Tratamiento e ilegalidades de los datos personales en el uso cotidiano de las redes sociales
Processing and illegalities of personal data in the daily use of social networks

Contreras Filiciotto, Angel Gabriel
Universidad Oberta de Catalunya
España
Correo: angelfiliciotto@gmail.com
ORCID: https://orcid.org/0009-0004-0783-6975

Entregado: 30 de mayo de 2025
Aprobado: 20 de junio de 2025
DOI https://doi.org/10.48204/j.aderecho.n55.a8712

Resumen

El principal interés en el presente trabajo es demostrarle al lector la relevancia que ha cobrado en los últimos años la materia de datos personales que gracias a la tecnología ha tenido y proyecta a un más un gran impacto y volatilidad en su aplicación. Es por eso que abordaremos el uso más común de los datos personales en el día a día de las personas, ya sea, en el uso personalísimo o como sujetos de responsabilidad institucional, esto sumado a las plataformas digitales y la necesidad creciente que ha adoptado el individuo a vivir su vida personal y profesional a través de ellas y de sus pantallas digitales sin distinguir muchas veces una de la otra.

Palabras clave: datos personales, redes sociales, legalidad, tratamiento, derecho comparado.

Abstract

The main focus of this paper is to demonstrate to the reader the importance that personal data has gained in recent years, which, thanks to technology, has had and continues to have a significant impact and volatility in its application. Therefore, we will address the most common use of personal data in people's daily lives, whether for personal use or as subjects of institutional responsibility. This, in addition to digital platforms and the growing need for individuals to live their personal and professional lives through them and their digital screens, often without distinguishing one from the other.

Key words: personal data, social network, legality, processing, comparative law.

Introduction

La problemática actual de los datos personales radica en que tenemos una capacidad de almacenamiento e interconexión que avanza exponencialmente y que la capacidad humana para asimilar tales cambios no parece ir a la misma velocidad. Es por eso, que vemos que se hace muy común que las personas no puedan diferenciar muchas veces cuando están en el uso doméstico y personal de sus datos o en el uso de datos personales ajenos, así como responsables del tratamiento de dichos datos por funciones públicas o empresariales.

Esto nos lleva a la hipótesis de que las personas en esencia son las mismas que hace años atrás, pero que no así en la importancia de la información que les pertenece, ya que, con la inmersión de las nuevas tecnologías esta información ha adquirido una relevancia crucial en muchos aspectos de nuestras vidas, donde un mal tratamiento puede generar daños irreparables para el individuo. Por lo que, los métodos que se usaban antes para temas sociales, profesionales e incluso judiciales no se puede contemplar de igual manera en la actualidad con la llegada de las nuevas tecnologías y las leyes de protección de datos.

Es así como trataremos de proyectar los elementos más graves y resaltantes dentro del uso cotidiano de los datos personales en las redes sociales, como es posible viciar procesos, caer en responsabilidades innecesarias y convertir a sujetos que infringen la ley en victimas por un pequeño error del tratamiento.

Legalidad del tratamiento

La legalidad del tratamiento de los Datos Personales pasa directamente por el cumplimiento de la norma, que es en esencia lo que significa el principio de legalidad. Para que la legalidad del tratamiento de los Datos Personales tenga vialidad jurídica debe respetarse en un inicio los derechos del titular y los principios del tratamiento, siendo, el consentimiento el derecho (art.15 de la ley 81 de 2019) rector del tratamiento, así como la totalidad de los principios de la norma. (art. 2 de la ley 81 del 2019)

Partimos de la realidad que hoy es poco practicada en la vida cotidiana y es que, en principio, aquel que posea una base de datos está obligado a custodiarla y darle el tratamiento idóneo que rige en la normativa actual. Si bien es cierto, y como veremos a continuación, para la norma no toda persona se considera un responsable de Datos Personales, no obstante, esto

no quiere decir que los derechos del titular sobre sus datos quedan en detrimento o son inexistente.

La problemática, a nuestro juicio, surge de la idea poco clara que se tiene hoy sobre la materia, y el valor que tienen los datos para las personas, pues, la paradoja más grande del momento es vivir en una sociedad digitalizada (red.es, 2024, pág. 13) y en una generación tecnológica (INEC, 2023) que no conoce la importancia y el valor de sus datos.

Ante una materia que para el interés jurídico es nueva, partimos también de que vivimos en una sociedad que todavía está en la etapa infantil o en algunos países más avanzados, la etapa adolescente, con respecto a la materia de Datos Personales.

Sin embargo, y más allá de los vacíos que pueda haber legal y doctrinalmente dentro de la legislación actual de datos personales, si consideramos pertinente el sentir de la norma en estudiar y considerar cada contexto del tratamiento (salvo en los casos de multas, donde la norma no tiene consideración sino una tasa fija de penalización). Es importante entender que, en principio, el titular es el que sabe cuándo y cómo ha sido violentado en sus derechos con respecto a los datos personales, como también, una persona natural con redes sociales no es igualmente responsable por el tratamiento de datos que la persona jurídica dueña de esas plataformas digitales, como tampoco, las cuentas creadas con fines comerciales. Es por eso, que profundizaremos en ambos apartados de manera individual para una mayor comprensión del elector.

Legalidad del tratamiento de la persona natural

En principio, para la norma panameña (así como para la europea), la persona natural en el uso personal o domestico de los Datos Personales son excluidos de la normativa. (art. 3 de la ley 81 del 2019)

Ahora, aquí tenemos que considerar pertinente una explicación y también criticamos la simpleza de la norma al plantear algo semejante sin ningún considerando o guía que pueda desarrollar mejor la idea, pues, es bastante errático pensar que se crea toda una norma de protección de datos personales cuyo artículo primero aluce a derechos fundamentales (en especial a la intimidad). Por lo que, es bastante iluso pensar que una persona por el hecho de utilizar su smartphone para redes sociales o actividades domésticas está exento de

responsabilidad, ya que, al fin y al cabo, el derecho del consentimiento del titular de los datos siempre está vigente, esto quiere decir, que si bien es cierto, la persona natural en principio y por el planteamiento anterior, no tiene la responsabilidad de un oficial y/o responsable de datos personales, no obstante, esto no quiere decir que puede usar cualquier dato personal que se le ocurra.

Esto radica en que sería absurdo considerar que el derecho que tiene el titular sobre sus datos personales que trasciende a derechos fundamentales pero que con el simple hecho de hacer el tratamiento de dichos datos de carácter personal o domestico permitan operar en un vacío jurídico que lo deje en indefensión. Por ende, lo que se debe considerar es que para la persona natural que use los datos de manera doméstica o personal, no se le pedirían los requisitos técnicos de control y protección sobre el tratamiento de los datos que posee en sus dispositivos digitales o que utiliza en su vida cotidiana que si se le exige al responsable del tratamiento. (art. 7 de la ley 81 del 2019)

Ahora bien, esto a nuestro juicio no quiere decir que no pueda responder por daños y perjuicios ante una negligencia, pues, el mal uso de los datos personales afectan por igual al titular de los datos, haya sido una empresa o una persona natural, por lo que, nos parece un poco irresponsable que el legislador no haya contemplado la realidad tecnológica imperante de nuestro tiempo, pues, es común que las personas en el uso de los datos dentro de su vida cotidiana manejen una cantidad absurda de datos personales ajenos donde en la mayoría de casos rozan la ilegalidad.

Si bien es cierto, no hay requerimiento ante este uso de los niveles técnicos de protección que se le pediría a una compañía como Meta, no obstante, el consentimiento para el uso de datos ajenos es un requisito *"sine qua non"* para mantener a raya el principio de legalidad. Así, por ejemplo, una *"selfie"* en un parque donde pueda quedar expuesto el rostro de terceras personas podría acarrear responsabilidades para el que tomo la fotografía, así como tomar fotografías ajenas en redes sociales para otro tipo de uso, teniendo en cuenta que el derecho de imagen está protegido tanto por el código de la familia de Panamá como por la ley de protección de datos personales.

Por lo que nos queda entonces con que el uso personal y domestico de los datos personales en la actualidad es una escasa parte de la vida cotidiana, como sería, por ejemplo, los chats, los contactos, fotografías sin publicar, documentos varios, etc. Pues, la exposición no consentida de datos personales ajenos lo deben hacer responsable por violación directa de la norma, aunque, no partamos de la consideración del responsable del tratamiento, pero si, de la violación a los derechos del titular de los datos.

También hay que considerar, que cuando la persona natural se dedica a alguna actividad comercial, política o similar, que escape de la concepción personal en el uso, si tendría cierto nivel de responsabilidad del tratamiento de los datos, pues, ya se le consideraría de otra forma, si la cuenta de redes sociales está configurada de una manera diferente a la personal, no podemos bajo ninguna circunstancia considerar que la legislación no es aplicable o que su deber de responsable no existe.

Legalidad del tratamiento como persona jurídica

Para el caso de la persona jurídica si cambia con respecto a la persona natural, aquí no se puede considerar que pueda existir un tratamiento personal o doméstico, pues, por la constitución de la persona jurídica tendrá los elementos claros de que el tratamiento debe responder entonces a los parámetros establecidos por la norma, empezando por la obligación de tener un responsable de datos personales, pues, este es el encargado de responder ante cualquier derecho de los titulares o cualquier vicio a los principios del tratamiento.

Así, todo aquel que maneje datos personales a este nivel debe considerarse responsable del mismo, y debe preocuparse por el debido funcionamiento del tratamiento de dichos datos, pues, como veremos más adelante, es una materia en exceso volátil, que puede girar de una materia a otra, incluso deslindarse de su competencia inicial que es de índole administrativa. De ahí que surjan procedimientos como el sistema de seguridad de la información (International Organization for Standardization, 2022) y el sistema de gestión de la continuidad del negocio. (International Organization for Standardization, 2019)

Para las instituciones que pertenezcan al Estado panameño se le exige adicional al responsable de datos personales, el oficial de datos personales (art. 42 del DE 281 del 2021), que por defecto, seria aquel que maneja la ley de transparencia, mientras que, para las

personas morales de índole privado no es obligatorio este último, pero, consideramos que es recomendable contar en los equipos legales con un experto en la materia para evitar malos tratamiento que puedan perjudicar económica, social y políticamente a la institución privada, que incluso, podrían llevar a cabo los protocolos como oficial de tratamiento de datos y gestión de continuidad del negocio.

Por lo que, en este rubro, no es negociable el respeto de todos los derechos contenidos en la norma a favor del titular, así como los principios del tratamiento que son la brújula de la legalidad de la materia.

Los datos personales en redes sociales

Partimos de la idea de que los datos expuestos voluntariamente por sus titulares en redes sociales son públicos, así como, la no responsabilidad de los usuarios que las utilizan para su uso personal como vimos anteriormente, al igual que las configuraciones de la cuenta en dichas plataformas y de las cuentas de personas jurídicas.

Esto es importante entenderlo, pues, de ahí se consideraría las responsabilidades varias sobre el tratamiento de los datos personales por parte de estas cuentas de redes sociales según sea su configuración porque no se comportan igual las cuentas abiertas al público o con interés comercial que las cuentas personales.,

En principio se consideran que son públicos, pero que, al profundizar la norma vemos que es una especie de caramelo envenenado, pues, no habría en principio responsabilidad por mantener un dato público, como por ejemplo, una fotografía que haya sido expuesta en redes sociales, no obstante, la finalidad del tratamiento podría cambiar de un momento a otro, siendo este, especifico desde el momento que el titular de dicha fotografía la haya publicado en redes sociales, no se podría cambiar salvo consentimiento de la parte afectada, por lo que, si bien es cierto, tenemos un dato público, este no sería viable para cualquier tratamiento. (dincat, 2023, pág. 17)

Paradojas de la aplicación de los datos personales en redes sociales

En este apartado partimos de la idea de la politización ideológica de las redes sociales, es decir, más allá de que nuestros datos parten de los derechos fundamentales y humanos

consagrados en el principio de libertad y privacidad (por lo menos de los países que siguen el civil law), tenemos con que, todo tratamiento que tienda a manipular a los usuarios es potencialmente ilícito.

Por lo que tenemos ejemplos múltiples en un periodo corto de tiempo, así desde el 2020 hemos vivido como sociedad un flujo de información constante en una sola vía, incluso, en temas electorales hemos vivido grandes paradojas mediáticas en redes sociales.

Partimos del hecho de que hay quienes se consideran dueños de la verdad absoluta, partiendo por los dueños de las megacorporaciones que son titulares de las redes sociales, como Meta o Twitter (hoy "X"). Donde se parte con la premisa de que al ser empresas pueden censurar a diestra y siniestra, pero que, si la libertad de expresión y en especial, el tratamiento de datos personales que no puede usarse para discriminar según la legislación occidental, partimos del hecho de que es contrario al orden público (Boutin I., 2018, pág. 409), debido proceso y leyes varias las censuras de cuenta, cierres o similares por comentarios dentro de la misma, pues, la empresa privada no es competente para restringir dichos derechos. (C. Filiciotto, 2024)

Por otro lado, partimos de la manipulación, tildada de "sugerencias" del algoritmo ¿Cómo podríamos considerar lo que es sugerencia y lo que es manipulación? Por supuesto, es un tanto subjetivo, pues, la realidad es que las preferencias son tantas como personas hay en la tierra, no obstante, tenemos ejemplos en USA y Europa de compañías dueñas de redes sociales multadas por cientos de millones de dólares por tener alguna manipulación dentro de sus plataformas, lo que nos indica que las preferencias pueden ser múltiples, mientras que, las sugerencias no, pues estas tienen preferencias económicas, políticas y sociales según sea quien las maneje, de ahí que veamos que políticas como el "shadobanning" no sean producto de la casualidad. (Narayanan, 2023, pág. 16)

La manipulación dentro de las redes sociales la pudiéramos ver potencialmente como el tratamiento de los datos personales con un fin contrario a la voluntad del titular, es decir, guiarlo de una manera que no le quede de otra elegir la opción preestablecida por los algoritmos. (Muñoz Iturriera, 2023, pág. 49) Así, ante un bombardeo constante pasamos de la era de la verdad a la post-verdad, donde no importa lo que vean los ojos o escuchen nuestros oídos, importa la cantidad de veces que vemos comentarios o información destinada

a convencer de lo contrario (McLuhan, 1996, pág. 29), así vimos como a finales de agosto del 2024 un titular conmociono al mundo (al cegado al menos), cuando el dueño de Meta, Mark Zuckerberg admitió que fue manipulado por la administración Biden para censurar información sobre la pandemia, así como, los casos ilícitos del hijo del Presidente demócrata Joe Biden, Hunter Biden. (BBC, 2024)

Igualmente paso, con las elecciones del 2020 con el artículo que salió del Times en el 2021, donde confirmaron la reunión y un pacto para beneficiar a uno de los candidatos hacia la presidencia de Estados Unidos de América, so pretexto de proteger la democracia, cuando en teoría, la democracia partiría por la elección voluntaria de la mayoría, y para que ese consentimiento se dé voluntariamente no es posible una manipulación o censura de la contraparte de por medio. (C. Filiciotto, 2024, pág. 201)

Esto es importante, pues, estas redes sociales usan los datos personales de millones de personas, donde muchos de ellos están protegidos por sus leyes sobre datos personales o leyes básicas de derechos humanos y fundamentales, por lo que, todo uso de nuestros datos destinado a manipular o discriminar nuestras ideas o comentarios es por supuesto totalmente ilícito. Recordemos que los datos personales deben seguir ciertos principios, adicional a los derechos de los titulares, el vicio de los mismos ya constituye una infracción a la legislación de datos, peor, cuando se usan datos sensibles como las posturas políticas para censurar o discriminar.

Es fundamental considerar que una verdad a medias no es tan diferente a la mentira, de hecho partimos de la idea que son sinónimos, pues el resultado es el mismo porque cuando los datos solo se comparten de una manera en particular, como fue el caso del 2020 (Ball, 2021) o las búsquedas de Google en Europa (Google LLC vs. CNIL, 2019), estamos ante una manipulación directa, pues, la información total no es compartida, ni la disidencia de dicho discurso, por lo que, no es posible escapar del vicio del consentimiento ante la redirección planificada por el algoritmo y las intenciones de quienes los manejan.

Internacionalización de los datos

La actualidad tecnológica ha permitido que lo que antes era casi imposible, hoy sea el pan de cada día, pues, la realidad de las redes sociales, es que, lo que allí se publica automáticamente

se convierte en un dato trasnacional, ya que, los servidores de las plataformas antes mencionadas no están en territorio nacional, por lo que, estamos ante el Derecho Internacional Privado día a día dentro de ellas. (art. 2 del Código de Derecho Internacional Privado)

La modernidad de los datos personales parece haberle dado una época dorada moderna a la rama del derecho mencionada, lo que, vuelve para los estudiosos del derecho una rama elemental de estudio en la actualidad.

Ahora bien, esto conlleva múltiples problemas a la hora de proteger los derechos de los usuarios dentro de las redes sociales y plataformas digitales, así como la responsabilidad de los mismos a la hora de usarlas, pues, un mal uso podría ser interpretado como ilícito en otras jurisdicciones y ser más que viable la imputación de cargos o responsabilidades de todo tipo, aunque nunca se haya pisado físicamente dicho territorio, siguiendo los principios "lex rei sitae", "lex loci delicti commissi", "lex locus regit actum" (Contreras Filiciotto, 2025, pág. 20), que son características que ocurren mucho en el ámbito del ciberespacio, donde una persona con un solo acto puede violar varias leyes y cometer daños a distancia. (Miró, 2012)

El primer problema de las plataformas digitales es que la legislación panameña al no poder ejercer su capacidad de imperio tiende a dejar expuesto los derechos de sus nacionales y residentes, pues, la viabilidad de responsabilizar a dichas corporaciones meta capitalistas se hace casi imposible sin los servidores en suelo patrio, así como las investigaciones pertinentes del mal tratamiento de datos, pues el acceso es casi inexistente y los tramites como los exhortos o cartas rogatorias para un derecho digitalizado se vuelve poco práctico ante la rapidez con que fluye la información, así como el daño cuando esta es mal manejada. De hecho, la intención de la ley panameña como de la ley europea plantea precisamente la extraterritorialidad del tratamiento de datos, con el fin de arropar o atraer la aplicación de datos fuera de sus fronteras hacia el interior de las mismas entendiendo el impacto tecnológico que trae al derecho internacional contemporáneo. (Trooboff, 2021)

Esto no quiere decir que la utilización de datos fuera de las fronteras no pueda generar impactos en países donde el tratamiento no se realiza, pero si la obtención de información. Así hay varios casos como el de *"Clearview ai"*, que es una empresa estadounidense radicada

en Manhattan, New York, que se dedica a ofrecer software de reconocimiento facial a fuerzas del orden y demás agencias gubernamentales que estuvo implicada en múltiples procesos legales por ilegalidades varias en la recopilación y utilización de los datos personales en países como, Estados Unidos de América, Canadá, Italia, Austria, Francia, Grecia, Reino Unido y Países Bajos. (Forbes, 2024)

El caso de Uber en Países Bajos por la transferencia ilícita desde ese país a Estados Unidos de América de usuarios de su plataforma sin la debida protección y tratamiento adecuado donde había datos generales de cuentas, licencias de taxi, ubicaciones, fotos, detalles de pago, documentos de identidad, hasta historial policivo y datos médicos. (AP vs Uber, 2024)

Otro caso interesante fue el caso de TikTok vs Irlanda, donde no se adecuaban los métodos de transferencia de los usuarios de dicho país a los servidores y personal de la plataforma en China, donde en principio la plataforma negaba dicha transferencia de datos personales. (TikTok vs DPC, 2023)

De igual forma, ha ocurrido en Panamá en los últimos años con las famosas video llamadas por WhatsApp de países lejanos como la India, Pakistán, Sudáfrica y otros. Donde el *"modus operandi"* trataba de ciberextorsion y robo de identidad mediante IA, donde el usuario al abrir la video llamada en la pantalla veía imágenes de desnudos de menores de edad, y los perpetradores usaban luego su imagen para extorsionarlo haciendo ver al usuario como consumidor de contenido pornográfico de menores de edad. (TVN, 2023) Caso interesante seria saber dónde y que institución fue la que permitió la filtración de información, dado que, el usuario podría haber sido víctima de tal cosa al incluir información telefónica o acceder a páginas de dudosa legalidad, no obstante, aquellos que recibieron video llamadas de dicha índole fueron múltiples, dando a entender que la filtración tuvo que venir de una base de datos amplia por parte de una institución y no de cada usuario de manera individual.

En casos de ciberdelitos por estafa en territorio patrio se ha recibido exhortos o cartas rogatorias desde Grecia, a raíz de estafas realizadas por criptomonedas en plataformas digitales a través de una empresa domiciliada en Panamá. (Exhorto o Carta Rogatoria desde el Tribunal de Primera Instancia de Atenas, 2022)

Responsabilidad del uso de datos

Por otro lado, la responsabilidad del usuario, que parte como no responsable del tratamiento de datos personales, siempre y cuando, como hemos visto, no violente el derecho principal del titular, es decir, el consentimiento para el uso de sus datos, así como el principio de finalidad. Es decir, que, ante un uso de datos personales no consentidos por el titular, así como darle un uso distinto al fin inicialmente otorgado podría acarrear alguna responsabilidad porque estaría rozando la ilegalidad.

Así tenemos, por ejemplo, que en principio el titular de la cuenta podría ser responsable de algún delito si los comentarios que hace en la comunidad internacional que son las redes sociales acarrea un tipo penal dentro de cualquier país que tenga acceso a dicha publicación, así como el uso indiscriminado de datos personales ajenos, cuyo tratamiento no radica en el capricho de algún inadaptado irresponsable con acceso a internet, así tenemos el caso de una modelo argentina que publico fotos con su esposo en Twitter donde aparecían cazando animales en Sudáfrica, por lo que recibieron insultos, ataques, amenazas durante días en dicha red social y que dio con la orden judicial de eliminar cualquier contenido creado contra dicha modelo que hicieran referencias a adjetivos despectivos producto de dicho evento. (Vanucci v. Twitter, 2016) En el mismo contexto, podemos incluir el uso de fotografías para hacer daño a la imagen, uso distinto al fin inicial, violación a la intimidad y de manera muy literal el uso sin consentimiento de datos personales de menores de edad que están protegidos de una manera férrea por la ley y el derecho comparado. (NANDIVALE S.L vs AEPD, 2023) En este punto hay que precisar que el simple hecho de tomar imágenes de una cuenta de Instagram privada y hacerla pública en otro medio acarrearía potencialmente responsabilidad. (Joly Digital vs AEPD, 2022)

Lo que se debe tener en consideración en la sociedad actual, es que, las redes sociales exponen a la comunidad internacional a cualquiera que las utilice, pues, una publicación puede ser vista *"ipso facto"* por cualquier persona con internet alrededor del mundo. Por lo que, tenemos que partir de la idea donde el desconocimiento de la norma no es causal de eximente de responsabilidad alguna, como tampoco se hace viable el infantilismo eterno de los individuos en las redes sociales donde la práctica común es el ilícito como lo es el uso no consentido de datos personales ajenos, donde delitos como la injuria y la calumnia están a la orden del día por los "adictos de la cancelación". (RV vs AEPD, 2020)

Las responsabilidades pueden ser variadas, en principio, la legislación de datos personales trata infracciones de índole administrativo, que van desde carácter económico hasta prohibitivo en el sentido de volver a tratar o ser parte de un tratamiento de datos personales. En Panamá las infracciones son leves, graves y muy graves; y el monto máximo de multa económica es de $10,000.00. (art. 36 de la ley 81 del 2019).

Esto no es limitante para que un reglamento interno de cualquier institución pueda determinar alguna sanción interna a un mal uso de datos personales, así como la vía administrativa tampoco agota otras vías judiciales como la civil, penal e incluso laboral.

Esto radica en la volatilidad de la materia donde un mal tratamiento de datos que viole la intimidad puede generar la responsabilidad del tratamiento mismo ante la ANTAI, daños y perjuicios en juzgados civiles y delito contra la intimidad en el SPA.

Lamentablemente muchas veces las responsabilidades en redes sociales por mal uso de datos personales llegan de personas que piensan que no están haciendo nada malo, como el caso de las fotos intimas de menores de edad en un entorno familiar, pero que, sigue siendo material que no debe por ley ser expuesto en dicho entorno. Incluso, algo que es común ver hoy, cuando pasa algún escándalo sexual en vías o lugares públicos y se suben a internet, si bien es cierto, dichos actos conllevan sanciones, el acto en si de grabar y subirlo a internet conlleva a un delito contra la intimidad según el código penal patrio y que ya tiene jurisprudencia en el derecho comparado.

Buenas prácticas de los datos personales en redes sociales

Partimos de la idea del uso de redes sociales y por supuesto, de datos personales por parte de personas comunes y corrientes en el día a día. Principalmente y por mandato de ley se considera que la persona natural en estas circunstancias no tiene la obligación de un responsable de datos personales, siempre y cuando se mantengan en la condición *"personal o doméstica"*. La problemática surge en el uso cotidiano de prostitución de la información a la que está sometida la persona, incluyendo la ignorancia generalizada en la materia.

Así, por ejemplo, podríamos estar en el binomio “personal o doméstico” siempre y cuando la persona utilice sus redes sociales única y exclusivamente para publicar contenido de su autoría y solo donde sus datos personales son expuestos por sí mismo, como los chats o

interacciones con terceros se mantengan confidenciales, es decir, no se exponga los chats o interacciones similares a terceros, esto debe incluir cuentas de redes sociales privadas o restringidas al acceso libre. Esto quiere decir, que, si aun cuando el individuo no tiene la obligación de un responsable de datos personales, esto no quiere decir que la persona natural puede considerar no aplicable la normativa ante el uso de datos personales de terceros, pues, el consentimiento del titular sigue existiendo, así como todos los principios del tratamiento de datos personales.

Ahora bien, explicado el apartado de cuando estamos en la aplicación de la norma, tenemos que partir del uso cotidiano de las redes sociales, y es que, podríamos decir que el común denominador de occidente (en especial Panamá), no son más que constantes imprudencias. Así tenemos que el mejor de los casos (que es ilegal dentro de la literalidad de la norma), es publicar una fotografía donde salgan terceros sin previo consentimiento, así como exponer en historias o publicaciones similares los chats privados con terceros, ya sea, de buena fe o para exponerlos creyendo de que se protege un derecho o similar, como sería el caso del ciberacoso o ilegalidades dentro del ciberespacio. Esto incluye, el uso de datos personales públicos en dichas plataformas, pero que, teniendo un fin determinado, no podríamos considerar que la adquisición de estos datos para ser usados en otra base de datos en circunstancias diferentes sea licito, más allá de haber esquivado lícitamente el apartado del consentimiento.

Aunque la ciberseguridad del usuario como consumidor de plataformas digitales no es exigible por los usos *"personal y/o doméstico"*, si se debe considerar como elemento básico y completamente obligatorio el mínimo de responsabilidad ante el uso de información privada y sensible de terceros, es decir, aquella información que pueda generar doxing, phishing, ciberacoso o similares. Dentro de este tipo de información se encontrarías; números de teléfono, dirección de correo electrónico, preferencias de todo tipo (en especial políticos, sexuales, religiosas y similares), documentos de identificación, dirección de viviendas, dirección de trabajado, entre otros.

Es así como vemos que los *"trending"* parecen inofensivos y solo una tendencia más dentro de un mundo donde exponer las preferencias parece ser lo normal y cotidiano, hasta que, nos damos cuenta que nuestro perfume favorito, así como nuestra primera mascota, nombre de

padres, hermanos o cualquier familiar, ciudad natal, idioma, ciudad favorita, país favorito, comida favorita, deporte favorito, color favorito, entre otras preguntas o gustos, son en efecto preguntas frecuentes de seguridad en cualquier cuenta bancaria por ejemplo.

Esto se suma a la prostitución a diestra y siniestra de los más vulnerables, siendo el caso por excelencia, los menores de edad, que se auto-exponen o son expuestos por familiares, que, aunque procedan de buena fe, esto no reduce la responsabilidad, ilegalidad, negligencia y daño. Pues, ante un entorno donde el "online grooming" crece cada día, producto de toda clase de "depredadores cibernéticos", también tenemos de que dicha información podría usarse para causar más daño, pues, es común ver como padres exponen fotos intimas de sus bebes, así como el primer día de clases, donde salen, profesores, amigos del menor, nombre del colegio, escudo del colegio y horario en el que este permanece en el plantel, así como el nombre y apellido, todos datos personales que pueden utilizarse para planear un secuestro o peor. Donde ya ha habido sanciones a madres por exponer de manera indiscriminada a sus hijos, que comúnmente es conocido por el término *"sharenting"*. (Sharenting, 2017)

Es por eso, que aunque no haya exigencias técnicas de ciberseguridad, sigue siendo un porcentaje alto la responsabilidad general que se tiene a la hora de proteger los datos personales propios y de terceros cercanos a nosotros, pues, el solo hecho de exponer datos o de utilizar aplicaciones ilícitas (piratas) que terminan siendo una aspiradora de datos dan como resultado que en la vida cotidiana sea el común denominador la sobre exposición de datos, sin tener en cuenta la gran responsabilidad que tenemos en la actualidad y el gran valor de nuestros datos personales.

Debemos entender que ante la volatilidad de la materia puede ser fácil mutar de una responsabilidad administrativa (la inicial de la legislación de datos personales), a una civil o penal, pues, recordemos que podríamos incurrir en un conflicto de calificación (Boutin I., 2018, pág. 369) y no solamente entrar en una responsabilidad familiar por publicar una foto intima de familiares menores de edad, sino directamente ser considerado como pornografía infantil por las autoridades. Debemos entender el espacio en el que nos encontramos y las responsabilidades en las que incurrimos en prostituir datos personales ajenos, pues, las circunstancias puedes ser infinitas.

En el caso de las empresas la obligación es mayor, pues, es común ver toda clase de distribución de información personal en las plataformas digitales de las instituciones. Por lo que, el oficial de gestión de la información, como el de continuidad de los negocios aquí juega un papel fundamental a la hora de asesorar adecuadamente según el contexto de cada organización. Casos como el de la distribución de fotografías de menores por parte de sus escuelas (Colegio Virgen de Europa, S.L. vs AEPD, 2023) o de publicación de imágenes de cámaras de videovigilancia en redes sociales. (CUI ZSQ FOOD, S.L. vs AEPD, 2024)

Las redes sociales como "curriculum vitae"

Como hemos visto, el tratamiento de los datos personales está arraigados a los principios y los derechos del titular, por ende, una cuenta particular dentro de una plataforma que es ajena al entorno laboral no es susceptible a consideraciones para cargo o puesto alguno, pues, estarían basándose en sustentos improcedentes para el mismo, dado que la vida personal de los individuos en redes sociales no es equiparable a la función laboral o a la capacidad laboral del mismo.

Es cierto, que en la práctica se podría considerar que la vida dentro de redes sociales tiene implicaciones en el desarrollo laboral de una persona, así podríamos considerar que una persona que sale mucho de fiesta podría ser un trabajador menos responsable, así como los gastos desproporcionados que puedan mostrar en sus plataformas, incluso, para temas meramente sociales como con que chica o chico salir podríamos determinar la potencialidad con un simple vistazo en redes sociales.

Lo anterior incluye a que el empleado no estará obligado a seguir a nadie de la empresa o institución en la que trabaja, así como a no aceptar a nadie de su entorno laboral en sus redes sociales, esto se tomaría como una medida desproporcionada y que nada tiene que ver con las funciones laborales (en principio), así como ocurriría en el caso de la desconexión digital, que debe ser un derecho del trabajador de no ser molestado en ninguna plataforma digital (WhatsApp por ejemplo) mientras este se encuentre fuera de sus funciones u horario laboral.

Pero en estricta legalidad, las redes sociales que se manejen o tengan la configuración de personales y no públicas, económicas o similares, no pueden ser sustento para una relación laboral entre empleado y empleador, considerando además que tenemos ejemplos que si son

procedentes como es el caso de Linkedin, que es una red social para fines meramente laborales, es una especie de CV abierto y continuo donde los usuarios comparten todos sus logros académicos y profesionales. (AEPD, 2021, pág. 22)

Entorno de los datos

Los datos personales encuentran su entorno donde pueden ser almacenados y utilizados, el tema radica es que en la actualidad tenemos dos entornos por excelencia, el físico, donde desarrollamos nuestra vida basados en todos los sentidos, en especial el tacto; mientras que, en los últimos años, surge exponencialmente el entorno digital. (Platonova & al., 2022)

El entorno físico requiere menos conocimientos técnicos que su homologo tecnológico, pues, los elementos que trae a colación son menos que aquel. En el entorno físico basta tener un conocimiento claro de cómo mantener los datos físicamente alejados de aquellos que no están autorizados, así como, por ejemplo, tener archivos cerrados con llave o bóvedas, como no filtrar la información verbalmente, a *"grosso modo"* estos serían los elementos más importantes a la hora de proteger la información de manera física.

Por parte de la información que hoy está dentro del cosmos digital (ciberespacio), así como dentro de los múltiples dispositivos móviles (tablets y celulares) y fijos (como las PC), donde no solo se necesitan conocimientos básicos de manejo de dichos sistemas o programas, sino también, muchas veces, equipos técnicos que puedan defender y proteger la información de ataques una y otra vez.

Es por eso, que una de las consideraciones básicas que hay que tener en ciberdelincuencia, es que, no es posible (por lo menos de manera responsable), digitalizar la información donde no hay el equipo idóneo para hacerlo y protegerla en el tiempo, pues, el tratamiento de los datos personales dentro del ciberespacio requiere de los conocimientos idóneos, como los protocolos ISO, en este caso, de gestión de la información y de continuidad del negocio. Por lo que, se hace necesario entender que no podemos digitalizar por digitalizar, so pretexto de mejorar el servicio o los tramites, eso por supuesto, es loable, para que los usuarios tengan un mejor trato en trámites burocráticos o cualquiera que sea que generalmente son tediosos, pero la ética y responsabilidad legal dentro del tratamiento de datos es siempre y en todo momento una obligación. (Jones & Wynn, 2023)

El problema, es que, la información contenida en el ciberespacio sigue una volatilidad sin precedentes donde generalmente las personas no tienen todavía las condiciones profesionales y académicas de entender, aunque sea la mitad de los elementos importantes del entorno donde se encuentran los datos que están tratando. (Sandvik & al., 2022) Esto deja la puerta abierta a un sin número de negligencias y posteriores responsabilidades, podríamos decir sin temor a equivocarnos que la primera *"back door o brecha" de* un sistema informático es la ignorancia de quien lo maneja.

Basta ver el común denominador del comportamiento generalizado de la sociedad en redes sociales para saber el desconocimiento claro de los riesgos dentro del ciberespacio, la prostitución empedernida de la información, incluso con aquellos que son más vulnerables (por ejemplo, menores de edad).

Vivimos en una sociedad que es infantil en el manejo de sus redes sociales y que no deja de prostituir su información más preciada por unos miseros *"likes"* que lo único que hacen es alimentar el ego individual que no debe generar más que una ligera liberación de dopamina. Tenemos que partir de la idea de que una vez publicada la información en rede sociales es en extremo difícil, casi imposible, que se elimine en su totalidad una vez que se ha arrepentido el titular de haberla expuesto.

El uso de datos por parte de funcionarios en redes sociales

Para efectos prácticos de este punto vamos a dividirlo en dos partes que siguen compartiendo la misma responsabilidad porque al final un funcionario o un político siguen siendo parte del Estado y de sus funciones, la diferencia radica en que uno es puesto por capacidad (o contactos) y el otro generalmente por un concurso de popularidad (llamado elecciones) que en la actualidad se desarrolla en gran medida en redes sociales.

Ahora bien, partimos por el político, un pseudo influencer actual, que puede no llegar a influir realmente en la población o ser realmente un actor de época que hace cambiar ideológicamente a las personas en masa, así mismo pasa con su efectividad, en general la política como diría el Dr. Huerta de Soto "es una borrachera de mentiras", donde prácticamente es imposible encontrar un político que cumpla con lo prometido al cien por ciento en campaña.

Pero, el punto que nos lleva hoy a analizar a estos potenciales mentirosos empedernidos, es que, desde las elecciones de Barack Obama en el 2008, es imposible imaginar en la actualidad que un político pueda llegar a un cargo de elección popular sin el uso de las redes sociales, pues, el electorado tiene en estas el desarrollo social y político casi en su totalidad.

La problemática se centra en que no es lo mismo ser un influencer que graba bailes para Tik Tok, de comentarios sobre temas que no conocen, haciendo obras benéficas, o incluso apoyando a políticos del establishment, que se un funcionario. La realidad que vemos en la actualidad es que cuando uno de estos sujetos llega a materializar su popularidad en un concurso político para ocupar un cargo de mando y jurisdicción, el comportamiento social dentro de las plataformas digitales no cambia mucho, es decir, el manejo de la información y por supuesto, de datos personales sigue siendo el mismo, lo cual es un error. Es un error antes de ser candidatos y políticos, pero, se acrecienta siendo ya un funcionario, pues, podríamos estar incluso ante delitos por mal manejo de la información que obtienen por su puesto de elección popular.

Por lo que, recordemos partes elementales del tratamiento de datos, en el caso de los principios; fin y proporcionalidad; en el caso del entorno, no es lo mismo, físico que digital y/o electrónico, como hemos visto. Así como la confidencialidad del proceso en todo momento. (art. 2.7 de la ley 81 del 2019)

Ahora bien, recordemos que en esencia dentro del Estado, y por supuesto, las diversas funciones que llevan a cabo los funcionarios hay tramites específicos y un manejo de datos igual, por ende, no es posible o compatible el prostituir información del cargo en redes sociales de manera licita, pues, el entorno puede que no sea el mismo, como sería el caso de un expediente físico elevado al ciberespacio a través de una fotografía, así, como la prostitución de los nombres de las partes dentro del expediente que es totalmente contrario a las leyes procesales (art. 14 de la ley 6 del 2002, el caso de los arts. 189-191 del nuevo Código Procesal Civil o el art. 496 del Código Judicial). Así, también tenemos el escarmiento que se ha popularizado en la comunidad panameña en los últimos tiempos como lo son las multas de tránsito, y es que, prostituir nombres, cedula de identidad, placa vehicular, entre otros datos personales no es jurídicamente viable bajo la legislación actual de protección de datos (como tampoco lo es en el derecho comparado). Pues, aunque podríamos en interés público,

ejercicio o protección de un derecho denunciar las irregularidades de tránsito, la toma de esas fotos debe ser confidencial, al igual que el tratamiento, incluso, una vez haya procedido la multa por violación a la ley de tránsito esta no podría ser publicada en las redes sociales como han hecho usuarios e incluso políticos y como se ha visto en el tratamiento de datos en el derecho comparado.

Esto deja claro, que no es lo mismo ser un influencer y un político, pues, aunque el influencer no trata los datos de manera licita en muchas de las ocasiones en el uso de sus redes sociales, la gravedad del político radica en que podría caer en responsabilidades penales debido al ejercicio de sus funciones, pues, valerse de su condición para acceder a bases de datos específicas y exponerlas al conglomerado internacional de las redes sociales es una ilegalidad tremenda que podría acarrear en el mejor de los casos, su separación del cargo, en el peor de los casos, la prisión. Todo esto, por el simple hecho de no saber la legislación actual ni tener los asesores especializados en la materia, en este caso, el oficial de datos de cada institución tiene una tarea de alto impacto, pero, no es limitación que cuente con un equipo experto según sea el contexto y magnitud de la institución.

La realidad política no dista mucho de la realidad social, pues, tanto los usuarios que prostituyen sus datos por *"likes"* en redes sociales como los políticos que se creen modernos y correctos al mostrar lo que hacen como sinónimo de trabajo, esfuerzo y cumplimiento de su deber, no hay mucha diferencia, en ambas situaciones la ilegalidad está a la orden del día, pues, como hemos visto los datos personales dentro de procedimientos específicos no deben ser expuestos.

Para el caso de los funcionarios que no son electos por voto popular y que se dedican al manejo de expedientes como el caso del Órgano Judicial, es imperativo que se capacite a todo el personal, pues, la cantidad de ilegalidades en la sobreexposición de expedientes es algo que se ve día a día en redes sociales donde los funcionarios durante y después de sus audiencias se toman "selfies" donde se pueda ver algún fragmento de información del caso que llevan, o peor aún, cuando son auxiliares de jueces y terminan publicando los expedientes que llevan solo para mostrarle a sus seguidores lo "arduo" que trabajan, y eso no se discute, lo que si se discute es la ilegalidad de publicar los expedientes en redes sociales, así como usar celulares personales y WhatsApp para comunicaciones del personal de fiscalía.

Lo anterior aplica para cada institución pública realmente, no solo para expedientes judiciales, toda base de dato que el funcionario maneje debe mantenerla confidencial a como dé lugar, no puede sobreexponerla en redes sociales, salvo en los casos de transparencia donde el común denominador es la publicidad de la información, pero que, aun así, tiene su protocolo por ley.

Valor de los Datos Personales según el derecho comparado

Para efectos de este punto vamos a comparar resumidamente la legislación panameña, europea y estadounidense. En el caso panameño la ley que rige la protección de datos personales es la ley 81 del 2019; para el caso europeo el reglamento 679/2016; y por último, el caso estadounidense que no tiene como tal una ley federal sobre datos personales, sino que, los estadounidenses dentro de las leyes especiales para cada materia regulan lo concerniente a los datos que se utilizan, no obstante, la más cercana a ser la homologa de las leyes anteriormente mencionadas seria la ley de California, consumer privacy act (CCPA) del 2020.

La diferencia de los sistemas radica en la filosofía política, así como sus semejanzas (en el caso europeo y panameño). Por ende, partimos que aquellos países o regiones que han mantenido una tradición romanista en sus ordenamientos jurídicos consideran a sus datos personales como parte de sus derechos fundamentales y humano. Por ende, no es negociable en principio ante la negativa de sus titulares el tratamiento y se entendería que aun habiendo consentimiento si el tratamiento vicia sus derechos más elementales no podría realizarse, pues, los derechos humanos se consideran como mínimos e irrenunciables.

Mientras que, el caso estadounidense se fundamenta en el comercio y consumo, así, vemos que a lo largo de la legislación el tratamiento de datos se fundamenta en la capacidad que tengan las partes para comercializarlo y sacarle un valor económico a los mismos, no parten de sus derechos fundamentales y derechos humanos, parten de sus derechos económicos como consumidores. Si bien es cierto, aquí tenemos derechos similares como el de eliminar (que sería suprimir en la legislación panameña), no discriminación y derecho a saber (que sería como el principio de transparencia), la intención inicial del responsable del tratamiento

es buscarles un uso económico a los datos y no fundamentarse en un derecho fundamental y humano.

Incluso dentro de nuestra legislación tenemos proyecciones diferentes, con la Ley de Transparencia por un lado y por la Ley de Protección de Datos Personales, donde el legislador considera que hay información personal que debe ser expuesta a modo de transparencia, mientras que, en el otro lado considera la protección y confidencialidad como principio rector. Esto más que traer alguna discrepancia entre las leyes, a nuestro juicio se proyecta por el lado de la transparencia una sobre exposición del funcionario, que queda merced de los cazadores informáticos al ser expuesto su salario, cédula, nombre y cargo.

Conclusión

Tenemos entonces que la materia de datos personales es de suma importancia por múltiples circunstancias, en principio por su tratamiento, dado que, ante la utilidad de la información se requiere que se use para diferentes contextos dentro de una institución, pero que, la necesidad de tratarlos debe ir de la mano con diferentes protocolos que las normas actuales exigen.

Vemos de igual forma que la utilidad es diversa y en algunas situaciones debemos mantener la información confidencial y en otras circunstancias darle la publicidad correspondiente, pero que, deben seguir protocolos adecuados de tratamiento, pues, como se ha desarrollado la materia hay que ser conscientes de que las diferencias muchas veces son mínimas y que un pequeño error puede viciar todo un proceso y convertir al victimario en víctima.

Así como el deber y función de cada individuo, pues las responsabilidades como vimos no son iguales, de ahí surge la persona natural por usos domésticos y personales que no es un concepto absoluto, así como el deber de los funcionarios y de los asesores de cada institución de mantener la legalidad siempre y en todo momento. Queda claro la facilidad y volatilidad con la que la materia puede sufrir vicios, donde el individuo que cumple funciones especiales y críticas muchas veces no sabe diferenciar entre su vida personal y la información que le es ajena a ese contexto.

El tratamiento y protección de datos personales es una materia que seguirá creciendo en su uso e importancia, por lo que, se hace fundamental la profundización de la materia

entendiendo el contexto tecnológico actual que permite una interconectividad nunca antes vista.

Bibliografía

AEPD. (2021). *La protección de datos en las relaciones laborales.* Madrid: AEPD.

AP vs Uber (Autoriteit Persoonsgegevens 22 de julio de 2024).

Ball, M. (4 de Febrero de 2021). *TIME*. Obtenido de https://time.com/5936036/secret-2020-election-campaign/?utm_source=twitter&utm_medium=social&utm_campaign=editorial&utm_term=politics_2020-election&linkId=110717147

BBC. (27 de agosto de 2024). *BBC News Mundo*. Obtenido de https://www.bbc.com/mundo/articles/cpvy724vyp7o

Boutin I., G. (2018). *Derecho Internacional Privado.* Panamá: Maître Boutin.

C. Filiciotto, A. G. (2024). Los Datos Personales. Una crítica a la interpretación. *Anuario de la Facultad de Derecho y Ciencias Políticas de la Universidad de Panamá*, 191-213.

Colegio Virgen de Europa, S.L. vs AEPD, 202209078 (Autoridad Española de Protección de Datos 22 de junio de 2023).

Contreras Filiciotto, A. (2025). *TFM: LA CIBERDELINCUENCIA DENTRO DEL E-COMMERCE COMO CONSECUENCIA DE UN MAL TRATAMIENTO DE DATOS PERSONALES (ANÁLISIS DE DOS MARCOS JURÍDICOS).* Panamá/Barcelona: FUOC.

CUI ZSQ FOOD, S.L. vs AEPD, 202300692 (Autoridad Española de Protección de Datos 20 de junio de 2024).

dincat. (2023). *Guía sobre internet y las redes sociales.* Barcelona: dincat.

Exhorto o Carta Rogatoria desde el Tribunal de Primera Instancia de Atenas, E578492022-08-08-12-16-PR-AT-RJ0031-26132022 (Corte Suprema de Justicia, Sala Cuarta, República de Panamá 30 de agosto de 2022).

Forbes. (3 de Septiembre de 2024). *Forbes*. Obtenido de https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/

Google LLC vs. CNIL, C-507/17 (TJUE 29 de septiembre de 2019).

INEC. (2023). *Líneas de teléfonos celulares activos en la República de Panamá.* Panamá: INEC.

International Organization for Standardization. (2019). *ISO 22301.* GInebra: ISO.

International Organization for Standardization. (2022). *ISO 27001.* Ginebra: ISO.

Joly Digital vs AEPD, 202207521 (Autoridad Española de Protección de Datos 21 de agosto de 2022).

Jones, P., & Wynn, M. (2023). Corporate responsability in the digital era. *Creative Commons*, 1-11.

McLuhan, M. (1996). *Comprender los medios de comunicación: Las extensiones del ser humano.* Barcelona: PAIDÓS.

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Muñoz Iturriera, P. (2023). *Apaga el Celular y Enciende tu Cerebro.* Nashville: HarperEnfoque.

NANDIVALE S.L vs AEPD, 202211618 (Autoridad Española de Protección de Datos 31 de mayo de 2023).

Narayanan, A. (2023). *Understanding Social Media Recommendation Algorithms.* New York: Knight First Amendment Institute at Columbia University.

Platonova, & al., e. (2022). Knowledge in digital environments: A systematic review of literature. *Frontiers*, 1-12.

red.es. (2024). *La sociedad digital.* Madrid: red.es.

RV vs AEPD, 00227 (Autoridad Española de Protección de Datos 10 de noviembre de 2020).

Sandvik, J.-P., & al., E. (2022). Quantifying data volatility for IoT forensics with examples from Contiki OS. *Forensic Science International: Digital Investigation*, 1-10.

Sharenting, R.G.39913 (Tribunale di Roma. Prima Sezione Civile 21 de diciembre de 2017).

TikTok vs DPC, IN-21-9-1 (Data Protection Comission 1 de septiembre de 2023).

Trooboff, P. D. (2021). GLOBALIZATION, PERSONAL JURISDICTION AND THE INTERNET. *The Hague Academy Collected Courses (Vol 415)*, 1-313.

TVN. (3 de octubre de 2023). *TVN Noticias*. Obtenido de https://www.tvn-2.com/nacionales/tenga-cuidado-estafadores-utilizan-video_1_2082510.html

Vanucci v. Twitter, 8671/2016 (Juzgado Civil y Comercial Federal 2. República Argentina 27 de diciembre de 2016).