisol del conocimiento, expresión de los más altos valores, y guía para las comunidades en las que se inserta. En nuestro país, como en tantos otros, además ha desempeñado un papel de liderazgo en la defensa y reivindicación de los derechos humanos. El

compromiso con la privacidad en la transformación digital de la Universidad debe formar parte consustancial de nuestros esfuerzos. Obviarlo no sería otra cosa que traicionar nuestra esencia, traicionar a la sociedad para la que existimos y a la que deberíamos servir.

Bibliografía

- BOSTROM, Nick. *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press, 2014.

- BRANDT, Richard. *Un click. Jeff Bezos y el auge de amazon.com*. Barcelona, Gestión, 2000.

- CAVOUKIAN, Ann. *The Seven Foundational Principles*. [Fecha de consulta: 27/03/2018]. Disponible en https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/ También disponible en https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf

- FORD, Martin. *El ascenso de los robots*. *La amenaza de un futuro sin empleo*. Ciudad de México, Paidós, 2016.

- KAPLAN, Jerry. *Abstenerse humanos*. TEELL, 2016.

- LESSIG, Lawrence. C*ode version 2.0*. New York, Basic Books. Perseus Books Group. [Fecha de consulta: 21/05/2017]. Disponible en http://pdf.codev2.cc/Lessig-Codev2.pdf También disponible en http://www.articaonline.com/wp-content/uploads/2011/07/El-c%C3%B3digo-2.0-Lawrence-Lessig.pdf

- LÓPEZ DE MÁNTARAS BADÍA, Ramón; MESSEGUER GONZÁLEZ, Pedro. *Inteligencia Artificial*. Madrid, Catarata-CSIC, 2017.

- MANYIKA, James. *What's Now and Next in Analytics, AI, Aad Automation*. McKinsey Global Institute. Briefing Note May 2017. 6. [Fecha de consulta: 11/04/2018]. Disponible en https://www.mckinsey.com/global-themes/digital-disruption/whats-now-and-next-in-analytics-ai-and-automation

- MARTÍNEZ MARTÍNEZ, Ricard. Big data, investigación en salud y protección de datos personales: ¿Un falso debate? En *Revista Valenciana d'Estudis Autonòmics*, n. 62, 2017, p. 235-280. [Fecha de consulta: 11/04/2018] Disponible en http://bit.ly/2EDdjig

- MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data*. Madrid, Turner, 2013.

- NADELLA, Satya. *Pulsa actualizar*. Madrid, Harper Collins, 2017.

- O'NEIL, Cathy. *Weapons of Math Destruction*. New York, Crown, 2016, p. 3.

- PARISER, Eli. *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos*. Barcelona, Taurus, 2017.

- RODOTÀ, Stefano. *Il mondo nella rete. Quali i diritti, quali i vincoli*. 6ª ed. Roma, Laterza, 2018.

- SCHWAB, Klaus. *La cuarta revolución industrial*. Barcelona, Debate. 2016.

- UNITED KINGDOM GOVERNMENT. *UK Digital Strategy 2017*. [Fecha de acceso: 11/04/2018] Disponible en https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy

Autoridades de protección de datos personales

- AEPD. *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, [Fecha de consulta: 11/04/2018]. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

- CNIL. *Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*. Diciembre 2017. [Fecha de consulta: 11/04/2018]. Disponible en https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

- WORKING PARTY ARTICLE 29. *Guidelines on Data Protection Officers* ('DPOs') (wp243rev.01). [Fecha de consulta: 11/04/2018]. Disponible en http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

- WORKING PARTY ARTICLE 29. *Guidelines on Data Protection Impact Assessment* (DPIA) (wp248rev.01). [Fecha de consulta: 11/04/2018]. Disponible en http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

Jurisprudencia

Tribunal de Justicia de la Unión Europea, asuntos:

- C-131/12 - Google Spain y Google.

- C-288/12 - Commission v Hungary.

- C-293/12 - Digital Rights Ireland y Seitlinger y otros.

- C-362/14 – Schrems.

Blogsfera. Artículos del autor

- *Las medidas de seguridad en el Reglamento general de protección de datos*. [Fecha de consulta: 11/04/2018]. Disponible en http://lopdyseguridad.es/GDPR1/

- *¿Por qué debería tener éxito GDPR en la Administración Pública Española?* [Fecha de consulta: 11/04/2018]. Disponible en http://lopdyseguridad.es/triunfogdpradmon/

- *¿Por qué podría fracasar GDPR en la Administración Pública Española?* [Fecha de consulta: 11/04/2018]. Disponible en http://lopdyseguridad.es/fracasogdpradmon/

- *10 Lecciones aprendidas en el Curso de formación en Auditoría Tecnológica, de Seguridad y Legal de Sistemas de Información*. [Fecha de consulta: 11/04/2018]. Disponible en http://lopdyseguridad.es/10lecciones/