https://doi.org/10.26439/advocatus2021.n39.5114



# Ciberseguridad y protección de datos personales en el Perú

**José Álvaro Quiroga León**

Abogado por la Pontificia Universidad Católica del Perú.
Maestría en Derecho Civil de la Pontificia Universidad Católica del Perú.
Miembro del Consejo de Defensa Jurídica del Estado peruano.
Ex Director General de la Autoridad Nacional de Protección de Datos Personales.
Presidente de la Comisión que elaboró el Proyecto de Reglamento de la Ley de Protección de Datos Personales.

## RESUMEN:

En la presente ocasión, ***ADVOCATUS*** tuvo la oportunidad de entrevistar a José Álvaro Quiroga León, abogado peruano especialista en protección de datos personales y ciberseguridad. A través de las siguientes líneas nos ofrece sus opiniones sobre la implementación de medidas de seguridad y la importancia de la protección de datos personales en el marco de las transacciones e interacciones en línea, el Reglamento de Aplicación de la Medida de Vigilancia Electrónica Personal aprobado mediante Decreto Supremo N° 012-2020-JUS, entre otros.


Palabras clave: protección de datos personales, ciberseguridad, transacciones en línea, vigilancia electrónica.



## ABSTRACT:

***ADVOCATUS*** had the opportunity to interview José Álvaro Quiroga León, Peruvian lawyer specialized in Data Protection Law and cybersecurity. In the following lines he offers his opinions about the implementation of security measures and the importance of personal data protection within the framework of online transactions and interactions, the Regulations for the Application of the Personal Electronic Surveillance Measure approved by Supreme Decree N° 012-2020-JUS, among others.


Keywords: data protection, cyber security, online transactions, electronic surveillance.


**1. Tras el aumento de las transacciones en línea durante el 2020, ¿qué medidas deben emplear las entidades financieras y comerciales para garantizar la seguridad de sus usuarios?**

Efectivamente, la situación de emergencia sanitaria ha limitado nuestra movilización y con ello disminuyen nuestras actuaciones presenciales y aumentan las actividades en línea. Ello ha hecho visible la necesidad de seguridad en este tipo de actividades, pero los riesgos ni son nuevos ni están limitados a entidades financieras o comerciales.

El crecimiento explosivo de actividades en línea y los servicios en los que su uso es masivo son un indicador de la importancia de la protección de la información en general y de la información personal en particular, pero también los servicios no masivos requieren de medidas de protección. Pensemos en el psicólogo, el médico particular, el cirujano plástico o el abogado y en la información sensible que manejan, aun sin ser masiva ni comercial. Ciertamente, regresando al tema, la masividad es un elemento de complejidad que debe ser atendido, además, porque en el entorno financiero o comercial el tratamiento inadecuado de la información personal de los clientes tendrá gran repercusión reputacional, más allá de las contingencias administrativas sancionadoras.

Por eso, en mi opinión, la primera medida que se debe tomar es comprender que la responsabilidad sobre la información de los clientes no es solo un tema de cumplimiento normativo o sólo un tema tecnológico, es un tema que atañe al "diseño del negocio", que lejos de ser un sobre costo o el efecto de una regulación incómoda, es un valor que puede ser sumado a la empresa.

Con eso en mente, las principales líneas de trabajo tienen que ver con diseñar medidas que controlen y neutralicen la pérdida o deterioro de información, los accesos no autorizados o las fugas de información.

Esas medidas involucran diversos aspectos:

a) Hay medidas organizativas que requieren transmitir a toda la estructura de la entidad los roles y responsabilidades que conciernen a cada quien en materia de protección de la información. Si no hay conciencia de la importancia de una clave de acceso o de cómo disponer de material impreso, por ejemplo, los fallos aparecerán en el lugar menos tecnológico y menos esperado.

b) Hay medidas de cumplimiento legal vinculadas con la transmisión, el diseño adecuado, en cuanto a datos, tratamientos y finalidades, de cláusulas de consentimiento

y contratos con colaboradores o terceros, por poner algunos ejemplos.

c) Hay medidas de seguridad técnica vinculadas directamente con la seguridad que se refieren a gestión de accesos físicos o contraseñas, privilegios de acceso, sistemas de bloqueo, eliminación de información en soportes removibles —o su destrucción—, por ejemplo.

Afortunadamente, la complejidad de las medidas no es uniforme y elevada para todos. Es la complejidad del negocio la que determina la complejidad de los tratamientos de datos y, consecuentemente, eleva o reduce la complejidad de la tarea por hacer en materia de protección de la información.

En nuestro país contamos con un instrumento facilitador muy importante y útil: la Directiva de Seguridad que diseñamos en la Autoridad Nacional de Protección de Datos Personales y que se aprobó mediante Resolución Directoral N° 019-2013-JUS/DGPDP para entregar la versión impresa gratuitamente y tenerla disponible en línea. Ha sido impresionante para mí conocer en el extranjero que este instrumento puesto al servicio de los operadores de nuestro país es reconocido entre los mejores a nivel mundial. Lo usan, lo aplican y lo recomiendan en otros países, aquí debería estar en el día a día de todas las empresas. ¿Cuál es su mérito? Es simple, operativa, permite identificar el nivel de complejidad de los tratamientos y diseñar seguridad "a la medida".

Otra herramienta es el tutorial DATA en línea que significa Diagnóstico Anónimo de Tratamiento Adecuado y que permite identificar el nivel de complejidad de los bancos y las medidas que les corresponden tomar. Este producto, que desarrollamos a partir de un convenio de colaboración y donación de la Agencia Española, está disponible en línea y me temo que la falta de difusión de su existencia lo mantiene "sub utilizado".

Finalmente, otra medida que puede adoptarse es aproximarse a los conceptos de "privacidad desde el diseño" de modo que los modelos de negocio o servicios se conciban y desarrollen sin afectar la privacidad —evitando que luego de mucho trabajo aparezca la objeción legal sobre lo diseñado por el área comercial o de informática—; y al de "privacidad por defecto" de modo que al tomar decisiones sobre la forma de hacer las cosas, se opte siempre por aquella que resulta más protectora de la privacidad de las personas.

**2. Recientemente se aprobó el Reglamento de Aplicación de la Medida de Vigilancia Electrónica Personal a través del Decreto Supremo Nº 012-2020-JUS, mediante el cual se regula la vigilancia electrónica personal, la cual es evaluada y aplicada a personas procesadas o condenadas (a) de manera preferente sobre la prisión preventiva y la pena privativa de libertad, (b) como regla de conducta en el caso de la aplicación de beneficios penitenciarios, conversión de pena u otras medidas de liberación anticipada y, (c) como alternativa a la custodia policial o privada en la detención domiciliaria. Al aplicar estas medidas, ¿cómo se podrían proteger los datos personales y el derecho a la intimidad de las personas procesadas o condenadas?**

A veces, cuando nos referimos a la protección de los datos personales, la privacidad o la intimidad, tenemos en mente la identificación de protección con ningún uso o tratamiento o ningún acceso. Algunos han llegado a la ridiculez de afirmar que la protección de datos pretende que olvidemos lo que hemos conocido.

Lo cierto es que la protección de datos no tiene por objeto inmovilizar o hacer secretos los datos de las personas, eso, además de imposible, haría inviable una vida normal para cualquiera que no sea un ermitaño real —porque los ermitaños digitales son, más bien, los que solo se comunican digitalmente—. De lo que se trata es que los datos de las personas sean tratados de forma útil y respetuosa, es decir, para finalidades legítimas y en las formas menos intrusivas posibles.

No voy a entrar aquí a la distinción, clara y existente, entre protección de datos, autodeterminación informativa, privacidad e intimidad. Para estos efectos, imaginemos que aluden a la misma esfera de la personalidad y dignidad de las personas.

Entonces, ¿es posible que un sistema de vigilancia personal no afecte la privacidad de una persona? Si entendemos afectación como una intrusión, acceso o conocimiento sin carga negativa, incluso para efectos positivos, siempre que se exponga nuestra privacidad habrá afectación. En ese sentido, por ejemplo, decir que la video vigilancia, fotografiar a una persona o anotar sus datos médicos, no afecta la privacidad son afirmaciones inexactas puesto que describen un ingreso a la esfera privada de una persona y por tanto una afectación. Otra cosa es analizar si se trata de una afectación legítima por estar autorizada por ley o consentimiento —el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo [de la Unión Europea][1] ha introducido otros criterios de legitimación que en nuestro sistema serían considerados "autorización legal"—; o una afectación ilegítima o proscrita.

En este contexto, es claro que la vigilancia descrita en la pregunta implica necesariamente la afectación —en sentido neutral— de la privacidad de los sujetos, pero dicha afectación obedece a una finalidad legítima y autorizada por norma de interés público. ¿Eso significa que allí se agotó la protección? Por supuesto que no. La norma establece con toda claridad que la información obtenida está bajo responsabilidad del Instituto Nacional Penitenciario del Perú-INPE y sujeta a las disposiciones de la Ley de Protección de Datos Personales. Esto, en versión corta, significa que deben respetarse los principios centrales de la protección de datos, a saber:

a) Finalidad: se recoge la información que sirva únicamente para vigilar la actividad del sujeto, con relación a las medidas restrictivas que le han sido impuestas.

b) Proporcionalidad: limitando la información que se recoge y guarda únicamente a aquella que sea indispensable para la finalidad y realizando los tratamientos, de acceso y transferencia, por ejemplo, solo en cuanto sea indispensable para las finalidades de vigilancia.

c) Calidad: de modo que se tenga el registro actualizado, debidamente identificado y con garantía de que está operando adherido al sujeto vigilado.

d) Seguridad: de modo que la recepción, el almacenamiento, la transferencia y el acceso que fuera necesario para el cumplimiento de la finalidad se realice por medios que garanticen la conservación inalterada y eviten pérdidas o accesos no autorizados.

Esperemos que no tengamos que ver en los noticieros los movimientos y actividades de los sujetos vigilados, tal como vemos todas las noches las grabaciones de video vigilancia que deberían respetar las mismas condiciones.

De hecho, otros aspectos de protección que la propia norma establece son un plazo de conservación seguido de un mandato de destrucción. Es de esperar que las directivas complementarias mantengan esta línea de respeto a la protección de la privacidad.

**3. ¿Cómo se puede fomentar la implementación de mecanismos de protección de datos cuando existen barreras de acceso como (i) el costo —especialmente para**

1. Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión [Europea], y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1725&from=ES.

**pequeñas y medianas empresas—, (ii) y la comprensión de la tecnología?**

La pregunta requiere que haga algunos comentarios previos. Los conceptos de barreras de acceso provienen del ámbito comercial, de la defensa del consumidor o de las normas sobre libre competencia, y aunque eso no los descalifica, sí implica situarse en un escenario distinto. La perspectiva de la protección de datos como una parte de la protección del consumidor es una visión de la regulación norteamericana que se extiende, de alguna forma, al Foro de Cooperación Económica Asia-Pacífico—APEC—. En esa concepción lo que se protege es el funcionamiento del mercado y la persona ocupa un lugar en el funcionamiento del mercado como consumidor. La regulación peruana se alimenta de la versión europea que tiene como centro de gravedad y objeto de protección a la dignidad de la persona humana como centro de todo el sistema jurídico en su condición de ciudadano.

Desde esa perspectiva, proteger un derecho fundamental no puede ser considerado un sobre costo, aunque es posible que sí tenga un costo. Como hemos visto, las medidas que han de tomarse para proteger la privacidad dependen directamente de la complejidad y dimensión del negocio. Así que si hablamos de pequeñas y medianas empresas, lo más probable es que tengan que implementar medidas organizativas que no son costosas y medidas de seguridad que pueden ser tan simples como limitar accesos con llaves, pestillos, controles de ingreso, cuadernos de control o claves de seguridad como las que ya usamos —o deberíamos— para dispositivos que están en nuestro bolsillo, de forma que no veo cómo el costo de tomar esas medidas puedan considerarse una barrera o cómo podrían exigir conocimientos tecnológicos exagerados.

Se trata, en todo caso, de un costo legítimo que debe ser asumido por quien toma, para su beneficio o como parte de una actividad económica que libremente ha decidido llevar adelante, algo que corresponde a la esfera personal de otro. Entonces, pensar que puedo tomar algo tuyo, usarlo para mi provecho y que no tengo por qué protegerte de los riesgos o daños que mi actividad te puede ocasionar no parece una mirada muy correcta, más aún si se recuerda que los datos de las personas constituyen un insumo empresarial que se toma a costo cero.

A este momento ya hay voces que plantean que si reconocemos que los datos personales son estratégicos, la nueva moneda, activos empresariales y constatamos que su monetización sostiene a las más grandes prestadoras de servicios, redes y aplicaciones de Internet, cabe explorar la posibilidad de que los titulares de los datos también encuentren una forma de "monetizar sus propios datos". Por ahora siguen siendo materia prima gratuita y lo menos que se puede hacer es no perjudicar a sus titulares. De eso se trata la protección de datos.

En cuanto al nivel de complejidad tecnológica, éste no viene dado por las normas de protección de datos, sino por la actividad económica o comercial que cada quien decide realizar. Si tu negocio es simple, la tecnología será simple, si tu negocio es sofisticado, la tecnología será más compleja y eso es para todos los aspectos del negocio. ¿Por qué sería diferente para la protección de la información?

**4. ¿Cuáles son las implicancias para los consumidores o usuarios por no leer los términos y condiciones y aceptarlos?**

Depende. La pregunta vuelve a presentar el tema desde la perspectiva de la defensa al consumidor y eso, que puede parecer intrascendente, no lo es.

Si hablamos de información transmitida y aceptación del "usuario" —yo prefiero "titular de los datos"— de lo que estamos hablando es del consentimiento para el tratamiento de datos.

Para efectos de centrar la respuesta hay tres características del consentimiento que debemos tener presentes y claras: debe ser libre, informado y expreso.

Que sea libre implica que se otorgue sin error, fraude, mala fe, violencia o dolo. De acuerdo

con nuestra legislación, no se admite la coacción, aunque esta venga encubierta, como cuando se configura el otorgamiento del consentimiento como parte obligatoria de un contrato, sin otorgar la posibilidad de no consentir, pero sí contratar.

Es muy frecuente que al diseñar cláusulas de consentimiento, como parte de un contrato mayor, se olvide que dicho consentimiento sólo es necesario para tratamientos que no son indispensables para la ejecución del contrato que el titular del dato celebra, puesto que, aquellos que sí son indispensables están exonerados de obtener consentimiento, razón por la que amarrar ese consentimiento al resto del contrato afecta la libertad del consentimiento, simplemente porque no se otorga la posibilidad de decir que no.

Otra práctica se vincula con los conceptos de "captura de consentimiento" propia del diseño informático y "ventana de oportunidad" normalmente proveniente del área de marketing. Combinándolos se diseñan fórmulas para que el titular del dato se vea llevado a consentir por su interés o necesidad de acceder a algún servicio, a veces al extremo de hacerlo sin darse cuenta. Por ejemplo, si se van a actualizar datos necesarios para el desarrollo de contrato o un servicio, se aprovecha para que suscriba una autorización general. Lo curioso es que la justificación para proceder así suele ser que "si se lo pido claramente, dirá que no", con lo cual se reconoce la falta de respeto a la voluntad del cliente y, lo más importante, la ausencia de libertad al otorgar el consentimiento, que evidentemente, no resulta válido.

También es frecuente encontrar cláusulas en las que se plantea que el titular consiente "en cumplimiento de la ley…" planteando una inversión de las cosas: ya no es el responsable del tratamiento el que cumple con la ley, solicitando el consentimiento y esperando un sí o un no, es el titular del dato el que debe consentir para cumplir con la ley. Como es obvio, este esquema engañoso también afecta la libertad del consentimiento así obtenido.

Lo que se debe comprender es que el consentimiento es una manifestación de voluntad que debe ser solicitada para obtener una respuesta, y no capturada. De nada sirve gastar energías, esfuerzos creativos y tecnológicos para "capturar consentimientos" que no son sanos y por tanto no servirán para justificar los tratamientos que se pretenden realizar.

Que sea informado implica que quien recibe el pedido de consentimiento reciba, de forma clara, sencilla y fácilmente accesible, una cierta información que garantice que, llegado el momento, podrá ejercer sus derechos frente al responsable del tratamiento de sus datos.

Que sea expreso implica que tiene que ser exteriorizado directamente sin que se requiera presumir, o asumir la existencia de una voluntad que no ha sido expresamente manifestada. No obstante, se siguen elaborando fórmulas de consentimiento tácito e increíblemente no faltan los "expertos" que sostienen que nuestra legislación —que señala que el consentimiento debe ser expreso— admite el consentimiento tácito. Veamos: la manifestación de voluntad tácita tiene dos características. La primera es, justamente, que no es expresa, sino que requiere asumir o presumir que una voluntad o conducta exteriorizada implica otra manifestación de voluntad que no ha sido exteriorizada. De hecho, lo tácito y lo expreso se definen por diferencia de uno con el otro, es decir, si no son contrarios o antónimos son, por lo menos, claramente diferentes. Entonces, lo tácito, por definición, no puede ser expreso. La otra característica, asumiendo por un instante que el consentimiento tácito sea viable, es que requiere que previamente se haya establecido, tanto cuál es la manifestación o conducta de la que se derivará la manifestación tácita, como cuál es la voluntad que se asumirá o presumirá y esto tiene que haber sido acordado por los involucrados en un acto previo o estar establecido en una norma que los obligue. Ningún sujeto de derecho puede imponerle a otro, por su propia voluntad que "su silencio significa esto o aquello" o "que dar otro clic, o continuar navegando en un portal web, significa que consiente sobre esto o aquello". Los esquemas de "captura de consentimiento" con estos diseños ni siquiera

pueden calificarse de consentimiento tácito, son cláusulas erróneas que no contienen ningún tipo de consentimiento. No importa cómo lo llamen o cuánto enfaticen que es expreso. Recordemos que en Derecho, las cosas son lo que son, por su naturaleza y contenido, no por cómo se les llame.

Un ejemplo que he usado durante años y ante diversos auditorios es el siguiente: imaginen que al salir del salón encuentran un cartel que dice "el solo tránsito por esta puerta significa la manifestación, expresa, libre e informada de que cada persona que pasa consiente en entregar su dinero al expositor". Ineludiblemente explotaba la risa haciendo innecesaria mayor explicación. Y, sin embargo, hay quienes siguen usando estas fórmulas.

¿Por qué se siguen usando estas fórmulas inconducentes? Mi impresión es que hay mucho desconocimiento y también una distorsión que tiene que ver con la primera parte de mi respuesta y aterriza en su núcleo.

La defensa del consumidor traslada nociones de la protección de la privacidad estadounidense, que como ya mencioné tiene como centro de protección al mercado y no al ciudadano. En ese contexto es de alta relevancia el concepto de las "expectativas de privacidad", de modo que tanto las advertencias de "siguiente clic" como la elaboración de términos y condiciones mediante políticas de privacidad tienen el efecto de reducir o eliminar las "expectativas de privacidad", porque cumplen función de "advertencia".

El problema del traslado de esas nociones a nuestra realidad es que las "advertencias sobre expectativas de privacidad" son unilaterales, mientras que nuestro sistema regula el consentimiento que, además de no estar basado en las expectativas de privacidad, es bilateral, en el sentido que uno lo pide —con ciertos requisitos— y depende de que el otro conteste de manera expresa.

En nuestro marco legal la política de privacidad no es una advertencia sino una forma de trasladar información sobre términos y condiciones. Ahora bien, cumplir con ese traslado no implica haber obtenido el consentimiento, hay que cumplir los demás requisitos y tenemos norma expresa al respecto: el artículo 13 del Reglamento de la Ley de Protección de Datos Personales, de forma que en nuestro sistema lo que se acepta o no se acepta no son "términos y condiciones" sino el otorgamiento de consentimiento para que ciertos datos, sean objeto de ciertos tratamientos, para ciertas finalidades, por parte de cierto responsable.

En cualquier caso, no le recomiendo a nadie aceptar nada sin informarse.