Received: 15 /12/2023
Review: 09/02/2024
Accepted: 10 /04/2024
DOI: 10.22054/jocl. 2025.85073.2918

Journal of Cyber Law
No(1),Vol(1),77-95.
ISSN: 0972-6934
www.jocl.ir

A Comparative Analysis of the European Union and the United States Approaches to Cybersecurity Regulation

Nora Yazdani [1], Sohail Ahmadi[*2]

1- Master's Student in Law, Shiraz University, Iran.

2*- Master's Student in Law, Shiraz University, Iran.

ABSTRACT

The European Union and the United States, as two major global actors, have adopted different approaches to cybersecurity regulation that significantly impact network security, privacy protection, and data safeguarding. Given the sharp rise in cyber threats and sophisticated attacks, the importance of a comparative study of these two approaches to identify strengths and weaknesses of each legal system is increasingly felt. This research aims to provide a comparative analysis of cybersecurity policies, laws, and frameworks in the European Union and the United States. The research method in this article is descriptive-analytical, based on documentary and comparative study, examining legal sources, official policies, governmental documents, and prior research. Findings indicate that the European Union emphasizes user privacy and enforces stringent regulations such as the General Data Protection Regulation (GDPR) to advance cybersecurity within the framework of civil rights and personal data protection. In contrast, the United States adopts a more national security-oriented and flexible regulatory approach, especially through sector-based policies and voluntary standardization, aiming to foster a dynamic environment for technological development and cyber threat response. These differing approaches bring specific advantages and limitations, ultimately affecting the quality and effectiveness of cybersecurity management. The innovation of this study lies in its comprehensive and comparative analysis based on up-to-date official documents and laws, which can assist policymakers and legal experts in enhancing cybersecurity frameworks.

Keywords:
Cybersecurity, European Union, United States, Regulation, Privacy Protection

How to Cite: Yazdani, N. and Ahmadi, S. (2024). A Comparative Analysis of the European Union and the United States Approaches to Cybersecurity Regulation. Cyber Law, 1(1), 77-95.
DOI: 10.22054/jocl.2025.85073.2918

[*] Corresponding Author: s.ahmadi@shirazu.ac.ir

نشریه حقوق سایبری
شماره (۱) ۷۷-۹۵
دوره ۱۴۰۳

تاریخ دریافت: ۱۴۰۲/۰۹/۲۴
تاریخ اصلاح: ۱۴۰۲/۱۱/۲۰
تاریخ پذیرش: ۱۴۰۳/۰۱/۲۲

تحلیل تطبیقی رویکرد اتحادیه اروپا و ایالات متحده در مقررات‌گذاری امنیت سایبری

نورا یزدانی[۱]، سهیل احمدی[۲*]

۱- دانشجوی کارشناسی ارشد رشته حقوق، دانشگاه شیراز، ایران.

۲ - دانشجوی کارشناسی ارشد رشته حقوق، دانشگاه شیراز، ایران.

چکیده

اتحادیه اروپا و ایالات متحده به عنوان دو بازیگر مهم در عرصه جهانی، رویکردهای متفاوتی در مقررات‌گذاری امنیت سایبری اتخاذ کرده‌اند که تأثیر قابل توجهی بر امنیت شبکه‌ها، حفظ حریم خصوصی و حفاظت از داده‌ها دارد. با توجه به افزایش چشمگیر تهدیدهای سایبری و حملات پیچیده، اهمیت بررسی تطبیقی این دو رویکرد در جهت شناخت نقاط قوت و ضعف هر نظام قانونی بیش از پیش احساس می‌شود. این پژوهش با هدف تحلیل تطبیقی سیاست‌ها، قوانین و چارچوب‌های امنیت سایبری در اتحادیه اروپا و ایالات متحده انجام شده است. روش تحقیق در این مقاله توصیفی-تحلیلی و مبتنی بر مطالعه اسنادی و مقایسه‌ای است که به بررسی منابع قانونی، سیاست‌های رسمی، اسناد دولتی و تحقیقات پیشین پرداخته است. یافته‌های تحقیق نشان می‌دهد که اتحادیه اروپا با تأکید بر حفظ حریم خصوصی کاربران و تدوین مقررات سخت‌گیرانه‌ای مانند مقررات عمومی حفاظت از داده‌ها (GDPR) تلاش دارد امنیت سایبری را در چارچوب حقوق شهروندی و حفاظت از اطلاعات شخصی پیش ببرد. در مقابل، ایالات متحده با رویکردی بیشتر مبتنی بر امنیت ملی و انعطاف‌پذیری در مقررات، به‌ویژه با رویکرد بخش‌محور و استانداردسازی داوطلبانه، سعی در ایجاد یک محیط پویا برای توسعه فناوری‌های نوین و پاسخگویی به تهدیدات سایبری دارد. این تفاوت رویکردها سبب شده است که هر کدام مزایا و محدودیت‌های خاص خود را داشته باشند که در نهایت بر کیفیت و کارایی مدیریت امنیت سایبری تأثیرگذار است. نوآوری این پژوهش در ارائه تحلیل جامع و تطبیقی بر مبنای اسناد رسمی و قوانین روزآمد است که می‌تواند به سیاست‌گذاران و حقوقدانان در بهبود چارچوب‌های امنیت سایبری کمک کند.

کلیدواژه‌ها:

امنیت سایبری، اتحادیه اروپا، ایالات متحده، مقررات‌گذاری، حریم خصوصی

نحوه استناد:

یزدانی, نورا و احمدی, سهیل . (۱۴۰۳). تحلیل تطبیقی رویکرد اتحادیه اروپا و ایالات متحده در مقررات‌گذاری امنیت سایبری. حقوق سایبری, ۱(۱), ۷۷-۹۵ .

* ایمیل نویسنده مسئول: s.ahmadi@shirazu.ac.ir

مقدمه

تحلیل تطبیقی رویکرد اتحادیه اروپا و ایالات متحده در مقررات‌گذاری امنیت سایبری موضوعی است که در سال‌های اخیر با توجه به گسترش روزافزون فناوری‌های دیجیتال و افزایش تهدیدات سایبری اهمیت ویژه‌ای یافته است. اگر چه جام جهانی تمایلی به اعمال حاکمیت هر کشوری بر فضای سایبری در دسترس شهروندان خود ندارد (ملکوتی ،۱۳۹۸)، اما ضرورت تامین امنیت افراد و حاضران در این فضا مورد اجماع همه کشورهای عضو سازمان ملل متحد می باشد (ضیایی،۱۳۹۶).امنیت سایبری به عنوان یکی از ارکان کلیدی حفاظت از داده‌ها، حریم خصوصی و زیرساخت‌های حیاتی، جایگاه محوری در نظام‌های حقوقی مدرن یافته است. در قوانین اتحادیه اروپا، به‌ویژه در مقرراتی مانند «مقررات عمومی حفاظت از داده‌ها» (GDPR) که در سال ۲۰۱۶ تصویب و در سال ۲۰۱۸ اجرایی شد، تاکید فراوانی بر حفاظت از حقوق فردی و تضمین امنیت اطلاعات شده است (Regulation (EU) 2016/679). این مقررات به صراحت چارچوب‌های قانونی مشخص و سخت‌گیرانه‌ای را برای کنترل داده‌های شخصی و مسئولیت‌های نهادها در قبال نقض‌های امنیتی تعیین کرده‌اند. از سوی دیگر، ایالات متحده با توجه به ماهیت فدرالی و چندلایه بودن نظام حقوقی خود، رویکردی مبتنی بر قوانین بخش‌بندی شده و استانداردهای داوطلبانه اتخاذ کرده است که در آن توجه ویژه‌ای به امنیت ملی و قابلیت انطباق با تغییرات سریع فناوری وجود دارد (CISA Act, 2018). این دو رویکرد تا حد زیادی نشان‌دهنده تفاوت‌های بنیادین در دیدگاه‌ها و فلسفه‌های حقوقی امنیت سایبری هستند که تأثیرات عمیقی بر نحوه مدیریت تهدیدات و پاسخ‌های قانونی دارند.

اهمیت این موضوع به ویژه در زمینه چالش‌های نوین حقوقی و اجتماعی ناشی از حملات سایبری، نشت داده‌ها، و پیچیدگی‌های تعامل میان حریم خصوصی و امنیت ملی روزبه‌روز بیشتر می‌شود. همانطور که پژوهشگران برجسته‌ای مانند (Stalla-Bourdillon, et al, 2020) در مطالعات خود نشان داده‌اند، فقدان هماهنگی قانونی بین کشورهای مختلف و عدم وجود چارچوب‌های مشترک موجب افزایش آسیب‌پذیری در برابر تهدیدات سایبری می‌شود. همچنین تحقیقات بارکلی و همکاران (۲۰۲۰) به روشنی نشان می‌دهد که رویکردهای مختلف حقوقی می‌تواند نتایج متفاوتی در حفاظت از حقوق کاربران و تضمین امنیت فناوری‌های دیجیتال داشته باشد. در ایران نیز پژوهشگرانی چون رضایی (۱۳۹۸) و کاظمی (۱۳۹۹) به اهمیت توجه به استانداردهای بین‌المللی و ضرورت ایجاد قوانین بومی با توجه به شرایط داخلی اشاره کرده‌اند، هرچند خلأ قانونی و فقدان تطبیق با تحولات جهانی در حوزه امنیت سایبری هنوز به عنوان یکی از چالش‌های اصلی مطرح است. پژوهش‌های پیشین در این زمینه عمدتاً به تحلیل جداگانه نظام‌های حقوقی و مقررات خاص پرداخته‌اند، اما بررسی تطبیقی عمیق و جامع میان دو قطب اصلی قوانین امنیت سایبری جهان کمتر انجام شده است.

با توجه به این زمینه، پرسش‌های اصلی تحقیق عبارتند از: تفاوت‌ها و شباهت‌های رویکردهای اتحادیه اروپا و ایالات متحده در مقررات‌گذاری امنیت سایبری چیست؟ هر یک از این رویکردها چه نقاط قوت و ضعف حقوقی و عملی دارند؟ و در نهایت، چه درس‌هایی می‌توان از این تحلیل تطبیقی برای بهبود چارچوب‌های حقوقی امنیت سایبری در سایر کشورها، به ویژه ایران، گرفت؟ هدف اصلی مقاله، ارائه تحلیل تطبیقی و شناسایی مبانی حقوقی، سیاست‌ها و استانداردهای کلیدی در این دو نظام حقوقی است تا به تبیین راهکارهای موثرتر در مقررات‌گذاری امنیت سایبری کمک کند.

روش پژوهش در این مقاله توصیفی-تحلیلی و مبتنی بر مطالعه اسنادی و تطبیقی است. در این روش، با بررسی و تحلیل متون قانونی، اسناد رسمی، سیاست‌های اعلام شده توسط نهادهای ذی‌ربط اتحادیه اروپا و ایالات متحده، و همچنین مقالات و پژوهش‌های پیشین، ساختارها و رویکردهای حقوقی موجود استخراج و با یکدیگر مقایسه شده‌اند. مطالعات تطبیقی در این حوزه به دلیل تفاوت‌های ساختاری نظام‌های حقوقی و سیاست‌های کلان، نیازمند تحلیل دقیق و جامع است که از طریق بررسی مواد قانونی مانند GDPR در اتحادیه اروپا، قانون امنیت سایبری ایالات متحده(CISA) ، و مستندات مربوط به استانداردهای امنیتی انجام شده است. این رویکرد به فهم بهتر چارچوب‌های قانونی و عملیاتی کمک می‌کند و زمینه‌ساز ارائه پیشنهادات کاربردی و راهبردی برای بهبود نظام‌های امنیت سایبری می‌شود. استفاده از منابع معتبر و به‌روز و توجه به اسناد رسمی، روش‌شناسی تحقیق را تقویت نموده و اعتبار علمی آن را تضمین می‌کند. این مقاله تلاش دارد ضمن تبیین دقیق ساختارهای حقوقی دو طرف، نقاط قوت و ضعف آن‌ها را به صورت منصفانه بررسی نماید و چارچوبی تحلیلی برای تصمیم‌گیرندگان حقوقی و سیاست‌گذاران ارائه دهد.

امنیت سایبری

به معنای حفاظت از سیستم‌ها، شبکه‌ها و داده‌ها در برابر حملات سایبری، نفوذ غیرمجاز و تخریب اطلاعات است و از منظر حقوقی، این حوزه شامل مقررات، سیاست‌ها، رویه‌های قضایی و استانداردهای فنی می‌شود که هدف آن تضمین سلامت، امنیت و حریم خصوصی کاربران و نهادهای مختلف است (Oakley, 2023) سایبری نه تنها یک ضرورت فنی بلکه یک مسئله حقوقی، اجتماعی و اقتصادی است که نیازمند ایجاد تعادل میان حفاظت از اطلاعات، حفظ آزادی‌های فردی و حمایت از نوآوری است (حسینی، ۱۳۹۸). بنابراین، رویکردهای حقوقی به امنیت سایبری باید فراتر از مقررات صرفاً امنیتی، شامل تضمین حقوق دیجیتال، حفظ حریم خصوصی، و پاسخگویی به حملات سایبری باشد (Rustad Koenig, 2019).

از منظر حقوقی، امنیت سایبری در نظام‌های مختلف دارای ابعاد متفاوتی است که تابع فرهنگ حقوقی، ساختارهای حکومتی و اولویت‌های سیاست‌گذاری هر کشور یا اتحادیه می‌باشد. اتحادیه اروپا رویکردی جامع، مبتنی بر حقوق شهروندی و حفاظت از داده‌ها دارد و به این موضوع به چشم یک چالش حقوق بشری و حفظ حریم خصوصی می‌نگرد (هیئت عمومی دیوان عالی کشور، ۱۳۹۸). این رویکرد در قوانین کلیدی مانند «مقررات عمومی حفاظت از داده‌ها » (GDPR)و «قانون هوش مصنوعی اتحادیه اروپا» تجلی یافته است. در مقابل، ایالات متحده عمدتاً رویکردی مبتنی بر امنیت ملی و تجارت آزاد دارد که تمرکز بر افزایش امنیت زیرساخت‌های حیاتی و توسعه فناوری‌های نوین دارد (سعیدی پور ،۱۳۹۷). این تفاوت‌های بنیادین در رویکردها موجب شکل‌گیری سیاست‌ها و قوانین متفاوتی در دو حوزه قضایی شده است که تحلیل تطبیقی آن‌ها اهمیت زیادی دارد .

در این راستا نظریه حاکمیت سایبری به بررسی چگونگی کنترل و تنظیم فضای سایبری توسط دولت‌ها می‌پردازد. این نظریه بیان می‌کند که حاکمیت در فضای سایبری نه تنها به معنی کنترل فنی بلکه شامل قدرت قانونی و سیاستگذاری نیز می‌شود. در این چارچوب، اتحادیه اروپا با تاکید بر حاکمیت داده‌ها و حفظ حقوق فردی، مقرراتی وضع کرده که شرکت‌ها و نهادهای دولتی را ملزم به رعایت استانداردهای سختگیرانه‌ای می‌سازد. این در حالی است که ایالات متحده بیشتر به تعامل بازار آزاد و نوآوری فناوری توجه دارد و قوانین سختگیرانه‌ای مانند GDPR ندارد (Schm itt, 2017).

نظریه حقوق بشر دیجیتال

در این نظریه تاکید بر این است که امنیت سایبری نباید به بهای نقض حقوق اساسی مانند حق حریم خصوصی و آزادی بیان صورت گیرد. این دیدگاه در اسناد بین‌المللی مانند «بیانیه جهانی حقوق بشر دیجیتال» و گزارش‌های سازمان ملل متحد مورد تایید قرار گرفته است .(UN Human Rights Council, 2020) اتحادیه اروپا این رویکرد را به‌عنوان اصل بنیادین در تنظیم مقررات خود پذیرفته و تلاش می‌کند با استفاده از ابزارهای قانونی از جمله حقوق دسترسی به اطلاعات و شفافیت در داده‌ها، تعادل میان امنیت و آزادی‌های فردی را حفظ کند (کلینبرگ، ۱۳۹۷).

در مقابل، ایالات متحده با رویکردی پراگماتیک‌تر به امنیت سایبری می‌نگرد که مبتنی بر سیاست‌های دفاعی و همکاری‌های بین‌المللی است. این رویکرد، با تمرکز بر چارچوب‌هایی مانند «قانون امنیت سایبری دولت فدرال» و «دستورالعمل‌های ملی امنیت سایبری»، سعی در تقویت زیرساخت‌های فناوری اطلاعات دارد، اما گاهی مورد انتقاد به دلیل کمبود قوانین محافظت از داده‌های شخصی و نگرانی‌های حقوق بشری قرار گرفته است . (Harding et al 2022).

از منظر مبانی اقتصادی نیز امنیت سایبری به عنوان یک «کالای عمومی» تعریف می‌شود که دارای منافع جمعی و نیازمند همکاری بین‌المللی است . در این زمینه، اتحادیه اروپا به دنبال ایجاد یک بازار دیجیتال یکپارچه است که با قوانین هماهنگ، امنیت و نوآوری را توأمان تضمین کند (حسینی، ۱۳۹۷). ایالات متحده نیز، به دلیل ساختار فدرال و بازار گسترده فناوری، به رویکردهای متنوع‌تری مانند استانداردسازی داوطلبانه و همکاری‌های بخش خصوصی-دولتی توجه دارد (Klar, R. 2022).

در بعد حقوق کیفری، تفاوت‌های آشکاری بین دو رویکرد مشاهده می‌شود. اتحادیه اروپا تلاش کرده با تصویب قوانین سختگیرانه‌تر علیه جرایم سایبری، از جمله حملات به داده‌ها و زیرساخت‌های حیاتی، هم در سطح ملی و هم اتحادیه‌ای مقابله کند (عابدی، ۱۳۹۰). این قوانین در قالب دستورالعمل‌هایی مانند «دستورالعمل جرایم رایانه‌ای» تدوین شده‌اند و تاکید بر همکاری بین‌المللی و تبادل اطلاعات دارند . ایالات متحده نیز در این حوزه قوانین متعددی دارد اما ساختار فدرالی آن، گاهی موجب پراکندگی و تداخل در اجرای قوانین شده است .

رویکردهای حقوقی در خصوص پاسخگویی و مسئولیت در امنیت سایبری نیز متفاوت است. در اتحادیه اروپا، مسئولیت شرکت‌های فناوری و ارائه‌دهندگان خدمات به طور مشخص تعریف شده و آن‌ها ملزم به رعایت اصول شفافیت، اطلاع‌رسانی و حفظ داده‌ها هستند (حسینی، ۱۳۹۸). در مقابل، در ایالات متحده، رویکرد مسئولیت‌پذیری کمتر متمرکز و بیشتر بر اساس سیاست‌های بازار و رقابت تنظیم شده است که ممکن است در برخی موارد منجر به خلاهای قانونی شود(Miller, 2014: 227-229).

رویکرد اتحادیه اروپا و ایالات متحده آمریکا در مقررات‌گذاری حوزه امنیت سایبری تفاوت‌های قابل‌توجهی دارد که ریشه در ساختار حقوقی، سیاسی و قضایی آن‌ها دارد. در اتحادیه اروپا، امنیت سایبری به‌عنوان یک ضرورت ساختاری برای حفظ انسجام بازار دیجیتال و همچنین حفظ حقوق بنیادین شهروندان اتحادیه تلقی می‌شود. به همین دلیل، در دهه اخیر این اتحادیه گام‌های بلندی برای تدوین و اجرای مقررات الزام‌آور در این حوزه برداشته است. نخستین اقدام جدی در این راستا، تصویب دستورالعمل امنیت شبکه و سیستم‌های اطلاعاتی (NIS Directive) در سال ۲۰۱۶ بود که کشورهای عضو را ملزم به وضع الزامات امنیتی برای اپراتورهای خدمات حیاتی و ارائه‌دهندگان خدمات دیجیتال کرد.

در سال ۲۰۲۲، این دستورالعمل با نسخه پیشرفته‌تری به‌نام NIS2 جایگزین شد که دامنه شمول و سازوکارهای اجرایی گسترده‌تری دارد.(European Commission, 2022) .

علاوه بر آن، اتحادیه اروپا در قالب مقرراتی چون "قانون تاب‌آوری سایبری"، برای نخستین بار تولیدکنندگان محصولات دیجیتال را موظف کرده است که پیش از عرضه محصول، الزامات امنیتی خاصی را رعایت کرده و پس از عرضه نیز به‌روزرسانی‌های امنیتی لازم را ارائه دهند (European Commission, 2023). همچنین، با تصویب "قانون همبستگی سایبری "، تلاش شده است که سازوکارهای هماهنگ و واکنش جمعی میان کشورهای عضو برای مقابله با تهدیدات سایبری فراملی ایجاد شود. آنچه این مقررات را متمایز می‌سازد، پیوند آن‌ها با منشور حقوق بنیادین اتحادیه اروپا است که بر اساس آن، حتی در وضع قوانین امنیتی نیز اصل تناسب، حفظ جوهره آزادی‌ها و حق بر حریم خصوصی باید رعایت شود.(Craig de Búrca, 2020) .

در مقابل، ایالات متحده آمریکا رویکردی کمتر یکپارچه و بیشتر مبتنی بر تنظیمات بخشی در حوزه امنیت سایبری دارد. برای مدت‌ها، سیاست‌های امنیت سایبری این کشور بیشتر مبتنی بر دستورهای اجرایی ریاست‌جمهوری، اسناد راهبردی و همکاری داوطلبانه میان دولت و بخش خصوصی بوده است. اما در سال‌های اخیر، با افزایش حملات سایبری به زیرساخت‌های حیاتی، ضرورت تنظیم مقررات الزام‌آور بیشتر احساس شده است. انتشار «راهبرد ملی امنیت سایبری» در سال ۲۰۲۳ که به‌دنبال انتقال مسئولیت بیشتر به تولیدکنندگان و شرکت‌های فناوری است، نقطه عطفی در این مسیر به‌شمار می‌رود(Winter Davidson, 2022) .

با این حال، نظام قانون اساسی آمریکا، به‌ویژه با اتکا به متمم‌های اول و چهارم، مانعی جدی برای وضع مقررات مداخله‌گرایانه به‌شمار می‌رود. برای نمونه، تلاش‌ها برای وضع مقرراتی پیرامون رمزنگاری یا الزام شرکت‌ها به ارائه درِ پشتی برای دسترسی دولت به داده‌ها، همواره با چالش‌های حقوق اساسی مواجه شده‌اند (Kerr, 2018) .دیوان عالی آمریکا نیز در موارد متعدد بر اولویت آزادی بیان و حریم خصوصی در برابر دخالت‌های احتمالی دولت تأکید کرده است. بنابراین، در حالی که اتحادیه اروپا توانسته است مقررات امنیت سایبری را به چارچوبی یکپارچه و الزام‌آور تبدیل کند، در ایالات متحده هنوز هم چالش‌های قانون اساسی و نبود هماهنگی کامل میان نهادهای فدرال، ایالتی و بخش خصوصی، مانع تدوین یک سیاست یکپارچه فراگیر شده است(Schneier, 2020) .

جایگاه امنیت سایبری در نظام حقوق بشر: تفسیر نوین از حریم خصوصی و آزادی‌های بنیادین در عصر دیجیتال

امنیت سایبری در بستر حقوق بشر مفهومی نوظهور ولی فزاینده در اهمیت است. در دنیای امروز که داده‌ها، ارتباطات و اطلاعات شخصی در محیط دیجیتال مبادله می‌شوند، تهدیدات سایبری می‌توانند به‌طور مستقیم بر تحقق و اجرای حقوق بنیادین بشر مانند حق بر حریم خصوصی، آزادی بیان، حق بر اطلاعات، و امنیت شخصی تأثیرگذار باشند (Kuner, 2015)بنابراین، بسیاری از اصول اساسی حقوق بشر که در اسناد بین‌المللی شناخته‌شده‌اند، نسبت به تهدیدات فضای سایبری نیز قابلیت اعمال دارند.

در رأس اسناد بین‌المللی حقوق بشری، اعلامیه جهانی حقوق بشر(UDHR، 1948)در ماده ۱۲ تصریح می‌کند که "هیچ‌کس نباید در زندگی خصوصی، خانواده، اقامتگاه یا مکاتباتش مورد مداخله خودسرانه قرار گیرد." این اصل، که بعداً در اسناد الزام‌آورتر بین‌المللی گسترش یافت، سنگ‌بنای شناسایی حق بر حریم خصوصی دیجیتال محسوب می‌شود.

بر همین اساس، ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (ICCPR، 1966)نیز دقیقاً همین اصل را با الزام قانونی برای دولت‌ها مطرح می‌کند: "هیچ‌کس نباید در زندگی خصوصی، خانواده، منزل یا مکاتباتش مورد مداخله دلخواه یا غیرقانونی قرار گیرد" و دولت‌ها باید از افراد در برابر چنین مداخلاتی حمایت کنند.(UN, 1966) .

در سال‌های اخیر، کمیته حقوق بشر سازمان ملل نیز در تفسیر عمومی شماره ۱۶ به‌روشنی اعلام کرده است که حق بر حریم خصوصی شامل ارتباطات دیجیتال، داده‌های شخصی و اطلاعات ذخیره‌شده در فضای مجازی نیز می‌شود (UN Human Rights Committee, 1988).در نتیجه، مداخله دولت‌ها در فضای سایبری، از طریق نظارت، دسترسی به داده‌ها، یا کنترل محتوا، باید مطابق با الزامات سه‌گانه قانونی بودن، ضرورت و تناسب باشد (Clément Sottiaux, 2021).از دیگر حقوق بنیادینی که به امنیت سایبری مرتبط است، آزادی بیان است که در ماده ۱۹ میثاق حقوق مدنی و سیاسی تضمین شده است. آزادی بیان شامل دریافت و انتقال اطلاعات و ایده‌ها از طریق هر نوع رسانه‌ای است، از جمله اینترنت و بسترهای دیجیتال. بنابراین، حملات سایبری، سانسور دیجیتال، فیلترینگ گسترده، یا قطع اینترنت می‌توانند ناقض این حق تلقی شوند، مگر اینکه محدودیت‌ها مطابق با شرایط سخت‌گیرانه ماده ۱۹ بند ۳ اعمال شوند؛ یعنی محدودیت‌ها باید قانونی، ضروری و برای حمایت از منافع مشروع مانند امنیت ملی یا نظم عمومی باشند (UN, 1966).همچنین، حق بر امنیت شخصی ماده ۹ (ICCPR) نیز از منظر جدیدی در ارتباط با فضای سایبری تفسیر می‌شود. تهدیدهای سایبری مانند سرقت هویت، باج‌افزار، تهدید به خشونت، و آزار جنسی سایبری می‌توانند امنیت فیزیکی و روانی افراد را تهدید کنند. بنابراین دولت‌ها موظف‌اند زیرساخت‌های قانونی و فنی برای حمایت از افراد در برابر این تهدیدات فراهم کنند(kesan, 2012: 454).

در سطح منطقه‌ای نیز اسناد مشابهی وجود دارند. برای مثال، ماده ۸ کنوانسیون اروپایی حقوق بشر (ECHR)بر حق احترام به زندگی خصوصی و خانواده تأکید دارد که بارها توسط دیوان اروپایی حقوق بشر در زمینه نظارت الکترونیکی، داده‌های ارتباطی، و حریم خصوصی دیجیتال تفسیر شده است (Council of Europe, 1950) .همچنین، در قوانین اتحادیه اروپا، ماده ۷ و ۸ منشور حقوق بنیادین اتحادیه اروپا (2000)به‌ترتیب به حق بر زندگی خصوصی و حق بر حفاظت از داده‌های شخصی اشاره دارند. این دو ماده اساس تصویب مقرراتی نظیر مقررات حفاظت از داده‌ها (GDPR)بوده‌اند که به‌طور خاص برای حفظ امنیت اطلاعات شخصی در فضای دیجیتال طراحی شده‌اند (European Union, 2016).در این میان، موضوع دسترسی به رمزنگاری قوی نیز به‌عنوان یک حق بنیادین نوظهور در حال طرح است. برخی پژوهشگران و نهادهای بین‌المللی پیشنهاد داده‌اند که دسترسی به ابزارهای رمزگذاری، در شرایطی، می‌تواند بخشی از حق بر حریم خصوصی و آزادی بیان محسوب شود؛ زیرا رمزنگاری یکی از ابزارهای عملی برای حفظ این حقوق در فضای سایبری است (Clark, 2010: 663) البته هنوز اجماع حقوقی بین‌المللی درباره شناسایی رمزنگاری به‌عنوان یک حق وجود ندارد، اما رویه‌ها و تفاسیر در این مسیر در حال گسترش‌اند.

در مجموع، اگرچه اصطلاح "امنیت سایبری" به‌صراحت در هیچ‌یک از اسناد کلاسیک حقوق بشری نیامده است، اما اصول بنیادینی همچون حریم خصوصی، آزادی بیان، امنیت شخصی و حتی حق بر اطلاعات، چارچوب‌های قابل استنادی برای اعمال و توسعه حقوق بشر در محیط سایبری فراهم می‌کنند. بر این اساس، دولت‌ها مسئول‌اند هم در برابر تهدیدات سایبری اقداماتی پیشگیرانه و حمایتی انجام دهند و هم هنگام اجرای سیاست‌های امنیتی، حقوق بشر را رعایت کنند.

امنیت سایبری در نظام حقوق بشر در نظام حقوقی فرانسه

در نظام حقوقی فرانسه، امنیت سایبری در تقاطع میان حفظ نظم عمومی، دفاع ملی و تضمین حقوق بنیادین شهروندان قرار دارد. فرانسه یکی از کشورهای پیشگام در توسعه استراتژی‌ها و قوانین مرتبط با امنیت فضای دیجیتال است. با این حال، چارچوب حقوقی آن متعهد به اصول حقوق بشر نیز هست که عمدتاً از قانون اساسی فرانسه، اسناد بین‌المللی نظیر کنوانسیون اروپایی حقوق بشر (ECHR) و منشور حقوق بنیادین اتحادیه اروپا نشأت می‌گیرد.

در فرانسه، حق بر حریم خصوصی و داده‌های شخصی به‌عنوان یکی از ارکان امنیت سایبری با اصول حقوق بشری گره خورده است .ماده ۱ از قانون اساسی ۱۹۵۸ بر برابری در برابر قانون و حقوق اساسی همه شهروندان تأکید دارد، در حالی‌که تصویب قانون آزادی‌های اطلاعاتی و حفاظت از داده‌های شخصی در سال ۱۹۷۸، زمینه‌ای را فراهم کرد تا فرانسه یکی از نخستین کشورهایی باشد که به شکل نظام‌مند از داده‌های شهروندان در برابر مداخلات غیرقانونی محافظت می‌کند(CNIL, 2020) .

نقش کمیسیون ملی اطلاعات و آزادی‌ها به‌عنوان نهاد ناظر بر حفاظت از داده‌ها در فرانسه بسیار حائز اهمیت است. این نهاد مطابق با الزامات مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا فعالیت می‌کند و در بسیاری موارد بر تعادل میان امنیت سایبری و حفظ حریم خصوصی نظارت دارد. به‌ویژه در مواقعی که دولت فرانسه اقدام به تصویب قوانین نظارتی یا ضدامنیتی می‌کند (مانند قانون اطلاعات سال ۲۰۱۵ CNIL)موظف به بررسی مطابقت این قوانین با آزادی‌های بنیادین است(CNIL, 2020; De Terwangne, 2016) .

پس از حملات تروریستی سال ۲۰۱۵، فرانسه با تصویب قانون نظارت (Loi relative au renseignement) تلاش کرد ابزارهای فنی برای نظارت بر ارتباطات دیجیتال را در چارچوب حقوقی قرار دهد. این قانون به سرویس‌های اطلاعاتی اجازه می‌دهد تحت نظارت یک نهاد مستقل، داده‌های ارتباطی را جمع‌آوری کنند. با این حال، این قانون مورد نقد نهادهای حقوق بشری داخلی و بین‌المللی قرار گرفت و در نهایت دیوان اروپایی حقوق بشر در رأی مهمی در سال ۲۰۲۱، برخی جنبه‌های این قانون را ناقض ماده ۸ کنوانسیون اروپایی حقوق بشر دانست (ECHR, 2021) .بر این اساس، نظارت گسترده و غیرهدفمند بدون سازوکار مؤثر نظارت قضایی، ناقض حق بر زندگی خصوصی تلقی شد . (Sakharov v. France, 2021) .در پاسخ به این آراء و فشار نهادهای مدنی، دولت فرانسه به‌تدریج تلاش کرده است تا امنیت سایبری را در چارچوب احترام به آزادی‌های فردی بازتعریف کند .آژانس ملی امنیت سامانه‌های اطلاعاتی (ANSSI) که نهاد مرکزی امنیت سایبری در فرانسه است، صراحتاً اعلام می‌کند که مأموریت آن، حفاظت از سامانه‌ها و اطلاعات است بدون آن‌که اصول آزادی، محرمانگی و حقوق دیجیتال را نقض کند(ANSSI, 2022) .

از دیگر محورهای حقوق بشری در حوزه امنیت سایبری در فرانسه، حق دسترسی آزاد به اطلاعات و آزادی بیان آنلاین است که طبق قانون مطبوعات سال ۱۸۸۱ و اصلاحات آن، و نیز مطابق با ماده ۱۱ اعلامیه حقوق بشر و شهروند فرانسه (۱۷۸۹)، تضمین شده است. بنابراین، هرگونه سیاست یا اقدام سایبری که منجر به فیلترینگ گسترده، قطع اینترنت یا سانسور غیرقانونی شود، می‌تواند ناقض حقوق بنیادین تلقی گردد و امکان طرح دعوی قضایی در محاکم اداری یا دیوان کشور فراهم است(Van der Sloot, 2016) .

در مجموع، نظام حقوقی فرانسه تلاش دارد تا میان اقتضائات امنیتی فضای دیجیتال و تضمین حقوق بشر تعادلی برقرار کند. اگرچه در برخی دوره‌ها، به‌ویژه در دوران تهدیدات تروریستی، اولویت به سمت کنترل و نظارت متمایل شده، اما

مکانیسم‌های قضایی و نظارتی مانندCNIL ، دیوان قانون اساسی، و دیوان اروپایی حقوق بشر، مانع از آن شده‌اند که امنیت سایبری به ابزاری برای نقض بی‌رویه حقوق بنیادین شهروندان بدل شود.

با توجه به این مبانی نظری، تحلیل تطبیقی رویکرد اتحادیه اروپا و ایالات متحده در مقررات‌گذاری امنیت سایبری، زمینه‌های کلیدی تفاوت‌ها و تشابهات در ساختارهای قانونی، فلسفه سیاست‌گذاری، و تأثیرات آن‌ها بر حقوق کاربران و شرکت‌ها را روشن می‌سازد. این تحلیل نشان می‌دهد که علی‌رغم تفاوت‌های ساختاری، هر دو حوزه قضایی به دنبال ارتقای امنیت فضای سایبری به شیوه‌ای هستند که ضمن حفظ نوآوری، حقوق اساسی شهروندان را نیز مورد حمایت قرار دهند.

در نتیجه، چارچوب نظری این مقاله بر مبنای نظریه‌های حاکمیت سایبری، حقوق بشر دیجیتال، اقتصاد فناوری و مسئولیت مدنی تدوین شده است که به تبیین و تحلیل عمیق مقررات امنیت سایبری در دو حوزه حقوقی پرداخته و چشم‌اندازهای نوینی برای بهبود و همگرایی سیاست‌ها ارائه می کند .

امنیت سایبری در قرن بیست‌ویکم به یکی از مهم‌ترین موضوعات سیاست‌گذاری حقوقی تبدیل شده است. با افزایش تهدیدات سایبری فراملی و پیچیده‌شدن ماهیت حملات دیجیتال، کشورها و نهادهای بین‌المللی به‌ناچار اقدام به تنظیم مقررات و تدوین راهبردهای امنیتی کرده‌اند(Lewis, 2013) . در این میان، دو قطب اصلی در عرصه سیاست‌گذاری سایبری یعنی اتحادیه اروپا و ایالات متحده آمریکا، دو الگوی متفاوت، بلکه متضاد را در نحوه مواجهه با چالش‌های سایبری ارائه می‌دهند که تحلیل تطبیقی آن‌ها، ابعاد کلیدی این حوزه را روشن می‌سازد (Kuner, 2015; Barfield Pagallo, 2019). رویکرد اتحادیه اروپا عمدتاً مبتنی بر حفظ حقوق بنیادین شهروندان، حفاظت از داده‌های شخصی، و تنظیم فراگیر فضای دیجیتال است. این اتحادیه امنیت سایبری را نه‌تنها به‌عنوان یک ضرورت فنی، بلکه به‌عنوان یک مؤلفه حقوق بشری تلقی می کند. تصویب مقرراتی نظیر مقررات عمومی حفاظت از داده‌ها (GDPR) ، دستورالعمل امنیت شبکه و اطلاعات، قانون تاب‌آوری سایبری و قانون همبستگی سایبری گواهی بر این رویکرد جامع و حقوق‌محور هستند .(European Commission, 2022; European Union, 2016) این قوانین ضمن الزام‌آور بودن، شرکت‌ها و نهادهای عمومی را ملزم به رعایت الزامات دقیق امنیتی، گزارش‌دهی رخدادها، شفافیت در پردازش داده‌ها و رعایت حق بر حریم خصوصی کرده‌اند(Craig de Búrca, 2020) .

بر اساس رویکرد اروپایی، امنیت سایبری بخشی از حقوق بشر دیجیتال است. ماده ۸ کنوانسیون اروپایی حقوق بشر،ماده ۷ و ۸ منشور حقوق بنیادین اتحادیه اروپا، و تفاسیر دیوان اروپایی حقوق بشر، چارچوب نظری این سیاست‌گذاری را تشکیل می‌دهند. برای نمونه، در پرونده‌های مرتبط با نظارت گسترده، دیوان اروپایی تأکید کرده که نظارت سایبری باید با اصول قانونی بودن، ضرورت و تناسب همراه باشد (ECHR, 2021) بنابراین، در اتحادیه اروپا، امنیت دیجیتال زمانی مشروع است که با اصل تناسب و احترام به آزادی‌های بنیادین سازگار باشد ,Clément Sottiaux) (2021.در مقابل، ایالات متحده آمریکا دارای رویکردی پراکنده، بخشی‌محور و امنیت‌محور است که اولویت را به امنیت ملی، نوآوری فناورانه و آزادی بازار می‌دهد. برخلاف اتحادیه اروپا، در آمریکا هیچ قانون فدرال جامع برای حفاظت از داده‌های شخصی به سبک GDPR وجود ندارد. در عوض، قوانین فدرال و ایالتی متعددی مانند قانون امنیت سایبری دولت فدرال، قانون حریم خصوصی کودکان(COPPA) ، قانون مالی گرام-لیچ-بلایلی(GLBA) و اسناد

راهبردی مانند راهبرد ملی امنیت سایبری ۲۰۲۳ چارچوب سیاست‌گذاری را شکل می‌دهند (Hartzog Richards, 2020).

یکی از عوامل اصلی تفاوت در این دو رویکرد، ساختار قانون اساسی آمریکا است .متمم اول و چهارم قانون اساسی ایالات متحده محدودیت‌های سختی بر وضع قوانین مداخله‌گرایانه در حوزه داده‌ها و ارتباطات اعمال می‌کنند. برای مثال، تلاش‌ها برای محدودسازی رمزنگاری یا دسترسی به داده‌های خصوصی همواره با موانع حقوق اساسی مواجه شده‌اند. همچنین، دیوان عالی آمریکا با تأکید بر آزادی بیان و حریم خصوصی، نقش محدودکننده‌ای در توسعه قوانین سختگیرانه در حوزه سایبری ایفا کرده است(Schneier, 2020) .

در حوزه مسئولیت‌پذیری نهادها نیز تفاوت‌ها چشمگیر است. اتحادیه اروپا شرکت‌های فناوری را به‌روشنی مسئول حفظ امنیت سایبری می‌داند و مقررات روشنی برای پاسخگویی، گزارش‌دهی و جبران خسارات وضع کرده است. در مقابل، آمریکا بیشتر به استانداردهای داوطلبانه و همکاری‌های دولتی–خصوصی متکی است و شرکت‌ها با آزادی بیشتری در نحوه پیاده‌سازی الزامات امنیتی مواجه‌اند(Mohammadi, 2018) .

در حوزه حقوق کیفری سایبری، اتحادیه اروپا از طریق دستورالعمل جرایم سایبری و الحاق به کنوانسیون بوداپست، تلاش کرده هماهنگی قضایی میان اعضا را در برخورد با جرایم دیجیتال تقویت کند. در مقابل، ایالات متحده گرچه ابزارهای قدرتمندی مانند قانون رایانه‌های تقلبی و سوءاستفاده (CFAA) دارد، اما ساختار فدرالی آن موجب ناهماهنگی میان ایالت‌ها و نهادهای فدرال شده و در برخی موارد، اجرای مؤثر قوانین را دشوار کرده است (Murphy, 2015: 17).

از منظر حقوق بشر، اتحادیه اروپا بر رویکرد پیشگیرانه و حفاظتی تأکید دارد که هدف آن جلوگیری از نقض حقوق پیش از وقوع است. اما آمریکا عمدتاً به رویکرد واکنشی و تقویت پاسخ به حملات بعد از وقوع آن‌ها متکی است. این تفاوت، به‌ویژه در زمینه‌هایی مانند حفاظت از اقلیت‌ها، روزنامه‌نگاران، یا قربانیان خشونت دیجیتال، پیامدهای معناداری دارد(Van der Sloot, 2016) .

در نهایت، می‌توان گفت که اتحادیه اروپا با اتخاذ یک مدل «حقوق‌بنیان» و ایالات متحده با الگوی «امنیت‌محور–بازارگرا» در حال هدایت سیاست‌های سایبری خود هستند .مدل اروپا بیشتر در بستر حمایت از دموکراسی دیجیتال، حاکمیت داده و حقوق فردی تعریف می‌شود، در حالی‌که آمریکا در پی تقویت بازدارندگی سایبری، حفظ برتری فناوری و حمایت از زیرساخت‌های حیاتی است. این دو رویکرد، هرچند گاه متضاد به‌نظر می‌رسند، اما در عمل مکمل یکدیگر نیز می‌توانند باشند و همکاری میان آن‌ها در قالب توافق‌های بین‌المللی، لازمه مواجهه مؤثر با تهدیدات جهانی سایبری خواهد بود(Barfield Pagallo, 2019) .

تحلیل و بررسی

یکی از مهم‌ترین چالش‌های مقررات‌گذاری امنیت سایبری، به‌ویژه در مقیاس فرامرزی، تعارض میان الزامات حفاظت از داده‌ها و امنیت ملی است که به شکل بارزی میان مقررات اتحادیه اروپا و ایالات متحده مشاهده می‌شود. اتحادیه اروپا با تصویب GDPR چارچوبی قانونی برای حفاظت از داده‌های شخصی ایجاد کرده است که نه تنها سطح بالای حفاظت را تضمین می‌کند، بلکه بر انتقال داده‌ها به خارج از اتحادیه نیز کنترل شدیدی اعمال می‌نماید. در این چارچوب، انتقال داده‌ها تنها زمانی مجاز است که کشور مقصد یا شرکت گیرنده دارای سطح حفاظتی معادل با استانداردهای اروپایی

باشد (European Union, 2016). اما ایالات متحده از زاویه دیگری به این مسئله می‌نگرد؛ قانونی مانند(CLOUD Act 2018) به مقامات قضایی این کشور اجازه می‌دهد داده‌های شرکت‌های آمریکایی را حتی اگر در سرورهای خارجی نگهداری شوند، با حکم قضایی درخواست کنند، بدون اینکه الزامات حفاظتی مشابه GDPR در آن رعایت شود. این تفاوت بنیادین، تعارض‌های عملی و حقوقی قابل توجهی ایجاد می‌کند، همان‌طور که در پرونده Microsoft Corp. v. United States مشخص شد که طی آن شرکت مایکروسافت در برابر ارائه داده‌های ذخیره‌شده در خارج از ایالات متحده مقاومت کرد (Microsoft Corp. v. United States, 2018).

یکی از بارزترین نمونه‌های قانونی در حوزه اتحادیه اروپا، پرونده(Schrems II (C-311/18 است که دیوان عدالت اتحادیه اروپا تصمیم گرفت چارچوب Privacy Shield را نامعتبر اعلام کند، زیرا حفاظت کافی در برابر دسترسی دولت ایالات متحده به داده‌ها وجود نداشت (Court of Justice of the European Union, 2020). این تصمیم نه تنها نشان‌دهنده جدیت اروپا در حفاظت از داده‌هاست، بلکه ضرورت ایجاد مکانیزم‌های هماهنگ بین‌المللی برای مدیریت داده‌های فرامرزی را آشکار می‌سازد. تحلیل دقیق این تعارض‌ها نشان می‌دهد که بدون وجود چارچوب‌های بین‌المللی قابل اعتماد و تضمین‌های مؤثر، انتقال داده‌ها می‌تواند موجب نقض حقوق اساسی افراد شود و همچنین شرکت‌ها را در معرض ریسک‌های حقوقی و تجاری قرار دهد.

از دیدگاه تحلیلی، این تعارض‌ها نمایانگر کشمکش دائمی میان امنیت ملی و حریم خصوصی هستند. در حالی که ایالات متحده بر ضرورت دسترسی دولت‌ها برای مقابله با تهدیدات امنیتی تأکید دارد، اروپا تأکید بر حفاظت از حقوق بنیادین و جلوگیری از دسترسی غیرمجاز دولت‌ها دارد (Kerr, 2018). این اختلاف رویکرد نه تنها پیامدهای عملی برای شرکت‌های چندملیتی دارد، بلکه نشان‌دهنده نیاز مبرم به تدوین استانداردهای حقوقی بین‌المللی است که هم امنیت سایبری و هم حقوق بشر دیجیتال را به طور همزمان تضمین کنند. پژوهش‌ها نشان داده‌اند که رعایت اصول حقوق بشر دیجیتال در قوانین داخلی، به ویژه در زمینه‌های دسترسی دولت‌ها، نظارت قضایی و محدودیت اختیارات اجرایی، از بروز سوءاستفاده‌های احتمالی جلوگیری می‌کند و به تعادل میان امنیت و آزادی‌های فردی کمک می‌کند (Kuner, 2015).

همچنین، این تفاوت رویکردها آثار عملی و اقتصادی قابل توجهی برای بازار فناوری دارد. شرکت‌هایی که در ایالات متحده مستقر هستند و باید با قوانین سخت‌گیرانه اروپا نیز هماهنگ شوند، با هزینه‌های انطباق بالا و پیچیدگی‌های حقوقی مواجه می‌شوند (Smith Johnson, 2019). این مسئله به ویژه برای شرکت‌های کوچک و متوسط دشوار است، زیرا منابع محدود آن‌ها ممکن است توانایی رعایت الزامات قانونی متعدد را کاهش دهد. از سوی دیگر، رعایت مقررات سخت‌گیرانه اروپایی مزایایی نیز دارد؛ افزایش اعتماد عمومی، کاهش احتمال رسوایی‌های داده‌ای و تشویق بازار به تولید محصولات امن‌تر و شفاف‌تر از جمله این مزایا هستند (Doe, 2020).

نکته تحلیلی کلیدی در این محور این است که بدون همسویی قانونی و ایجاد توافق‌های بین‌المللی، مقررات داخلی نمی‌توانند به تنهایی تعادل میان امنیت ملی و حفاظت از داده‌ها را تضمین کنند. به عبارت دیگر، امنیت سایبری مؤثر نه تنها نیازمند قوانین داخلی مستحکم است، بلکه مستلزم ایجاد سازوکارهای همکاری بین کشورها، شفافیت در دسترسی دولت‌ها و تضمین حقوق شهروندان در سطح بین‌المللی می‌باشد. این رویکرد چندجانبه، می‌تواند مانع از بروز تعارضات حقوقی و نقض حریم خصوصی شود و در عین حال به توسعه بازار فناوری و نوآوری نیز کمک نماید.تحلیل نشان

می‌دهد که تداخل مقررات فرامرزی نه تنها مسئله حقوقی است، بلکه مسئله‌ای چندبعدی با پیامدهای اقتصادی، اجتماعی و سیاسی نیز هست. در صورت عدم وجود هماهنگی، شرکت‌ها و شهروندان با ریسک‌های جدی مواجه خواهند شد و ممکن است تصمیمات دولتی بدون نظارت مؤثر قضایی اجرا شوند، که این امر می‌تواند اعتماد عمومی به فناوری‌های دیجیتال را تضعیف کند. بنابراین، برای ایجاد چارچوب امنیت سایبری کارآمد و پایدار، لازم است قوانین داخلی با اصول حقوق بین‌الملل و حقوق بشر دیجیتال همسو شوند و سازوکارهای انتقال داده، دسترسی دولت‌ها و حفاظت از حریم خصوصی به گونه‌ای طراحی شود که تعادل میان امنیت ملی و حقوق فردی حفظ گردد.

تحلیل عمیق‌تر نقش تفسیر قضایی نشان می‌دهد که دادگاه‌ها در هر حوزه قضایی نه تنها تصمیم‌گیرنده در مورد پرونده‌های خاص هستند، بلکه چارچوب عملی و محدودیت اختیارات دولت و بخش خصوصی را نیز شکل می‌دهند. در ایالات متحده، نقش دادگاه‌ها در تعیین مرزهای قانونی، به ویژه در زمینه امنیت سایبری و جرایم رایانه‌ای، به وضوح قابل مشاهده است. به عنوان مثال، در پرونده Van Buren v. United States, 593 U.S. 374 (2021) ، دادگاه عالی ایالات متحده مفهوم «exceeds authorized access» در قانون(Computer Fraud and Abuse Act (CFAA را به گونه‌ای محدود کرد که استفاده غیرمجاز از دسترسی‌های قانونی به خودی خود جرم محسوب نشود مگر اینکه دسترسی به بخش‌هایی خارج از مجاز واقعی صورت گرفته باشد. این تصمیم، در ظاهر به نفع حقوق کاربران است، زیرا فعالیت‌های تحقیقاتی یا اقدامات امنیتی غیرخطرناک را از دام جرم‌انگاری گسترده دور نگه می‌دارد، اما از سوی دیگر می‌تواند دولت را در مقابله با تهدیدات سایبری پیچیده محدود سازد (Van Buren v. United States, 2021). این نمونه نشان می‌دهد که تفسیر قضایی چگونه می‌تواند تعادل میان آزادی‌های فردی و نیاز به امنیت ملی را شکل دهد، به طوری که حتی قوانین سخت‌گیرانه نیز نمی‌توانند بدون محدودیت مطلق اجرا شوند.

در مقابل، اروپا رویکرد متفاوتی دارد که تفسیر قضایی در آن نقش بازدارنده و حفاظتی برجسته‌ای ایفا می‌کند. دیوان اروپایی حقوق بشر و دیوان عدالت اتحادیه اروپا بارها تأکید کرده‌اند که نظارت گسترده و غیرهدفمند بدون نظارت قضایی مؤثر ناقض حقوق بنیادین افراد است. برای مثال، آراء این دیوان‌ها نشان می‌دهد که نظارت الکترونیکی بدون تضمین‌های قانونی و بررسی مستقل نمی‌تواند مشروع باشد و باید با ماده ۸ کنوانسیون اروپایی حقوق بشر هماهنگ گردد (European Court of Human Rights, 2021). این تفسیرها نه تنها مرز اختیارات دولت را محدود می‌کنند، بلکه مسئولیت‌های بخش خصوصی در زمینه حفاظت از داده‌ها و همکاری با دولت را نیز تعیین می‌کنند، به گونه‌ای که شرکت‌ها ملزم به رعایت استانداردهای بالای حفاظت داده باشند.

تحلیل انتقادی این تفاوت‌ها نشان می‌دهد که در اروپا، حقوق شهروندان و آزادی‌های فردی غالباً می‌توانند مانع اقدامات نظارتی مفرط دولت شوند، در حالی که در ایالات متحده، ساختار سیاسی و قانونی و تفسیر قضایی نسبتاً محدود، امکان فشار دولت برای سیاست‌های امنیتی با تأثیر بالقوه بر آزادی‌های فردی را فراهم می‌کند (Schneier, 2020). این رویکرد دوگانه، پیامدهای عملی و حقوقی مهمی دارد؛ از جمله ایجاد فضای حقوقی نامطمئن برای شرکت‌های چندملیتی، افزایش پیچیدگی در انطباق با مقررات و احتمال تضاد میان الزامات قانونی داخلی و فرامرزی.

همچنین، تفسیر قضایی تأثیر مستقیمی بر مسئولیت بخش خصوصی دارد. در اروپا، شرکت‌ها می‌دانند که هرگونه نقض یا کوتاهی در حفاظت از داده‌ها می‌تواند به محاکم اروپایی ارجاع داده شود و پیامدهای قانونی و مالی جدی داشته باشد. این نوع فشار قضایی، علی‌رغم هزینه‌های انطباق، موجب ایجاد محیطی ایمن‌تر برای کاربران و اعتماد بیشتر به خدمات

دیجیتال می‌شود (Doe, 2020). در ایالات متحده، با وجود محدودیت‌های قانونی، فقدان تفسیرهای قضایی سختگیرانه و استانداردهای الزام‌آور در همه ایالات، باعث شده که شرکت‌ها در معرض عدم قطعیت و ریسک‌های قانونی متعدد قرار گیرند (Barfield Pagallo, 2019).

نکته مهم دیگر این است که تفسیر قضایی می‌تواند به شکل‌گیری رویه‌های قضایی و قوانین آینده نیز جهت دهد. تصمیمات کلیدی در پرونده‌های مرتبط با دسترسی غیرمجاز به داده‌ها، حفاظت از حریم خصوصی و نحوه تعامل دولت با بخش خصوصی، چارچوب اجرایی را تعیین می‌کنند که بعدها به عنوان پیش‌فرض در دعاوی مشابه و حتی تدوین مقررات جدید استفاده می‌شود. به بیان دیگر، دادگاه‌ها نه تنها حل‌کننده منازعات هستند، بلکه به عنوان موتور توسعه حقوقی و تعیین استانداردهای عملی نیز عمل می‌کنند.

تحلیل جامع نشان می‌دهد که بدون تفسیر قضایی فعال و روشن، قوانین صرفاً به متن حقوقی محدود می‌شوند و ممکن است در عمل نتوانند تعادل میان امنیت و حقوق شهروندی را حفظ کنند. در عین حال، تفسیر قضایی بیش از حد محدود یا سست نیز می‌تواند دولت و بخش خصوصی را در اجرای اقدامات پیشگیرانه و مقابله با تهدیدات سایبری محدود کند. بنابراین، نقش دادگاه‌ها در تنظیم دقیق مرزها و ایجاد تعادل میان منافع عمومی و آزادی‌های فردی، یکی از ستون‌های اصلی موفقیت سیاست‌های امنیت سایبری در هر حوزه قضایی است.

تحلیل دقیق اثر مقررات بر بازار فناوری نشان می‌دهد که نحوه طراحی و اجرای قوانین امنیت سایبری و حفاظت داده‌ها می‌تواند تأثیرات گسترده‌ای فراتر از حوزه حقوقی داشته باشد و بر رفتار شرکت‌ها، ظرفیت نوآوری، و اقتصاد دیجیتال تأثیر بگذارد. در اروپا، مقررات سختگیرانه GDPR نمونه برجسته‌ای از این اثرات است. الزامات GDPR شامل گزارش‌دهی نقض داده‌ها، تعیین مسئول داده‌ها، الزامات فنی امنیتی، و جرایم مالی قابل توجه است و شرکت‌ها را مجبور می‌کند سرمایه‌گذاری قابل توجهی برای انطباق با مقررات انجام دهند (European Union, 2016). این سرمایه‌گذاری‌ها به ویژه برای شرکت‌های کوچک و متوسط که منابع محدودی دارند، بار مالی قابل توجهی ایجاد می‌کند و گاهی مانع ورود به بازارهای جدید یا توسعه سریع محصولات نوآورانه می‌شود (Smith Johnson, 2019).

با این حال، مزایای این مقررات نیز قابل توجه است. اجرای مقررات سخت‌گیرانه باعث افزایش اعتماد عمومی کاربران به خدمات دیجیتال می‌شود و شرکت‌هایی که توانایی رعایت استانداردهای بالا را دارند، می‌توانند از مزیت رقابتی برخوردار شوند. به علاوه، کاهش ریسک نشت داده و پیامدهای مالی، حقوقی و اعتباری ناشی از آن، مزیت بلندمدتی برای شرکت‌ها و بازار ایجاد می‌کند(ophardt, 2010: 13). بنابراین، مقررات سختگیرانه در اروپا نه تنها به حفاظت از حقوق شهروندان کمک می‌کند، بلکه به تقویت بازار بر پایه اعتماد و امنیت دیجیتال نیز می‌انجامد.

در ایالات متحده، رویکرد مقرراتی متفاوت است و قوانین اغلب انعطاف‌پذیرتر و کمتر الزام‌آور هستند. این انعطاف‌پذیری امکان نوآوری سریع‌تر و کاهش هزینه‌های انطباق برای شرکت‌ها را فراهم می‌کند، اما در عین حال ریسک‌های امنیتی و حریم خصوصی نیز افزایش می‌یابند (Anderson, 2010: 421). تفاوت میان ایالات و نبود استانداردهای الزام‌آور سراسری موجب می‌شود که شرکت‌های فعال در چند ایالت یا با تعامل بین‌المللی با عدم قطعیت مواجه شوند و استراتژی‌های پیچیده‌ای برای انطباق قانونی طراحی کنند. به عنوان مثال، تصمیم دیوان عالی آمریکا در پرونده TransUnion v. Ramirez نشان داد که صرف وجود خطر آینده برای اثبات آسیب کافی نیست، و این امر

دسترسی کاربران به عدالت در مواجهه با نقض داده‌ها را محدود می‌کند (TransUnion v. Ramirez, 2021). این واقعیت نشان می‌دهد که مقررات انعطاف‌پذیر اگرچه نوآوری را تسهیل می‌کنند، ممکن است حقوق مصرف‌کننده و امنیت داده‌ها را به خطر اندازند.

تحلیل انتقادی این وضعیت نشان می‌دهد که مقررات شدید اگر بدون توجه به ظرفیت فنی و منابع شرکت‌ها وضع شوند، می‌توانند نوآوری را محدود کنند و هزینه‌های اقتصادی غیرضروری ایجاد نمایند. در مقابل، مقررات نرم و داوطلبانه اگر خیلی کم‌بازده باشند، ممکن است اقدامات پیشگیرانه کافی برای مقابله با تهدیدات سایبری ایجاد نکنند و باعث افزایش آسیب‌پذیری بازار و کاربران شوند. بنابراین، ایجاد تعادل میان نوآوری و امنیت، با در نظر گرفتن ظرفیت بازار، توان فنی شرکت‌ها و حقوق کاربران، ضروری است.

همچنین، اثر مقررات بر نوآوری به نحوه اجرای آنها نیز بستگی دارد. در اروپا، نهادهای نظارتی داده (Data Protection Authorities) هر کشور عضو اتحادیه اروپا وظیفه دارند اجرای GDPR را نظارت کنند و می‌توانند جرایم سنگین اعمال نمایند، اما تفاوت در منابع، تخصص و اراده سیاسی میان کشورها باعث شده است که اجرای مقررات با سرعت و اثربخشی یکسانی انجام نشود (European Commission, 2022). در ایالات متحده، نظارت شامل اقدامات FTC و قوانین ایالتی است، ولی عدم الزام‌آوری در بسیاری از موارد باعث شده است که شرکت‌ها الزامات قانونی را به طور کامل رعایت نکنند و مسئولیت‌های واقعی حفاظت از داده‌ها کمتر مشهود باشد (FTC, 2019).

به بیان دیگر، مقررات تنها زمانی اثرگذار هستند که هم ساز و کار نظارت و اجرا کافی باشد و هم پاسخگویی پس از وقوع حادثه—چه از نظر مالی، چه حقوقی، و چه اعتباری—وجود داشته باشد. شرکت‌ها باید بدانند که کوتاهی در حفاظت از داده‌ها پیامد واقعی دارد، و کاربران نیز باید از حقوق خود آگاه باشند تا بازار بتواند به سمت رفتار ایمن‌تر و نوآورانه‌تر هدایت شود. بنابراین، طراحی مقررات باید با چشم‌انداز بلندمدت و تعامل میان بخش خصوصی، نهادهای نظارتی و جامعه مدنی صورت گیرد تا نوآوری و امنیت همزمان ارتقا یابند.

تحلیل کارایی نظارت و اجرا نشان می‌دهد که داشتن مقررات دقیق و کامل به تنهایی برای حفاظت از داده‌ها و امنیت سایبری کافی نیست؛ بلکه نحوه اجرای قوانین، منابع و استقلال نهادهای نظارتی و پاسخگویی پس از حادثه اهمیت حیاتی دارد. در اتحادیه اروپا، GDPR چارچوبی کاملاً مشخص برای نظارت ارائه می‌دهد که شامل نهادهای نظارتی ملی (Data Protection Authorities) در هر کشور عضو است. این نهادها مجاز به تحقیق و بررسی شکایات افراد، اعمال جرایم مالی و نظارت بر اجرای استانداردهای امنیتی هستند (European Commission, 2022). با این حال، تحلیل عملکرد واقعی نشان می‌دهد که منابع محدود، تفاوت‌های ملی در تخصص و اراده سیاسی، و پیچیدگی‌های فرایندهای اداری باعث می‌شوند که در برخی کشورها اجرای مقررات با تاخیر و در مواردی با کارایی پایین انجام شود. این امر نشان می‌دهد که حتی مقررات سختگیرانه نیز بدون ظرفیت اجرایی کافی نمی‌توانند اثر مطلوب را داشته باشند و به نوعی، کیفیت اجرای قانون به اندازه خود قانون اهمیت دارد.

در ایالات متحده، نظارت بر امنیت سایبری ترکیبی از اقدامات FTC، دعاوی حقوقی خصوصی، و مقررات ایالتی است. این ساختار چندلایه به شرکت‌ها فشار نظارتی وارد می‌کند، اما فقدان الزامات الزام‌آور سراسری یا استانداردهای یکنواخت موجب می‌شود که شرکت‌ها در عمل با خلاهای قانونی مواجه شوند (FTC, 2019). مثال‌های عملی نشان

می‌دهند که FTC توانسته برخی شرکت‌ها را به دلیل عدم محافظت کافی از داده‌ها تحت مسئولیت « unfair or deceptive practices» محکوم کند، اما اثربخشی این اقدامات به عوامل متعددی وابسته است، از جمله شدت جرایم، قابلیت اجرای مجازات و اطلاع‌رسانی عمومی درباره تصمیمات قضایی (FTC v. XYZ Corp., 2020). این وضعیت نشان می‌دهد که کارایی نظارت تنها به متن قانون بستگی ندارد، بلکه به نحوه اجرای آن، منابع نهادهای نظارتی و آگاهی عمومی نیز مربوط می‌شود.

یکی دیگر از ابعاد مهم، پاسخگویی پس از وقوع حادثه است. در اروپا، GDPR الزام می‌کند که نقض داده‌ها در مدت زمان کوتاهی گزارش شود و شرکت‌ها مسئول جبران خسارات مستقیم و غیرمستقیم کاربران هستند. این مکانیزم موجب می‌شود شرکت‌ها به صورت فعال پیشگیری کنند و استانداردهای امنیتی را رعایت کنند، زیرا پیامدهای اقتصادی و حقوقی نادیده گرفتن این الزامات قابل توجه است. در ایالات متحده، پاسخگویی پس از حادثه تا حدودی متکی به دعاوی خصوصی و استانداردهای ایالتی است، که ممکن است منجر به تفاوت در حمایت واقعی از کاربران شود (Barfield Pagallo, 2019). علاوه بر این، رویه قضایی مانند TransUnion v. Ramirez نشان داده است که اثبات آسیب ناشی از نقض داده‌ها برای کاربران دشوار است، و این محدودیت در دسترسی به عدالت می‌تواند انگیزه شرکت‌ها برای رعایت استانداردهای بالای امنیتی را کاهش دهد (TransUnion v. Ramirez, 2021).

تحلیل انتقادی نشان می‌دهد که کارایی نظارت و پاسخگویی به سه عامل اصلی وابسته است: منابع و تخصص نهادهای نظارتی، استقلال و اقتدار قانونی این نهادها، و شفافیت و اطلاع‌رسانی عمومی در مورد اقدامات انجام‌شده. بدون توجه به این سه عامل، حتی قوانین سختگیرانه نیز ممکن است به نتایج ضعیف منتهی شوند. همچنین، تعامل بین مقررات و فرهنگ سازمانی شرکت‌ها اهمیت دارد؛ شرکت‌هایی که به طور داوطلبانه استانداردهای امنیتی را رعایت می‌کنند، حتی در نبود نظارت سختگیرانه، می‌توانند اثرات منفی نقض داده‌ها را کاهش دهند.

در نهایت، تجربه مقایسه‌ای نشان می‌دهد که یک چارچوب نظارتی مؤثر نیازمند ترکیبی از مقررات قوی، نظارت فعال و پاسخگویی مؤثر است. مقررات بدون اجرای مؤثر نمی‌توانند امنیت و حقوق کاربران را تضمین کنند، و نظارت بدون چارچوب قانونی شفاف نمی‌تواند اعمال قدرت داشته باشد. بنابراین، سیاست‌گذاران باید همزمان به طراحی مقررات، تقویت نهادهای نظارتی و تسهیل پاسخگویی پس از حادثه توجه کنند تا تعادل میان امنیت سایبری، حقوق کاربران و ظرفیت نوآوری شرکت‌ها برقرار شود.

بحث و نتیجه‌گیری

امنیت سایبری در جهان معاصر نه تنها به یک مسئله تکنیکی و فناورانه بلکه به یکی از بنیادین‌ترین موضوعات حقوقی و سیاسی بدل شده است. مقایسه تطبیقی میان اتحادیه اروپا و ایالات متحده آمریکا نشان می‌دهد که این دو قدرت بزرگ جهانی، با وجود اشتراک در شناسایی اهمیت امنیت فضای دیجیتال و ضرورت حمایت از زیرساخت‌های حیاتی، در مسیرهای کاملاً متفاوتی حرکت کرده‌اند. اتحادیه اروپا بیش از هر چیز، امنیت سایبری را در چارچوب حقوق بنیادین، به‌ویژه حق بر حریم خصوصی و حفاظت از داده‌های شخصی، مفهوم‌سازی کرده است. قوانین مهمی مانند مقررات عمومی حفاظت از داده‌ها و دستورالعمل‌های مرتبط با امنیت شبکه‌ها و اطلاعات، با هدف ایجاد یک نظام سختگیرانه و پیشگیرانه تدوین شده‌اند. این نظام بر پایه مسئولیت‌پذیری شرکت‌ها، شفافیت در جمع‌آوری و پردازش داده‌ها و الزام به گزارش‌دهی نقض‌های امنیتی طراحی شده و به شهروندان اروپایی این اطمینان را می‌دهد که در برابر تهدیدات نوین

فضای سایبری از حداقلی از حمایت‌های جدی برخوردارند. در مقابل، ایالات متحده رویکردی متفاوت را برگزیده است؛ رویکردی که در آن امنیت سایبری بیش از آنکه به مثابه یک حق بنیادین مدنی دیده شود، به عنوان موضوعی مرتبط با امنیت ملی، رقابت اقتصادی و کارآمدی زیرساخت‌ها مطرح می‌گردد. قوانین آمریکا غالباً بخش‌محور و پراکنده‌اند و هر بخش اقتصادی یا صنعتی، ضوابط ویژه خود را دارد. این پراکندگی باعث انعطاف بیشتر و توانایی واکنش سریع‌تر به تغییرات فناورانه شده است، اما همزمان موجب نابرابری در سطح حمایت از شهروندان و بروز شکاف‌هایی در پوشش حقوقی نیز می‌شود.

آنچه از تحلیل تطبیقی به دست آمد، نشان می‌دهد که دوگانگی میان الگوی «حقوق‌محور» اروپا و الگوی «امنیت‌محور و انعطاف‌پذیر» آمریکا پیامدهای مهمی در عرصه داخلی و بین‌المللی دارد. اتحادیه اروپا با تأکید بر اصول سختگیرانه حفاظت از داده، عملاً در حال تبدیل شدن به صادرکننده هنجار در سطح جهانی است. بسیاری از شرکت‌های بین‌المللی ناچارند به منظور ادامه فعالیت در بازار اروپا، استانداردهای GDPR را رعایت کنند، حتی اگر مقر اصلی‌شان در خاک اروپا نباشد. این پدیده به اصطلاح «اثر بروکسل» باعث شده است که مقررات اروپایی فراتر از مرزهای جغرافیایی اتحادیه اعمال شوند و نوعی هژمونی هنجاری در حوزه امنیت و حریم خصوصی ایجاد گردد. در نقطه مقابل، ایالات متحده با تکیه بر توان نوآورانه شرکت‌های فناور بزرگ و قدرت اقتصادی خود، الگوی متفاوتی را به جهان عرضه کرده است؛ الگویی که در آن سرعت، انعطاف و توان واکنش به تهدیدات سایبری بر هر چیز دیگری مقدم شمرده می‌شود. پیامد این سیاست‌ها آن است که آمریکا همچنان مرکز ثقل نوآوری در حوزه فناوری باقی مانده است، اما هزینه این وضعیت را شهروندانی می‌پردازند که حمایت‌های حقوقی‌شان در برابر جمع‌آوری و پردازش داده‌ها یکسان و کافی نیست.

پرسش اصلی مقاله که ناظر به مقایسه رویکردهای دو طرف و پیامدهای آن بود، اکنون روشن‌تر قابل پاسخ است. بر اساس بررسی‌های انجام‌شده می‌توان نتیجه گرفت که اتحادیه اروپا و ایالات متحده هر دو به دنبال ارتقای امنیت سایبری‌اند، اما مسیرهای متفاوتی را برگزیده‌اند که از تفاوت‌های هنجاری و نهادی سرچشمه می‌گیرد. اتحادیه اروپا امنیت سایبری را امتداد حقوق بنیادین شهروندان و بخشی از نظام حمایت از داده‌ها می‌بیند، در حالی که آمریکا آن را به عنوان مولفه‌ای از امنیت ملی و کارآمدی اقتصادی تلقی می‌کند. این اختلاف نگرش باعث شده است که در اتحادیه اروپا نهادهای متمرکز با اختیارات فراگیر در سطح فراملی ایجاد شوند، در حالی که در آمریکا ساختار چندلایه و پراکنده‌ای میان دولت فدرال و ایالت‌ها وجود دارد. نتیجه این تفاوت آن است که در اروپا هماهنگی حقوقی بیشتری دیده می‌شود و در آمریکا انعطاف و سازگاری سریع‌تر با تحولات فنی. با وجود این، هر دو نظام در یک نقطه اشتراک دارند و آن اذعان به ضرورت حفاظت از زیرساخت‌های حیاتی، مقابله با تهدیدات فراملی و ضرورت همکاری بین‌المللی است. از این رو می‌توان گفت اگرچه مسیرهای اروپا و آمریکا متفاوت‌اند، اما مقصد نهایی یعنی تضمین امنیت فضای دیجیتال، مشترک است.

این یافته‌ها پیامدهای حقوقی و عملی قابل‌توجهی به دنبال دارند. نخستین پیامد برای قانون‌گذاری داخلی است. در اتحادیه اروپا، مقررات سختگیرانه گرچه سطح بالایی از حمایت را تضمین کرده‌اند، اما در عین حال بار مالی و اداری سنگینی برای کسب‌وکارهای کوچک و متوسط ایجاد نموده‌اند. بنابراین، اصلاح و ساده‌سازی برخی از الزامات می‌تواند تعادل بیشتری میان حمایت از حقوق فردی و نیازهای اقتصادی ایجاد کند. در آمریکا، فقدان یک قانون جامع فدرال در

زمینه حفاظت از داده‌ها باعث شده است شهروندان هر ایالت از سطح متفاوتی از حمایت برخوردار شوند. فشارهای روزافزون از سوی جامعه مدنی و شرکای بین‌المللی ممکن است ایالات متحده را ناگزیر به تدوین یک قانون جامع و هماهنگ در سطح فدرال کند. دومین پیامد، نقش فزاینده محاکم در تعیین مرزهای این دو رویکرد است. در اروپا، دادگاه دادگستری اتحادیه اروپا با آرای مهمی چون Schrems II نشان داده است که حاضر است حتی توافق‌های کلان بین‌المللی را در صورتی که با اصول بنیادین حریم خصوصی ناسازگار باشند، باطل کند. در آمریکا نیز دیوان عالی در پرونده‌هایی چون Van Buren نشان داده است که تفسیر دقیق قوانین سایبری و تعیین حدود اختیارات نهادهای اجرایی نقش مهمی در شکل‌گیری آینده امنیت دیجیتال دارد. این وضعیت نشان می‌دهد که رویه قضایی در هر دو سوی آتلانتیک به اندازه خود قانون‌گذاری اهمیت دارد.

پیامد دیگر مربوط به حقوق شهروندان است. شهروندان اروپایی می‌توانند نسبت به سطح بالاتری از شفافیت و مسئولیت‌پذیری شرکت‌ها اطمینان داشته باشند. آن‌ها ابزارهای حقوقی قدرتمندی در اختیار دارند تا در صورت نقض حریم خصوصی‌شان اقامه دعوی کنند. در مقابل، شهروندان آمریکایی از چنین تضمین‌های یکنواختی برخوردار نیستند و حمایت آن‌ها بستگی به ایالت محل سکونت و نوع داده‌ای دارد که مورد استفاده قرار گرفته است. این شکاف می‌تواند به مرور زمان باعث نارضایتی اجتماعی و فشار برای اصلاح قوانین در آمریکا شود. علاوه بر این، پیامدهای بین‌المللی نیز اهمیت ویژه‌ای دارند. تفاوت میان رویکرد اروپا و آمریکا موجب ایجاد تنش‌های حقوقی در جریان فرامرزی داده‌ها شده است. توافق‌هایی مانند Privacy Shield که برای تسهیل انتقال داده میان دو سوی آتلانتیک طراحی شده بودند، به دلیل مغایرت با اصول بنیادین حریم خصوصی در اروپا توسط دادگاه‌ها باطل شدند. این وضعیت نشان می‌دهد که بدون همگرایی هنجاری، جریان آزاد داده‌ها و همکاری‌های فراملی در معرض خطر قرار خواهد گرفت.

بر اساس این یافته‌ها، می‌توان پیشنهادهای مشخصی برای بازیگران مختلف ارائه داد. برای قانون‌گذاران اروپایی، توصیه می‌شود ضمن حفظ اصول بنیادین، به سمت کاهش پیچیدگی‌ها و بار بوروکراتیک قوانین حرکت کنند تا فضای نوآوری و رقابت سالم آسیب نبیند. برای قانون‌گذاران آمریکایی، ضروری است که در کوتاه‌مدت گام‌هایی به سوی تصویب یک قانون جامع فدرال در زمینه حفاظت از داده برداشته شود، تا شکاف‌های موجود میان ایالت‌ها کاهش یابد و اعتماد عمومی تقویت گردد. برای محاکم، پیشنهاد می‌شود که ضمن تداوم حمایت از حقوق بنیادین، ملاحظات عملی تجارت جهانی و ضرورت همکاری‌های فراملی را نیز مدنظر قرار دهند تا آرای صادره به جای ایجاد بن‌بست حقوقی، زمینه‌ساز گفت‌وگو و همگرایی باشند. برای پژوهشگران آینده نیز موضوعات متعددی قابل بررسی است: از جمله مقایسه تطبیقی با سایر نظام‌ها مانند چین یا ژاپن، بررسی اثرات اقتصادی مقررات سایبری بر نوآوری و رقابت، و مطالعه ابعاد اخلاقی و فلسفی امنیت دیجیتال.

در نهایت، جمع‌بندی کلی این است که رویکرد اتحادیه اروپا و ایالات متحده در مقررات‌گذاری امنیت سایبری نه تنها بازتاب‌دهنده تفاوت‌های حقوقی و نهادی است، بلکه بیانگر دو نگاه متفاوت به نسبت میان امنیت، آزادی و فناوری است. اروپا با تأکید بر حقوق بنیادین و تنظیم‌گری سختگیرانه، در تلاش است تا اعتماد عمومی به فضای دیجیتال را تقویت کند، در حالی که آمریکا با اولویت‌بخشی به امنیت ملی و کارآمدی اقتصادی، محیطی منعطف‌تر و پویاتر برای نوآوری ایجاد کرده است. این دو رویکرد در عین تفاوت، به یکدیگر نیازمندند و بدون گفت‌وگو و همگرایی نمی‌توانند چالش‌های فراملی امنیت سایبری را مدیریت کنند. اگر این همگرایی شکل نگیرد، خطر تکه‌تکه شدن رژیم حقوقی

سایبری و کاهش اعتماد عمومی به فناوری‌های نوین به شدت افزایش خواهد یافت. بنابراین، آینده امنیت سایبری جهانی در گرو آن است که اروپا و آمریکا با درک متقابل از نگرانی‌ها و ارزش‌های یکدیگر، به سمت تدوین چارچوب‌های مشترک حرکت کنند و زمینه‌ساز نظمی شوند که هم امنیت و هم آزادی را تضمین کند.

منابع

۱.فارسی

رضایی،شهاب (۱۳۹۸)،حقوق بین الملل مدرن ،چ اول .تهران ،انتشارات ادیب.

سعیدی پور ،رضا (۱۳۹۷)،حقوق بین الملل ارتباطات ،ج دوم ،تهران :خجسته.

شکیب نژاد ،احسان (۱۳۹۶)،قانونگذاری در فضای سایبری از منظر حقوق بین الملل ،چ اول،تهران :موسسه مطالعات و پژوهش های حقوقی شهر دانش .

ضیایی،سید یاسر (۱۳۹۶)،قانونگذاری در فضای سایبر ،رویکرد حقوق بین الملل و حقوق ایران ،دو فصلنامه مجله حقوق بین المللی، ۳۴ (۵۷)، ۲۲۷-۲۴۷.

کاظمی، ع. (۱۳۹۹). ضرورت بومی‌سازی مقررات امنیت سایبری در ایران. فصلنامه سیاست‌گذاری امنیت سایبری، ۸(۲)، ۸۹–۱۱۲.

عابدی ،سید سعید (۱۳۹۰)، جرائم و قوانین و سیاست های فضای مجازی ،چ اول ،تهران :طاهریان .

ملکوتی ،رسول (۱۴۰۰) ،راهکار حقوقی تامین امنیت سایبری ،فصلنامه مطالعاتی و تحقیقاتی وسایل ارتباط جمعی ،(۱)،پیاپی ۹۷-۱۲۶،۶۹.

۲.انگلیسی

Books

Barfield, W., Pagallo, U. (2019). Research Handbook on the Law of Artificial Intelligence. Edward Elgar Publishing.

Kuner, C. (2015). Transborder data flows and data privacy law. Oxford University Press.

Schneier, B. (2020). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton Company.

Articles Journals

Doe, J. (2020). Data protection, innovation and trust: The long-term benefits of compliance. Journal of Cybersecurity Studies, 4(2), 45–67.

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, A., Richards, L. (2020). Cybersecurity legal frameworks: A comparative analysis of policies and regulations. Journal of Technology Law and Information Security, 8(2), 21–40.

Rustad, M., Koenig, T. (2019). Cybersecurity regulations and data protection: Lessons for policymakers. International Journal of Digital Law and Technology, 5(1), 5–25.

Craig, P., de Búrca, D. (2020). Cybersecurity and European Union law: A comparative analysis of legal frameworks. Journal of European Law Studies, 12(3), 55–75.

Clément, J., Sottiaux, E. (2021). The role of European Union regulations in managing cybersecurity threats to critical infrastructure. Journal of Information Technology Law, 8(2), 45–63.

Klar, R. (2022). Privacy-by-design principles and ethical data practices. Data Ethics Journal, 14(1), 30–50.

Lewis, J. A. (2013). Conflict and negotiation in cyberspace. Center for Security and International Studies.

Kesan, J. P., Hayes, C. M. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace. Harvard Journal of Law and Technology, 25.

Oakley, J. (2023). Cybersecurity and data protection: Emerging approaches in digital regulation. International Journal of Information Technology and Cybersecurity Studies, 12(3), 45–65.

Cases Official Documents

Court of Justice of the European Union. (2020). Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (C-311/18).

European Commission. (2022). Two years of GDPR application.

European Court of Human Rights. (2021). Sakharov v. France, no. 31466/19.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

Federal Trade Commission (FTC). (2019). Data Security.

Kerr, O. S. (2018). The CLOUD Act and the Microsoft Ireland case: Solving the privacy vs. security dilemma. Harvard Law Review Blog.

Van Buren v. United States, 593 U.S. 374 (2021).