UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA PORFESIONAL DE DERECHO

TRABAJO DE SUFICIENCIA PROFESIONAL

LA AUTORIDAD NACIONAL DE PROTECCION DE DATOS PERSONALES Y EL PRINCIPIO DE IGUALDAD

PRESENTADO POR:

Bach. TOROMANYA ORE, LUZ ROXANA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

ASESOR:

Mg. URIBE TAPAHUASCO, JUAN JOSE

ORCID: 0000-0003-2452-1524

DNI: 28237618

LIMA – PERÚ

2023

DEDICATORIA

La presente tesis la dedico a toda mi familia y amigos, principalmente a mi madre e hija que han sido un pilar fundamental en mi vida, dándome fuerzas para seguir adelante y así lograr las metas y objetivos propuestos.

AGRADECIMIENTO

Agradezco a Dios, por darme la oportunidad de estar en este mundo, en especial mi madre e hija, quienes siempre me dieron las fuerzas e impulsaron a seguir adelante, gracias.

INFORME DE SIMILITUD

UPCI
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

INFORME DE SIMILITUD N°114-2023-UPCI-FDCP-TT

A : **MG. HERMOZA OCHANTE RUBÉN EDGAR**
Decano (e) de la Facultad de Derecho y Ciencias Políticas

DE : **MG. HERMOZA OCHANTE, RUBEN EDGAR**
Docente Operador del Programa Turnitin

ASUNTO : Informe de evaluación de Similitud de Trabajo de Suficiencia Profesional: **BACHILLER TOROMANYA ORE, LUZ ROXANA**

FECHA : Lima, 11 de Octubre de 2023.

Tengo el agrado de dirigirme a usted con la finalidad de informar lo siguiente:

1. Mediante el uso del programa informático **Turnitin** (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 20 palabras) se ha analizado el Trabajo de Suficiencia Profesional titulada: **"LA AUTORIDAD NACIONAL DE PROTECCION DE DATOS PERSONALES Y EL PRINCIPIO DE IGUALDAD"**, presentado por la Bachiller **TOROMANYA ORE, LUZ ROXANA**.

2. Los resultados de la evaluación concluyen que el Trabajo de Suficiencia Profesional en mención tiene un **ÍNDICE DE SIMILITUD DE 19%** (cumpliendo con el artículo 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019).

3. Al término análisis, la Bachiller en mención **PUEDE CONTINUAR** su trámite ante la facultad, por lo que el resultado del análisis se adjunta para los efectos consiguientes.

Es cuanto hago de conocimiento para los fines que se sirva determinar.

Atentamente,

.....
MG. HERMOZA OCHANTE, RUBEN EDGAR
Universidad Peruana de Ciencias e Informática
Docente Operador del Programa Turnitin

Adjunto:

**Recibo digital turnitin*
**Resultado de similitud*

ÍNDICE

INTRODUCCIÓN

La presente investigación tiene como fin describir cómo se han ido desarrollando la tecnología de la información y el derecho a la intimidad y ello ha generado legislaciones nacionales e internacionales, con la finalidad de proteger una serie de derechos relativos a la intimidad y los datos personales, la creación de autoridad nacional de Protección de Datos personales y Principio de Igualdad

En este trabajo voy a dar algunos indicadores así como conceptos que se han ido generando en estas últimas décadas y que la no solución de dicha problemática se han ido manifestando en cuestiones de problemas legales como una respuesta a por ejemplo el tratamiento de los datos personales por las plataformas como google.

En la medida que dicha situación problemática se siga ahondando más en la sociedad más aún se verán conflictos difíciles de solucionar.

El presente trabajo es un aporte con la finalidad de establecer mejores lineamientos que permitan el tratamiento de dicha problemática.

CAPÍTULO I

PLANIFICACIÓN DEL TRABAJO DE SUFICIENCIA PROFESIONAL

1.1. Título y descripción del trabajo de suficiencia profesional

Título de Trabajo

El presente Trabajo de Suficiencia Profesional es: **La Autoridad Nacional de Protección de Datos Personales y el Principio de Legalidad.**

Descripción del Trabajo

El presente trabajo está dividido en cuatro capítulos:

Capítulo I **Planificación del Trabajo de Suficiencia Profesional**

Capítulo II **Marco Teórico**

Capítulo III **Desarrollo de las Actividades Programadas**

Capítulo IV **Resultados Obtenidos**

En el **Primer Capítulo** desarrollamos la Planificación del trabajo así como los objetivos y justificación de la investigación.

En el **Segundo Capítulo** establezco lo que doctrinariamente es la Autoridad Nacional de Protección de Datos Personales y el Principio de Igualdad.

En el **Tercer Capítulo** desarrollo los aspectos de la Autoridad Nacional de Protección de Datos Personales a nivel nacional.

Finalmente, en el **Cuarto Capítulo**, resaltamos conclusiones, recomendaciones

1.2. Diagnóstico y finalidad

A medida que los modelos de negocio digitales continúan evolucionando, los datos y aplicaciones empresariales se migran desde los centros de datos locales a la nube. Si bien este desarrollo ha dado a los individuos y a las industrias más control, ha reducido costos y ha permitido a las empresas operar de manera más eficiente que nunca, también ha transformado el papel de TI de un proveedor de seguridad local a una empresa global, la base de la empresa unificada. Es necesaria una solución de protección de datos para proteger los datos y evitar su pérdida.

Desarrollar una estrategia de seguridad que respalde la transición a la nueva realidad de datos distribuidos y adopción de la nube en toda la organización no es fácil y las empresas enfrentarán muchos desafíos.

1. **Pérdida de datos ocultos en el tráfico cifrado** Cuando los empleados están en la oficina y en la red de la empresa, los datos y las aplicaciones permanecen en un centro de datos central y el tráfico cifrado es limitado, las soluciones locales son suficientes. Con el paso a la nube, el cifrado ha pasado de ser la excepción a ser la regla. Si su solución de protección de datos no clasifica ni controla los datos en el tráfico cifrado, puede perderse la mayoría de las sesiones en las que puede producirse filtración y abuso de datos, lo que deja a su organización vulnerable a la pérdida y las filtraciones de datos.

2. **Diferencias entre los diferentes servicios de protección de datos -** Al pasar a la nube, los datos se distribuyen entre aplicaciones SaaS y aplicaciones de nube pública, cada una de las cuales suele ser creada y administrada por individuos y líneas de negocio dentro de una organización. Por ejemplo, los servicios CASB se utilizan para proteger aplicaciones SaaS, Secure Internet Gateway (SWG) con Data Loss Prevention (DLP) se utiliza para proteger aplicaciones de Internet y Cloud Security Protection with Stateful Management (CSPM) se utiliza para proteger aplicaciones públicas en el Nube. Esta complejidad dificulta la coherencia de la comunicación y la protección de datos y puede provocar duplicación de funciones y lagunas en la visibilidad y el control de las aplicaciones.
3. **Contexto limitado al controlar el uso de los datos** La visibilidad y el control detallado son esenciales para proteger los datos corporativos. La mayoría de las opciones de protección de datos solo brindan visibilidad de TI sobre quién intenta acceder, la ubicación del usuario y el estado de la aplicación, lo que limita los controles necesarios para usar los datos de manera eficiente y segura y complica innecesariamente las decisiones de protección de datos.
4. **Pobre experiencia de usuario**. A medida que los trabajadores y las aplicaciones pasan de los centros de datos locales a la nube, la infraestructura en uso es ahora la propia Internet, lo que limita la capacidad de TI para predecir, identificar y mitigar problemas. Se vuelve más difícil garantizar que los empleados tengan una buena experiencia de usuario y sean productivos cuando la mayoría de las aplicaciones que utilizan están fuera del control de la organización.
5. **Infracciones de cumplimiento en el cloud** El incumplimiento de los estándares de la industria puede resultar en multas importantes e incluso pérdida de ingresos.

Al compartir datos entre aplicaciones y servicios en la nube, la visibilidad del cumplimiento y las capacidades de remediación se reducen, lo que potencialmente pone en riesgo su negocio.

1.3. Objetivos del trabajo de suficiencia

1.3.1. Objetivo general

Analizar a la institució de **La Autoridad Nacional de Proteccion de Datos Personales y el Principio de Legalidad**.

1.3.2. Objetivos específicos

Describir cómo la Autoridad Nacional de Protección de Datos Personales maneja el Principio de Legalidad

1.4. Justificación

Después de declarar derechos fundamentales a la privacidad y al procesamiento adecuado de datos, los países se han centrado en legislar procedimientos y reglas apropiados para evitar consecuencias para los titulares de derechos. Las nuevas tecnologías brindan flexibilidad en el flujo de información a través de dispositivos tecnológicos que las personas llevan consigo en diversas aplicaciones que crean un intercambio internacional continuo de datos con servidores de todo el mundo. Las preocupaciones sobre el posible impacto en los derechos individuales crean incertidumbre sobre si las empresas u organizaciones procesan adecuadamente la información y brindan a las personas controles para proteger sus derechos. En Colombia, a pesar de las leyes pertinentes, las personas desconocen la cobertura de los mecanismos existentes y utilizan la tutela como mecanismo principal. El presente artículo tiene como objetivo abordar el tema de la protección administrativa de datos personales a nivel nacional a través del análisis jurídicoEste proyecto es muy importante y oportuno para las entidades responsables y/o responsables del tratamiento de datos personales a nivel regional (por

ejemplo, para personas públicas o a nivel institucional), ya que les proporciona un conocimiento claro y preciso del desarrollo. del sistema jurídico. regulación que requiere la adaptación o establecimiento de políticas y procedimientos de procesamiento de información para resolver solicitudes sin vulneración de datos personales. En resumen, el significado social de este proyecto de investigación es difundir el análisis de los instrumentos legales existentes para que las personas puedan evitar el uso ilegal o no autorizado de sus datos personales a través de medios procesales administrativos para proteger el derecho fundamental a la privacidad. Crea un buen nombre.

Capítulo II

MARCO TEÓRICO

2.1 Modelo Europeo

Inicialmente, el modelo europeo consideraba la protección de datos personales en el derecho privado como parte de los derechos personales, cuando las constituciones de los países europeos reconocían directa o indirectamente los datos personales como derechos fundamentales, se transfirieron al derecho público: en Alemania, p. , la Ley de Bonn se basa en la protección de datos personales, una interpretación de la dignidad y está claramente definida en el artículo 26(1) de la Constitución portuguesa de 1976. (Suárez Espino, 2008: 68-69). La revolución tecnológica comenzó a acercar la información para ser procesada con fines de toma de decisiones en los negocios, la política, la sociedad y la religión. Actualmente, ante la gran cantidad de tecnologías disponibles para el tratamiento y el interés por la tutela como garante de la igualdad, el desarrollo de la personalidad y la dignidad humana, el modelo europeo adopta un enfoque más activo y lo regula con una legislación general. Asignar la función de control y

restricción de cualquier base de datos a una autoridad pública similar al Defensor del Pueblo sueco. El derecho de hábeas corpus se conoce como derecho a la libertad informática. La citada directiva reconoce los derechos de las personas físicas respecto de sus datos personales (Artículos 12, 14, 15) y en determinadas partes de sus disposiciones se expresa la necesidad de tomar medidas para asegurar su efectiva aplicación (Artículos 22-24). se refuerzan los argumentos discutidos en los artículos 10, 23, 25, 38, 41, 45, 48, 52, 55, 61, 62 y 63; Se puede concluir que el Estado debe promover y garantizar el tratamiento legal de los datos personales y establecer procedimientos que permitan a las personas ejercer sus derechos de acceso, oposición, supresión y rectificación frente a instituciones públicas o particulares.

2.2 Modelo norteamericano

En el modelo norteamericano es difícil reconocer el derecho a la privacidad, por lo que la jurisprudencia se encarga de darle forma al concepto de privacidad, basándose en los antepasados del derecho a la privacidad, Samuel Warren y Louis Brandeis. Consideró el derecho a la privacidad como un "derecho a no ser molestado" dentro de los derechos de propiedad. La posición jurídica favorece claramente la protección del individuo frente a injerencias externas (Suárez Espino, 2008: 58-61). El modelo norteamericano lo considera parte de las libertades civiles basadas en las Enmiendas Sexta y Novena de la Constitución de 1787, que protegen la esfera privada. El reconocimiento de la naturaleza espiritual del hombre extiende a) el derecho a la vida, que brinda protección contra interferencias externas, como la protección contra el olor, y b) el derecho a la propiedad, que brinda protección legal a los intangibles. El nuevo invento, que abarcaba todos los aspectos de la vida personal estadounidense, era la situación perfecta para demostrar la necesidad del "derecho a ser dejado en paz" para

garantizar la inviolabilidad de la personalidad (Warren y Brandeis, 1891). El modelo norteamericano es más pragmático y enfatiza que la autonomía individual debe determinar qué información puede procesarse o compartirse, de modo que el gobierno o los individuos no puedan interferir. Por tanto, los conflictos o violaciones de la privacidad pueden resolverse judicialmente a través de la vía del agravio (Pérez Luño, 2005: 334), que es el caso de Prosser (1960: 389) de responsabilidad civil por la comisión de un hecho ilícito. Dividido en:

1) interferir en el dominio o asuntos privados de otras personas,

2) revelar públicamente hechos privados vergonzosos,

3) Revelar los hechos y crear una falsa impresión de los interesados en la sociedad;

4) Robar nombres y retratos de otras personas para beneficio personal.

En lo que respecta a la protección de datos personales, los incisos 1, 2 y 3 regulan, según corresponda, las definiciones de datos personales y procesamiento de información en la legislación norteamericana que interpreta el ámbito de la protección de datos. El modelo norteamericano considera que la protección de datos personales se limita a los individuos y sus relaciones comerciales y civiles.

2.3 Principios de la protección de datos personales

2.2.1 Principio de la licitud

La licitud como principio de protección de datos significa que el tratamiento de los datos personales debe realizarse siempre de forma lícita, lícita o fiable, de conformidad con las leyes y reglamentos aplicables y de conformidad con el acuerdo entre el responsable del tratamiento y los responsables de el procesamiento. El titular de los datos personales, de conformidad con las normas establecidas, para satisfacer expectativas razonables en materia de privacidad. Respecto a este principio, las directrices armonizadas de protección de datos de la Comunidad Iberoamericana establecen: "Los

datos sólo podrán ser recogidos y tratados de buena fe y con estricto cumplimiento de la ley y los derechos humanos. De conformidad con lo dispuesto en estas directrices".

Este es un principio que debe observarse en todo tratamiento de datos personales, de lo contrario el tratamiento será ilícito. Si los datos personales ya han sido tratados, el tratamiento que no cumpla con este principio será reconocido como ilícito y por tanto los datos personales deberán ser suprimidos.

2.3.2 Principio de consentimiento

Según la definición del artículo 3, fracción IV de la LFPDPPP, se entiende por consentimiento "la expresión de la voluntad del titular, con la que se realiza el tratamiento de los datos".

Respecto al consentimiento, el informe del CJI de la OEA señala que "En general, un individuo debe poder dar su consentimiento libremente para la recopilación de datos personales en la forma prevista y para los fines previstos. Por lo tanto, el consentimiento del individuo debe basarse en información suficiente y ser claro, es decir, que no debe crear dudas ni ambigüedades.

Sobre las intenciones humanas".

Al respecto, las directrices armonizadas de protección de datos de la Comunidad Iberoamericana establecen:

"3.1. la recolección y tratamiento de datos personales sólo podrá ser llevado a cabo con el consentimiento de la persona a la que se refieren esos datos. Esto implica que es necesario obtener el consentimiento de los usuarios o clientes antes de recoger o manejar cualquier información que les pertenezca.

3.2. Sin embargo, la ley podrá establecer circunstancias en las que el tratamiento de sus datos personales no requiera el consentimiento del interesado, teniendo en cuenta las circunstancias que se presenten en cada caso individual y en todas las circunstancias, si

las excepciones mencionadas no vulneran los derechos del interesado. En particular, esta ley puede permitir el tratamiento de datos sin el consentimiento del interesado, si el tratamiento se realiza en el marco de la relación jurídica o en el ejercicio de las facultades otorgadas por la autoridad competente".

Como también en el caso de los datos sensibles:

"3.3. la recolección o tratamiento de datos que revelen ideología, filiación religiosa, etc., sólo podrá ser llevado a cabo con el consentimiento del afectado, a menos que esos datos hubieran sido publicados por el afectado. Esto puede ser complicado de aplicar, ya que es necesario tener en cuenta el contexto en el que se revelaron esos datos.

3.4. los datos relacionados con la salud, el origen racial y la vida sexual de una persona sólo podrán ser recogidos y tratados si se obtiene el consentimiento del afectado, o en los supuestos que las leyes o normas reguladoras lo permitan. Es necesario tener en cuenta que estas son categorías de datos muy sensibles y debe respetarse la privacidad de los afectados al máximo.

3.5 Para aclarar, estas directrices no obstaculizarán el tratamiento médico ni la atención a una urgencia vital, siempre y cuando se cumplan los requisitos legales y normativos. En casos de urgencia vital, se podrá tratar información médica sin el consentimiento del paciente, pero solo en la medida necesaria para atender la emergencia

2.3.3 Principio de información

El principio de información exige que el responsable del tratamiento debe informar a los titulares de datos personales de la naturaleza y fin de la recogida y tratamiento de sus datos, además de otros aspectos importantes. Este principio está relacionado con otros principios como el de finalidad, el de calidad y el de consentimiento, entre otros. Es importante aclarar que la información que se debe dar debe ser clara, exacta y comprensible, de modo que el titular de los datos personales pueda

tomar conciencia del alcance y consecuencias del tratamiento que se le realizará a sus datos. Asimismo, se debe proporcionar la información de forma continua y en un lenguaje comprensible, para que sea fácil de entender y aplicar. Además, la información que proporcione el responsable del tratamiento al titular de los datos personales es fundamental para que éste ejerza sus derechos de acceso, rectificación, cancelación u oposición (derechos ARCO), ya que podrá saber quién está tratando sus datos personales. para contactarlo.

2.3.4 Medidas compensatorias

Las medidas compensatorias están específicamente incluidas en la normativa de protección de datos personales de México, por un lado, para dar soluciones a tratamientos de datos personales que ya tuvieron lugar antes de la entrada en vigor de la LFPDPPP, y por otro lado, aquellos que requieren o requieren esfuerzos excesivos. publicar avisos de privacidad. Proporcionar soluciones a situaciones.

El titular de los datos personales siempre debe estar informado sobre el tratamiento de sus datos personales, independientemente de cómo se obtengan los datos personales de forma directa, indirecta o personal. Es decir, si bien pueden existir excepciones a la necesidad del consentimiento, porque el tratamiento de datos personales es requerido por ley o necesario para la ejecución de un contrato, dicho tratamiento debe ser notificado al titular de los datos a través de un aviso de privacidad.

Sin embargo, en algunos casos la notificación al titular de los datos personales puede resultar difícil por una serie de razones establecidas en el PDPO, lo que significa que el responsable del tratamiento debe implementar medidas correctoras. Estos incluyen, por ejemplo, que el responsable del tratamiento notifique al titular de los datos personales mediante la distribución de un aviso de privacidad a través de su sitio web, periódicos de circulación nacional, carteles informativos u otros medios de comunicación masiva. Esto

significa que siempre se debe presentar una declaración de confidencialidad, y sólo en ciertos casos el responsable puede incluso necesitar obtener permiso del INAI. Este aviso de privacidad podrá distribuirse a través de medios como Internet, periódicos u otros medios de comunicación. En todo caso, el titular de los datos personales también deberá prestar atención a los avisos de privacidad así transmitidos a fin de informarse sobre el tratamiento de sus datos personales y la posibilidad de ejercer sus derechos. También se debe tener en cuenta que la declaración de privacidad es un medio para que el administrador cumpla con los principios de información, y el hecho de no proporcionar una declaración de privacidad puede significar una violación de la legislación de protección de datos personales, lo que puede resultar en un procesamiento ilegal.

2.3.5 Principio de calidad

Como se indica en el informe del CJI y otros, la calidad de los datos personales significa en principio que "deben ser correctos, exactos, completos y actualizados según sea necesario de acuerdo con los fines para los que fueron recopilados". Organizaciones de Estados Americanos.

los Estándares Internacionales exigen que la información de los datos personales deba ser precisa, completa y actualizada, de manera que sea apropiada para la finalidad del tratamiento a que se destine. Por ejemplo, una empresa no podría basarse en un currículum viejo o en una dirección obsoleta para realizar un tratamiento, ya que esto sería contrario a los principios de exactitud y actualización de la información, lo cual iría en contra de los estándares internacionales. Esto es importante, ya que la información errónea o desactualizada podría provocar decisiones injustas o incorrectas, o una falta de protección de datos personales. Por eso, es esencial que la información personal sea precisa y actualizada.

Específicamente, los comentarios al proyecto de divulgación de la LFPDPPP se refieren a este principio como "que refleja de manera realista y veraz la situación real de la información que se procesa". También precisa que este principio "debe entenderse específicamente relacionado con la preservación de la veracidad y exactitud de los datos personales".

2.3.6 Principio de finalidad

Las notificaciones del proyecto de decreto por el que se expide la LFPDPPP hacen referencia a este principio, señalando que "el diseño esencial de la privacidad en relación con el tratamiento de datos personales se basa en que el tratamiento se realice sólo para fines específicos, claros y fines legítimos relacionados con las actividades del responsable." Adentro

Además de esta regla general, también reconocemos la posibilidad de dicho tratamiento para otras finalidades, siempre que no sean incompatibles con las finalidades para las que fueron tratados originalmente los datos. "

También es un principio clave de la protección de datos personales y está vinculado a otros principios, en particular los principios de información, consentimiento y calidad.

Los datos personales sólo podrán ser recogidos y tratados con una finalidad específica, y que esta finalidad debe ser justificada. Por ejemplo, una empresa no podría recolectar datos personales de sus clientes para luego usarlos para algo distinto a lo que se les informó inicialmente.

2.3.7 Principio de lealtad

El principio de confianza está relacionado con el principio de derecho, o principio de confiabilidad y legalidad. Según lo establece el manual del INAI sobre el cumplimiento de los principios y obligaciones de la LFPDPPP, “los datos personales

deben ser tratados de manera lícita y leal por los responsables, lo que implica que deben actuar de conformidad con las leyes generales. En particular, las disposiciones sobre protección de datos personales.”

Al respecto, el dictamen publicado por la LFPDPPP y la versión final del proyecto de orden explican este principio, señalando que "esto significa que el tratamiento de datos personales debe realizarse de manera justa y legal, es decir, en pleno cumplimiento". con la ley y el respeto a la integridad y derechos de las personas tratadas.

El tratamiento de datos personales sólo podrá ser realizado si el tratamiento es lícito, o sea, que se cumpla con la normativa aplicable y se respeten los principios de la Ley de Protección de Datos Personales, que garantizan que dicho tratamiento sea legal, de forma apropiada y transparente. Si estos principios no son respetados, el tratamiento será considerado ilegal2

.3.8 Principio de proporcionalidad

Como se explica en el informe del CJI de la OEA, el principio de proporcionalidad se refiere a la necesidad y minimización del procesamiento de datos personales, lo que significa que las personas que procesan datos personales "sólo deben utilizarlos de manera que sea consistente con los fines claramente establecidos para los cuales fue recopilado; si deben proporcionar los servicios o productos solicitados por el individuo. De manera similar, los recolectores de datos y procesadores de datos deben adherirse a un estándar de "limitación" o "minimización", mediante el cual deben hacer esfuerzos razonables para garantizar que los datos personales, proceso cumple claramente con el mínimo necesario para tal fin.

2.3.9 Principio de responsabilidad

El informe del CJI de la OEA también incluye entre los principios el principio de rendición de cuentas, que establece de manera general que "los responsables del

tratamiento deberán tomar e implementar medidas apropiadas para cumplir con estos principios". La "responsabilidad" de quienes procesan datos personales es fundamental para una "protección eficaz de la privacidad y de los datos".

A continuación, incide en el hecho de que este principio: “Se necesita establecerse metas apropiadas en cuanto a la protección de la privacidad. Los controladores de datos, como las empresas y otras entidades, deben respetar estas metas. Al mismo tiempo, deben determinar las medidas más apropiadas para alcanzar esas metas y asegurar que son cumplidas.

2.3.10 Privacidad desde el diseño

Los principios de privacidad por defecto están reconocidos internacionalmente, aunque no están claramente recogidos en las normativas de muchos países. Los principios "pretenden ser un método para permitir que nuevos modelos o prácticas comerciales, especificaciones técnicas e infraestructura física incorporen principios de privacidad de una manera que respete el derecho fundamental a la protección de datos personales".
la privacidad por diseño es un concepto que promueve que la privacidad no debe ser vista sólo como algo que se debe cumplir, sino que debe estar incorporada en todas las partes de la operación de una organización. De esta forma, la privacidad se convierte en un aspecto integral y natural de la organización, en vez de algo que se debe cubrir de forma adicional o específica

2.3.11 Privacidad por defecto

Otro principio importante de protección de datos personales a nivel internacional es el principio de privacidad por defecto (en inglés "default Privacy"), que se menciona en la propuesta de la Comisión para el Reglamento General de Protección de Datos en la actualización de la directiva europea 95/46/CE, y especificado en su artículo. 23, apartado 2: "El responsable del tratamiento implementará mecanismos para garantizar que solo se

procesen en las circunstancias dadas los datos personales necesarios para cada propósito específico, en particular en lo que respecta a la cantidad de datos y al período de almacenamiento recopilados o almacenados que son necesarios para estos fines, estos mecanismos garantizarán específicamente que un número indeterminado de personas no tengan acceso a los datos personales por defecto.

Esto significa que p.e. cuando el responsable del tratamiento desarrolle una solicitud ("Presentación"), prepare un proyecto empresarial o inicie cualquier otra actividad relacionada con el tratamiento de datos personales, deberá hacerlo de tal manera que se garanticen los derechos sobre los datos. el controlador. Proteger los datos personales durante todo su ciclo de vida y en todas las etapas del tratamiento. Esto significa que la protección de los datos personales debe considerarse desde el principio,

Esto nos permitirá promover un alto nivel de protección de los datos personales antes de procesarlos, creando así la confianza necesaria.

CAPITULO III

DESARROLLO DE LAS ACTIVIDADES PROGRAMADAS

3.1 Dirección General de Protección de Datos Personales

La Dirección General de Protección de Datos Personales es la autoridad nacional de protección de datos personales, a la que le corresponde supervisar la gestión y actualización del registro nacional de datos personales y resolver los reclamos de los titulares de datos personales. Protege tus derechos de acceso, rectificación, cancelación y oposición. También brinda opiniones técnicas vinculantes sobre proyectos de normatividad que regulan los datos personales y brinda orientación sobre la correcta aplicación de la Ley de Datos Personales y sus disposiciones.

La Dirección General de Protección de Datos Personales (DGPDP) ejerce sus funciones administrativas y regulatorias a través de unidades orgánicas. En otras palabras, la DGPDP controla la protección de datos personales a través de diferentes áreas, como unidades de asesoría, resolución de problemas, normatividad y sanción.

3.1.1 Dirección de Registro Nacional de Protección de Datos Personales

La Autoridad Estatal de Registro de Protección de Datos Personales es una unidad estructural adscrita a la Administración General de Protección de Datos Personales y es responsable del registro de las bases de datos de datos personales de personas públicas y privadas; sus funciones son:

- Registro de bases de datos personales de gestión pública o privada y de los datos necesarios relacionados con dichas bases de datos, para que los titulares de los datos personales puedan ejercer sus derechos.

Los mandatos, sanciones administrativas, medidas preventivas y correctivas que determinen las autoridades competentes de conformidad con la Ley núm. 29733 (Ley de Protección de Datos Personales). - Código de conducta de las entidades registradas a nombre de propietarios o gestores de bases de datos personales de gestión privada. - Publicar la lista de bases de datos personales de instituciones administrativas públicas y privadas utilizando el portal de la agencia.

3.1.2 Dirección de Supervisión y Control

la Dirección de Supervisión y Control (DSC) es una unidad orgánica de la DGPDP, la cual tiene la tarea de fiscalizar, por oficio o a petición, la protección de los datos personales. La DSC debe supervisar y fiscalizar que todos los actores que traten datos personales estén cumpliendo con la Ley de Protección de Datos Personales y sus disposiciones técnicas.

La DSC supervisa que los datos personales no sean transferidos fuera del país, salvo en casos específicos. Si detecta problemas, comunica a la Dirección de Sanciones para que inicie las sanciones aplicables.

3.1.3 Dirección de Sanciones

La Autoridad Sancionadora es un organismo natural que depende de la Dirección General de Protección de Datos Personales y es responsable de:

- Iniciar procedimientos administrativos sancionadores con base en las actividades inspectoras de la Dirección de Inspección y Control y resolverlos a la mayor brevedad posible.

- Ejecutar las sanciones administrativas impuestas y ejecutar medidas preventivas, correctivas o administrativas en el ámbito de su competencia.

- Imponer multas obligatorias a las personas que no cumplan con sus obligaciones relacionadas con las sanciones en el caso de sanciones.

- Proporcionar al registro nacional de protección de datos personales información actualizada sobre sanciones, medidas preventivas o correctivas.

3.1.4 Dirección de Normatividad y Asistencia Legal

La Oficina de Normatividad y Asistencia Jurídica es una unidad estructural adscrita a la Dirección General de Protección de Datos Personales. Es responsable de formular actos regulatorios relacionados con la protección de datos personales y realiza actividades publicitarias y promocionales de protección de datos. Está controlado por:

- Elaborar proyectos normativos y emitir opiniones sobre los proyectos que se someten a consideración de la Dirección General de Protección de Datos Personales. También prepara informes técnicos basados en las solicitudes de los propietarios de perfiles y de los propietarios de bases de datos de perfiles. - Desarrollar e implementar medidas de comunicación y promoción relacionadas con la protección de datos personales.

3.2 Resolución Schrems

El rápido desarrollo de las tecnologías de comunicación digital significa cambios sin precedentes en la historia de la humanidad. Estas nuevas formas de comunicación

crean nuevos espacios para la participación democrática y brindan a los defensores de los derechos humanos nuevas herramientas para documentar y denunciar los abusos contra los derechos humanos. Además, la popularidad de redes sociales como Facebook o Twitter ha mejorado significativamente el acceso a la información y la comunicación en tiempo real. Sin embargo, esta era digital también presenta desafíos importantes porque la forma en que operan estas comunicaciones digitales aumenta el poder y la capacidad de los gobiernos, las empresas y los individuos para participar en actividades de vigilancia, escuchas telefónicas y recopilación de datos a gran escala y prácticamente ilimitadas.

En particular, las revelaciones del caso Snowden resaltaron estos problemas, ya que revelaron la vulnerabilidad de las comunicaciones digitales a la creación de programas de vigilancia que brindan acceso a grandes cantidades de datos personales. Esto ha atraído considerable atención a nivel internacional y se refleja en diversas iniciativas de las Naciones Unidas y de organizaciones internacionales regionales. De hecho, la Asamblea General de las Naciones Unidas (en adelante, la "Asamblea General de las Naciones Unidas") ha emitido dos resoluciones sobre este tema, instando a los países a proteger los derechos fundamentales en línea, en particular el derecho a la privacidad, y encargando al Alto Comisionado de las Naciones Unidas por los Derechos Humanos. notario. Derechos Humanos (en adelante Oficina Especial del Alto Comisionado para los Derechos Humanos) para redactar un informe sobre el caso.

Sobre la base de lo anterior, la Oficina del Alto Comisionado ha elaborado un interesante informe, que concluye que la vigilancia electrónica a gran escala es una invasión del derecho a la privacidad y que la legalidad de dicha vigilancia debe cumplir con los estándares de legalidad y proporcionalidad. . y deberían sujetarse a los mismos estándares que los derechos efectivos. El derecho a la protección jurídica se refiere a un

cierto grado de supervisión. Por su parte, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión ha emitido varios informes sobre el impacto de las medidas antiterroristas en la protección de estos derechos. A nivel regional y europeo, el Tribunal Europeo de Derechos Humanos (TEDH) ya está escuchando un caso sobre la participación de los servicios de inteligencia británicos en programas de vigilancia masiva. En cuanto a las Américas, la Relatoría Especial de la CIDH ha hecho un informe sobre la libertad de expresión en internet, y ha emitido declaraciones sobre el impacto que pueden tener los programas de vigilancia masiva en los derechos fundamentales

. Para lograr un equilibrio entre la política de seguridad nacional privada y el respeto de la privacidad, la decisión Schrems se considera en este contexto como un caso histórico que finalmente invalidó el Acuerdo de Puerto Seguro porque no respetó el derecho fundamental de vigilancia comunitaria. marco. En base a ello, el presente artículo tiene como objetivo analizar el 6. emitido en octubre de 2015 por el Tribunal de Justicia de la Unión Europea (en adelante, el Tribunal de Justicia de la Unión Europea) Maksimilians Shrems y el comisionado de protección de datos. Para ello, primero hay que analizar el contexto legislativo en el que se pronunció la frase para poder comprenderla mejor.. En segundo lugar, se exponen brevemente los hechos, seguido de un análisis de los argumentos esenciales de la sentencia, que se refieren a dos aspectos fundamentales: por un lado, las competencias de la autoridad nacional de control en materia de protección de datos para tomar decisiones en materia de protección de datos. Por otro lado, según la Carta de Derechos Fundamentales de la Unión Europea (en adelante "CD fue"), esta es la razón principal por la que el Tribunal de Justicia de las Comunidades Europeas reconoce como inválida la decisión de la Comisión Europea.

3.2.1 Contextualización normativa

El artículo 7 de la CDFUE, en la primera parte del inciso 1, establece la existencia del derecho a la privacidad, con respecto a la persona física, o en español, “La protección de los datos de carácter personal respeta fundamentalmente la libertad y la dignidad del hombre”. Esta medida, que se incluyó en el artículo 7, es clave ya que, aunque en la legislación de protección de firma como uno de los principios fundamentales de protección de los datos de carácter personal. A su vez, el artículo 8 establece el respeto de este principio como una garantía en sí mismo. El artículo 8, sección 1, afirma “Cada persona tiene derecho a la protección de sus datos personales.

El artículo 16 del Tratado de Funcionamiento de la Unión Europea (en adelante, el TFUE) confirma claramente el lugar central que ocupa la protección de datos en el sistema jurídico de la Unión Europea (en lo sucesivo, la UE), establece que toda persona tiene el derecho derecho a la protección de los datos personales que les conciernen, y encarga al Parlamento Europeo y al Consejo que desarrollen normas para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En relación con lo anterior, cabe señalar que recientemente ha entrado en vigor el nuevo Reglamento General de Protección de Datos, que sustituye a la anterior Directiva 95/46/CE en la materia. El nuevo Reglamento ha unificado las normas de protección de datos personales en la UE, eliminando la fragmentación que había existido. El nuevo marco regulatorio es más transparente y uniforme, y exige el mismo nivel de obligaciones a todos los responsables del tratamiento de datos personales.

Aunque se menciona el contenido anterior, debe aclararse que el procesamiento de datos personales y la libre circulación de estos datos (en adelante, las instrucciones). Esta instrucción crea un sistema regulatorio detallado para información personal sobre

personas naturales basadas en transacciones comerciales aprobadas por el Sistema de Mercado Europeo

Aunque se menciona el contenido anterior, debe aclararse que el procesamiento de datos personales y la libre circulación de estos datos (en adelante, las instrucciones). Esta instrucción crea un sistema regulatorio detallado para información personal sobre personas naturales basadas en transacciones comerciales aprobadas por el Sistema de Mercado Europeo

De conformidad con este marco jurídico, la Comisión llegó a un acuerdo con el Departamento de Comercio de Estados Unidos, que dio lugar a la adopción de la Decisión 2000/520 (la "Decisión"), que es vinculante para todos los Estados miembros y es la base de esta Resolución El caso Schrem. La decisión creó un sistema de autocertificación bajo el cual las empresas estadounidenses se comprometen a gestionar los datos personales transferidos a los EE.UU. de acuerdo con los principios de "puerto seguro". Tan pronto como las empresas autocertifiquen que cumplen estos principios, se podrá considerar que han alcanzado el nivel de protección establecido en la directiva. Sin embargo, con la revelación del incidente de Snowden, una declaración de la Comisión Europea, donde alerta sobre el incumplimiento del Acuerdo de Puerto Seguro por parte de Estados Unidos. El problema radicaba en que las empresas acreditadas no cumplían con los principios y normas del Acuerdo, lo cual permitía a las autoridades de Estados Unidos acceder y tratar los datos. La Comisión señala que las autoridades de Estados Unidos podían tratar los datos en más ámbitos de lo que debían, yendo más allá de lo que era necesario para la protección de la seguridad nacional. Por ejemplo, las autoridades podían acceder a los datos para fines de investigación judicial o comerciales, de manera incompatible con el Acuerdo. La Comisión también afirmó en dichas cartas que las

personas afectadas ni siquiera cuentan con medios administrativos o legales para acceder a la información que les concierne y, en su caso, corregirla o eliminarla. Estas declaraciones son significativas dado que el TJUE las incorporó al marco jurídico que sirvió de base para resolver las cuestiones subyacentes al caso Schrems.

3.2.2 Los hechos del caso: ¿una muerte anunciada de los principios de puerto seguro?

Los hechos de este caso se relacionan con la demanda ante el Tribunal.

La autoridad irlandesa de protección de datos, el Comisionado Irlandés de Protección de Datos, está dirigida por un joven abogado austriaco que vive en Irlanda, Maximilian Schrem. Como menciona brevemente la orden, el caso está directamente relacionado con las revelaciones de Edward Snowden sobre una serie de programas de vigilancia masiva llevados a cabo por la Agencia de Seguridad Nacional (NSA) y otras agencias asociadas, como la Oficina de Comunicaciones del Gobierno de Estados Unidos. Reino (gchq). os atentados del 11 de septiembre, en Estados Unidos, motivaron la aplicación de programas de recopilación masiva de datos, aplicables a todo el mundo. Esta recopilación no era selectiva, incluyendo a personas no sospechosas de delitos. Esto era incompatible con la finalidad del Acuerdo de Puerto Seguro, y por ello la Comisión consideró que dicho Acuerdo no ofrecía un nivel adecuado de protección para los datos personales transferidos a Estados Unidos. De esta manera, se consideró necesario un nuevo mecanismo de protección de los datos personales para poder trasladarlos a Estados Unidos, con un nivel de seguridad que respetara la protección de los datos personales en la UE. De este modo, se creó el nuevo Acuerdo "Privacy Shield" como mecanismo de protección. La finalidad del tratamiento de los datos recogidos es la de recabar información útil para la prevención y sanción de delitos terroristas. El alcance de estas actividades es internacional y afecta

no sólo a los ciudadanos norteamericanos, sino al mundo entero. Además, estos planes se implementaron en absoluto secreto, con pocas garantías de revisión judicial y una base legal formal en las regulaciones internas. Young Shrems es usuario de Facebook de una de las empresas de telecomunicaciones más importantes del mundo.

Los datos personales de usuarios europeos en Facebook eran trasladados a Estados Unidos. Este proceso era controvertido porque las medidas de protección de datos no eran adecuadas. A causa de ello, Schrems solicitó la prohibición de esa transferencia. a Alta Corte decidió que la Decisión de la Comisión sobre la validez del Acuerdo de Puerto Seguro se había quedado obsoleta. Esto hizo que la Comisión creadora de dicho Acuerdo reanudara los trámites para establecer un nuevo sistema de transferencia, esta vez en pleno cumplimiento de los principios del derecho de protección de datos europeo dio lugar al Acuerdo Privacy Shield, que sustituye al anterior Acuerdo de Puerto Seguro. Este nuevo acuerdo, más restringido que el anterior, se basa en una declaración jurada de las empresas estadounidenses y en un sistema de mecanismos alternativos de protección como garantía de seguridad, lo que ya no es una mera declaración de la Comisión sobre la validez de la protección de datosAdemás, consideró que la interpretación de la decisión de la Comisión Europea de conformidad con la Directiva 95/46/CE planteaba la cuestión de la aplicación de la legislación de la UE en los Estados miembros de conformidad con el artículo 51 cd, por lo que decidió presentar un informe preliminar. sentencia al Tribunal de Justicia de las Comunidades Europeas (Tribunal). de la Unión Europea). Utilizando este mecanismo, el Tribunal Superior formuló las siguientes preguntas: 1) En primer lugar, preguntó si el Comisario irlandés estaba obligado por la protección de los derechos fundamentales contenidos en la Carta de Niza, aunque la decisión aceptaba que Estados Unidos garantiza un cierto nivel de derechos fundamentales. derechos. protección adecuada. 2) En segundo

lugar, preguntó si el Comisario irlandés podría abrir una investigación independiente sin perjuicio de las disposiciones de esta decisión.

El TJUE dio una larga explicación sobre los motivos por los cuales invalidó el Acuerdo de Puerto Seguro. En primer lugar, el TJUE afirmó que la Ley de Inteligencia de Estados Unidos, que otorgaba autoridad a la agencia de seguridad nacional de Estados Unidos (nsa) para realizar programas de vigilancia masiva, no garantiza un nivel de protección adecuado para los datos personales transferidos a Estados. Las autoridades nacionales de control de datos son una parte fundamental de la protección de los derechos fundamentales. Su función es velar por la correcta implementación de la normativa de la UE en el campo de la protección de los datos personales. Estas autoridades deben garantizar la protección de los derechos fundamentales de las personasPara que estas agencias puedan desempeñar sus funciones eficazmente, deben ser agencias independientes. A este respecto, el Tribunal de Justicia de las Comunidades Europeas ha afirmado reiteradamente en su jurisprudencia que "dicha independencia excluye no sólo cualquier influencia que pueda ser ejercida por la entidad controlada, sino también cualquier orden o influencia externa, directa o indirecta, que pueda dar lugar a a las obligaciones". La tarea de las instituciones antes mencionadas es crear un equilibrio razonable entre la protección de la privacidad y el libre intercambio de datos personales. "En este sentido, el Tribunal de Justicia de la Unión Europea ha emitido una serie de sentencias en las que considera que determinados Estados miembros han violado la directiva, al no estar garantizada la "completa independencia" de estas instituciones en el desempeño de sus funciones. Cabe señalar también que estas autoridades tienen amplios poderes, en particular: poderes de investigación, como el poder de recopilar toda la información necesaria para llevar a cabo sus tareas de control, poderes de intervención efectiva, como una prohibición temporal o inequívoca del procesamiento de datos. . , e

incluso la posibilidad de reunirse en los tribunales. La *Sentencia de Schrems en el Tribunal de Justicia de las Comunidades Europeas 221 National Law Journal Número 40, enero-junio de 2018, página 221. La Ley N° 209-236 reconoció en el caso Weltimmo que la autoridad de control no sólo puede imponer. Estos poderes también pueden usarse contra empresas utilizando poderes efectivos y reales a través de robustas instalaciones de procesamiento de datos personales. El territorio del país donde está ubicada la autoridad de control. Por tanto, la sentencia citada se refiere a un concepto bastante flexible de "empresa".* Con esta sentencia, el Tribunal utilizó el principio de territorialidad para abordar eficazmente la cuestión de las empresas que crean realidades comerciales alternativas para vincularse al régimen legal y de aplicación de otro Estado miembro más permisivo, ya que las leyes nacionales de protección de datos no son actualmente las mismo. todas las instituciones Es positivo que también existan ciertas diferencias en la traducción de las directivas entre los distintos Estados miembros

El principal debate del TJUE es si las autoridades nacionales, como el Comisario Irlandés, tienen la facultad de examinar las solicitudes y autorizar o rechazar las transferencias de datos hacia Estados Unidos. El TJUE intenta responder a la pregunta de si la Decisión de la Comisión impide que las autoridades nacionales realicen este tipo de verificaciones. A A este respecto, el Tribunal señaló que incluso si la Comisión toma una decisión, siempre que se garantice una protección suficiente, las autoridades nacionales de control tendrán derecho a examinar la denuncia para comprobar si la transferencia de datos de personas físicas a terceros países es llevado a cabo adecuadamente. de acuerdo con los requisitos de la directiva. Las personas antes mencionadas son los máximos responsables de la supervisión del procesamiento de datos en su territorio, lo que incluye el control de las transferencias de datos personales fuera de la UE. Además, el Tribunal afirmó que la Directiva debe interpretarse de conformidad con la Carta y no contiene disposiciones que

impidan a estas autoridades controlar las transferencias de datos a terceros países si se toma una decisión sobre el nivel adecuado de protección.

el TJUE considera que, mientras la Decisión no haya sido declarada invalida por él, no pueden adoptarse medidas contrarias. Las autoridades nacionales como el Comisario Irlandés deben respetar la Decisión, por tratarse de una norma que es obligatoria para todos los Estados miembros. Entonces, si la Decisión aún no ha sido declarada inválida, no pueden tomar medidas contrarias a la Decisión. Esto significa que mientras que la Decisión no sea declarada inválida, no pueden prohibir las transferencias de datos a Estados Unidos. El TJUE hace hincapié en que esto no significa que los ciudadanos o empresas no tengan derecho a interponer acciones legales que reclamen la protección de sus derechos en los tribunales nacionales. Las autoridades de control tienen que examinar las solicitudes con la diligencia necesaria. Esto implica que deben analizar si la solicitud es razonable, si los datos que apoya son válidos y si se pueden tomar medidas alternativas. En primer lugar, las autoridades concluyeron que los datos que respaldaban la solicitud eran infundados y por lo tanto la rechazaron. En tal caso, la persona que presenta la solicitud debe disponer de recursos legales que le permitan impugnar la decisión ante un tribunal nacional. Si estos tribunales consideran que se han establecido uno o más motivos de nulidad, invocados por las partes o conocidos de oficio, están obligados a suspender el caso y someter cuestiones preliminares de validez al Tribunal de Justicia de las Comunidades Europeas. Más bien, si la Agencia considera que las acusaciones están bien fundadas, debería tener competencia para comparecer ante el tribunal nacional con su consentimiento para plantear cuestiones preliminares sobre la validez de la decisión de la Comisión.

sentencia podría haber incluido la posibilidad de que las autoridades de control pudieran solicitar una modificación de la Decisión de la Comisión si hubiesen dudas sobre su validez, en lugar de obligar a los ciudadanos a tomar el asunto a un tribunal

La sentencia refuerza el papel de las autoridades nacionales de control, obligándolas a actuar como guardianes de los derechos fundamentales y, al mismo tiempo, les da claridad en la acción que deben tomar ante una decisión de la Comisión que afecte esos derecho. Estas facultades son las siguientes: 1) investigar quejas presentadas por personas naturales sobre el procesamiento de sus datos personales en otros países; 2) presentar casos ante los tribunales nacionales para impugnar la validez y el cumplimiento de las decisiones; 3) suspender el uso de datos personales si se considera que no se ha logrado un nivel de protección suficiente. Transferencia de datos personales a otros países. 4El papel de los derechos fundamentales en la invalidez de las normas comunitarias El aspecto más llamativo de la decisión Schrems es, sin duda, que el reconocimiento de la invalidez de normas jurídicas comunitarias (como las decisiones de la Comisión Europea) se basa en el hecho de que este argumento está en conflicto con el discurso CD se han considerado los derechos fundamentales para este fin como base reguladora. Los derechos fundamentales considerados vulnerados en este caso fueron el derecho a la vida privada y el derecho a la tutela judicial efectiva. se podría afirmar que la sentencia Schrems deja abierto el debate sobre la relación y distinción entre el derecho a la privacidad y el derecho a la protección de datos personales. Dado que son dos derechos distintos, ¿pueden existir aplicaciones diferentes en cuanto a su protección? ¿Qué sentido tiene, entonces, la sentencia, que contempla la noción de “dato personal” sin llegar a definirla? ¿Cómo puede una sentencia regular y proteger un concepto que no se define? Esto deja una ausencia en la jurisprudencia y la legislación en torno a este concepto. Epl,l derecho a la protección de datos personales no es simplemente una

cuestión de privacidad, sino que es un derecho de control. En lugar de solamente proteger el acceso a la información personal, este derecho permite ejercer control sobre el tratamiento de esa información y su uso, sin duda una noción más amplia que el concepto de privacidadIndependientemente de estas consideraciones, creemos que el Tribunal de la UE debería intentar separar conceptualmente estos dos derechos en la jurisprudencia futura. Sin embargo, Schrem considera que se ha vulnerado el contenido esencial del derecho a la intimidad y a la tutela jurídica efectiva y realiza los siguientes comentarios. 4.1. Elementos básicos de las violaciones de la privacidad La decisión de la Comisión Europea supone que Estados Unidos cumple con el nivel adecuado de protección de la Directiva. Dado que la Directiva no proporciona una definición, cabe preguntarse qué significa "apropiado". Al interpretar la Directiva, la sentencia Schrems determinó que el nivel adecuado de protección debe evaluarse a la luz de una serie de factores relevantes para la transferencia de datos, todos los cuales se establecen en el artículo 25, apartado. El criterio más importante para determinar si la protección es suficiente es la protección de los derechos fundamentales de terceros países, en particular la protección del derecho a la vida privada. Para cumplir con este criterio, el Tribunal sostuvo que los terceros países no deberían tener el mismo nivel de protección que la UE, sino que debería ser "sustancialmente equivalente". Para matizar esta cuestión hay que tener en cuenta los términos del CD, de lo contrario la transferencia de datos a terceros países violará los derechos fundamentales de los ciudadanos de la UE. En resumen, es comprensible que el sistema jurídico de un tercer país pueda ofrecer diversos medios de protección, pero en realidad su nivel de eficacia debería corresponder básicamente al nivel de protección garantizado por los 59 países de la UE.

Para determinar si se había violado el derecho a la privacidad previsto en el artículo 7 del CD, la decisión Schrems se basó en un doble razonamiento. En primer lugar, aclaró que se está obstaculizando el ejercicio de estos derechos en detrimento de los ciudadanos europeos. En segundo lugar, afirma que dicha interferencia constituye una violación del derecho fundamental a la privacidad. A continuación se presenta un análisis en profundidad de estos dos argumentos. Para determinar si se produjo interferencia, el fallo Schrems evaluó el sistema legal interno de los Estados Unidos para determinar si protegía adecuadamente los datos personales transferidos desde Europa. el tjue consideró que la Decisión de la Comisión no garantizaba la protección adecuada del derecho a la privacidad. De hecho, no estaba claro si este principio tenía un papel similar a la seguridad nacional norteamericana, y se podía inferir que se priorizaba esta última a costa del primer. Esto, según el Tribunal, daba una impresión de inferioridad de los principios de la Dirección General para la Protección de Datos. El tjue considera que, por la naturaleza del Acuerdo, la autocertificación por parte de las empresas tampoco garantizaba la protección adecuada de los datos personales, ya que podía estar supeditada a la legislación norteamericana y ponerse en conflicto con los principios del Acuerdo.

El tribunal reconoció que una configuración intrusiva no viola automáticamente el derecho a la privacidad porque dichas intrusiones pueden limitarse cumpliendo ciertos estándares que han sido sostenidos en su jurisprudencia anterior. De hecho, según el artículo 52(1) de la era de la CD, las limitaciones de los derechos protegidos por este tratado deben cumplir dos criterios principales: el contenido esencial y el principio de proporcionalidad. El objetivo de esta disposición es advertir que la legalidad de las restricciones al ejercicio de los derechos fundamentales dependerá del cumplimiento de estos estándares fundamentales. El tribunal reconoció que una configuración intrusiva no

viola automáticamente el derecho a la privacidad porque dichas intrusiones pueden limitarse cumpliendo ciertos estándares que han sido sostenidos en su jurisprudencia anterior. De hecho, según el artículo 52(1) de la era de la CD, las limitaciones de los derechos protegidos por este tratado deben cumplir dos criterios principales: el contenido esencial y el principio de proporcionalidad. El objetivo de esta disposición es advertir que la legalidad de las restricciones al ejercicio de los derechos fundamentales dependerá del cumplimiento de estos estándares fundamentalesSin embargo, esta posición sigue siendo controvertida, ya que la distinción entre contenido del mensaje y metadatos se vuelve borrosa en el contexto de la protección de la privacidad. Acceder al contenido de la comunicación. Creemos que la recopilación y el procesamiento de metadatos pueden violar los elementos básicos de la privacidad porque permite sacar "conclusiones muy precisas sobre la privacidad de la persona cuyos datos se almacenan, como hábitos diarios, lugar de residencia permanente o temporal", rutina diaria. u otras actividades, actividades realizadas, relaciones sociales y redes sociales de uso frecuente. Sin embargo, al no acreditarse el acceso a los contenidos, la Agencia Irlandesa de Derechos Digitales concluyó que se había vulnerado el derecho a la privacidad por no respetar el principio de proporcionalidad. En resumen, según la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, el test de proporcionalidad en casos de privacidad debe cumplir tres criterios: 1) la interferencia se produce para lograr un objetivo legítimo; 2) se completa la verificación de cumplimiento, es decir la interferencia es apropiada para lograr el objetivo establecido 3) Llevar a cabo la prueba de necesidad, es decir. la intervención es absolutamente necesaria para lograr el objetivo planteadoLa ley digital irlandesa determinó que este último criterio se incumplió porque el sistema de almacenamiento de datos no cumplía con ciertas salvaguardias mínimas, como limitaciones de alcance, intervención de las autoridades reguladoras nacionales, la

introducción y la posibilidad de un período de retención de datos reducido. medidas correctivas efectivas. Lo sorprendente de la sentencia Schrems es que el Tribunal de Justicia de las Comunidades Europeas cambió el contenido de la sentencia anterior y concluyó que se había violado el contenido básico del derecho a la privacidad. Consideró que "las reglas que brindan a las autoridades públicas acceso general al contenido de las comunicaciones electrónicas violan un elemento esencial del derecho fundamental a la privacidad". Schrem aplicó este estándar al principio de puerto seguro y concluyó que, dado el mandato general de preservar la regulación, los datos personales de todos los individuos no se limitan a lo estrictamente necesario, lo que efectivamente es una violación de contenido sustancial. Las transferencias de la UE a EE.UU. no establecen distinciones, limitaciones o excepciones basadas en las finalidades indicadas, ni contienen criterios objetivos para limitar el acceso y posterior uso de los datos por parte de las autoridades públicas. Fines limitados y específicos para justificar la terminación del acceso y uso de estos datosLa opinión fue crucial porque demostró que el tribunal creía que los programas de vigilancia masiva revelados por Snowden eran creíbles, incluso si no se detuvo a reflexionar sobre su respaldo probatorio. Además, considera este tipo de acuerdos una violación inaceptable del derecho a la vida privada y, por tanto, establece un estándar que debe aplicarse en futuros casos de naturaleza similar y debe ser tenido en cuenta por otros tribunales internacionales. Finalmente, cabe señalar que el Tribunal de Justicia de la Unión Europea consideró que se había violado el contenido esencial del derecho a la privacidad y se negó a analizar el principio de proporcionalidad. Esta conclusión es instructiva y permite demostrar que el Tribunal de Justicia de las Comunidades Europeas considera que estas medidas afectan en cierta medida a la protección de los derechos fundamentales. 4.2. Violación del contenido básico del derecho a la tutela judicial efectiva La sentencia Shrems también consideró que se había

violado el contenido básico del derecho a la tutela judicial efectiva. La jurisprudencia del Tribunal de Justicia de la Unión Europea enfatiza que la existencia de un control judicial efectivo para garantizar el cumplimiento de la legislación de la UE es una característica integral del Estado de derecho. En este caso, la legislación nacional norteamericana no proporciona un recurso efectivo para que un ciudadano europeo afirme que se han violado sus derechos fundamentales en relación con los datos personales80 porque "necesita estas garantías aún más" cuando los datos personales se procesan y se accede a ellos automáticamente. ilegalmente. Esto es importante cuando hay mucho en juego. " En consecuencia, se vulnera claramente el contenido esencial del derecho a la tutela judicial efectiva. Además, la aplicación de la legislación comunitaria no puede impedir la implementación de una protección jurídica efectiva, que en el caso de los datos personales se proporciona a través de las autoridades nacionales de control.

3.3 Protección de Datos Personales y el principio de Legalidad

Ley General del Procedimiento Administrativo Decreto Conjunto No. El texto de la 27444, aprobado por Decreto Supremo 004-2019-JUS, establece el derecho de oposición en procedimientos administrativos a favor de una persona que se rige por el artículo 217. Estos derechos se realizan a través de lo que llamamos derechos administrativos. recursos. En vista de ello, el artículo 218 de la mencionada autoridad de control establece que los recursos administrativos incluyen el retratamiento, el recurso y la revisión. Sin embargo, es necesario aclarar la naturaleza de estos recursos, por lo que la Corte Constitucional dispone lo siguiente en su decisión en el oficio No. 3741-2004-AA/TC.

(RAMÓN HERNANDO SALAZAR y ARLENQUE, 2005):

El derecho a recurrir una decisión administrativa no debe, por supuesto, confundirse con el derecho de apelación o el derecho a duplicar el proceso administrativo, que, como ha dicho esta academia, no pueden configurarse como derechos constitucionales ejecutivos. , porque bajo ningún concepto se puede obligar al ejecutivo a considerar la doble pena como un derecho fundamental. El derecho a recurrir decisiones administrativas prevé la posibilidad de subvertir dichas decisiones tanto en el propio proceso administrativo, invocando el mecanismo previsto en la ley, como en todo caso de forma amplia y en toda la defensa, cuando se vea amenazado el impacto de los derechos fundamentales. . Las denuncias pueden presentarse ante los tribunales mediante procedimientos administrativos contradictorios o incluso a través de las propias denuncias.

Aunado a ello, tenemos que (CHAVARRI CARDENAS, 2018), ha precisado lo siguiente:

> *(...) Las agencias administrativas no son una protección real para los gobernados, ni un sistema judicial está configurado adecuadamente para proteger a los gobernados de la interferencia del gobierno. En otras palabras, a nivel administrativo, la existencia de una o más agencias responde a principios organizativos administrativos más que a la existencia de garantías a favor de los directivos. También debe quedar claro que las mencionadas "garantías reales" incluyen asegurar que el administrador reciba una decisión objetiva de una autoridad judicial que no tenga relación con ninguna autoridad administrativa de la entidad cuya decisión se impugna. Por tanto, no es juez y parte como en los casos administrativos*

En resumen, el derecho a disentir por la vía administrativa puede considerarse como la materialización del derecho a la defensa previsto en el artículo 139, numeral 14 de la Constitución Política del Perú, ya que contiene un mecanismo para que los órganos administrativos impugnen una decisión gubernamental, no confundirse con el derecho a audiencias múltiples de conformidad con el artículo 139, párrafo 1. El artículo 6 de la constitución política del Perú, que limitaría su aplicación a la sede del poder judicial.

1. Situación Controversial

Ahora bien, en relación con el derecho a la protección de datos personales como expresión del derecho a la autodeterminación informativa, tenemos la Ley No. 29733 sobre protección de datos personales y sus disposiciones, aprobado por Decreto Supremo n. 003-2013-. LA LEY. Cabe señalar que dicha autoridad de control, entre otras cosas, monitorea los procedimientos de sanciones administrativas llevados a cabo por la autoridad nacional de protección de datos personales, iniciados por posibles violaciones al derecho a la protección de datos personales.

En este contexto y la situación actual, cabe señalar que la Ley de Protección de Datos Personales núm. 29733 Artículo 117, aprobado por Decreto Supremo núm. 003-2013-JUS, le permite tomar decisiones razonables. en los casos en que no sea necesario iniciar procedimientos sancionadores. Nuevamente, su significado literal es que el denunciante puede ejercer el derecho de apelar contra tal decisión..

En este contexto, aunque generalmente en los procedimientos administrativos sancionadores no se considera que los denunciantes estén sujetos a este procedimiento, las disposiciones especiales en materia de protección de datos personales definen una categoría separada a tal efecto: cada denunciante tiene el derecho Contradicción: acto administrativo de que se trata. en la decisión sobre el inicio de un caso que no está justificado para el inicio del proceso sancionador.

2. Cuestión en Debate

Ahora consideramos necesario aclarar que el Artículo 4, Parte 1.1. Ley núm. 27444 Ley de Procedimiento Administrativo General aprobada por Decreto Supremo no. 004-2019-JUS, el título transitorio del texto del procedimiento general establece los siguientes principios: Legalidad, que señala: “Las instituciones administrativas deben

cumplir con la Constitución, las leyes y los derechos en el ámbito de sus competencias y de conformidad con las fines para los cuales son asignados."

En relación con este tema, hemos manifestado (GUZMAN NAPURI, 2017) lo siguiente: "(…) El principio de legalidad es uno de los elementos que integran el Estado de derecho, porque es una limitación efectiva de la norma. del derecho. El poder del Estado es la observancia de los derechos individuales.

En complemento a ello, (MORON URBINA, 2017), indica lo siguiente:

Si bien se ha utilizado el tradicional nombre de "legalidad" para referirse a este principio, realmente debe reconocerse que los órganos administrativos se rigen por la ley y no sólo por una de sus fuentes, como la ley, como prefieren llamarla algunos autores. "legalidad". Según este principio, los sujetos deben entenderse sujetos a todo el sistema normativo, desde los principios generales del derecho y la constitución estatal hasta los simples precedentes administrativos que garantizan la igualdad en su fiscalización a través del derecho formal, el ámbito general de las actividades administrativas y finalmente las administrativas definidas. contratos.

Sin embargo, es claro que cada unidad estructural de la administración estatal, observando las condiciones del principio de legalidad, debe legalizar sus acciones, es decir, en el marco de todo el sistema regulatorio, independientemente del alcance o naturaleza de la legislación. . el precio. Por lo tanto, la Ley de Protección de Datos Personales N° aprobada por Decreto Supremo 003-2013-JUS 29733 El cumplimiento de lo dispuesto en el artículo 117 encuentra mayor sustento en los principios antes mencionados.

Sin embargo, la Autoridad Estatal de Protección de Datos Personales (Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales) señaló en diversos comunicados[3] que las quejas administrativas presentadas por diversos denunciantes sobre la decisión resolvieron la improcedencia temporal. La agencia no analiza su denuncia (o equivalente: no vale la pena iniciar procedimientos sancionadores por posibles violaciones de las normas de protección de datos personales). La razón es que no tienen la condición de tercero gobernado porque no están involucrados en el caso y, por lo tanto, no tienen derecho legal a expresar una opinión.

Esta justificación es contraria a lo dispuesto en él, pues según la Ley núm. 29733 Artículo 117 de la Ley de Protección de Datos Personales, aprobada por Decreto Supremo 003-2013-JUS, Artículo 4, Inciso 4. 1, apartados iniciales 1.1. sección, de conformidad con el Artículo 004 - Ley General del Procedimiento Administrativo, Ley Nro. 27444 texto de la orden unificada aprobada por Decreto Supremo núm. 2019-JUS, brinda soporte jurídico suficiente y efectivo a la decisión sobre el recurso administrativo interpuesto por el denunciante por encima del umbral de infracción.

CAPITULO IV

RESULTADOS OBTENIDOS

Conclusiones

1. El derecho a oponerse en el proceso administrativo es una concreción del derecho a la defensa previsto en el artículo 139, apartado 14 de la Constitución Política del Perú, al contener un mecanismo destinado a que las personas sujetas a la administración puedan impugnar decisiones administrativas.
2. El derecho a disentir en procedimientos administrativos no debe confundirse con el derecho a múltiples audiencias previsto en el artículo 139, apartado 1. El artículo 6 de la constitución política del Perú, que limitaría su aplicación al poder judicial.
3. Aunque en los casos de sanciones administrativas el denunciante no suele ser considerado sujeto del proceso, la Ley de Protección de Datos de las Personas Físicas núm. 29733 Se aprueba el artículo 117 mediante Decreto Supremo núm. 003-2013-JUS Ordret y sin duda. , cada denunciante tiene derecho a impugnar la actuación administrativa contenida en la decisión de inicio del expediente, que no esté justificada para el inicio de procedimientos sancionadores.
4. El principio de legalidad definido en el artículo 4. Por Decreto Supremo No. 004-2019-JUS aprobó Ley de Procedimiento Administrativo General núm. 27444 del título transitorio del texto del procedimiento general 1.1. El punto señala que la administración estatal de cada entidad debe formular sus acciones en el marco legal (es decir, todo el sistema regulatorio), independientemente del alcance o tipo de marco legal.

4. En respuesta a las quejas administrativas presentadas por diversos denunciantes respecto de las actuaciones administrativas, la Autoridad Estatal de Control de Datos Personales manifestó que estas actuaciones administrativas no son motivo para el inicio de procedimientos sancionadores por posibles violaciones al Reglamento de Datos Personales y que así lo han sido. por lo tanto, porque las referidas denuncias no formaron parte de la parte procesal y, por tanto, no se les administra la condición de tercero y por lo tanto no están legalmente facultadas para pronunciarse.

Recomendaciones

1. Teniendo en cuenta la Ley núm. 29733 sobre protección de datos personales, aprobado por Decreto Supremo n. 003, lo dispuesto en el artículo 117, flagrante violación de la ley por parte de la Oficina Estatal de Protección de Datos Personales. obvio. 2013-JUS, de conformidad con el artículo 4 de la Ley N° aprobada por el Decreto Supremo 004-2019-JUS. 27444 "Ley de Procedimiento Administrativo General" en la sección introductoria del texto de la orden combinada 1.1 tiene suficiente sustento legal, por lo que se recomienda que la ley sea adoptada a nivel legislativo. Se modifica para especificar completamente la autoridad nacional de control de protección de datos que atiende o decide sobre las quejas y que forman parte del procedimiento.

Referencias Bibliográficas

1. ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. (1999). La defensa de la intimidad de los ciudadanos y la tecnología informática. Editorial Aranzadi.
2. BERNALES BALLESTEROS, E. (1999) La Constitución de 1993. Comentarios. 5º Edición. Editora RAO SRL.
3. CARNOY, M. (2000). El trabajo flexible en la era de la información. Alianza Editorial.
4. CASTELLS M. (2000). La era de la información, economía, sociedad y cultura. La sociedad red. Vol. 1. Editorial Alianza.
5. CORRAL TALCIANI, H. (2000) "Configuración jurídica del derecho a la privacidad I: Origen, desarrollo y fundamentos" en Revista Chilena de Derecho, Volumen 27, Nº 1.
6. CORRALES, M.; BARNITZKE, B y FORGÓ NIKOLAUS; BOUCHOUX, María Clara. (2011). Aspectos Legales de la computación en la Nube: protección de datos y marco general sobre propiedad intelectual en la legislación europea. Tomo I. Editorial Allbremática.
7. COSTA PICAZO, R. (trad.) (2001) IBM y el Holocausto. Editorial Atlántida.
8. CUKIER, K. (2014) Losbig datayelfuturode losnegocios. Editorial del BBVA.
9. EVANS, P. (2014) Reinventarla empresaen la eradigital. Editorial del BBVA.
10. FUNDACIÓN KONRAD ADENAUER STIFTUNG. (2009). Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de

las sentencias más relevantes compiladas por JürgenSchwabe. Editorial Fundación Konrad Adenauer.

11. GARCÍA MEXÍA (2005) PrincipiosdeDerechodeInternet.Editorial Tirant lo Blanch.

12. GONZÁLEZ, ENRIC (2001) "IBM, al servicio del holocausto: Un libro describe cómo el régimen de Hitler clasificó a sus víctimas con material de la firma estadounidense" en Diario El País, Ediciones El País S.L.

13. GONZÁLEZ, F. (2015) Reinventar la empresa en la era digital. Editorial BBVA, Madrid, 2015.

14. GOZAÍNI, O. (2001) Habeas data protección de datos personales. Editorial RubinzalCulzoni, Buenos Aires. 15. HERNÁNDEZ LÓPEZ, J. (2013). El derecho a la protección de Datos Personales en la Doctrina del Tribunal Constitucional, Editorial Thomson Reuters Aranzadi.

16. HERRÁN ORTIZ, A. (1998) La violación de la intimidad en la protección de datos personales. Editorial Dykinson.

17. KRESALJA, B.; OCHOA C. (2009) Derecho Constitucional Económico. Fondo Editorial de la Universidad Católica del Perú. 1

8. ISACA (2009) Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y Aseguramiento, Editorial Isaca.

ANEXOS

Anexo 1. Evidencia de Similitud Digital

LA AUTORIDAD NACIONAL DE PROTECCION DE DATOS PERSONALES Y EL PRINCIPIO DE IGUALDAD

INFORME DE ORIGINALIDAD

19%	19%	8%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	revistas.uexternado.edu.co Fuente de Internet	4%
3	repositorio.upci.edu.pe Fuente de Internet	2%
4	www.scielo.org.co Fuente de Internet	2%
5	cdn.www.gob.pe Fuente de Internet	1%
6	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	1%
7	documentop.com Fuente de Internet	1%
8	docplayer.es Fuente de Internet	<1%

Anexo 2. Autorización de Publicación en el Repositorio

UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACION O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: TORCHONYA DAE LUZ ROXANA

DNI: 73052439 Correo electrónico: luzete@gmail.com

Domicilio: Av. SALAVERRY S/N BARRIO MURALLONES - CHACHAPOYAS

Teléfono fijo: _____ Teléfono celular: 952 334 837

2.- IDENTIFICACIÓN DEL TRABAJO o TESIS

Facultad/Escuela: _____

Tipo: Trabajo de Investigación Bachiller ( ) Tesis ( ) Trabajo de Suficiencia Profesional (X)

Titulo del Trabajo de Investigación / Tesis:

LA AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES Y EL PRINCIPIO DE IGUALDAD

3.- OBTENER:

Bachiller ( ) Titulo (x) Mg ( ) Dr ( ) PhD ( )

4 AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRONICA

Por la presente declaro que el (trabajo/tesis) TRABAJO indicada en el item 2 es de mi autoria y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencia e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art 23 y Art. 33.

Autorizo la publicación (marque con una X):
(x) Sí, autorizo el depósito total.
( ) Sí, autorizo el depósito y solo las partes: _____
( ) No autorizo el depósito.

Como constancia firmo el presente documento en la ciudad de Lima, a los 16 días del mes de NOVIEMBRE de 2023.

Huella digital

Firma