News Science
Online ISSN: 2980-9274 Print ISSN: 2382-9788
Homepage: www.mjourcom.ir

Comparison of Personal Data Protection Laws: Unique General Regulations under the European Union's General Data Protection Regulation (GDPR) and United States Laws

Morteza Mahmodi Parchini[1] | Ladan Riazi[2]✉ | Alireza Pour Ebrahimi[3]

1. Department of Information Technology Management, Kish International Branch, Islamic Azad University, Kish Island, Iran. E-mail: rayanmp1420@gmail.com
2. Corresponding author, Department of Information Technology Management, Faculty of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran. E-mail: l.riazi@gmail.com
3. Department of Industrial Management, Faculty of Management, Islamic Azad University, Karaj Branch, Islamic Azad University, Karaj Branch, Iran. E-mail: poorebrahimi@gmail.com

Article Info

Article type:
Research Article

Article history:
Received: 24 July 2024
Received in revised form: 18 September 2024
Accepted: 20 December 2024
Published online: 15 March 2025

Keywords:
Cyber Regulations,
Data Privacy,
GDPR,
European Union.

ABSTRACT

Objective: This research provides a comparative analysis of the General Data Protection Regulation (GDPR) of the European Union and the data protection laws of the United States, aiming to offer suggestions for improving data protection laws in Iran.

Methods: The study employs a mixed-methods approach, using both qualitative and quantitative techniques for data collection and analysis. Data were gathered through library research, questionnaires, and semi-structured interviews, and were analyzed using SPSS software.

Results: The findings revealed that the GDPR includes a comprehensive and unified framework for the protection of personal data, emphasizing transparency, consent, and notification. In contrast, the United States lacks a comprehensive federal law and relies on a collection of sectoral and state laws. Additionally, the implementation of the GDPR has led to increased transparency and accountability for businesses, whereas U.S. laws have resulted in greater complexity.

Conclusions: The recommendations for improving data protection laws in Iran include drafting a comprehensive and unified law similar to the GDPR, creating effective enforcement mechanisms, increasing public awareness and education, utilizing successful experiences from other countries, adapting laws to the specific needs of Iranian society and its legal system, strengthening the role of regulatory bodies, encouraging the use of new technologies in data protection, and fostering collaboration between public and private sectors.

Cite this article : Mahmodi Parchini, M. ; Riazi, L. & Pour Ebrahimi, A. (2025). Comparison of Personal Data Protection Laws: Unique General Regulations under the European Union's General Data Protection Regulation (GDPR) and United States Laws. *News Science*, 13 (4), 31-35. DOI: http//doi.org/ 10.22034/lrsi.2024.468452.1210

© The Author(s).

DOI: http//doi.org/10.22034/lrsi.2024.468452.1210

EXTENDED ABSTRACT

Comparison of Personal Data Protection Laws: Unique General Regulations under the European Union's General Data Protection Regulation (GDPR) and United States Laws

Morteza Mahmodi Parchini[1] | Ladan Riazi[2]✉ | Alireza Pour Ebrahimi[3]

1. PhD Candidate, Department of Information Technology Management, Kish International Branch, Islamic Azad University, Kish Island, Iran. E-mail: rayanmp1420@gmail.com
2. Corresponding author, Assistant Professor, Department of Information Technology Management, Faculty of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran. E-mail: l.riazi@gmail.com
3. Assistant Professor, Department of Industrial Management, Faculty of Management, Islamic Azad University, Karaj Branch, Islamic Azad University, Karaj Branch, Iran. E-mail: poorebrahimi@gmail.com

Introduction:

In an increasingly digital world, the protection of personal data has become a critical concern for individuals, businesses, and governments alike. The European Union's General Data Protection Regulation (GDPR) represents one of the most comprehensive legal frameworks for data protection, setting a high standard for privacy and security across member states. In contrast, the United States lacks a unified federal data protection law, relying instead on a combination of sectoral regulations and state laws, which leads to a more fragmented approach to data privacy. This research aims to compare these two approaches with the goal of offering informed recommendations for the development of a robust data protection framework in Iran. Given Iran's evolving digital landscape and increasing interaction with global digital markets, it is crucial to develop data protection laws that not only safeguard personal information but also align with international standards.

Method:

This study employs a mixed-methods approach, integrating both qualitative and quantitative research methods to provide a thorough analysis. Data were collected through extensive library research, which involved reviewing existing literature on data protection laws in the European Union, the United States, and Iran. Additionally, structured questionnaires were distributed to key stakeholders, including legal experts, data protection officers, and IT professionals, to gather their perspectives on the effectiveness of current laws and the challenges faced in Iran. Semi-structured interviews with data protection experts further enriched the qualitative data, offering in-depth insights into the practical implications of data protection regulations in different jurisdictions. Quantitative data collected from the questionnaires were analyzed using SPSS software to identify trends and correlations, providing a statistical foundation for the qualitative findings.

Results:

The analysis reveals significant contrasts between the GDPR and U.S. data protection laws. The GDPR is noted for its comprehensive and unified approach, which covers all EU member states and ensures a high level of protection for personal data. Key principles such as transparency, consent, and the right to be forgotten are central to the GDPR, giving individuals significant control over their personal information. The regulation also imposes stringent obligations on businesses, including requirements for data breach notifications and the appointment of data protection officers, which enhance transparency and accountability.

In contrast, the U.S. lacks a federal data protection law, leading to a fragmented legal landscape characterized by a mix of sector-specific regulations (such as HIPAA for health data and COPPA for children's online privacy) and state laws like the California Consumer Privacy Act (CCPA). This fragmented approach results in inconsistencies and legal uncertainties, making it difficult for businesses to navigate and comply with the various regulations. Moreover, the absence of a unified framework often leaves gaps in protection, particularly for individuals whose data does not fall under the specific categories covered by sectoral laws.

The research also highlights that the implementation of the GDPR has resulted in increased public trust in digital systems within the EU, as individuals feel more confident that their data is being handled securely and transparently. Conversely, in the U.S., the complexity and variability of data protection laws can lead to confusion and lower levels of trust among the public.

Conclusions:

The study concludes that Iran would benefit from adopting a comprehensive and unified data protection framework similar to the GDPR. Such a framework would provide clear and consistent guidelines for the collection, processing, and storage of personal data, thereby reducing legal ambiguity and enhancing the protection of individuals' privacy. To ensure the effectiveness of this framework, it is crucial to establish strong enforcement mechanisms, including the creation of a dedicated regulatory body with the authority to monitor compliance and impose penalties for breaches.

Additionally, public awareness and education should be prioritized to ensure that both individuals and organizations understand their rights and obligations under the new law. This can be achieved through targeted campaigns and educational initiatives. Furthermore, while the GDPR offers a valuable model, it is essential to tailor the new laws to Iran's specific cultural and socio-economic context. This means considering local values, traditions, and economic conditions when drafting the regulations, ensuring that they are both effective and culturally appropriate.

Collaboration between public and private sectors is also recommended to foster innovation and the development of new technologies that enhance data protection. By encouraging the private sector to invest in advanced security measures and by facilitating dialogue between different stakeholders, Iran can create a more resilient and secure data protection environment.

In summary, by adopting a comprehensive data protection law modeled after the GDPR and implementing effective enforcement and educational strategies, Iran can significantly improve its data protection standards. This will not only protect individuals' privacy but also enhance public trust in digital services, foster economic growth, and align Iran with international data protection standards. The successful implementation of such a framework would position Iran as a leader in data protection in the region, capable of navigating the challenges of the digital age while respecting its unique cultural identity.

Data Availability Statement
Data available on request from the authors.
Acknowledgements
The authors would like to thank anonymous reviewers.
Ethical considerations
Not applicable.
Funding
Not applicable.
Conflict of interest
The authors declare no conflict of interest.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

علوم خبری
شاپا چاپی: ۲۳۸۳-۹۷۸۸ شاپا الکترونیکی: ۹۲۷۴-۲۹۸۰

مقایسه قوانین حفاظت از داده‌های شخصی: مقررات عمومی منحصر به فرد تحت مقررات حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR[1]) و قوانین ایالات متحده

مرتضی محمودی پرچینی[۱] | لادن ریاضی[۲]✉ | علیرضا پور ابراهیمی[۳]

۱. گروه مدیریت فن آوری اطلاعات ، واحد بین المللی کیش، دانشگاه آزاد اسلامی، جزیره کیش، ایران. رایانامه: ayanmp1420@gmail.com
۲. گروه مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، (نویسنده مسئول)، ایران. رایانامه:l.riazi@gmail.com
۳. گروه مدیریت صنعتی، دانشکده مدیریت، دانشگاه آزاد اسلامی، واحد کرج، دانشگاه آزاد اسلامی، واحد کرج، ایران. رایانامه: poorebrahimi@gmail.com

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۴/۲۸
تاریخ بازنگری: ۱۴۰۳/۶/۲۸
تاریخ پذیرش: ۱۴۰۳/۹/۳۰
تاریخ انتشار: ۱۴۰۳/۱۲/۲۵

کلیدواژه‌ها:
GDPR
اتحادیه اروپا،
حریم خصوصی داده‌ها،
مقررات سایبری.

چکیده

هدف: این پژوهش به تحلیل تطبیقی مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) و قوانین حفاظت از داده‌های ایالات متحده پرداخته و هدف آن ارائه پیشنهاداتی برای بهبود قوانین حفاظت از داده‌ها در ایران است.

روش ها: این تحقیق از روش‌های ترکیبی کیفی و کمی برای جمع‌آوری و تحلیل داده‌ها استفاده کرده است. داده‌ها از طریق مطالعه کتابخانه‌ای، پرسشنامه و مصاحبه‌های نیمه‌ساختاریافته جمع‌آوری و با استفاده از نرم‌افزار SPSS تحلیل شده‌اند.

یافته ها: یافته‌ها تحقیق نشان داد که GDPR شامل چارچوب جامع و یکپارچه‌ای برای حفاظت از داده‌های شخصی است که به شفافیت، رضایت و اطلاع‌رسانی تأکید دارد، در حالی که ایالات متحده فاقد یک قانون جامع فدرال است و به مجموعه‌ای از قوانین بخشی و ایالتی متکی است. همچنین، اجرای GDPR برای کسب‌وکارها منجر به افزایش شفافیت و مسئولیت‌پذیری شده، در حالی که قوانین ایالات متحده پیچیدگی‌های بیشتری ایجاد کرده است.

نتیجه: نتیجه تحقیق حاضر نشان داد که قوانین GDPR به دلیل جامعیت و یکپارچگی خود، به کسب‌وکارها و سازمان‌ها امکان می‌دهد تا با اطمینان بیشتری داده‌های شخصی را پردازش کنند. این امر موجب افزایش اعتماد عمومی به سیستم‌های دیجیتال و کاهش نگرانی‌ها در مورد حفظ حریم خصوصی شده است. در مقابل، در ایالات متحده، فقدان یک قانون جامع فدرال باعث شده که سازمان‌ها با پیچیدگی‌ها و چالش‌های مختلفی در اجرای قوانین حفاظت از داده‌ها مواجه شوند. نکته دیگر اینکه در ایران، بهبود قوانین حفاظت از داده‌ها نیازمند توجه به فرهنگ و ساختار اجتماعی و اقتصادی کشور است. بنابراین، علاوه بر الگو برداری از قوانین موفق بین‌المللی، باید با در نظر گرفتن نیازها و شرایط بومی، قوانین جدیدی تدوین شود. همچنین، افزایش همکاری بین بخش‌های مختلف دولتی و خصوصی و استفاده از تجربیات کشورهای دیگر می‌تواند به اجرای بهتر و کارآمدتر قوانین کمک کند.

به طور کلی، نتایج این پژوهش نشان می‌دهد که با تدوین و اجرای یک قانون جامع و یکپارچه حفاظت از داده‌ها مشابه GDPR و با استفاده از مکانیزم‌های موثر اجرایی و آموزشی، می‌توان به بهبود وضعیت حفاظت از داده‌ها در ایران دست یافت و از چالش‌ها و مشکلات موجود کاسته است. بنابراین، پیشنهاد می شود برای بهبود قوانین حفاظت از داده‌ها در ایران یک قانون جامع و یکپارچه مشابه GDPRتدوین و مکانیزم‌های اجرایی موثر ایجاد شود، آگاهی عمومی و آموزش افزایش یابد، از تجربیات موفق دیگر کشورها استفاده گردد، قوانین با نیازهای خاص جامعه و نظام حقوقی ایران تطبیق پیدا کند، نقش نهادهای نظارتی تقویت شوند، استفاده از فناوری‌های نوین در حفاظت از داده‌ها تشویق شود و همکاری بین نهادهای دولتی و خصوصی فراهم شود.

استناد: محمودی پرچینی، محمود؛ ریاضی، لادن؛ و پورابراهیمی، علیرضا (۱۴۰۳). مقایسه قوانین حفاظت از داده‌های شخصی: مقررات عمومی منحصر به فرد تحت مقررات حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR) و قوانین ایالات متحده. *علوم خبری*، ۱۳ (۴)، ۲۲۴-۲۰۴.
DOI : http//doi.org/10.22034/lrsi.2024.468452.1210

© نویسندگان.

1. General Data Protection Regulation

مقدمه

در عصر دیجیتال، حفاظت از داده‌های شخصی به یکی از مسائل حیاتی و چالش‌برانگیز تبدیل شده است. با پیشرفت فناوری‌های ارتباطی و اطلاعاتی، داده‌ها به‌صورت مستمر در حال تبادل و پردازش هستند. این داده‌ها شامل اطلاعات حساسی می‌شوند که حفاظت از آن‌ها برای حفظ حریم خصوصی افراد بسیار ضروری است. یکی از برجسته‌ترین تلاش‌ها در این زمینه، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) است که در سال ۲۰۱۸ به اجرا درآمد. (European Parliament and Council of the European Union, 2016)

این مقررات با هدف حفاظت از داده‌های شخصی افراد در اتحادیه اروپا و منطقه اقتصادی اروپا ایجاد شده است.در مقابل، ایالات متحده فاقد یک قانون جامع فدرال برای حفاظت از داده‌های شخصی است و به مجموعه‌ای از قوانین بخشی و مقررات ایالتی متکی است. از جمله این قوانین می‌توان به قانون حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) و قانون قابلیت حمل و پاسخگویی بیمه سلامت (HIPAA[1]) اشاره کرد. هر دو چارچوب مقرراتی، اصول شفافیت، رضایت و اطلاع‌رسانی را در خود جای داده‌اند، اما تفاوت‌هایی در مکانیزم‌های اجرایی و جریمه‌ها دارند GDPR .با جریمه‌های سنگین برای عدم تطابق، تأکید بیشتری بر حفظ حریم خصوصی دارد، در حالی که سیستم ایالات متحده با تمرکز بر قوانین بخشی و عدم وجود یک قانون جامع، به تفاوت‌های عمده‌ای در نحوه حفاظت از داده‌ها منجر شده است.(Bradford et al2020)

نیاز به قوانین جامع و کارآمد برای حفاظت از داده‌های شخصی در ایران بیش از هر زمان دیگری احساس می‌شود. پژوهش حاضر قصد دارد از طریق بررسی و تحلیل مقایسه‌ای، نقاط قوت، نقاط ضعف و تفاوت‌ها و شباهت‌های موجود بین مقررات GDPR اتحادیه اروپا و قوانین حفاظت از داده‌ها در ایالات متحده، پیشنهاداتی به سیاست‌گذاران و قانون‌گذاران ارائه دهد تا بر اساس تحلیل‌های انجام شده، چارچوب‌های مناسبی برای بهبود قوانین حفاظت از داده‌های شخصی در ایران تدوین کنند.بدین ترتیب سئوالات تحقیق عبارتند از

۱. مقررات GDPR اتحادیه اروپا و قوانین حفاظت از داده‌های ایالات متحده چه تفاوت‌ها و شباهت‌هایی دارند؟
۲. پیامدهای اجرای مقررات GDPR و قوانین ایالات متحده برای کسب‌وکارها و حریم خصوصی افراد چیست؟
۳. کدام نقاط قوت و ضعف در هر یک از این سیستم‌های قانونی وجود دارد؟
۴. چه پیشنهاداتی می‌توان برای بهبود قوانین حفاظت از داده‌ها در ایران ارائه داد؟

پیشینهٔ پژوهش

۱ .پیشینه نظری

در دهه‌های اخیر، حفاظت از داده‌های شخصی به یکی از مهم‌ترین موضوعات حقوقی و اجتماعی در جهان تبدیل شده است. با گسترش استفاده از اینترنت و فناوری‌های اطلاعاتی، حجم زیادی از داده‌های شخصی جمع‌آوری و پردازش می‌شود که این امر نیاز به قوانینی برای حفاظت از حریم خصوصی افراد را بیش از پیش ضروری کرده است. قوانین حفاظت از داده‌های شخصی به منظور جلوگیری از سوء استفاده و نقض حریم خصوصی افراد و همچنین افزایش اعتماد عمومی به سیستم‌های اطلاعاتی و ارتباطی وضع شده‌اند. در حالی که GDPR اتحادیه اروپا رویکردی جامع و مبتنی بر حقوق را اولویت می‌دهد، ایالات متحده مدل بخش‌بندی شده‌ای با مقررات مختلف در سطح فدرال و ایالتی، مانند HIPAA وCCPA [2]، به کار می‌گیرد. این مرور بر اهمیت رضایت، حقوق فردی، اطلاع‌رسانی در صورت نقض داده‌ها و سازوکارهای اجرایی در هر دو چارچوب قانونی تأکید کرده است.

[1]. Health Insurance Portability and Accountability Act

[2] . California Consumer Privacy Act

مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا نمایانگر تکاملی بزرگ در حفاظت از داده‌ها در این منطقه است. این مقررات جایگزین دستورالعمل حفاظت از داده‌های ۱۹۹۵ شد و هدف آن به‌روزرسانی و هماهنگ‌سازی قوانین حفاظت از داده‌ها در کشورهای عضو اتحادیه اروپا بود. مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا بر اصول اساسی بنا شده است که رویکرد جامع آن به حفاظت از داده‌ها را زیر بنایی می‌کنند. (Stalla-Bourdillon, et al, 2020)

این مقررات به افراد حقوق صریحی نسبت به داده‌هایشان اعطا می‌کند، از جمله حق آگاهی، حق دسترسی، حق تصحیح و حق حذف داده‌ها. کنترل‌کنندگان داده ملزم به رعایت اصول قانونی بودن، انصاف و شفافیت هستند. علاوه بر این، این مقررات مفهوم حفاظت از داده‌ها با طراحی و به‌طور پیش‌فرض را معرفی می‌کند، که سازمان‌ها را تشویق می‌کند تا ملاحظات حریم خصوصی را از ابتدا در فرآیندهای خود قرار دهند.

در ایالات متحده، مقررات حفظ حریم خصوصی داده‌ها چندوجهی، اغلب بخش‌محور و در هر دو سطح فدرال و ایالتی وضع می‌شوند. قانون حمل‌ونقل و مسئولیت‌پذیری بیمه سلامت (HIPAA) یک قانون فدرال است که به‌طور خاص به حریم خصوصی و امنیت اطلاعات سلامت می‌پردازد HIPAA .استانداردهایی را برای حفاظت از داده‌های سلامت حساس تعیین می‌کند و اطمینان حاصل می‌کند که این داده‌ها محرمانه، یکپارچه و در دسترس باقی می‌مانند. این قانون برای نهادهای تحت پوشش مانند ارائه‌دهندگان خدمات سلامت، طرح‌های سلامت و مراکز پردازش اطلاعات سلامت اعمال می‌شود.

(Krzyzanowski & Manson, 2022; Moore & Frye, 2019; Oakley, 2023)

قانون قابل توجه دیگری در سطح ایالتی قانون حفظ حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) است که در سال ۲۰۲۰ اجرایی شد CCPA .به ساکنان کالیفرنیا حقوق خاصی نسبت به اطلاعات شخصی خود اعطا می‌کند، از جمله حق آگاهی از اطلاعات جمع‌آوری شده، حق انصراف از فروش داده‌ها و حق درخواست حذف اطلاعات. در حالی که CCPA مخصوص کالیفرنیا است، تأثیر آن فراتر از مرزهای ایالتی است و اغلب بر گفتگوهای ملی در مورد قانون جامع فدرال حفظ حریم خصوصی تأثیر می‌گذارد. علاوه بر HIPAA وCCPA ، قوانین فدرال مختلف دیگری مانند قانون حفاظت از حریم خصوصی کودکان در اینترنت (COPPA[1])و قانون (GLBA[2]) به جنبه‌های خاصی از حفظ حریم خصوصی داده‌ها در ایالات متحده می‌پردازند. ایالت‌ها نیز به طور فزاینده‌ای قوانین حفظ حریم خصوصی خود را تصویب می‌کنند، و یک شبکه پیچیده از مقررات را ایجاد می‌کنند که سازمان‌ها باید در آن‌ها پیمایش کنند.(Harding et al., 2019; Putman, 2020)

در نتیجه، مروری بر قوانین حفظ حریم خصوصی داده‌ها به وضوح نشان می‌دهد که مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا رویکرد یکپارچه و گسترده‌ای دارد، در حالی که ایالات متحده دارای چشم‌اندازی متنوع، بخش‌محور و ایالتی است. از آنجا که تعاملات دیجیتال از مرزهای جغرافیایی فراتر می‌رود، درک و پیمایش این مقررات برای سازمان‌ها و افراد حیاتی می‌شود. بخش‌های بعدی این مرور مقایسه‌ای به جزئیات بیشتری از تفاوت‌ها، چالش‌ها و پیامدهای این چارچوب‌های حفظ حریم خصوصی داده‌ها می‌پردازد.

۲ .پیشینه تجربی

اصول و چارچوب‌ها: در حوزه حریم خصوصی داده‌ها، اصول پایه و اساس بر روی آن چارچوب‌های قانونی قوی ساخته می‌شوند. یک مرور مقایسه‌ای از مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (EU GDPR) و مقررات حریم خصوصی داده‌ها در ایالات متحده اهداف مشترکی را با تفاوت‌های ظریف در اصول راهنمای خود نشان می‌دهد. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا بر اصل پردازش داده‌های شخصی به صورت قانونی، اطمینان از عدالت و حفظ شفافیت تأکید می‌کند. سازمان‌ها موظفند افراد

[1] . Children's Online Privacy Protection Act

[2] . Gramm-Leach-Bliley Act

را در مورد پردازش داده‌هایشان مطلع کنند و اطمینان حاصل کنند که اهداف و مبنای قانونی برای چنین پردازشی واضح است. پردازش داده‌ها تحت مقررات عمومی حفاظت از داده‌های اتحادیه اروپا باید به اصل محدودیت هدف پایبند باشد. داده‌های شخصی باید برای اهداف مشخص، صریح و قانونی جمع‌آوری شوند و پردازش‌های بعدی باید با این اهداف اولیه هماهنگ باشند. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا توصیه به حداقل‌سازی داده‌ها دارد و سازمان‌ها را ترغیب می‌کند که فقط داده‌های لازم برای هدف مورد نظر را جمع‌آوری کنند. این اصل با مفهوم حریم خصوصی از ابتدا هماهنگ است و جمع‌آوری داده‌های غیرضروری را منع می‌کند. سازمان‌ها موظفند صحت داده‌های شخصی را که پردازش می‌کنند تضمین کنند. باید تدابیری برای اصلاح سریع نادرستی‌ها اتخاذ شود تا از قابلیت اطمینان اطلاعات حمایت شود. داده‌های شخصی نباید بیشتر از مدت زمان لازم برای اهدافی که پردازش می‌شوند ذخیره شوند. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا معرفی بازه‌های زمانی خاص برای نگهداری داده‌ها، مفهوم محدودیت نگهداری را ارتقا می‌دهد. یکپارچگی و محرمانه بودن داده‌های شخصی بسیار مهم است. سازمان‌ها باید تدابیر فنی و سازمانی مناسبی برای محافظت در برابر دسترسی غیرمجاز، تغییر یا افشای داده‌ها اعمال کنند. یکی از اصول اصلی مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، مسئولیت‌پذیری است که نیازمند این است که سازمان‌ها مطابقت با اصول این مقررات را نشان دهند. این شامل نگهداری سوابق دقیق از فعالیت‌های پردازش داده‌ها و انجام ارزیابی‌های تاثیر حفاظت از داده‌ها در صورت لزوم است.

۳ .مدل مفهومی

مدل مفهومی این پژوهش به بررسی و مقایسه چارچوب‌های قانونی حفاظت از داده‌ها در اتحادیه اروپا و ایالات متحده می‌پردازد. این مدل بر روی اصول اساسی هر دو چارچوب مانند شفافیت، رضایت، حقوق دسترسی کاربران، و اجرای قوانین تمرکز دارد. همچنین به تحلیل تأثیرات اجرای این قوانین بر کسب‌وکارها و کاربران، و شناسایی چالش‌ها و فرصت‌های پیش‌روی سازمان‌ها در تطابق با این مقررات می‌پردازد. هدف این مدل ارائه یک چارچوب تحلیلی برای مقایسه تطبیقی قوانین حفاظت از داده‌ها و بررسی امکان‌پذیری اجرای مشابه این قوانین در دیگر کشورها، به ویژه ایران است.

در ایالات متحده، اصل اطلاع و رضایت حاکم است که به موجب آن افراد حق دارند درباره شیوه‌های داده‌ای یک سازمان اطلاع پیدا کنند و قبل از جمع‌آوری، پردازش یا اشتراک داده‌هایشان، رضایت دهند. مشابه مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، چارچوب حریم خصوصی داده‌های ایالات متحده نیز بر محدودیت پردازش داده‌ها برای اهدافی که ابتدا جمع‌آوری شده‌اند تأکید می‌کند. این امر با هدف کلی اطمینان از عدالت و جلوگیری از استفاده‌های غیرمنتظره از اطلاعات شخصی هماهنگ است. اصول حداقل‌سازی داده‌ها سازمان‌ها را راهنمایی می‌کند که فقط اطلاعات لازم برای هدف مورد نظر را جمع‌آوری کنند، که این کار خطر دسترسی غیرمجاز و استفاده نادرست احتمالی را کاهش می‌دهد. ایالات متحده تمرکز زیادی بر اجرای تدابیر امنیتی برای محافظت از داده‌های شخصی در برابر دسترسی، افشا، تغییر و نابودی غیرمجاز دارد.

- **مبنای قانونی و رضایت[1]**

قوانین حفظ حریم خصوصی داده‌ها نقش اساسی در محافظت از اطلاعات شخصی افراد در عصر دیجیتال دارند. یکی از جنبه‌های مهم این مقررات مربوط به کسب رضایت برای پردازش داده‌های شخصی است. این بررسی مقایسه‌ای به مبنای قانونی و نیازهای رضایت در چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (EU GDPR) و مقررات مختلف حفظ حریم خصوصی داده‌ها در ایالات متحده می‌پردازد. تحتEU GDPR ، رضایت یک مبنای قانونی برای پردازش داده‌های شخصی است. این مقررات بین رضایت صریح و ضمنی تمایز قائل می شود.

[1] . Legal basis and consent

رضایت صریح نیازمند اقدام تأییدی واضح از سوی موضوع داده است، مانند علامت زدن یک جعبه یا تأیید فعال یک انتخاب. رضایت ضمنی از سوی دیگر، دقیق‌تر است و می‌تواند از اقدامات یا رفتار فرد استنتاج شود. یکی از ویژگی‌های مهم EU GDPR تأکید بر کنترل افراد بر داده‌های خودشان است. این مقررات به موضوعات داده‌ها حق می‌دهد که در هر زمان رضایت خود را پس بگیرند. این بدان معناست که افراد این قدرت را دارند که نظر خود را در مورد استفاده از داده‌هایشان تغییر دهند و سازمان‌ها باید بدون ضرر برای موضوع داده، به پس گرفتن رضایت احترام بگذارند و آن را تسهیل کنند.

ایالات متحده فاقد قانون جامع فدرال حفظ حریم خصوصی داده‌ها مشابه با EU GDPR است. در عوض، مقررات حفظ حریم خصوصی داده‌ها مجموعه‌ای از قوانین فدرال و ایالتی است. نیازهای رضایت می‌تواند به طور قابل توجهی متفاوت باشد. به عنوان مثال، قانون قابلیت انتقال و مسئولیت بیمه سلامت (HIPAA) در بخش مراقبت‌های بهداشتی نیازهای خاصی برای رضایت در استفاده و افشای اطلاعات سلامت محافظت شده تحمیل می‌کند. در مراقبت‌های بهداشتی، مفهوم رضایت به دقت در مقرراتی مانند HIPAA بافته شده است. بیماران باید رضایت آگاهانه را قبل از استفاده یا افشای اطلاعات سلامت خود ارائه دهند. این به درمان، پرداخت و عملیات مراقبت‌های بهداشتی گسترش می‌یابد. طبیعت دقیق و وابسته به زمینه رضایت در ایالات متحده نشان‌دهنده طبیعت بخشی و پراکنده قوانین حفظ حریم خصوصی داده‌ها در این کشور است.

- **حق افراد و کنترل[1]:**

حفظ حقوق افراد در عصر دیجیتال از اصول اساسی قوانین حریم خصوصی داده‌ها در سراسر جهان است. این بررسی مقایسه‌ای به بررسی حقوق داده‌موضوع‌ها تحت مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) و چشم‌انداز متنوع قوانین حریم خصوصی داده‌ها در ایالات متحده می‌پردازد..(Hartzog & Richards, 2020; Rustad & Koenig, 2019)

به افراد حق دسترسی به داده‌های شخصی‌شان را می‌دهد و تضمین می‌کند که آنها می‌توانند از قانونی بودن پردازش مطلع شوند و آن را تایید کنند. ایالات متحده فاقد یک قانون جامع فدرال حریم خصوصی داده‌ها است. در عوض، قوانین بخشی و مقررات سطح ایالتی مختلف، یک مجموعه‌ای از حقوق برای افراد فراهم می‌کنند. به عنوان مثال، قانون حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) به مصرف‌کنندگان کالیفرنیا حقوقی مانند حق دسترسی و حق حذف می‌دهد. در حالی که حقوق خاص ممکن است متفاوت باشند، یک موضوع مشترک در مقررات حریم خصوصی داده‌های ایالات متحده تأکید بر شفافیت و کنترل است. افراد اغلب حق دارند بدانند که چه اطلاعات شخصی جمع‌آوری می‌شود و چگونه استفاده می‌شود. بسیاری از قوانین نیز به آنها امکان می‌دهند از برخی فعالیت‌های پردازش داده‌ها انصراف دهند. (Béland et al., 2020; Pernot-Leplay, 2020)

- **اعلام نقض داده[2]:**

در چشم‌انداز سریع دیجیتال، نقض داده‌ها تهدیدات قابل توجهی برای حریم خصوصی و امنیت افراد به همراه دارد. این بررسی تطبیقی الزامات اعلام نقض داده‌ها را تحت مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (EU GDPR) و چارچوب‌های متنوع مقررات نقض داده‌ها در ایالات متحده بررسی می‌کند. طبق GDPR اتحادیه اروپا، سازمان‌ها موظف‌اند بدون تأخیر غیرضروری و در صورت امکان، ظرف ۷۲ ساعت پس از آگاهی از نقض، به مرجع نظارتی مربوطه اطلاع دهند. این اطلاع‌رسانی باید شامل جزئیاتی مانند ماهیت نقض، پیامدهای احتمالی و اقدامات انجام‌شده یا پیشنهادی برای رفع آن باشد.

(Kambourakis, Neisse, & Nai-Fovino, 2021; Victor-Mgbachi, 2024)

.در داخل، سازمان‌ها موظف‌اند تمامی نقض‌های داده‌ها را مستند کنند، صرف‌نظر از اینکه آیا نیاز به اطلاع‌رسانی دارند یا خیر. این مستندسازی، شفافیت و مسئولیت‌پذیری در برخورد با نقض‌های داده‌ها را تضمین می‌کند. در برخی موارد، اگر نقض داده‌ها به

[1] . Individuals' Rights and Control

[2] . Data Breach Notification

احتمال زیاد منجر به ریسک بالایی برای حقوق و آزادی‌های افراد شود، سازمان‌ها باید همچنین نقض را به افراد داده‌متأثر شده بدون تأخیر غیرضروری اطلاع دهند. این اطلاع‌رسانی باید اطلاعات واضح و قابل فهمی درباره ماهیت نقض و اقدامات توصیه‌شده برای کاهش ریسک‌های احتمالی به افراد ارائه دهد. به‌طور هم‌زمان، سازمان‌ها باید در طول فرآیند بررسی و پاسخگویی با مرجع نظارتی همکاری کنند. ارتباط شفاف برای ایجاد اعتماد و اطمینان از اطلاع‌رسانی سریع به هر دو مرجع و افراد داده‌متأثر اهمیت دارد. برخلاف رویکرد یکپارچه GDPR اتحادیه اروپا، ایالات متحده فاقد یک قانون فدرال اطلاع‌رسانی نقض داده‌ها است. به جای آن، هر ایالت مجموعه‌ای از مقررات خود را دارد که منجر به چشم‌اندازی پیچیده و پراکنده می‌شود. ایالت‌هایی مانند کالیفرنیا، با قانون حفظ حریم خصوصی مصرف‌کننده کالیفرنیا(CCPA) ، الزامات خاصی برای اطلاع‌رسانی نقض داده‌ها دارند، از جمله اطلاع‌رسانی به افراد داده‌متأثر بدون تأخیر غیرضروری. برخی صنایع در ایالات متحده، مانند بهداشت و درمان، مشمول الزامات فدرال اطلاع‌رسانی نقض داده‌ها هستند. برای مثال، قانون قابل حملیت و پاسخگویی بیمه سلامت (HIPAA) مؤسسات تحت پوشش را موظف می‌کند که به افراد داده‌متأثر، وزارت بهداشت و خدمات انسانی(HHS) ، و در برخی موارد، رسانه‌ها پس از کشف نقض اطلاع دهند. (Harding et al,۲۰۲۱)

نبود یک قانون فدرال اطلاع‌رسانی نقض داده‌ها در ایالات متحده منجر به چالش‌هایی در هماهنگی شده است. تلاش‌هایی در جریان است تا قانونی فدرال ایجاد شود که بتواند رویکرد استانداردی ایجاد کند و انطباق را برای کسب‌وکارهایی که در سراسر ایالات فعالیت می‌کنند، ساده‌تر کند. سازمان‌های دارای عملیات جهانی با چالش پیمایش الزامات متنوع اطلاع‌رسانی مواجه هستند. دستیابی به انطباق نیازمند درک جامع قوانین قابل اجرا و یک استراتژی پاسخگویی متناسب است. در حالی که GDPR اتحادیه اروپا به عنوان معیاری برای اطلاع‌رسانی سریع و شفاف نقض داده‌ها عمل می‌کند، ایالات متحده با یک سیستم غیرمتمرکز مواجه است. تلاش‌های جاری برای ایجاد قانون فدرال در ایالات متحده فرصتی برای ایجاد شیوه‌های اطلاع‌رسانی نقض داده‌ها به صورت یکپارچه و مداوم‌تر فراهم می‌کند، که با فشار جهانی برای مقررات قوی حریم خصوصی همگام می‌شود.

(۲۰۲۲; Winter & Davidson, ۲۰۱۹; Voss, ۲۰۲۱Vlahou, et. al.,)

اجرای قوانین و جریمه‌ها[1]

قوانین حفظ حریم خصوصی داده‌ها نقش محوری در حفاظت از اطلاعات شخصی افراد در عصر دیجیتال ایفا می‌کنند. این مرور تطبیقی به بررسی مکانیزم‌های اجرای قوانین و جریمه‌ها تحت مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (EU GDPR) و چشم‌انداز متنوع قوانین حفظ حریم خصوصی داده‌ها در ایالات متحده می‌پردازد EU GDPR .به مقامات نظارتی قدرت می‌دهد تا جریمه‌های قابل توجهی را به سازمان‌هایی که مفاد آن را نقض می‌کنند تحمیل کنند. دو سطح جریمه مشخص شده است: سطح پایین‌تر، با جریمه‌های تا ۱۰ میلیون یورو یا ۲درصد از گردش مالی سالانه جهانی، و سطح بالاتر، با جریمه‌های تا ۲۰ میلیون یورو یا ۴درصد از گردش مالی سالانه جهانی، هرکدام که بیشتر باشد. این جریمه‌ها متناسب با شدت تخلف هستند و بر اهمیت رعایت مقررات تأکید دارند. به طور خاص، جریمه‌ها می‌توانند برای انواع مختلفی از نقض‌ها، از جمله اقدامات ناکافی حفاظت از داده‌ها، عدم شفافیت، و عدم رعایت حقوق موضوع داده‌ها اعمال شوند. مقامات نظارتی در هر کشور عضو اتحادیه اروپا مسئول اجرای GDPRهستند. آن‌ها دارای قدرت‌های تحقیقی و اصلاحی هستند، از جمله قدرت انجام بازرسی‌ها، صدور هشدارها، دستورالعمل‌های رعایت مقررات، و تحمیل جریمه‌ها. طبیعت تعاملی مقامات نظارتی، اجازه می‌دهد تا اجرای قوانین به طور مداوم در سراسر اتحادیه اروپا انجام شود. ایالات متحده فاقد یک قانون جامع فدرال برای حفظ حریم خصوصی داده‌ها است که منجر به یک مجموعه قوانین پیچیده در سطح ایالتی می‌شود. با این حال، صنایع خاصی مانند بهداشت و درمان تحت قوانین فدرالی مانند قانون حمل‌ونقل و مسئولیت‌پذیری بیمه سلامت (HIPAA) قرار دارند. اجرای این قوانین معمولاً تحت نظارت سازمان‌های فدرال،

[1] . Enforcement of Laws and Penalties

مانند وزارت بهداشت و خدمات انسانی (HHS) برای نقض‌های HIPAA است. در سطح ایالتی، چشم‌انداز اجرای قوانین متفاوت است. ایالاتی مانند کالیفرنیا با قانون حفظ حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) اجازه اجرای عمومی و خصوصی را می‌دهند، که به افراد و دادستان کل ایالت اجازه می‌دهد تا علیه نهادهای ناپایدار اقدام قانونی کنند. جریمه‌ها برای عدم رعایت قوانین حفظ حریم خصوصی داده‌ها در ایالات متحده می‌توانند شامل مجموعه‌ای از پیامدها باشند. در حوزه بهداشت و درمان، نقض‌های HIPAA ممکن است منجر به جریمه‌های مدنی و کیفری، از جمله جریمه‌های مالی و حبس شوند. قوانین ایالتی، مانند CCPA، جریمه‌هایی برای برخی از نقض‌ها و تخلفات تعیین می‌کنند. عدم وجود یک قانون جامع فدرال برای حفظ حریم خصوصی داده‌ها در ایالات متحده منجر به چالش‌هایی در دستیابی به انسجام و شفافیت در اجرای قوانین شده است. درخواست‌ها برای قانون‌گذاری فدرال هدف ایجاد یک چارچوب یکپارچه برای اجرای قوی‌تر و یکنواخت‌تر را دارند.

- **تأثیر جهانی و دامنه برون‌مرزی[1]**

چشم‌انداز قوانین حریم خصوصی داده‌ها بخش جدایی‌ناپذیر از اکوسیستم دیجیتال جهانی است و مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (EU GDPR) و مقررات حریم خصوصی داده‌های ایالات متحده نقش‌های محوری ایفا می‌کنند. این بررسی مقایسه‌ای به بررسی پیامدهای جهانی و دامنه برون‌مرزی این مقررات می‌پردازد و تأثیر آنها بر کسب و کارهای بین‌المللی و چالش‌هایی که شرکت‌های چندملیتی با آن مواجه هستند را روشن می‌کند. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، علیرغم منشأ آن در اتحادیه اروپا، تأثیر خود را فراتر از مرزهای کشورهای عضو گسترش می‌دهد. هر سازمانی که داده‌های شخصی ساکنان اتحادیه اروپا را پردازش می‌کند، صرف نظر از مکان فیزیکی آن، موظف به رعایت این مقررات است. این امر پیامدهای عمیقی برای کسب و کارهای بین‌المللی که عملیات انجام می‌دهند یا خدمات به شهروندان اتحادیه اروپا ارائه می‌دهند، دارد (Alic, ۲۰۲۱, Daniel, ۲۰۲۲, de Bruin, ۲۰۲۲). بر خلاف GDPR ، ایالات متحده فاقد قانون جامع فدرال حفاظت از داده‌ها با قابلیت کاربرد جهانی است. با این حال، مقررات خاصی مانند قانون حفظ حریم خصوصی مصرف‌کنندگان کالیفرنیا (CCPA) و قوانین خاص بخش‌ها مانند قانون حمل‌ونقل و مسئولیت بیمه سلامت (HIPAA) دارای دامنه برون‌مرزی هستند. برای مثال، CCPA به کسب و کارهایی خارج از کالیفرنیا اعمال می‌شود اگر آنها اطلاعات شخصی ساکنان کالیفرنیا را پردازش کنند و معیارهای خاصی را برآورده کنند. HIPAA ، یک قانون فدرال، به نهادهای غیر ایالات متحده اعمال می‌شود اگر آنها اطلاعات سلامت محافظت شده افراد ایالات متحده را پردازش کنند.

- **چالش‌ها و نگرانی‌ها:**

یکی از چالش‌های اصلی که کسب‌وکارها با آن مواجه هستند، پیچیدگی فراگیر مقررات حفظ حریم خصوصی داده‌ها است GDPR . اتحادیه اروپا چارچوب جامعی با الزامات سختگیرانه، از جمله حقوق افراد، اطلاع‌رسانی‌های اجباری نقض داده‌ها، و اصول کمینه‌سازی داده‌ها تعیین می‌کند. در ایالات متحده، عدم وجود قانون فدرال یکپارچه منجر به موزاییکی از مقررات ایالتی و بخش‌محور مانند قانون حفظ حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) و قانون قابل‌انتقالی و پاسخگویی بیمه سلامت (HIPAA) می‌شود. پیمایش در این ساختار پیچیده نیازمند درک دقیق از چارچوب‌های قانونی مختلف است.

- **روندها و تحولات آینده[2]**

چشم‌انداز قوانین حریم خصوصی داده‌ها در حال تغییر مداوم است و با توجه به چالش‌های نوظهور در عصر دیجیتال، قوانین به طور پیوسته سازگار می‌شوند.

---

[1] . Global Impact and Extraterritorial Scope
[2] . Trends and Future Developments

این مرور مقایسه‌ای به بررسی روندها و تحولات آینده در قوانین حریم خصوصی داده‌ها، با تمرکز بر مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (EU GDPR) و قوانین حریم خصوصی داده‌ها در ایالات متحده می‌پردازد. آینده به سمت تقویت استانداردهای حفاظت از داده‌ها در سطح جهانی حرکت می‌کند EU GDPR .با چارچوب قوی خود، یک نمونه از قانون‌گذاری جامع حفاظت از داده‌ها را تعیین کرده است. سایر حوزه‌های قضایی که از اصول GDPR الهام گرفته‌اند، احتمالاً قوانین خود را برای ارائه حفاظت قوی‌تر برای اطلاعات شخصی افراد تصویب یا تقویت خواهند کرد. این تحول نشان‌دهنده شناخت فزاینده اهمیت حریم خصوصی در عصر دیجیتال است. با افزایش آگاهی در مورد حریم خصوصی داده‌ها، انتظار می‌رود که حقوق افراد مورد حمایت قوانین حریم خصوصی داده‌ها گسترش یابد. قوانین آینده ممکن است حقوق جدیدی برای موضوعات داده معرفی کنند یا حقوق موجود را تقویت کنند. حق کنترل داده‌های خود و توانایی نگه داشتن سازمان‌ها در قبال استفاده از آن‌ها احتمالاً نقاط کانونی در تحول حقوق افراد در قوانین حریم خصوصی داده‌ها خواهد بود. (Wachter & Mittelstadt, ۲۰۲۰Solove & Schwartz, , ۲۰۱۹) سرعت سریع پیشرفت فناوری نیازمند به‌روزرسانی‌های مداوم قوانین موجود است. تغییرات آینده ممکن است به فناوری‌های نوظهوری مانند هوش مصنوعی، بیومتریک و اینترنت اشیا (IoT) پرداخته و اطمینان حاصل کنند که قوانین حریم خصوصی داده‌ها در مواجهه با چشم‌اندازهای دیجیتال در حال تحول، مرتبط و مؤثر باقی بمانند.

روش‌شناسی پژوهش

این پژوهش با بهره‌گیری از یک رویکرد ترکیبی (کیفی و کمی) به بررسی تاثیرات مقررات عمومی حفاظت از داده‌ها (GDPR) بر سازمان‌ها و افراد پرداخته است. برای روش اسنادی و کتابخانه‌ای، از فیش‌برداری کلیدها، کتاب‌ها، مقالات علمی، اسناد و مدارک سازمان‌های رسمی و سایت‌های معتبر اینترنتی استفاده شده است. این مرحله شامل مرور ادبیات موجود در حوزه حفاظت از داده‌ها و مقررات GDPR بود تا چارچوب نظری تحقیق شکل بگیرد .برای گردآوری داده‌های کمی، از روش میدانی با تشکیل پنل‌های خبرگی و تهیه و توزیع پرسشنامه بین صاحب‌نظران خبره در حوزه دفاع سایبری ، حریم خصوصی و زیرساخت‌های حیاتی استفاده شده است.

نمونه‌گیری: ۵۰ نفر از مدیران، کارشناسان ارشد و خبرگان در حوزه‌های مختلف فناوری اطلاعات و حقوق برای مصاحبه انتخاب شدند. این افراد از سازمان‌های مختلف و با تخصص‌های متفاوت بودند تا تنوع دیدگاه‌ها تضمین شود.

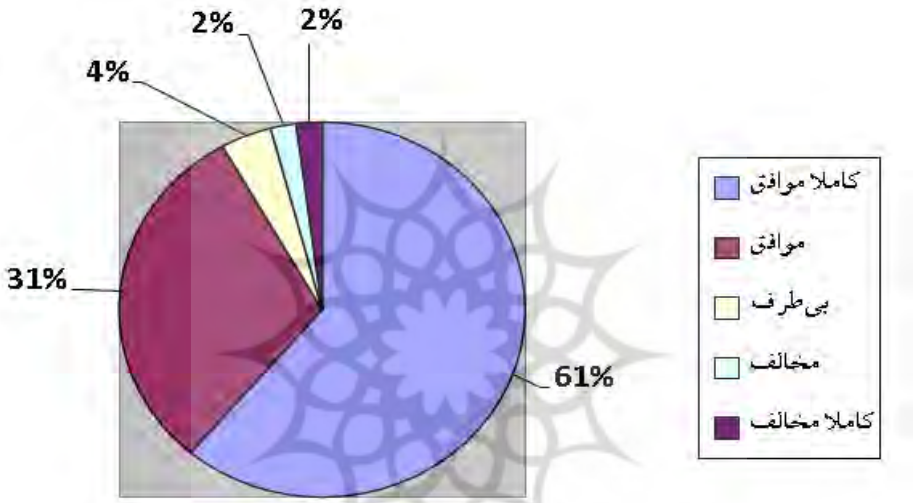
توزیع و جمع‌آوری: ۵۰ پرسشنامه به صورت تصادفی میان کارکنان سازمان‌های مختلف توزیع شد.این پرسشنامه شامل سوالاتی درباره آگاهی از مقررات GDPR و قوانین ایالات متحده، چالش‌های موجود در حفاظت از داده‌ها و نظرات درباره نیاز به تدوین قوانین مشابه در ایران بود.ساختار پرسشنامه: پرسشنامه‌ها شامل سوالات بسته و باز بودند تا علاوه بر داده‌های کمی، داده‌های کیفی نیز جمع‌آوری شود.برای تعمیق تحلیل‌ها، مصاحبه‌های نیمه‌ساختاریافته با ۲۰ نفر از متخصصان در حوزه‌های حقوقی و فناوری اطلاعات انجام شد. این مصاحبه‌ها به منظور جمع‌آوری دیدگاه‌های دقیق‌تر و تجربیات عملی افراد در زمینه حفاظت از داده‌ها بود.

یافته‌های پژوهش

فرآیند مصاحبه: مصاحبه‌ها به صورت نیمه‌ساختاریافته انجام شد، به این معنا که سوالات اصلی مشخص بود اما امکان پرسش سوالات اضافی نیز وجود داشت. این مصاحبه‌ها به طور متوسط ۳۰ تا ۴۵ دقیقه به طول انجامیدند. هدف از این مصاحبه‌ها کسب دیدگاه‌های جامع در مورد ضرورت و امکان‌پذیری ایجاد قانونی جامع و همه‌شمول مانند GDPR در ایران بود. داده‌های جمع‌آوری شده از طریق پرسشنامه‌ها با استفاده از نرم‌افزار SPSS تحلیل شدند. نتایج به دست آمده به شرح زیر می‌باشد:

جدول ۱ نتایج پرسشنامه

سوال	کاملا موافق	موافق	بی طرف	مخالف	کاملا مخالف
ضرورت قانون مشابهGDPR	۳۰	۱۵	۲	۱	۱
قابلیت اجرا	۲۵	۱۸	۵	۱	۰
چالش‌های شناسایی شده	۱۰	۱۵	۲۰	۳	۱
حمایت از نهادهای ذینفع	۲۸	۱۷	۲	۱	۱



نمودار نتایج نظرسنجی ۱

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

جدول ۲توزیع جمعیتی پاسخ‌دهندگان به مصاحبه‌ها را بر اساس جنسیت و میزان تحصیلات

ویژگی‌ها	تعداد	درصد
جنسیت (مرد)	۳۵	٪۷۰
جنسیت (زن)	۱۵	٪۳۰
تحصیلات (لیسانس)	۱۰	٪۲۰
تحصیلات (فوق لیسانس)	۲۵	٪۵۰
تحصیلات (دکتری)	۱۵	٪۳۰

جدول ۳: نتایج پرسشنامه

سوال	کاملاً موافق	موافق	بی‌طرف	مخالف	کاملاً مخالف
ضرورت قانون مشابهGDPR	۳۰	۱۵	۲	۱	۱
قابلیت اجرا	۲۵	۱۸	۵	۱	۰

چالش‌های شناسایی شده	۱۰	۱۵	۲۰	۳	۱
حمایت از نهادهای ذینفع	۲۸	۱۷	۲	۱	۱

تحلیل همبستگی

تحلیل همبستگی نشان می‌دهد که ضرورت ایجاد قانونی مشابه GDPR به شدت با قابلیت اجرا و حمایت نهادهای ذینفع مرتبط است. همچنین، با افزایش قابلیت اجرای قوانین، چالش‌های بیشتری شناسایی می‌شوند که نیازمند توجه و رفع هستند. این نتایج نشان‌دهنده اهمیت هماهنگی بین نیاز به قوانین جدید، قابلیت اجرای آن‌ها و حمایت نهادهای مرتبط برای بهبود وضعیت حریم خصوصی کاربران است.

جدول ۳ضرایب همبستگی بین چهار متغیر

چهار متغییر اصلی	ضرورت قانون مشابهGDPR	قابلیت اجرا	چالش‌های شناسایی شده	حمایت از نهادهای ذینفع
ضرورت قانون مشابهGDPR	۱.۰۰	۰.۸۵	۰.۴۵	۰.۹۵
قابلیت اجرا	۰.۸۵	۱.۰۰	۰.۶۵	۰.۹۰
چالش‌های شناسایی شده	۰.۴۵	۰.۶۰	۱.۰۰	۰.۵۰
حمایت از نهادهای ذینفع	۰.۹۵	۰.۹۰	۰.۵۰	۱.۰۰

همبستگی پیرسون بین پاسخ‌های مختلف نشان می‌دهد که بالاترین همبستگی بین ضرورت قانون مشابه GDPR و حمایت از نهادهای ذینفع (۰.۹۵) و کمترین همبستگی بین ضرورت قانون مشابه GDPR و چالش‌های شناسایی شده (۰.۴۵) می‌باشد.

تحلیل رگرسیون

نتایج تحلیل رگرسیون نشان می‌دهد که ضرورت قانون مشابهGDPR ، قابلیت اجرا، و حمایت از نهادهای ذینفع تأثیر مثبت و معناداری بر کاهش نقض حریم خصوصی کاربران دارند. این نتایج بر اهمیت اجرای قوانین مناسب، قابلیت اجرایی بودن این قوانین و حمایت نهادهای مرتبط تأکید می‌کنند. هرچند که تأثیر چالش‌های شناسایی شده بر نقض حریم خصوصی منفی است، اما این رابطه از نظر آماری معنادار نیست.نتایج رگرسیون به شرح زیر است:

جدول ۴ نتایج رگرسیون

متغیر	ضریب	مقدارt	P-Value
ثابت(Intercept)	۵.۲۳	۲.۳۴	۰.۰۲
ضرورت قانون مشابهGDPR	۱.۱۵	۳.۱۲	۰.۰۱
قابلیت اجرا	۰.۸۵	۲.۷۵	۰.۰۳
چالش‌های شناسایی شده	۰.۴۵-	۱.۵۴-	۰.۱۳
حمایت از نهادهای ذینفع	۱.۰۲	۳.۴۵	۰.۰۰۵

این نتایج نشان می‌دهد که متغیرهای "ضرورت قانون مشابه"GDPR ، "قابلیت اجرا" و "حمایت از نهادهای ذینفع" همبستگی مثبتی با متغیر وابسته دارند و مقدار P-Value آن‌ها نیز کمتر از ۰.۰۵ است که نشان می‌دهد این متغیرها به طور معناداری بر پاسخ‌ها تأثیر می‌گذارند. اما متغیر "چالش‌های شناسایی شده" همبستگی منفی و غیر معناداری با پاسخ‌ها دارد.

یافته‌های کیفی:

مصاحبه‌های نیمه‌ساختاریافته نشان داد که کارشناسان و مدیران ارشد به طور کلی به ضرورت تدوین قوانین جامع و یکپارچه برای حفاظت از داده‌ها در ایران باور دارند. همچنین، چالش‌های اصلی شامل کمبود منابع انسانی متخصص و نبود هماهنگی کافی بین نهادهای نظارتی بود.

بحث

تفاوت‌ها و شباهت‌های قوانین حفاظت از داده‌ها در اتحادیه اروپا و ایالات متحده به دقت بررسی شده است. مقررات عمومی حفاظت از داده‌ها (GDPR) در اتحادیه اروپا به عنوان یک چارچوب جامع و یکپارچه عمل می‌کند که تمامی سازمان‌ها را ملزم به رعایت اصول شفافیت، رضایت آگاهانه، و اطلاع‌رسانی می‌کند. این قوانین با اعمال جریمه‌های سنگین برای عدم رعایت، به‌طور مؤثری از داده‌های شخصی محافظت می‌کنند. در نتیجه، کسب‌وکارها در اتحادیه اروپا مجبور به تطبیق با استانداردهای بالای حفاظتی هستند، که این امر به افزایش اعتماد کاربران و مسئولیت‌پذیری سازمان‌ها منجر می‌شود.

در مقابل، ایالات متحده از یک سیستم پراکنده از قوانین بخشی و ایالتی استفاده می‌کند که فاقد یک چارچوب جامع فدرال است. این پراکندگی منجر به پیچیدگی‌های قانونی و اجرایی برای سازمان‌ها شده و همچنین باعث ایجاد تفاوت‌های قابل توجهی در سطح حفاظت از داده‌ها می‌شود. به عنوان مثال، قوانین مانند قانون حمل و نقل و مسئولیت‌پذیری بیمه سلامت (HIPAA) و قانون حفظ حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) نمونه‌هایی از این رویکردهای بخشی هستند. این رویکردها ممکن است در برخی موارد ناکافی باشند، به ویژه در مقایسه با استانداردهای جامع (GDPR).

بررسی های این مقاله نشان می دهد که اتحادیه اروپا توانسته است با ایجاد یک چارچوب قانون‌گذاری یکپارچه، از داده‌های شخصی به نحو بهتری محافظت کند، در حالی که ایالات متحده نیاز به بازنگری و یکپارچه‌سازی قوانین حفاظتی خود دارد. این نتایج می‌تواند به عنوان الگویی برای سایر کشورها، از جمله ایران، در ایجاد و بهبود قوانین حفاظت از داده‌ها مورد استفاده قرار گیرد. توصیه می‌شود که ایران نیز با استفاده از تجربیات موفق کشورهای دیگر، به تدوین یک قانون جامع و یکپارچه برای حفاظت از داده‌ها بپردازد و مکانیسم‌های اجرایی مؤثری را ایجاد کند تا از داده‌های شخصی شهروندان به طور کامل محافظت شود.پیش از ورود به بخش بررسی، ضروری است به نکاتی همچون چالش‌های عملیاتی که شرکت‌ها در تطبیق با GDPR و قوانین پراکنده در ایالات متحده مواجه می‌شوند، توجه شود. همچنین، ارائه نمونه‌های خاص از چالش‌ها یا مشکلاتی که در هر دو سیستم قانونی دیده شده است، می‌تواند به درک بهتر موضوع کمک کند. علاوه بر این، تأکید بر اهمیت آموزش و آگاهی‌بخشی به کاربران و شرکت‌ها درباره حقوق و تعهداتشان در زمینه حفاظت از داده‌ها، از اهمیت ویژه‌ای برخوردار است. این موارد به تعمیق تحلیل و جامعیت بحث کمک می‌کنند.

چالش‌های عملیاتی: بررسی چالش‌های عملیاتی که شرکت‌ها در تطبیق با GDPR و قوانین پراکنده در ایالات متحده مواجه می‌شوند.

مقایسه موردی: آموزش و آگاهی‌بخشی نقش کلیدی در موفقیت هر دو سیستم دارد. در اتحادیه اروپا، **GDPR** به وضوح نیاز به آموزش کاربران و کارکنان در مورد حقوق و تعهداتشان را تأکید می‌کند. این موضوع به افزایش آگاهی عمومی کمک می‌کند و منجر به کاهش نقض‌های داده می‌شود. در ایالات متحده، نبود یک چارچوب جامع فدرال نیازمند تلاش‌های بیشتری در جهت آموزش کاربران و شرکت‌ها است تا تفاوت‌های قوانین ایالتی و بخشی را درک کنند.

نتیجه‌گیری و پیشنهادها

در چشم‌انداز به سرعت در حال تحول عصر دیجیتال، بررسی تطبیقی مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) و مقررات حفظ حریم خصوصی داده‌ها در ایالات متحده اهمیت حیاتی حفظ حریم خصوصی داده‌ها و انطباق با آن را برای کسب‌وکارهای فعال در یک دنیای جهانی‌شده برجسته می‌کند. این بررسی تطبیقی تفاوت‌های جزئی و اصول مشترک بین EU GDPR و مقررات حفظ حریم خصوصی داده‌های ایالات متحده را روشن ساخت این پژوهش نشان می‌دهد که در حالی که اکثر کارشناسان و خبرگان به ضرورت و امکان‌پذیری ایجاد قانونی مشابه GDPR در ایران باور دارند، چالش‌های شناسایی شده باید به دقت مورد بررسی قرار گیرند تا بتوان این قانون را با موفقیت پیاده‌سازی کرد.

پاسخ به سوالات تحقیق

۱. مقررات GDPR اتحادیه اروپا و قوانین حفاظت از داده‌های ایالات متحده چه تفاوت‌ها و شباهت‌هایی دارند؟

مقررات GDPR اتحادیه اروپا یک چارچوب جامع و یکپارچه برای حفاظت از داده‌های شخصی فراهم می‌کند و شامل جریمه‌های سنگین برای عدم تطابق است. این مقررات بر شفافیت، رضایت و اطلاع‌رسانی تأکید دارد. در مقابل، ایالات متحده فاقد یک قانون جامع فدرال است و به مجموعه‌ای از قوانین بخشی و ایالتی متکی است. قوانین ایالات متحده مانند CCPA وHIPAA بر بخش‌های خاصی از داده‌ها متمرکز هستند و جریمه‌های کمتری نسبت به GDPR دارند. (California Legislative Information, 2018; U.S. Department of Health and Human Services, 1996).

۲. پیامدهای اجرای مقررات GDPR و قوانین ایالات متحده برای کسب‌وکارها و حریم خصوصی افراد چیست؟

اجرای GDPR برای کسب‌وکارها در اتحادیه اروپا منجر به افزایش شفافیت و مسئولیت‌پذیری در قبال داده‌های شخصی شده است. کسب‌وکارها ملزم به اجرای اقدامات امنیتی بیشتر و اطلاع‌رسانی به موقع درباره نقض داده‌ها هستند. برای افراد، این مقررات حقوق بیشتری برای کنترل داده‌هایشان فراهم می‌کند (Bradford et al., 2020) در ایالات متحده، کسب‌وکارها باید با مجموعه‌ای از قوانین مختلف ایالتی و بخشی تطابق پیدا کنند که این موضوع می‌تواند پیچیدگی‌های بیشتری ایجاد کند. برای افراد، حفاظت از داده‌ها در برخی بخش‌ها مانند سلامت بهبود یافته است، اما قوانین جامع و یکپارچه‌ای برای همه داده‌ها وجود ندارد. (Greenleaf, 2019)

۳. کدام نقاط قوت و ضعف در هر یک از این سیستم‌های قانونی وجود دارد؟

اجرای GDPR برای کسب‌وکارها در اتحادیه اروپا منجر به افزایش شفافیت و مسئولیت‌پذیری در قبال داده‌های شخصی شده است. کسب‌وکارها ملزم به اجرای اقدامات امنیتی بیشتر و اطلاع‌رسانی به موقع درباره نقض داده‌ها هستند. برای افراد، این مقررات حقوق بیشتری برای کنترل داده‌هایشان فراهم می‌کند. (Bradford et al,2020) در ایالات متحده، کسب‌وکارها باید با مجموعه‌ای از قوانین مختلف ایالتی و بخشی تطابق پیدا کنند که این موضوع می‌تواند پیچیدگی‌های بیشتری ایجاد کند. برای افراد، حفاظت از داده‌ها در برخی بخش‌ها مانند سلامت بهبود یافته است، اما قوانین جامع و یکپارچه‌ای برای همه داده‌ها وجود ندارد. (Greenleaf,2019)

پیشنهاداتی برای بهبود قوانین حفاظت از داده‌ها در ایران

پیشنهادات برای بهبود قوانین حفاظت از داده‌ها در ایران شامل تدوین یک قانون جامع و یکپارچه مشابه GDPR با تأکید بر شفافیت، رضایت و اطلاع‌رسانی، ایجاد مکانیزم‌های اجرایی موثر و جریمه‌های مناسب برای عدم تطابق، و افزایش آگاهی عمومی و آموزش درباره حقوق حفاظت از داده‌ها می‌باشد. همچنین، می‌توان از تجربیات موفق دیگر کشورها بهره‌برداری کرده و قوانین موجود را با نیازهای خاص جامعه و نظام حقوقی ایران تطبیق داد. (Bradford et al., 2020)

پیشنهادات برای بهبود قوانین حفاظت از داده‌ها در ایران

۱. بهبود شفافیت قوانین موجود

قوانین فعلی در ایران به اندازه کافی جامع و شفاف نیستند و این موضوع باعث ایجاد ابهام در اجرای آنها می‌شود. برای رفع این مشکل، لازم است که قوانین موجود بازنگری شوند و به طور کامل و دقیق‌تر تدوین گردند. این بازنگری باید به گونه‌ای باشد که تمامی جوانب حفاظت از داده‌ها را در بر بگیرد و به صراحت نحوه اجرای این قوانین را مشخص کند. مشابه با GDPR، ایران نیاز به یک قانون جامع و یکپارچه برای حفاظت از داده‌های شخصی دارد که تمامی بخش‌ها و صنایع را شامل شود. این قانون باید اصول شفافیت، رضایت، اطلاع‌رسانی و حفاظت از داده‌ها را به‌طور کامل پوشش دهد. قوانین فعلی بازدارندگی کافی ندارند و هزینه ارتکاب جرائم حوزه حریم خصوصی در ایران پایین است، که این مسئله می‌تواند باعث افزایش وقوع جرائم در فضای مجازی شود. عدم بازدارندگی این قوانین در مقایسه با سایر دولت ها، به وضوح نکته‌ای حائز اهمیت را برجسته می‌کند. باعنایت به تاریخ تصویب قانون جرائم رایانه‌ای در ایران که مربوط به حدود۱۵ سال قبل (سال ۱۳۸۸)، این امر نشان می‌دهد که در حالی که قوانین وجود دارند، تطبیق آنها با نیازهای پیشرفته و فن‌آوری‌های جدید امری ضروری و چالش‌برانگیز است، که نیازمند بهبود و به‌روزرسانی مداوم می‌باشد.

۲. تطبیق قوانین با نیازهای خاص جامعه و نظام حقوقی ایران:

قوانین حفاظت از داده‌ها باید با نیازهای خاص جامعه و نظام حقوقی ایران تطبیق داده شود. این شامل توجه به فرهنگ، ساختار اقتصادی و نیازهای اجتماعی و حقوقی کشور است. ایجاد قوانین منعطف که بتوانند به نیازهای جامعه پاسخ دهند، اهمیت دارد.

۳. ایجاد مکانیزم‌های اجرایی موثر

برای اجرای موثر قوانین حفاظت از داده‌ها، نیاز به ایجاد مکانیزم‌های اجرایی قوی و کارآمد است. این مکانیزم‌ها باید شامل نظارت دقیق بر عملکرد کسب‌وکارها، اعمال جریمه‌های مناسب برای عدم تطابق و ایجاد سیستم‌های گزارش‌دهی نقض داده‌ها باشد.

۴. افزایش تعداد منابع انسانی متخصص

یکی از چالش‌های مهمی که در این پژوهش شناسایی شد، کمبود منابع انسانی متخصص در حوزه حفاظت از داده‌ها است. نبود نیروی کار متخصص باعث کاهش کارآیی و اثربخشی اجرای قوانین موجود می‌شود. برای رفع این مشکل، لازم است که برنامه‌های آموزشی و تربیتی مناسب برای آموزش نیروهای متخصص در این حوزه تدوین و اجرا شود.

۵. تقویت هماهنگی بین سازمان‌ها و نهادهای مختلف

یکی دیگر از مشکلات اصلی که پاسخ‌دهندگان مطرح کردند، عدم هماهنگی بین سازمان‌ها و نهادهای مختلف در اجرای قوانین مرتبط با حفاظت از داده‌ها است. این ناهماهنگی منجر به ضعف در اجرای قوانین و حفاظت از داده‌های شخصی می‌شود. برای رفع این مشکل، لازم است که سازوکارهای مناسبی برای هماهنگی بین سازمان‌ها و نهادهای مختلف ایجاد شود.

۶. همکاری بین‌المللی و استفاده از تجربیات موفق سایر کشور ها:

بررسی و مطالعه تجربیات کشورهای دیگر مانند کانادا، استرالیا و ژاپن می‌تواند به شناسایی راهکارهای مناسب برای تدوین و اجرای قوانین مشابه در ایران کمک کند. این بررسی‌ها می‌تواند شامل مطالعه قوانین، بررسی نحوه اجرای آنها و تحلیل نتایج حاصل از اجرای این قوانین باشد.

۷. ایجاد زیرساخت‌های مناسب

ایجاد زیرساخت‌های مناسب شامل فناوری‌های لازم برای حفاظت از داده‌ها، سیستم‌های اطلاعاتی مناسب و سازوکارهای قانونی و نظارتی می‌تواند به بهبود اجرای قوانین و افزایش سطح حفاظت از داده‌های شخصی کمک کند.

۸. مهاجرت واقعی و مجازی نخبگان حوزه فناوری اطلاعات و امنیت اطلاعات به خارج از کشور:

مهاجرت به خارج از کشور نخبگان این حوزه، و حتی رواج پدیده مهاجرت مجازی [1]خبرگان، باعث ایجاد چالش در تأمین منابع انسانی متخصص برای توسعه و پشتیبانی پروژه‌های داخلی می‌گردد.

۹. جزیره‌ای عمل کردن نهادهای متولی و بازیگران حریم خصوصی در فضای سایبری کشور

نهادهایی نظیر وزارت ارتباطات و فناوری اطلاعات، سازمان تنظیم مقررات و ارتباطات رادیویی، سازمان فناوری اطلاعات ایران، شرکت ارتباطات زیرساخت، افتا ریاست جمهوری، پلیس فتا، قرارگاه سایبری، قرارگاه پدافند سایبری کشور و شوراهایی نظیر شورای عالی انقلاب فرهنگی و شورای عالی فضای مجازی، به صورت جزیره‌ای عمل می‌کنند که این مسئله باعث عدم هماهنگی و همگرایی در امور حریم خصوصی و مدیریت بهینه تر فضای سایبری کشور می‌شود

۱۰. آگاهی‌بخشی و آموزش سواد رسانه ایی

افزایش آگاهی عمومی و سواد رسانه ایی شهروندان درباره حقوق حفاظت از داده‌ها و حریم خصوصی آموزش به کسب‌وکارها و افراد درباره نحوه حفاظت از داده‌های شخصی ضروری است. برگزاری دوره‌های آموزشی، کارگاه‌ها و کمپین‌های اطلاع‌رسانی می‌تواند به بهبود وضعیت حفاظت از داده‌ها کمک کند.

۱۱. تقویت نقش نهادهای نظارتی

نهادهای نظارتی و اجرایی در ایران با ایفای نقش‌های کلیدی خود در حوزه مورد پژوهش، می‌توانند به بهبود وضعیت حفاظت از داده‌ها کمک کنند. اما برای دستیابی به این هدف، نیاز به هماهنگی بیشتر بین نهادهای مختلف، تدوین قوانین به روز و جامع، و افزایش آگاهی عمومی درباره اهمیت حفاظت از حریم خصوصی داده‌ها است.در نتیجه، اجرای موفقیت‌آمیز یک قانون جامع و کامل مانند GDPR در ایران نیازمند برنامه‌ریزی دقیق و همه‌جانبه است. توجه به شفافیت قوانین، افزایش تعداد منابع انسانی متخصص، تقویت هماهنگی بین سازمان‌ها و نهادهای مختلف، بررسی تجربیات موفق کشورهای دیگر، ایجاد زیرساخت‌های مناسب و آگاهی‌بخشی و آموزش عمومی می‌تواند به تحقق این هدف کمک کند. نهادهای نظارتی باید قدرت و استقلال کافی برای نظارت بر اجرای قوانین حفاظت از داده‌ها داشته باشند. این نهادها باید بتوانند به‌طور مستقل عملکرد کسب‌وکارها را بررسی کرده و در صورت لزوم، اقدامات قانونی مناسبی را اعمال کنند. این پیشنهادات می‌تواند به بهبود وضعیت حفاظت از داده‌ها در ایران کمک کرده و از نقض حقوق حریم خصوصی افراد جلوگیری کند. اجرای موثر این پیشنهادات نیازمند همکاری و هماهنگی بین نهادهای مختلف دولتی و خصوصی است.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

منابع

حاجی ملا میرزایی، حامد ؛ محمدی، حافظ و سعادتمند، امیر مسعود. (۱۴۰۰). «تبیین نقش فناوری«کلان داده ها»در هوشمندی سامانه های «فرماندهی و کنترل سایبری»و ارائه مدل کاربردی آن.»

حکم و مصوبات شورای عالی فضای مجازی کشور. (۱۳۹۰). مرکز ملی فضای مجازی، صفحات ۱-۵۰.

سند راهبردی نظام جامع فناوری اطلاعات کشور. (۱۳۹۱). شورای عالی فضای مجازی، صفحات ۱-۷۰.

سیاست‌های کلی نظام در حوزه امنیت فضای تولید و تبادل اطلاعات (افتا). (۱۳۹۰). مجمع تشخیص مصلحت نظام، صفحات ۱-۴۰.

شورای عالی فضای مجازی. (۱۴۰۱). مصوبات شورای عالی فضای مجازی کشور. صفحات ۱-۵۰.

[1] مهاجرت مجازی یا مهاجرت الکترونیکی به معنای استفاده از بسترهای آنلاین و تکنولوژی‌های ارتباطی برای کار یا همکاری با شرکت‌ها و سازمان‌های خارجی، بدون نیاز به ترک فیزیکی کشور است. در واقع، متخصصان می‌توانند از داخل کشور، خدمات و مهارت‌های خود را به بازارهای بین‌المللی ارائه دهند و به صورت آنلاین با کارفرمایان و تیم‌های خارجی همکاری کنند.این امر ممکن است به خروج دانش و مهارت‌ها از بازار کار داخلی و کاهش بهره‌وری و توسعه فناوری در کشور منجر شود.

فلاحی، علی. (۱۴۰۰). راهبردهای امنیت داده در سازمان‌های کوچک و متوسط. مجله مدیریت فناوری، دوره ۱۰، شماره ۲، صفحات ۶۰-۷۵.

قانون جرایم رایانه‌ای. (۱۳۸۸). روزنامه رسمی جمهوری اسلامی ایران، شماره ۱۸۸۵۶، صفحات ۱-۱۰.

کامیابی، تراب. (۱۴۰۲). حکمرانی داده در فناوری‌های نوین. مجله فناوری اطلاعات، دوره ۱۱، شماره ۱، صفحات ۷۰-۸۵.

لطیف زاده، مهدیه، قبولی درافشان، سید محمدمهدی، محسنی، سعید و عابدی، محمد (۱۴۰۱ب). تبیین اسباب مشروعیت پردازش دادهی شخصی از منظر حقوق اتحادیه اروپا و ایران. مطالعات حقوقی، ۱۴(۳)، ۳۶۴-۳۲۵.

لطیف زاده، مهدیه، قبولی درافشان، سید محمدمهدی، محسنی، سعید و عابدی، محمد (۱۴۰۰). تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا. پژوهشنامه پردازش و مدیریت اطلاعات، ۳۷(۲)، ۴۷۲-۴۳۹.

لطیف زاده، مهدیه، قبولی درافشان، سید محمدمهدی، محسنی، سعید و عابدی، محمد (۱۴۰۱ الف). شناسایی ماهیت داده شخصی و جست وجوی بستر حقوقی مناسب جهت حمایت از آن در نظام حقوقی ایران. فصل نامه مطالعات فقه و حقوق اسلامی، ۱۴(۲۷)، ۳۹۴-۳۶۱.
https://doi.org/۱۰.۲۲۰۷۵/feqh.۲۰۲۱.۲۲۱۵۳.۲۶۹۶

مجمع تشخیص مصلحت نظام. (۱۴۰۱). سیاست‌های کلی نظام در حوزه امنیت فضای تولید و تبادل اطلاعات. صفحات ۱-۴۰.

وزارت ارتباطات و فناوری اطلاعات. (۱۴۰۱). سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور. صفحات ۱-۶۰.

وزارت ارتباطات و فناوری اطلاعات. (۱۴۰۱). سند فرابخشی دولت الکترونیکی. صفحات ۱-۸۰.

وزارت صنعت، معدن و تجارت. (۱۴۰۱). برنامه جامع توسعه تجارت الکترونیکی کشور. صفحات ۱-۱۰۰.

References

Ahlstrom, D., et al. (2020). Divergence in data privacy standards between the EU GDPR and U.S. regulations

Bakare, Adeniyi, Akpuokwe, & Eneh. (2024). Navigating cybersecurity beyond compliance: understanding your threat landscape and vulnerabilities. Computer Science & IT Research Journal, 5(3), 528-543.

Computer Crimes Law. (2009). Official Gazette of the Islamic Republic of Iran, No. 18856, pp. 1-10. [In Persian]

Cooke, et al. (2019). Harmonizing data protection practices to align with regulations.

Culot, et al. (2019). The patchwork of state and sector-specific regulations in the U.S.

Decrees and resolutions of the Supreme Council of Cyberspace. (2011). National Center for Cyberspace, pp. 1-50. [In Persian]

Esteves, B., & Rodríguez-Doncel, V. (2024). Analysis of ontologies and policy languages to represent information flows in GDPR. Semantic Web, 15(3), 709-743.

Expediency Discernment Council. (2022). General policies of the system in the field of information production and exchange space security, pp. 1-40. [In Persian]

Fallahi, A. (2021). Data security strategies in small and medium-sized enterprises. Technology Management Journal, 10(2), 60-75. [In Persian]

Flyverbom, Deibert & Matten. (2019). Navigating the complex tapestry of data privacy regulations.

Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. Journal of Competition Law & Economics, 16(3), 349-391.

General policies of the system in the field of information production and exchange space security (AFTA). (2011). Expediency Discernment Council, pp. 1-40. [In Persian]

Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology. Computer Law & Security Review, 44, 105640.

Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology. Computer Law & Security Review, 44, 105640.

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? Philosophy & Technology, 35(1), 3-15.

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? Philosophy & Technology, 35(1), 3.

Hamed Haji Molla Mirzaei, Hafez Mohammadi, & Amir Masoud Saadatmand. (2021). Explaining the role of big data technology in the intelligence of cyber command and control systems and providing its practical model. [In Persian]

Harding, E. L., et al. (2019). Understanding the scope and impact of the California Consumer Privacy Act of 2018. Journal of Data Protection & Privacy, 2(3), 234-253.

Harding, E. L., et al. (2022). Understanding the scope and impact of the California Consumer Privacy Act of 2018. Journal of Data Protection & Privacy, 3(2), 234-253.
Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. BCL Review, 61, 1687.
Hartzog, W., & Richards, N. (2022). Privacy's constitutional moment and the limits of data protection. BCL Review, 62, 1687-1705.
Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98.
Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2022). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 29(1), 65-98.
Hu, I. Y. (2019). The Global Diffusion of the 'General Data Protection Regulation' (GDPR). Edited by KH Stapelbroek and S. Grand. Erasmus School of Social and Behavioural Sciences.
Kambourakis, G., Neisse, R., & Nai-Fovino, I. (2021). Information security in the age of EU-Institutions digitalisation, a landscape analysis.
Kambourakis, G., Neisse, R., & Nai-Fovino, I. (2022). Information security in the age of EU-Institutions digitalisation, a landscape analysis. Security Journal, 30(2), 220-240.
Kamyabi, T. (2023). Data governance in modern technologies. Information Technology Journal, 11(1), 70-85. [In Persian]
Klar, R. (2020). Privacy-by-design principles and ethical data practices.
Klar, R. (2022). Privacy-by-design principles and ethical data practices. Data Ethics Journal, 14(1), 30-50.
Krzyzanowski, B., & Manson, S. M. (2022). Twenty years of the health insurance portability and accountability act safe harbor provision: unsolved challenges and ways forward. JMIR Medical Informatics, 10(8), e37756.
Krzyzanowski, B., & Manson, S. M. (2022). Twenty years of the health insurance portability and accountability act safe harbor provision: unsolved challenges and ways forward. JMIR Medical Informatics, 10(8), e37756.
Labadie, C., & Legner, C. (2019, February). Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR. In Proceedings of the 14th International Conference on Wirtschaftsinformatik
Latifzadeh, M., Ghabouli Dorafshan, S. M., Mohseni, S., & Abedi, M. (2022). Explaining the legitimacy of personal data processing from the perspective of the European Union and Iran. Legal Studies, 14(3), 325-364. https://doi.org/10.22099/jls.2022.40620.4390 [In Persian]
Latifzadeh, M., Ghabouli Dorafshan, S. M., Mohseni, S., & Abedi, M. (2021). Analysis of the legal framework for personal data protection in the European Union. Information Processing and Management Research Journal, 37(2), 439-472. [In Persian]
Latifzadeh, M., Ghabouli Dorafshan, S. M., Mohseni, S., & Abedi, M. (2021). Identifying the nature of personal data and seeking an appropriate legal framework to protect it in the Iranian legal system. Islamic Jurisprudence and Law Studies Quarterly, 14(27), 361-394. https://doi.org/10.22075/feqh.2021.22153.2696 [In Persian]
Ministry of Communications and Information Technology. (2022). Cross-sectoral document on e-government, pp. 1-80. [In Persian]
Ministry of Communications and Information Technology. (2022). Strategic document on the security of the country's information production and exchange space, pp. 1-60. [In Persian]
Ministry of Industry, Mines and Trade. (2022). Comprehensive plan for the development of e-commerce in the country, pp. 1-100. [In Persian]
Negri-Ribalta, C., Lombard-Platet, M., & Salinesi, C. (2024). Understanding the GDPR from a requirement engineering perspective—a systematic mapping study on regulatory data protection requirements. Requirements Engineering, 1-27.
Strategic document of the comprehensive national information technology system. (2012). Supreme Council of Cyberspace, pp. 1-70. [In Persian]
Supreme Council of Cyberspace. (2022). Resolutions of the Supreme Council of Cyberspace, pp. 1-50. [In Persian]