تاریخ دریافت: ۱۴۰۴/۱۲/۲۰ تاریخ پذیرش: ۱۴۰۵/۰۲/۱۵ صفحه ۶۵ تا ۹۵

حریم خصوصی و امنیت سایبری؛ بررسی تطبیقی عملکرد پلیس فتا در ایران و آلمان از منظر امنیت سازمانی

محمد تجری[۱]، سید ابوالقاسم نقیبی[۲]، سیدمحمدصادق موسوی[۳]

چکیده

در دهه‌های اخیر، پیشـــرفت فناوری‌های دیجیتال و افزایش جرایم ســـایبری، نقش پلیس‌های فضای مجازی در حفاظت از امنیت ملی و کاربران اینترنت را پررنگ‌تر کرده اســـت. اســـتفاده گسترده از ابزارهای نوین نظارتی، چالش‌های جدی در زمینه حریم خصوصی ایجاد کرده و سوالاتی درباره تعادل میان امنیت و آزادی‌های فردی مطرح می‌کند. ایران و آلمان به عنوان دو کشور با رویکردهای متفاوت در حوزه امنیت سایبری و حفاظت از داده‌ها، نمونه‌ای مناسب برای مطالعه تطبیقی محسوب می‌شوند. بر این اساس، مساعی نویسندگان در پژوهش حاضر بحث و بررسی پیرامون نحوه استفاده پلیس فتا از فناوری‌های نوین در ایران و مقایسه آن با رویکردهای مشابه در آلمان، با تمرکز بر چالش‌های حریم خصوصی و پیامدهای بین‌المللی این اقدامات می‌باشد. سوال اصلی پژوهش این است که: «چگونه تفاوت‌های قانونی، فناورانه و سیاسی میان ایران و آلمان بر عملکرد پلیس‌های سایبری و رعایت حریم خصوصی شهروندان تأثیر می‌گذارد؟» در پایخ به این ســـوال اصلی به نظر می‌رســـد استفاده از فناوری‌های نوین توسط پلیس فتا در ایران نسبت به آلمان محدودتر بوده و چالش‌های حریم خصوصی بیشـــتری ایجاد می‌کند، که پیامدهای قابل توجهی در روابط بین‌الملل و تعاملات دیپلماتیک دارد. یافته‌های پژوهش با استفاده از روش تحقیق ترکیبی (تحلیل تطبیقی، بررســـی اســـناد قانونی، گزارش‌های رسمی پلیس دو کشور ایران و آلمان) و استفاده از بر نظریه‌های روابط بین‌الملل، به ویژه رویکرد امنیتی-سایبری و نظریه واقع‌گرایی (که به تحلیل تأثیر اقدامات سایبری کشورها بـــر منافـــع و امنیت ملی و تعاملات بین‌المللی می‌پردازد) نشـــان داد که آلمان با بهره‌گیری از فناوری‌های پیشرفته و چارچوب قانونی محافظتی، توانسته تعادل نسبی میان امنیت سایبری و حریم خصوصی برقرار کند و دسترسی غیرمجاز به داده‌های شهروندان را محدود نماید. در ایران، به دلیل محدودیت‌های قانونی و فناورانه، چالش‌های بیشـــتری در حفاظت از حریم خصوصی کاربران وجود دارد و گاه نگرانی‌های حقوق بشـــری و انتقادات بین‌المللی را به همراه دارد. همچنین تفاوت در ســـطح شفافیت و پاسخگویی پلیس‌ها موجب تفاوت چشـــمگیر در اعتماد عمومی به سیســـتم‌های سایبری در دو کشور شده است. علاوه بر این، این اختلافات، نحوه تعاملات و همکاری‌های بین‌المللی در زمینه مبارزه با جرایم سایبری را تحت تأثیر قرار می‌دهد و نشان می‌دهد که پذیرش استانداردهای جهانی بدون تطبیق قانونی و فنی امکان‌پذیر نیست. نتایج پژوهش نیز حاکی از آن است که بهبود عملکرد پلیس فتا و ارتقای استانداردهای حریم خصوصی نیازمند قوانین شفاف، ابزارهای فناورانه پیشرفته و تعاملات بین‌المللی مؤثر است.

واژگان کلیدی: پلیس فتا، حریم خصوصی، امنیت سایبری، روابط بین‌الملل، آلمان.

---

۱. گروه فقه و مبانی حقوق اسلامی،واحد علوم تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.

۲۲. گروه فقه و حقوق خصوصی، مدرسه عالی و دانشگاه شهید مطهری، تهران، ایران.(نویسنده مسئول).

رایانامه: Da.naghibi@motahari.ac.ir

۳. گروه فقه و حقوق خصوصی، مدرسه عالی و دانشگاه شهید مطهری، تهران، ایران.

Privacy and Cybersecurity, A Comparative Study of the Performance of Iran's FATA Police and Germany from an International Relations Perspective

Mohammad Tajari[1], Seyed Abolghasem Naghibi[2], Mohammad Sadegh Mousavi[3]

Abstract

In recent decades, advancements in digital technologies and the increase in cybercrime have elevated the role of cyber police in safeguarding national security and internet users. The extensive use of modern surveillance tools has raised significant challenges regarding privacy and has prompted questions about the balance between security and individual freedoms. Iran and Germany, as two countries with differing approaches to cybersecurity and data protection, provide a suitable basis for a comparative study. Accordingly, this research examines how Iran's FATA police utilize modern technologies and compares their approach with similar practices in Germany, focusing on privacy challenges and the international implications of these measures. The main research question is: "How do legal, technological, and political differences between Iran and Germany affect the performance of cyber police and the protection of citizens' privacy?" In response, it appears that Iran's use of modern technologies by the FATA police is more limited compared to Germany, creating greater privacy challenges with significant implications for international relations and diplomatic interactions. Using a mixed-methods approach including comparative analysis, review of legal documents, and official police reports from Iran and Germany and guided by international relations theories, particularly the cyber-security perspective and realism (which analyze the impact of cyber activities on national interests, security, and international interactions), the study found that Germany, through advanced technologies and protective legal frameworks, has maintained a relative balance between cybersecurity and privacy, limiting unauthorized access to citizens' data. In Iran, legal and technological constraints create greater challenges for protecting user privacy, occasionally generating human rights concerns and international criticism. Differences in transparency and accountability of police institutions also significantly affect public trust in cyber systems in both countries. Furthermore, these disparities influence international cooperation in combating cybercrime, demonstrating that global standards cannot be effectively implemented without legal and technical adaptation. The findings indicate that improving the performance of Iran's FATA police and enhancing privacy standards require transparent laws, advanced technological tools, and effective international collaboration.

Keywords: FATA Police, Privacy, Cybersecurity, International Relations, Germany .

---

1. Department of Jurisprudence and Fundamentals of Islamic Law, SrC, Islamic Azad University, Tehran, Iran.

2. Department of Jurisprudence and Private Law, Shahid Motahari University, Tehran, Iran. (Corresponding author). Email: Da.naghibi@motahari.ac.ir

3. Department of Jurisprudence and Private Law, Shahid Motahari University, Tehran, Iran.

مقدمه

در دهه‌های اخیر، تحولات سریع فناوری‌های دیجیتال و گسترش استفاده از اینترنت، نقش فضای سایبری در زندگی اجتماعی، اقتصادی و سیاسی کشورها را پررنگ‌تر کرده است. افزایش تعاملات آنلاین و تراکنش‌های دیجیتال موجب شکل‌گیری تهدیدات جدید سایبری شده است که می‌تواند امنیت ملی، حریم خصوصی کاربران و منافع اقتصادی کشورها را به خطر اندازد (اندرسن، ۱۴۰۰: ۶). در چنین شرایطی، پلیس‌های سایبری به‌عنوان نهادهای مسئول حفظ امنیت فضای مجازی، وظایف گسترده‌ای در پیشگیری و مقابله با جرایم اینترنتی بر عهده دارند. با این حال، استفاده از فناوری‌های نوین نظارتی و جمع‌آوری داده‌های دیجیتال، چالش‌های جدی در زمینه حریم خصوصی ایجاد کرده و تعادل میان امنیت و آزادی‌های فردی را به مسأله‌ای پیچیده تبدیل کرده است (محقق، ۱۴۰۴: ۱۱). در این رابطه، ایران و آلمان به‌عنوان دو کشور با رویکردهای متفاوت در زمینه امنیت سایبری و حفاظت از داده‌ها، نمونه‌ای مناسب برای مطالعه تطبیقی محسوب می‌شوند. در ایران، پلیس فتا با محدودیت‌های قانونی و فناورانه، تلاش می‌کند امنیت کاربران اینترنت را تأمین کند، اما در این مسیر با چالش‌های جدی حریم خصوصی مواجه است. در مقابل، آلمان با بهره‌گیری از قوانین محافظتی مانند BDSG[1] و استانداردهای GDPR[2] اتحادیه اروپا، توانسته تعادل نسبی میان امنیت سایبری و حفظ حریم خصوصی شهروندان برقرار کند. این تفاوت‌ها موجب شده است که مطالعه تطبیقی میان ایران و آلمان، به‌ویژه از منظر روابط بین‌الملل، بتواند چارچوبی مفید برای تحلیل پیامدهای حقوقی، تکنولوژیک و دیپلماتیک اقدامات سایبری ارائه دهد.

همانگونه که در فوق تبیین شد، رشد سریع فناوری‌های دیجیتال و گسترش تهدیدات سایبری، نقش پلیس‌های سایبری را در تضمین امنیت دیجیتال شهروندان بیش از پیش برجسته کرده است. در چنین شرایطی، چگونگی استفاده از ابزارهای فناورانه توسط پلیس سایبری و میزان انطباق آن با اصول حریم خصوصی به مسئله‌ای بنیادین در حکمرانی فضای مجازی تبدیل

---

۱. این اصطلاح مخفف (Bundesdatenschutzgesetz)، قانون فدرال حفاظت از داده‌های آلمان است و چارچوب حقوقی نحوه جمع‌آوری، پردازش و نگهداری داده‌های شخصی در آلمان را مشخص می‌کند.

۲. این اصطلاح مخفف (General Data Protection Regulation)، قانون جامع حفاظت از داده‌های اتحادیه اروپا است که از سال ۲۰۱۸ اجرا می‌شود و یکی از سخت‌گیرانه‌ترین استانداردهای دنیا در زمینه حفظ حریم خصوصی و پردازش داده‌های شخصی است.

شـــده اســـت. بر این اساس، مســـأله اصلی پژوهش حاضر دلالت بر این موضوع دارد که استفاده از فناوری‌های نوین توسط پلیس فتا در ایران تا چه اندازه با رعایت حریم خصوصی کاربران مطابقت دارد و تفاوت‌های قانونی، فناورانه و سیاســـی میان ایران و آلمان چه تأثیری بر عملکرد پلیس‌های سایبری و حفاظت از اطلاعات شهروندان دارد. این مسئله زمانی اهمیت بیشتری می‌یابد که تفاوت الگوهای حکمرانی، میزان شفافیت نهادی، ساختارهای قانونی و سطح تعاملات بین‌المللی دو کشور در نظر گرفته شود. عملکرد پلیس سایبری نه تنها امنیت داخلی را تحت تأثیر قرار می‌دهد، بلکه پیامدهـــای فرامرزی، دیپلماتیک و هنجاری نیز ایجاد می‌کند و بر ظرفیت کشـــور در همگرایی با اســـتانداردهای جهانی اثر می‌گذارد. ازاین‌رو تبیین دقیق این مسئله برای شناخت جایگاه ایران و آلمان در عرصه امنیت سایبری و بررسی شکاف‌ها و فرصت‌های موجود ضروری است.

اهمیت این پژوهش در چند محور قابل تبیین اســـت. نخســـت، افزایش جرایم سایبری فرامرزی و حساســـیت جهانی نسبت به رعایت حریم خصوصی موجب شده است که عملکرد نهادهای سایبری کشـــورها در معرض ارزیابی بین‌المللی قرار گیرد. بررســـی کارآمدی پلیس فتا و میزان تطابق آن با اســـتانداردهای رایج، برای حفظ اعتماد عمومی و کاهش آســـیب‌پذیری‌های ملی ضروری است. دوم، پژوهش حاضر با تحلیل مقایسه‌ای میان ایران و آلمان می‌تواند شکاف‌های حقوقی، فناورانه و ساختاری ایران را شناسایی کرده و نشان دهد که این شکاف‌ها چگونه بر کارآمدی پلیس فتا و ادراک شهروندان از امنیت و حریم خصوصی اثر می‌گذارند. سوم، مطالعه رفتار سایبری دو کشور، امکان فهم پیامدهای بین‌المللی اقدامات سایبری ایران را فراهم می‌کند؛ از جمله تأثیر این اقدامات بر مشروعیت بین‌المللی، دیپلماسی دیجیتال و توان کشور در تعامل با نهادهای جهانی. مجموع این ضرورت‌ها نشان می‌دهد که پژوهش حاضر علاوه بر کمک به تقویت امنیت سایبری داخلی، می‌تواند شناخت روشن‌تری از موقعیت ایران در نظام بین‌المللی و مسیرهای ارتقای هم‌سویی با هنجارهای جهانی ارائه دهد.

بر این اساس، هدف نویسندگان در پژوهش حاضر، بررسی تطبیقی عملکرد پلیس فتا در ایران و آلمان از منظر امنیت سازمانی با تأکید بر مفاهیم حریم خصوصی و امنیت سایبری است. پرسش اصلی عبارت است از: «چگونه تفاوت‌های قانونی، فناورانه و سیاسی میان ایران و آلمان بر عملکرد پلیس‌های سایبری و رعایت حریم خصوصی شهروندان تأثیر می‌گذارد؟»

مبانی نظری

در فضای بین‌المللی امروز، مفهوم «امنیت» از معنای سنتی خود که بیشتر بر تهدیدات نظامی

متمرکز بود فراتر رفته و ابعاد جدیدی همچون امنیت سایبری، امنیت اطلاعات و امنیت انسانی را دربر گرفته است. در این میان، روابط بین‌الملل در عصر دیجیتال شاهد تحولی بنیادین در تعریف مفاهیم قدرت، حاکمیت و تهدید است. فضای سایبری اکنون نه تنها ابزاری برای ارتباط و توسعه اقتصادی، بلکه میدانی برای رقابت سیاسی و امنیتی میان کشورها محسوب می‌شود. در چنین بستری، نقش نهادهایی چون پلیس سایبری در هر کشور، به عنوان ابزار تحقق سیاست‌های امنیتی و حاکمیتی، اهمیتی دوچندان یافته است.

۱-۲- تعریف مفاهیم

۱. حریم خصوصی: حریم خصوصی به مجموعه‌ای از حقوق و آزادی‌های فردی اشاره دارد که بر اساس آن هر شخص اختیار کنترل اطلاعات، ارتباطات و فعالیت‌های شخصی خود را دارد. این مفهوم تضمین می‌کند که داده‌ها و رفتارهای فرد بدون اجازه، مورد دسترسی، نظارت یا انتشار قرار نگیرند. حریم خصوصی از بنیانی‌ترین اصول حقوق شهروندی و لازمه اعتماد در فضای دیجیتال است (دینگ[1]، ۲۰۲۴: ۱۱۷-۱۲۱).

۲. اعتماد: اعتماد به باورواطمینانی گفته می‌شود که افراد نسبت به صداقت، مسئولیت‌پذیری و پیش‌بینی‌پذیری یک نهاد یا سیستم دارند. در حوزه سایبری، اعتماد زمانی شکل می‌گیرد که کاربران اطمینان یابند داده‌هایشان به‌درستی محافظت می‌شود و نهادهای مسئول از آن سوءاستفاده نمی‌کنند. اعتماد سرمایه‌ای حیاتی برای حکمرانی دیجیتال و مشارکت شهروندان در خدمات آنلاین است (برندز[2] و همکاران، ۲۰۲۴: ۱۳-۱۶).

۳. ظرفیت فنی: ظرفیت فنی به میزان توانایی سازمان‌ها یا نهادها در استفاده، توسعه و مدیریت فناوری‌های موردنیاز برای اجرای وظایف خود اشاره دارد. این ظرفیت شامل زیرساخت‌های دیجیتال، نیروی انسانی متخصص، ابزارهای پیشرفته و توان واکنش سریع به تهدیدات است. هرچه ظرفیت فنی بالاتر باشد، کارآمدی، سرعت و دقت عملکرد سایبری نیز افزایش می‌یابد (هاکمه[3] و همکاران، ۲۰۲۴: ۷۱-۷۳).

۴. حقوق‌محوری: حقوق‌محوری رویکردی است که در آن اولویت تصمیم‌گیری‌ها و

---

1. Ding
2. Barends
3. Hakmeh

سیاســـت‌گذاری‌ها بر حفظ حقوق شـــهروندی، شفافیت، پاســـخ‌گویی و رعایت اصول قانونی اســـتوار اســـت. در این رویکـــرد، امنیت و فناوری باید در خدمـــت آزادی‌ها و حقوق بنیادین افراد باشـــد. حقوق‌محوری موجب افزایش اعتماد عمومی و هم‌سویی با استانداردهای جهانی می‌شود (هوگان[1] و همکاران، ۲۰۲۴: ۱۹۴-۱۹۶).

۵. امنیت‌محوری: امنیت‌محوری رویکردی است که در آن تأمین نظم، کنترل تهدیدات و حفظ ثبات در اولویت اصلی قرار دارد و سایر مؤلفه‌ها از جمله حریم خصوصی در نسبت با الزامات امنیتی تعریف می‌شـــوند. این رویکرد معمولاً منجر به تمرکز قدرت، نظارت گســـترده و تقدم امنیت ملی بر آزادی‌های فردی می‌شـــود. امنیت‌محوری در شـــرایط تهدید شدید مؤثر است، اما در بلندمدت می‌تواند چالش‌هایی برای مشـــروعیت و اعتماد اجتماعی ایجـــاد کند (اوتوکویا[2]، ۲۰۲۴: ۱۷۶۱-۱۷۶۳).

۲-۲- امنیت سایبری در روابط بین‌الملل

در روابـــط بین‌الملل، نظریه‌های مختلفی به تحلیل امنیت در عصر دیجیتال پرداخته‌اند. در این پژوهش، دو رویکرد اصلی مبنای تحلیل قرار می‌گیرد:

نظریـــه واقع‌گرایـــی[3]: واقع‌گرایان معتقدند که دولت‌ها بازیگران اصلی نظام بین‌الملل هســـتند و هـــدف اصلـــی آنان حفظ بقا و قدرت در برابر تهدیدات اســـت (محمـــود[4]، ۲۰۲۵: ۳۴). از منظر واقع‌گرایی، فضای ســـایبری نیز به عرصه‌ای جدید برای رقابت قدرت تبدیل شـــده است، جایی که کشورها برای حفظ منافع ملی خود، از ابزارهای سایبری از جمله نظارت دیجیتال، جمع‌آوری داده و کنترل اطلاعات استفاده می‌کنند. در این چارچوب، فعالیت پلیس فتا در ایران یا پلیس سایبری آلمان، جلوه‌ای از سیاست امنیت ملی است که هر دولت در راستای منافع خود به کار می‌گیرد.

نظریه امنیتی‌ســـازی[5]: بر اســـاس دیدگاه مکتب کپنهاگ، امنیت پدیده‌ای گفتمانی است که از طریق «امنیتی‌سازی» موضوعات غیرنظامی حاصل می‌شود. در این دیدگاه، دولت‌ها با طرح برخی مســـائل (مانند حریم خصوصی، داده‌های دیجیتال یا شبکه‌های اجتماعی) به‌عنوان تهدیدی برای

1. Hogan
2. Otukoya
3. Realism
4. Mahmood
5. Securitization Theory

امنیت ملی، اقدام به مشروعیت‌بخشـــی برای نظارت و کنتـــرل می‌کنند (دوراک[1]، ۲۰۲۴: ۱۶۳-۱۶۴). این رویکرد به‌ویژه در ایران مصداق دارد، جایی که نهادهای امنیتی و پلیسی، فعالیت‌های کاربـــران را ذیـــل حفظ امنیت ملی تعریف می‌کنند. در مقابل، در آلمان، فرآیند امنیتی‌ســـازی با محدودیت‌های قانونی و نظارت نهادهای مدنی همراه است تا مانع از نقض حقوق فردی شود.

۲-۳- رابطه امنیت و حریم خصوصی

یکی از چالش‌های اصلی در عصر دیجیتال، تعادل میان امنیت و حریم خصوصی است. بر اساس رویکردهای نظری موجود در روابط بین‌الملل، دو الگوی متفاوت در این زمینه قابل مشاهده است:

الگوی امنیت‌محور: در این الگو، که در کشورهای در حال توسعه از جمله ایران مشاهده می‌شود، امنیت ملی و ثبات سیاســـی در اولویت قرار دارد. دولت‌ها با توجیه مقابله با تهدیدات ســـایبری، اختیارات گسترده‌ای به پلیس سایبری برای رصد، کنترل و نظارت بر داده‌ها اعطا می‌کنند. در این حالت، حریم خصوصی به عنوان امری ثانویه در برابر امنیت تفسیر می‌شود.

الگوی حقوق‌محور: در کشـــورهای پیشرفته مانند آلمان، رویکرد غالب مبتنی بر امنیت انسانی و حقوق دیجیتال است. این دیدگاه که از نظریه‌های لیبرالی در روابط بین‌الملل الهام می‌گیرد، بر این باور است که امنیت واقعی زمانی تحقق می‌یابد که حقوق بنیادین شهروندان، از جمله حق بر حریـــم خصوصی، محفوظ بمانـــد. در این چارچوب، قوانین مانند GDPR نه تنها ابزار حفاظت از داده‌ها هستند، بلکه به‌عنوان سازوکار اعتمادسازی میان دولت و جامعه نیز عمل می‌کنند.

۲-۴- چارچوب نظری تعاملات بین‌المللی در حوزه سایبری

فضای ســـایبری به دلیل ماهیت فرامرزی خود، نیازمند همکاری‌های بین‌المللی برای مقابله با تهدیدات و جرایم اســـت. از منظر روابط بین‌الملل، همکاری‌های ســـایبری می‌تواند در سه سطح مورد بررسی قرار گیرد:

ســـطح ملی: هر دولت تلاش می‌کند ســـاختارهای قانونی و فنی لازم بـــرای مقابله با تهدیدات سایبری را ایجاد کند. در ایران، این نقش بر عهده پلیس فتا است؛ در حالی که در آلمان، چندین نهاد از جمله دفتر فدرال امنیت اطلاعات[2] و پلیس فدرال مسئولیت دارند.

---

1. Durak
2. BSI

سطح منطقه‌ای: در آلمان، همکاری‌های گسترده‌ای با اتحادیه اروپا در زمینه امنیت سایبری وجود دارد، در حالی که ایران فاقد چارچوب منطقه‌ای مؤثر در این حوزه است.

سطح بین‌المللی: کنوانسیون بوداپست درباره جرایم سایبری (۲۰۰۱) به عنوان نخستین معاهده بین‌المللی در این زمینه، مبنایی برای همکاری کشورهاست(مارکن[1]، ۲۰۲۴: ۸۷-۸۸). آلمان به این کنوانسیون پیوسته است اما ایران هنوز عضو آن نیست، که همین امر موجب محدودیت در تبادل داده‌ها و همکاری قضایی فرامرزی می‌شود.

۲-۵- پیوند نظریه واقع‌گرایی و امنیتی‌سازی با عملکرد پلیس سایبری

با ترکیب دو نظریه واقع‌گرایی و امنیتی‌سازی می‌توان درک عمیق‌تری از عملکرد پلیس سایبری در ایران و آلمان به دست آورد. در ایران، واقع‌گرایی دولتی و اولویت امنیت ملی، موجب شده است که حریم خصوصی در سطحی پایین‌تر از امنیت تلقی شود. در مقابل، در آلمان، هرچند واقع‌گرایی در سیاست‌های امنیتی نقش دارد، اما فرآیند امنیتی‌سازی از طریق مکانیسم‌های حقوقی و نظارتی کنترل می‌شود تا مانع از نقض حقوق شهروندان گردد. این تفاوت، بازتابی از دو نوع برداشت از امنیت در روابط بین‌الملل است: امنیت دولت‌محور در ایران و امنیت انسان‌محور در آلمان.

از طرفی، از منظر روابط بین‌الملل، نحوه برخورد کشورها با حریم خصوصی و امنیت سایبری، تأثیر مستقیم بر روابط دیپلماتیک و تصویر بین‌المللی آن‌ها دارد. کشورهایی که به رعایت حقوق دیجیتال متعهدند، در عرصه جهانی اعتبار و مشروعیت بیشتری کسب می‌کنند. در مقابل، کشورهایی که با محدودیت‌های حقوقی و شفافیت کمتر مواجه‌اند، معمولاً با انتقادات بین‌المللی در زمینه حقوق بشر و آزادی‌های دیجیتال روبه‌رو می‌شوند. بنابراین، چارچوب نظری این پژوهش تأکید دارد که سیاست‌های سایبری نه تنها بعد فنی یا امنیتی، بلکه بعدی کاملاً سیاسی و دیپلماتیک دارند که می‌تواند بر جایگاه بین‌المللی کشور تأثیرگذار باشد.

بر اساس مبانی نظری فوق، چارچوب مفهومی پژوهش به صورت زیر ارائه می‌شود:

حریم خصوصی دیجیتال: حق افراد برای کنترل اطلاعات شخصی خود در فضای مجازی.

امنیت سایبری: مجموعه اقدامات و سیاست‌هایی که برای حفظ یکپارچگی، محرمانگی و دسترسی‌پذیری داده‌ها انجام می‌شود.

پلیس فتا (در ایران): نهاد مسئول نظارت و مقابله با جرایم سایبری در ایران.

1. Marcen

پلیس سایبری فدرال (در آلمان): نهاد هماهنگ‌کننده اقدامات امنیتی و حفاظتی سایبری در آلمان.

روابط بین‌الملل: بستر تحلیل تعاملات دیپلماتیک و حقوقی کشورها در فضای سایبری.

روش‌شناسی تحقیق

روش تحقیق پژوهش حاضر به صورت ترکیبی طراحی شده است. ابتدا با استفاده از تحلیل تطبیقی، سیاست‌ها، قوانین و ابزارهای سایبری ایران و آلمان بررسی می‌شود. سپس با مطالعه اسناد قانونی و گزارش‌های رسمی پلیس دو کشور به ویژه در خلال سال‌های ۱۴۰۰ تا ۱۴۰۴ (۲۰۲۱ تا ۲۰۲۵ میلادی که در پژوهش حاضر نویسندگان از ۱۲ گزارش رسمی پلیس فتای ایران و پلیس فدرال آلمان بهره بردند) داده‌های مورد نیاز جمع‌آوری و تحلیل می‌شوند. در نهایت، چارچوب نظری تحقیق مبتنی بر نظریه‌های روابط بین‌الملل، به ویژه رویکرد امنیتی-سایبری و نظریه واقع‌گرایی، برای تحلیل تأثیر اقدامات سایبری کشورها بر امنیت ملی و روابط بین‌المللی به کار گرفته خواهد شد.

یافته‌ها و تجزیه‌وتحلیل داده‌ها

۳-۱- بررسی عملکرد پلیس فتا در ایران در موضوع حریم خصوصی و امنیت سایبری

در ایران، فضای مجازی به‌عنوان یکی از ابعاد نوین و حساس امنیت ملی تلقی می‌شود. از اوایل دهه ۱۳۹۰، سیاست‌گذاران کشور با درک تهدیدات و فرصت‌های ناشی از تحولات دیجیتال، اقدام به طراحی ساختارهایی برای مدیریت و کنترل فضای سایبری کرده‌اند. تأسیس نهادهایی مانند «پلیس فضای تولید و تبادل اطلاعات» (فتا) نقطه عطفی در این مسیر بود که هدف آن ایجاد سازوکارهایی برای نظارت، پیشگیری و مقابله با جرایم سایبری نظیر نفوذ، سرقت داده، کلاهبرداری آنلاین و نشر اطلاعات نادرست است (کمال، ۱۴۰۳: ۵۱). از طرفی، رشد سریع فناوری اطلاعات، افزایش کاربران شبکه‌های اجتماعی و وابستگی روزافزون نهادهای اقتصادی و حکومتی به بسترهای دیجیتال، سطح آسیب‌پذیری کشور را در برابر تهدیدات سایبری به‌شدت بالا برده است. در چنین شرایطی، امنیت سایبری نه‌تنها به مسئله‌ای فنی، بلکه به موضوعی راهبردی و سیاسی تبدیل شده است. با این حال، عملکرد و حدود اختیارات پلیس فتا و سایر نهادهای نظارتی، همواره محل بحث و مناقشه بوده است؛ زیرا گسترش کنترل و نظارت دولتی

در فضـــای مجازی می‌تواند با حقوق کاربـــران، حریم خصوصی و آزادی بیان در تعارض قرار گیرد (جوکار، ۱۴۰۳: ۲۷-۲۸).

از دیدگاه روابط بین‌الملل، این وضعیت را می‌توان در چارچوب روند جهانی امنیتی‌سازی فضای سایبری تحلیل کرد. در این روند، دولت‌ها با طرح فضای مجازی به‌عنوان تهدیدی برای ثبات ملی، مشـــروعیت لازم برای گسترش اختیارات نظارتی و محدودسازی جریان آزاد اطلاعات را به دست می‌آورنـــد (فولن و میبائور[1]، ۲۰۲۴: ۴۳۴-۴۳۵). در ایران نیـــز این رویکرد با گفتمان‌هایی مانند «صیانت از فضای مجازی» و «حفظ امنیت فرهنگی و اجتماعی» همراه شده است؛ گفتمانی که بر ضرورت پاسداری از ارزش‌ها و هویت ملی در برابر تهدیدات فرهنگی و سیاسی ناشی از جهانی‌شدن دیجیتال تأکید دارد. در مجموع، چالش اصلی سیاست سایبری ایران در یافتن تعادل میان امنیت و آزادی نهفته است؛ تعادلی که حفظ آن می‌تواند ضامن توسعه پایدار و اعتماد عمومی در فضای مجازی باشد (سهلانی، ۱۳۹۸: ۷۹-۸۳).

۳-۲- چارچوب قانونی و سیاست‌های ملی

پایه‌های قانونی فعالیت پلیس فتا در ایران به قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ بازمی‌گردد؛ قانونی که نقطه‌عطفی در تاریخ حقوق سایبری کشور به‌شمار می‌آید. این قانون برای نخستین بار در نظام حقوقی ایران، مفاهیم و مصادیق جدیدی مانند دسترسی غیرمجاز به سامانه‌های رایانه‌ای، شـــنود غیرقانونی داده‌های دیجیتال، تخریب یا اختلال در داده‌ها و انتشـــار محتوای مجرمانه در فضـــای مجـــازی را تعریف و جرم‌انـــگاری کرد. پیش از تصویب این قانون، نظام قضایی و پلیســـی کشـــور فاقد چارچوب مشخصی برای رســـیدگی به جرایم مرتبط با فناوری اطلاعات بود و همین امر موجب ســـردرگمی در برخورد با تخلفات نوظهور ســـایبری می‌شد (فرزین‌مهر، ۱۴۰۳: ۲۶). با وجود اهمیت قانون ۱۳۸۸، بســـیاری از پژوهشـــگران و کارشناسان معتقدند که این قانون از نظر دامنه، شـــفافیت و هم‌خوانی با اســـتانداردهای بین‌المللی با کاستی‌هایی مواجه است. برای نمونه، در مقایســـه با کنوانســـیون بوداپست درباره جرایم سایبری (۲۰۰۱) که سند پایه در سطح جهانی محســـوب می‌شود، قانون ایران فاقد مقررات صریح در زمینه حفاظت از داده‌های شخصی، حقوق کاربران در برابر نظارت دولتی، و ســـازوکارهای همکاری بین‌المللی اســـت. در نتیجه، اگرچه قانون جرایـــم رایانـــه‌ای چارچوبی مقدماتی برای مقابله با تهدیدات دیجیتال فراهم کرده، اما نتوانســـته

1. Foulon & Meibauer

تعادلی پایدار میان امنیت و آزادی‌های فردی در فضای مجازی ایجاد کند (بیات، ۱۴۰۳: ۶). در کنار این قانون، نهادهایی چون شورای عالی فضای مجازی و مرکز ملی فضای مجازی نقش کلیدی در سیاست‌گذاری کلان دارند. این دو نهاد به‌منزله بازوی راهبردی دولت، مسئول تدوین سیاست‌ها، مقررات و برنامه‌های کلان در حوزه فضای سایبری‌اند. اسناد بالادستی مانند «سند نظام جامع پیشگیری و مقابله با جرایم سایبری» و «سند طرح کلان و معماری شبکه ملی اطلاعات» بیانگر رویکرد ایران به تمرکزگرایی، حاکمیت داده و کنترل جریان اطلاعات هستند. در واقع، سیاست سایبری کشور عمدتاً بر حفظ امنیت ملی، صیانت فرهنگی و مدیریت زیرساخت‌های حیاتی متمرکز است (فاطمی‌خواه، ۱۴۰۲: ۶۰). ازسوی دیگر، عدم عضویت ایران درمعاهدات بین‌المللی همچون کنوانسیون بوداپست و فقدان توافق‌های دوجانبه مؤثر در زمینه همکاری‌های سایبری، باعث شده است که تعاملات قضایی و پلیسی کشور در سطح جهانی محدود باقی بماند. این موضوع پیامدهایی جدی بر مشروعیت بین‌المللی، اعتمادسازی دیجیتال و مبارزه مؤثر با جرایم فرامرزی دارد. بسیاری از جرایم سایبری ماهیت بین‌المللی دارند و بدون همکاری فرامرزی قابل پیگیری نیستند. در غیاب این همکاری‌ها، روند شناسایی و تعقیب مجرمان دشوار می‌شود و ایران در برخی پرونده‌ها با انزوای سایبری مواجه می‌گردد (سعیدی، ۱۴۰۳: ۲۹-۳۱).

از دیدگاه روابط بین‌الملل، این وضعیت نشانگر تعارض میان حاکمیت ملی و همکاری جهانی در فضای سایبری است. ایران، همانند بسیاری از کشورهای در حال توسعه، بر ضرورت حفظ کنترل داخلی بر داده‌ها و شبکه‌ها تأکید دارد؛ در حالی که نظم بین‌المللی سایبری بر مبنای اشتراک اطلاعات و همکاری فراملی شکل گرفته است. این دو رویکرد گاه در تضاد با یکدیگر قرار می‌گیرند و موجب شکاف میان نظام حقوقی داخلی و استانداردهای جهانی می‌شوند. در مجموع، سیاست سایبری ایران در مرحله‌ای گذار قرار دارد: از یک‌سو، نیاز به تقویت امنیت دیجیتال و مقابله با تهدیدات نوپدید احساس می‌شود؛ و از سوی دیگر، ضرورت تدوین قوانین جامع‌تر، شفاف‌تر و مبتنی بر حقوق کاربران مطرح است. آینده نظام حقوق سایبری کشور تا حد زیادی به توانایی آن در ایجاد توازن میان امنیت، حاکمیت و آزادی دیجیتال وابسته خواهد بود.

۳-۳- ساختار نهادی پلیس فتا

پلیس فضای تولید و تبادل اطلاعات (فتا) در سال ۱۳۹۰ به‌صورت رسمی و به‌عنوان یکی از زیرمجموعه‌های نیروی انتظامی جمهوری اسلامی ایران تأسیس شد. مأموریت اصلی این نهاد،

مطابق با اساســـنامه و بیانیه رســـمی تأســـیس آن، «تأمین امنیت فضای تولید و تبادل اطلاعات کشور» اعلام گردید. ایجاد این نهاد در پاسخ به رشد سریع استفاده از اینترنت، گسترش شبکه‌های اجتماعی و افزایش جرایم نوپدید سایبری مانند سرقت داده، کلاهبرداری آنلاین، هک سامانه‌های بانکی و نشـــر محتوای غیرقانونی بود. در واقع، فتا پاســـخی نهادی به نیاز کشـــور برای مدیریت و کنترل تهدیدات دیجیتال در عصر ارتباطات محسوب می‌شود (محقق، ۱۴۰۴: ۴۵-۴۷). ساختار پلیس فتا شـــامل واحدهای تخصصی در تمامی اســـتان‌ها، مراکز پاسخ‌گویی به جرایم سایبری، آزمایشـــگاه‌های تحلیل دیجیتال و بخش‌های فنی برای ردیابی و تحلیل رفتار مجرمان اینترنتی اســـت. در حوزه فنی، این نهاد از ابزارهایی مانند ســـامانه‌های مانیتورینگ ترافیک داده، تحلیل ردپـــای دیجیتال، رهگیری IP، بازیابی داده‌های حذف‌شـــده و پایش شـــبکه‌های اجتماعی بهره می‌برد. با وجود این، به دلیل محدودیت دسترســـی به فناوری‌های پیشرفته نظارتی، رمزنگاری و امنیت داده در ســـطح جهانی، بخشـــی از توان فتا به همکاری با سایر نهادهای امنیتی و اطلاعاتی کشـــور وابسته اســـت. این همکاری میان‌سازمانی، اگرچه ظرفیت عملیاتی فتا را افزایش داده، اما گاه موجب هم‌پوشانی وظایف و چالش در شفافیت عملکرد نیز شده است (آل رسول و مرشدی، ۱۴۰۳: ۷۸-۷۹).

از نظر عملکرد، فتا علاوه بر مقابله با جرایم فنی و اقتصادی ســـایبری (مانند نفوذ، ســـرقت داده و فیشـــینگ)، تمرکز ویژه‌ای بر جرایم اخلاقی و فرهنگی دارد. پیگیری پرونده‌هایی نظیر انتشـــار محتوای غیراخلاقی، فعالیت رســـانه‌های مخالف نظام یا مدیریت صفحات انتقادی در شـــبکه‌های اجتماعی، نشـــان‌دهنده پیوند این نهاد با گفتمان امنیت فرهنگی و صیانت از فضای مجازی است. به همین دلیل، برخی تحلیلگران معتقدند که پلیس فتا صرفاً یک نهاد انتظامی فنی نیست، بلکه ابزاری برای سیاســـت‌گذاری فرهنگی و کنترل اجتماعی نیز به شـــمار می‌رود (امیریان فارسانی و همکاران، ۱۳۹۶: ۲۴۴-۲۴۵).

از منظر روابط بین‌الملل و مطالعات امنیتی، ساختار و رویکرد فتا بازتابی از الگوی کلی سیاست ســـایبری ایران اســـت؛ الگویی که بر تمرکز قدرت، کنترل جریان اطلاعات و حفظ ثبات داخلی تأکید دارد. در این چارچوب، فضای مجازی به‌عنوان بخشـــی از حوزه امنیت ملی تعریف می‌شود و دولت تلاش می‌کند با گســـترش نظارت، از تهدیدات فرهنگی، سیاســـی و اطلاعاتی جلوگیری کند. با این حال، این رویکرد پرســـش‌هایی را درباره مرز میان امنیت ســـایبری و آزادی دیجیتال برانگیخته است.

۳-۴- حریم خصوصی و چالش‌های قانونی

یکی از محورهای مهم و مورد بحث در ایران، نبود قانون جامع و یکپارچه «حفاظت از داده‌های شخصی» است. در کشورهای پیشرفته مانند آلمان، قوانین صریحی برای حفاظت از داده‌ها وجود دارد و علاوه بر قانون ملی، مقررات عمومی اتحادیه اروپا[1] نیز اجرا می‌شود که چارچوب مشخص و شفافی برای دسترسی به اطلاعات کاربران و مسئولیت نهادهای دولتی فراهم می‌آورد. در ایران اما وضعیت متفاوت است و مقررات مربوط به داده‌ها پراکنده، ناقص و غیرسیستمی هستند؛ نتیجه آن، نبود شفافیت کافی در اختیارات پلیس فتا و سایر نهادهای امنیتی در دسترسی به داده‌های خصوصی کاربران است (حدیثی، ۱۴۰۳: ۳۳-۳۴). تحلیل برخی از گزارش‌های رسمی فتا نشان می‌دهد که بسیاری از اقدامات نظارتی، ردیابی و حتی توقیف حساب‌های کاربری، نه بر اساس دستور قضایی صریح، بلکه مبتنی بر مصوبات داخلی و دستورهای امنیتی انجام می‌شوند. این امر موجب شده تا چارچوب قانونی مشخصی برای تضمین حقوق کاربران و نظارت بر عملکرد نهادهای امنیتی وجود نداشته باشد. از دیدگاه حقوق دیجیتال و روابط بین‌الملل، این وضعیت باعث ایجاد نگرانی‌ها و انتقادات بین‌المللی شده است (هدائی، ۱۴۰۴: ۱۹). سازمان‌ها و نهادهای بین‌المللی، از جمله گزارشگران ویژه سازمان ملل، بارها هشدار داده‌اند که برخی اقدامات پلیس سایبری ایران می‌تواند با اصل تناسب در نظارت بر داده‌ها و حفاظت از حریم خصوصی کاربران در تضاد باشد. به بیان دیگر، فقدان قوانین شفاف و واحد در حوزه حفاظت از داده‌ها، نه تنها چالش داخلی برای مدیریت فضای مجازی ایجاد می‌کند، بلکه به اعتبار بین‌المللی کشور و تعاملات فرامرزی آن در حوزه سایبری نیز آسیب می‌رساند.

۳-۵- ابعاد دیپلماتیک و بین‌المللی

در سطح بین‌المللی، ایران رویکردی دوگانه دارد: از یک سو، در مجامع جهانی بر لزوم احترام به حاکمیت ملی در فضای مجازی تأکید می‌کند و هرگونه دخالت خارجی در زیرساخت‌های سایبری را مردود می‌داند؛ از سوی دیگر، تمایل به همکاری در زمینه مقابله با جرایم سایبری را ابراز می‌کند. با این حال، نبود اعتماد متقابل میان ایران و کشورهای غربی، و عدم عضویت در معاهدات بین‌المللی، مانع شکل‌گیری همکاری عملی مؤثر شده است (سلحشور، ۱۴۰۴: ۶۶-۶۷). از منظر نظریه واقع‌گرایی

1. GDPR

در روابط بین‌الملل، رفتار ایران در این حوزه را می‌توان بر اساس حفظ استقلال سایبری[1] خود از نفوذ و وابســـتگی به قدرت‌های فناوری تفســـیر نمود. بر این اساس، سیاست‌هایی چون توسعه شبکه ملی اطلاعات، بومی‌سازی پیام‌رسان‌ها، و محدودسازی دسترسی به پلتفرم‌های خارجی مورد تأکید است. با این حال، این سیاســـت‌ها پیامدهایی نیز دارند. کاهش اعتماد بین‌المللی، افزایش شـــکاف فناورانه با کشورهای توسعه‌یافته، و محدود شدن فرصت‌های همکاری در حوزه امنیت سایبری. در نتیجه، ایران از بســـیاری از پروژه‌های بین‌المللی در زمینه مدیریت بحران‌های ســـایبری، تبادل داده‌های تهدید[2] و آموزش نیروهای تخصصی محروم مانده است. از طرفی، تحلیل داده‌های منتشرشده از سوی فتا و مرکز پژوهش‌های مجلس نشـــان می‌دهد که بخش عمده‌ای از جرایم ســـایبری در ایران شامل کلاهبرداری اینترنتی، نفوذ به حســـاب‌های بانکی، فیشینگ و سوءاستفاده از داده‌های شخصی است. پلیس فتا در کشف بسیاری از این جرایم موفق عمل کرده و سامانه‌های پاسخ‌گویی (مانند سایت و تماس ۰۹۶۳۸۰) را فعال کرده است اما چالش اصلی، کمبود شفافیت، پاسخ‌گویی نهادی و نظارت مدنی است. در حالی که در کشـــورهای پیشرفته، فعالیت پلیس سایبری زیر نظر مراجع مستقل داده و نهادهای حقوق بشری قرار دارد، در ایران چنین ســـاختار نظارتی در عمـــل وجود ندارد. این امر منجر به افزایش نگرانی‌های عمومی در خصوص «نظارت گسترده دولتی» و تضعیف اعتماد کاربران به خدمات آنلاین شده است. از طرفی، از دیدگاه سیاستی، می‌توان گفت که عملکرد فتا در محور امنیت‌محور و بازدارنده موفق‌تر از محور حقوق‌محور و حمایتی از کاربران بوده است(ریاحی، ۱۴۰۳: ۵۰-۵۳). از منظر روابط بین‌الملل، این وضعیت بازتابی از سیاست کلی ایران در حوزه امنیت ملی است که در آن، فضای مجازی به‌عنوان جبهه‌ای از نبرد نرم و تهدیدات خارجی تلقی می‌شـــود. در نتیجه، امنیت ســـایبری بر حقوق دیجیتال اولویت یافته اســـت. با این حال، تجربه جهانی نشـــان می‌دهد که امنیت پایدار در فضای مجازی بدون اعتماد عمومی و همکاری بین‌المللی امکان‌پذیر نیســـت. بنابراین، در صورت اصلاحات قانونی (مانند تصویب قانون جامع حفاظت از داده‌ها)، تقویت نظارت مدنی، و گسترش تعاملات با نهادهای بین‌المللی، ایران می‌تواند ضمن حفظ استقلال سایبری، جایگاه خود را در نظام سایبری جهانی ارتقا دهد.

۳-۶- بررسی عملکرد پلیس آلمان در موضوع حریم خصوصی و امنیت سایبری

آلمان یکی از کشـــورهای پیشـــرو در زمینه سیاست‌گذاری و اجرای نظام‌های امنیت سایبری و

1. Cyber Sovereignty
2. Cyber Threat Intelligence

حفاظت از داده‌های شـــخصی در جهان اســـت. تجربه تاریخی این کشور در زمینه سوءاستفاده از داده‌ها در دوران آلمان شرقی و نازی‌ها، موجب شد که حساسیت اجتماعی و سیاسی بسیار بالایی نســـبت به حریم خصوصی و نظارت دولتی شکل گیرد. همین امر سبب شده تا آلمان امروز نه‌تنها به‌عنوان قدرت صنعتی، بلکه به‌عنوان الگوی حقوقی و سیاســـتی در حوزه حکمرانی ســـایبری و حفاظت از داده‌ها شناخته شود (انگرر[1]، ۲۰۲۴: ۳۷۱-۳۷۲). در سطح بین‌المللی، آلمان به‌عنوان یکی از اعضای فعال اتحادیه اروپا و ناتو، نقش مهمی در تعیین استانداردهای جهانی امنیت سایبری دارد. سیاست سایبری آلمان تلاش می‌کند میان سه عنصر کلیدی تعادل برقرار کند. نخست؛ حفظ امنیت ملی و مقابله با تهدیدات ســـایبری؛ دوم؛ احترام به حقوق بشر دیجیتال و آزادی‌های مدنی و سوم؛ تقویت همکاری‌های بین‌المللی برای مقابله با جرایم فرامرزی.

۳-۶-۱- چارچوب قانونی و سیاست‌های ملی

چارچوب قانونی حاکم بر امنیت ســـایبری و حریم خصوصی در آلمان بر پایه چند ســـند کلیدی استوار است:

نخست؛ قانون فدرال حفاظت از داده‌ها[2] مصوب سال ۲۰۱۷ و همسو با مقررات عمومی حفاظت از داده‌ها[3] در اتحادیه اروپا؛

دوم؛ قانون امنیت فناوری اطلاعات[4] که در ســـال ۲۰۱۵ به تصویب رســـید و در ســـال ۲۰۲۱ به نسخه دوم[5] ارتقا یافت؛

ســـوم؛ استراتژی امنیت ســـایبری ملی آلمان[6] که هر چهار ســـال یک‌بار به‌روزرسانی می‌شود و آخرین نسخه آن در سال ۲۰۲۱ منتشر شده است(اشنایدر[7]، ۲۰۲۵: ۹۱-۹۲). این مجموعه قوانین، نظامی چندسطحی را برای حکمرانی فضای مجازی ایجاد کرده است. بر اساس این نظام، حفاظت از داده‌ها یک حق بنیادین شهروندی تلقی می‌شود و هرگونه جمع‌آوری، ذخیره یا پردازش داده‌ها باید با رضایت آگاهانه فرد و تحت نظارت نهادهای مستقل انجام شود. در عین حال، دولت موظف

1. Angerer
2. BDSG
3. GDPR
4. IT-Sicherheitsgesetz
5. IT-SiG 2.0
6. National Cyber Security Strategy
7. **Schneider**

است زیرساخت‌های حیاتی (مانند انرژی، حمل‌ونقل و ارتباطات) را از تهدیدات سایبری محافظت کند (کاتنبرگ[1]، ۲۰۲۴: ۱۶۹-۱۷۰).

چارچوب قانونی آلمان در حوزه امنیت سایبری و حفاظت از داده‌ها نه تنها ابزاری برای تنظیم روابط داخلی میان دولت، شهروندان و شرکت‌هاست، بلکه بازتابی از جایگاه و رویکرد بین‌المللی این کشور در نظم سایبری جهانی به شمار می‌آید. در واقع، سیاست سایبری آلمان در پی ایجاد تعادلی میان دو حوزه ظاهراً متضاد است: امنیت ملی و حقوق بنیادین بشر در عصر دیجیتال.

۱. پیوند میان حقوق بشر دیجیتال و امنیت ملی: در سطح نظری، این پیوند بیانگر دیدگاهی است که در اتحادیه اروپا به شکل گسترده پذیرفته شده است؛ دیدگاهی که امنیت سایبری را بدون تضمین آزادی‌های دیجیتال ناممکن می‌داند. در نتیجه، مقرراتی مانند قانون فدرال حفاظت از داده‌ها و مقررات عمومی حفاظت از داده‌های اتحادیه اروپا تنها ابزارهای فنی یا بوروکراتیک نیستند، بلکه نوعی دیپلماسی هنجاری[2] را شکل می‌دهند(پوفال[3] و همکاران، ۲۰۲۴: ۶۹-۷۱). در این رویکرد، اروپا و در رأس آن آلمان سعی دارد مدلی مبتنی بر «اعتماد، شفافیت و پاسخ‌گویی» را در حکمرانی فضای سایبری جهانی ترویج کند؛ مدلی که در برابر رویکردهای امنیت‌محورتر ایالات متحده یا کنترل‌محور چین قرار می‌گیرد

۲. نقش آلمان در سیاست سایبری اتحادیه اروپا و نهادهای بین‌المللی: آلمان یکی از پیش‌گامان تدوین استراتژی سایبری اتحادیه اروپا است و از سال ۲۰۱۶ به بعد، نقش فعالی در مذاکرات مربوط به چارچوب رفتار مسئولانه دولت‌ها در فضای سایبری در سازمان ملل[4] ایفا کرده است. بر اساس اسناد منتشرشده، برلین تأکید دارد که قوانین بین‌الملل، از جمله منشور ملل متحد، در فضای مجازی نیز معتبر است و اصولی چون حاکمیت، تمامیت ارضی و منع مداخله باید در حوزه سایبری رعایت شوند. هم‌زمان، آلمان از مفهوم «حاکمیت دیجیتال[5]» دفاع می‌کند، اما نه به معنای انزواگرایی دیجیتال، بلکه به معنای افزایش توان راهبردی اتحادیه اروپا در برابر وابستگی به بازیگران خارجی در حوزه فناوری. این مفهوم

1. Kattenberg
2. Normative diplomacy
3. Pufahl
4. UN GGE
5. Digital sovereignty

در همکاری‌های آلمان با فرانسه، هلند و کشورهای شمال اروپا به‌ویژه در قالب طرح‌هایی مانند گایا ایکس[1] GAIA-X زیرساخت ابری اروپایی متجلی شده است (رینگوالد[2]، ۲۰۲۴: ۱۷۷-۱۷۹).

۳. امنیت سایبری به‌عنوان محور همکاری‌ها و رقابت‌های جهانی: چارچوب قانونی آلمان همچنین ابزار سیاست خارجی این کشور برای تعریف نقش فعال در حکمرانی سایبری جهانی است. آلمان از طریق ابتکار راهنمای سیاست خارجی سایبری[3] امنیت سایبری را به یکی از ستون‌های دیپلماسی خود بدل کرده است[4]. این سیاست‌ها بر سه محور استوارند: نخست؛ ترویج حقوق بشر در فضای مجازی (از جمله حق حریم خصوصی و آزادی بیان آنلاین)؛ دوم؛ تقویت تاب‌آوری دیجیتال شرکای بین‌المللی و نهایتاً مشارکت در تدوین هنجارهای جهانی و جلوگیری از نظامی‌سازی فضای سایبری (فردریش الکساندر[5]، ۲۰۲۴: ۳۴۱-۳۴۵). از این منظر، چارچوب داخلی حفاظت از داده و امنیت سایبری آلمان، نه صرفاً یک سازوکار ملی، بلکه الگویی برای صدور ارزش‌های لیبرال‌دموکراتیک به حوزه بین‌الملل است.

۳-۶-۲- ساختار نهادی پلیس و نهادهای امنیت سایبری

در آلمان، وظایف مرتبط با امنیت سایبری و مقابله با جرایم اینترنتی میان چند نهاد تقسیم شده است که مهم‌ترین آن‌ها عبارت‌اند از:

۱. اداره فدرال امنیت اطلاعات[6]: نهاد مرکزی سیاست‌گذاری، پیشگیری و هماهنگی در حوزه امنیت سایبری است. این اداره، مسئول نظارت بر استانداردهای امنیتی در بخش دولتی و خصوصی و واکنش به حملات سایبری است؛

---

۱. طرح گایا-ایکس (GAIA-X) یک ابتکار اروپایی است که با هدف ایجاد زیرساخت ابری (Cloud Infrastructure) و داده‌محور اروپایی راه‌اندازی شده است. این طرح در سال ۲۰۱۹ به ابتکار مشترک آلمان و فرانسه آغاز شد و سپس کشورهای دیگری مانند هلند، بلژیک، اسپانیا و کشورهای شمال اروپا نیز به آن پیوستند.

2. Ringwald

3. Cyber Foreign Policy

۴. این سند در ابتدا توسط وزارت امور خارجه آلمان (Auswärtiges Amt) در سال ۲۰۲۱ منتشر شد تا نشان دهد آلمان چگونه می‌خواهد اصول، منافع و ارزش‌های خود را در فضای دیجیتال جهانی دنبال کند.

5. Friedrich-Alexander

6. Bundesamt für Sicherheit in der Informationstechnik - BSI

۲. اداره فدرال جنایی[1]: نهاد اصلی اجرای قانون در زمینه جرایم سایبری است. این نهاد، دارای دپارتمـــان ویژه‌ای برای «تحقیقات دیجیتال» اســـت که وظیفـــه تحلیل داده‌های دیجیتال، ردیابی حملات سایبری و همکاری با پلیس بین‌الملل (اینترپل و یوروپل) را بر عهده دارد؛

۳. مرکز ملی دفاع ســـایبری[2]: این مرکز از ســـال ۲۰۱۱ برای هماهنگی بین نهادهای نظامی، اطلاعاتی، پلیســـی و خصوصی ایجاد شـــده اســـت و نمونه‌ای از مدیریت چندسطحی امنیت سایبری محسوب می‌شود.

ویژگی بارز ســـاختار آلمانی، توزیع مســـئولیت‌ها میان نهادهای مســـتقل و در عین حال وجود سازوکارهای نظارتی شفاف است. هیچ نهادی اجازه ندارد بدون مجوز قانونی به داده‌های خصوصی کاربران دسترســـی پیدا کند، و تمامی فعالیت‌ها تحت نظارت دادگاه‌های فدرال و نهاد حفاظت از داده‌ها قرار دارد (کلبر[3]، ۲۰۲۴: ۲۳-۲۵).

۳-۶-۳- حریم خصوصی و سیاست‌های حفاظتی

آلمان در اجرای مقررات عمومی حفاظت از داده‌ها پیشگام است و اصول بنیادین آن در سیاست داخلی کاملاً نهادینه شده است. مهم‌ترین این اصول عبارت‌اند از:

نخست؛ اصل حداقل‌گرایی در داده[4]: فقط داده‌های ضروری باید جمع‌آوری شود؛

دوم؛ اصل شفافیت و پاسخ‌گویی: نهادهای دولتی موظف‌اند اهداف جمع‌آوری داده را اعلام کنند؛

سوم؛ اصل حق فراموش شدن[5]: هر فرد حق دارد داده‌های خود را از سامانه‌ها حذف کند(موهلرت[6]، ۲۰۲۴: ۹۷-۹۹).

در چارچوب اجرای اصول حقوقی یادشده، پلیس فدرال آلمان[7] و سایر نهادهای امنیتی موظف‌اند هرگونه دسترسی، جمع‌آوری یا تحلیل داده‌های دیجیتال را به‌صورت رسمی، قابل‌ردیابی و تحت نظارت نهادهای مســـتقل نظارتی مانند کمیسر فدرال حفاظت از داده‌ها[8] ثبت و گزارش کنند. این

1. Bundeskriminalamt - BKA
2. Nationales Cyber-Abwehrzentrum - Cyber-AZ
3. Kleber
4. Data Minimization
5. Right to be Forgotten
6. Muhlert
7. Bundeskriminalamt
8. BfDI

الزام قانونی، یکی از مهم‌ترین جلوه‌های «پاسخ‌گویی نهادی در حوزه دیجیتال» محسوب می‌شود؛ یعنی حتی در حوزه امنیت ملی، اصل شـــفافیت و کنترل دموکراتیک بر عملکرد نهادهای امنیتی حفظ می‌گردد (بامدیک[1]، ۲۰۲۴: ۲۲۴-۲۲۶).

از منظر تحلیلی، این سازوکار دو کارکرد کلیدی دارد:

نخست؛ حفاظت از حریم خصوصی به‌عنوان حق بنیادین شهروندی؛ زیرا هرگونه نقض احتمالی داده‌ها قابل ردیابی و پیگرد حقوقی است؛

دوم؛ تقویـــت ســـرمایه اجتماعی و اعتماد عمومـــی به نهادهای امنیتی؛ عاملـــی که در جوامع دیجیتالی‌شده، شرط ضروری برای اثربخشی سیاست‌های امنیتی به‌شمار می‌آید.

بر اساس داده‌های مؤسسات پژوهشی اروپایی از جمله یوروبارومتر[2] و مؤسسه فراون‌هوفر[3]، بیش از ۷۰٪ شـــهروندان آلمانی به عملکرد پلیس فدرال و نهادهای امنیتی در حوزه امنیت ســـایبری اعتماد دارند. این رقم به‌طور معناداری بالاتر از میانگین اتحادیه اروپا است، جایی که در بسیاری از کشورها این میزان کمتر از ٤٠٪ گزارش شده است. چنین سطحی از اعتماد، پیامد مستقیم توازن میان کارایی امنیتی و رعایت اصول حقوق بشر دیجیتال است(دابیچ[4]، ۲۰۲۴: ۷-۸).

از منظر روابط بین‌الملل، این تجربه برای ســـایر کشـــورها نیز واجد اهمیت است. آلمان با تأکید بر شـــفافیت، نظارت دموکراتیک و پاســـخ‌گویی نهادی در حکمرانی داده، در واقع الگوی «امنیت مبتنی بر اعتماد» را در برابر مدل‌های امنیتی مبتنی بر کنترل یا نظارت فراگیر مطرح کرده است. این الگو به‌ویژه در تعاملات اتحادیه اروپا با شرکای بین‌المللی در حوزه امنیت سایبری از جمله در چارچوب «جعبه ابزار دیپلماسی سایبری[5]» مورد استفاده قرار می‌گیرد. بدین ترتیب، نظام نظارتی آلمان نه تنها در خدمت حفاظت از داده‌ها در ســـطح ملی اســـت، بلکه به‌صورت غیرمستقیم قدرت نرم و مشروعیت بین‌المللی این کشور را نیز تقویت می‌کند. زیرا نشان می‌دهد که می‌توان امنیت ســـایبری را در چارچوب دموکراسی، شفافیت و حقوق بشـــر تحقق بخشید؛ امری که در گفتمان سیاست جهانی سایبری به عنوان «مدل اروپایی حکمرانی دیجیتال» شناخته می‌شود.

---

1. Baumdick
2. Eurobarometer
3. Fraunhofer ISI
4. Dabic
5. Cyber Diplomacy Toolbox

۳-۶-۴- ابعاد دیپلماتیک و بین‌المللی

آلمان در عرصه بین‌المللی یکی از بازیگران فعال در شکل‌دهی به رژیم حکمرانی سایبری است. سیاست خارجی آلمان در این حوزه بر پایه سه محور شکل گرفته است:

نخست؛ دیپلماسی سایبری: آلمان از طریق وزارت امور خارجه خود، واحد ویژه‌ای به نام Cyber Foreign Policy ایجاد کرده که هدف آن گسترش همکاری‌های بین‌المللی برای مقابله با تهدیدات سایبری است؛

دوم؛ همکاری در چارچوب اتحادیه اروپا: آلمان در طراحی استراتژی‌های جمعی اتحادیه اروپا برای دفاع سایبری، مانند قانون امنیت سایبری اتحادیه اروپا[1] و نسخه دوم دستورالعمل امنیت شبکه و اطلاعات[2]، نقش محوری دارد؛

سوم؛ تعهد به چندجانبه‌گرایی سایبری: آلمان از رویکردی حمایت می‌کند که بر پایه همکاری دولت‌ها، بخش خصوصی و جامعه مدنی استوار است. این کشور مخالف دیدگاه‌های محدودگرایانه درباره «حاکمیت ملی مطلق بر فضای مجازی» است و بر استانداردهای بین‌المللی مبتنی بر حقوق بشر تأکید می‌کند (اشمیت[3]، ۲۰۲۵: ۸۷-۹۰).

از منظر نظریه‌های روابط بین‌الملل، سیاست آلمان در حوزه امنیت سایبری به‌وضوح با نهادگرایی لیبرال همخوانی دارد. همانگونه که پیشتر تبیین گردید، این دیدگاه معتقد است که حتی در نظام بین‌الملل به ظاهر آنارشیک، همکاری، ایجاد اعتماد متقابل و پیروی از قواعد و هنجارهای مشترک می‌تواند امنیت جمعی را تضمین کند. بر این اساس، آلمان بر این باور است که امنیت سایبری جهانی تنها از طریق تعامل مستمر میان دولت‌ها، سازمان‌های چندجانبه و نهادهای بین‌المللی قابل تحقق است و نه از طریق رقابت قدرت‌ها یا اقدامات یک‌جانبه بازدارنده. این رویکرد در سیاست عملی آلمان به وضوح مشاهده می‌شود. به‌عنوان مثال، این کشور نقش محوری در طراحی و اجرای استراتژی‌های جمعی اتحادیه اروپا برای امنیت سایبری، مانند قانون امنیت سایبری اتحادیه اروپا و نسخه دوم دستورالعمل امنیت شبکه و اطلاعات دارد و همچنین در چارچوب جعبه ابزار دیپلماسی سایبری اتحادیه اروپا، بر ارتقای شفافیت، پاسخگویی و همکاری فراملی تمرکز می‌کند. آلمان با تأکید بر شفافیت نهادها، حفاظت از حقوق دیجیتال شهروندان و تبادل اطلاعات امنیتی، سعی

1. EU Cybersecurity Act
2. EU NIS2 Directive
3. Schmidt

دارد اعتماد میان دولت‌ها و بازیگران بین‌المللی را تقویت کند و زمینه شکل‌گیری یک نظم سایبری قانون‌محور و چندجانبه را فراهم آورد. به بیان دیگر، سیاست سایبری آلمان ترکیبی از امنیت از طریق همکاری[1] و قدرت نرم هنجاری[2] است. این کشور با الگوسازی در زمینه حریم خصوصی دیجیتال، پاسخ‌گویی نهادها و محافظت از داده‌ها، نشان می‌دهد که امنیت سایبری و حقوق بشر دیجیتال می‌توانند همزمان تحقق یابند و از این طریق، مشروعیت بین‌المللی و نفوذ هنجاری خود را در عرصه جهانی افزایش می‌دهد. این رویکرد همچنین الگویی برای سایر کشورهای عضو اتحادیه اروپا و شرکای بین‌المللی فراهم می‌آورد تا امنیت سایبری را به‌عنوان مسئولیت مشترک و کالایی عمومی جهانی دنبال کنند.

۳-۶-۵- عملکرد پلیس سایبری در عمل

تحلیل گزارش‌های رسمی پلیس فدرال جنایی آلمان[3] و دفتر فدرال امنیت اطلاعات آلمان[4] نشان می‌دهد که در سال‌های اخیر، آلمان با افزایش حملات سایبری روبه‌رو بوده است به‌ویژه در حوزه‌های مالی، زیرساخت‌های حیاتی و اطلاعات دولتی. تنها در سال ۲۰۲۳ بیش از ۱۳۰ هزار پرونده مرتبط با جرایم سایبری ثبت شده است. با این حال، واکنش نهادی به این تهدیدها بسیار منظم و قانون‌مند بوده است. سیستم واکنش اضطراری کامپیوتری[5] که زیرمجموعه دفتر فدرال امنیت اطلاعات آلمان است، با نهادهای دولتی و شرکت‌های خصوصی همکاری می‌کند تا حملات را در زمان واقعی شناسایی و خنثی کند. همچنین، پلیس فدرال در همکاری با یوروپل و FBI در چند عملیات بین‌المللی، از جمله شناسایی شبکه‌های فیشینگ و باج‌افزار، مشارکت داشته است. در بعد داخلی، پلیس فدرال جنایی آلمان از فناوری‌های پیشرفته داده‌کاوی و هوش مصنوعی برای تحلیل الگوهای مجرمانه استفاده می‌کند، اما این فناوری‌ها تحت قوانین سخت‌گیرانه حفظ حریم خصوصی به کار گرفته می‌شوند(مولر[6]، ۲۰۲۵: ۴۱-۴۴). برخلاف بسیاری از کشورها، هیچ برنامه گسترده نظارتی بدون مجوز قانونی در آلمان اجرا نمی‌شود، و پارلمان فدرال و دادگاه قانون اساسی

1. Security through cooperation
2. Normative soft power
3. Federal Criminal Police Office
4. Federal Office for Information Securit
5. CERT-Bund (Computer Emergency Response Team)
6. **Müller**

بر این موضوع نظارت مستقیم دارن. با وجود موفقیت‌ها، سیاست سایبری آلمان نیز با چالش‌هایی مواجه اســت. برخی کارشناســان بر این باورند که ســخت‌گیری بیش از حد در قوانین حفاظت از داده‌ها می‌تواند ســرعت واکنش به حملات سایبری را کاهش دهد. همچنین، نگرانی‌هایی درباره نفوذ خارجی، به‌ویژه از سوی روسیه و چین، وجود دارد که دولت را وادار به تقویت زیرساخت‌های دفاعی کرده است (واگنر[1]، ۲۰۲۵: ۱۰۷-۱۰۹).

از دیدگاه روابط بین‌الملل، چالش دیگر آلمان در توازن میان امنیت و ارزش‌های لیبرال اســت. این کشــور تــلاش می‌کند ضمن حفظ آزادی‌هــای دیجیتال، در محیطی جهانــی که بازیگران غیردموکراتیک به ســرعت در حال افزایش توان ســایبری خود هستند، قدرت بازدارندگی مؤثری داشــته باشــد.در جمع‌بندی کلی می‌توان گفت که مدل آلمانی امنیت ســایبری بر پایه ترکیب شــفافیت، نظارت قانونی، و همکاری بین‌المللی شــکل گرفته اســت. برخلاف الگوهای اقتدارگرا، آلمان توانســته میان «امنیت ملی» و «آزادی دیجیتال» تعادل نســبی ایجاد کند. از منظر روابط بین‌الملل، این الگو مصداقی از قدرت نرم سایبری[2] اســت؛ یعنی کشــوری که از طریق نهادسازی، قانون‌گرایی و مشارکت بین‌المللی، نفوذ خود را در حکمرانی جهانی فضای مجازی افزایش می‌دهد. در مقابل، آلمان با چالش‌هایی مانند افزایش تهدیدات بین‌المللی و نیاز به سرمایه‌گذاری بیشتر در دفاع ســایبری روبه‌رو است، اما با اتکا به چارچوب‌های چندجانبه و نهادهای دموکراتیک، توانسته جایگاه خود را به‌عنوان الگوی موفق حکمرانی سایبری حفظ کند.

۳-۷- بررسی تطبیقی عملکرد پلیس فتا در ایران و آلمان در موضوع حریم خصوصی و امنیت سایبری

تطبیق ایران و آلمان در حوزه امنیت سایبری و حریم خصوصی، تقابل دو منطق حکمرانی را بازتاب می‌دهد: «امنیت‌محوری دولتی و حاکمیت اطلاعات» در ایران در برابر «حقوق‌محوری، شفافیت و نهادگرایی» در آلمان. این تقابل نه تنها در قواعد و ساختارهای نهادی قابل مشاهده اســت، بلکه در گفتمان سیاسی، سطح اعتماد عمومی، و ظرفیت همکاری بین‌المللی نیز نمود دارد. تحلیــل تطبیقی باید از ســه بعد همزمان صورت گیــرد: (۱) بعد حقوقی و مقرراتی؛ (۲) بعــد نهــادی و فنی؛ و (۳) بعد دیپلماتیک و بین‌المللی. پیوند دادن این ســه بعد با نظریه‌های

1. **Wagner**
2. Cyber Soft Power

واقع‌گرایی و امنیتی‌سازی، امکان درک پیامدهای فراملی سیاست‌های سایبری را فراهم می‌سازد.

۳-۷-۱- مقایسه در سطح قواعد و حقوق

آلمان بر پایه مقررات عمومی حفاظت از داده‌ها و قوانین ملی مانند قانون فدرال حفاظت از داده‌ها یک چارچوب حقوقی شفاف، الزام‌آور و مبتنی بر حقوق فردی ایجاد کرده است. اصولی همچون شفافیت در پردازش داده، حداقلی‌سازی جمع‌آوری داده، و نظارت مستقل نهادهای حفاظت از داده، هسته حقوق‌محور سیاست آلمانی را شکل می‌دهد. این چارچوب قانونی به‌صورت مستقیم بر نحوه عمل پلیس فدرال تاثیر گذاشته و هر گونه دسترسی به داده‌های خصوصی را مقید به الزامات قضایی و اداری کرده است. در مقابل، در ایران چارچوب قانونی پراکنده، مبتنی بر قانون جرایم رایانه‌ای و مجموعه‌ای از آیین‌نامه‌ها و مصوبات اداری است. فقدان قانون جامع حفاظت از داده‌ها و نبود نهاد نظارتی مستقل موجب شده مرزبندی حقوقی بین وظایف امنیتی و حقوق فردی مبهم بماند. این ابهام به نفع تفاسیر امنیتی و دستورهای اجرایی شده و زمینه گسترده‌تری برای اقدامات نظارتی فراتر از حد ضرورت فراهم می‌آورد. از منظر روابط بین‌الملل، این اختلافات حقوقی بر قابلیت همکاری فرامرزی نیز اثر می‌گذارد؛ آلمان می‌تواند بر پایه قوانین شفافی که از استانداردهای بین‌المللی تبعیت می‌کند همکاری‌های متعدد قضایی و پلیسی برقرار سازد، در حالی که ایران به دلیل شکاف‌های حقوقی و عدم عضویت در معاهدات کلیدی، دسترسی به شبکه‌های تعاملی بین‌المللی محدودتری دارد.

۳-۷-۲- مقایسه ساختارهای نهادی و ظرفیت فنی

آلمان یک معماری نهادی چندلایه دارد: نهادهای تخصصی[1]، نهادهای اجرایی[2] و ساختارهای هماهنگ‌کننده[3]. این توزیع نقش‌ها به همراه نظارت پارلمانی و حقوقی، امکان واکنش سریع و مشروع به تهدیدات را فراهم می‌سازد، در حالی که از حقوق شهروندی نیز حفاظت می‌کند. ظرفیت فنی آلمان در بهره‌گیری از سیستم‌های CERT، شبکه‌های اشتراک اطلاعات تهدید و همکاری

1. BSI
2. BKA
3. CERT-Bund و Cyber-AZ

عمومی-خصوصی قوی، سطح پیشگیری و بازدارندگی را بالا برده است. پلیس فتا در ایران نیز دارای ساختار استانی و توان عملیاتی در حوزه‌های ردیابی و رسیدگی به پرونده‌های فنی است، اما ظرفیت‌های فنی غالباً در چارچوب وابستگی به نهادهای امنیتی کلان و محدودیت‌های فناوری به‌واسطه تحریم‌ها و کمبود توسعه بومی قرار دارد. ضعف در سازوکارهای اشتراک‌گذاری اطلاعات بین‌المللی و داخلی (بین دستگاهی)، و نبود سازوکارهای مستقل پاسخ‌گویی، کارایی عملیاتی را کاهش داده و گاهی تمرکز را صرف اقدامات کنترلی نموده است.

۳-۷-۳-گفتمان، مشروعیت و اعتماد عمومی

در آلمان، گفتمان عمومی نسبت به حریم خصوصی حساس و مبتنی بر خاطرات تاریخی است؛ این حساسیت به شکل‌گیری قوانین سختگیرانه و حضور فعال جامعه مدنی در نظارت بر قدرت دولتی منتهی شده است. نتیجه این روند، سطح بالای اعتماد عمومی و پذیرش اقداماتی است که هم امنیت را تقویت می‌کنند و هم حقوق فردی را ضمانت می‌کنند. در ایران، گفتمان غالب درباره ضرورت «صیانت از امنیت و ارزش‌های فرهنگی» است. امنیتی‌سازی فضای سایبری، که توسط بازیگران امنیتی و سیاسی پیش برده می‌شود، مشروعیت‌بخشی به اقدامات نظارتی می‌دهد اما اعتماد عمومی نسبت به نهادهای نظارتی در حوزه سایبری تضعیف می‌شود؛ زیرا شهروندان و نخبگان مدنی از شفافیت و پاسخ‌گویی کافی محروم‌اند. این ضعف اعتماد، هزینه‌های اجتماعی و اقتصادی (مثل کاهش استفاده از خدمات آنلاین، مخاطرات برای اقتصاد دیجیتال) نیز به همراه دارد.

۳-۷-۴-پیامدهای بین‌المللی و دیپلماتیک

آلمان با پیوند دادن محافظت از داده‌ها به قراردادها و استانداردهای بین‌المللی، از ابزار سیاست خارجی بهره می‌برد؛ به‌عنوان مثال، با ترویج استانداردهای مقررات عمومی حفاظت از داده‌ها در مذاکرات تجاری و همکاری‌های تکنولوژیک، قدرت نرم خود را افزایش می‌دهد. عضویت در کنوانسیون‌ها و همکاری با یوروپل و سایر نهادها موجب شده آلمان در شبکه‌های جهانی مبارزه با جرایم سایبری فعال باشد. ایران با سیاست «حاکمیت سایبری» و تلاش برای کنترل پهنه داخلی، در عرصه بین‌المللی با محدودیت همکاری و فقدان اعتماد مواجه است. این وضع سبب کاهش تبادل اطلاعات قضایی، محرومیت از بسیاری از پروژه‌های مشترک و افزایش مخاطرات در مدیریت تهدیدات فرامرزی می‌شود. از منظر واقع‌گرایی، ایران این سیاست را به‌عنوان ابزار حفظ

بقا و مقاومت در برابر نفوذ خارجی می‌بیند، اما در عمل هزینه‌هایی در قالب کاهش همکاری‌های فنی و اطلاعاتی پرداخت می‌کند.

۳-۷-۵-نقاط قوت و ضعف تطبیقی (تحلیل سیاستی)

نقاط قوت آلمان: چارچوب قانونی شفاف و متناسب با استانداردهای بین‌المللی؛ نهادهای مستقل نظارتی؛ ظرفیت فنی پیشـــرفته؛ شـــبکه‌های همکاری بین‌المللی؛ سطح بالای اعتماد عمومی. این نقاط قوت به آلمان امکان می‌دهد که همزمان از امنیت سایبری محافظت کند و ارزش‌های حقوقی را نیز حفظ نماید.

نقـــاط ضعـــف آلمان: پیچیدگی قانونی که گاهی ســـرعت عملیاتی را کاهـــش می‌دهد؛ نیاز به هماهنگی میان فدرال و ایالتی که فرایند پاسخ‌دهی را طولانی می‌کند؛ چالش‌های جدید تهدیدات پیچیده بین‌المللی.

نقاط قوت ایران: تمرکزگرایی و پاســـخ‌دهی ســـریع در برخی موارد امنیتی؛ اراده سیاسی برای حاکمیت ســـایبری و توسعه زیرســـاخت‌های داخلی؛ توانایی اعمال کنترل فراگیر در سطح شبکه ملی اطلاعات.

نقاط ضعف ایران: خلأ حقوقی در حفاظت از داده‌ها؛ کمبود شفافیت و نهادهای نظارتی مستقل؛ محدودیت‌هـــای فنی و همـــکاری بین‌المللی؛ هزینه‌های کاهش اعتمـــاد عمومی و تأثیر منفی بر اقتصاد دیجیتال.

۳-۷-۶- نتیجه تحلیل تطبیقی از منظر روابط بین‌الملل

از منظـــر نظریه واقع‌گرایی، هر دو کشـــور ســـعی در محافظت از منافع ملـــی دارند اما ابزارها و اولویت‌هـــا متفاوت‌اند؛ آلمان از نهادگرایی و حقوق‌محوری بهره می‌برد تا مشـــروعیت و همکاری بین‌المللی کسب کند، در حالی که ایران با تأکید بر حاکمیت و کنترل، استقلال داخلی را تقویت می‌کند اما از هزینه‌های بین‌المللی غفلت ندارد. نظریه امنیتی‌ســـازی گویای این اســـت که چگونه گفتمان‌ســـازی امنیتی می‌تواند مرزهای حقوقی را جابه‌جا کند؛ در ایران این فرایند زمینه‌ســـاز گسترش اختیارات شده و در آلمان تحت کنترل حقوقی و مدنی قرار دارد. ترکیب این دو چشم‌انداز نشان می‌دهد که راهبردی میانجی که هم امنیت ملی را تأمین کند و هم حقوق دیجیتال را تضمین نماید بهترین مسیر برای کاهش هزینه‌های داخلی و افزایش ظرفیت بین‌المللی است.

جدول ۱- بررسی تطبیقی عملکرد پلیس فتای ایران و آلمان در موضوع حریم خصوصی و امنیت سایبری از منظر امنیت سازمانی (منبع: یافته‌های پژوهش)

بُعد / مولفه	ایران (پلیس فتا)	آلمان BSI / BKA و نهادها
چارچوب قانونی	پراکنده، مبتنی بر قانون جرایم رایانه‌ای، فاقد قانون جامع حفاظت از داده	قانون BDSG، اجرای GDPR، IT-SiG، چارچوب حقوقی شفاف
ساختار نهادی	متمرکز تحت نیروی انتظامی، وابستگی به نهادهای امنیتی	چندلایه: BSI، BKA، Cyber-AZ، نظارت پارلمانی
دسترسی و محدودیت‌های نظارتی	گسترده اما ابهام‌آمیز و کم‌شفاف	محدود به مجوز قانونی، ثبت و نظارت مستقل
ظرفیت فنی	موجود ولی محدود؛ وابستگی به همکاری‌های داخلی	بالاتر؛ شبکه‌های CERT، هوش تهدید، همکاری عمومی-خصوصی
سطح اعتماد عمومی	پایین‌تر به‌دلیل شفافیت و پاسخ‌گویی محدود	بالاتر؛ قوانین و نهادهای نظارتی تقویت‌کننده اعتماد
همکاری بین‌المللی	محدود، عدم عضویت در برخی معاهدات	فعال، عضو نهادهای منطقه‌ای و بین‌المللی، همکاری گسترده
گفتمان غالب	امنیت‌محور، حاکمیت سایبری، صیانت فرهنگی	حقوق‌محور، حفاظت از داده، نهادگرایی و چندجانبه‌گرایی
پیامدهای دیپلماتیک	انزوای نسبی، محدودیت تبادل داده و همکاری قضایی	افزایش نفوذ نرم، امکان همکاری و تبادل اطلاعات گسترده
ریسک‌ها	نقض حقوق دیجیتال، کاهش اعتماد، محدودیت همکاری	کندی عملیاتی در برخی موارد به‌خاطر مقررات سخت
مسیر توصیه‌شده	تصویب قانون حفاظت داده، ایجاد نهاد مستقل، تعامل بین‌المللی	حفظ تعادل حقوقی-امنیتی، افزایش تبادل تجربه با شرکا

نتیجه‌گیری و پیشنهاد

هدف پژوهش حاضر، مقایسه عملکرد پلیس فتا در ایران با نهادهای سایبری آلمان و پاسخ به این پرسش اساسی بوده است که «چگونه تفاوت در برداشت امنیتی و حقوقی دو کشور بر توان

و جایـــگاه آن‌هـــا در عرصه روابط بین‌الملل تأثیر می‌گذارد؟». نتایج اصلی و کلی پژوهش دلالت بر این مهم داشـــت که ریشـــه اصلی تفاوت‌ها نه در ابزارهای فنی، بلکه در نوع فهم دو کشور از مفهوم امنیت سایبری و نقش دولت در مدیریت فضای دیجیتال است.

مطالعه تطبیقی میان عملکرد پلیس فتا در ایران با نهادهای ســـایبری آلمان نشان داد که ایران امنیت سایبری را ذیل امنیت ملی و کنترل تهدیدات داخلی تعریف می‌کند؛ ازاین‌رو الگوی فعلی مبتنی بر تمرکز قدرت، غلبه نگاه امنیتی و تقدم کنترل بر شفافیت است. در مقابل، آلمان امنیت ســـایبری را در پیوند با حقوق شهروندی، مسئولیت‌پذیری نهادی و حکمرانی شفاف قرار می‌دهد. این تمایز سبب شده است که آلمان در روابط بین‌الملل به صادرکننده هنجارهای داده و بازیگری فعال در دیپلماسی دیجیتال تبدیل شود، در حالی‌که ایران تعامل محدودتری را تجربه می‌کند.

در ادامـــه نیـــز بخش مهم دیگری از یافته‌ها نشـــان دادند که رفتار ایـــران با منطق واقع‌گرایی و خودیاری سازگار است، در حالی‌که رفتار آلمان با نهادگرایی و همکاری چندجانبه همخوانی دارد. ایـــن دو الگو هرچند از نظـــر منافع ملی قابل توجیه‌اند، اما از نظر کارآمدی بلندمدت، مدل مبتنی بر قانون‌مندی و اعتماد اجتماعی ظرفیت بیشتری برای تولید امنیت پایدار ایجاد می‌کند. موضوع مهمـــی کـــه باید بدان توجه نمود آنکـــه چالش اصلی ایران نه در کمبود فنـــاوری، بلکه در ضعف حکمرانی داده، نبود نهادهای مســـتقل و محدود بودن مشارکت بین‌المللی است. همچنین روشن شـــد که رابطه میان «امنیت» و «حریم خصوصی» رابطه‌ای تعادلی است و هرگونه غلبه یک‌جانبه بر دیگری، موجب کاهش مشـــروعیت و کارآمدی خواهد شد. بنابراین آینده امنیت سایبری ایران در حرکت به سوی تعادل میان اقتدار، قانون و اعتماد اجتماعی قرار دارد.

راهکارهای پیشنهادی

۱. تدوین قانون جامع و یکپارچه حفاظت از داده‌ها: اصلاح ساختار حقوقی با تصویب قانونی ملی که مرز میان مأموریت‌های امنیتی و حقوق شـــهروندی را مشخص کند. این قانون باید دارای ضمانت اجرای قضایی بوده و از تداخل نهادی جلوگیری نماید؛ زیرا یافته‌های پژوهش نشان می‌دهـــد ضعف حقوقی، یکی از عوامل اصلی کاهـــش اعتماد عمومی و ناکارآمدی حکمرانی سایبری در ایران است.

۲. ایجاد نهاد مستقل نظارت بر حریم خصوصی و حکمرانی داده: بر اساس نتایج پژوهش، نبود نهاد مستقل از چالش‌های بنیادین ایران است. تشکیل نهادی ملی با استقلال اداری و وظیفه

نظارت، ارزیابی و انتشـــار گزارش‌های عمومی می‌تواند شکاف میان امنیت و اعتماد اجتماعی را کاهش دهد و شفافیت را تقویت کند.

۳. تقویت دیپلماسی سایبری و مشارکت در همکاری‌های بین‌المللی: یافته‌ها نشان داد محدودیت تعامل خارجی، توان ایران را در مدیریت تهدیدات فرامرزی کاهش می‌دهد. مشارکت هدفمند در ســـازوکارهای منطقه‌ای و جهانی، تبادل تجربه و تعامل با کشورهای پیشرفته می‌تواند به ارتقای ظرفیت فنی و افزایش مشروعیت بین‌المللی منجر شود.

۴. توســـعه چارچوب حکمرانی مبتنی بر تعادل امنیت و حقوق دیجیتال: نتایج پژوهش تأکید می‌کند که امنیت پایدار زمانی حاصل می‌شـــود که حقوق دیجیتال بخشی از سیاست‌گذاری امنیتی باشـــد. ایجاد شاخص‌های ارزیابی عملکرد، تقویت پاسخ‌گویی نهادی و پذیرش حریم خصوصی به‌عنوان مؤلفه امنیت ملی، مســـیر تولید امنیت پایدار و افزایش ســـرمایه اجتماعی را هموار می‌کند.

فهرست منابع

۱. آل رسول، میرالتفات و مرشدی، مسعود (۱۴۰۳). «نقش آموزش در پیشگیری از بزه‌دیدگی سایبری». پژوهش‌های جرم‌شناسی کاربردی، ۲(۵)، ۷۳-۹۹.

۲. امیریان فارسانی، امین- مالمیر، محمود- اشرافی، محمود و حیدری، مسعود (۱۴۰۳). «کارکردهای نظری و عملی پلیس فتا در پیشگیری از جرایم سایبری و موانع حاکم بر آن». تحقیقات حقوقی بین المللی، ۳۵(۱۰)، ۲۶۵-۲۳۷.

۳. اندرسن، بلا (۱۴۰۰). جرایم سایبری: تهدیدهای مجرمانه ناشی از فضای سایبری. ترجمهٔ حسین اسکندری صدق، تهران: ناقوس.

۴. بیات، معصومه (۱۴۰۳). جرایم فضای سایبری و راه‌های پیشگیری از آن با تاکید بر اقدامات و وظایف پلیس فتا. تهران: علم.

۵. جوکار، حسین (۱۴۰۳). امنیت سایبری در شبکه‌های هوشمند. تهران: دادگستر.

۶. حدیثی، حسین (۱۴۰۳). جرائم سایبری از منظر حقوق جزا. تهران: آزادی قلم.

۷. ریاحی، ایمان (۱۴۰۳). تاثیر وقوع جرایم و حملات سایبری بر ابعاد امنیت. تهران: مجد.

۸. سعیدی، سیامک (۱۴۰۳). جرائم سایبری و نقش پلیس در تعقیب کیفری جرم. تهران: دارالهدایه.

۹. سلحشور، ناصر (۱۴۰۴). جرایم رایانه‌ای: مسئولیت کیفری اشخاص حقوقی در جرایم سایبری. تهران: فردوس مهر.

۱۰. سهلانی، حسین (۱۳۹۸). آشنایی با تهدیدات فضای سایبری. تهران: دانشگاه علوم انتظامی امین.

۱۱. فاطمی‌خواه، مریم. (۱۴۰۲). نقش پلیس فتا در جرائم سرقت رایانه. تهران: ارشدان.

۱۲. فرزین‌مهر، فردین (۱۴۰۳). نقش پلیس در پیشگیری از جرایم رایانه‌ای. تهران: سنجش و دانش.

۱۳. کمال، حامد (۱۴۰۳). انواع ناامنی در فضای مجازی. تهران: فلق.

۱۴. محقق، علیرضا (۱۴۰۴). جنایت تجاوز سایبری از منظر دیوان کیفری بین‌المللی. تهران: سهامی انتشار.

۱۵. هدائی، فرخ (۱۴۰۴). جرایم امنیتی سایبری در پرتو حقوق کیفری. تهران: قانون یار.

16. Barends, E., Wietrak, E., & Rousseau, D. M. (2024). *Intra-organisational trust: An evidence review. Scientific summary.* NewYork: Chartered Institute of Personnel and Development.

17. Ding, X., & Huang, H. (2024). For whom is privacy policy written? A

new understanding of privacy policies. *Journal of Computer Law & Security Review*, (55), 114-133.
18. Durak, G. (2024). Contribution of Copenhagen school to the security studies. *Journal of Global Cybersecurity and International Law*, 14(1), 157-186.
19. Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Journal of Contemporary Security Policy*, 45(3), 426-458.
20. Hakmeh, J., Swali, A., & Collett, R. (2024). *A principles-based approach to cyber capacity-building (CCB): Understanding and operationalizing the OEWG CCB principles*. NewYork: Chatham House.
21. Hogan, L., & Lasek-Markey, M. (2024). Towards a human rights-based approach to ethical AI governance in Europe. *Journal of Philosophies*, 9(6), 181-205.
22. Relations: Insights from Realist and Liberal Theories. *Journal of International Relations*, 21(8), 25-47.
23. Marcen, A, G. (2024). The Budapest Convention and the UN Cybercrime Convention negotiations. *Journal of Global Cybersecurity and International Law*, 28(1), 81-106.
24. Otukoya, T. A. (2024). Applying securitization theory in armed conflict. *International Journal of Science and Research Archive*, 11(1), 1756-1767.
25. آلمانی
26. Angerer, J. (2024). *Quo vadis Cybercrime: Aufsatz / Impulsvortrag, veröffentlicht in Kriminalistik*, Kriminalistik.
27. Baumdick, K. (2024). *Faszination Cybercrime: Das umfassende Cybercrime & -security Kompendium*. Tübingen: Mohr Siebeck Verlag
28. Dabic, M. (2024). *Cybersecurity: Fachbuch, deutschsprachige Ausgabe*. Verlag: Springer International.

29. Friedrich-Alexander, L. (2024). Bundeslagebild Cybercrime. *Zeitschrift für Rechtspolitik*, 28(2), 328-355.
30. Kattenberg, T. (2024). Beitrag zu Cyberthemen / Jugend und Online-Risiken. *JuristenZeitung* (3), 166-193.
31. Kleber, T. J. (2024). *Cybersecurity für Einsteiger: In 30 Minuten sicher im Netz*. München: C.H. Beck Verlag.
32. Muhlert, M. (2024). *Navigating the Cyber Maze: Insights and Humor on the Digital Frontier*. Baden-Baden: Nomos Verlagsgesellschaft.
33. Müller, M. (2025). *Bundeslagebild Cybercrime*. Berlin: Walter de Gruyter Verlag.
34. Pufahl, M., Paulsen, P., & Arndt, P. (2024). *Cybersecurity für Manager: Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis*. Wiesbaden: Springer Gabler.
35. Ringwald, J. (2024). *Digital, kriminell, menschlich: Eine Cyberstaatsanwältin ermittelt*. Hamburg: Murmann Verlag.
36. Schmidt, P. (2025). *Die Lage der IT-Sicherheit in Deutschland*. Berlin: Duncker & Humblot Verlag.
37. Schneider, P, S. (2025). *Kosten und Schäden durch Cyber-Kriminalität*. Marburg: Tectum Verlag.
38. Wagner, K. (2025). *Polizeiliche Kriminalstatistik*. Frankfurt: Peter Lang Verlag.