WHITE PAPER

Más allá del RGPD y la CCPA:

El control de las identidades ayuda a las empresas a cumplir la ley y aumentar la confianza de sus clientes

Akamai

Resumen ejecutivo

Las normativas de privacidad que afectan a las empresas son una tendencia global en constante expansión. El famoso Reglamento General de Protección de Datos (RGPD) de la Unión Europea entró en vigor en 2018. Asimismo, el 1 de enero de 2020, entra en vigor la Ley de Privacidad del Consumidor de California (CCPA, por sus siglas en inglés), que afectará a todas las empresas que operan en California, la quinta economía más grande del mundo.

Pero esto es solo el principio. La promulgación de nuevas normativas en materia de privacidad y cumplimiento que está teniendo lugar a un ritmo apresurado en todo el mundo está motivada por la gran cantidad de filtraciones de datos, robos de identidad y otros escándalos relacionados que han recibido una gran atención mediática. Solo en Estados Unidos, nueve estados han presentado o aprobado proyectos de ley que obligan a las empresas y organizaciones a proporcionar a los consumidores una mayor transparencia y control sobre la información de identificación personal (PII).

Las empresas no pueden permitirse ignorar estas nuevas leyes y normativas sobre privacidad. Desde el punto de vista financiero, las multas moderadas que se impusieron durante los 12 primeros meses de la aplicación del RGPD han dado paso a multas exorbitantes que superan los 200 millones de dólares, lo que aún queda lejos del límite legal del 4 % del volumen de negocio anual global. Sin embargo, el coste para las empresas multinacionales va más allá del aspecto puramente económico. La confianza del consumidor está en juego.

Si los clientes no confían en que una empresa u organización protejan su valiosa privacidad, el alcance de sus ventas y de sus iniciativas de marketing se verá afectado. Hoy en día, las empresas necesitan el consentimiento expreso de los clientes para procesar sus datos personales, y el consentimiento requiere confianza. Sin confianza, no hay consentimiento, y sin consentimiento, no hay datos. Y eso se traduce en campañas de ventas o de marketing totalmente ineficaces.

Respetar la privacidad no es solo una cuestión de cumplimiento, sino también una ventaja empresarial clave. El control de la privacidad y las identidades ayuda a las empresas y organizaciones a establecer relaciones de confianza con los usuarios y clientes, lo que se traduce en una mayor fidelidad y en la posibilidad de que la empresa obtenga unos ingresos más elevados.

Este documento contiene una descripción general del RGPD, la ley CCPA y otras normativas globales sobre privacidad relacionadas. Además, ofrece argumentos para fomentar la confianza de los clientes a través del cumplimiento de normativas, el control de identidades y la protección de datos, y analiza la necesidad de contar con soluciones de gestión de identidades adecuadas. También se presentan ejemplos que muestran cómo dos marcas líderes han alcanzado sus objetivos de cumplimiento en materia de privacidad.

Reglamento General de Protección de Datos

El 25 de mayo de 2018, el RGPD se convirtió en una realidad a nivel mundial. El objetivo de esta ley es armonizar la legislación local de protección de datos en toda Europa. La ley se aplica no solo a las empresas europeas, sino también a cualquier empresa u organización que opere dentro de la Unión Europea.

El RGPD establece numerosos requisitos sobre cómo recopilar, almacenar y utilizar la información de identificación personal, y cómo proteger los datos contra un acceso no autorizado[1]. Esto implica no solo aprender a identificar y proteger los datos personales, sino también saber cómo cumplir los nuevos requisitos de transparencia, cómo detectar e informar sobre las filtraciones de datos personales y cómo formar al personal encargado de la privacidad.

El incumplimiento de los principios del RGPD puede afectar notablemente al estado financiero de una organización, debido a las sanciones que se contemplan en dicho reglamento. Aunque las infracciones iniciales de la privacidad han dado lugar a multas modestas, el sector ahora está alerta, ya que las multas impuestas recientemente están apareciendo en titulares de todo el mundo. Dos multas importantes, una de ellas a una importante aerolínea[2] (230 millones de dólares) por una filtración de datos que afectó a 500 000 personas y la otra a una empresa hotelera internacional[3] (123 millones de dólares) por el pirateo de información personal de 383 millones de huéspedes, han recibido especial atención por parte de las empresas internacionales.

Ley de Privacidad del Consumidor de California

Con un aumento de la presión sobre las empresas para proteger la privacidad, ha comenzado la cuenta atrás para la entrada en vigor de la Ley de Privacidad del Consumidor de California (CCPA)[4]. El 1 de enero de 2020, la mayoría de las empresas u organizaciones de gran tamaño que operan en California deberán cumplir la nueva y estricta legislación de privacidad del estado, que establece un derecho legal y aplicable de privacidad para todos los residentes de California. Al igual que con el RGPD, estas nuevas normativas no son solo para empresas con sede en California; se aplican a todas las empresas que prestan sus servicios o llevan a cabo su actividad comercial en el estado.

La CCPA otorga las siguientes protecciones a todos los consumidores del estado de California en relación con sus datos personales:[5]

- **Propiedad.** Protege los derechos de los consumidores para que una empresa no comparta ni venda información personal.
- **Control.** Proporciona al consumidor el control sobre la información personal que se recopila sobre él.
- **Seguridad.** Hace responsables a las empresas de proteger la información personal.
- Cualquier empresa u organización tendrá que ajustarse a lo estipulado en la CCPA si cumple al menos uno de los siguientes criterios:
  - Tiene ingresos superiores a 25 millones de dólares.
  - Compra, recibe, vende o comparte la información personal de 50 000 o más consumidores, hogares o dispositivos con fines comerciales.
  - Recibe el 50 % de los ingresos anuales de la venta de la información personal de los consumidores.

Si bien muchas empresas se enfrentaron a importantes obstáculos el año pasado para cumplir con el RGPD, ahora también deben cumplir con la CCPA. Con la fecha de entrada en vigor a la vuelta de la esquina, se agota el tiempo. Las empresas que recopilan datos de identidad de cliente en California y crean perfiles de clientes para campañas de marketing personalizadas deben actuar ahora o arriesgarse a posibles multas de gran envergadura.

¿En qué se parecen el RGPD y la CCPA?

Aunque la CCPA presenta un ámbito algo diferente al del RGPD, otorga a los consumidores derechos similares en lo relativo al control y revisión del uso de sus datos. Ambas normativas exigen que las empresas almacenen los datos de forma segura, sean transparentes sobre los tipos de datos personales recopilados y gestionen las solicitudes de los consumidores para la eliminación de datos personales (lo que se conoce como "derecho al olvido"), lo que significa que pueden borrar los datos personales de todos los sistemas de la organización.

Cuando la base legal para el procesamiento de datos es el consentimiento, la CCPA exige ofrecer a los usuarios la posibilidad de optar por quedar excluidos de la recopilación o darse de baja, mientras que el RGPD exige el consentimiento explícito antes de la recopilación de información personal.

Otras normativas internacionales

Pese a su importancia, el RGPD y la CCPA son solo el principio de esta tendencia global. En todo el mundo, se están presentado o aprobando numerosas leyes de privacidad y cumplimiento. Solo en Estados Unidos, los legisladores de otros nueve estados han presentado algunos proyectos de ley que impondrían importantes obligaciones a las empresas con el fin de proporcionar a los consumidores una mayor transparencia y control sobre la PII[6].

A nivel internacional, la tendencia a una regulación de la privacidad más estricta (y con repercusiones para las empresas) es un fenómeno global que las empresas y organizaciones no pueden ignorar. En la tabla que figura a continuación se detallan algunas de las nuevas normativas, así como otras que están pendientes de aprobación, como la Ley de Protección de Datos Personales y Documentos Electrónicos (PIPEDA, por sus siglas en inglés) canadiense.

Tabla. Ejemplos de normativas de protección de datos y privacidad actuales, futuras o propuestas

AMÉRICA	EMEA	ASIA-PACÍFICO
Argentina: PDPL/Proyecto de ley n.º MEN-2018-147-APN-PTE[7] EE. UU.: California: CCPA (AB 375) Canadá: PIPEDA[8] Hawái: SB 418[9] Maryland: SB 0613[10] Massachusetts: SD 341[11] Misisipi: HB 2153[12] Nuevo México: SB 176[13] Nueva York: S00224[14] Dakota del Norte: HB 1485[15] Rhode Island: S0234[16] Texas: HB 4518[17]	Unión Europea: RGPD Rusia: Ley federal n.º 152-FZ[18]	Australia: Privacy Act 1988/ Information Privacy Principles (IPPs)[19] China: Normativa de protección de datos personales[20] India: Proyecto de ley de protección de datos personales[21] Japón: APPI[22]

Más allá del cumplimiento de normativas: la generación de confianza

En vista de todas estas normativas, ganar la confianza de los consumidores se ha vuelto una prioridad aún mayor para las empresas y organizaciones de todo el mundo. El RGPD y la CCPA, así como otras normativas, exigen que las empresas, cuando corresponda, soliciten a los clientes su consentimiento antes de recopilar y utilizar sus datos, y, por supuesto, mantener un registro del consentimiento.

Además del cumplimiento de las normativas, la privacidad es crucial para las empresas que desean forjar una relación sólida y de confianza con sus clientes dentro del ámbito digital. Los clientes tienen expectativas cada vez más altas y esperan que sus datos personales mantengan su confidencialidad y estén protegidos. Los numerosos casos conocidos de abuso de datos, vulneraciones y robos de identidad han elevado el listón para que las empresas puedan demostrar que son depositarios de confianza de los datos personales. Cuando los clientes entregan sus datos a una organización, suscriben un contrato de confianza; si esa confianza se rompe, será difícil recuperarla

Las personas solo darán su consentimiento para que una marca procese sus datos si la empresa ofrece un valor a cambio, pero también si confían en la marca. Si no hay confianza, no hay consentimiento, y si no hay consentimiento, no hay datos, lo que significa que no se podrán aplicar (o al menos de forma eficiente) las estrategias de marketing y ventas. La confianza se ha bautizado como la "nueva moneda" de las empresas que desean obtener datos de sus clientes.

La importancia del consentimiento: replantearse la experiencia de usuario

Con arreglo al RGPD y la CCPA, los clientes deben poder consultar, modificar e incluso revocar su consentimiento en cualquier momento. En otras palabras, no cumplirán los requisitos las empresas que crean formularios web sencillos para obtener el consentimiento y que luego dificultan deliberadamente su revocación al solicitar que se siga un proceso burocrático complicado. Además, las empresas deben informar claramente a las personas del motivo y los fines por los que están recopilando los datos.

Para las organizaciones de marketing, esto acarrea bastantes implicaciones. Por ejemplo, en virtud del RGPD, las organizaciones ya no pueden utilizar casillas previamente marcadas para obtener el consentimiento en las páginas de inicio con contenido bloqueado para la generación de clientes potenciales. El consentimiento debe ser explícito. Es decir, los consumidores deben marcar la casilla para aceptar. Sin embargo, en virtud de la CCPA, el consentimiento implícito sigue estando permitido, por lo que una casilla previamente marcada cumple la normativa. Esta diferencia puede causar quebraderos de cabeza a las empresas multinacionales que se enfrentan a la perspectiva de dirigirse a dos mercados importantes con sitios web y aplicaciones que deben mostrar diferentes formularios de registro. O incluso a crear sitios web y aplicaciones completamente independientes para atender diferentes regiones, lo que multiplica el esfuerzo en el desarrollo y mantenimiento del código.

Las nuevas normativas también prohíben la recopilación excesiva de datos. Las empresas solo pueden recopilar los datos personales que necesitan para ofrecer sus servicios o productos. Ya no se permite solicitar un número de teléfono o preguntar el sexo solo para enviar un boletín por correo electrónico o permitir la descarga de un white paper. Esto significa que las empresas deben replantearse y rediseñar sus experiencias de usuario y eliminar todos los campos de datos de las páginas de registro y otros formularios que podrían considerarse una recopilación de datos excesiva.

Un retailer internacional implementa una solución centralizada para simplificar el cumplimiento de las leyes de privacidad actuales y futuras

Un retailer internacional solucionó recientemente sus problemas de cumplimiento de las normativas de privacidad con la ayuda de Akamai Identity Cloud. La solución ha permitido a la empresa ofrecer a sus clientes transparencia y control sobre sus datos personales. Para ello, minimizan la PII que se recopila durante el registro y, antes de procesar cualquier dato, solicitan el consentimiento del usuario.

Identity Cloud les permite invocar formularios de consentimiento de forma progresiva para cada propósito, y les ofrece la posibilidad de personalizar la experiencia de usuario durante el registro e inicio de sesión. Esto ha permitido que los consumidores de la empresa conozcan claramente el propósito de los datos para los que dan su consentimiento de uso, así como los casos en que han decidido no darlo. Los consumidores pueden revisar, cambiar y revocar sus opciones de consentimiento en cualquier momento.

La empresa confía en las funciones de acceso de Identity Cloud para restringir el acceso a los registros de datos (y a campos específicos en los registros) dependiendo de la función del personal de la empresa que accede a los datos de identidad. Esto significa, por ejemplo, que un representante del servicio de atención al cliente tiene derechos de acceso diferentes a los asignados al personal de marketing o a los desarrolladores. Esta característica única reduce los riesgos de exposición de los datos de los clientes y proporciona un nivel inigualable de seguridad de datos.

Al proporcionar un repositorio central de datos de clientes con un control de acceso detallado, la solución puede mitigar la proliferación de datos de identidad "tóxicos" (por ejemplo, datos que aún se almacenan en la base de datos después de que el cliente haya revocado su consentimiento o solicitado su eliminación). El repositorio central también simplifica la supresión de datos en el contexto de solicitudes de "derecho al olvido".

Por último, todas las opciones de consentimiento se almacenan con el perfil del cliente en un formulario preparado para auditorías, junto con los registros de cambios y de auditoría sobre quién accedió a qué recursos y cuándo.

Garantizar la protección de datos

El cumplimiento va más allá de las preocupaciones por la privacidad. Mantener la seguridad de los datos de los clientes y protegerlos contra posibles amenazas implica también garantizar la privacidad. Los datos de identidad personal se han convertido en el objetivo principal de los ataques de hackers, puesto que es fácil explotarlos y sacarles partido. En el informe sobre el coste de las filtraciones de datos de 2018[23] que ha llevado a cabo Ponemon Institute con el patrocinio de IBM Security, se descubrió que el 48 % de las organizaciones encuestadas identificaban un ataque malicioso o delictivo como la causa principal de una filtración de datos, con un coste medio de aproximadamente 157 dólares por cada registro de identidad filtrado.

Debido a que las filtraciones suelen afectar a cientos de miles de registros (a veces, incluso millones), el coste derivado puede representar un golpe devastador para una empresa, sin contar la pérdida de ingresos que conlleva el daño a su reputación, el menoscabo de la confianza de los clientes y las posibles multas por el incumplimiento del RGPD y la CCPA.

La necesidad del control de identidades

Las identidades personales son activos valiosos, no solo para las empresas que recopilan PII, sino también para los consumidores propietarios de dicha información, que desean protegerla frente a cualquier uso indebido.

A medida que el mundo digital se expande a cada vez más ámbitos de la vida personal de los consumidores, aumenta la cantidad de datos personales que engrosan los datos de perfil de las empresas. Nombre, dirección, número de teléfono, sexo, información de pago, preferencias personales o los historiales de búsqueda y compras son solo algunos de los datos que quedan expuestos. La necesidad de que las empresas protejan estos datos tan vitales ha crecido considerablemente, y los entes reguladores de todo el mundo están respondiendo a esta necesidad en forma de normativas cada vez más estrictas.

El cumplimiento de las normativas y la seguridad son factores clave que aumentan en gran medida la complejidad y la importancia de la gestión de identidades. No obstante, las soluciones de gestión de identidades de nivel empresarial pueden ofrecer a los clientes transparencia y control sobre sus datos personales al minimizar los datos que se recopilan durante el registro y al solicitar su consentimiento antes de procesar cualquier tipo de información.

Con una gestión de identidades adecuada, las empresas pueden recuperar la confianza de los consumidores.

Una empresa multinacional de bebidas logra un rápido cumplimiento del RGPD

Una empresa multinacional de bebidas se enfrentó a un abrumador plazo de dos meses para cumplir con todos los requisitos de privacidad que exigía el RGPD para sus clientes europeos antes de la fecha de entrada en vigor. La empresa ya había implementado Identity Cloud, pero necesitaba garantizar rápidamente el cumplimiento de las cambiantes normativas de privacidad del consumidor.

El cumplimiento íntegro se logró en tan solo dos meses. El objetivo de la empresa era obtener el consentimiento explícito de los consumidores para el uso de sus datos con fines de marketing y personalización de acuerdo con los requisitos del RGPD. Identity Cloud proporcionó a la empresa formularios de consentimiento detallados y altamente personalizables que se podían invocar progresivamente en cualquier propiedad digital, desde sitios web y aplicaciones móviles hasta dispositivos IoT. Además de permitir el cumplimiento del RGPD, esta potente solución les ayudó a ganarse la confianza de sus clientes al facilitarles la comprensión y gestión de sus preferencias de consentimiento.

Una de las tareas más difíciles de la implementación fue lograr el perfecto equilibrio entre el "derecho al olvido" del RGPD y las obligaciones legales de conservación de datos durante una promoción. Identity Cloud les permitió garantizar que los datos se conservaban durante el periodo legal y se borraban al final de dicho plazo, además de poder comunicárselo al cliente.

Akamai Identity Cloud

Identity Cloud es la solución de Akamai para el control de acceso e identidades de los clientes. La plataforma proporciona todo lo que las empresas necesitan para que sus clientes puedan crear cuentas personales e iniciar sesión de forma segura en sitios web, aplicaciones móviles o aplicaciones basadas en el IoT. Identity Cloud proporciona herramientas que se pueden utilizar para reducir de forma significativa los esfuerzos necesarios para el cumplimiento de normativas de privacidad, al tiempo que proporciona a las empresas un repositorio de perfiles de clientes muy seguro y permite una visión integral del cliente.

Identity Cloud ofrece capacidades y experiencias de usuario específicas que pueden ayudar a las empresas a cumplir los requisitos normativos. Las funciones de protección y privacidad de Identity Cloud incluyen registro de clientes, inicio de sesión, autenticación, inicio de sesión único, control de acceso delimitado, gestión de preferencias y consentimiento y muchas otras funciones necesarias para recopilar, gestionar y proteger datos personales.

Identity Cloud pone las siguientes funciones a disposición de las empresas para que cumplan las normativas en materia de privacidad:

- casillas de verificación para el consentimiento explícito;
- gestión centralizada para el control del acceso;
- obtención de permisos, registro y elaboración de perfiles progresivos;
- mecanismos sencillos de acceso a los registros de datos;
- mecanismos de integridad y corrección de datos;
- portabilidad de datos;
- borrado o eliminación de datos;
- acceso delimitado para usuarios e integraciones;
- seudonimización de datos;
- clasificación por edades.

Al implementar Identity Cloud, las empresas y las organizaciones pueden utilizar la gestión de identidades empresarial de forma rápida y flexible. Diseñada con una arquitectura nativa en la nube, la solución se amplía de manera inteligente en función de las exigencias para adaptarse a los picos de tráfico y ofrecer una y experiencia extraordinaria a cientos de millones de usuarios. Akamai Identity Cloud se ha diseñado para ayudar a las organizaciones a cumplir las normativas internacionales de privacidad, fomentar la confianza en su marca, gestionar los datos de los clientes y mitigar los riesgos, al lograr que los datos estén disponibles de forma segura en todas las regiones y aplicaciones.

Para obtener más información sobre Akamai Identity Cloud, visite akamai.com/identitycloud.

Conclusión

El cumplimiento del RGPD, la CCPA y otras normativas de privacidad relacionadas, así como la garantía de seguridad, son factores críticos para cualquier empresa u organización que desee desarrollar y mantener relaciones de confianza con sus clientes. Los consumidores esperan transparencia y exigen que sus valiosos datos personales se mantengan privados y seguros. Las recientes filtraciones de datos, robos de identidades y otros sucesos globales relacionados subrayan la urgente necesidad de que las empresas estén en posición de custodiar debidamente la PII.

Cuando los clientes permiten que una organización recopile y almacene su información privada, básicamente están firmando un contrato de confianza. Si esa confianza se rompe, es muy difícil restablecerla. La recopilación y el almacenamiento de datos de los clientes, así como el procesamiento de las credenciales y la información personal de los clientes, es un compromiso que las empresas hoy en día no pueden permitirse vulnerar o poner en peligro. Si se rompe la confianza, se puede poner en riesgo fácilmente la reputación de la marca, la fidelidad del cliente y, en última instancia, los ingresos corrientes y el éxito empresarial.

Apéndice: descripción general de los requisitos normativos de privacidad

Este apéndice presenta un resumen de los tipos generales de requisitos que se pueden encontrar en el RGPD, la CCPA y en muchas de las principales normativas de protección de datos y privacidad de todo el mundo: consentimiento, derecho de oposición, derecho de acceso, derecho al olvido, portabilidad de datos, seguridad y notificación de filtraciones. La implementación de estos derechos varía entre las diferentes leyes de privacidad y protección de datos que se están promulgando. Para determinar de qué manera le afecta cada una de ellas, debe consultar a un asesor legal.

Si desea obtener información sobre la forma en que Akamai Identity Cloud puede ayudarle a superar estos requisitos de cumplimiento normativo, lea nuestra entrada de blog.

Consentimiento	Normalmente, las organizaciones deben obtener el consentimiento de los usuarios finales antes de recopilar y procesar sus datos personales con determinados fines. Los requisitos para obtener un consentimiento válido y las situaciones en que este es necesario varían entre las regulaciones aplicables.
Derecho de oposición	Los requisitos autorizan al interesado a oponerse a la utilización de sus datos personales para determinados tipos de tratamiento, como el marketing directo o el análisis estadístico.
Derecho de acceso	Muchas leyes otorgan al interesado el derecho a acceder, revisar y corregir los datos personales que se van a procesar y, en algunos casos, a buscar información adicional sobre los usos y las divulgaciones de dichos datos.

Derecho a borrar o eliminar datos personales	Muchas leyes incluyen el "derecho al olvido" para que los consumidores puedan solicitar que se borren sus datos personales y se dejen de distribuir a terceros o exponer a un tratamiento por parte de terceros.
Portabilidad de datos	Las empresas deben proporcionar a los interesados copias de sus datos en un formato de uso común y legible por máquina para que puedan transferirlos a otra organización sin ningún obstáculo.
Seguridad	Las empresas deben implementar medidas de protección de datos acordes al riesgo para garantizar en todo momento que no se tenga acceso, se modifique, se pierda, se destruya o se divulgue información de manera inadvertida o ilícita.
Notificación de filtraciones	Las organizaciones deben notificar a los usuarios finales de cualquier filtración de datos en un plazo de tiempo determinado después de haber tenido conocimiento de la situación.

FUENTES

1) https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/
3) https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
4) https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
5) https://www.caprivacy.org/
6) https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf
8) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
9) https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=418&year=2019
10) http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=billpage&stab=01&id=sb0613&tab=subject3&ys=2019rs
11) https://malegislature.gov/Bills/191/SD341
12) http://billstatus.ls.state.ms.us/documents/2019/html/HB/1200-1299/HB1253IN.htm
13) https://www.nmlegis.gov/Legislation/Legislation?chamber=S&legType=B&legNo=176&year=19
14) https://assembly.state.ny.us/leg/?default_fld=&bn=S00224&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y
15) https://www.legis.nd.gov/assembly/66-2019/bill-index/bi1485.html
16) http://webserver.rilin.state.ri.us/billtext19/senatetext19/S0234.htm
17) https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04518I.htm
18) https://pd.rkn.gov.ru/authority/p146/p164/
19) https://pd.rkn.gov.ru/authority/p146/p164/
20) https://www.tc260.org.cn/front/postDetail.html?id=20190201173320
21) https://meity.gov.in/content/personal-data-protection-bill-2018
22) https://www.ppc.go.jp/en/
23) https://www.ibm.com/security/data-breach