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

Conceptualizing Personal Data Protection and Privacy in Cyberspace: A Comparative Study of the United States and European Legal Traditions

Amin shahnaz [1] | Hamid Bahremand [2]✉ | Abbas Sheikholeslami [3] | Mohammad Farajiha [4]

1. PhD Candidate of Criminal Law and Criminology, Department of Law, Mashhad Branch, Islamic Azad University, Mashhad, Iran. Email: amin.shahnaz@iau.ac.ir
2. Corresponding Author, Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law, University of Tehran, Tehran, Iran. Email: Bahremand@ut.ac.ir
3. Associate Professor, Law Department, Mashhad Branch, Islamic Azad University, Mashhad, Iran. Email: Sheikholeslami@mshdiau.ac.ir
4. Associate Professor of Criminal Law and Criminology, Faculty of Law, Tarbiat Modares University, Tehran, Iran. Email:Farajihay@modares.ac.ir

Article Info

Article type:
Research Article

Article history:
Received:1 October 2025
Received in revised form: 5 May 2026
Accepted: 31 May 2026
Published online: 30 July 2026

Keywords:
Cyberspace,
Personal Data Privacy,
Europe,
United States.

ABSTRACT

Objective: This study elucidates the conceptual shift from traditional privacy doctrines to the independent notion of personal data protection within cyberspace. Traditional privacy frameworks - grounded in protection against physical intrusion and rooted in negative rights - prove inadequate in addressing the challenges posed by contemporary surveillance regimes and big data analytics. A comparative examination of the American tradition (characterized by liberal individualism and a negative, non-interventionist approach) and the European tradition (underpinned by human dignity and a positive, regulatory orientation) demonstrates that personal data protection constitutes a fundamental transformation in rights discourse. This evolution carries significant implications for journalism, investigative reporting, and media information management.

Method: This research employs a comparative analytical method, utilizing qualitative content analysis of legislation, judicial precedents, and academic texts from both American and European jurisdictions. The study traces the conceptual transition from location-based privacy to personal data protection in cyberspace through documentary and library-based sources.

Results: The findings reveal a pronounced dichotomy in approaches. The American tradition - grounded in individualism, negative liberty, and state non-intervention - defines privacy through the lens of individual control and the right to be let alone, thereby producing a reactive, fragmented, and inherently limited framework that struggles to counteract the power of technology monopolies. By contrast, the European tradition, anchored in human dignity and the regulatory state, has established a proactive and integrated framework, exemplified by the General Data Protection Regulation (GDPR). This model recognizes affirmative rights - including access, rectification, erasure, and compensation - imposes binding obligations on data processors, and offers a clearer legal basis for reconciling journalistic freedoms with data privacy protections.

Conclusion: This paper ultimately argues that personal data protection has evolved into an independent, affirmative, and third-generation right, complementing and, in many respects, surpassing the negative and defensive right to privacy. The relative success of the European model in balancing individual and collective interests - through the mandates of transparency, accountability, and Privacy by Design - presents a framework that is adaptable, yet requires intelligent localization for developing legal systems, including in the domain of regulating media and journalistic activities. The future of governance in the digital age depends upon embracing this paradigm shift and establishing effective regulatory institutions capable of addressing emerging challenges.

Cite this article: Shahnaz, A; Bahremand, H.: Sheikholeslami, A.& Farajiha, M. (2026), Conceptualizing Personal Data Protection and Privacy in Cyberspace: A Comparative Study of the United States and European Legal Traditions, ***News Science***, 15 (2), 45-49. DOI: http//doi.org/10.22034/lrsi.2026.523001.1365

Publisher: Press Institute for Contemporary International Journalism (PICIJ)

DOI: http//doi.org/10.22034/lrsi.2026.523001.1365

The Journal of *News Science*
Vol. 15, No. 2, Ser.58, summer 2026, P. 45- 49
Journal homepage: https://www.mjourcom.ir/
DOI : http//doi.org/10.22034/lrsi.2026.523001.1365

Open Access

ORIGINAL ARTICLE

Conceptualizing Personal Data Protection and Privacy in Cyberspace: A Comparative Study of the United States and European Legal Traditions

Amin shahnaz [1] | Hamid Bahremand [2]✉ | Abbas Sheikholeslami [3] | Mohammad Farajiha [4]

5. PhD Candidate of Criminal Law and Criminology, Department of Law, Mashhad Branch, Islamic Azad University, Mashhad, Iran. Email: amin.shahnaz@iau.ac.ir
6. Corresponding Author, Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law, University of Tehran, Tehran, Iran. Email: Bahremand@ut.ac.ir
7. Associate Professor, Law Department, Mashhad Branch, Islamic Azad University, Mashhad, Iran. Email: Sheikholeslami@mshdiau.ac.ir
8. Associate Professor of Criminal Law and Criminology, Faculty of Law, Tarbiat Modares University, Tehran, Iran. Email:Farajihay@modares.ac.ir

Received: October 1, 2025 Accepted: May 31, 2026

EXTENDED ABSTRACT

Introduction:

This study seeks to provide an innovative explanation of the paradigmatic shift from traditional privacy to the independent concept of personal data protection in cyberspace. In the contemporary era of data governance, classical privacy doctrines - largely grounded in protection against physical intrusion, secrecy, and negative rights - have become increasingly inadequate in responding to advanced surveillance technologies, algorithmic profiling, and large-scale data processing. Within this context, the research argues that personal data protection can no longer be treated merely as a

subsidiary aspect of privacy, but must be understood as an autonomous legal and normative concept. Through a comparative analysis of two major legal traditions - namely, the American and European models - the study highlights the deeper philosophical and structural differences underlying their approaches. The American tradition, shaped by liberal individualism and a predominantly negative conception of rights, tends to emphasize individual control and limited state intervention. In contrast, the European tradition, grounded in human dignity, social solidarity, and a positive understanding of rights, supports a more active regulatory framework. The findings show that the emergence of personal data protection represents a fundamental transformation in the domain of fundamental rights, with important practical implications for journalism, investigative reporting, and media information governance.

Method:

This research employs a comparative-analytical method, relying on qualitative content analysis of foundational documents, enacted legislation, landmark judicial precedents, and core academic texts from both American and European contexts. The scope focuses on tracing the historical-conceptual evolution from physical, location-based privacy toward personal data protection in the virtual space, and provides an in-depth examination of the philosophical underpinnings, legal implications, and social functions of each tradition. The data collection method is documentary and library-based.

Findings:

The findings reveal a fundamental dichotomy between the American and European approaches to privacy and personal data protection. The American legal tradition, rooted in liberal individualism, negative liberty, and a strong preference for limited state intervention, has historically shaped the concept of privacy around the notions of individual "control" over personal information and the "right to be let alone." As a result, the regulatory landscape in the United States has developed in a largely reactive and fragmented manner, relying on sector-specific laws and judicial interpretations rather than a unified regulatory framework. This structure often limits the state's capacity to effectively confront the growing informational power and monopolistic practices of large technology companies.

In contrast, the European legal tradition is grounded in the principle of human dignity as a foundational value of the social and legal order and accepts a more active role for the state as a regulatory authority. This perspective has facilitated the development of a coherent, integrated, and proactive system of personal data protection, most prominently embodied in the General Data Protection Regulation (GDPR). Within this framework, a range of positive rights - such as the rights of access, rectification, erasure (the right to be forgotten), and compensation - are formally recognized, while substantial legal obligations are imposed on data controllers and processors. Consequently, this model provides a clearer normative and institutional basis for balancing competing interests in sensitive fields such as journalism, where the public's right to information must be carefully reconciled with individuals' rights to privacy and data protection.

Conclusion:

This paper ultimately argues that personal data protection has evolved into an independent, affirmative, and third-generation right that both complements and, in many respects, extends beyond the traditional negative and defensive conception of privacy. While classical privacy

primarily focused on shielding individuals from intrusion or interference, the contemporary framework of data protection introduces proactive legal mechanisms designed to regulate the collection, processing, and circulation of personal information in complex digital environments. In this sense, personal data protection represents a structural transformation in the understanding of fundamental rights in the information age.

Within this context, the European regulatory model has demonstrated a relative degree of success in establishing a more balanced relationship between individual rights and broader societal interests. By embedding principles such as transparency, accountability, and Privacy by Design into legal and institutional frameworks - particularly through instruments like the GDPR - the European approach seeks to ensure that technological innovation and data-driven governance remain compatible with the protection of human dignity and personal autonomy.

However, the study emphasizes that while this model provides a valuable normative and regulatory reference, it cannot be transferred mechanically to other legal systems. For developing legal orders - especially in areas such as media regulation, journalism, and information governance - effective implementation requires thoughtful adaptation and institutional localization. Ultimately, the future of governance in the digital era will depend on recognizing this conceptual shift and establishing effective regulatory institutions capable of safeguarding personal data while maintaining democratic accountability.

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.

References:

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509.

Alfino, M., & Mayes, G. R. (2002). Reconstructing the right to privacy. Social Theory and Practice, 29(1), 4.

Ansari, B. (2014). Rights of privacy (Vol. 15). SAMT Publications. (in Persian)

Ansari, B., Attar, S., Salehi, A. H., & Zand, H. (2022). Comparative study of personal data protection in Europe, America, China, and Iran (pp. 94–108). Sahami Publishing Company. (in Persian)

Attar, S. (2016). The protection of privacy within virtual social networks (p. 41). Khorsandi. (in Persian)

Basu, S. (2012). Privacy protection: A tale of two cultures. Journal of Law & Technology, 6(1), 10.

Blume, P. (2010). Data protection and privacy—basic concepts in a changing world. Scandinavian Studies in Law, 56, 155.

Buttarelli, G., Giakoumopoulos, C., & O'Flaherty, M. (2018). Handbook on European data protection law (p. 57). Publications Office of the European Union.

Carpenter v. United States, 585 U.S. (2018). https://supreme.justia.com/cases/federal/us/585/16-402/

Cofone, I. (2017). The dynamic effect of information privacy law. Minnesota Journal of Law, Science & Technology, 18(2), 519–547.

De L., K. M. M., & Bergstra. (2007). History of privacy. In The history of information security: A comprehensive handbook (1st ed., p. 3). Elsevier.

Dorraji, E., & Barcys, M. (2014). Privacy in digital age: Dead or alive?! Regarding the new EU data protection regulations. Social Technologies, 4(2), 315.
Farhadi Alashti, Z. (2016). Situational prevention of cybercrimes (Strategies and challenges) (p. 13). Mizan. (in Persian)
Ferretti, F. (2014). Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights? Common Market Law Review, 51(3), 855–884.
Gaskin v. Finland, Application No. 001-57491 (1989). https://hudoc.echr.coe.int/tur?i=001-57491
Ghajjar Ghayoonloo, S. (2012). Introduction to cyber law (An approach to the sociology of development law and prerequisites for legislation in cyberspace) (p. 343). Mizan. (in Persian)
Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12 (2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131
Griswold v. Connecticut, 381 U.S. 479 (1965). https://tile.loc.gov/storage-services/service/ll/usrep/usrep381/usrep381479/usrep381479.pdf
Heydari, M. (2019). Manteq-e hemli [Predicate logic] (pp. 64–65). Astan Quds Razavi Publishing and Printing Institute. (in Persian)
Lukacs, A. (2016). What is privacy? The history and definition of privacy. Scandinavian Studies in Law, 56, 257.
Maximillian Schrems v. Data Protection Commissioner [GC], Case C-362/14 (2015). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362
Mohseni, F. (2015). Information privacy (A criminal law study in the laws of Iran, the United States of America, and Imamiyah jurisprudence) (p. 6). Imam Sadiq University (AS). (in Persian)
Mousazadeh, I., & Mostafazadeh, F. (2012). A look at the concept and foundations of the right to privacy in the common law legal system. Public Law Review, 1(2), 57. (in Persian)
Petrucco, F. (2019). The right to privacy and new technologies: Between evolution and decay. Media Law Magazine, 1, 5.
Post, R. C. (2001). Three concepts of privacy. Georgetown Law Journal, 89, 2089–2095.
Purtova, N. (2010). Private law solution in European data protection: Relationship to privacy, and waiver of data protection rights. Netherlands Quarterly of Human Rights, 28(2), 247–265.
Roman Zakharov v. Russia*, Application No. 47143/06 (2015). Police and Human Rights Resources. https://hudoc.echr.coe.int/eng?i=001-159565
Sinha, A. (2022). Social networks and the politics of power (M. Jazini & A. Pasandepour, Trans.). Pileh Publications. (in Persian)
Solove, D. J. (2002). Conceptualizing privacy. California Law Review, 90, 1087–1155.
Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. International Review of Law, Computers & Technology, 28(3), 277–286.

.

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

مفهوم‌سازی حمایت از داده‌های شخصی از حریم خصوصی در فضای سایبر؛ مطالعه تطبیقی آمریکا و سنت حقوقی اروپا

امین شهناز [۱] | حمید بهره مند [۲] ✉ | عباس شیخ الاسلامی [۳] | محمد فرجیها [۴]

۱. دانشجوی دکتری حقوق جزا و جرمشناسی، گروه حقوق، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران.رایانامه:amin.shahnaz@iau.ac.ir
۲. استادیار گروه حقوق جزا و جرم شناسی، دانشکده حقوق، دانشگاه تهران، تهران.ایران (نویسنده مسئول).رایانامه: bahremand@ut.ac.ir
۳. دانشیار گروه حقوق، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران.رایانامه:: sheikholeslami@mshdiau.ac.ir
۴. دانشیار گروه حقوق جزا و جرمشناسی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران.رایانامه: Farajihay@modares.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۷/۹
تاریخ بازنگری: ۱۴۰۵/۲/۱۵
تاریخ پذیرش: ۱۴۰۵/۳/۱۰
تاریخ انتشار: ۱۴۰۵/۵/۸

کلیدواژه‌ها:
حریم خصوصی،
داده های شخصی،
حمایت از داده ها،
اروپا،
آمریکا.

چکیده

هدف: این پژوهش با هدف تبیین گذار پارادایمی از حریم خصوصی سنتی به مفهوم مستقل حمایت از داده‌های شخصی در فضای سایبر انجام شده است.آموزه‌های سنتی حریم خصوصی که بر حفاظت در برابر مداخله فیزیکی و حقوق منفی استوار بودند، در برابر فناوری‌های پیشرفته نظارت و پردازش کلان‌داده ناکارآمد شده‌اند.تطبیق دو سنت حقوقی آمریکا با محوریت فردگرایی لیبرال و رویکرد سلبی و اروپا با محوریت کرامت انسانی، همبستگی اجتماعی و رویکرد ایجابی نشان می‌دهد که تکوین مفهوم مستقل حمایت از داده‌های شخصی ضرورتی اساسی در حقوق بنیادین است.این گذار مفهومی، به‌ویژه در حوزه‌های حساسی مانند علوم خبری، روزنامه‌نگاری تحقیقی و مدیریت اطلاعات رسانه‌ای، کاربردهای عملی گسترده‌ای دارد و نحوه تعادل میان حق‌های متعارض را بازتعریف می‌کند.

روش پژوهش: این پژوهش با رویکرد تطبیقی ـ تحلیلی و با تکیه بر تحلیل اسناد بالادستی، قوانین مصوب، رویه‌های قضایی شاخص و متون آکادمیک بنیادین در دو حوزه حقوقی آمریکا و اروپا انجام شده است.داده‌ها نیز از طریق روش گردآوری اسنادی و مطالعات کتابخانه‌ای گردآوری و تحلیل شده‌اند.

یافته‌ها: یافته‌ها از دوگانگی بنیادین میان رویکردهای آمریکا و اروپا حکایت دارد.در سنت آمریکایی، حریم خصوصی بر کنترل فردی و حق بر تنها گذاشته‌شدن استوار شده و در نتیجه نظامی واکنشی، پراکنده و کم‌قدرت در برابر انحصارهای اطلاعاتی شرکت‌های فناوری شکل گرفته است.در مقابل، سنت اروپایی با اتکا به کرامت انسانی و نقش دولت تنظیم‌گر، چارچوبی فعال، ایجابی، یکپارچه و تنظیم‌گرا ایجاد کرده که در مقرراتی مانند مقررات عمومی حفاظت از داده‌ها (GDPR) متجلی است.این چارچوب حقوقی مانند اصلاح و جبران خسارت را به رسمیت می‌شناسد و تکالیف سنگینی بر پردازش‌کنندگان داده تحمیل می‌کند؛ ازاین‌رو در حوزه‌های حساسی مانند علوم خبری، موازنه مؤثرتری میان حق اطلاع عمومی و حق حریم خصوصی فراهم می‌آورد.

نتیجه‌گیری: این پژوهش استدلال می‌کند که حمایت از داده‌های شخصی به‌عنوان حقی مستقل، ایجابی و نسل‌سومی تکوین یافته که مکمل و در بسیاری موارد فراتر از حق منفی و دفاعی حریم خصوصی است.مدل اروپایی، با تأکید بر شفافیت، پاسخگویی و محافظت از حریم خصوصی از طریق طراحی، الگویی قابل اقتباس اما نیازمند بومی‌سازی برای نظام‌های حقوقی در حال توسعه است.

استناد: شهناز ، امین؛ بهره مند، حمید؛ شیخ الاسلامی، عباس و فرجیها، محمد. (۱۴۰۵). مفهوم‌سازی حمایت از داده‌های شخصی از حریم خصوصی در فضای سایبر؛ مطالعه تطبیقی آمریکا و سنت حقوقی اروپا. فصلنامه ***علوم خبری***، ۱۵ (۲)، ۲۱۰-۱۹۱.
DOI: http//doi.org/10.22034/lrsi.2026.523001.1365

ناشر: موسسه مطبوعاتی روزنامه نگاری بین المللی معاصر.

مقدمه

گسترش فناوری‌های دیجیتال و ظهور «جامعه اطلاعاتی» یا «جامعه داده‌بنیان»، نه تنها شیوه زندگی و تعاملات اجتماعی را دگرگون کرده، بلکه رابطه سنتی و دیرپای میان «حریم خصوصی» فرد و قدرت نظارتی «دولت» و «بازار» را به کلی بازتعریف نموده است و پیوستگی اجتناب‌ناپذیری میان پیشرفت، رفاه و توسعهٔ تمدن بشری را از یک سو و استفاده از این فناوری‌های مدرن را از سوی دیگر ایجاد کرده است(فرهادی آلاشتی، ۱۳۹۵). در این فضای نوین، داده‌های شخصی به کالایی استراتژیک، منبع تولید ارزش اقتصادی و ابزاری برای اعمال قدرت تبدیل شده‌اند. همزمان، این داده‌ها که متضمن طرز زندگی، اعمال، رفتار و عقاید ما می باشند به عرصه‌ای آسیب‌پذیر برای تعرض، نظارت گسترده و دستکاری رفتاری بدل شده‌اند (قاجار قیونلو، ۱۳۹۱).

این نگاه اقتصادی به داده ها به همراه انتقال رو به تزاید فعالیت های انسانی از فضای فیزیکی به فضای مجازی نگرانی هایی را در خصوص حریم خصوصی برانگیخته است.از همین رو مسئله اصلی این پژوهش، تبیین ناکارآمدی روزافزون آموزه سنتی و کلاسیک حریم خصوصی است که عمدتاً به عنوان حقی منفی برای «به حال خود واگذاشته شدن» در برابر مداخله فیزیکی یا افشاء ناخواسته در مواجهه با چالش‌های پیچیده، سیال و سیستماتیک نقض داده‌ها توسط نهادهای قدرتمند دولتی و شرکت‌های انحصاری فناوری تعریف می شد؛ ناکارآمدی که صرفاً فنی نیست، بلکه مفهومی است زیرا به نظر می رسد ابزارهای مفهومی گذشته برای درک و مهار قدرت داده‌ها در عصر حاضر دیگر کافی نیست.

پرسش‌های پژوهش

این خلأ مفهومی و عملی، سؤالات اساسی ذیل را به میان می‌آورد:

سؤال اصلی

سیر مفهوم‌سازی حقوقی حمایت از داده‌های شخصی در فضای سایبر چگونه و بر پایه چه مبانی فلسفی از آموزه حریم خصوصی فاصله گرفته و به عنوان حقی مستقل و ایجابی تکوین یافته است؟

سؤالات فرعی

۱. مبانی فلسفی، تاریخی و اجتماعی دو سنت حقوقی آمریکایی و اروپایی در مفهوم‌سازی «حریم خصوصی» و سپس «حمایت از داده‌ها» چیست؟ چه ارزش‌هایی در کانون هر یک قرار دارد؟

۲. نقاط قوت، ضعف و پیامدهای عملی هر یک از این دو سنت در مواجهه با چالش‌های حکمرانی در عصر دیجیتال (نظیر کلان‌داده‌ها، امنیت ملی و غیره) کدامند؟

۳. این گذار مفهومی از حریم خصوصی به حمایت از داده‌ها، چه تأثیرات و پیامدهای مشخصی برای حوزه‌های حساسی مانند فعالیت‌های خبری، روزنامه‌نگاری تحقیقی و آزادی بیان دارد؟ چگونه می‌توان بین حق بر حفاظت از داده‌ها و حق عمومی بر اطلاع تعادل ایجاد کرد؟

اهمیت و ضرورت پژوهش

اهمیت این پژوهش تنها نظری نیست. درک این گذار برای تنظیم‌گری مؤثر فضای مجازی به‌ویژه در حوزه علوم خبری و رسانه مهم و ضروری است. از یک سو، آزادی مطبوعات و حق دسترسی به اطلاعات (ارکان دموکراسی) و فعالیت‌های خبری به طور ذاتی با جمع‌آوری و پردازش اطلاعات (از جمله داده‌های شخصی) سروکار دارد. از سوی دیگر، حق افراد بر حفظ حریم خصوصی داده‌های ایشان نیز از حقوق بنیادین محسوب می‌شود. رویکردهای متفاوت آمریکا و اروپا به این تعارض، آزمایشگاهی طبیعی و غنی برای بررسی نتایج عملی هر کدام از این چارچوب‌های مفهومی فراهم می‌آورد. آیا رویکرد مبتنی بر «کنترل» و «آزادی منفی» آمریکا که به رسانه‌ها میدان وسیع‌تری می‌دهد، در عصر دیجیتال پایدار است؟ یا رویکرد «ایجابی» و «تنظیم‌گر» اروپا که

محدودیت‌های بیشتری ایجاد می‌کند، در نهایت حافظ دموکراسی و اعتماد عمومی به رسانه‌ها خواهد بود؟ پاسخ به این سؤالات برای آینده حرفه روزنامه‌نگاری و سلامت فضای عمومی گفت‌وگو ضروری است.

ساختار پژوهش

این پژوهش پس از این مقدمه به بررسی مفهوم‌سازی و اسلوب‌های آن می‌پردازد. سپس سیر تاریخی تحول مفهوم حریم خصوصی از استعاره فضا تا حق «به حال خود واگذاشته شدن» را مرور می‌کند.پس از آن به ترتیب سنت حقوقی آمریکا (با محوریت کنترل و خودمختاری) و سنت حقوقی اروپا (با محوریت کرامت و مبانی حقوقی حمایت از داده ها) را به طور عمیق تحلیل می‌کند. بعد از آن چالش های ظهور حریم خصوصی اطلاعاتی را در سه بستر نوظهور (کلان‌داده، پروفایل سازی، پاسخ به نقض داده و امنیت ملی) بررسی می‌کند.سپس علوم خبری و فعالیت های روزنامه نگاری را در دو سنت آمریکایی و اروپایی بررسی می‌کند.و در نهایت، پس از نتیجه‌گیری و ارائه یافته ها، پیشنهادها و کاربست‌های عملی پژوهش را ارائه می دهد.

مفهوم‌سازی و اسلوب‌های آن: در جست‌وجوی تعریف امر خصوصی

پیش از ورود به تحلیل تطبیقی، لازم است به این پرسش بنیادین پاسخ دهیم: «مفهوم‌سازی» چیست و چگونه در مورد پدیده‌ای پیچیده و چندوجهی مانند «حریم خصوصی» به کار می‌رود؟ مفهوم‌سازی فرآیند انتزاع و تعریف مشخصات یک پدیده (در اینجا حریم خصوصی) برای درک و تمایز آن از دیگر پدیده‌هاست(حیدری، ۱۳۹۸).در حوزه حریم خصوصی، دو رویکرد اصلی روش‌شناختی مطرح شده است که هر کدام نتایج متفاوتی به بار آورده‌اند.

اولین نگرش، رویکرد سنتی (تعریف‌محور یا ذات‌گرا) نام دارد. این رویکرد به دنبال یافتن جوهره مشترک یا تعریف ضروری و کافی از حریم خصوصی است. پرسش محوری در این تعریف آن است که «ذات حریم خصوصی چیست؟ چه عناصر مشترکی در تمام مصادیق آن وجود دارد که آن را از امور عمومی متمایز می‌سازد؟» این روش، حریم خصوصی را به مثابه حوزه‌ای ثابت و دارای مرزهای مشخص در نظر می‌گیرد. مثال کلاسیک آن، تلاش‌های وارن و برندیس[1] برای تعریف حریم خصوصی به عنوان «حق بر تنها گذاشته شدن» یا ایده «کنترل اطلاعات شخصی» آلن وستین[2] است. مشکل اصلی این رویکرد تقلیل گرایی و انعطاف‌ناپذیری آن است.چرا که در مواجهه با فناوری‌های جدید که مرزهای ارتباط را در می نوردند (مانند ردیابی برخط یا تحلیل کلان‌داده‌ها)، تعاریف ذات‌گرا یا بسیار مضیق یا آنقدر گسترده می شوند که عملاً بی‌فایده می‌گردند.

رویکرد دوم، شباهت های خانوادگی است.لودویگ ویتگنشتاین[3]، فیلسوف اتریشی، در کتاب «پژوهش‌های فلسفی» نشان داد که بسیاری از مفاهیم زبانی مانند «بازی» فاقد یک خصیصه مشترک واحد در تمام مصادیق خود هستند. در عوض، شبکه‌ای از «شباهت‌های خانوادگی»[4] بین مصادیق مختلف وجود دارد؛ برخی ویژگی‌ها با هم همپوشانی دارند، اما هیچ ویژگی واحدی در همه موارد حاضر نیست (سولو[5]، ۲۰۰۲).[6] این دیدگاه انقلابی در مفهوم‌سازی حریم خصوصی ایجاد کرد.به عبارتی به جای جست‌وجوی یک ذات واحد، باید به کارکردهای اجتماعی، بافت فرهنگی و روابط قدرتی نگاه کرد که در یک زمان و مکان خاص، امری را «خصوصی» می‌سازند.در اینجا حریم خصوصی یک مفهوم رابطه‌ای و پویاست که در تعامل با هنجارهای اجتماعی، فناوری و قدرت

---

1 . Warren & Brandeis
2 . Alan Westin
3 . Ludwig Wittgenstein
4 . Family Resemblances
5 .Solove

۶ . شاید مثال چرخ در اینجا راهگشا باشد. در روش سنتی مفهوم‌سازی، مفاهیم به مثابه پره‌های پیوند خورده توسط توپی یک چرخ نگریسته می‌شود که همگی توسط یک نقطه مشترک (توپی) بهم پیوند خورده‌اند. این توپی یا نقطهٔ اشتراک در جایی که تمام پره‌ها بهم می‌رسند، روشی را تعریف می‌کند که در آن پره‌ها بهم مرتبط می‌شوند. اما در نظریهٔ شباهت خانوادگی، به نظر ویتگنشتاین گاهی اوقات توپی مشترکی وجود ندارد، بلکه شبکه‌ای از اجزای بهم مرتبط داریم که نقطهٔ مرکزی واحدی ندارند، در حالی که اجزا هنوز بهم مرتبطند (سولو، ۲۰۰۲)

شکل می‌گیرد و تغییر می‌کند. این رویکرد، انعطاف لازم برای درک تحولات دیجیتال را فراهم می‌آورد. برای مثال، آنچه امروزه تحت عنوان پروفایل‌سازی[۱] رفتاری توسط پلتفرم‌ها به عنوان نقض حریم خصوصی اطلاعاتی شناخته می‌شود دو دهه قبل حتی قابل تصور هم نبود.

انتخاب ناخودآگاه یا آگاهانه هر یک از این دو روش، مسیر بعدی تحلیل را تعیین می‌کند. سنت آمریکایی، با گرایش به فردگرایی و حقوق طبیعی، بیشتر به سمت تعاریف ذات‌گرا (مانند حوزه شخصی، کنترل) تمایل یافته است.در مقابل، سنت اروپایی با توجه به نقش جامعه و هنجارهای جمعی، همخوانی بیشتری با رویکرد شباهت‌های خانوادگی دارد و حریم خصوصی را بیشتر بر اساس هنجارهای اجتماعی ناشی از کرامت انسانی تعریف می‌کند. این تفاوت روش‌شناختی، سرچشمه بسیاری از تفاوت‌های عملی بین این دو سنت است.

سیر تاریخی تحول: از استعاره «فضا» تا حق «به حال خود واگذاشته شدن»

ایدهٔ حریم خصوصی سنتاً از تفاوت قائل شدن میان «خصوصی» و «عمومی» برمی‌آید و این تفاوت از نیاز طبیعی به قدمت بشریت افراد برای ایجاد تمایز میان خود و جهان خارج سرچشمه می‌گیرد (لوکاچ[۲]، ۲۰۱۶).از همین رو برای درک عمیق‌تر این تقابل، باید ریشه‌های تاریخی مفهوم حریم خصوصی را ردیابی کرد.سیری که نشان می‌دهد چگونه درک بشر از امر خصوصی همواره متأثر از شرایط مادی، اجتماعی و فناورانه زمانه خود بوده است و دائماً میان حوزهٔ خصوصی و حوزهٔ عمومی در حال تغییر و تحول است (عطار، ۱۳۹۵).

در دوران باستان و قرون وسطی، نخستین و ملموس‌ترین درک از حریم خصوصی، مرتبط با مکان فیزیکی(استعاره فضا) بود (دی لیو و همکاران[۳]، ۲۰۰۷). ارسطو در اثر سیاست، تمایز بین حوزه عمومی (پولیس[۴] یا شهر) و حوزه خصوصی (اویکوس[۵] یا خانه) را بنیان نهاد (موسی زاده و مصطفی زاده، ۱۳۹۱). به عبارتی حریم خصوصی در درجه اول به معنای امنیت درون خانه در برابر مزاحمت بیرون بود و از همان ابتدا بر فضا (دائمی به نام مسکن) تأکید داشت (بلوم[۶]، ۲۰۱۰). در حقوق روم نیز مفهوم «حریم منزل» مقدس شمرده می‌شد. در قرون وسطی، این ایده با حق مالکیت خصوصی گره می خورد و حق مالکیت دیگر یک حق اقتصادی نیست، بلکه حقی است که فضایی از حاکمیت شخصی برای مالک ایجاد می کند. حقوقدانان کامن‌لا نیز این ایده را با مفهوم « یوس اکسکلوئندی آلیوس»[۷] (یعنی حق محروم کردن دیگران) پیوند دادند(پتروکو[۸]، ۲۰۱۹). در این دوره، حریم خصوصی عمدتاً حق اشراف، اربابان و مردان خانه بود و به طور مساوی شامل تمام اعضای جامعه نمی‌شد.

عصر روشنگری: جدایی حوزه عمومی و خصوصی

در عصر روشنگری اندیشه‌های خردگرایانه با محوریت قرار دادن عقلانیت فردی و حقوق طبیعی، زمینه را برای شکل‌گیری مفهوم مدرن حریم خصوصی فراهم کرد.در اینجا مالکیت نه تنها بر اموال، بلکه در نهایت بر خود نیز تعمیم می یافت.با این حال، طرح حریم خصوصی به عنوان حقی مستقل و متمایز از مالکیت هنوز زود بود زیرا آنچه بیش از همه افراد را آزار می‌داد، صدمه دیدن استیفای کامل حق مالکیت خصوصی بود که توسط کامن‌لا به رسمیت شناخته شده بود. صدمه‌ای که به دلیل ماهیت قراردادی حقوق خصوصی و «وزن» اقتصادی بالقوه متفاوتِ طرفین، مداخلهٔ حقوق عمومی را طلب می‌کرد (پتروکو، ۲۰۱۹).

---

[1] . Profiling
[2] . Lukacs
[3] . de Leeuw et.al
[4] . Polis
[5] . Oikos
[6] . Blume
[7] . Ius Excludendi Alios
[8] . Petrucco

تحولات اجتماعی ناشی از انقلاب صنعتی از جمله رشد شهرنشینی، پیدایش مطبوعات زرد و فناوری‌های جدید مانند دوربین عکاسی قابل حمل احساس نیاز به حفاظتی فراتر از مالکیت فیزیکی را برانگیخت. مقاله مشهور ساموئل وارن و لوییس برندیس با عنوان «حق بر حریم خصوصی» به مثابه یک حق شخصی نقطه عطفی تاریخی در این زمینه است. آن‌ها استدلال کردند که حقوق موجود مانند مالکیت، قرارداد یا افترا، برای محافظت از آنچه «حق بر تنها گذاشته شدن» نام دارد، کافی نیست (دی لیو و همکاران، ۲۰۰۷). آن‌ها این حق را حق شخصی (و نه مالی) دانستند که از «احساسات» و «شرافت» فرد در برابر افشای ناخواسته زندگی خصوصی محافظت می‌کند (موسی زاده و مصطفی زاده، ۱۳۹۱). این ایده، حریم خصوصی را از حفاظت از مکان (خانه) به سمت حفاظت از شخصیت و اطلاعات مربوط به فرد سوق داد. با این حال، تمرکز همچنان بر محافظت در برابر مداخله‌های ملموس و افشاگری‌های خاص بود.

در دهه‌های ۱۹۶۰ و ۱۹۷۰، با گسترش رایانه‌ها و پایگاه‌های داده دولتی، نگرانی‌ها از «جامعه تحت نظارت» اوج گرفت.نیمه دوم قرن بیستم شاهد ظهور نظریه پردازان مدرن همچون آلن وستین بود که حریم خصوصی را «ادعای افراد، گروه‌ها یا مؤسسات برای تعیین این که چه زمانی، چگونه و تا چه حد اطلاعات مربوط به آن‌ها به دیگران منتقل می‌شود» می دانستند(انصاری، ۱۳۹۳). این تعریف بر کنترل اطلاعات تأکید داشت و پیوندی میان حریم خصوصی و خودمختاری فردی ایجاد کرد. نظریه‌پردازان دیگری مانند چارلز فرید[1] آن را با صمیمیت و اعتماد مرتبط دانستند؛ یعنی برسمیت شناختن نقش انتخاب فرد برخوردار از حریم خصوصی در اعطاء یا عدم اعطاء دسترسی به افراد به اطلاعات مربوط به خود (محسنی، ۱۳۹۴). با این حال، ظهور اینترنت و جهانی شدن جریان داده در پایان قرن بیستم، نشان داد که مدل‌های مبتنی بر کنترل فردی، در برابر مقیاس و پیچیدگی جمع‌آوری داده‌ها، آسیب‌پذیر هستند. این بحران، زمینه را برای ظهور پارادایم جدید «حمایت از داده‌ها» فراهم کرد.

سنت حقوقی آمریکا: فردگرایی، آزادی منفی و منطق کنترل

سنت حقوقی آمریکا در مورد حریم خصوصی، ریشه در تاریخ سیاسی، فلسفه لیبرال کلاسیک و ساختار قانون اساسی این کشور دارد. سه اصل بنیادین این سنت عبارتند از: فردگرایی شدید، سوءظن عمیق به قدرت دولت، و اولویت آزادی‌های منفی.

برخلاف تصور رایج، قانون اساسی آمریکا صراحتاً حقی به نام «حق حریم خصوصی» را تضمین نکرده است. حمایت از حریم خصوصی عمدتاً از طریق تفسیر قضایی از چند اصلاحیه، به ویژه اصلاحیه اول (آزادی بیان و مطبوعات)، اصلاحیه چهارم (ممنوعیت تفتیش و توقیف) و اصلاحیه پنجم (حق منع خود–اتهامی) استنباط شده است.برای مثال در رأی تاریخی گریسوولد علیه کنتیکت (۱۹۶۵)[2]، دیوان عالی آمریکا برای اولین بار «حق حریم خصوصی» را به عنوان حق ضمنی (پنهان) که از «هاله های حمایتی» چندین متمم قانونی اساسی نشأت می گرفت، به رسمیت شناخت.[3]

مفهوم‌سازی «کنترل» و «خودمختاری»

در گفتمان دانشگاهی و حقوقی آمریکا، دو مفهوم بیش از همه بر تعریف حریم خصوصی سایه افکنده‌اند:

از پیشگامان سنت نسبتاً جدید کنترل در مفهوم سازی آقای آلن وستین است.وی با شناسایی دو بُعد رابطه ای و اطلاعاتی برای حریم خصوصی، آن را حق فرد برای کنترل جریان اطلاعات مربوط به خود می‌داند. رضایت فرد، محور اصلی در ایده کنترل

---

[1] . Charles Fried

[2] . Griswold v. Connecticut (1965)

[3] . در این پرونده، دادگاه این مفهوم را در مورد قانون خاصی در کنتیکت که استفاده از وسایل جلوگیری از بارداری را برای زوج‌های متأهل ممنوع می‌کرد، به کار برد. دادگاه استدلال کرد که تصمیم در مورد استفاده یا عدم استفاده از وسایل جلوگیری از بارداری در خلوتگاه زناشویی، جنبه‌ای اساسی از زندگی مشترک است. این تصمیم آنقدر شخصی و مرکزی برای رابطه زناشویی بود که در «منطقه حریم خصوصی» ایجاد شده توسط هاله‌های متمم‌های اول، سوم، چهارم، پنجم و نهم ذکر شده قرار می‌گرفت.برای مطالعه بیشتر ر.ک:https://tile.loc.gov/storage.services/service/ll/usrep/usrep381/usrep381479/usrep381479.pdf

است. این مدل در قوانینی مانند قانون حریم خصوصی ۱۹۷۴[1] و قانون جابجایی پذیری و مسئولیت پذیری بیمه های درمانی(هیپا)[2] در خصوص اتخاذ استانداردهایی برای تبادل الکترونیکی داده های مربوط به سلامت دیده می شود (انصاری و همکاران، ۱۴۰۱).

مفهوم خودمختاری که بیشتر در حوزه‌های اخلاق زیستی و حقوق مطرح شد، حریم خصوصی را به حق تصمیم‌گیری مستقل فرد درباره امور مهم زندگی خود گره می‌زند و با پیوند دادن مستقیم حریم خصوصی و شخصیت، استدلال می کند کنترل یک نفر بر اطلاعات خود باید به عنوان سنگر خودمختاری وی در نظر گرفته شود و متقابلاً هرگونه تعرض به حریم خصوصی باید حمله‌ای به شخصیت و فردیت وی ترجمه شود (آلفینو و مایز[3]، ۲۰۰۲). خودمختاری این مزیت را دارد که هم در فضای خلوت و شخصی و هم در فضاهای جمعی از سوژه اطلاعات حمایت می‌کند و باعث می‌شود که حریم خصوصی به عنوان قلمروی برای ابراز هویت و انتخاب‌های شخصی انسان ها تعبیر شود (سولو، ۲۰۰۲).

فردگرایی از انتقادات جدی وارده بر نظریه کنترل است.منتقدانی مانند پال شوارتز[4] معتقدند مدل کنترل بر چند فرض غیرواقعی استوار است: نخست، این مفهوم به غلط فرض را بر این می گذارد که افراد در اعمال کنترل بر داده های شخصی خود در تمام موقعیت ها دارای خودمختاری هستند و از خطرات پردازش داده‌ها آگاهی کامل دارند (مساله ای که در سیستم‌های پیچیده غیر ممکن است)؛ دوم، قدرت چانه‌زنی برابری میان فرد و شرکت های بزرگ فناوری (با توجه به اختلافی که در دانش و قدرت دارند) وجود دارد و سوم، «رضایت» است که در شرایط عدم تقارن اطلاعات، اغلب بی‌معناست (سولو، ۲۰۰۲). در عمل، این مدل منجر به وابستگی افراطی به اعلامیه‌های حریم خصوصی طولانی و نامفهومی می شود که به کاربران توهم کنترل می‌دهد، در حالی که شرکت‌ها به جمع‌آوری گسترده داده‌ها ادامه می‌دهند.

چارچوب قانونی: رویکرد بخشی و غیرمداخله‌گرا

آمریکا فاقد یک قانون جامع فدرال در زمینه حفاظت از داده‌ها است.اما یک چهل‌تکه قانونی وجود دارد که هر بخش به حوزه‌ای خاص می‌پردازد، برای مثال قانون هیپا برای سلامت، قانون گرام- لیچ- بلیلی[5] برای امور مالی و قانون حریم خصوصی کودکان در فضای سایبر (کوپا)[6] برای حمایت از داده‌های ایشان در فضای مجازی.این رویکرد بخشی، شکاف‌های بزرگ محافظتی ایجاد می‌کند و شرکت‌های فناوری می‌توانند با حرکت داده‌ها بین بخش‌های مختلف قانون، مقررات را دور بزنند. نقش دولت فدرال هم عمدتاً مقابله با انحصار از طریق کمیسیون تجارت فدرال و اجرای قوانین خاص در صورت تخلف آشکار است و نه تنظیم‌گری پیش‌دستانه.قدرت اصلی به دادگاه‌ها و دادخواست‌های گروهی واگذار شده است که نظامی پسینی و هزینه‌بر است.

انعطاف‌پذیری، حفظ فضای گسترده برای نوآوری تجاری، حمایت قوی از آزادی بیان و مطبوعات در برابر محدودیت‌های دولتی از نقاط قوت این رویکرد است.در مقابل، ناتوانی در مقابله با سرمایه‌داری نظارتی، عدم وجود حمایت یکسان برای همه شهروندان در تمام حوزه‌ها، پیچیدگی و هزینه بر بودن رفع اختلاف برای افراد عادی، و ایجاد بازاری برای داده‌های شخصی که در آن کنترل واقعی بر اطلاعات از دست رفته است را می توان از نقاط ضعف آن بر شمرد.از همین روست که این سنت در مواجهه با مسائلی مانند نظارت گسترده آژانس امنیت ملی یا سوءاستفاده شرکت‌های فناوری بزرگ مانند فیسبوک-کمبریج آنالیتیکا[7]، به شدت مورد انتقاد قرار گرفته است و فشار برای تصویب یک قانون فدرال جامع را افزایش داده است.

---

1 . The Privacy Act (1974)
2 . Health Insurance Portability and Accountability Act (HIPPA) (1996)
3 . Alfino & Mayes
4 . Paul Schwartz
5 . Gramm.Leach.Bliley Act (GLBA) (1999)
6 . Children's Online Privacy Protection Act (COPPA) (1998)
7 . رسوایی فیسبوک.کمبریج آنالیتیکا به افشای استفاده غیرمجاز از اطلاعات شخصی میلیون‌ها کاربر فیسبوک توسط شرکت کمبریج آنالیتیکا اشاره دارد که از این داده‌ها برای اهداف کمپین‌های سیاسی استفاده شد (سینها، ۱۴۰۱)

سنت حقوقی اروپا: کرامت و دولت تنظیم‌گر فعال

سنت حقوقی اروپا در مورد حریم خصوصی و حفاظت از داده‌ها، مسیری کاملاً متفاوت را پیموده است. این مسیر ریشه در تجربه‌های تلخ تاریخی- نظارت و جمع آوری اطلاعات به مثابه ابزار کنترل و سرکوب مردم توسط فاشیسم و نظارت استالینیستی- و فلسفه اجتماعی قاره‌ای -که در آن فرد نه به‌صورت موجودی منزوی، بلکه به‌عنوان عضوی از جامعه‌ای دیده می‌شود که نیازمند حمایت فعال قانون است- دارد که بر کرامت انسان، دولت رفاه و نقش قانون در شکل‌دهی جامعه عادلانه تأکید می‌ورزد.

محور کلیدی و سنگ بنای نظم حقوقی اروپایی مفهوم «کرامت انسانی» است که در ماده یک منشور حقوق بنیادین اتحادیه اروپا[1] و قوانین اساسی کشورهای اروپایی مانند فرانسه و آلمان جای دارد. کرامت انسان ذاتی، سلب‌ناپذیر و غیرقابل معامله است. از این منظر، حریم خصوصی و داده‌های شخصی بازتابی از شخصیت و هویت «خود» فرد هستند که مبتنی بر اهمیت «کرامت» است که نقض آن‌ها نه صرفاً یک زیان اقتصادی یا مزاحمت، بلکه تهدیدی برای خودمختاری، آزادی و شرافت انسان است (پُست[2]، ۲۰۰۱).این نگاه، حریم خصوصی را از یک حق فردی اختیاری به یک شرط ضروری برای زندگی انسانی در جامعه ارتقاء می‌دهد و می‌تواند بنیانی برای مقررات عام یک گفتمان اختصاصی برای حفاظت از حریم خصوصی فراهم آورد (باسو[3]، ۲۰۱۲).

نظریه «منشأ مستقل دوگانه»

نظریه‌پردازانی مانند جیمز ویتمن[4] معتقدند مفهوم امروزی حریم خصوصی/ حفاظت از داده در اروپا از بهم پیوستن دو جریان فکری مستقل ایجاد شده است.نخست، جریان حقوق خصوصی قاره‌ای است که حول مفهوم کامن لایی مالکیت و آزادی از دولت می چرخد و مبتنی بر حفاظت از شخصیت و منزلت فرد در برابر تجاوز دیگران است (برای مثال در قالب حفاظت در برابر افترا یا انتشار غیرمجاز تصاویر). و دوم، جریان حقوق عمومی/ حقوق بشر است که با سرچشمه گرفتن از مفهوم کهن رژیم منزلت و احترام و محوریت محدود کردن قدرت دولت و تضمین فضایی برای رشد فردی در ماده ۸ کنوانسیون اروپایی حقوق بشر (حق بر احترام به زندگی خصوصی و خانوادگی، خانه و مکاتبات) تجلی یافته است (پتروکو، ۲۰۱۹). ترکیب این دو، حقی را ایجاد کرد که هم در برابر دولت و هم در برابر افراد و شرکت‌های خصوصی قابل استناد است.

مبانی حقوقی حمایت از داده‌ها: از نظریه تا اقدام

سطح نظری: پال دِهِرت[5] و سِرج گاتورث[6] در تحلیلی استدلال می کنند حریم خصوصی یک حق دفاعی و منفی است. ابزاری است برای حفظ «گُنگی» و ایجاد فضایی محفوظ از مداخله دیگران (به ویژه دولت) که منطق آن ممنوعیت و محدودیت است.اما حفاظت از داده‌ها یک حق ایجابی و مثبت است. ابزاری است برای ایجاد «شفافیت» و «کنترل» بر جریان اطلاعات که منطق آن تنظیم شرایط قانونی پردازش است (پورتووا[7]، ۲۰۱۰). این دو مکمل یکدیگرند اما یکی نیستند؛زیرا شرایطی را تدوین می کنند که پردازش داده ها ذیل آن قانونی است و حق حریم خصوصی سنتی نمی‌تواند حق دسترسی به داده‌های خود یا حق اصلاح اطلاعات نادرست را ایجاد کند. این کارکردها ذیل حق جدید «حمایت از داده» معنا می‌یابند (فرتی[8]، ۲۰۱۴).

سطح اقدام حقوقی: همانطور که پیش تر ذکر شد، ماده ۸ کنوانسیون اروپایی حقوق بشر یک حق کلاسیک و عمدتاً سلبی است که حمایت مناسبی از داده ها را ارائه نمی دهد.از همین رو، برای جبران این کاستی رویه قضایی دادگاه اروپایی حقوق بشر با توسل به دو آموزه، این حق را برای عصر داده‌ها کاربست‌پذیر کرد:نخست، آموزه بهره‌مندی مؤثر از حقوق است.طبق این اصل دولت‌ها

---

[1] . Charter of Fundamental Rights of the European Union
[2] . Post
[3] . Basu
[4] . James Whitman
[5] . Paul Dehert
[6] . Serge Gutwirth
[7] . Purtova
[8] . Ferretti

نه تنها باید از مداخله خودداری کنند، بلکه باید اقدامات ایجابی برای تضمین احترام عملی به این حق را صورت دهند.مساله ای که در پرونده گاسکین علیه فنلاند (۱۹۸۹)[۱] بدان صحه گذاشته شد.دوم، اثر افقی است.طبق این آموزه تکالیف مندرج در کنوانسیون تنها میان فرد و دولت نیست، بلکه دولت موظف است از طریق قوانین خود، از افراد در برابر نقض حقوق توسط اشخاص خصوصی (مانند شرکت‌ها) نیز محافظت کند(پورتووا، ۲۰۱۰).این تفسیر گسترده، پل نظری میان حق سلبی حریم خصوصی و تکالیف ایجابی حفاظت از داده‌ها را ایجاد کرد.در نهایت، این منشور بود که این تحول را نهادینه کرد و با ذکر جداگانه دو ماده (۷ و (۱)۸) استقلال حق حفاظت از داده‌ها را به رسمیت شناخت.

ظهور «حق بر حفاظت از داده‌های شخصی» به عنوان حقی مستقل

سنت حقوقی اروپا خیلی زود دریافت که صرف اتکاء به ماده ۸ کنوانسیون اروپایی حقوق بشر و نظریه منشأ مستقل دوگانه برای مواجهه و کنترل پردازش خودکار داده‌ها کافی نیست.از همین رو کنوانسیون ۱۰۸ شورای اروپا (۱۹۸۱) اولین معاهده بین‌المللی بود که به طور خاص به «حفاظت از افراد در رابطه با پردازش خودکار داده‌های شخصی» پرداخت. این روند با رهنمود حفاظت از داده ۱۹۹۵ اتحادیه اروپا[۲] و در نهایت مقررات عمومی حفاظت از داده‌ها (GDPR)[۳] در سال ۲۰۱۶ به اوج خود رسید.مهم در این سیر تقنینی، تفکیک رسمی این حق از حق حریم خصوصی بود که صرفاً تفسیر موسعی از ماده ۸ کنوانسیون اروپایی حقوق بشر نبود، به گونه ای که ماده ۷ [۴] منشور حقوق بنیادین به «احترام به زندگی خصوصی و خانوادگی» و ماده (۱)۸[۵] به طور مستقل به «حفاظت از داده‌های شخصی» پرداخت. این جداسازی، ماهیت ایجابی و فرآیند–محور حق جدید «حفاظت از داده‌ها» را تأیید کرد.

ویژگی‌های کلیدی مدل اروپایی (با محوریت مقررات عمومی حفاظت از داده‌ها)

۱. در این مدل تمرکز قانونگذار بر قبل از وقوع نقض است.برای مثال داشتن مبنای قانونی (مانند رضایت، قرارداد، منفعت مشروع و غیره) برای پردازش داده‌ها، رعایت اصولی مانند کمینه سازی داده‌ها، و محدودیت هدف در پردازش داده ها و یا حریم خصوصی از طریق پیشفرض[۶] یا حریم خصوصی از طریق طراحی[۷] همگی حکایت از اتخاذ رویکردی پیشگیرانه دارد.

۲. این قانون حقوق قوی و فراتر از کنترل برای افراد موضوع داده پیش بینی کرده است.حقوقی نظیر دسترسی، اصلاح، فراموشی، محدودیت پردازش، ابلاغ نقض داده، جبران خسارت و مهم‌تر از همه، حق اعتراض به پردازش و عدم تبعیت از یک تصمیم‌گیری کاملاً خودکار.

۳. تکالیف سنگین برای کنترلگران و پردازشگران از دیگر مقررات این قانون است. ایشان موظف به اثبات رعایت قانون بر اساس اصل پاسخگویی هستند.[۸]در مواردی باید مامور حفاظت از داده[۹] منصوب کنند، تأثیرات ارزیابی حفاظت از داده[۱۰] را برای فعالیت‌های پرخطر پردازشی انجام دهند و در صورت نقض داده‌ها، به نهاد ناظر و افراد موضوع داده گزارش دهند.

---

[1] . Gaskin v. Finland (1989)

در این پرونده دیوان اروپایی حقوق بشر مقرر داشت که دولت فنلاند در مورد خانم گاسکین، با عدم دسترسی کامل او به سوابق مربوط به دوران کودکی‌اش در مراکزحمایتی، ماده ۸ کنوانسیون اروپایی حقوق بشر را نقض کرده است. دیوان تأکید کرد که حق دسترسی به اطلاعات شخصی، به ویژه در مواردی که به دوران کودکی و روابط خانوادگی مربوط می‌شود، بخشی از حق حفظ حریم خصوصی و زندگی خانوادگی است.https://hudoc.echr.coe.int/tur?i=001.57491

[2] . Directive 95/46/EC

[3] . General Data Protection Regulation

[۴] .« هر کس حق دارد که به زندگی خصوصی و خانوادگی، خانه و مکاتباتش احترام گذاشته شود.»

[۵] .« هر کس حق دارد که داده‌های شخصی مربوط به او محافظت شود.»

[6] - Privacy by Default

[7] - Privacy by Design

[۸] . ماده (۲)۵ مقررات عمومی حفاظت از داده ها

[9] . Data Protection Officer:DPO

[10] . Data Protection Impact Assessment: DPIA

۴. هر کشور عضو موظف است یک مرجع نظارتی مستقل (مانند کمیسیون ملی انفورماتیک و آزادی‌ها در فرانسه)[۱] ایجاد کند.این نهاد قدرت تحقیق، صدور دستور توقف پردازش و اعمال جریمه‌های سنگین (تا ۴٪ از گردش مالی سالانه جهانی یا ۲۰ میلیون یورو) را براساس مقررات عمومی حفاظت از داده‌ها دارد.

۵. این مقررات نه تنها بر شرکت‌های اروپایی، بلکه بر هر شرکتی که به شهروندان اروپایی کالا / خدمات ارائه دهد یا رفتار آنان را رصد کند، اعمال می‌شود (اصل قلمرو فرامرزی). این امر مقررات عمومی حفاظت از داده‌ها را به یک استاندارد جهانی تبدیل کرده است.[۲]

حمایت یکسان و قدرتمند برای همه شهروندان، ایجاد استانداردهای شفاف و قابل پیش‌بینی، تقویت اعتماد در اقتصاد دیجیتال، توانایی مقابله با انحصارهای اطلاعاتی از نقاط قوت مدل جدید اروپایی است.در خصوص چالش ها می توان به پیچیدگی و هزینه‌بر بودن انطباق با این مدل برای کسب‌وکارهای کوچک، امکان تفسیرهای متفاوت نهادهای ناظر کشورهای عضو، جریمه‌های سنگین، کندی فرآیندهای اداری و همچنین نگرانی‌هایی در باب تحمیل بیش از حد بار اداری و تأثیر احتمالی آن بر نوآوری اشاره کرد.

حریم خصوصی اطلاعاتی: تقابل دو سنت در عمل

رشد پر شتاب فناوری‌های اطلاعاتی– ارتباطی، ماهیت تسهیل‌گر- ناقض فناوری و کثرت و تنوع ایجاد مسیرهای اطلاعاتی توسط افراد در بکارگیری این فناوری‌ها با به چالش کشیدن کنترل اطلاعات (دراجی و بارسیس[۳]، ۲۰۱۴) زمینه تعاملات مربوط به حقوق داده‌ها را تغییر می‌دهند که به تبع آن دامنه مطلوب حفاظت از حریم خصوصی اطلاعاتی نیز تغییر می‌یابد (کوفونه[۴]، ۲۰۱۷).کلان داده‌ها، پاسخ ها به نقض داده و امنیت ملی نمونه های مناسبی از تقابل دو سنت آمریکایی و اروپایی در مواجهه با چالش های حریم خصوصی اطلاعاتی در عمل هستند.

در مواجهه با پدیده کلان‌داده‌ها و پروفایل‌سازی رویکرد غالب در حقوق آمریکا خود–تنظیمی صنعتی و شفافیت (از طریق اعلامیه حریم خصوصی)[۵] است. تا زمانی که شرکت‌ها رضایت افراد موضوع داده را (اغلب از طریق کلیک روی دکمه «موافقم») کسب کنند و به تعهدات خود در اعلامیه عمل کنند، جمع‌آوری و تحلیل کلان‌داده برای اهداف بازاریابی رفتاری عموماً مجاز است و کمیسیون تجارت فدرال تنها در صورت فریب یا اقدام غیرمنصفانه مداخله می‌نماید و هیچ حق عمومی برای اعتراض به پروفایل‌سازی یا درخواست توجیه یک تصمیم خودکار وجود ندارد (انصاری و همکاران، ۱۴۰۱).

در رژیم حفاظت از داده اروپایی (GDPR) پردازش کلان‌داده‌ها مشمول مداخلاتی تنظیم گرانه و محدودیت‌های سخت‌گیرانه است (رایت و راب[۶]، ۲۰۱۴).رضایت برای این نوع پردازش باید آزادانه، مشخص، آگاهانه و بدون ابهام باشد و فرد حق رجوع از آن را دارد. اگر پردازش بر مبنای «منفعت مشروع» کنترل‌کننده است (مثلاً بازاریابی مستقیم)، فرد می‌تواند در هر زمان اعتراض کند.به ویژه، هرگونه تصمیم‌گیری کاملاً خودکار (از جمله پروفایل سازی) که تأثیر حقوقی یا مشابه قابل توجهی بر فرد دارد، مشروط به رضایت صریح یا ضرورت قراردادی است و فرد حق دارد توضیحی در مورد منطق تصمیم دریافت کند. این امر از یکسو شرکت‌ها را مجبور می‌سازد فرآیندهای خود را شفاف‌تر و قابل توضیح‌تر سازند و از سوی دیگر قدرت اشخاص موضوع داده را در برابر قدرت شرکت‌های تجاری و دولت‌هایی که داده‌های ایشان را نگهداری می‌کردند، تقویت می کند (آکوئیستی و همکاران[۷]، ۲۰۱۵).

---

[1] . Commission Nationale de l'Informatique et des Libertés: CNIL

[۲] . ماده ۳ مقررات عمومی حفاظت از داده ها

[3] . Dorraji & Barcys

[4] . Cofone

[۵] . اعلامیه فوق مبتنی بر سیاست اطلاع و انتخاب *(Notice and Choice)* است.طبق این سیاست شرکت ها با قرار دادن سیاست های حریم خصوصی خود در وبگاه هایشان به اطلاع مخاطبین و یازدیدکنندگان می رسانند که داده های شخصی ایشان به چه صورت جمع آوری و پردازش می شود (انصاری و همکاران، ۱۴۰۱)

[6] . Wright & Raab

[7] . Acquisti et.al

در زمینه پاسخ به نقض داده‌های شخصی، قوانین اعلام نقض داده در آمریکا در سطح ایالتی متفاوت است. معمولاً شرکت‌ها موظفند در صورت نقض اطلاعات حساس، به افراد و گاهی به مقامات ایالتی اطلاع دهند.[۱] سازوکار اصلی جبران خسارت، دادخواست گروهی است که نتیجه آن اغلب پول نقد ناچیز برای کاربران و جریمه‌های چند میلیون دلاری برای شرکت‌ها است که در مقایسه با سود آنها ناچیز است.[۲]

اما طبق مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا، کنترل‌کنندگان موظفند ظرف ۷۲ ساعت پس از آگاهی از نقض، به مرجع نظارتی گزارش دهد، مگر آنکه بعید باشد نقض صورت گرفته خطری برای حقوق افراد ایجاد کند.[۳] اگر نقض احتمال خطر بالایی برای حقوق افراد داشته باشد، باید بلافاصله به خود ایشان نیز اطلاع‌رسانی شود.[۴] برخلاف سنت آمریکایی، مراجع نظارتی در این مدل قدرت اعمال جریمه‌های مستقیم و بسیار سنگینی را دارند.[۵]

در حوزه نظارت دولتی و امنیت ملی تنش میان آزادی‌های مدنی (حفاظت از حریم خصوصی تحت متمم چهارم قانون اساسی) و امنیت ملی در آمریکا یک تناقض ساختاری است که پس از حوادث ۱۱ سپتامبر با ابزارهایی مانند قانون میهنی[۶] تشدید شده است.با این حال رویه قضایی دیوان عالی (پرونده کارپنتر علیه ایالات متحده (۲۰۱۸) درباره ردیابی موقعیت مکانی تلفنی)[۷] گاه این اقدامات را محدود کرده است.اما به طور کلی جمع‌آوری فراداده‌ها به عنوان ابزاری قدرتمند برای نظارت، به دلیل حجم زیاد و توانایی در آشکارسازی الگوهای زندگی، روابط اجتماعی، و باورهای سیاسی یک فرد، همچنان یک میدان نبرد حقوقی و سیاسی است.

در اروپا، محاکم اروپایی نسبت به نظارت گسترده حساسیت بسیار بیشتری نشان داده‌اند. دیوان دادگستری اتحادیه اروپا در رأی مشهور شرمز(۲۰۲۰)[۸]، توافقنامه «پرایوسی شیلد»[۹] بین اتحادیه اروپا و آمریکا را باطل اعلام کرد. زیرا مکانیسم‌های نظارتی آمریکا برای محافظت از داده‌های اروپایی در برابر دسترسی مقامات امنیتی آن کشور را ناکافی دانست.در همین راستا، دادگاه اروپایی حقوق بشر نیز بر لزوم نظارت قضایی مستقل بر فعالیت‌های نظارتی و وجود راهکارهای مؤثر شکایتی تأکید کرده است. مساله‌ای که به وضوح در پرونده زاخارو علیه روسیه (۲۰۱۵)[۱۰] قابل مشاهده است.

---

[1] . California Civil Code § 1798.82

[۲] . برای مثال طبق ماده ۱۵۰(a) قانون حریم خصوصی مصرف کنندگان کالیفرنیا، برای هر تخلف هر کسب کار خسارتی که کمتر از ۱۰۰ دلار و بیش از ۷۵۰ دلار نباشد را در نظر گرفته است.

[۳] . ماده ۳۳ مقررا عمومی حفاظت از داده‌ها

[۴] . ماده ۳۴ مقررا عمومی حفاظت از داده‌ها

[۵] . مواد ۸۳ و ۸۴ از فصل هشتم مقررات عمومی حفاظت از داده‌ها

[6] . Patriot Act (2001)

[۷] . در پرونده Carpenter v. United States(2018) دیوان عالی مقرر داشت که جمع‌آوری سوابق موقعیت مکانی تلفن همراه که برای مدت طولانی به دست آمده است، نیازمند حکم تفتیش است، زیرا این داده‌ها نمایانگر «نقشه زندگی» فرد هستند. این حکم بر اساس متمم چهارم قانون اساسی (حفاظت در برابر تفتیش و توقیف غیرمنطقی) صادر گردید:https://supreme.justia.com/cases/federal/us/585/16.402/

[8] . CJEU, C.362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015.

شرِمز، شهروندی اتریشی است که شکایتی را به مرجع حفاظت از داده‌ها ایرلند تسلیم کرد تا انتقال داده‌های شخصی خود از نمایندگی ایرلندی فیس‌بوک به شرکت فیس‌بوک و سرورهای واقع در آمریکا را که داده‌ها در آنجا پردازش می‌شوند، محکوم کند. استدلال او این بود که با توجه به افشاگری‌های سال ۲۰۱۳ ادوارد اسنودن، در رابطه با فعالیت‌های نظارتی سرویس‌های نظارتی آمریکا، قانون و رویهٔ آمریکا حمایت کافی از داده‌های شخصی منتقل شده به خاک این کشور را ارائه نمی‌کند (باترلی و همکاران، ۲۰۱۸)

[9] . Privacy Shield

[۱۰] . در پرونده Zakharov v. Russia (2015) دادگاه اروپایی حقوق بشر تأکید کرد که هر گونه مداخله در حریم خصوصی، حتی در راستای امنیت ملی، باید به طور **صریح و قابل دسترس** توسط قانون ملی پیش‌بینی شده باشد و صرف اینکه یک قانون کلی وجود داشته باشد کافی نیست:
Roman Zakharov v. Russia (Application No. 47143/06) . Police and Human Rights Resources

خبر و رسانه: میدان نبرد حق‌ها

حوزه خبر و رسانه، آزمایشگاه ایده‌آلی برای بررسی تقابل این دو سنت است.آزادی بیان، حق بر فراموشی و حفاظت از منابع خبری مستقیماً با حق بر حفاظت از داده‌های شخصی (در مدل اروپایی) با حق حریم خصوصی (در مدل آمریکایی) تزاحم پیدا می‌کند.

در نظام حقوقی آمریکا، اصلاحیه اول قانون اساسی (حق آزادی بیان) جایگاهی تقریباً بی‌همتا دارد. دیوان عالی آمریکا در احکام متعددی افشای اطلاعات مربوط به افراد مشهور یا درگیر در امور عمومی، حتی اگر خصوصی باشد، در صورتی که دارای «ارزش خبری» باشد را مشمول حمایت اصلاحیه اول دانسته است. استاندارد سخت‌گیرانه‌ای برای اثبات افتراء وجود دارد. حریم خصوصی منبع خبری نیز تحت حمایت قوانین محافظت از منبع خبری قرار دارد، اما این حمایت مطلق نیست.کفه ترازو به نفع جریان آزاد اطلاعات سنگینی می کند.نقض حریم خصوصی افراد غیر مشهور ممکن است قابل پیگرد باشد، اما بار اثبات بر عهده خواهان است. این چارچوب حقوقی به رسانه‌ها فضای گسترده‌ای برای مانور می‌دهد، اما می‌تواند منجر به قربانی شدن حریم خصوصی افراد شود.

در سنت اروپایی، مقررات عمومی حفاظت از داده ها به صراحت معافیت‌هایی برای پردازش داده به منظور اهداف خبری در نظر گرفته است. این مقررات به کشورهای عضو اجازه می‌دهد با وضع قوانین ملی، تعادلی بین حق بر حفاظت از داده و حق بر آزادی بیان و اطلاعات ایجاد کنند. اما این معافیت مطلق نیست و اصول بنیادین پردازش (مانند اصل قانونی بودن، اصل صحت داده‌ها یا اصل امنیت) همچنان باید رعایت شوند که موازنه نسبتاً دقیقی مبتنی بر منافع مشروع را رقم می زند. روزنامه‌نگار نمی‌تواند به بهانه «خبر»، داده‌های نادرست را منتشر کند یا داده‌ها را به صورت ناامن نگهداری نماید.[۱] با این حال انتشار اطلاعات درباره یک سیاستمدار یا شخصیت عمومی ممکن است با استناد به منفعت عمومی (مشروع) توجیه شود.

حق بر فراموشی یکی از چالش‌های بزرگ رسانه‌ها در عصر حاضر است.برای مثال دیوان دادگستری اتحادیه اروپا در پرونده گوگل اسپانیا (۲۰۱۴)[۲] مقرر داشت موتورهای جست‌وجو (به عنوان کنترل‌گران داده) موظفند در صورت درخواست فرد، لینک‌ها به اطلاعات نادرست، نامربوط یا متجاوز از هدف پردازش داده را حذف کنند. با این حال، این حق مطلق نیست و بطور خاص باید با حق عمومی دسترسی به اطلاعات تعدیل گردد (باترلی و همکاران[۳]، ۲۰۱۸). زیرا حذف یک لینک از نتایج جست‌وجو به معنای سانسور اصل خبر نیست.

در خصوص حفاظت از منابع خبری مقررات عمومی حفاظت از داده ها بر این اصل صحه می گذارد که قوانین معافیت باید حفاظت از منابع محرمانه را نیز در نظر بگیرند.[۴] به عبارت دیگر پردازش داده‌های شخصی که صرفاً برای اهداف روزنامه‌نگاری صورت می‌گیرد، در صورتی که برای سازگاری میان حق حفاظت از داده‌های شخصی با حق آزادی بیان و اطلاعات ضروری باشد، همانطور که در ماده ۱۱ منشور تثبیت شده است، مشمول معافیت‌ها یا استثنائات خاصی از برخی مواد مقررات عمومی حفاظت از داده ها می باشد.

نتیجه آنکه، مدل اروپایی پیش‌بینی پذیرتر و ساختاریافته‌تر است. رسانه‌ها باید از قبل درباره مبانی قانونی پردازش داده‌های شخصی (منفعت عمومی، رضایت و ....) و اصل تناسب (آیا انتشار تمام این جزئیات ضروری است؟) تدبیر نمایند. این امر ممکن است بار اداری ایجاد کند، اما شفافیت و مسئولیت‌پذیری را افزایش می‌دهد.در مقابل مدل آمریکایی انعطاف‌پذیرتر و کم‌هزینه‌تر برای رسانه‌هاست، اما ممکن است در مواردی به قربانی شدن بی‌دلیل حریم خصوصی بینجامد و اعتماد عمومی را تضعیف کند.

---

[۱] . ماده ۸۵(۲) مقررات عمومی حفاظت از داده ها

[2] . Google Inc. v. Agencia Española de Protección de Datos (AEPD) (2014)

[3] . Buttarelli et.al

[۴] . بند ۱۵۳ مقدمه توجیهی مقررات عمومی حفاظت از داده ها

نتیجه‌گیری و چشم‌انداز

این پژوهش نشان داد که مفهوم «حمایت از داده‌های شخصی» صرفاً یک بروزرسانی فنی یا گسترش حوزه حریم خصوصی سنتی نیست، بلکه نشان‌دهنده یک گذار پارادایمی عمیق در حقوق بنیادین است: گذار از حقی منفی، دفاعی، فضامحور و فردگرا به سمت حقی ایجابی، فعال، فرآیندمحور و جمع‌گرا. سنت آمریکایی با تمام نقاط قوت خود در زمینه حفظ آزادی‌های سیاسی و فضای نوآوری، در دام فردگرایی افراطی و منطق بازار گرفتار آمده است. مدل مبتنی بر «کنترل» و «خودمختاری» در برابر منطق انباشت و پردازش کلان‌داده‌ها توسط انحصارهای فناوری، شکست خورده است. این نظام واکنشی و پراکنده، قدرت لازم برای مهار «سرمایه‌داری نظارتی» را ندارد و شهروندان را در وضعیت نابرابر رها کرده است.در حالی که سنت اروپایی با اتکاء به مفهوم کرامت انسانی به عنوان کانون نظم اجتماعی و پذیرش نقش دولت تنظیم‌گر مردم‌سالار، چارچوبی مقاوم‌تر، آینده‌نگر و مبتنی بر عدالت اطلاعاتی ایجاد کرده است. مقررات عمومی حفاظت از داده‌ها با تحمیل تکالیف سنگین بر کنترل کنندگان و اعطاء حقوق قوی به افراد موضوع داده، توازن قدرت را تا حدی بازتوزیع می‌کند و اگرچه با چالش‌های اجرایی و انتقاداتی درباره سنگینی بار اداری مواجه است، اما به یک استاندارد جهانی اثرگذار تبدیل شده است.

در خصوص یافته نهایی و اصلی این پژوهش باید خاطرنشان ساخت آینده حکمرانی در عصر دیجیتال نه در پیروی کورکورانه از یکی از این دو مدل، بلکه در تلفیق هوشمندانه و بومی‌سازی شده عناصر کلیدی هر دو سنت است. یک نظام حقوقی کارآمد باید بتواند:

۱. آزادی‌های فردی و فضای ضروری برای نوآوری و بیان (برگرفته از مدل آمریکایی) را حفظ کند؛

۲. تکالیف ایجابی، پاسخگویی و شفافیت برای نهادهای قدرتمند (دولتی و خصوصی) و حقوق مثبت قابل اجرا برای افراد (بر گرفته از مدل اروپایی) را وضع نماید؛

۳. یک نهاد نظارتی مستقل، تخصصی و قدرتمند (برگرفته از مدل اروپایی) ایجاد نماید که بتواند با سرعت فناوری همگام شود؛

۴. در حوزه‌های خاص مانند فعالیت خبری و روزنامه نگاری، تعادلی شفاف، مبتنی بر قانون و موردی میان حقوق متعارض برقرار نماید و از قربانی شدن یکی از حقوق متعارض جلوگیری نماید.در این سنتز، تقلید صرف از مقررات عمومی حفاظت ازداده‌ها بدون توجه به بافت سیاسی. فرهنگی و سطح توسعه نهادی ممکن است به قانونی بی‌اثر یا سرکوبگر بینجامد و در عین حال، غفلت از درس‌های بنیادین مدل اروپایی درباره نقش تنظیم‌گری و حقوق ایجابی، می تواند کشورها را در برابر قدرت شرکت‌های فناوری بزرگ و اشتهای فزاینده‌ی آنها در پردازش و جمع آوری داده‌های شخصی بی‌پناه گذارد (رایت و راب، ۲۰۱۴).

پیشنهادها و کاربست‌ها

برای نظام‌های حقوقی در حال توسعه (با تأکید بر ایران)

۱. تدوین قانون جامع حفاظت از داده‌ها با ماهیت ایجابی: قانون آینده نباید صرفاً یک قانون مجازات یا نقض باشد. باید مبتنی بر اصول اساسی پردازش، ترجیحاً مقررات عمومی حفاظت از داده‌ها اروپا (مانند حریم‌خصوصی از طریق طراحی، کمینه سازی داده، پاسخگویی) و در عین حال متناسب با شرایط داخلی باشد.ایجاد معافیت‌های پردازشی مشروط و مشخص برای حوزه‌های حساسی مانند تحقیقات علمی و فعالیت‌های خبری نیز نباید مورد غفلت قرار گیرد.

۲. ایجاد نهاد تنظیم‌گر مستقل، تخصصی و قدرتمند: این نهاد باید دارای استقلال اداری و مالی، اختیارات وسیع نظارتی (بازرسی، دستور توقف، جریمه)، صلاحیت رسیدگی سریع به شکایات و تفسیر قانون را داشته باشد.

۳. ترویج فرهنگ سازمانی حفاظت از داده: آموزش عمومی و تخصصی (برای کسب‌وکارها، روزنامه‌نگاران، کارمندان دولت) درباره حقوق و تکالیف جدید در برابر داده‌های شخصی باید از هم‌اکنون آغاز شود.

برای حوزه علوم خبری و رسانه ها

۱. بازنگری در اخلاق حرفه‌ای روزنامه‌نگاری: نهادهای صنفی رسانه‌ای باید دستورالعمل‌های عملی برای تطبیق فعالیت‌های خبری با اصول پردازش و حفاظت از داده‌ها تدوین کنند. همچنین اصل تناسب (انتشار حداقل اطلاعات لازم برای روایت داستان خبری) و احترام به حق فراموشی در موارد استثنایی نیز باید مورد توجه ویژه قرار گیرد.

۲. توسعه روزنامه‌نگاری امن: آموزش و ترویج استفاده از ابزارهای رمزنگاری انتها به انتها[1]، ارتباطات امن و روش‌های ناشناس‌سازی[2] و مستعارسازی[3] داده برای محافظت از منابع و مصاحبه‌شوندگان.

۳. پژوهش‌های میان‌رشته‌ای: انجام مطالعات تجربی درباره تأثیر عملی قوانین حفاظت از داده‌ها (مانند GDPR) بر کیفیت، دامنه و روش گزارشگری تحقیقی در کشورهای مختلف.همچنین پژوهش در مورد درک و نگرش روزنامه‌نگاران نسبت به این مقررات.

برای پژوهش‌های آتی:

۱. مطالعه تطبیقی مدل‌های غیرغربی: بررسی رویکردهای حفاظت از داده کشورهایی مانند چین (مدل نظارتی- امنیتی) یا برزیل (ال جی پی دی[4] به عنوان اقتباسی از GDPR) در حوزه علوم خبری و فعالیت های رسانه ای.

۲. تحلیل فناوری‌های نوین به عنوان راه‌حل: مطالعه امکان‌سنجی و چالش‌های استفاده از فناوری‌هایی مانند حریم خصوصی از طریق طراحی و یا از طریق پیشفرض برای ایجاد سازش عملی بین تحلیل داده و حفظ حریم خصوصی در حوزه فعالیت‌های خبری.

۳. بررسی نقش حقوق رقابت: تحلیل تقاطع میان حقوق حفاظت از داده و حقوق رقابت برای مقابله با انحصارهای اطلاعاتی؛ آیا می‌توان غول‌های فناوری را به دلیل انباشت بی‌رویه داده‌های شخصی (که به عنوان یک «دارایی ضروری» عمل می‌کند) مهار کرد؟

منابع

انصاری، باقر(۱۳۹۳). حقوق حریم خصوصی.تهران: سمت.

انصاری، باقر؛عطار، شیما؛صالحی، امیر حسین؛ زند، حسین(۱۴۰۱).مطالعه تطبیقی حمایت از داده های شخصی در اروپا، آمریکا، چین و ایران.تهران: شرکت انتشارات سهامی.

حیدری، مرتضی(۱۳۹۸).منطق حملی.مشهد:موسسه چاپ و انتشارات آستان قدس رضوی، ۶۴-۶۵.

سینها، آمبر(۱۴۰۱).*شبکه‌های اجتماعی و سیاست قدرت* (م. جزینی و ا. پسنده پور، مترجمان).تهران:انتشارات پیله، ۱۰۶-۱۰۹.

عطار، شیما(۱۳۹۵). حمایت از حریم خصوصی در شبکه های اجتماعی مجازی.تهران: انتشارات خرسندی.

فرهادی آلاشتی، زهرا(۱۳۹۵). پیشگیری وضعی از جرایم سایبری (راهکارها و چالش ها). تهران: انتشارات میزان،۱۳.

قاجار قیونلو، سیامک(۱۳۹۱). مقدمه حقوق سایبر(درآمدی بر جامعه شناسی حقوق توسعه و پیش نیازهای قانون نویسی در فضای سایبر). تهران:انتشارات میزان.

محسنی، فرید(۱۳۹۴). حریم خصوصی اطلاعات (مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه). تهران:دانشگاه امام صادق (ع)/

موسی زاده، ابراهیم؛مصطفی زاده، فهیم(۱۳۹۱). نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی، فصلنامه بررسی های حقوق عمومی،۲، ۴۵-۶۶.

[1] . End.to.End
[2] . Anonymisation
[3] . Pseudonymisation
[4] . LGPD: Lei Geral de Proteção de Dados

References:

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509.

Alfino, M., & Mayes, G. R. (2002). Reconstructing the right to privacy. Social Theory and Practice, 29(1), 4.

Ansari, B. (2014). Rights of privacy (Vol. 15). SAMT Publications. (in Persian)

Ansari, B., Attar, S., Salehi, A. H., & Zand, H. (2022). Comparative study of personal data protection in Europe, America, China, and Iran (pp. 94–108). Sahami Publishing Company. (in Persian)

Attar, S. (2016). The protection of privacy within virtual social networks (p. 41). Khorsandi. (in Persian)

Basu, S. (2012). Privacy protection: A tale of two cultures. Journal of Law & Technology, 6(1), 10.

Blume, P. (2010). Data protection and privacy—basic concepts in a changing world. Scandinavian Studies in Law, 56, 155.

Buttarelli, G., Giakoumopoulos, C., & O'Flaherty, M. (2018). Handbook on European data protection law (p. 57). Publications Office of the European Union.

Carpenter v. United States, 585 U.S. (2018). https://supreme.justia.com/cases/federal/us/585/16-402/

Cofone, I. (2017). The dynamic effect of information privacy law. Minnesota Journal of Law, Science & Technology, 18(2), 519–547.

De L., K. M. M., & Bergstra. (2007). History of privacy. In The history of information security: A comprehensive handbook (1st ed., p. 3). Elsevier.

Dorraji, E., & Barcys, M. (2014). Privacy in digital age: Dead or alive?! Regarding the new EU data protection regulations. Social Technologies, 4(2), 315.

Farhadi Alashti, Z. (2016). Situational prevention of cybercrimes (Strategies and challenges) (p. 13). Mizan. (in Persian)

Ferretti, F. (2014). Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights? Common Market Law Review, 51(3), 855–884.

Gaskin v. Finland, Application No. 001-57491 (1989). https://hudoc.echr.coe.int/tur?i=001-57491

Ghajjar Ghayoonloo, S. (2012). Introduction to cyber law (An approach to the sociology of development law and prerequisites for legislation in cyberspace) (p. 343). Mizan. (in Persian)

Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12 (2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131

Griswold v. Connecticut, 381 U.S. 479 (1965). https://tile.loc.gov/storage-services/service/ll/usrep/usrep381/usrep381479/usrep381479.pdf

Heydari, M. (2019). Manteq-e hemli [Predicate logic] (pp. 64–65). Astan Quds Razavi Publishing and Printing Institute. (in Persian)

Lukacs, A. (2016). What is privacy? The history and definition of privacy. Scandinavian Studies in Law, 56, 257.

Maximillian Schrems v. Data Protection Commissioner [GC], Case C-362/14 (2015). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362

Mohseni, F. (2015). Information privacy (A criminal law study in the laws of Iran, the United States of America, and Imamiyah jurisprudence) (p. 6). Imam Sadiq University (AS). (in Persian)

Mousazadeh, I., & Mostafazadeh, F. (2012). A look at the concept and foundations of the right to privacy in the common law legal system. Public Law Review, 1(2), 57. (in Persian)

Petrucco, F. (2019). The right to privacy and new technologies: Between evolution and decay. Media Law Magazine, 1, 5.

Post, R. C. (2001). Three concepts of privacy. Georgetown Law Journal, 89, 2089–2095.

Purtova, N. (2010). Private law solution in European data protection: Relationship to privacy, and waiver of data protection rights. Netherlands Quarterly of Human Rights, 28(2), 247–265.

Roman Zakharov v. Russia*, Application No. 47143/06 (2015). Police and Human Rights Resources. https://hudoc.echr.coe.int/eng?i=001-159565

Sinha, A. (2022). Social networks and the politics of power (M. Jazini & A. Pasandepour, Trans.). Pileh Publications. (in Persian)

Solove, D. J. (2002). Conceptualizing privacy. California Law Review, 90, 1087–1155.
Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. International Review of Law, Computers & Technology, 28(3), 277–286.