Caso de estudio sobre GDPR aplicado en Sistemas de Gestión Académica

Lía Hebe Molinari[1], María Alejandra Sebastián[1], Nadia Estefanía Vázquez[1]
[1]Universidad Nacional de La Plata - Facultad de Informática
50 y 120 - La Plata, Argentina
lmolinari@info.unlp.edu.ar, asebastian@linti.unlp.edu.ar , nvazquez@linti.unlp.edu.ar

Resumen: El reglamento europeo para la protección de los datos (General Data Privacy Regulation, GDPR), fue publicado en Mayo de 2016 y comenzó a aplicarse a partir del 25 de Mayo de 2018. Como toda nueva normativa su puesta en vigor exige su cumplimiento, e inevitablemente interpela a las organizaciones en cuanto a los cambios formales, administrativos y culturales que conlleva; cuándo y cómo se debe aplicar, qué nuevos roles incorpora en la estructura organizacional, cómo y a quién se informa de dichos cambios son temas que se deben resolver. Este artículo aborda un caso de estudio en el ámbito académico nacional argentino poniendo en evidencia cómo una regulación europea tiene incidencia en repositorios locales.

Palabras Clave: Reglamento General de Protección de Datos. GDPR. Datos Privados. Derechos fundamentales. Protección de datos personales.

1 Introducción

Uno de los mayores retos con los que nos hemos enfrentado en los últimos años es la regulación de los datos que circulan en la red, es decir, el establecimiento de mecanismos para la protección integral de los datos personales de cualquier ciudadano que haya quedado almacenado en un archivo, registro, banco de datos u otro medio externo, ya sea público o privado [1].

En Europa, el 25 de Mayo de 2018 entró en vigencia el nuevo reglamento 2016/679 del Parlamento Europeo y del Consejo (en inglés, Global Data Privacy Regulation, conocido como GDPR) [2], que dispone que el flujo de datos personales hacia países terceros podrá hacerse libremente, siempre y cuando esos países cuenten con legislación que garantice, a juicio de la Comisión Europea, un nivel de protección adecuado. Tras la finalización de la reforma de la normativa de protección de datos, la Unión Europea (UE) asume que la protección y el intercambio de datos personales no son mutuamente excluyentes, y concluye que un sistema sólido de protección de datos facilita la circulación de los mismos en cualquier ámbito (educativo, económico, etc.) y/o país. Por esto, la Comisión al Parlamento Europeo y al Consejo, ha emitido el comunicado “Intercambio y protección de los datos personales en un mundo globalizado”, donde proporciona una serie de mecanismos para permitir las transferencias internacionales de datos. El objetivo es garantizar que, cuando se

transfieran datos personales de ciudadanos europeos a terceros países, se mantenga el mismo nivel de protección con respecto a los mismos.
Este reglamento exige a los países que están por fuera de la UE, analizar y establecer medidas sobre datos inherentes a ciudadanos europeos que puedan alojarse en sus repositorios y a reveer sus legislaciones en el contexto de la protección de los datos personales.
En paralelo a la aprobación del GDPR, en Argentina se han producido cambios normativos. A comienzos del 2000, la Dirección Nacional de Protección de Datos Personales elaboró un anteproyecto de reforma de la legislación, sobre la cual recientemente se produjo un importante avance cualitativo alineado con los estándares internacionales vigentes, al otorgar desde fines de 2017 el carácter de autoridad de aplicación en materia de protección de datos personales a un organismo autárquico y con autonomía funcional como es la Agencia de Acceso a la Información Pública (AAIP). La AAIP es el organismo nacional que tiene como función el garantizar el cumplimiento de la Ley de Acceso a la Información Pública, la protección de los datos personales y el funcionamiento del Registro Nacional "No Llame".

2 Reglamento General de Protección de Datos (GDPR)

GDPR ha reforzado los derechos relativos a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos, añadiendo nuevos elementos que mejoran la capacidad de decisión y control de los ciudadanos sobre sus propios datos.
El reglamento busca proteger los datos y la forma en la que las organizaciones los procesan, almacenan y destruyen cuando ya no son requeridos. Establece normas más estrictas, como el autocontrol o control individual, o cómo las compañías pueden usar la información que está directa y personalmente relacionada con los ciudadanos. Estas normas rigen además lo que sucede si se viola el acceso a los datos personales de un individuo y las secuelas (penalidades) que las organizaciones pueden padecer en tal caso [3].
En el tiempo que regía la Directiva de Protección de datos EU, cuando una entidad sufría una filtración no estaba obligada a informar de ella. Sin embargo debido a la cantidad de situaciones que han puesto en evidencia los escasos controles orientados a proteger nuestra información más privada, las entidades se vieron en el compromiso de dar las explicaciones necesarias, especialmente acerca de la forma en que la filtración afectó directamente a sus clientes.
El GDPR va a tener un impacto significativo para las organizaciones y su forma de administrar los datos, con sanciones para aquellas entidades que provoquen una violación que pueden llegar a una multa que involucre hasta un 4% de los ingresos globales.

2.1 Alcance del GDPR

Por medio de esta regulación, la UE quiere dar más control sobre los datos personales y la utilización de las mismas, y a las entidades un entorno jurídico más simple y más claro para operar, haciendo que la ley de protección de datos sea idéntica en todo el mercado.
La aplicación de la reglamentación se extiende a [4]:

- Organizaciones con presencia física en al menos algún país miembro de la Unión Europea.
- Organizaciones que procesan o almacenan datos sobre individuos que residen en la Unión Europea.
- Organizaciones que utilizan servicios de terceros que procesan o almacenan información sobre individuos que residen en la Unión Europea.

2.2 ¿Qué se entiende por datos personales?

La era digital que transitamos plantea diariamente desafíos complejos relacionados con la recopilación y uso de la información personal en áreas muy distintas pero que a su vez se entrecruzan, como la economía, las políticas, las telecomunicaciones, la salud. Desde la perspectiva legal, los datos y la información personal online siempre se han enfrentado al desafío de garantizar a los consumidores-usuarios la misma protección y seguridad jurídica que en un mercado físico. El significado del concepto de dato personal no es uniforme. A continuación se detallan definiciones de "datos personales" de distintas legislaciones [5]:

- La Ley 25.326 de Protección de los datos personales de Argentina, en el Art.2 define a los datos personales como *"Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"*.

- El GDPR en el Art.4 del Reglamento expresa que: «***"datos personales"**: toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*».

Es decir, si la persona es identificable, toda la información que se tenga sobre ella serán datos personales**.** En la actualidad, una persona está directamente identificada por su "nombre y apellido". Aunque en ocasiones el nombre y apellido no son suficientes para identificar a una persona y deberán complementarse con otros datos, como una dirección, una foto de perfil o un número de cobertura social. En esos casos en que los identificadores que disponemos no permiten a nadie individualizar a una persona determinada, pero al combinarlos con otros datos (tanto si tenemos conocimiento de ellos como si no) es posible distinguir a la persona de otras, entenderemos que la persona es *indirectamente identificable*. También puede

considerarse a una persona identificada cuando se disponga de otros identificadores que nos permitirán individualizar a una persona, crear un perfil y atribuirle decisiones. Las definiciones presentadas se limitan a la protección de las personas físicas vivas, excluyendo a las personas fallecidas. El reglamento expresa en el Art 27: *"El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de éstas"*.
De este análisis surge una clasificación de datos que se debe tener en cuenta para la protección de la misma:

1. Básicos: toda información relativa a una persona.
2. Especiales: los datos especiales son los que poseen contenido de origen étnico o racial, datos genéticos o biométricos; convicciones religiosas o filosóficas, opiniones políticas, afiliación sindical; datos de Salud, vida sexual u origen sexual. (art.9 GDPR)
3. Penales: datos relativos a condenas y delitos penales o medidas de seguridad afines.

2.3 Derechos

La regulación otorga a los involucrados el control sobre qué información pueden utilizar que esté directamente vinculada con ellos y les proporciona ocho derechos específicos. Estos derechos adquieren el nombre de "*Derechos de Sujetos de Datos*". Esto significa que No son entidades pasivas que no tienen más opción que aceptar lo que sea que suceda con sus datos personales, sino que son propietarios independientes de sus datos y determinan cómo quieren que sean usados.
Los derechos que proporciona la misma son: derechos de acceso (art.12 y art.15 GDPR); de rectificación (art.12 y art.16 GDPR); derecho de oposición (art.12 y art.21 GDPR); derecho de supresión ("al olvido") (art.12 y art.17 GDPR); derecho a la limitación del tratamiento (art.12 y art.18 GDPR); derecho a la portabilidad (art.12 y art.20 GDPR); derecho a no ser objeto de decisiones individuales automatizadas (art.12 y art.22 GDPR) y derecho de información: (art.12, art.13 y art.14 GDPR).

2.4. Tratamiento y Consentimiento

Uno de los cambios más importantes que impone la regulación fuertemente es el consentimiento del usuario sobre sus datos, definiendo en el artículo al término "consentimiento del interesado" como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.*" (art.4 GDPR).

2.4.1 Aplicación de los Principios del tratamiento

El reglamento dedica el capítulo 2 a los "Principios" y especifica que deben ser aplicados a toda la información relativa a una persona y los datos que lo identifiquen.
El tratamiento debe ser lícito, es decir legítimo, para ello debe definirse un contrato con el interesado, o celebrar un consentimiento explícito para fines específicos. Si los datos se obtienen de un acceso público, entonces su procedencia debe ser de una fuente pública o expresamente el interesado los ha hecho públicos.

El sujeto obligado a verificar el cumplimiento de todos estos requisitos será el Responsable del Tratamiento que además deberá ser capaz de demostrar de forma activa que cumple con ellos: «responsabilidad proactiva».

2. 4.2 Consentimiento y Consentimiento Explícito

El consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento de los datos.
A partir de la vigencia del GDPR, la forma que más se utilizaba era utilizando una clara acción afirmativa como, por ejemplo, marcar una casilla de una web, el movimiento físico del teléfono, grabaciones de voz. Ahora el tratamiento sólo será lícito si un individuo dio el consentimiento para uno o varios fines específicos (art.6.1 GDPR). Y el consentimiento deberá ser explícito para el tratamiento de categorías especiales de datos (art.9.2ª GDPR).
La diferencia del consentimiento explícito con el general radica en que el primero no debe dejar lugar a la libre interpretación, siendo confeccionado de manera precisa y clara, y los responsables de los datos tendrán que asegurarse de la obtención de dicho consentimiento de manera indiscutible. Tal y como ha especificado la oficina británica (ICO), "la declaración para obtener el consentimiento explícito debe especificar la naturaleza de los datos a recopilar, los detalles de la decisión automatizada y sus efectos o los detalles de los datos que se van a transferir y los riesgos de tal transferencia".

2.5 El enfoque de riesgo

La transformación tecnológica que se ha estado desarrollando, y sigue aún, en el ámbito del tratamiento de la información personal producto de la entrada en vigencia del GDPR, ha producido que las entidades públicas o privadas deban estar preparadas para adoptar las medidas técnicas y organizativas adecuadas al uso de los datos "no anonimizados" no solo para aquellas pertenecientes a la UE sino que a todas que salvaguarden información de ciudadanos europeos. Como piezas claves para que convivir con la nueva legislación, las entidades deberían analizar los riesgos que conllevan la utilización de datos personales de sus usuarios, y por consiguiente satisfacer la necesidad de creación de una figura profesional responsable del buen uso de esos datos [6].
Para las entidades que traten datos con un nivel de riesgo elevado, deberán establecer las medidas que sean necesarias para garantizar los derechos y libertades de las personas [7].

3 Caso de estudio: Sistemas de gestión académica y cumplimiento GDPR

EL GDPR se aplica al Espacio Económico Europeo (EEE), que incluye todos los países de la Unión Europea, más Islandia, Liechtenstein y Noruega. Cuando los datos personales se transfieren fuera del EEE, la protección que ofrece el GDPR debe viajar con los datos. Esto significa que, para exportar datos al extranjero, las entidades deben garantizar que existen determinadas garantías.

El GDPR ofrece un conjunto variado de mecanismos para transferir datos a terceros países. Dichas transferencias están permitidas en los casos siguientes:

1. la UE considera adecuadas las protecciones del país, o
2. la entidad que trata los datos, por ejemplo, toma las medidas necesarias para ofrecer garantías adecuadas, como incluir cláusulas específicas en el contrato celebrado con el importador de fuera de la UE de los datos personales, o
3. la entidad, por ejemplo, se basa en motivos específicos («excepciones»), para la transferencia como el consentimiento del interesado.

Sin embargo, para poder realizar transferencias internacionales sin requerir ninguna autorización específica, es cuando la Comisión de la UE decida el nivel de adecuación en relación con el tercer país o un territorio o un sector específico del mismo, o con una organización internacional.

La decisión de adecuación es una resolución adoptada por la Comisión que garantiza que la transferencia internacional de datos posee un nivel de protección suficiente. La Comisión podrá derogar, modificar o suspender cualquier decisión de adecuación sin efecto retroactivo. En la actualidad, Argentina se encuentra dentro de los países que tienen una decisión de adecuación.

3.1 Planteo del Problema

Al contemplar esta situación y como el GDPR impactaría en Argentina, nuestro foco se dirigió a lo que sucede dentro del ámbito educativo y las herramientas de soporte que se utilizan para la gestión de los datos.

La cuestión surge a partir de que la Constitución Nacional Argentina establece que cualquier extranjero que consiga la residencia puede estudiar en las universidades públicas, con los mismos derechos que un ciudadano nacido en el país.

En los últimos años, el ingreso y egreso de alumnos extranjeros en las universidades argentinas incluyendo alumnos que son ciudadanos de países de la UE. En consecuencia, como se describió en la sección 2 del artículo, se debe realizar un análisis de los sistemas de gestión ya que almacena información de ciudadanos de la UE, y verificar que se cumplen con todas los puntos detallados en el GDPR, siempre y cuando no se contradiga con la normativa Argentina, el Habeas Data[5].

3.2 Análisis del problema

3.2.1 Funcionalidad del Sistema de Gestión Académica

Un Sistema de Gestión Académica (SGA) es una herramienta integrada que permite registrar y administrar todas las actividades académicas de la universidad y sus dependencias académicas, desde que un alumno se inscribe hasta que egresa. El objetivo del SGA es la administración de las tareas académicas en forma óptima y segura, con la finalidad de obtener información consistente para los niveles operativos y directivos.

El SGA no es un sistema en sí mismo, sino que es un conjunto de diferentes aplicaciones que interactúan entre sí, y que comparten la información que almacena cada una.

Las principales prestaciones que cuenta el sistema son:

- Almacena la totalidad de la oferta educativa de la institución: carreras, certificaciones, competencias, títulos, etc. / Flexibilidad de planes de estudio.
- Presenta una organización por módulos relacionados a la gestión: matrícula, asistencia, cursadas, egresos, etc.
- Almacena los registros de directa relación con la vida del alumno dentro de la institución, desde la postulación del aspirante hasta el circuito de egreso del mismo.
- Almacena los Registros del docente, desde sus antecedentes hasta asistencia en las distintas instancias.
- Gestión de múltiples perfiles de datos (información) y funcionales (sobre operaciones).
- Personalización de reportes, operaciones y módulos.

Como se puede notar, las funcionalidades del SGA requieren que se registre mucha información sensible y privada de las personas que intervienen en los diferentes procesos administrativos.
En el análisis de los tipos de datos que se almacenan de los diferentes actores que utilizan el sistema y dado un perfil básico, habitualmente un SGA registra datos del tipo:

- Datos personales
- Datos familiares
- Datos acerca de cobertura social
- Datos secundarios
- Fuente de financiamiento de estudios
- Situación laboral
- Deporte
- Idioma y nivel
- Discapacidad

Teniendo en cuenta toda esta información y la exigencia de la regulación sobre la obligación de informar a las personas interesadas sobre el tratamiento de sus datos, un SGA debería, en una primera instancia, verificar si con respecto al tipo de información que almacena, cumple con los ítems detallados:

1. Información Básica:
    a. Se notifica el responsable de tratamiento, es decir a la persona encargada de la gestión de los datos y de coordinar la administración del almacenamiento de los mismos?
    b. Se realiza una descripción sencilla de los fines del tratamiento?
    c. Se notifica los plazos y el criterio de conservación de los datos?
    d. Se hace referencia sobre los derechos que tiene los involucrados?

2. Información detallada:
    a. Se notifica la posibilidad de destinatarios de los datos personales?
    b. Existe un interés legítimo en el responsable?
    c. Se notifica políticas para decisiones automatizadas y/o perfiles?

d. Se notifica el derecho al retirar el consentimiento prestado?

En ambos aspectos esta información debe proporcionarse en el momento en el que se soliciten los datos.
Además un SGA debería informar si:

1. se recogen los datos personales con fines determinados,
2. los datos personales se mantienen exactos,
3. se informa del derecho a solicitar la rectificación o supresión de sus datos.

En todos estos casos, el sistema estará obteniendo datos personales de los usuarios, por lo que, en primera medida es necesario que inserte un aviso legal para dar cumplimiento al deber de información y consentimiento. Es necesario que los usuarios **acepten expresamente** dicho aviso.

3.2.2 Sistemas de gestión académica universitaria y el Consentimiento.

Dado que el GDPR pone en énfasis el consentimiento de los involucrados, y que los SGA registran mucha información sensible, debería realizarlos siguientes preguntas:

1. ¿El SGA gestiona el concepto de consentimiento de forma clara e independiente compatible con el GDPR?
2. ¿Hay algún registro o manera en la que se puede demostrar que el usuario (alumno, docente, etc...) dio su consentimiento para el tratamiento?
3. ¿El SGA solicita el consentimiento de forma inteligible y de fácil acceso para aquel que va a registrarse en el sistema?
4. ¿Se utiliza un lenguaje claro y sencillo en el consentimiento?
5. ¿Se le informa previamente en el consentimiento al usuario la información (o datos personales) que será almacenada recabar?
6. ¿El SGA implementa algún mecanismo que permita prescindir del consentimiento con la misma facilidad que se acepta?
7. ¿El SGA ofrece los medios para retirar el consentimiento en cualquier momento?
8. ¿Se recaba el libre consentimiento?

3.2.3 Recomendaciones para cumplimiento del GDPR en SGA

Más allá de las medidas de seguridad que el SGA implemente, es importante realizar una evaluación acerca del cumplimiento de la normativa, de manera que se asegure de adoptar una serie de medidas de seguridad, de carácter técnico y organizativo para proteger todos los datos.
Con el lineamiento en la regulación un SGA debería:

- Antes de implementar nuevas medidas de seguridad o reforzarlas, aquellas personas que tengan el rol para tratar los datos personales deben llevar a

cabo una evaluación de los riesgos para garantizar un nivel de seguridad adecuado.

- Si se produce una quiebra de seguridad que afecte los datos personales de los usuarios, poniendo en riesgo sus derechos y libertades, con carácter general, deberán contar con un mecanismo para comunicar tal quiebre se seguridad y los efectos que produjo o que pueden llegar a producir.
- Si el SGA va a realizar tratamientos que supongan de alto riesgo para los derechos y libertades de los usuarios, antes de empezar a ejecutarlo, deberá realizar una evaluación de impacto relativa a la protección de datos.
- El SGA deberá tener en cuenta la 'Privacidad por diseño' y 'Privacidad por defecto'.
- Deberá incluir medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento de los datos
- Deberá contar con medidas de seguridad para evitar pérdida, destrucción o daño accidental
- El SGA en todo proceso de análisis deberá tener en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado.
- Deberá tener un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas

4 Conclusiones y trabajos futuros

GDPR regula la forma en que las entidades tratan y gestionan los datos personales; y al mismo tiempo provee mecanismos para la transferencia de datos transfronterizos. En materia de protección de datos, de acuerdo a esta legislación europea, todo lugar que guarde información sensible sobre ciudadanos europeos debe ajustarse a la misma. GDPR representa una nueva oportunidad para mejorar la gestión de los datos personales y, posteriormente, aumente la confianza de todas las personas que intervienen.

Como trabajo futuro se propone analizar GDPR en otro ámbitos, teniendo un principal cuidado en ámbitos donde se registren datos de menores considerando que la regulación plantea un mayor cuidado de los mismos.

En el ámbito de la gestión pública son varias las dependencias que están analizando el cumplimiento de GDPR. En este caso hay mucho por hacer definiendo una metodología que incluya el proceso de análisis de riesgo, tratamiento de los datos, consentimiento, análisis del puesto de PDO, análisis del tratamiento de los datos y mejoras de diseño en el sistema.

Referencias

[1] Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados. https://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf

[2] Dictamen 4/2007 sobre el concepto de datos personales http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. http://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[4] Comunicación de la comisión al parlamento europeo y al consejo.https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0007&from=ES

[5] Ley de Protección de los Datos Personales. http://www.jus.gob.ar/media/3210629/anteproyecto_de_ley_de_protecci_n_de_los_datos_personales.pdf

[6] Guía práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

[7] Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al GDPR https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

[8] Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. http://44jaiio.sadio.org.ar/sites/default/files/sid227-249.pdf

[9] PROTECCIÓN DE DATOS Luis Felipe López Álvarez. http://www.isaca.org/chapters7/Madrid/Events/Eventos/Documents/20180320%20AGRC18/20180320%20ISACAMadrid%20AGRC18%20Luis%20Felipe%20Lopez.pdf