Análisis comparativo de la protección de datos y la ciberseguridad. Modelos europeo, americano y chino

Nombre: XINRUI LI

Tutor: Joan Lluís Pérez Francesch

Fecha: junio de 2024

Trabajo Final del Máster en Integración Europea

Resumen

Con el avance continuo de la era digital, el rápido desarrollo de la digitalización ha traído consigo problemas de seguridad a las redes cada vez más abiertas. La ciberseguridad, es decir, el ataque de algunos delincuentes a los sistemas de hardware a través de la red para robar, alterar la información y los datos de los usuarios, e incluso algunos hackers pueden realizar estafas y extorsiones a través de la red. Desde el inicio del nuevo siglo, los problemas relacionados con la ciberseguridad han ido aumentando gradualmente, causando un cierto impacto en la vida de las personas de manera invisible, así como afectando a la propiedad y operaciones normales de las empresas. Dada la importancia de los problemas de ciberseguridad, este documento analiza las políticas de la Unión Europea (RGPD), Estados Unidos (CBPR) y China (Ley de Seguridad de Datos de China) con respecto a la seguridad de redes y el flujo transfronterizo de datos. Tomando como ejemplo los modelos comerciales de exportación de vehículos de cada región, se realiza un análisis detallado de las estrategias, implementación, efectividad, prácticas tecnológicas y la percepción pública de las leyes en cada región, con el fin de determinar qué legislación es relativamente más efectiva y práctica.

Palabras clave: Ciberseguridad, protección de datos, privacidad, modelo europeo, americano y chino

Abstract

As the digital age continues to advance, the rapid development of digitization has brought about security issues to gradually open networks. Cybersecurity, which involves some criminals attacking the hardware of network systems through the internet, thereby stealing, altering users' information and data, and even some hackers engaging in scams and extortion through the network. Since the beginning of the new century, issues related to cybersecurity have gradually increased, causing a certain impact on people's lives invisibly, as well as affecting the property and normal operations of enterprises. Therefore, based on the importance of cybersecurity issues, this article analyzes the policies of the European Union (RGPD), the United States (CBPR), and China (China's Data Security Law) regarding network security and cross-border data flow. Taking the trade forms of vehicle exports in each region as practical examples, a detailed analysis is conducted on the strategies, implementation, effectiveness, technical practices, and public perceptions of the laws in each region, in order to determine which laws are relatively more effective and practical.

Key words: Cybersecurity, data protection, privacy, European, American, and Chinese models.

Índice

1.Introducción

1.1. Presentación del tema y su relevancia

En la era digital, los datos se han convertido en un recurso invaluable para nuestra sociedad, a menudo comparados con el "nuevo sol" debido a su ubicuidad y papel fundamental en casi todas las actividades humanas[1]. Según reportes de *The Economist*[2], las organizaciones están cada vez más enfocadas en acumular grandes cantidades de datos con relativamente pocas restricciones, con el objetivo de someterlos a análisis avanzados y así obtener beneficios económicos. Por ejemplo, datos de la OCDE indican que en 2017 estas actividades generaron alrededor de 600 mil millones de dólares en ganancias en los Estados Unidos y 500 mil millones de euros en la Unión Europea.

En el mundo interconectado y digitalizado de hoy, los datos se han convertido en uno de los recursos más valiosos. Los problemas y desafíos relacionados con la seguridad nacional, la protección de datos personales, entre otros, se han vuelto cada vez más prominentes, convirtiéndose en temas centrales en el comercio, la industria, la economía, la política y la sociedad en general de cada país. En el modelo económico impulsado por los datos, las organizaciones recopilan y utilizan datos, mientras que los usuarios proporcionan sus datos personales sin un pleno consentimiento informado. La mayoría de los debates sobre el flujo transfronterizo de datos giran en torno a la información personal identificable, lo que ha suscitado preocupaciones nacionales, sociales e individuales sobre la privacidad. Desde bases de datos fundamentales, datos como etnia, afiliación política o religiosa, características biométricas, datos de salud, orientación sexual, y ubicación geográfica precisa, entre otros, pueden dejar de ser privados.

---

[1] Castellanos Rodríguez, Albert. (2021). *Descontruyendo las transferencias de datos personales, desprotección en los Estados Unidos de América y el entorno asiático*, Barcelona.

[2] Ker, Daniel. (2020). Perspectives on the value of data and data flows, *OECD Digital Economy Papers*, No. 299, P15, Publicado por OECD, Paris.

Según informes públicos, en 2020 el costo promedio de las pérdidas globales por filtraciones de datos fue de 11.45 millones de dólares estadounidenses, con un total de 7,098 incidentes de filtración de datos en 2019, que involucraron 15.1 mil millones de registros de datos, lo que representa un aumento del 284% en comparación con 2018. Los incidentes de filtración de datos tienen un impacto significativo y causan pérdidas importantes. La protección efectiva de estos datos y la seguridad de la infraestructura digital son cruciales para garantizar la confianza en la economía digital, fomentar la innovación y proteger los derechos individuales. Con la implementación de regulaciones como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y el creciente enfoque en amenazas cibernéticas como el robo de datos, el espionaje cibernético y los ataques de ransomware, comprender las diferencias y similitudes en los enfoques de protección de datos y ciberseguridad entre regiones se vuelve vital para establecer estándares en este campo y fomentar la cooperación internacional. Con el crecimiento exponencial en la generación y compartición de datos en línea, junto con la complejidad de las amenazas cibernéticas, es necesario examinar cómo diferentes regiones del mundo están abordando estos desafíos. En este contexto, el análisis comparativo de los modelos de protección de datos y ciberseguridad en Europa, Estados Unidos y China se presenta como un enfoque crucial para comprender las fortalezas, debilidades y diferencias entre estos sistemas. A través de este análisis comparativo, se puede obtener una comprensión más profunda de las prácticas, regulaciones y desafíos enfrentados por cada región, así como el impacto de estos modelos en la seguridad y privacidad de individuos, organizaciones y países.

1.2 Objetivos de la investigación

En la actual gobernanza del ciberespacio, no hay ningún tema que contenga una discusión tan compleja como la seguridad de los datos en la red: soberanía de los datos, protección de la privacidad, aplicación y jurisdicción legal, e incluso las

reglas del comercio internacional. Especialmente después del ***evento de Snowden en 2013***[3], con la propagación de la preocupación por la seguridad, los gobiernos de varios países han introducido una variedad de requisitos de localización, lo que ha aumentado la confusión y el malentendido sobre las políticas de flujo transfronterizo de datos. El principal objetivo de esta investigación es realizar un análisis comparativo exhaustivo de los modelos de protección de datos y seguridad cibernética en Europa, Estados Unidos y China, evaluando detalladamente las leyes, regulaciones, políticas y prácticas implementadas en cada región. A través de este análisis, nuestro objetivo es comprender en profundidad los enfoques adoptados por cada región y su impacto en la protección de datos y la seguridad cibernética a nivel global. Mediante casos de estudio prácticos, se realizará un detallado contraste entre las políticas más representativas de seguridad cibernética y flujo transfronterizo de datos de la Unión Europea, Estados Unidos y China, extrayendo similitudes y diferencias. Además, se propondrán sugerencias de mejora de políticas basadas en la reflexión sobre la reforma institucional de la UE en relación con las políticas de flujo transfronterizo de datos. Finalmente, se evaluará la razonabilidad y eficacia de las políticas implementadas por cada modelo, así como la percepción pública de las mismas, para determinar cuál país cuenta con políticas más adecuadas y efectivas.

1.3 Justificación de la comparación entre los modelos de ciberseguridad

La comparación entre los modelos de ciberseguridad en Europa, Estados Unidos y China es de suma importancia. En primer lugar, estas tres regiones representan algunos de los actores más influyentes en el espacio digital global, cada uno con

[3] ***El caso Edward Snowden*** (2013) se refiere a cuando él reveló a los medios el programa de vigilancia secreto de la Agencia de Seguridad Nacional (NSA) de Estados Unidos. Snowden, un ex-empleado de la Agencia Central de Inteligencia (CIA) y contratista, expuso en junio de 2013 un programa de vigilancia gubernamental a gran escala, que incluía la vigilancia de registros de comunicaciones telefónicas e internet. Reveló la actividad de vigilancia masiva del gobierno de Estados Unidos sobre ciudadanos globales mediante la filtración de documentos clasificados, lo que provocó atención y controversia a nivel mundial.

enfoques regulatorios y culturales únicos. Comparar los modelos de seguridad cibernética en Europa, Estados Unidos y China es crucial para comprender cómo diferentes contextos culturales, políticos y económicos influyen en las estrategias y enfoques adoptados en este campo. Además, la globalización y la interconexión económica están aumentando la necesidad de coordinación y cooperación en materia de protección de datos y seguridad cibernética. Identificar las mejores prácticas y desafíos comunes en diferentes regiones proporciona información para la formulación de políticas y decisiones a nivel nacional e internacional, fortaleciendo así la seguridad cibernética a nivel global. Dada la naturaleza global de las amenazas cibernéticas, esta comparación es crucial para fomentar la cooperación transfronteriza y el intercambio de conocimientos en la lucha contra el cibercrimen y la protección de la privacidad en el mundo digital de hoy.

2. Contexto Teórico y Conceptual de la Ciberseguridad

2.1 Fundamentos de la ciberseguridad y protección de datos

La ciberseguridad de las redes, por lo general, se refiere a la seguridad de las redes informáticas, el procesamiento y la transmisión de información. Dado que la red es un soporte de transmisión de información, la seguridad de la información está estrechamente relacionada con la seguridad de la red. El objetivo fundamental de una red informática es compartir recursos, y la red de comunicación es una forma de realizar la compartición de recursos de red; por tanto, una red informática es segura, y la red de comunicación informática correspondiente también debe ser segura. Los tres pilares fundamentales de la ciberseguridad son la confidencialidad, la integridad y la disponibilidad. Los tres pilares fundamentales son la confidencialidad, la integridad y la disponibilidad. Este concepto engloba todas las actividades de defensa mediadas por infraestructuras TIC[4].

[4] El Centro Nacional de Criptografía se creó en 2004 por Real Decreto 421/2004 y forma parte del CNI (Centro Nacional de Inteligencia). El CNI se rige por la Ley 11/2002, de 6 de mayo, que le asigna todas las funciones relativas a la seguridad de

Desde el punto de vista del usuario (particular o empresa), desea que la información personal transmitida a través de la red (como números de cuentas bancarias y contraseñas de acceso a Internet, etc.) no sea detectada por terceros, y que la información transmitida a través de la red esté libre de amenazas como escuchas, robos, manipulaciones, etc., lo que se conoce como confidencialidad. Desde el punto de vista de los operadores y gestores de la red, desean que la red de información local funcione con normalidad, preste servicios con normalidad, esté libre de ataques fuera de la red y de amenazas como virus informáticos, accesos no autorizados, denegación de servicio, ocupación no autorizada y control no autorizado de los recursos de la red. Desde el punto de vista del Departamento de Seguridad y Confidencialidad, quiere filtrar y bloquear la información ilegal y perjudicial que afecte a la seguridad nacional o a secretos comerciales, evitar la filtración de información sobre seguridad nacional o secretos comerciales a través de la red, y evitar causar daños a la sociedad y pérdidas económicas a las empresas. Desde la perspectiva de la educación social y la ideología, hay que evitar la difusión de contenidos malsanos y orientar correctamente la cultura positiva de la red.

Lo más esencial de la ciberseguridad son las prácticas, estrategias y tecnologías diseñadas para proteger los sistemas informáticos, las redes, los equipos y los datos de diversas formas de ataque y daño (como ataques de malware, piratería informática, robo de identidad, fraude en la red, etc.) y garantizar el funcionamiento continuo y estable de los servicios de red. La aplicación de medidas de seguridad adecuadas es otra de las claves de la seguridad de la red. Estas medidas pueden incluir la configuración de seguridad de sistemas y redes, la aplicación de parches de seguridad, el uso de cortafuegos y sistemas de detección de intrusos, la adopción de políticas de autenticación, etc. Por ejemplo, la instalación de cortafuegos puede bloquear eficazmente los ataques

---

las tecnologías de la información y la protección de la información clasificada), 2013, P9.

malintencionados y los accesos no autorizados; la aplicación de sistemas de detección de intrusos puede detectar y responder a tiempo a posibles amenazas a la seguridad; y el cifrado de datos puede garantizar la confidencialidad e integridad de la información durante su transmisión y almacenamiento. Estas medidas actúan como un escudo protector de la seguridad de la red. Pretenden crear una barrera eficaz contra posibles ataques, maximizar la protección efectiva de nuestro cibermundo y reducir las amenazas potenciales combinando las medidads.

Además de las medidas técnicas, la educación y la concienciación en materia de seguridad digital desempeñan un papel crucial en la protección de datos. Los usuarios deben recibir formación para identificar y evitar prácticas peligrosas, como prohibir hacer clic en enlaces sospechosos o revelar información sensible a personas no autorizadas. Promover una cultura de ciberseguridad en todo el mundo es clave para reforzar la resistencia frente a las ciberamenazas.

La ciberseguridad y la protección de datos se basan en la comprensión de las amenazas, la aplicación de medidas de seguridad adecuadas y el fomento de una cultura de la seguridad. Estos elementos constituyen los pilares para construir defensas de la información en un entorno digital cada vez más complejo y volátil.

2.2 Importancia en la era digital en el entorno actual

Con el rápido desarrollo de la tecnología informática, la ciberseguridad de información se han convertido en una importante garantía del desarrollo social. Hay mucha información sensible, incluso secretos de Estado. Por ello, es inevitable que se produzcan todo tipo de ataques de origen humano en todo el mundo (por ejemplo, fuga de información, robo de información, manipulación de datos, borrado de datos, virus informáticos, etc.). Las brechas de seguridad pueden tener consecuencias económicas devastadoras para las empresas. Por ejemplo, en 2017, ***Equifax***[5], una de las principales agencias de informes de

[5] ***Equifax*** es una agencia de informes crediticios del consumidor fundada en los

crédito de Estados Unidos, sufrió una violación de datos en la que se vio comprometida la información personal de más de 147 millones de personas. La brecha resultó en millones de dólares en multas, pérdida de clientes y daños a la reputación de la empresa, con un impacto significativo en su valor de mercado y operaciones comerciales. Uno de los retos tecnológicos más importantes de la era de las redes digitales es cómo gestionar eficazmente el volumen y la diversidad sin precedentes de datos de IoT. Los dispositivos IoT generan enormes cantidades de datos, incluidos datos personales.

La ciberseguridad abarca una amplia gama de dimensiones, como la protección de la privacidad personal, la seguridad empresarial, la seguridad nacional y la seguridad financiera, y es la piedra angular del desarrollo de la sociedad de la información.[6]

En la era digital actual, en la que la tecnología es omnipresente y los sistemas y dispositivos están interconectados a escala mundial, la ciberseguridad se ha convertido en un factor clave que afecta a las personas y a las organizaciones, así como a la sociedad en su conjunto. La importancia de la seguridad en la red se refleja principalmente en los siguientes aspectos:

1. Protección de datos sensibles: Se almacena información personal y datos sensibles en la red, y en un mundo en el que la información es un activo valioso, proteger los datos sensibles es fundamental. Desde información personal y financiera hasta secretos comerciales, la exposición indebida de estos datos puede

---

Estados Unidos en 1899 que recopila y almacena información sobre más de 800 millones de consumidores y más de 88 millones de empresas en todo el mundo. En septiembre de 2017, Equifax sufrió un ataque de ciberseguridad a gran escala. Los piratas informáticos accedieron a los datos personales de aproximadamente 143 millones de consumidores y obtuvieron información de identidad, como nombres de consumidores, números de seguro social, fechas de nacimiento y direcciones. Al menos 200.000 clientes sufrieron el robo de la información de sus tarjetas de crédito. Fue una de las mayores filtraciones de datos en la historia de Estados Unidos y afectó a casi la mitad de la población estadounidense.

[6] Jia Wenshan & Zhao Limin. (2022). *La protección de datos personales en la era de la economía de los datos, Instituto para la Cooperación y el Entendimiento Global*, Pekin.

tener consecuencias individuales y colectivas devastadoras. La ciberseguridad también es importante para protegerse de la propagación de programas como ransomware y troyanos, ataques que tienen un grave impacto en la seguridad pública de la sociedad. La ciberseguridad es esencial para garantizar que las transacciones financieras y las operaciones en línea sean seguras, y que las transacciones y la información financiera no sean robadas o manipuladas. La ciberseguridad proporciona las herramientas y estrategias necesarias para proteger esta información de amenazas como el robo de identidad, la extorsión y el ciberespionaje.[7] Una ciberseguridad suficientemente sólida protege esta información frente a robos y la privacidad personal y la seguridad de la propiedad frente a amenazas inminentes. Para las empresas y organizaciones, la ciberseguridad puede proteger los secretos comerciales y la propiedad intelectual contra el robo y la divulgación.

Además, la ciberseguridad es una cuestión de seguridad nacional. En la era de la información, la seguridad nacional y la ciberseguridad son inseparables. No hay seguridad nacional sin ciberseguridad, y la ciberseguridad afecta a la seguridad política, económica y militar del país, y los ciberataques y la ciberdelincuencia se han convertido en una de las graves amenazas para la seguridad nacional.[8] Si la red no es segura, la información confidencial del país puede ser robada o filtrada, lo que supone una grave amenaza para la seguridad nacional. Por ejemplo, las organizaciones de piratas informáticos pueden atacar los sistemas de red del gobierno, robar información confidencial o dañar infraestructuras críticas, lo que supone una gran amenaza para la seguridad nacional.

2. Confianza de los consumidores: En la economía digital actual, en la que las transacciones en línea son cada vez más habituales, la confianza de los consumidores es fundamental para el éxito de las empresas. Los consumidores

[7] Serrano Pérez, María Mercedes. (2003). *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid.

[8] ¿Por qué es importante la seguridad de los datos? ¿Cómo protegerlo?, *Revista de información de Internet de China.* (2022), consultado 13.05.2024 desde https://news.cctv.com/2022/06/21/ARTIdhgLL1sSK5Hjl0uYWybr220621.shtml

esperan que las empresas protejan adecuadamente su información personal y financiera. La ciberseguridad desempeña un papel clave en la creación y el mantenimiento de esta confianza al proteger la información personal y financiera de los clientes frente a posibles ciberamenazas. Por ejemplo, los minoristas en línea que protegen los datos de los clientes mediante el uso de tecnologías de cifrado y protección contra el fraude pueden ganarse la confianza de los consumidores y aumentar las ventas. La falta de ciberseguridad puede reducir la confianza del consumidor, provocando la pérdida de clientes y dañando la reputación de la marca.

3. Reducir la ciberdelincuencia: En la era digital, la ciberdelincuencia ha experimentado un preocupante aumento. Desde el robo de información personal, al fraude en el sector financiero, pasando por el ciberespionaje y el ciberterrorismo para la seguridad nacional, estos delitos se han convertido en una grave amenaza para la privacidad personal, los intereses de las empresas y la seguridad de los gobiernos. Necesitamos tomar medidas más eficaces para prevenir y responder a la ciberdelincuencia. La ciberseguridad desempeña un papel vital en la mitigación de estas amenazas mediante la identificación, prevención y respuesta a las actividades de ciberdelincuencia, protegiendo así a individuos, organizaciones y gobiernos de pérdidas económicas y compromisos de seguridad. Esto incluye no sólo las defensas a nivel técnico, como la construcción de cortafuegos y bases de datos de virus más potentes, sino también la necesidad de concienciar a la sociedad en su conjunto sobre la ciberseguridad, para que todo el mundo sea consciente de la importancia de la ciberseguridad y aprenda a proteger la seguridad de su propia información.

Además, el Gobierno y las organizaciones pertinentes también deben reforzar la lucha contra la ciberdelincuencia y frenar su propagación mediante leyes y políticas más estrictas. Al mismo tiempo, también necesitamos reforzar la cooperación internacional para afrontar conjuntamente los retos de la ciberdelincuencia transnacional.

Reducir la ciberdelincuencia es una tarea importante que debemos afrontar en la era digital. Sólo mediante los esfuerzos conjuntos de toda la sociedad para mejorar continuamente la concienciación sobre la ciberseguridad y las capacidades de defensa podremos crear un entorno digital seguro y digno de confianza y salvaguardar los derechos e intereses y la seguridad de todos.

En la era digital actual, la importancia de la seguridad de las redes va más allá de los límites de la seguridad informática tradicional. Desde proteger datos sensibles hasta garantizar la continuidad de las empresas o aumentar la confianza de los consumidores, la ciberseguridad se ha convertido en un pilar fundamental para el funcionamiento seguro y eficiente de la sociedad moderna. La ciberseguridad desempeña un papel fundamental en la protección de los activos digitales y la creación de un entorno digital seguro y de confianza que no puede subestimarse.

2.3 Marco teórico de protección de datos y privacidad en un entorno globalizado

Primero presento las ramas básicas de la seguridad de la información.

Gráfica 1：Marco de información[9]

A medida que nuestras sociedades y economías dependen cada vez más de las tecnologías digitales, crece la necesidad de compartir y transferir activos de datos, incluidos los datos personales, a través de Internet. Los flujos transfronterizos de datos son fundamentales para el comercio internacional y el desarrollo económico

[9] Yamith Andrés, Niño Wilches. (2015). *Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo pymes*, Washington.

mundial. De hecho, la transformación digital de la economía mundial no sería posible sin la arquitectura abierta y global de Internet y la capacidad de los datos para cruzar las fronteras nacionales. Las empresas y organizaciones multinacionales deben cumplir la normativa de protección de datos en múltiples jurisdicciones para garantizar la transferencia y el uso lícitos de los datos. Además, los flujos de datos transfronterizos plantean riesgos para la seguridad y la privacidad de los datos, lo que exige medidas de seguridad adicionales para protegerlos.

En la economía globalizada actual, las transferencias internacionales de datos se han convertido en una práctica habitual. Sin embargo, estas transferencias conllevan riesgos significativos en términos de privacidad y seguridad de los datos, lo que exige garantizar que los datos se transfieren de forma segura y de conformidad con las estrictas normativas de protección de datos aplicables en las distintas jurisdicciones.

A continuación, se presenta un marco teórico para la protección de datos y la privacidad en un entorno globalizado a través de algunas perspectivas personales:

1. Reglamentos y normas internacionales:

En un entorno globalizado, las empresas deben cumplir los reglamentos y normas internacionales relativos a la transferencia internacional de datos. Por ejemplo, el Reglamento General de Protección de Datos (RGPD)[10] de la Unión Europea establece requisitos estrictos para las transferencias de datos fuera del Espacio Económico Europeo (EEE), exigiendo a los países receptores que adopten garantías adecuadas de protección de datos. El Reglamento pretende proteger la privacidad de los ciudadanos europeos aunque sus datos se transfieran a países con normas de protección de datos menos estrictas.

[10] El Reglamento General de Protección de Datos (RGPD) es una regulación de protección de datos y privacidad en la legislación de la UE para todos los individuos de la UE, que cubre la exportación de datos personales fuera de Europa. Los principales objetivos del RGPD son recuperar el control individual sobre los datos personales y simplificar la armonización de las regulaciones dentro de la UE para los negocios internacionales.

2. Armonizar la normativa internacional:

En un mundo cada vez más interconectado, es cada vez más necesario armonizar las normas y reglamentos de protección de datos a nivel internacional. La falta de coherencia entre las distintas legislaciones nacionales puede obstaculizar la transferencia segura de datos a través de las fronteras. La armonización de normativas como el RGPD de la UE con estándares globales puede facilitar las transferencias internacionales de datos mediante la creación de un marco común de protección de datos y privacidad.

3. Seguridad de las transferencias de datos:

La seguridad de las transferencias de datos es fundamental para proteger la transferencia transfronteriza de información sensible. Las empresas deben adoptar fuertes medidas de seguridad, como el cifrado de extremo a extremo y el uso de redes privadas virtuales (VPN), para proteger los datos de la interceptación y los ciberataques durante la transmisión. Por ejemplo, no es posible utilizar redes que no tengan direcciones IP chinas dentro de China, mientras que el uso de una VPN para navegar por extranets también está prohibido.

4. Evaluación de riesgos y cumplimiento de la normativa:

Antes de participar en transferencias internacionales de datos, las empresas deben llevar a cabo una evaluación exhaustiva de los riesgos asociados, incluidos los riesgos de ciberseguridad y los riesgos legales asociados al cumplimiento normativo. Esto incluye identificar las amenazas potenciales a la seguridad de los datos durante las transferencias de datos y garantizar que se aplican las medidas de ciberseguridad adecuadas para mitigar estos riesgos.

5. Protección de datos en terceros países:

En muchos casos, una empresa puede necesitar transferir datos a un país con un nivel de protección de datos diferente al de su país de origen. En estos casos, las empresas deben tomar medidas adicionales para garantizar la protección de los datos transferidos. Esto puede incluir la aplicación de cláusulas contractuales estándar, el uso de códigos de conducta acreditados o la adhesión a sistemas de

certificación acreditados para garantizar que los datos están adecuadamente protegidos incluso en terceros países.

6. Soberanía de los datos y jurisdicción transfronteriza

En un entorno globalizado en el que los datos pueden almacenarse y tratarse en servidores situados en distintos países, el concepto de soberanía de los datos plantea un reto. Esto plantea cuestiones de jurisdicción y de aplicación de las leyes de protección de datos. Por ejemplo, ¿qué ocurre si los datos de un ciudadano de un país se almacenan en un servidor de otro país con leyes de protección de la intimidad diferentes? Para hacer frente a estos retos será necesaria una mayor cooperación internacional y planteamientos innovadores que garanticen la protección de los datos incluso cuando se transfieren a países con normas de protección de datos diferentes.

El marco teórico de la protección de datos y la privacidad en un entorno globalizado es un elemento clave para garantizar la seguridad y la privacidad de los datos. Los marcos teóricos pretenden equilibrar el flujo de datos y la necesidad de protección de la privacidad para garantizar el uso legítimo de los datos y la protección de la privacidad individual. El marco teórico de la protección de datos y la privacidad incluye los principios fundamentales de confidencialidad, integridad y disponibilidad de los datos. Estos principios exigen que los datos estén debidamente encriptados y almacenados de forma segura para garantizar la integridad y disponibilidad de los datos, al tiempo que se impide su acceso y uso no autorizados. La ciberseguridad desempeña un papel clave en la transferencia internacional de datos en un entorno globalizado. Mediante la adopción de medidas de ciberseguridad adecuadas y el cumplimiento de las normas y reglamentos internacionales, las empresas pueden garantizar la protección de la privacidad y la seguridad de los datos durante las transferencias transfronterizas y la protección de los datos frente a posibles ciberamenazas en un mundo digitalmente interconectado.

Por lo tanto, es necesario un marco doctrinal armonizado para la protección de datos y la privacidad. Este marco debe tener en cuenta las diferencias jurídicas y culturales entre jurisdicciones y promover la cooperación y la normalización internacionales. Mediante el desarrollo de normas y mejores prácticas internacionales, puede garantizarse el flujo legal, seguro y fiable de datos, protegiendo al mismo tiempo la privacidad individual y la seguridad de los datos.

3. Leyes y Enfoques del Modelo Europeo sobre la Transferencia de Datos: Europa(RGPD)，Modelo Americano (CBPR) y Modelo Chino(Ley de Seguridad de Datos de China)

3.1 Detalles y principios fundamentales del RGPD

El RGPD hace referencia al Reglamento General de Protección de Datos de la Unión Europea, identificado con el número de regulación (UE) 2016/679. Es una normativa promulgada y aplicada por el Parlamento Europeo y el Consejo de la Unión Europea el 25 de mayo de 2018, que establece normas para la protección de datos y la privacidad de todas las personas de la Unión Europea, así como para la exportación de datos personales fuera de Europa, reemplazando a la antigua Directiva de Protección de Datos[11] 95/46/CE. El objetivo principal del RGPD es devolver el control de los datos personales a los individuos y simplificar las regulaciones uniformes dentro de la Unión Europea para facilitar el comercio internacional. Este reglamento incluye disposiciones y requisitos sobre la información personal identificable de los sujetos de datos dentro de la Unión

[11] La Directiva de Protección de Datos (Directiva 95/46/CE relativa a la protección de personas físicas en lo respectivo al tratamiento de datos personales y a la libre circulación de estos datos) fue una directiva de la Unión Europea adoptada en 1995 que regulaba el procesamiento de datos personales dentro de la Unión Europea. Esta directiva fue sustituida en 2016 por el Reglamento General de Protección de Datos de la Unión Europea, aplicable en todos los países de la unión.

Europea y es aplicable a todas las empresas que hacen negocios en Europa, independientemente de su ubicación física. Los datos personales deben ser almacenados de manera seudonimizada o anonimizada, y se deben utilizar los ajustes de privacidad más altos por defecto para evitar la divulgación de datos sin un consentimiento explícito, y no se pueden utilizar para identificar a los sujetos sin información adicional almacenada por separado. Cualquier procesamiento de datos personales debe contar con el consentimiento explícito del titular de los datos, a menos que se realice sobre la base de una justificación legal establecida por la normativa.

El RGPD se aplica a las actividades de procesamiento de datos personales relacionadas con ciudadanos de la Unión Europea, tanto dentro como fuera del territorio de la UE. Este reglamento enfatiza la importancia de la protección de datos personales y establece una serie de normas que las organizaciones deben cumplir, que incluyen la definición clara de los propósitos del procesamiento de datos, la obtención del consentimiento del usuario, la garantía de la seguridad de los datos y la notificación a las autoridades reguladoras en caso de violación de datos, entre otros aspectos. El incumplimiento del RGPD puede acarrear sanciones económicas significativas. La normativa refuerza la legislación general de protección de datos en Europa y unifica la supervisión reguladora bajo una sola autoridad.

El Reglamento General de Protección de Datos (RGPD) aborda principalmente el tema de la transferencia transfronteriza de datos en los artículos 44 al 49. A continuación se presentan los principales aspectos y disposiciones relacionadas con la transferencia transfronteriza de datos[12]:

1. Restricciones a la transferencia de datos: Según lo establecido en el RGPD, los datos personales solo pueden transferirse a países u organizaciones

[12] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Art. 44-49.

internacionales que no hayan sido reconocidos por la Unión Europea si dichos países u organizaciones ofrecen medidas de protección adecuadas.

2. Medidas de protección adecuadas: El RGPD enumera claramente varias medidas de protección destinadas a garantizar la seguridad de los datos personales durante la transferencia transfronteriza. Estas medidas incluyen: leyes de protección de datos específicas de países reconocidos por la Comisión Europea, cláusulas contractuales estándar aplicables a la transferencia de datos, normas y reglas de carácter vinculante, normas de organismos acreditados, acuerdos y compromisos contractuales, así como reglas corporativas vinculantes.

3. Transferencia de datos en circunstancias especiales: El RGPD también establece reglas para la transferencia de datos en circunstancias especiales, como cuando el sujeto de datos da su consentimiento explícito para la transferencia transfronteriza, cuando la transferencia es necesaria para cumplir un contrato, cuando es necesaria para proteger intereses vitales del sujeto de datos, o cuando la transferencia se lleva a cabo por razones de interés público.

4. Responsabilidades de las autoridades de supervisión: El RGPD asigna responsabilidades a las autoridades de protección de datos de los diferentes Estados miembros de la Unión Europea para supervisar la conformidad de la transferencia transfronteriza de datos y tomar medidas contra conductas no conformes. Las disposiciones principales sobre el mecanismo de transferencia transfronteriza de datos del RGPD se encuentran en el Capítulo V (artículos 44 al 49), que establece las condiciones que deben cumplir los responsables del tratamiento de datos y los encargados del tratamiento.

Siempre y cuando el responsable del tratamiento o el encargado del tratamiento utilice las demás medidas de garantía previstas en el artículo 49 en ausencia de una decisión de adecuación, se permite la transferencia transfronteriza de datos. Estas medidas de garantía incluyen:

1. Documentos legalmente vinculantes y ejecutables entre autoridades o instituciones públicas.

2. Reglas corporativas vinculantes (***BCRs***[13]) establecidas de conformidad con el artículo 47.

3. Cláusulas contractuales tipo de protección de datos aprobadas por la Comisión mediante un procedimiento de examen conforme al artículo 93, apartado 2.

4. Cláusulas contractuales tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión Europea mediante un procedimiento de examen conforme al artículo 93, apartado 2[14].

5. Códigos de conducta aprobados conforme al artículo 40, así como compromisos vinculantes y ejecutables adoptados por responsables o encargados establecidos en terceros países, que apliquen las garantías adecuadas para proteger los derechos de los interesados.

6. Mecanismos de certificación aprobados conforme al artículo 42, así como compromisos vinculantes y ejecutables adoptados por responsables o encargados establecidos en terceros países, que apliquen las garantías adecuadas para proteger los derechos de los interesados.

3.2 Análisis de leyes y enfoques en ciberseguridad en EE. UU(CBPR)

El modelo de la Unión Europea es el más ampliamente adoptado en el mundo en términos de protección de datos personales. La mayoría de los países han legislado basándose en la Directiva de Protección de Datos de 1995 (DPD), que es el predecesor del actual RGPD implementado en 2018. Algunos países han adoptado la mayor parte del contenido de la DPD, mientras que otros han tomado elementos clave. La única excepción es Estados Unidos, que no ha adoptado el

---

[13] ***BCRs*** (*Binding Corporate Rules*). Dicha aprobación ha sido otorgada por parte de la AEPD (Agencia Española de Protección de Datos) tras la participación del resto de autoridades europeas y del Comité Europeo de Protección de Datos (EDPB) para garantizar un correcto uso de los datos personales y mantener la Privacidad.

[14] Decisión de Ejecución (UE) 2021/915 de la Comisión de 4 de junio de 2021, relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el Art. 28, Apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el Art. 29, Apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo.

modelo de protección de datos de la UE. Conviene remarcar que, en el ámbito internacional EE.UU, ha ratificado las Directrices sobre protección de la vida privada de la OCDE de 1980 y reafirmaron su aplicabilidad, con especial referencia al e-commerce, en 1998[15].En los Estados Unidos, el enfoque del mecanismo APEC CBPR (Reglas de Privacidad Transfronteriza de APEC) se considera ampliamente como un mejor modelo para la transferencia transfronteriza de datos. El CBPR se estableció en 2012 como un mecanismo de protección de la privacidad regional en el que los países miembros participan de forma voluntaria, con el objetivo de promover el flujo transfronterizo seguro y legal de datos personales y empresariales entre los países miembros. Dado que no tiene las regulaciones estrictas del RGPD de la UE, es más propicio para facilitar el flujo de datos entre países. En 2012, Estados Unidos se convirtió en el primer país en unirse al mecanismo CBPR, y la Comisión Federal de Comercio (FTC) de Estados Unidos se convirtió en la primera agencia de aplicación interna. El CBPR de APEC se basa en el Marco de Privacidad de APEC, que tiene como objetivo equilibrar la libre circulación transfronteriza de datos con la protección de la información personal y la privacidad. Las empresas que participan en el CBPR deben ser auditadas por organismos de certificación independientes para garantizar que el tratamiento y la transferencia de datos cumplan con los requisitos del CBPR.

El CBPR requiere que las empresas tomen medidas de seguridad adecuadas para proteger la seguridad de los datos transferidos transfronterizamente. Esto puede incluir medidas como el cifrado, protocolos de transmisión segura y control de acceso, entre otros, para prevenir accesos no autorizados y filtraciones de datos. El CBPR también exige que el receptor de los datos cumpla con los requisitos del CBPR para garantizar que los datos transferidos transfronterizamente estén

[15] Arribas Luque, José María. (2002). Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: El sistema de principios de Puerto Seguro, *Diario La Ley*, No. 549, P2.

protegidos y manejados adecuadamente en el receptor. El receptor debe cumplir con los fines acordados para el uso de los datos y garantizar su seguridad. El CBPR fomenta el reconocimiento mutuo de la certificación de empresas entre los países miembros para promover el flujo de datos y garantizar un nivel uniforme de protección de la privacidad de los datos. Esto facilita que las empresas que transfieren datos entre los países miembros de la APEC cumplan con estándares de protección de la privacidad uniformes. El Marco de Privacidad de APEC es un estándar negociado que enumera los elementos básicos de los estándares mínimos de protección de datos que los miembros de la APEC deben establecer o revisar cuando formulan leyes internas. Establece requisitos mínimos de protección de datos cuando no existe legislación o leyes internas que proporcionen una protección sustancialmente menor a los titulares de datos.

El mecanismo CBPR se compone de tres partes[16]: en primer lugar, establece el marco de requisitos básicos de protección de datos; en segundo lugar, implica la selección de organismos de rendición de cuentas y un sistema de certificación, estos organismos son terceros independientes reconocidos por la APEC y tienen la capacidad de evaluar y certificar las prácticas de privacidad de las empresas según el marco; y en tercer lugar, establece un mecanismo interno de ejecución.

Para que los países miembros de la APEC se unan a este mecanismo, el CBPR incluye ciertos requisitos específicos que permiten una implementación mínima del marco. Los miembros de la APEC también deben reconocer los organismos de rendición de cuentas, los cuales certifican las prácticas de privacidad de las empresas que desean unirse al mecanismo CBPR y se encargan de resolver las disputas relacionadas con las empresas certificadas.

La Unión Europea considera que la legislación de Estados Unidos no ofrece una protección adecuada de datos. Para abordar este problema y fomentar el flujo de datos entre la UE y Estados Unidos, en 2016 la UE y Estados Unidos llegaron a

---

[16] Bignami, Francesca. (2015). Transatlantic Privacy Regulation: Conflict and Cooperation, 78, *Law and Contemporary Problems*, P231-266.

un acuerdo conocido como el Escudo de Privacidad UE-EE.UU. ***(EU and US Privacy Shield)***[17]. El Privacy Shield implementa los estándares de protección de datos exigidos por la UE a través de un mecanismo de adhesión voluntaria similar al CBPR. El Privacy Shield incluye garantías del gobierno de Estados Unidos sobre el acceso limitado a los datos, así como disposiciones relacionadas con el cumplimiento y la aplicación de la ley en Estados Unidos[18]. El Departamento de Comercio de Estados Unidos supervisa el cumplimiento, mientras que la Comisión Federal de Comercio (FTC) es responsable de la ejecución.

El CBPR proporciona a individuos y empresas un mecanismo para transferir datos transfronterizos cumpliendo con estándares internacionales de protección de la privacidad. Al adoptar el CBPR, las empresas pueden mejorar la seguridad y el cumplimiento de la transferencia de datos, al tiempo que protegen la privacidad de los datos personales.

3.3 Visión general de las leyes y enfoques de ciberseguridad en China (Ley de Seguridad de Datos de China)

La Ley de Seguridad de Datos de la República Popular China es una importante legislación promulgada por el órgano legislativo nacional de China en el campo de la seguridad de datos. Fue aprobada el 10 de junio de 2021 y entró en vigor el 1 de septiembre de 2021. Su objetivo es regular las actividades de procesamiento de datos en industrias principales como la industrial, las telecomunicaciones, el transporte, las finanzas, los recursos naturales, la salud, la educación, la tecnología, entre otras, garantizando la seguridad de los datos, fomentando el desarrollo y uso de los datos, protegiendo los derechos e intereses legítimos de

---

[17] El Marco del Escudo de Privacidad fue diseñado por el Departamento de Comercio de EE. UU. y la Comisión Europea para proporcionar a las empresas de ambos lados del Atlántico un mecanismo para cumplir con los requisitos de protección de datos al transferir datos personales de la Unión Europea a los Estados Unidos en apoyo del comercio transatlántico.

[18] Atoum, Issa. (2014). *A holistic cyber security implementation framework*. Information Management & Computer Security.

individuos y organizaciones, y defendiendo la soberanía, seguridad y los intereses de desarrollo del país. Sus principales disposiciones incluyen[19]:

1. Principios básicos de seguridad de datos: La Ley de Seguridad de Datos establece claramente los principios básicos de protección de la seguridad de datos, que incluyen los principios de legalidad, legitimidad y necesidad, así como los principios de minimización de datos, propósito específico, publicidad y transparencia.

2. Protección de la información personal: La ley enfatiza la importancia de la protección de la información personal, estableciendo que la recopilación, uso, procesamiento, almacenamiento y transmisión de información personal deben cumplir con los principios de legalidad, legitimidad y necesidad, para garantizar los derechos e intereses legítimos de los sujetos de información personal.

3. Protección de datos importantes: La legislación establece requisitos para la protección de datos importantes, definiendo claramente la responsabilidad del Estado en la protección de la seguridad de los datos importantes y especificando el alcance y las medidas de protección de los datos importantes.

4. Sistema de gestión de seguridad de datos: La ley exige que los gobiernos de todos los niveles y los departamentos relevantes establezcan un sistema de gestión de seguridad de datos sólido para fortalecer la supervisión y protección de la seguridad de los datos.

5. Transferencia transfronteriza de datos: La legislación establece requisitos de gestión para la transferencia transfronteriza de datos, especificando los procedimientos y requisitos para la aprobación de la transferencia transfronteriza de datos que involucran intereses importantes como la seguridad nacional y el interés público.

6. Evaluación de seguridad y supervisión y verificación: La ley establece un sistema para la evaluación de seguridad y la supervisión y verificación de las

[19] El Congreso Nacional Popular de la República Popular China. (2021). *Ley de Seguridad de Datos de la República Popular China*, Pekin.

actividades de procesamiento de datos, fortaleciendo la supervisión y gestión del trabajo de seguridad de datos.

China otorga gran importancia a la transferencia transfronteriza de datos. Las situaciones que implican la seguridad nacional, intereses públicos significativos y otros intereses importantes requieren procedimientos de aprobación. Antes de la exportación de datos, se debe realizar una evaluación de seguridad de exportación de datos.[20] Esta evaluación incluye la seguridad de los datos, los riesgos potenciales después de la exportación y el impacto en la cooperación económica y tecnológica internacional, así como en los intercambios internacionales. Después de la exportación de datos, el receptor de los datos debe protegerlos de acuerdo con los acuerdos contractuales y los requisitos legales, y no debe utilizar los datos fuera del alcance previsto. La ley fomenta y apoya la colaboración del gobierno chino con otros países y organizaciones internacionales en el ámbito de la seguridad de los datos, para promover conjuntamente una transferencia transfronteriza de datos segura y ordenada.

La Ley de Seguridad de los Datos de la República Popular China establece un sistema integral de gestión de la seguridad de los datos, con el objetivo de proteger la seguridad nacional y los intereses públicos, garantizar la seguridad de la información personal y los datos importantes, y promover una transferencia transfronteriza de datos razonable, ordenada y segura.

4. Estudio de un caso. Análisis sobre la exportación de vehículos europeo, americano y chino

Todos los países deben aplicar formalmente las regulaciones correspondientes promulgadas para abordar un problema específico, ya que solo así estas regulaciones tienen sentido en términos de gestión normativa. Del mismo modo, las políticas sobre el flujo transfronterizo de datos en relación con la seguridad cibernética son positivas

[20] ¿Profundidad-Interpretación integral de la "Ley de Seguridad de Datos", Instituto para la Industria de Internet, Universidad de Tsinghua. (2021), consultado 06.04.2024 desde https://www.iii.tsinghua.edu.cn/info/1058/2668.html

para ayudar a los países respectivos a proteger la seguridad en línea y controlar el flujo de datos. A continuación, se realizará un análisis comparativo de los modelos de seguridad cibernética de diferentes países, tomando como ejemplo la exportación de vehículos de China.

4.1 Comparación de la estrategia de cada modelo

1. RGPD (Reglamento General de Protección de Datos):

Alcance de aplicación:

El RGPD se aplica a cualquier organización que opere dentro del territorio de la Unión Europea o tenga relaciones comerciales con ella. Se aplica tanto al sector privado como al público en el procesamiento de datos personales, incluido el procesamiento de datos personales de fabricantes y proveedores de vehículos.

En resumen, el RGPD no solo se aplica a organizaciones empresariales dentro del territorio de la UE, sino también a aquellas fuera de la UE, siempre que ofrezcan productos, servicios o monitoreen el comportamiento relacionado con los datos de los sujetos en la UE, o procesen y mantengan datos personales de sujetos que residen dentro del territorio de la UE.

Requisitos de protección de datos:

El RGPD establece estrictos estándares de protección de datos. Los fabricantes y proveedores de vehículos deben garantizar que el procesamiento de datos personales durante la producción, venta y servicio postventa sea legal, transparente y proteja la seguridad y privacidad de los datos. El RGPD se centra en proteger los derechos y libertades fundamentales de las personas, con un énfasis especial en la protección de los derechos de los datos personales. Los datos personales pueden incluir el nombre, dirección y contacto del propietario del vehículo, así como datos de conducción y registros de mantenimiento del vehículo. Se requiere que las empresas proporcionen a los sujetos de datos derechos de control pertinentes, al tiempo que enfatizan la seguridad de los datos y la protección de la privacidad.

Procesamiento de datos:

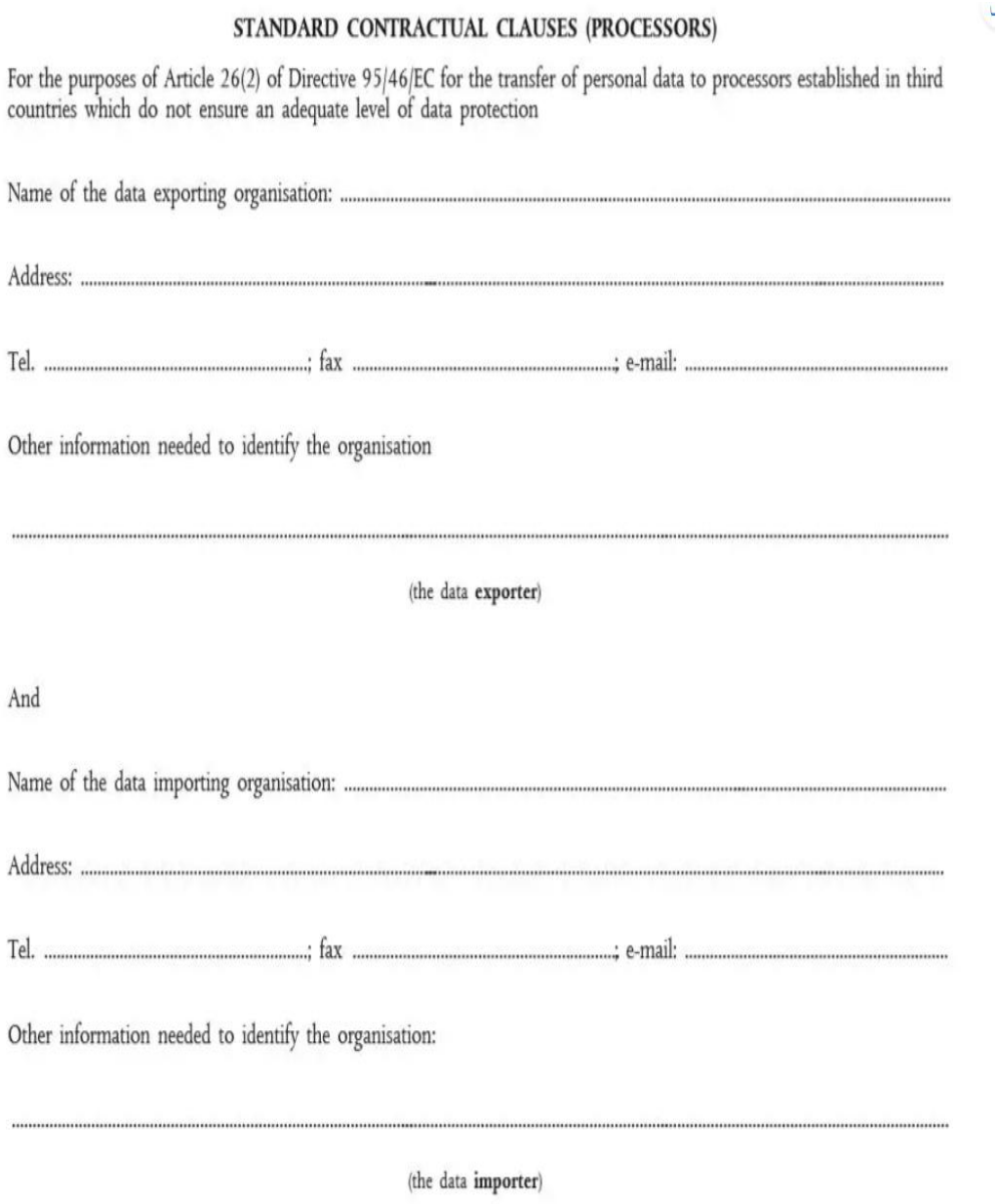
La definición de procesamiento de datos en el RGPD de la UE es amplia e incluye la recopilación, registro, divulgación mediante transmisión y eliminación, y especialmente abarca el procesamiento total o parcialmente automatizado en el contexto de IoT. El artículo 5 del RGPD de la UE establece que la recopilación de datos personales debe realizarse con un propósito específico, claro y legal, y no se pueden procesar de manera incompatible con ese propósito. El RGPD de la UE regula el procesamiento de información, incluida la descripción de qué tipos de datos se procesan, quiénes son los destinatarios de los datos, los derechos de los sujetos de datos, el origen de los datos, si los datos están sujetos a análisis automatizado, la importancia del procesamiento para los sujetos de datos y las consecuencias previstas. Las recientes disposiciones de ***inteligencia artificial (IA) de la Unión Europea***[21] establecen claramente regulaciones para la información de datos transmitida a través de la red, normando que la aplicación y desarrollo de la IA no representen una amenaza para la privacidad y seguridad de los ciudadanos de la Unión Europea. Estas disposiciones de inteligencia artificial de la Unión Europea suelen incluir medidas de protección de datos personales para garantizar que los sistemas de IA cumplan con el RGPD y otras regulaciones pertinentes al procesar datos. Principalmente previenen la filtración, el abuso o el acceso no autorizado a los datos públicos, fortaleciendo así la seguridad en línea.

Restricciones de transferencia de datos:

El RGPD establece restricciones para la transferencia transfronteriza de datos personales, que solo pueden realizarse bajo condiciones específicas, como la celebración de cláusulas contractuales estándar (SCC) o la obtención de la aprobación de la autoridad de protección de datos de la UE. Los fabricantes y

[21] La "Ley de Inteligencia Artificial" es una regulación oficial publicada por la Unión Europea el 13 de marzo de 2024. Esta ley tiene como objetivo establecer un marco regulatorio y legal común para la introducción de la inteligencia artificial. Su alcance abarca todas las categorías de inteligencia artificial. Se clasifica y regula todas las actividades relacionadas con la red, incluida la aplicación de medidas de aplicación de la ley contra el abuso de la identificación biométrica en tiempo real.

proveedores de vehículos deben cumplir con las disposiciones del RGPD al transferir datos personales transfronterizos, garantizando la legalidad y seguridad de la transferencia de datos.



STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel. .....; fax .....; e-mail: .....

Other information needed to identify the organisation

.....

(the data **exporter**)

And

Name of the data importing organisation: .....

Address: .....

Tel. .....; fax .....; e-mail: .....

Other information needed to identify the organisation:

.....

(the data **importer**)

Gráfica 2: Muestra de convenio de SCC[22]

2. APEC CBPR:

Alcance de aplicación:

[22] Sun Bihua. (2018). *Explicación detallada del sistema RGPD (3): el secreto de la transmisión transfronteriza*, Shenzhen.

El APEC CBPR es un mecanismo de protección de la privacidad utilizado principalmente en los Estados Unidos y se aplica a la transferencia de datos entre todos los países miembros de APEC.

Requisitos de protección de datos[23]:

El CBPR enfatiza los principios de protección de la privacidad, incluida la transparencia, la limitación de la finalidad y la seguridad de los datos, pero no tiene requisitos legales específicos y obligatorios como el RGPD. Más bien, depende más de la adhesión voluntaria y el reconocimiento. El marco del APEC CBPR generalmente no protege los datos personales que ya están disponibles al público, ni los datos personales recopilados directamente de los sujetos de datos. Los fabricantes y proveedores de vehículos pueden unirse voluntariamente al marco del CBPR y demostrar su cumplimiento de los requisitos del APEC CBPR mediante la auto certificación.

Procesamiento de datos:

El marco del APEC CBPR no define el procesamiento de datos, pero su definición de "controlador de información personal" menciona algunas actividades de procesamiento específicas, como la "recopilación, tenencia, procesamiento, uso, divulgación o transferencia de información personal"[24]. El marco del APEC CBPR señala que es posible que los controladores de información personal no estén obligados a proporcionar notificaciones sobre la recopilación y el uso de información pública, lo cual es muy diferente al RGPD de la UE. Los requisitos básicos del marco del APEC CBPR suelen ser menos estrictos que los del RGPD, ya que solo establece que la recopilación debe realizarse de manera legal y justa, y notificar al sujeto de datos en casos apropiados.

Reglas de transferencia de datos:

---

[23] Solove, Daniel. (2016). A Brief History of Information Privacy Law, *GWU(George Washington University) Law School Public Law Research Paper*, No. 215, P16.

[24] RGPD de la UE vs. CBPR de APEC: Análisis comparativo de los mecanismos de transferencia de datos transfronterizos, Seguridad Neican. (2022), consultado 08.03.2024 desde https://www.secrss.com/articles/42244

El marco del CBPR no impone restricciones estrictas a la transferencia de datos, sino que fomenta la adhesión voluntaria entre los países miembros y proporciona un mecanismo de auto certificación para demostrar el cumplimiento de los sistemas de protección de datos. Las empresas que se unen al marco del APEC CBPR pueden transferir datos transfronterizos entre los países miembros de APEC de manera más conveniente, pero no tienen restricciones tan estrictas en la transferencia transfronteriza de datos como el RGPD.

Aunque el RGPD tiene un mecanismo similar de adhesión voluntaria, el CBPR generalmente es más atractivo para las empresas estadounidenses porque es menos complejo y normativo, lo que favorece el flujo transfronterizo de datos. De hecho, el enfoque del mecanismo CBPR difiere del RGPD, ya que este último se centra principalmente en las obligaciones de derechos humanos de la UE con respecto a la protección de la información personal y la privacidad. Por el contrario, el CBPR se centra principalmente en facilitar el flujo transfronterizo de datos.

3. Ley de Seguridad de Datos de China:

Alcance de aplicación:

La Ley de Seguridad de Datos de China se aplica a todas las organizaciones y personas dentro del territorio chino, así como a la transferencia transfronteriza de datos que involucre datos personales chinos.

Requisitos de protección de datos:

La Ley de Seguridad de Datos de China establece requisitos específicos para la protección de datos personales y datos importantes. Las empresas deben garantizar que los datos personales que procesen sean legales y seguros, y cumplir con las disposiciones legales pertinentes. Los fabricantes y proveedores de vehículos también pueden necesitar considerar la gestión segura de datos importantes, como los datos técnicos del vehículo y la información de investigación y desarrollo.

Procesamiento de datos[25]:

El procesamiento de datos debe ser transparente, y los sujetos de datos deben ser plenamente informados sobre la recopilación, uso y almacenamiento de datos, obteniendo su consentimiento cuando sea necesario. Los procesadores de datos deben minimizar la recopilación y el uso de datos, limitándose a lo estrictamente necesario.

Aprobación de transferencia de datos:

Para la transferencia transfronteriza de datos que involucre intereses importantes como la seguridad nacional y el interés público, se requiere aprobación y supervisión para garantizar la seguridad de los datos. Los fabricantes y proveedores de vehículos deben cumplir con los requisitos de la Ley de Seguridad de Datos de China al obtener la aprobación para la transferencia transfronteriza de datos y asegurarse de cumplir con los requisitos legales.

En el caso práctico de exportación de vehículos, estas regulaciones afectarán las actividades de procesamiento y transferencia transfronteriza de datos de los fabricantes y proveedores de vehículos. El RGPD establece requisitos estrictos para la protección de datos personales y aplica restricciones a la transferencia transfronteriza, lo que requiere que las empresas tomen medidas adecuadas para garantizar el cumplimiento. Por otro lado, el CBPR proporciona un mecanismo de protección de la privacidad voluntario, enfatizando la cooperación y la confianza entre los países miembros. El marco del APEC CBPR establece un estándar mínimo de protección de datos, mientras que el RGPD de la UE establece requisitos más detallados y vinculantes que pueden aplicarse directamente como ley. Por último, la Ley de Seguridad de Datos de China establece requisitos específicos para la protección de datos personales y datos importantes, fortaleciendo la aprobación y gestión de la transferencia de datos para garantizar su seguridad. Las empresas deben desarrollar estrategias de gestión de datos y

[25] Ministerio de Asuntos Civiles de la República Popular China. (2022). Análisis de los puntos clave legales de la "Ley de Seguridad de Datos de la República Popular China".

transferencia transfronteriza adecuadas de acuerdo con los requisitos de las diferentes regulaciones para garantizar la seguridad y el cumplimiento de los datos.

4.2 Evaluación comparativa de la implementación y efectividad de cada modelo

1. RGPD (Reglamento General de Protección de Datos):

El RGPD requiere que las empresas supervisen y gestionen exhaustivamente las actividades de procesamiento de datos personales. Las empresas deben establecer procesos detallados de procesamiento de datos, que abarquen la recopilación, uso, almacenamiento y eliminación de datos, garantizando que todas las operaciones relacionadas con los datos cumplan con los requisitos legales. Se exige a las empresas que implementen medidas técnicas y organizativas para proteger la seguridad de los datos personales, como la encriptación de datos, el control de acceso y los protocolos de transmisión segura. El RGPD impone restricciones estrictas a la transferencia transfronteriza de datos, requiriendo que las empresas evalúen la legalidad y los riesgos de la transferencia de datos, y tomen medidas necesarias para garantizar la seguridad de los datos. En Europa, la implementación del RGPD ha elevado el nivel de protección de datos personales, fortaleciendo los derechos de los titulares de datos y aumentando las sanciones por incumplimiento. Las empresas enfrentan regulaciones más estrictas sobre el procesamiento de datos y mayores costos de cumplimiento. Además, algunos países no europeos también se ven afectados por el RGPD, especialmente aquellos que comercian con la Unión Europea. Algunos países pueden adoptar marcos legales similares al RGPD para mejorar los estándares de protección de datos y cooperar con Europa.

2. APEC CBPR (Reglas de Privacidad Transfronteriza del Foro de Cooperación Económica Asia-Pacífico):

APEC CBPR enfatiza los principios de protección de la privacidad, pero no establece regulaciones estrictas sobre los procesos de gestión de datos específicos de las empresas, dependiendo en gran medida de la auto certificación. Las empresas pueden unirse voluntariamente al marco CBPR y demostrar su cumplimiento con los requisitos de CBPR a través de la auto certificación, incluyendo la transparencia y seguridad de los datos. La adhesión al marco APEC CBPR puede simplificar los procedimientos de transferencia transfronteriza de datos, pero no impone restricciones obligatorias; las empresas pueden elegir libremente los métodos y mecanismos de transferencia de datos según su situación.

3. Ley de Seguridad de Datos de China:

La Ley de Seguridad de Datos de China establece requisitos específicos para la protección de datos personales y datos importantes, incluyendo legalidad, claridad de propósito, transparencia y seguridad. Las empresas deben establecer sistemas de gestión de datos integrales, que incluyan la clasificación, protección por niveles, almacenamiento y copia de seguridad de datos, asegurando que las actividades de procesamiento de datos cumplan con los requisitos legales. Para la transferencia transfronteriza de datos que involucre intereses importantes como la seguridad nacional y el interés público, se requiere aprobación y supervisión para garantizar la seguridad de los datos. Las empresas deben evaluar la legalidad y los riesgos de la transferencia de datos, y obtener la aprobación y gestión de acuerdo con los requisitos legales, garantizando la seguridad y el cumplimiento de los datos[26]. El impacto de la Ley de Seguridad de Datos de China también puede extenderse a otros países, especialmente aquellos con estrechos vínculos

[26] Instituto de Investigación Tencent. (2021). *Comparación de las leyes de protección de información personal en China, Estados Unidos y Europa*, Shenzhen.

económicos con China, lo que podría requerir que las empresas de esos países ajusten sus procesos comerciales para cumplir con los requisitos legales de China.

En resumen, el RGPD, APEC CBPR y la Ley de Seguridad de Datos de China adoptan modelos de implementación diferentes. Las empresas deben considerar las regulaciones de diferentes países según sus necesidades comerciales y posición en el mercado, y desarrollar estrategias adecuadas para garantizar la seguridad y el cumplimiento de los datos.

4.3 Exploración de las tecnologías y prácticas utilizadas en cada región

1. RGPD (Reglamento General de Protección de Datos):

- Encriptación de datos: Los fabricantes y proveedores de vehículos pueden emplear tecnologías de encriptación de extremo a extremo para garantizar la seguridad durante la transmisión y almacenamiento de datos.

- Anonimización y desidentificación: Para los datos que no necesitan estar directamente vinculados a la identidad de una persona, se pueden utilizar técnicas de anonimización o desidentificación para reducir el riesgo de filtración de datos.

- Control de acceso y gestión de permisos: Es crucial establecer un riguroso mecanismo de control de acceso que permita únicamente a personal autorizado acceder y procesar los datos, previniendo accesos no autorizados.

- Capacitación en seguridad de datos: Se deben brindar capacitaciones sobre conciencia en seguridad de datos a los empleados para fortalecer la protección de datos y reducir los riesgos de filtración causados por errores humanos.

2. APEC CBPR (Reglas de Privacidad Transfronteriza del Foro de Cooperación Económica Asia-Pacífico):

- Auto certificación: Las empresas pueden demostrar su cumplimiento con los requisitos de CBPR mediante la auto certificación, posiblemente utilizando servicios de organismos de certificación de terceros para evaluar y certificar sus sistemas de protección de datos.

- Revisión de cumplimiento de datos: Se realiza una revisión de cumplimiento antes de la transferencia de datos para garantizar que cumpla con los requisitos de APEC CBPR, asegurando al mismo tiempo la seguridad y la privacidad de los datos.

- Transparencia en el flujo de datos: Proporcionar a los titulares de datos información detallada sobre los procesos de tratamiento de datos y las políticas de privacidad para aumentar la transparencia y confiabilidad en la gestión de datos.

3. Ley de Seguridad de Datos de China:

- Clasificación y protección de datos por niveles: Se clasifican los datos según su importancia y sensibilidad, implementando medidas de seguridad correspondientes para garantizar su protección.

- Auditoría y monitoreo de seguridad: Se establece un sistema de auditoría y monitoreo de seguridad de datos para supervisar en tiempo real el uso y acceso a los datos, detectando y respondiendo rápidamente a eventos de seguridad.

- Localización de datos: Según los requisitos legales, los datos importantes se almacenan localmente para reducir los riesgos de transferencia transfronteriza y garantizar la protección legal de los datos.

En resumen, el RGPD, APEC CBPR y la Ley de Seguridad de Datos de China utilizan diferentes tecnologías y prácticas en la gestión y transferencia de datos en diversas regiones. Las empresas deben adaptar medidas de gestión y transferencia de datos de acuerdo con los requisitos legales de su área geográfica para garantizar la seguridad y el cumplimiento de los datos.[27] Además, es importante

[27] RGPD de la UE vs. CBPR de APEC: Análisis comparativo de los mecanismos de transferencia de datos transfronterizos, Seguridad Neican. (2022), consultado 08.03.2024 desde https://www.secrss.com/articles/42244

seguir innovando tecnológicamente y explorar nuevas prácticas para mejorar continuamente la gestión de seguridad de datos y adaptarse a los cambios constantes en el entorno legal y las necesidades comerciales.

4.4 Evaluación de la percepción pública sobre la seguridad de datos y sistemas

Desde la perspectiva de la protección de la privacidad de datos, en la región de la Unión Europea, el público en general considera que el RGPD es una regulación positiva, ya que enfatiza el respeto hacia la protección de los datos personales y los derechos de privacidad, lo que puede aumentar la confianza en el uso y la transmisión de datos. Tomando como ejemplo la exportación de vehículos, el público puede estar más preocupado por la protección de su información personal, especialmente los datos relacionados con los vehículos, como los datos de conducción y la información del propietario. Esperan que los fabricantes de vehículos y las empresas relacionadas cumplan con los requisitos del RGPD, refuercen la protección de los datos personales y garanticen su transmisión y tratamiento seguros para prevenir la filtración y el abuso de datos. Es probable que la gente favorezca esta regulación ya que aumenta el control y la transparencia sobre los datos personales.

Para el público estadounidense, es posible que tengan opiniones divergentes. Algunas personas pueden considerar que el CBPR proporciona una forma flexible de gestionar los datos personales, pero otras pueden preocuparse de que no sea lo suficientemente estricto o efectivo, especialmente en lo que respecta a la protección de la privacidad.[28] En general, el público apoya tomar medidas para proteger la privacidad y la seguridad de los datos. Pueden considerar que las empresas que participan en el APEC CBPR son más confiables, ya que siguen los

[28] RGPD de la UE vs. CBPR de APEC: Análisis comparativo de los mecanismos de transferencia de datos transfronterizos, Seguridad Neican. (2022), consultado 08.03.2024 desde https://www.secrss.com/articles/42244

estándares internacionales de protección de la privacidad y son más propensas a proteger la información personal de los propietarios y conductores de vehículos.

En China, el público en general apoya la Ley de Seguridad Cibernética porque tiene como objetivo mejorar el nivel de seguridad de los datos y la red, y prevenir la filtración de datos y los ataques cibernéticos. La gente cree que esta ley ayuda a proteger la información personal y los datos importantes, y mejora la seguridad en la transmisión y el procesamiento de datos. El público puede estar más preocupado por la protección de la información de los vehículos personales, y esperan que los fabricantes de vehículos y las empresas relacionadas cumplan estrictamente con los requisitos de la ley de seguridad de datos para proteger su privacidad y la seguridad de la información de los vehículos, lo que a su vez contribuye a proteger la información personal y la seguridad nacional.

Desde el punto de vista de la implementación de regulaciones y el cumplimiento empresarial, en Europa, es probable que el público esté más preocupado por si las empresas cumplen estrictamente con los requisitos del RGPD y si las agencias reguladoras ejecutan efectivamente estas normas. Es probable que apoyen tomar medidas contra las empresas que violen las disposiciones del RGPD. El público estadounidense puede mostrar escepticismo sobre si las empresas se unen voluntariamente al marco del CBPR, y están interesados en ver cómo se implementa en la práctica. Pueden esperar que las agencias reguladoras gubernamentales sancionen adecuadamente a las empresas que violen las regulaciones del CBPR. Los ciudadanos chinos pueden estar más interesados en la implementación por parte del gobierno de la ley de seguridad cibernética y si las empresas están tomando las medidas de seguridad necesarias según lo requerido por la ley. Pueden esperar que el gobierno imponga duras sanciones a las empresas que violen las regulaciones.

Desde la perspectiva de la soberanía nacional y el flujo de datos, algunos europeos pueden preocuparse por las restricciones del RGPD en el flujo de datos, especialmente en la transferencia transfronteriza de datos. Sin embargo, otros

pueden ver estas restricciones como una medida para proteger los datos personales y la soberanía nacional. Los estadounidenses pueden estar interesados en saber si el marco del CBPR ayuda a promover el flujo transfronterizo de datos mientras protege la privacidad personal y la seguridad nacional. Los chinos pueden apoyar la Ley de Seguridad Cibernética de China porque creen que ayuda a proteger la soberanía nacional y la seguridad cibernética, aunque pueda imponer ciertas restricciones al flujo transfronterizo de datos.

5. Conclusiones y Recomendaciones

5.1 Conclusiones finales sobre la efectividad y las implicaciones en la ciberseguridad

La comparación y el análisis de las leyes y métodos de protección de datos y seguridad en línea entre Europa, Estados Unidos y China revelan diferentes enfoques y enfoques hacia la privacidad de datos y la transferencia transfronteriza de información. Después de un análisis exhaustivo de los diferentes modelos de seguridad en línea propuestos en este estudio, se puede concluir que cada modelo tiene sus propias ventajas y desventajas en cuanto a la protección de datos y la privacidad en un entorno globalizado.

El Reglamento General de Protección de Datos (RGPD) de Europa destaca debido a su enfoque en la privacidad personal y los derechos de protección de datos, así como su énfasis en la transparencia y responsabilidad de las organizaciones en el procesamiento de datos personales. El RGPD establece un marco regulatorio integral que prioriza la protección de datos personales y la privacidad personal. Sus disposiciones claras y estrictas establecen altos estándares para el procesamiento y transferencia de datos personales, enfatizando el consentimiento explícito del sujeto de los datos y medidas de protección adecuadas. Establece reglas estrictas para cómo las organizaciones pueden recopilar, almacenar y procesar datos personales, y destaca especialmente la transparencia y la rendición de cuentas de las empresas en el manejo de estos

datos. El RGPD establece estándares estrictos y vinculantes para la protección de datos personales, aplicables tanto a las empresas dentro de la UE como a aquellas fuera de la UE que tratan con ciudadanos de la UE. Las empresas deben cumplir con requisitos detallados para el procesamiento de datos, seguridad y transferencia transfronteriza, lo que eleva el nivel de protección de datos y refuerza los derechos de los sujetos de datos. El RGPD de la UE ha sido elogiado por sus métodos avanzados de protección de la privacidad.

Por otro lado, el modelo estadounidense, representado por el Marco de Protección de la Privacidad entre la UE y los Estados Unidos (CBPR), se basa en los principios de autorregulación corporativa y cumplimiento voluntario para las empresas que transfieren datos entre la UE y los Estados Unidos. Aunque proporciona cierto grado de flexibilidad, ha sido criticado por inconsistencias en la efectividad y ejecución, así como preocupaciones sobre la supervisión y ejecución efectiva de los estándares de privacidad. El enfoque de APEC CBPR es más flexible y voluntario, dependiendo de la auto-certificación y cooperación entre los países miembros para garantizar la protección de la privacidad de los datos. Sin embargo, en comparación con el RGPD, este enfoque puede considerarse menos estricto y efectivo, especialmente en cuanto a la protección de los derechos individuales.

El modelo chino, representado por la Ley de Seguridad de los Datos de China, se caracteriza por su énfasis en la soberanía de los datos y la regulación gubernamental, lo que significa que el gobierno chino ejerce una fuerte regulación y control sobre el flujo y procesamiento de datos, centrándose en la aprobación y gestión de la transferencia de datos para garantizar su seguridad. Esto ha suscitado preocupaciones sobre la privacidad y la libertad de expresión.

En términos de percepción pública, el RGPD en Europa se considera una regulación que protege la privacidad individual y aumenta la confianza en el procesamiento de datos personales. En los Estados Unidos, puede haber opiniones divergentes sobre la efectividad del CBPR y si se necesita una

regulación más estricta. Mientras tanto, en China, la Ley de Seguridad de los Datos se ve como una medida positiva para mejorar la seguridad en línea, proteger la información personal y la soberanía nacional. Cada región prioriza diferentes aspectos: Europa enfatiza la protección de datos y la privacidad individual, Estados Unidos aboga por la flexibilidad y la autorregulación, y China busca un equilibrio entre la seguridad de los datos y la facilitación del intercambio internacional de información. Estas diferencias reflejan diferentes conceptos y prioridades sobre la protección de datos y la seguridad en línea en cada región.

A través de casos de exportación de automóviles reales en Europa, Estados Unidos y China, junto con un análisis de los marcos legales de protección de datos y seguridad en línea en estas tres regiones clave, hemos comprendido y comparado las estrategias y métodos específicos de cada modelo de seguridad en línea en un contexto industrial particular. Se ha evaluado cómo aplicar estas estrategias en la práctica, qué tecnologías y prácticas utilizar para proteger datos y sistemas, y cómo estas medidas afectan la percepción pública de la seguridad de datos y la confianza en los productos y servicios ofrecidos. En la UE, el RGPD establece estándares estrictos para la protección de datos, enfatizando la transparencia, seguridad y derechos individuales. Esto ha elevado el nivel de protección de datos en la región y ha impactado las actividades comerciales, especialmente en la exportación de vehículos que involucran procesamiento y transferencia de datos frecuentes. En los Estados Unidos, el enfoque de APEC CBPR es más flexible, basado en la auto-certificación y la cooperación voluntaria entre los países miembros. Aunque puede facilitar el flujo transfronterizo de datos, su efectividad y nivel de protección pueden ser objeto de controversia en comparación con el RGPD. La Ley de Seguridad de los Datos de China establece requisitos específicos para la protección de datos personales y la transferencia transfronteriza, con un énfasis en la aprobación y regulación gubernamental. Esto puede tener un impacto significativo en las estrategias de exportación de

vehículos que involucran datos sensibles (procedimientos de aprobación más complejos y restrictivos, que de hecho no son favorables para la exportación de comercio internacional). La percepción pública de la seguridad de datos y sistemas varía según la región. En la UE, el RGPD como medida de protección de la privacidad es generalmente bien recibido, mientras que en los Estados Unidos puede haber preocupaciones sobre la efectividad del CBPR. En China, la Ley de Seguridad de los Datos se ve como una medida positiva para mejorar la seguridad en línea y proteger la información personal y nacional. Las tecnologías y prácticas utilizadas en cada región afectarán la percepción pública de la seguridad de datos y sistemas.

Cada región tiene sus propios métodos y marcos legales de protección de datos en el contexto de la seguridad en línea, lo que refleja diferencias culturales, políticas y económicas. Sin embargo, la cooperación internacional y el interccambio de mejores prácticas son fundamentales para abordar los desafíos de seguridad en línea en un mundo cada vez más interconectado. La efectividad de cada modelo de seguridad en línea depende de varios factores, incluidos los contextos culturales, legales y tecnológicos de cada región, así como la cooperación internacional y la adaptación continua a nuevas amenazas y desafíos en línea. El éxito en la implementación de medidas de protección de datos requiere encontrar un equilibrio entre la protección de la privacidad y la facilitación del flujo de datos para fomentar la innovación y el desarrollo económico.

5.2 Recomendaciones para futuras acciones y políticas en ciberseguridad y protección de datos

Después de comprender completamente las políticas de ciberseguridad de Europa, Estados Unidos y China, a continuación se presentan algunas sugerencias personales para las futuras políticas de protección en cada región.

Para Europa:

- Continuar fortaleciendo la implementación y aplicabilidad del Reglamento General de Protección de Datos (RGPD) mediante la actualización periódica de sus disposiciones, especialmente en transparencia, seguridad y derechos individuales, para hacer frente a los nuevos desafíos en protección de datos y ciberseguridad. Establecer mecanismos de cumplimiento más estrictos y sanciones más severas para garantizar el cumplimiento efectivo del RGPD.[29]

- Fomentar la cooperación entre los estados miembros de la UE para asegurar una implementación efectiva y uniforme del RGPD a través de sectores y jurisdicciones. Se recomienda la firma de acuerdos bilaterales y multilaterales con países fuera de la UE para fomentar la cooperación internacional en la implementación del RGPD y garantizar la protección transfronteriza de datos.

- Invertir en programas de educación pública y concienciación sobre la importancia de la protección de datos y privacidad en línea para aumentar la comprensión y cumplimiento del RGPD.

- Estimular el desarrollo de tecnologías innovadoras de protección de datos, como la criptografía avanzada y la inteligencia artificial, para hacer frente a las cambiantes amenazas en línea y mantenerse a la vanguardia. Apoyar la inversión en empresas europeas de tecnología de ciberseguridad para promover la innovación y la competitividad en el mercado global.

Para Estados Unidos:

- Considerar la implementación de regulaciones más sólidas y vinculantes para proteger los datos personales, en lugar de depender únicamente de métodos de autorregulación como el Marco de Protección de la Privacidad entre la UE y los EE. UU. (CBPR).

- Mejorar la coordinación entre agencias federales, estatales y locales, así como con el sector privado, para abordar de manera más efectiva las amenazas

[29] Yamith Andrés, Niño Wilches. (2015). *Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo pymes*, Washington.

cibernéticas y garantizar una respuesta rápida y coordinada en caso de incidentes de seguridad.

- Promover la inversión en investigación y desarrollo de tecnologías de ciberseguridad innovadoras y en programas de formación y educación en ciberseguridad para satisfacer la creciente demanda de profesionales cualificados en este campo.
- Ofrecer incentivos fiscales y financieros a las empresas que se adhieran voluntariamente a estándares de ciberseguridad y protección de datos, con el fin de fomentar el cumplimiento de las mejores prácticas.

Para China:

- Buscar un equilibrio entre la seguridad de los datos y la facilitación del intercambio de información mediante la creación de regulaciones claras y transparentes que garanticen la protección de datos sin obstaculizar innecesariamente el flujo de información.[30]
- Mejorar la transparencia y claridad en la aplicación de la Ley de Seguridad de los Datos para proporcionar orientación clara a las empresas y garantizar una aplicación uniforme de las regulaciones de protección de datos en todo el país.
- Fomentar la cooperación internacional en ciberseguridad y protección de datos a través de acuerdos bilaterales y multilaterales para abordar preocupaciones globales de privacidad y seguridad y promover estándares internacionales de protección de datos.

En general, todas las regiones deben priorizar la cooperación internacional y el intercambio de mejores prácticas en ciberseguridad y protección de datos para hacer frente a los desafíos de un mundo cada vez más interconectado. Además, se debe fomentar la innovación y la inversión en tecnologías de ciberseguridad para

[30] Tendencias de desarrollo, desafíos y contramedidas para la seguridad de la red en la nueva era, China: Comisión nacional de desarrollo y reforma, Centro Nacional de Información. (2023), consultado 06.04.2024 desde https://www.ndrc.gov.cn/wsdwhfz/202311/t20231129_1362347.html

garantizar la protección efectiva de datos personales y de infraestructuras críticas. La seguridad cibernética y la protección de datos son elementos clave para garantizar la confianza, la estabilidad y el progreso en la economía y la sociedad digital actual. Se espera que estas medidas mejoren la seguridad cibernética global y protejan la privacidad de los ciudadanos en un mundo cada vez más digitalizado.

6 . Bibliografía

- Arribas Luque, José María. (2002). Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: El sistema de principios de Puerto Seguro, *Diario La Ley*, No. 549, P2.

- Atoum, Issa. (2014). *A holistic cyber security implementation framework*. Information Management & Computer Security.

- Bignami, Francesca. (2015). Transatlantic Privacy Regulation: Conflict and Cooperation, 78, *Law and Contemporary Problems,* P231-266.

- Castellanos Rodríguez, Albert. (2021). *Descontruyendo las transferencias de datos personales, desprotección en los Estados Unidos de América y el entorno asiático*, Barcelona.

- Ker, Daniel. (2020). Perspectives on the value of data and data flows, *OECD Digital Economy Papers*, No. 299, P15, Publicado por OECD, Paris.

- Serrano Pérez, María Mercedes. (2003). *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid.

- Solove, Daniel. (2016). A Brief History of Information Privacy Law, *GWU(George Washington University) Law School Public Law Research Paper*, No. 215, P16.

- Yamith Andrés, Niño Wilches. (2015). *Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo pymes*, Washington.

- Yamith Andrés, Niño Wilches. (2015). *Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo pymes,* Washington.

Bibliografía de China

- Jia Wenshan & Zhao Limin. (2022). *La protección de datos personales en la era de la economía de los datos*, Instituto para la Cooperación y el Entendimiento Global, Pekin.

- Sun Bihua. (2018). *Explicación detallada del sistema RGPD (3): el secreto de la transmisión transfronteriza,* Shenzhen.

- Instituto de Investigación Tencent. (2021). *Comparación de las leyes de protección de información personal en China*, *Estados Unidos y Europa*, Shenzhen.

Referencia a páginas web de China（algunos hay que acceder por vía VPN）

- ¿Profundidad-Interpretación integral de la “Ley de Seguridad de Datos”, Instituto para la Industria de Internet, Universidad de Tsinghua. (2021), consultado 06.04.2024 desde https://www.iii.tsinghua.edu.cn/info/1058/2668.html
- Tendencias de desarrollo, desafíos y contramedidas para la seguridad de la red en la nueva era, China: Comisión nacional de desarrollo y reforma, Centro Nacional de Información. (2023), consultado 06.04.2024 desde https://www.ndrc.gov.cn/wsdwhfz/202311/t20231129_1362347.html
- RGPD de la UE vs. CBPR de APEC: Análisis comparativo de los mecanismos de transferencia de datos transfronterizos, Seguridad Neican. (2022), consultado 08.03.2024 desde https://www.secrss.com/articles/42244
- ¿Por qué es importante la seguridad de los datos? ¿Cómo protegerlo?, Revista de información de Internet de China. (2022), consultado 13.05.2024 desde https://news.cctv.com/2022/06/21/ARTIdhgLL1sSK5Hjl0uYWybr220621.shtml

Normativa Europea

- Decisión de Ejecución (UE) 2021/915 de la Comisión de 4 de junio de 2021, relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el Art. 28, Apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el Art. 29, Apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Art. 44-49.

Normativa China

- El Congreso Nacional Popular de la República Popular China. (2021). Ley de Seguridad de Datos de la República Popular China, Pekin.

-Ministerio de Asuntos Civiles de la República Popular China. (2022). Análisis de los puntos clave legales de la “Ley de Seguridad de Datos de la República Popular China”.