Introducción a la privacidad y el cumplimiento para los consumidores (v3)

Por Clare Nelson

Actualizado por el Comité del Cuerpo de Conocimiento de IDPro

Para comentar sobre este artículo, visite nuestro repositorio de GitHub y envíe su consulta.

Tabla de Contenidos

Descargo de responsabilidad
Este artículo no debe considerarse un consejo legal. Los programas de identidad que respaldan la protección de datos y la privacidad como un derecho humano fundamental son complejos y altamente técnicos. Muchas de las leyes de privacidad y protección de datos en países de todo el mundo están evolucionando y están abiertas a interpretación. Consulte al asesor legal de su organización para obtener asesoramiento específico apropiado para su jurisdicción.

Resumen

Este artículo introductorio sobre privacidad y cumplimiento en el dominio IAM del consumidor sienta las bases para las secciones posteriores sobre privacidad dentro del Cuerpo de conocimientos de IDPro, y proporciona una descripción general de una variedad de temas, incluidas definiciones de privacidad, diferentes enfoques de la privacidad en el sector del consumidor versus el entorno laboral, entre otros temas.

Secciones relacionadas en el cuerpo de conocimientos de IDPro

Consulte otras secciones del *Cuerpo de conocimientos de IDPro*[1] para obtener información de apoyo y complementaria, en particular:

- "Una introducción al RGPD" de Andrew Cormack[2]
- "Impacto del RGPD en la gestión de acceso e identidad" de Andrew Hindle
- "Terminología en el Cuerpo de Conocimiento IDPro"

Introducción a la privacidad y el cumplimiento para los consumidores

Los profesionales de la identidad, incluidos los arquitectos de soluciones empresariales, los científicos de datos que trabajan en marketing, los profesionales de la privacidad, los gerentes de productos y los estrategas de los corredores de datos, tienen la oportunidad de mejorar la privacidad y el cumplimiento de las normas y leyes de protección de datos para las aplicaciones orientadas al consumidor. Varios problemas críticos impulsan la necesidad de mejora:

1. La identificación única de una persona física, como un consumidor, es más fácil que nunca. El fragmento más pequeño de información sobre actividades digitales, acciones físicas o atributos se puede recopilar, correlacionar a través del aprendizaje automático y analizar para identificar un consumidor u hogar único con suficiente probabilidad.
2. El consentimiento está roto. La complejidad de los avisos de privacidad y la extensión de las políticas de privacidad que rara vez se leen conducen a un patrón de ineficacia, la ilusión de elección, una carga para el consumidor y el eventual

[1] "Cuerpo de conocimiento de IDPro," IDPro, https://www.idpro.org/body-of-knowledge/.
[2] Cormack, Andrew, "Introducción al RGPD (v2)," Cuerpo de conocimiento de IDPro, 30 de junio de 2021, https://bok.idpro.org/article/id/11/.

acuerdo de términos amplios que pueden no tener límites o pueden modificarse en cualquier fecha futura tan solo con un aviso limitado o poco claro. Como ha declarado el experto en derecho y privacidad Daniel Solove, "Dar a las personas más tareas para administrar su privacidad no proporcionará una protección efectiva de la privacidad".[3] Cada vez se comprende más que las leyes de privacidad deben hacer que la administración de los datos sea responsabilidad del controlador de datos y/o del procesador de datos, no del consumidor.

3. Las leyes de privacidad de datos están atrasadas de varios años con respecto a las innovaciones tecnológicas, y eso hace que la brecha se esté expandiendo. Las leyes de privacidad no pueden seguir el ritmo de los avances tecnológicos y llevan años de retraso en ponerse al día con los 4000 corredores de datos y empresas de análisis que recopilan datos personales en todos los puntos de contacto, muchos de los cuales están ganando fuerza con el aprendizaje automático. Muchas empresas de marketing, además de algunas de las organizaciones más grandes del mundo, están buscando alternativas a las *cookies* de terceros para poder continuar identificando a los consumidores, todo dentro de las pautas permeables de la ley de privacidad actual.

4. El anonimato no existe y la seudonimización proporciona una protección débil
    a. Por ejemplo, los investigadores han demostrado que, basándose únicamente en la geolocalización, el anonimato no existe.
    b. Del mismo modo, los investigadores postulan que cada vez es más fácil volver a identificar a una persona:

        i. Una vez liberados al público, los datos no se pueden recuperar. A medida que pasa el tiempo, las técnicas de análisis de datos mejoran y se hacen públicos conjuntos de datos adicionales que pueden revelar información sobre los datos originales. De ello se deduce que los datos publicados serán cada vez más vulnerables a la re-identificación, a menos que se utilicen métodos con propiedades de privacidad comprobables para la publicación de datos.[4]

    b. *Comunicaciones de la ACM* publicó recientemente un artículo sobre el anonimato que confirma lo que muchos matemáticos siempre han sabido: sigue habiendo un patrón en los datos anónimos y una forma de quitarles el anonimato.[5]

---

[3] Solove, D., "*The Myth of the Privacy Paradox*," SSRN e-Library, 24 de febrero 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265.

[4] Narayanan, Arvind, Joanna Huey, and Edward W. Felton, "*A Precautionary Approach to Big Data Privacy*," 19 de marzo de 2015, https://www.cs.princeton.edu/~arvindn/publications/precautionary.pdf.

[5] "'*Anonymized' Data Can Never Be Totally Anonymous, says Study*," *The Guardian*, 24 de julio de 2019, https://cacm.acm.org/news/238352-anonymized-data-can-never-be-totally-anonymous-says-study/fulltext.

i. "Los datos anonimizados nunca pueden ser totalmente anónimos: la anonimización no es suficiente para que las empresas privadas eviten conflictos con leyes como el Reglamento General de Protección de Datos de Europa y la Ley de Privacidad del Consumidor de California".[6]

El alcance de la privacidad para lo que el RGPD llama personas físicas sigue ampliándose porque la capacidad de identificar de manera única a un ser humano con el más mínimo rastro de comportamiento en línea o fuera de línea sigue ampliándose. Cuándo una persona almorzó, la forma en que movió el ratón para encontrar el cursor, lo que le dijo a un representante de servicio por teléfono luego de la advertencia, "esta llamada puede grabarse con fines de calidad", lo que compró en línea, su dispositivo y todos sus atributos relacionados, o incluso dónde compraron el gas puede ser suficiente para identificar de manera única a una persona física. Atrás quedaron los días en que el nombre, la dirección, el número de seguro social y la fecha de nacimiento eran los únicos identificadores. Ahora, necesitamos proteger colecciones masivas de datos personales y relacionados para brindar privacidad a los consumidores.

Terminología y acrónimos

- Consentimiento: permiso para que algo suceda o acuerdo para hacer algo.
- RGPD – Reglamento General de Protección de Datos[7]
- CCPA (por sus siglas en inglés) – Ley de Privacidad del Consumidor de California[8]
- Persona Natural – un ser humano individual
- Ley *NY SHIELD* - Ley de Nueva York "Detener los hackeos y mejorar la seguridad de los datos electrónicos"[9]
- Privacidad: un concepto abstracto sin una definición única y común

Alcance

El noble objetivo de esta sección sobre *Privacidad y cumplimiento para los consumidores* es presentar una perspectiva global. Sin embargo, el lanzamiento inicial de esta sección se centra más en el RGPD, la CCPA y la Ley *NY SHIELD*, cubriendo más superficialmente el caso de China y el resto del mundo. Como se indica a continuación en la sección de recursos, la Asociación Internacional de Profesionales de la Privacidad (IAPP, por sus siglas en inglés) es

---

[6] Ibid

[7] "*Complete guide to GDPR compliance," Horizon 2020 Framework Programme of the European Union*, https://gdpr.eu/.

[8] "*California Consumer Privacy Act (CCPA)*," Oficina del fiscal general, Departamento de Justicia de California, https://oag.ca.gov/privacy/ccpa.

[9] "An act to amend the general business law and the state technology law, in relation to notification of a security breach," Proyecto de Ley del Senado S5575B, Senado del Estado de Nueva York, 7 de mayo de 2019, https://www.nysenate.gov/legislation/bills/2019/s5575.

una excelente fuente de información para una cobertura global inmediata, actual y completa.

Los requisitos para la protección de datos y las regulaciones de privacidad asociadas están aumentando en todo el mundo. El 21 de marzo de 2020 entró en vigor la Ley *NY SHIELD* y China está trabajando en una ley de privacidad actualizada. La mayoría está familiarizada con el RGPD y la CCPA.[10] La siguiente figura destaca la regulación y aplicación global como fuerte, robusta, moderada o limitada.

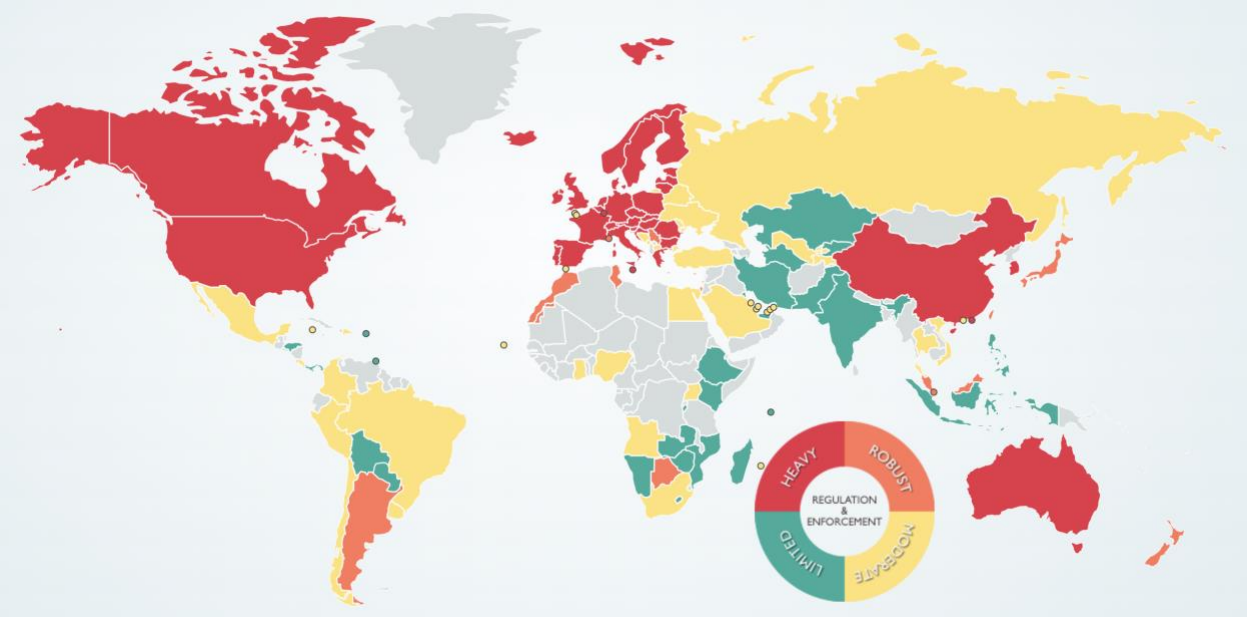


Figura 1: la regulación de privacidad global varía de pesada a limitada[11]

Además de un alcance global, esta sección cubre las identidades digitales, incluidos los servicios y aplicaciones en línea, así como las interacciones físicas (por ejemplo, clientes que ingresan a una tienda o establecimiento de servicios).

En esta sección, consideramos los datos personales obtenidos, almacenados o rastreados a través de una variedad de mecanismos, que incluyen *cookies*, comunicaciones electrónicas (Internet, correo electrónico, mensajería, aplicaciones), conexión inalámbrica, teléfono e Internet de las cosas (IoT, por sus siglas en inglés) . Todos estos datos se pueden utilizar para identificar a un individuo único y se pueden considerar privados, lo que requiere protección como un *derecho humano fundamental.* La primera consideración del

[10] "La Ley de Privacidad del Consumidor de California de 2018", Proyecto de Ley de la Asamblea No. 375, Capítulo 55, Legislatura del Estado de California, 29 de junio de 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[11] Mapa "Leyes de protección de datos del mundo," *DLA Piper Intelligence*, https://www.dlapiperdataprotection.com/

RGPD establece que la protección de datos es un derecho fundamental según la Carta de los Derechos Fundamentales de la Unión Europea y el Tratado de Funcionamiento de la Unión Europea (TEFU).[12,13]Las Naciones Unidas adoptaron la Declaración Universal de Derechos Humanos en 1948, un mandato global para la privacidad, como se articula en el Artículo 17:[14]

> *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor y reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

	RGPD UE	Directiva de privacidad electrónica de la UE	US CCPA, *NY* ***SHIELD***, otro	Ley de seguridad de IoT de California, Oregón; Singapur, otros	Resto del mundo
¿Qué está cubierto?	Datos personales, consentimiento de *cookies*	*Cookies*, Internet, correo electrónico, mensajería, teléfono; mecanismos de seguimiento, derecho de confidencialidad	Datos personales, datos del hogar bajo CCPA	Cualquier dispositivo conectado; tiene una dirección IP o una dirección Bluetooth	China - ninguno; APEC - Datos personales*

Tabla 1. Más allá de GDPR: los datos personales incluyen cookies, teléfono e IoT

*Según el marco de privacidad de la Cooperación Económica Asia-Pacífico (APEC), la información personal es cualquier información sobre una persona identificada o identificable. [15]

El RGPD está estrechamente relacionado con la Directiva de privacidad electrónica. La Directiva de privacidad electrónica pronto será reemplazada por el Reglamento de

---

[12] "Carta de los Derechos Fundamentales de la Unión Europea", Diario Oficial de la Unión Europea, C 392/391, 26 de octubre de 2012,http://data.europa.eu/eli/treaty/char_2012/oj.

[13] **"**Tratado de Funcionamiento de la Unión Europea", Diario Oficial de la Unión Europea, C 326, 26 de octubre de 2012, ttp://data.europa.eu/eli/treaty/tfeu_2012/oj.

[14] Naciones Unidas, "La Declaración Universal de los Derechos Humanos",1948, https://www.un.org/en/universal-declaration-human-rights/.

[15] *"APEC Privacy Framework," International Association of Privacy Professionals (IAPP), n.d.,* https://iapp.org/resources/article/apec-privacy-framework/.

privacidad electrónica. El RGPD y el Reglamento de privacidad electrónica son parte de la reforma de protección de datos en la UE; donde hay superposición, el Reglamento de privacidad electrónica anula el RGPD, especialmente para las *cookies* y la comunicación electrónica.[16]

A continuación, cubrimos la ley de IoT. Tenga en cuenta que las leyes emergentes buscan primero deshacerse de las contraseñas incrustadas o codificadas. Cuando un dispositivo IoT se envía con la contraseña ya instalada por el fabricante, esto facilita la violación de la privacidad y la creación de *software* malicioso de *botnet.*

Preparando el terreno

Académicos y expertos en privacidad, incluidos Hartzog, Zuboff, Schneier y Maler, preparan el terreno para examinar estos y más temas.

Hartzog

Woodrow Hartzog es profesor de Derecho y Ciencias de la Computación en la Universidad Northeastern y, entre otras funciones, es un académico afiliado en la Escuela de Derecho de Stanford para Internet y Sociedad. En abril de 2019, Hartzog fue coautor de *The Pathologies of Digital Consent* con Neil Richards, donde analizan los defectos que pueden sufrir los modelos de consentimiento, entre ellos: [17]

- Consentimiento involuntario
- Consentimiento forzado
- Consentimiento incapacitado

Estos defectos de consentimiento están muy lejos del *patrón oro de conocimiento y consentimiento voluntario*. Hartzog y Richards concluyen:

El uso excesivo del consentimiento en el contexto digital, combinado con una limitada supervisión del punto de vista legal de lo que constituye un consentimiento suficiente, ha permitido que se creen grandes fortunas sobre la base de datos personales, pero también ha expuesto a los consumidores a violaciones de datos, robo de identidad y una economía de vigilancia sin precedentes en la historia de la humanidad, que dilata tanto la noción misma de "consentimiento" que la aleja de lo que realmente alguna vez se consintió.

---

[16] "*The new EU ePrivacy Regulation: what you need to know*," i-SCOOP, n.d., https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/.

[17] "Richards, Neil, and Woodrow Hartzog, "*The Pathologies of Digital Consent*," SSRN e-Library, 11 de noviembre de 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433.

Más fundamentalmente, la fabricación del consentimiento mediante la explotación de las patologías del consentimiento ha disminuido la confianza en nuestro entorno digital, que es el ingrediente clave para un futuro mejor. Podemos hacerlo mejor, pero para hacerlo, debemos reconocer las patologías del consentimiento y limitar el consentimiento a los contextos en los que está más justificado. En el futuro, debemos confiar en estrategias distintas al consentimiento ficticio, fabricado o forzado para minimizar los riesgos y daños de nuestra economía de la información si buscamos aprovechar sus beneficios de una manera sostenible, ética y progresiva.

Estos problemas de consentimiento se analizan más a fondo en secciones posteriores, incluida una solución propuesta o una *teoría de la confianza del consumidor* como alternativa a una dependencia excesiva de modelos de consentimiento cada vez más patológicos.

Zuboff

En su libro reciente y galardonado, *La era del capitalismo de vigilancia: la lucha por un futuro humano y la nueva frontera del poder*, Shoshana Zuboff de Harvard articula claramente su bien documentada afirmación de que vivimos en un estado de *capitalismo de vigilancia*. El mensaje de Zuboff es claro:
"El capitalismo de vigilancia reclama unilateralmente la experiencia humana como materia prima gratuita para traducirla en datos de comportamiento.

- Aunque algunos de estos datos se aplican a la mejora del servicio, el resto se declara un excedente de comportamiento patentado introducido en procesos de fabricación avanzados conocidos como "inteligencia de máquina" para generar productos de predicción que anticipan lo que la persona hará ahora, pronto y más tarde.
- Finalmente, estos productos de predicción se negocian en un nuevo tipo de mercado que llamo mercados de futuros conductuales.
- Los capitalistas de vigilancia se han enriquecido inmensamente con estas operaciones comerciales, ya que muchas empresas están dispuestas a apostar por nuestro comportamiento futuro".[18]

Schneier

El libro de Zuboff de 2019 sobre el capitalismo de vigilancia hace que el libro de Bruce Schneier de 2015, *Datos y Goliat: las batallas ocultas para recopilar sus datos y controlar su mundo*, palidezca en comparación. Los consumidores quedan preguntándose: "¿Por qué no me dijeron que era tan malo?" porque Schneier no proporciona los detalles escalofriantes sobre cuánto han avanzado la vigilancia y la recolección de excedentes de

[18] Naughton, John, "'The goal is to automate us': welcome to the age of surveillance capitalism," The Guardian, 20 January 2020, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

comportamiento. Las palabras de Zuboff incluso se reflejan en los mensajes de marketing de los principales proveedores de "protección de datos", "La privacidad es el derecho de un individuo a estar libre de vigilancia no solicitada".[19]

Maler

En su charla de *Identiverse* de 2018, *No acondicione un camino de vaca para la privacidad: reconfigure el consentimiento para la nueva movilidad*, Eve Maler, jefa de tecnologías de ForgeRock, entonces vicepresidente de innovación y tecnologías emergentes, describe por qué el concepto de "consentimiento" no se puede escalar a los requisitos de correo electrónico, computadoras portátiles, y navegadores, aún menos a los dispositivos móviles y las aplicaciones.

- ¿Cuánto peor se pondrá la situación a medida que los dispositivos conectados se conviertan en una parte cada vez mayor de la vida de los consumidores y en un punto de integración cada vez más importante para todas las industrias?" Maler establece la "Nueva Movilidad como un escenario crítico para examinar los requisitos de confianza de los consumidores, los requisitos reglamentarios para la privacidad, cómo estos deben adaptarse a las experiencias de consentimiento y la gestión del consentimiento, y cómo podemos comenzar a enfrentar estos nuevos desafíos".[20]

Las palabras de Maler fueron proféticas porque, en la prisa por implementar el consentimiento para el cumplimiento del RGPD, muchas empresas simplemente han acondicionado un camino de vaca. Su charla describe cómo reconfigurar el consentimiento para adaptarse a los requisitos arquitectónicos actuales de asincronía, automatización y abstracción.

¿Qué es la privacidad?

La privacidad es un concepto abstracto con muchas definiciones e incluso más amenazas potenciales cuando se ataca ese concepto. Hay áreas como el manejo de inteligencia de fuente abierta (OSINT, por sus siglas en inglés) que pueden tener un enorme impacto en el individuo, pero donde los parámetros legales están mal especificados (si es que se especifican).[21] Las preocupaciones en torno a la politización y el posible uso de los datos

---

[19] Petters, Jeff, "*Data Privacy Guide: Definitions, Explanations and Legislations*," Varonis, 29 de marzo de 2020, https://www.varonis.com/blog/data-privacy/.

[20] Maler, Eve, "*Don't Pave Privacy Cow Paths: Retool Consent for the New Mobility*" (video), Identiverse 2018, 26 de junio de 2018, https://www.youtube.com/watch?v=eP5U2sA6EFk&t=254s.

[21] Hulsen, L. Ten, "*Open Sourcing Evidence from the Internet - The Protection of Privacy in Cvilian Criminal Investigations using OSINT (Open-Source Intelligence)*", Foro de derecho de Ámsterdam, vol 12.2, 2020, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/amslawf12&section=9.

personales como armas también resaltan los desafíos que presenta tener tantas percepciones de la privacidad.[22]

La privacidad como un derecho humano fundamental

La protección de datos personales a menudo se refiere a la autonomía y el control sobre los datos personales. Este nivel de autonomía y control varía según el contexto. En general, la definición de privacidad difiere de un país a otro o de un Estado a otro. Aunque EE. UU. es uno de los 48 países de las Naciones Unidas que votaron para adoptar la Declaración Universal de Derechos Humanos, EE. UU, no comparte la aceptación de la privacidad por parte de la UE como un *derecho humano fundamental*. Por ejemplo, en lugar de una ley federal integral, está creando un mosaico de leyes específicas para cada Estado.

- En la UE, la dignidad humana se reconoce como un derecho fundamental absoluto.
- En esta noción de dignidad, privacidad o el derecho a una vida privada, ser autónomo, tener el control de la información sobre uno mismo, que lo dejen solo, juega un papel fundamental. La privacidad no es sólo un derecho individual sino también un valor social.
- El derecho a la privacidad o a la vida privada está consagrado en la Declaración Universal de los Derechos Humanos (artículo 12), el Convenio Europeo de Derechos Humanos (artículo 8) y la Carta Europea de los Derechos Fundamentales (artículo 7).[23]

Westin. En la década de 1960, el pionero de la privacidad, Alan Westin, definió la privacidad como "el derecho de los individuos, grupos o instituciones a determinar por sí mismos cuándo, cómo y en qué medida se comunica información sobre ellos a otros".[24]

Corte Suprema de EE. UU. En 1989, la Corte Suprema de los EE. UU. escribió: "Tanto el derecho consuetudinario como la comprensión literal de la privacidad abarcan el control del individuo sobre la información relativa a su persona".[25]

China. En la República Popular China (RPC), una serie compleja de leyes rigen los datos personales y la privacidad, que se verán eclipsadas por una regulación integral en el futuro. La tendencia indica que "las personas están obteniendo importantes derechos de protección de datos en los sectores privados, pero no pueden reclamar ninguna solución

---

[22] Ver por ejemplo: Clausen, M.-L., 2021. *Challenges of using biometrics in Yemen, DIIS: Dansk Institut for Internationale Studier*. Obtenido de: https://policycommons.net/artifacts/1526658/challenges-of-using-biometrics-in-yemen/2214896/ el 10 de noviembre de 2022. CID: 20.500.12592/n9640f.

[23] "Protección de datos," Supervisor Europeo de Protección de Datos, n.d., https://edps.europa.eu/data-protection/data-protection_en

[24] Westin, Alan F. "Privacy and freedom." Washington and Lee Law Review 25, no. 1 (1968): 166.

[25] Cate, Fred H., Beth E. Cate, "*The Supreme Court and information privacy*," *International Data Privacy Law*, Volumen 2, Número 4, noviembre de 2012, p 255-267, https://doi.org/10.1093/idpl/ips024.

por las infracciones de su privacidad por parte del gobierno estatal".[26] Hoy en día, se aplican varias leyes, según el sector: servicios financieros, comercio electrónico, telecomunicaciones, servicios de Internet, proveedores de contenido o salud.

APEC. El marco de privacidad de la Cooperación Económica de Asia Pacífico (APEC) se puede descargar aquí. El marco de privacidad de APEC protege la privacidad dentro y fuera de las economías y permite transferencias regionales de información personal que benefician a consumidores, empresas y gobiernos. Este marco se utiliza como base para el Sistema de Reglas de Privacidad Transfronterizas (CBPR, por sus siglas en inglés) de APEC. Los países marco y los participantes incluyen los países en el mapa a continuación.

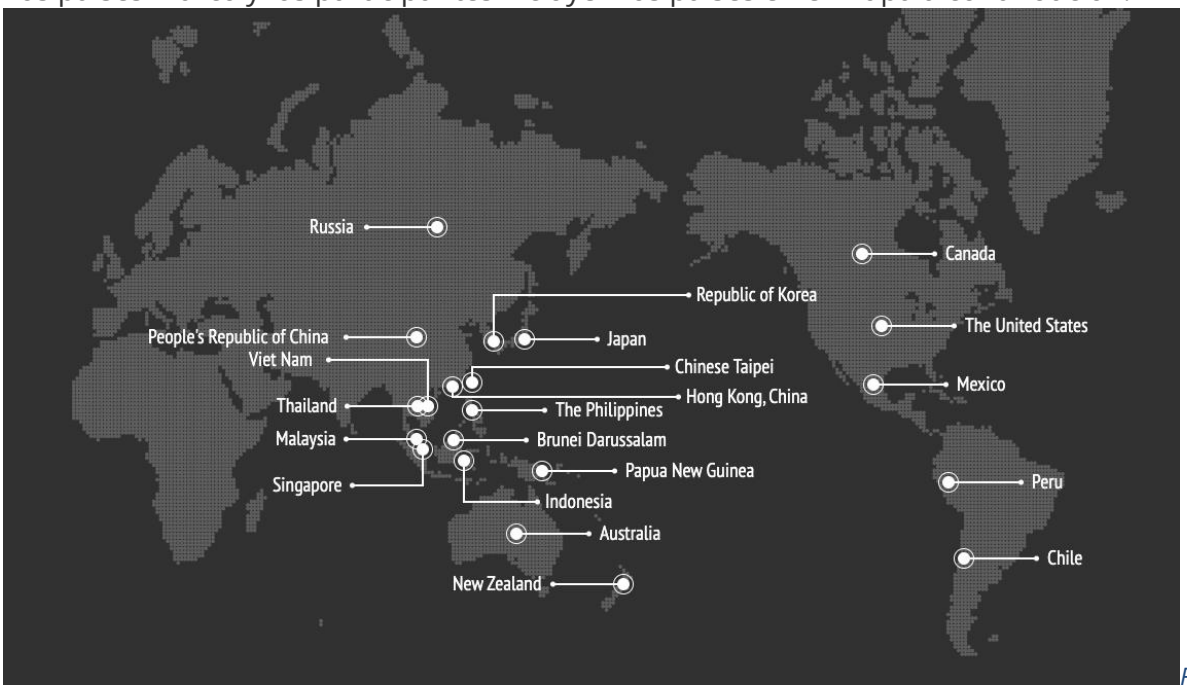


Figura 2 - Mapa de los países y participantes del marco del Sistema de Reglas de Privacidad Transfronterizas (CBPR) de APEC[27]

Modelos de privacidad

Según Samm Sacks, catedrática emérita de la facultad de derecho de Yale, *Paul Tsai China Center*, existen dos modelos básicos de privacidad: 1) China y 2) RGPD. Ella indica que tanto Vietnam como Kenia e India están más alineados con el modelo chino.[28] Aunque las leyes de privacidad de China están influenciadas por el RGPD, son diferentes tanto en los

[26] Pernot-Leplay, Emmanuel, "*Data Privacy Law in China: Comparison with the EU and U.S. Approaches*," (publicación de blog), 27 de marzo de 2020, https://epernot.com/data-privacy-law-china-comparison-europe-usa/.

[27] Mapa de economías miembros, Cooperación Económica Asia-Pacífico, https://www.apec.org/About-Us/About-APEC/Member-Economies.

[28] Sacks, Samm. "*China's Emerging Data Privacy System and GDPR*." *Washington, DC: Center for Strategic and International Studies* (2018).

detalles (por ejemplo, China apoya el consentimiento implícito, mientras que el RGPD requiere el consentimiento explícito) como en el espíritu (en general, los derechos del Estado reemplazan los derechos individuales). La dicotomía de la privacidad en China se evidencia por la mayor protección de los consumidores por parte de empresas de tecnología como Renren y otras contrapartes chinas de Facebook, incluso cuando se intensifica la vigilancia del gobierno.

Más allá de la ley de privacidad, las organizaciones abordan la privacidad de los consumidores de diversas maneras. El papel del profesional de identidad es primero comprender la postura de la organización con respecto a la privacidad, la seguridad y el riesgo.

Taxonomía de privacidad

Uno de los principales expertos mundiales en derecho de la privacidad es Daniel Solove, profesor de derecho e investigador *John Marshall Harlan* en la facultad de derecho de la Universidad George Washington. Como se muestra en la taxonomía de privacidad de Solove a continuación, la privacidad tiene dos partes principales:

- El titular de los datos, o el consumidor
- Los titulares de los datos, o encargado del tratamiento y responsable

  Los cuatro procesos principales en la taxonomía de privacidad comprenden:

- Recopilación de información
- Procesamiento de información
- Diseminación de información
- Invasiones

Los cuatro procesos se pueden ver en orden, comenzando con la recolección de Información y terminando con las invasiones. La recopilación de información de datos sobre un sujeto de datos la realiza el titular de los datos, o el procesador y controlador de datos para ponerlo en términos de RGPD. La recopilación de datos sobre un sujeto de datos o una persona puede ser realizada por otra persona, empresa, gobierno u organización externa mediante vigilancia o interrogatorio. El procesamiento de información incluye el almacenamiento de datos y cualquier paso adicional tomado para aplicar algo como un algoritmo de software para obtener más valor. La inseguridad se refiere a la falta de seguridad. La difusión de información incluye las cosas dañinas que pueden resultar en el caso de que la información sea parte de una lista de acciones indeseables, incluida una violación de la confidencialidad, divulgación, exposición, chantaje o distorsión. Las invasiones incluyen la intrusión y la interferencia en las decisiones, que

Solove describe como "la incursión del gobierno en las decisiones del sujeto de datos con respecto a sus asuntos privados".[29]

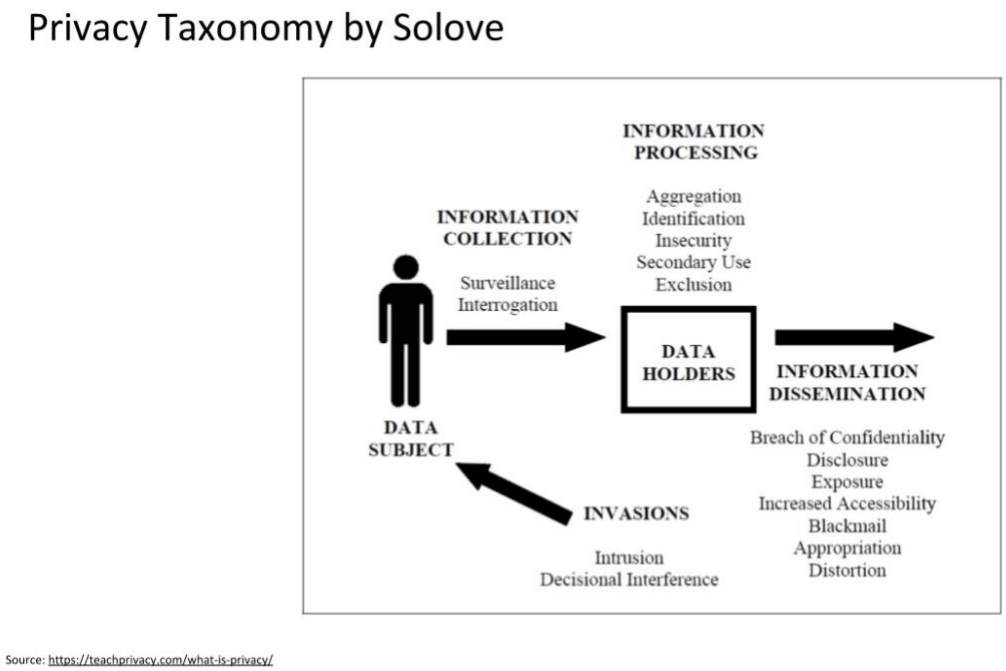


Figura 3 - Taxonomía de privacidad de Solove

[Permiso recibido del autor para usar este gráfico]

Privacidad por diseño

Privacidad por diseño es una creación de Ann Cavoukian, una de las principales expertas en privacidad del mundo; ex comisionada de información y privacidad de Ontario, Canadá; exprofesora visitante distinguida en la Universidad de Ryerson, donde también fue directora ejecutiva del Instituto de Privacidad y Big Data de Ryerson; y fundadora de Global Privacy and Security por Design Centre. Publicado originalmente en 2009, los Principios de Privacidad por Diseño, representados en la figura a continuación, son una parte integral del RGPD y las leyes de privacidad posteriores influenciadas por el RGPD. Privacidad por diseño adopta un enfoque holístico de ingeniería de sistemas y deja en claro que el cumplimiento de las normas no es suficiente. Además, promueve la opinión de que el futuro de la privacidad no puede garantizarse únicamente mediante el cumplimiento de

[29] Solove, Daniel J, "*A Taxonomy of Privacy*," *University of Pennsylvania Law Review*, Vol. 154, No. 3, enero de 2006, https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf.

los marcos normativos; más bien, la garantía de privacidad idealmente debe convertirse en el modo de operación predeterminado de una organización[30]

En la siguiente figura de Privacidad por diseño, tenga en cuenta que la *privacidad por defecto* es uno de los siete principios. El marcado contraste de las expectativas culturales puede sorprender a algunos. Si generalizamos, la sensibilidad de la UE es tener la privacidad por defecto como la norma, mientras que en los EE. UU., la privacidad por defecto es una rara excepción.

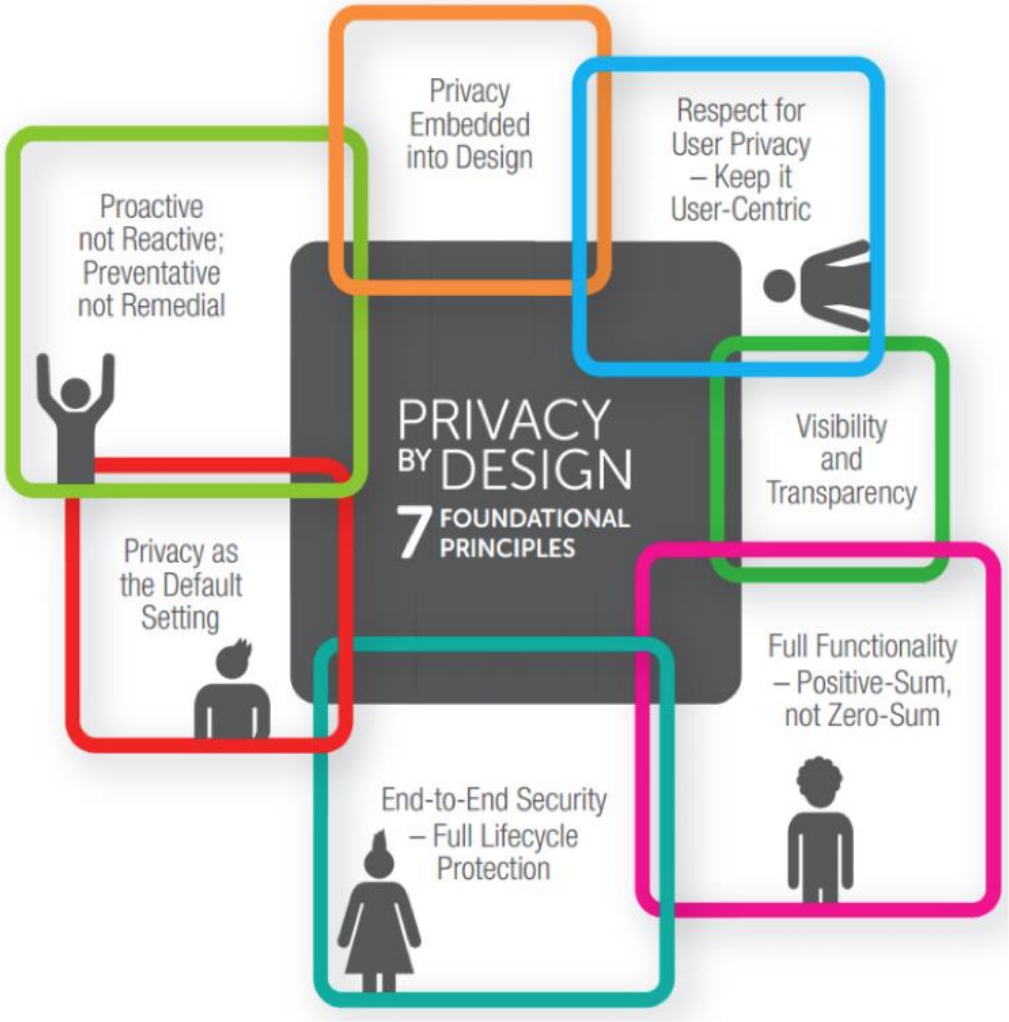


Figura 4 - Privacidad por diseño, siete principios fundamentales[31]

Cavoukian construye sobre su trabajo inicial de privacidad por diseño en un documento posterior, [7 leyes de identidad, el caso de las leyes de identidad integradas en la privacidad]

[30] Cavoukian, Ann, "Privacidad por diseño: los 7 principios fundamentales," www.privacybydesign.ca, n.d., https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
[31] Figura "Privacidad por diseño,", Aristi Ninja, n.d., https://aristininja.com/privacy-by-design/.

en la era digital, donde relaciona la información justa de privacidad con los principios de privacidad por diseño, lo que da como resultado "leyes de identidad integradas en la privacidad".[32] La autora advierte:

> *Un sistema de identidad universal tendrá un profundo impacto en la privacidad, ya que las identidades digitales de las personas, y los dispositivos asociados con ellas, constituyen información personal. Se debe tener mucho cuidado de que un sistema de identidad interoperable no se convierta en una infraestructura de vigilancia universal.*

El cumplimiento es necesario, pero no suficiente

Hasta cierto punto, la ley de privacidad hace cumplir la protección de datos. Esta sección aplaude los avances de la ley de privacidad, además explora algunas de las fallas y deficiencias de la ley de privacidad, incluidos los problemas de consentimiento, el retraso y la postura reactiva debido a que la ley no puede seguir el ritmo de las innovaciones actuales, y lo que Shoshana Zuboff de Harvard llama: el dominio asimétrico del poder de Google, Facebook y otros que son inmunes al impacto efectivo de la ley de privacidad porque la ley no cubre mucho de lo que hacen con la recolección de excedentes de comportamiento.

- **Cumplimiento ≠ privacidad o seguridad.** Como profesional de la identidad, recuerde que el hecho de que cumpla con las normas no significa que se haya alcanzado el nivel adecuado de privacidad y seguridad requerido por su organización (o esperado por sus clientes), con suerte documentado en sus políticas de riesgo y privacidad.
- **El "crecimiento de la brecha" de la Ley de Privacidad es exponencial.** El miembro distinguido de *Harvard Law*, Vivek Wadha, explica: "Las brechas en las leyes de privacidad han crecido exponencialmente. Estas brechas regulatorias existen porque las leyes no se han mantenido al día con los avances tecnológicos. Las brechas son cada vez más amplias a medida que la tecnología avanza y esto sucede cada vez más rápido".[33]

Las capacidades de privacidad y cumplimiento son fundamentales para cualquier programa de administración de acceso e identidad del consumidor (CIAM, por sus siglas en inglés) porque protegen los datos personales de los consumidores y protegen a las

---

[32] Cavoukian, Ann, "7 leyes de identidad: el caso de las leyes de identidad integradas en la privacidad en la era digital," Comisión de Información y Privacidad de Ontario, n.d., https://collections.ola.org/mon/15000/267376.pdf.

[33] Wadhwa, Vivek, "Las leyes y la ética no pueden seguir el ritmo de la tecnología," *MIT Technology Review*, 15 de abril de 2014, https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

organizaciones al definir pautas para el cumplimiento en consonancia con las políticas de administración de riesgos, seguridad y privacidad de la organización. Si las organizaciones no cumplen, hay muchas consecuencias negativas, que incluyen:

- Multas (para RGPD, hasta € 20 millones o 4% de la facturación anual, el monto más alto)
- Daño reputacional o de marca
- Pérdida de clientes, erosión de la lealtad.
- Demandas
- El CEO puede ser considerado personalmente responsable

Como profesional de la identidad, puede formar parte de un equipo responsable de algunos o todos los aspectos de la privacidad y el cumplimiento de los consumidores. Esta sección le permitirá contribuir y tener una comprensión básica de la jurisdicción, el consentimiento y la protección de datos en toda la organización. Para el cumplimiento de RGPD o CCPA, puede interactuar con recursos humanos, ingeniería de productos, seguridad, marketing, TI, legal, atención al cliente, adquisiciones y más, como se muestra en la figura a continuación.

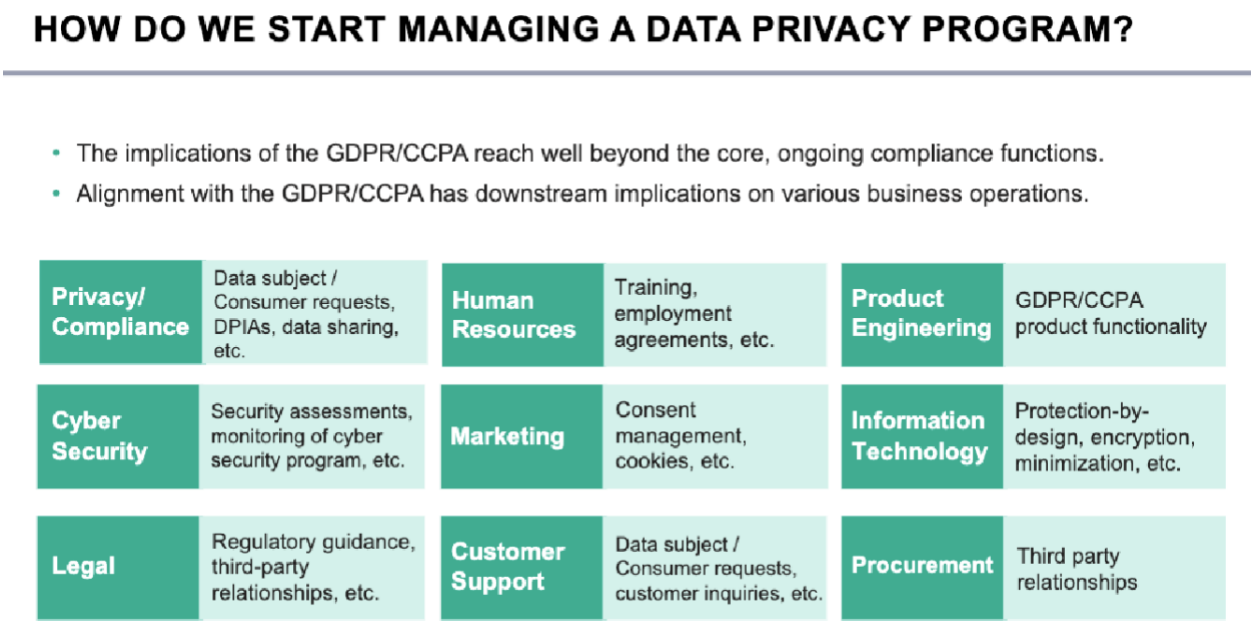


Figura 5: Cómo comenzar a administrar un programa de privacidad de datos, ejemplo[34]

[34] Seminario en línea ISACA, *Robotic Process Automation (RPA) and Audit*, 19 de marzo de 2020, https://www.isaca.org/education/online-events/lms_w031920

Por qué los servicios al consumidor necesitan diferentes estrategias de privacidad y cumplimiento

CIAM y fuerza laboral IAM

Las estrategias de privacidad y cumplimiento para IAM de la fuerza laboral se superponen con CIAM, pero CIAM difiere en algunos aspectos clave. Por esta razón, simplemente aplicar la privacidad y el cumplimiento de la fuerza laboral a los proyectos de CIAM puede no ser óptimo. A continuación, se presentan algunas de las diferencias clave entre las estrategias de privacidad y cumplimiento para la fuerza laboral y los proyectos CIAM:

- ESCALA: La escala de CIAM es a menudo órdenes de magnitud mayor para reflejar una gran población de consumidores versus una cantidad más pequeña y predecible de empleados y mano de obra.
- EXPERIENCIA DEL CLIENTE (CX): Los requisitos de CX para los consumidores son más exigentes. Para sus miembros, IAPP proporciona un documento centrado en RGPD, La guía UX para obtener consentimiento:
    - *"El consentimiento está en el corazón mismo de la protección de datos y la privacidad", y si bien es importante, no es el principio y el fin de un programa de privacidad; por ejemplo, una estrategia de notificación de privacidad inteligente o en capas puede ayudar a que las interacciones de privacidad sean menos engorrosas.*
    - *El sujeto de datos debe tener voz en los asuntos de cómo se recopilan, usan, comparten y destruyen sus datos personales.*
    - *Incluso si una opción no parece promocionarse, la redacción, el widget y la secuencia son importantes*.[35]

- LEY: Dependiendo de la jurisdicción, la ley de privacidad puede diferir en algunos casos para IAM versus CIAM.
- AUTOMATIZACIÓN: Los niveles apropiados de automatización difieren para satisfacer los picos de demandas o las demandas impredecibles de los consumidores.
- PUBLICIDAD: la publicidad conductual en línea en particular, y cualquier publicidad en general, generalmente está dirigida a los consumidores, no a la fuerza laboral.
- APRENDIZAJE AUTOMÁTICO Y PERFIL: Lo que RGPD define como "procesamiento automatizado", incluida la elaboración de perfiles (procesamiento automatizado de datos personales para evaluar ciertas cosas sobre un individuo); además, el aprendizaje automático a menudo se aplica a los datos del consumidor para diferentes propósitos para la fuerza laboral versus los consumidores.

---

[35] "*The UX Guide for Getting Consent*," IAPP, n.d., https://iapp.org/store/books/a191a000002FUZKAA4/.

CIAM e identidad social

CIAM a menudo se basa en la integración con los proveedores de identidad de las redes sociales. Hay varios beneficios en esta dirección, incluida la reducción de la fricción del usuario final durante el registro y el registro de autoservicio, la generación de menos nombres de usuario y contraseñas que el usuario final deba memorizar y procesos comerciales simplificados que permiten externalizar los procesos de recuperación de cuentas de usuario. Sin embargo, esta integración no está exenta de inconvenientes, ya que la integración con proveedores de identidad de redes sociales puede permitir el seguimiento de usuarios entre sitios sin su permiso.

La seguridad es crítica

Los profesionales de la identidad deben comprender las políticas de gestión de riesgos de seguridad y privacidad de su organización y trabajar en conjunto con los colegas que crean esas políticas, así como con los responsables de la implementación de estas. La política de seguridad es una dependencia necesaria para cualquier política de privacidad exitosa. Hay un dicho: "Puedes tener seguridad sin privacidad, pero no puedes tener privacidad sin seguridad".[36] Seguridad o ciberseguridad pueden usarse indistintamente. Algunos también usan el término seguridad de la información. En la siguiente figura del marco de privacidad del NIST, la relación entre los riesgos de seguridad cibernética y los riesgos de privacidad deja en claro que la gestión del riesgo de seguridad cibernética puede ayudar a mitigar el riesgo de privacidad, pero no es suficiente porque el riesgo de privacidad puede resultar en incidentes fuera del ámbito de los incidentes de seguridad cibernética. Por ejemplo, los medidores o los termostatos inteligentes pueden recopilar y registrar datos personales y posiblemente representar un riesgo para la privacidad, aunque funcionen según lo previsto.

---

[36] Schwartz, Karen D., "*Data Privacy and Data Security: What's the Difference?*" *ITPro Today*, 2 de mayo de 2019, https://www.itprotoday.com/security/data-privacy-and-data-security-what-s-difference.

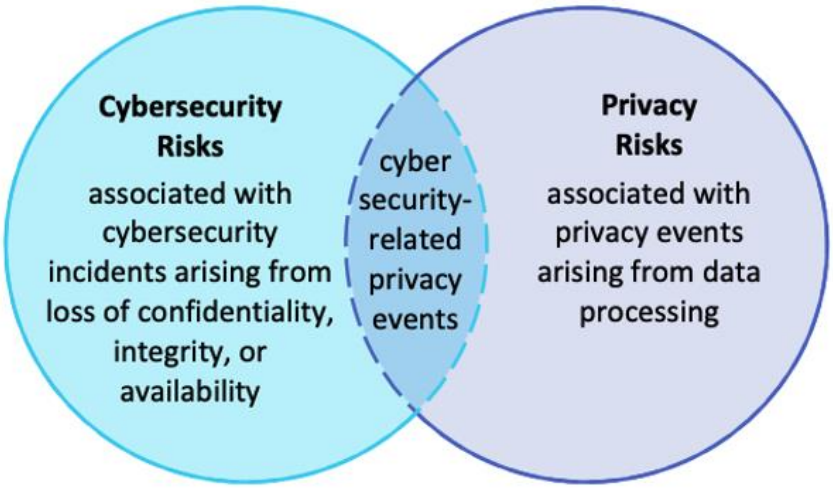


Figura 6 - Relación entre riesgos de ciberseguridad y riesgos de privacidad[37]

La política de privacidad es una decisión comercial

Una comprensión profunda de las políticas de una organización proporcionará claridad para el papel del profesional de identidad en la privacidad y el cumplimiento de los consumidores. Por ejemplo, en algunos casos, el departamento de marketing puede necesitar recopilar una gran cantidad de datos personales y la política de privacidad de la organización puede permitirlo. En otros casos, el negocio de la organización puede depender de la confianza y confidencialidad de los datos personales; y puede haber un presupuesto amplio para garantizar la protección de datos de los consumidores de manera visible, transparente y sólida.

Figura 7 - Relación entre riesgo de privacidad y riesgo organizacional[38]

---

[37] "*NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Versión 1.0," Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU., 16 de enero de 2020, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[38] Ibid

La forma en que una organización trata la privacidad del consumidor y cualquier riesgo asociado es una decisión comercial; la opción de mitigar, transferir, evitar o aceptar el riesgo puede realizarse junto con la formulación de la política de privacidad o en un momento posterior.

- Mitigar. Mitigar el riesgo (p. ej., las organizaciones pueden aplicar medidas técnicas y/o políticas a los sistemas, productos o servicios que minimicen el riesgo en un grado aceptable);
- Transferir. Transferir o compartir el riesgo (p. ej., los contratos son un medio para compartir o transferir el riesgo a otras organizaciones, los avisos de privacidad y los mecanismos de consentimiento son un medio para compartir el riesgo con las personas);
- Evitar. Evitar el riesgo (por ejemplo, las organizaciones pueden determinar que los riesgos superan los beneficios y renunciar o terminar el procesamiento de datos); o
- Aceptar. Aceptar el riesgo (por ejemplo, las organizaciones pueden determinar que los problemas para los consumidores son mínimos o poco probables; por lo tanto, los beneficios superan los riesgos y no es necesario invertir recursos en la mitigación).[39]

¿Es la privacidad una ventaja competitiva?

Como se señaló anteriormente, las leyes y reglamentaciones normalmente van a la zaga de las ofertas de productos y servicios innovadores. El cumplimiento de las leyes de privacidad actuales y futuras es solo el comienzo. La privacidad puede ser una ventaja competitiva o no. Depende de la organización y de sus consumidores. En 2010, el pionero y experto en protección de datos Alan Westin fue parafraseado: "La idea de que la privacidad se puede usar como una ventaja comercial es una idea muerta, los controles de privacidad son demasiado complejos para que los consumidores los entiendan y una cultura de certificación sería mucho más efectiva".[40] Otros toman partido por el contraargumento. Las organizaciones se dan cuenta de que muchos consumidores disfrutarían si tuvieran un mayor control sobre sus datos. La privacidad para los consumidores es una oportunidad para generar confianza. Entre otros, un documento de Akamai sobre el RGPD y la CCPA

---

[39] "*NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management*," Borrador preliminar, Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU., 6 de septiembre de 2019, https://www.nist.gov/system/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf.

[40] "*The Privacy Advisor*," IAPP, Vol. 10, No. 10, diciembre 2010, https://iapp.org/media/pdf/publications/Advisor_12-10_print.pdf.

proporciona "consejos para generar confianza en el cliente a través del cumplimiento normativo y la gobernanza de la identidad".[41]

Más allá de RGPD: ePrivacy y la nueva estrategia europea para datos

En febrero de 2020, la UE publicó "Una estrategia europea para los datos". El avance continuo y el liderazgo comprobado de la UE en protección de datos es una fuerza impulsora para el resto del mundo.

La estrategia europea para los datos es específica del sector, por ejemplo, existe una para la atención médica, y prevé que:

- Los datos pueden fluir dentro de la UE y entre sectores.
- Las normas y valores europeos, en particular la protección de datos personales, la legislación de protección del consumidor y la ley de competencia, se respetan plenamente.
- Las reglas para el acceso y uso de los datos son justas, prácticas y claras, y existen mecanismos claros y confiables de gobernanza de datos; existe un enfoque abierto pero asertivo de los flujos de datos internacionales basado en valores europeos.[42]

A través de su enfoque en la soberanía de los datos y el apoyo a la privacidad de las personas en su circunscripción, la Unión Europea proporciona una guía modelo sobre tecnologías más nuevas, como la Identidad Descentralizada (DID) y las Credenciales Verificables. Recogido en gran parte en el Reglamento sobre identificación electrónica y servicios de confianza (Reglamento eIDAS), este reglamento:

- garantiza que las personas y las empresas puedan utilizar sus propios sistemas nacionales de identificación electrónica (eID) para acceder a los servicios públicos disponibles en línea en otros países de la UE;
- crea un mercado interior europeo para los servicios de confianza al garantizar que funcionarán a través de las fronteras y tendrán el mismo estatus legal que sus equivalentes tradicionales en papel.[43]

---

[41] "*White Paper: GDPR, CCPA, and Beyond: How to Comply with Data Privacy Laws and Improve Customer Trust*," Akamai, n.d., https://www.akamai.com/us/en/campaign/assets/whitepapers/gdpr-ccpa-and-beyond-wp.jsp.

[42] "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones", Comisión Europea, COM(2020) 66 final, 19 de febrero de 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN.

[43] Sitio web Regulación eIDAS de la Comisión Europea, última actualización 7 de junio 2022, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

El Reglamento eIDAS está bajo consideración para una enmienda que evolucionará aún más la guía disponible para incluir más información sobre billeteras digitales y su uso.[44]

Cadena de bloques. La Estrategia Europea para los Datos incluye la evaluación de la tecnología de cadena de bloques (o *blockchain* en inglés).

- Las nuevas tecnologías digitales descentralizadas, como la cadena de bloques, ofrecen una posibilidad adicional para que las personas y las empresas gestionen los flujos y el uso de datos, sobre la base de la libre elección y la autodeterminación individual. Dichas tecnologías harán posible la portabilidad dinámica de datos en tiempo real para individuos y empresas, junto con varios modelos de compensación.[45]

Además, la autoridad francesa de protección de datos, conocida como la Comisión Nacional de Informática y Libertad (CNIL), ha encabezado el trabajo sobre el "uso responsable de la cadena de bloques en el contexto de los datos personales", sumado a los posibles riesgos de privacidad inherentes a la tecnología.

Los desafíos que plantean la cadena de bloques en términos de respeto de los derechos humanos y las libertades fundamentales requieren necesariamente una respuesta a nivel europeo. La CNIL es una de las primeras autoridades que está abordando oficialmente el asunto y **trabajará en cooperación con sus homólogos europeos para sugerir un enfoque sólido y armonizado.*[46]***

Conclusión

Aunque puede ser difícil definir lo que significa privacidad, los principios fundamentales de privacidad por diseño (representados en la Figura 5 anterior) crean una base bien definida para comprender e implementar la privacidad y el cumplimiento para los consumidores. Esta es la razón por la que la privacidad por diseño está incluida en el RGPD y la CCPA, y ha influido significativamente en las leyes y regulaciones de privacidad posteriores. A estas alturas, los profesionales de la identidad deben tener una imagen clara de las dependencias interrelacionadas entre identidad, privacidad y seguridad. La seguridad protege los datos; la forma en que se proporciona la privacidad se basa en las políticas

---

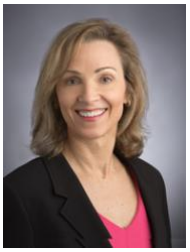
[44] Comisión Europea, "La Comisión propone una identidad digital confiable y segura para todos los europeos", comunicado de prensa, 3 de junio de 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663.

[45] Comisión Europea, COM(2020) 66 final, 19 de febrero de 2020.

[46] "*Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*," CNIL, 6 de noviembre de 2018, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

comerciales y de riesgo. El lado positivo de la abrumadora tarea de implementar la privacidad y el cumplimiento de esta para los consumidores es que puede verse como una ventaja competitiva y por tanto vale la pena el esfuerzo adicional.

Biografía de la autora



Clare Nelson, CISSP, CIPP/E, practicante certificada en la nube de AWS; es la CEO de *ClearMark Consulting*, especializada en desarrollo de negocios y estrategia de productos. Antes de eso, fue vicepresidenta de alianzas tecnológicas y ventas de canales para *Identity Governance* y líder de administración de acceso privilegiado en la nube, Saviynt, responsable de las asociaciones de AWS y Google Cloud. La pasión de Clare por la ciberseguridad se ve reflejada en sus especializaciones en identidad y privacidad que comprenden: MFA, IGA, PAM, así como pruebas de identidad, autenticación para preservar la privacidad basada en ZKP, robo de identidad, AML/KYC y GDPR. Clare ha ocupado posiciones de liderazgo en Novell, EMC2, Dell y AllClear ID. Es cofundadora de C1ph3r_Qu33ns, una organización dedicada a cultivar y apoyar las carreras de mujeres en ciberseguridad. Clare es una yogui y tecnóloga de segunda generación y tiene además una licenciatura en matemáticas de la Universidad de Tufts.

Historial de cambios

Fecha	Cambio
2020-06-17	V1 publicada
2021-09-30	V2 publicada: Fecha actualizada de la ley NY SHIELD; sección añadida sobre CIAM e identidad social; título de sección agregado para CIAM y fuerza laboral IAM; se añadió a Heather Flanagan como editora
2022-12-18	V3 publicada: resumen actualizado; se agregaron notas sobre: amenazas a la privacidad en "¿Qué es la privacidad?"; información añadida sobre eIDAS en “Más allá del RGPD”