Incumplimiento del deber de notificación de información: en la búsqueda de su sustento.

"*Entonces… entonces crees que puedes decirlo*", "Ojalá estuvieras aquí", de Pink Floyd

Deberías decirlo.

Dar malas noticias nunca es fácil. Darlas casi en tiempo real es aún más difícil. Y esto es exactamente lo que la mayoría de las leyes obligan a hacer cuando ocurre un incidente de seguridad de la información: notificar a miles o millones de personas en un período de tiempo muy limitado que sus datos personales han sido robados y probablemente mal utilizados.

Un incidente de seguridad de la información podría convertirse en una violación de datos. Así ocurre cuando hay una violación de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado o accidental a los datos personales transmitidos, almacenados o procesados.

Por lo general, notificar la violación de datos supone un gran peso para la organización que ha sido atacada, ya que tendrá que lidiar tanto con el ataque como con un proceso de notificación que puede ser largo, logísticamente complicado y muy probablemente costoso.

Así, la cuestión es si es razonable imponer tal deber a una organización que atraviesa una crisis que puede tener consecuencias devastadoras en sí misma, al mismo tiempo que se produce este calvario. Por difícil que sea, este deber radica en el derecho fundamental de una persona cuyos datos han sido violados a conocerlo lo antes posible. El propósito de este ensayo es dejarlo claro, mostrar por qué una tarea tan gravosa es sostenible y, al final del día, simplemente justa.

En realidad, esta obligación se está extendiendo por todas partes a medida que más y más países promulgan leyes que la imponen. De este universo de varios cuerpos de leyes, vamos a analizar sólo uno como muestra: el Reglamento General de Protección de Datos (RGPD) de la Comunidad Europea de 2018.

A continuación, abordaré el problema mencionado anteriormente. Luego, consideraré los diferentes derechos y responsabilidades, algo conflictivos, que deben tomarse en consideración y equilibrarse cuidadosamente para finalmente llegar a una conclusión.

Estado del arte: una muestra de legislación.

Se ha promulgado ampliamente nueva legislación que hace cumplir el deber de notificación. Dado que hacer un análisis legislativo de país a país excede con creces el alcance de este trabajo y posiblemente pondrá a prueba la paciencia de cada lector hasta sus límites, me centraré en el cuerpo de leyes que es el más influyente en este tema, la Ley General de Protección de Datos de 2018. Reglamento (GDPR) promulgado por la UE. Decir que este Reglamento se ha copiado en su totalidad desde entonces para cada reglamento que siguió es un poco extremo. Por otro lado, decir que echar un vistazo a sus reglas puede darnos una visión completa sobre el tema es muy correcto.

El Reglamento introdujo un requisito para que las organizaciones informen las infracciones de datos personales a la Autoridad de Supervisión correspondiente, tal como se define en el artículo 55, cuando la infracción presenta (plantea) un riesgo para las personas afectadas. Las organizaciones deben hacer esto dentro de las 72 horas posteriores a la toma de conocimiento de la infracción. En concreto, el artículo 33, 1. del RGPD establece:

“En caso de violación de datos personales, el responsable del tratamiento notificará sin demora indebida y, cuando sea factible, a más tardar 72 horas después de haber tenido conocimiento de ello, la violación de datos personales a la autoridad de control competente de conformidad con el artículo 55, a menos que la Es improbable que la violación de datos personales resulte en un riesgo para los derechos y libertades de las personas físicas. Cuando la notificación a la autoridad de control no se realice en el plazo de 72 horas, se acompañará de los motivos de la demora.”

Además del deber de “notificación” a la Autoridad de Control antes mencionado, el artículo 34 de la RGPD impone un deber de “comunicación” al interesado:

“Cuando sea probable que la violación de los datos personales dé lugar a un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará la violación de los datos personales al interesado sin demoras indebidas”.

Así, la ley establece que, dependiendo de las consecuencias de la violación de datos, tanto las autoridades de control como los sujetos deben ser notificados por la organización de que se produjo la violación. Sin embargo, con respecto a los sujetos, la notificación no es obligatoria, siempre que la violación de datos personales sea "*improbable que resulte en un alto riesgo para los derechos y libertades de la persona física*".

Por lo tanto, la organización deberá evaluar la gravedad del impacto potencial o real en las personas como resultado de una infracción. La evaluación debe ser cuidadosa (completamente realizada) y basada en una sólida política de detección de infracciones, una investigación exhaustiva y (de acuerdo con) procedimientos de informes internos permanentes. Esto facilitará la decisión de si debe notificar a la autoridad de control pertinente o a las personas afectadas, o a ambas. Analicemos un ejemplo:

“Se han divulgado los datos de los empleados de una empresa textil. Los datos incluían las direcciones personales, composición familiar, salario mensual y reclamaciones médicas de cada empleado. En tal caso, la empresa textil deberá poner en conocimiento de la autoridad de control el incumplimiento. Dado que los datos personales incluyen datos confidenciales, como datos de salud, la empresa también debe notificar a los empleados”.

Determinar si el incumplimiento debe ser notificado o comunicado es una cuestión de suma importancia. Esta evaluación debe llevarse a cabo con cuidado, ya que es posible que una infracción no notificada se intensifique más adelante. Una evaluación sin fundamento, basada en líneas comerciales o en una política de daños puramente de control, puede llevar a la organización a aguas turbulentas, por ejemplo, en incurrir en responsabilidad civil o penal.

Si bien no existe una guía completa sobre cómo determinar si se debe notificar un incumplimiento, ciertamente hay algunos estándares a seguir, como los que se indican a continuación, además de los dictados por las buenas prácticas, la buena fe y el sentido común

"Si hay dudas sobre si la notificación es realmente necesaria, considere:

- *La probabilidad de daño o consecuencias negativas para los interesados afectados;*
- *Cómo la notificación, en particular a los interesados, podría reducir los riesgos derivados de la violación de datos personales que razonablemente se cree que ha ocurrido; y*
- *Si los datos implican: Información que probablemente afectaría la seguridad nacional, la seguridad pública, el orden público o la salud pública;*
- *Por lo menos la afectación a datos de cien (100) personas físicas;*
- *Información requerida por todas las leyes o reglas aplicables para ser confidencial; o*
- *Datos personales de colectivos vulnerables."*

Dicho esto, cabe añadir que la respuesta pública a la obligación de notificación prevista por el Reglamento ha sido abrumadoramente positiva: *"Ocho meses después de la entrada en vigor del Reglamento General de Protección de Datos de la UE (18 de mayo de 2018), las autoridades europeas de protección de datos han recibió más de 59,000 informes de violación de datos, según el bufete de abogados DLA Piper".* El entusiasmo podría haber sido alimentado por un conjunto de duras sanciones que habrían tenido que enfrentar en caso de desobediencia. Al igual que con el resto de los deberes establecidos por el Reglamento, en caso de que no se lleven a cabo, el RGPD deja claro que *"Con el fin de fortalecer la aplicación de las normas de este Reglamento, se deben imponer sanciones, incluidas multas administrativas, por cualquier infracción de este Reglamento , además de, o en lugar de las medidas adecuadas impuestas por la autoridad de control de conformidad con el presente Reglamento"*.

En cuanto a los requisitos que exigen los procedimientos de notificación, el Reglamento sí contempla algunas sugerencias encaminadas a un procedimiento claro, fáctico y transparente que pueda ser plenamente comprendido tanto por las autoridades como por los sujetos.

Así, aun considerando que existen diferencias entre las formas en que cada país refrenda el deber de notificación, lo escrito anteriormente sobre el Reglamento de la UE es suficiente para proporcionar al lector una visión general sobre este asunto.

Por último, pero no menos importante, es importante considerar si la organización tiene un seguro contra riesgos de seguridad cibernética desde el comienzo del incidente de datos, porque la mayoría de las pólizas de seguro requieren que el asegurado notifique a la aseguradora sobre un incidente sospechoso.

Hacer lo correcto.

Como se dijo anteriormente, el deber de notificación debe cumplirse en un momento muy crítico: el de un ataque que probablemente aún no esté completamente controlado. En este momento de crisis, a menos que la organización haya establecido previamente un comité para tratarla, la confusión y el miedo pueden prevalecer. Es este comité, cuyos miembros tienen responsabilidades claramente definidas, el que probablemente asegurará una acción oportuna en caso de un incidente.

No es sorprendente que haya mucho trabajo de emergencia por hacer desde el principio: asegurar áreas físicas, estudiar tanto el ataque como a su perpetrador, recopilar archivos digitales, realizar procedimientos forenses para preservar el ESI, tratar con accionistas nerviosos y con un consejo de administración o Directorio que probablemente se sieta abrumado, obtener los fondos para pagar las primeras facturas y hablar con la aseguradora. La lista no está completa ya que no incluye, por ejemplo, negociar con los “chicos malos” como sucede en un caso de *ransomware*. Y si es necesario u obligatorio ¡hasta llamar a la policía!

Probablemente, la organización puede parecerse a un campo de batalla confuso y en mal estado. Y además, tiene que informar a las autoridades de control y titulares de los datos del incumplimiento, si es el caso. A primera vista, parece ser demasiado.

Sin embargo, no lo es. La notificación es parte del remedio, no del problema. Se sitúa junto al resto de medidas que deberían tomarse para restablecer un grado de orden y eventualmente de normalidad. Es un subproducto correcto, un resultado, no una desgracia.

Aún así, una pregunta común podría ser "¿por qué en este momento en particular?". ¿Por qué una organización no solo tiene que informar al interesado/autoridades de supervisión, sino que también tiene que hacerlo con tan poca antelación?

En primer lugar, porque el deber de notificación se basa en el derecho del titular del dato a saber que se ha accedido ilícitamente a sus datos personales, lo que pone de relieve los riesgos a los que se enfrentan. Además, la razón de su sincronización es que deben saber que, a partir del ataque, se pueden desencadenar un conjunto de consecuencias negativas. Para prepararse para lo peor, los titulares de los datos deben saber que: *“estar al tanto de una violación conduciría a estar alerta y tomar medidas para prevenir el robo de identidad o convertirse en víctimas de estafas”.* Sería como la advertencia de "Prepárense para el impacto" a los pasajeros de avión, sugiriendo que las cosas podrían empeorar. En segundo lugar, los titulares de los datos han delegado la seguridad de sus datos a la organización que los procesa. Por lo tanto, este último es el único responsable de su seguridad e integridad. Si su seguridad falla, la organización es responsable ante los propietarios de los datos. Cabe destacar que el consentimiento al tratamiento de los datos no incluye la cesión de su titularidad, sólo de su seguridad. Entonces, la cadena de responsabilidad va desde el sujeto de los datos hasta la organización, que es el procesador de datos.

El deber de información no significa que la organización deba cumplirlo descuidando los demás. Por ejemplo, controlar los daños y tomar medidas para minimizar tanto el impacto como el riesgo, es claramente inaplazable. Por tanto, la notificación del incumplimiento a la autoridad de control es uno de los elementos de la respuesta a un ataque, pero inevitablemente no es el primero ni el único.

Finalmente, el deber de notificación probablemente puede ser costoso y llevar mucho tiempo. Requerido para ser cumplido en medio de un incidente traumático, este deber parece agregar daño al insulto. Entonces, es necesario encontrar un equilibrio entre lidiar con esos inconvenientes y cumplir con el deber, que puede parecer caminar sobre la cuerda floja.

Al fin y al cabo hay una regla sencilla: quien trata datos ajenos debe cuidarlos; si se viola su seguridad, deben informarlo.