Journal of Socio-Political Developments in Contemporary Iran

Vol. 3, No. 9, Winter2024

http://doi.org/ 10.30510/pscci.2025.497314.1195

Policymaking on cybercrimes against emerging energy infrastructures and its representation in the criminal law system of Iran and France

Sudaba Soleimani[1]

Behzad Razavi Fard[2]

Maryam Safai [3]

Received: 23 May 2024

Reception: 12 September 2024

Abstract:

The main issue of this research is the analysis and representation of cyber crimes against new energies in the existing criminal laws in Iran and France, which target technical infrastructure and new energies. The existing challenges in the field of criminal procedure and substantive law, especially in the direction of identifying and pursuing these crimes in the cyber space, especially in the context of threats against vital and emerging infrastructures, cause gaps in the legal systemsIn addition to the use of scientific sources and legal articles, this research has been analyzed in a descriptive-analytical way, the adaptation of the criminal laws of Iran and France with the approach of cyber threats against technical infrastructures and new energies. The findings of the research show that in Iran and France, the existing criminal laws to deal with cyber crimes, especially threats against technical infrastructure and new energies, do not fully and effectively respond to today's needs. In Iranian law, the computer crimes law has specifically dealt with issues such as cyber threats against critical infrastructure, but due to technological developments, the need to amend and supplement these laws is felt. In France, despite the existence of laws to protect information and national security, cross-border cybercrimes and their complexities have caused serious challenges in identifying and tracking these threatsThe results of the research indicate that it is necessary to formulate new and differentiated criminal policies to deal with cybercrimes and to provide special measures in order to maintain the security of new energies.

[1]PhD student, Department of Criminal Law and Criminology, Bushehr Branch, Islamic Azad University, Bushehr, Iran

[2]Associate Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Sciences, Allameh Tabatabai University, Tehran, Iran

[3]Assistant Professor of Law Department, Bushehr Branch, Islamic Azad University, Bushehr, Ira

فصلنامه تحولات سیاسی اجتماعی معاصر ایران، سال سوم، شماره چهارم(پیاپی۹)، زمستان،۱۴۰۳، صص ۲۷۹-۲۵۱

http://doi.org/ 10.30510/pscci.2025.497314.1195

سیاستگذاری در مورد جرایم سایبری علیه زیر ساخت های انرژی های نو پدید و بازنمایی آن در نظام حقوق کیفری ایران و فرانسه

سودابه سلیمانی[۱]

بهزاد رضوی فرد[۲]

مریم صفایی[۳]

تاریخ دریافت :۰۳ /۱۴۰۳/۰۳

تاریخ پذیرش: ۱۴۰۳/۰۶/۲۲

چکیده

مسئله اساسی این تحقیق تحلیل و بازنمایی جرایم سایبری علیه انرژی‌های نو در قوانین کیفری موجود در دو کشور ایران و فرانسه است که زیرساخت‌های فنی وانرژی‌های نو را هدف قرار می‌دهند.چالش‌های موجود در حوزه آیین دادرسی کیفری و حقوق ماهوی،به‌ویژه در راستای شناسایی و پیگیری این جرایم در فضای سایبر،به‌طور خاص در زمینه تهدیدات علیه زیرساخت‌های حیاتی و نوظهور،موجب ایجاد خلأهایی در سیستم‌های حقوقی می‌شود.این تحقیق به روش توصیفی-تحلیلی علاوه بر استفاده از منابع علمی و مقالات حقوقی،تطبیق حقوق کیفری ایران و فرانسه با رویکرد تهدیدات سایبری علیه زیرساخت‌های فنی و انرژی‌های نو مورد بررسی قرار گرفته است.یافته‌های تحقیق نشان می‌دهد که در ایران و فرانسه، قوانین کیفری موجود برای مقابله با جرایم سایبری به‌ویژه تهدیدات علیه زیرساخت‌های فنی و انرژی‌های نو،به‌طورکامل و مؤثر پاسخگوی نیازهای روز نیستند.در حقوق ایران،قانون جرایم رایانه‌ای به‌طور خاص به مسائلی چون تهدیدات سایبری علیه زیرساخت‌های حیاتی پرداخته است،اما با توجه به تحولات فناوری،نیاز به اصلاح و تکمیل این قوانین احساس می‌شود. در فرانسه نیز،علی‌رغم وجود قوانینی برای حفاظت از اطلاعات و امنیت ملی،جرایم سایبری فرامرزی و پیچیدگی‌های آن‌ها موجب بروز چالش‌های جدی در شناسایی و پیگیری این تهدیدات شده است.نتایج تحقیق حاکی از ان است که ضرورت تدوین سیاست‌های کیفری افتراقی و نوین برای مقابله با جرایم سایبری و ارائه تدابیر خاص در راستای حفظ امنیت انرژی‌های نو و زیرساخت‌های فنی الزامی است.**کلیدواژگان**:جرایم سایبری؛انرژی های نو،زیر ساخت های فنی،سیاست کیفری افتراقی،حقوق ایران،حقوق فرانسه.

---

[۱]دانشجوی دکتری، گروه حقوق جزا و جرم شناسی، واحد بوشهر ، دانشگاه آزاد اسلامی ، بوشهر ، ایران

[۲]دانشیار گروه حقوق جزا و جرم‌شناسی ، دانشکده حقوق و علوم سیاسی ، دانشگاه علامه طباطبایی ، تهران ، ایران

[۳]استادیار گروه حقوق، واحد بوشهر، دانشگاه آزاد اسلامی، بوشهر، ایران

مقدمه

فضای سایبری با امکانات و تهدیدات بی‌شماری که ایجاد کـرده اسـت،نه تنها شکل جدیدی از جرایم سـنتی را معرفـی کـرده، بلکـه فرصـت‌هـای جدیدی برای ارتکاب انواع مختلف جرایم نوین،به‌ویـژه جـرایم سـایبری فراهم کرده است.این فضا به مجرمان سایبری این امکان را می‌دهد کـه در دنیای دیجیتال و از طریق شبکه‌هـای پیچیده،بـه فعالیـت‌هـای غیرقـانونی پرداختـه و از زیرسـاخت‌هـای مختلـف بهـره‌بـرداری کنند(انصـاری، ۵٤:۱۳۹٦).از این رو،یکی از حوزه‌های آسیب‌پـذیر در برابـر ایـن جـرایم، زیرسـاخت‌هـای انرژی،بـه‌ویـژه انـرژی‌هـای نوپدید،ماننـد انـرژی خورشیدی،بادی،هیدروژنی و دیگر فناوری‌های نوین انرژی اسـت کـه در دنیای امروز در حال گسترش و تحولی سریع هستند.این تهدیدات نه تنهـا می‌تواند امنیت این زیرساخت‌ها را تحت تأثیر قـرار دهد،بلکـه مـی‌توانـد اثرات عمیق و گسـترده‌ای بـر امنیـت ملی،اقتصـادی،اجتماعی،و فرهنگـی جوامـع بگـذارد.جـرایم سـایبری علیـه زیرسـاخت‌هـای انرژی،بـه‌ویـژه انرژی‌های نوپدید،دارای ویژگی‌هایی هسـتند کـه آن‌هـا را از دیگـر انـواع جرایم سایبری متمایز می‌سازد.از جمله این ویژگی‌ها می‌توان بـه سـهولت ارتکاب،ناشناخته بودن مرتکبان،فرامرزی بودن و تهدیدات چندجانبه آن‌ها اشاره کرد.به علاوه،این نوع جرایم می‌توانند در کوتاه‌ترین زمان ممکن بـه گسترش خسارت‌ها در سطح ملی و بین‌المللی منجر شـوند،به‌طـوری کـه حتی حملات به یک سامانه کوچـک مـی‌توانـد پیامـدهای عظیمـی بـرای زیرساخت‌های حیاتی و منابع طبیعی کشورهای مختلف بـه همـراه داشـته باشد.در این میان، نظام‌های حقوقی و قوانین کیفری کشورها باید توانـایی پاسخگویی به این تهدیدات پیچیده را داشته باشند و سیستم‌هـای قضـائی باید قادر باشند با این جرایم نوین و پیچیده به‌طور مـؤثر مقابلـه کننـد.در کشورهایی مانند ایران و فرانسه که در حال توسعه و گسترش انرژی‌هـای نوپدید هستند، توجه به قوانین و مقررات مخصوص برای مقابله با جرایم سایبری علیه این زیرساخت‌ها از اهمیت ویژه‌ای برخوردار است. ایـران و فرانسه به‌عنوان کشـورهای پیشـرو در حـوزه انـرژی‌هـای تجدیدپـذیر و

هوشمند، در معرض تهدیدات سایبری به این زیرساخت‌ها قرار دارند که ممکن است به‌طور مستقیم یا غیرمستقیم، به امنیت ملی و اقتصادی آن‌ها آسیب وارد کند.برای مثال،در ایران،که با پروژه‌های گسترده‌ای در حوزه انرژی خورشیدی و بادی مواجه است،تهدیدات سایبری علیه شبکه‌های هوشمند انرژی یا زیرساخت‌های حیاتی انرژی می‌تواند در شرایطی خاص به اختلال در تأمین انرژی و زیان‌های مالی و اجتماعی شدید منجر شود.از طرفی، فرانسه نیز که در حال توسعه شبکه‌های هوشمند انرژی و استفاده از منابع تجدیدپذیر است،به‌ویژه در مناطق حساس مانند ایستگاه‌های برق هسته‌ای و شبکه‌های توزیع انرژی با تهدیدات سایبری مواجه است. قوانین موجود در هر دو کشور،از جمله قانون جرایم رایانه‌ای ایران(۱۳۸۸)،قانون امنیت سایبری و قانون حفاظت از زیرساخت‌های حیاتی و قانون امنیت ملی فرانسه(۲۰۱۵)،به‌طور کلی به مقابله با جرایم سایبری پرداخته‌اند، اما هنوز نیاز به بازنگری و بروز رسانی در این قوانین به‌ویژه در زمینه جرایم سایبری علیه انرژی‌های نوپدید احساس می‌شود.

در این راستا،جرم‌شناسی و تحقیقات حقوقی می‌تواند نقش مهمی در شناسایی علل و عواملی که باعث وقوع این جرایم می‌شوند،ایفا کند.همچنین،با توجه به ویژگی‌های خاص فضای سایبری و تنوع تهدیدات آن،نیاز به توجه چندجانبه به علل زیستی،روانی،اجتماعی و فرهنگی در تحلیل جرایم سایبری و تدوین برنامه‌های پیشگیرانه وجود دارد.در این تحقیق،تلاش می‌شود تا با رویکرد کتابخانه‌ای و اسنادی به بررسی انحرافات فرهنگی و جرایم سایبری تأثیرگذار بر زیرساخت‌های انرژی نوپدید در حقوق ایران و فرانسه پرداخته شود و راهکارهایی برای تقویت قوانین و دادرسی‌های کیفری در مواجهه با این تهدیدات نوین و پیچیده ارائه گردد.این پژوهش همچنین به تحلیل چالش‌های حقوقی و جرم‌شناسی موجود در این زمینه و بررسی تطبیقی دو نظام حقوقی ایران و فرانسه خواهد پرداخت.در نتیجه، لازم است که هر دو کشور،به‌ویژه در حوزه‌های انرژی‌های تجدیدپذیر و زیرساخت‌های هوشمند انرژی،به‌طور

خاص به تدوین و بازنگری قوانین مرتبط با امنیت سایبری پرداخته و از همکاری‌های بین‌المللی در این زمینه بهره‌برداری کنند تا بتوانند از تهدیدات سایبری به این زیرساخت‌های حیاتی جلوگیری کرده و امنیت ملی و اقتصادی خود را حفظ کنند.

۱-تبیین جرم شناختی ماهیت و زمینه های جرایم سایبری

جرم‌انگاری جرم به هر دلیل و انگیزه‌ای که باشد نمی‌تواند به تشکیل یک سیاست جنایی مطلوب بیانجامد.هر چند که آن دلایل از حیث نظرات جرم‌شناسی کاملاً توجیه‌پذیر باشند آنچه که در این راستا اهمیت می‌یابد،جلوگیری از بحران و انسداد سیاست جنایی در مرحله اجرای آن در یک افق و دورنمای آینده است لذا توجیحات جرم‌شناسی برای واکنش کیفری به جرم،ممکن است تنها در کوتاه مدت اثر بخش بوده ولی در دراز مدت هیچگاه نمی‌تواند مطلوبیت سیاست جنایی را به نمایش بگذارد.

یکی از دیدگاه‌هایی که نسبت به رسانه‌ها و از جمله اینترنت در زمینه جرم‌شناسی وجود دارد،اعتقاد به تأثیر منفی رسانه‌ها از جنبه تهدید فرهنگ،اخلاق و قانون است،چرا که تصور می‌شود رسانه‌ها و به‌خصوص رسانه‌های تعاملی همچون اینترنت، به دلیل داشتن مخاطبانی از سرتاسر جهان و دسترسی‌های فراوان افراد به آن،در فرآیند جامعه‌پذیری و جهان‌دهی فرهنگی مخاطبان خود نقش عمده‌ای دارند و در مواردی الگوهای رفتاری و مراحل متضادی را ترویج می‌نمایند که بعضاً غیراخلاقی و مجرمانه هستند.معاشرت مکرر کاربران مسائلی با افراد یا گروه‌های مروج الگوهای مجرمانه در فضای مجازی،منجر به یادگیری و ارتکاب جرم توسط آنان می‌شود(بهرهمند و همکاران، ۱۳۹۳:۱۷۱).در واقع، با ظهور فضای مجازی نه تنها فرصت‌های جدیدی برای ارتکاب جرایم سنتی نظیر کلاهبرداری فراهم شده،بلکه با پدیدار شدن این فضا، جرایمی جدیدی مانند هک کردن محقق گردیده است که تا قبل از پیدایش اینترنت قابل تصور نبوده‌اند(ابراهیمی، ۱۳۹۳).جهت مقابله با تأثیر فضای مجازی در تکوین جرم، همچون فضای مادی،ابتدا باید به مطالعه

علمی جرم پرداخته شود تا بتوان از طریق شناسایی علل وقوع جرم،تـدابیر پیشگیرانه لازم را اتخاذ نمود.به عبارت دیگر،در فضای مجازی نه همچون فضای مادی بدون جستجوی علل وقـوع جـرم، ارائـه راهکارهـایی بـرای پیشگیری و مقابله با جرم،کار ممکن نخواهد بود(افتخارجهرمی و اسلامی، ۵۹:۱۳۹٤).است.

فرانســه،به‌عنــوان یکــی از کشــورهای پیشــرفته در زمینــه حفاظــت از زیرساخت‌ها و داده‌های دیجیتال،چارچوب‌های حقـوقی پیچیـده‌ای بـرای مقابله با جرایم سایبری دارد.فرانسـه از قـوانین متعـددی بـرای مقابلـه بـا جرایم سایبری استفاده می‌کند که از جمله آن‌ها می‌توان بـه قـانون امنیـت سایبری فرانسه و قانون حفاظـت از داده‌هـای شخصـی(GDPR) اشـاره کرد.این قوانین به‌طور خاص بر حفاظـت از اطلاعات،مقابلـه بـا حمـلات سایبری و مدیریت بحران‌های مرتبط با تهدیدات دیجیتال تمرکز دارند.در فرانسه، سازمان‌های مختلفی مانند۱ ANSSمسئول امنیت سایبری هسـتند و در مواردی که تهدیدات سایبری به زیرساخت‌های انـرژی نـو یـا سـایر بخش‌های حیاتی کشور مرتبط می‌شود،مداخله می‌کنند.در فرانسه، استفاده از فناوری‌های نوین در انرژی‌های تجدیدپذیر و هوشمندسازی شبکه‌های انرژی،این کشور را در معرض تهدیدات سایبری قرار داده است. حمـلات سایبری به سیستم‌های مدیریت انرژی و حملات به زیرساخت‌های تولیـد انرژی‌های تجدیدپذیر می‌توانند نه‌تنها منجر به اخـتلال در تـأمین انـرژی بلکـه خسـارات جبـران‌ناپـذیری بـه امنیـت ملـی وارد کننـد.هـدف از جرم‌انگاری این نوع اقدامات، حفظ امنیت عمومی و حفظ آسایش جامعـه است.

۱-۱حملات سایبری مبتنی بر تقابل امنیتی و انرژی

به دلیل ویژگی های منحصر بـه فـرد جـرایم سـایبری از جملـه سـهولت ارتکاب جرم، نامعلوم بودن آن،مرزی بودن جرم، سن کم مجرمـان، میـزان زیان وارده و تعداد زیاد قربانیان، جرایم سایبری منجـر شـده است.آسـیب

[1] - (Agence nationale de la sécurité des systèmes d'information)

های زیادی به امنیت ملی به ویژه در حوزه انرژی وارد می کند(ارشـدی و همکاران،۱٤۰۰:۸۳).

ماهیت گسترده و گستردگی جهانی فضای سـایبری زمینـه را بـرای ایجـاد تهدیـدات سـایبری در ابعـاد سیاسی،اقتصـادی، اجتماعی،فرهنگی،زیسـت محیطی و دفاعی–نظامی فراهم نموده است. تهدیـدات سـایبری در حـوزه نظامی و دفاعی بر خلاف ابعاد دیگر،رویکردی سخت و چهـره ای خشـن دارد. بسیاری از این تهدیدها احتمالاً به سبب محدودیت های بین المللـی وجود دارند و فقط جنبه بازدارندگی دارنـد. در صـورت افـزایش تـنش و درگیری بین کشورها،این تهدیدها به مرحله عملیات و جنگ می انجامـد.

در یک دسته بندی کلی، ویژگی های تهدیدات سایبری را می توان شـامل موارد زیر دانست: ۱- منبع تهدید: مزدوران سایبری یا گروه هـای مخفـی تحت حمایت دولت و...۲- پیامدهای تهدید: خطر سـایبری(احتمال سـوء استفاده از یک تهدید سایبری از آسیب پذیری سـایبری در یـک پایتخـت سایبری) و ... ۳–سطح تهدید: زیرساختی، سـازمانی، ملـی و...٤–احتمـال وقوع تهدید:احتمال اینکه یک تهدید از آسیب پـذیری بـرای ایجـاد یـک خطر سایبری سوءاستفاده کند شامل:بسیارکم،کم ،متوسط و زیـاد (بـالقوه) خطر سایبری).۵–شدت تهدیـد: شـدت بسـیار کـم ،شـدت پایین،شـدت متوسط و شدت بالا.بحـران هـا و زیـان‌هـایی ماننـد اخـتلال در اینترنـت بانکداری شبکه‌ای)، بیش از حد(خلیلی،۱٤۰۰:۱۰۲).

با توجه به افزایش حملات سایبری به زیرساخت‌های انرژی و تقابل‌هـای امنیتی ناشی از آن،کشورهای مختلف باید برای مقابلـه بـا ایـن تهدیـدات اقداماتی مؤثر انجام دهند.این اقدامات شامل تقویت زیرساخت‌های امنیتی سایبری،ارتقاء توانمندی‌های دفاعی سایبری،همکاری‌هـای بـین‌المللـی در زمینه امنیت انرژی و به‌ویژه توسعه سیسـتم‌هـای نظـارتی پیشـرفته بـرای شناسـایی و مقابلـه بـا حمـلات پـیش از وقـوع اسـت.همچنین، وجـود چارچوب‌های قانونی برای مقابله با تهدیدات سایبری و پاسخ به حملات، می‌تواند به کشورهای هدف کمک کند تـا بـا چـالش‌هـای ناشـی از ایـن حملات مقابله کنند و از آسیب‌های گسترده جلوگیری نمایند.در سال‌های

اخیر،تعدادی از حملات سایبری علیه زیرساخت‌های انرژی در سطح جهانی مشاهده شده است که نشان‌دهنده اهمیت روزافزون این تهدیدات در تقابل‌های امنیتی است:مانند حمله به شبکه برق اوکراین (۲۰۱۵)،حمله به شبکه برق ایالات متحده (۲۰۲۰)، Stuxnet (2010) .

۲-۱ اعمال هک‌های زیر ساخت های فنی و در دفاع از منافع اقتصادی دولتها

حملات سایبری به زیرساخت‌های فنی و فناوری‌های مرتبط با تأسیسات حیاتی یکی از چالش‌های بزرگ امنیتی در دنیای مدرن است.این حملات،که می‌توانند در راستای دفاع از منافع اقتصادی دولت‌ها یا در قالب جنگ‌های سایبری بین دولت‌ها صورت گیرند،تهدیدات جدی به شمار می‌آیند.این اقدامات،که به‌طور عمده به‌عنوان"هک‌های دولتی"یا"جنگ سایبری" شناخته می‌شوند،نه‌تنها می‌توانند امنیت ملی و زیرساخت‌های حساس مانند انرژی،حمل‌ونقل و ارتباطات را به خطر بیندازند،بلکه به‌شدت می‌توانند منافع اقتصادی کشورها را تحت تأثیر قرار دهند.

در بسیاری از موارد،دولت‌ها برای دفاع از منافع اقتصادی خود به انجام حملات سایبری متوسل می‌شوند.این حملات معمولاً تحت عنوان"جنگ‌های اقتصادی سایبری"شناخته می‌شوند و هدف آن‌ها می‌تواند شامل دسترسی به اطلاعات تجاری و صنعتی محرمانه،تخریب یا اختلال در عملکرد زیرساخت‌های اقتصادی،سرقت داده‌های مالی و اقتصادی و ممانعت از رقابت اقتصادی باشد.(میرخلیلی و عبداللهی، ۱۲۸:۱۳۹۷).به‌طور کلی،انگیزه‌های اصلی دولت‌ها از چنین حملاتی می‌تواند شامل موارد زیر باشد:

برخی دولت‌ها ممکن است از هک‌های سایبری برای حفاظت از زیرساخت‌های حیاتی اقتصادی خود استفاده کنند،مانند جلوگیری از سرقت فناوری‌های پیشرفته یا اطلاعات حساس در صنایع استراتژیک.در دنیای مدرن،دستیابی به فناوری‌های نوین و اطلاعات تجاری برای پیشی

گرفتن از رقبا امری حیاتی است.دولت‌ها ممکن است از حملات سایبری برای به دست آوردن اطلاعات حساس از شرکت‌های رقیب استفاده کنند.حملات سایبری به زیرساخت‌های کشورهای رقیب می‌تواند به‌عنوان ابزاری برای اعمال فشار سیاسی در راستای منافع اقتصادی یا ژئوپولتیک مورد استفاده قرار گیرد.یکی از مهم‌ترین حوزه‌هایی که هدف حملات سایبری دولتی قرار می‌گیرد،زیرساخت‌های انرژی است.این زیرساخت‌ها شامل تأسیسات تولید انرژی،شبکه‌های توزیع،سامانه‌های هوشمند انرژی و سیستم‌های ذخیره‌سازی انرژی هستند که نقش حیاتی در تأمین انرژی برای دولت‌ها و اقتصادهای کشورها دارند.حملات سایبری به این زیرساخت‌ها می‌توانند به‌طور عمدی برای آسیب رساندن به تأسیسات رقبا یا دشمنان اقتصادی صورت گیرند.

در ایران،قانون جرایم رایانه‌ای (مصوب ۱۳۸۸)به‌طور ویژه به جرایم سایبری پرداخته است.این قانون،که یکی از ابزارهای اصلی مقابله با حملات سایبری است،دسترسی غیرمجاز به سیستم‌های اطلاعاتی،سرقت داده‌ها و هک سیستم‌ها را جرم‌انگاری کرده است.ماده ۷۳۶ الی ۷۳۹ قانون مجازات اسلامی(بخش جرایم ضد امنیت داخلی و خارجی):این مواد به‌طور خاص به تخریب تأسیسات عمومی و حیاتی و اختلال عمدی در سیستم‌های حیاتی مانند انرژی پرداخته و مجازات‌هایی برای آن‌ها در نظر گرفته است.ماده ۱۰ قانون جرایم رایانه‌ای ایران با جرم‌انگاری حملات سایبری علیه سامانه‌های حیاتی،به‌ویژه در زمینه خدمات عمومی مانند آب، برق، گاز، مخابرات،حمل‌ونقل و بانکداری،نقش اساسی در حفاظت از امنیت ملی و آسایش عمومی ایفا می‌کند.با توجه به ماهیت حیاتی این زیرساخت‌ها و پیامدهای جدی هرگونه اختلال در عملکرد آن‌ها،مجازات‌های سنگین برای این نوع جرایم در نظر گرفته شده است تا از آسیب‌های اقتصادی،اجتماعی و سیاسی ناشی از تهدیدات سایبری جلوگیری شود.

در فرانسه،قانون امنیت سایبری و قانون حفاظت از زیرساخت‌های حیاتی به‌طور خاص به تهدیدات سایبری و حملات علیه زیرساخت‌های انرژی

پرداخته است.ماده L. 323-1 قانون کیفری فرانسه به‌طور خاص به جرم‌انگاری دسترسی غیرمجاز به سیستم‌های اطلاعاتی پرداخته است،که در بسیاری از موارد برای مقابله با حملات سایبری به تأسیسات انرژی و فناوری‌های حساس استفاده می‌شود.همچنین قانون امنیت ملی فرانسه (ماده L. 1332-1) به دولت این اختیار را می‌دهد که تدابیر ویژه‌ای برای حفاظت از زیرساخت‌های حیاتی کشور، از جمله شبکه‌های انرژی و اطلاعات، اتخاذ کند.

یکی از مهم‌ترین نکات در مورد هک‌های دولتی،تأثیرات اقتصادی آن‌ها است. این حملات می‌توانند موجب تخریب و اختلال در تجارت،سرقت اطلاعات اقتصادی و مختل کردن رقابت‌های اقتصادی شوند.در برخی موارد، این اقدامات می‌توانند به‌عنوان بخشی از جنگ اقتصادی یا به‌منظور ایجاد فضای رقابتی نامشروع انجام شوند.دولت‌ها می‌توانند برای کسب اطلاعات حساس و جلوگیری از پیشرفت رقبای اقتصادی خود، به سیستم‌های اطلاعاتی شرکت‌های رقیب حمله کنند.این حملات به‌ویژه در صنایع انرژی و فناوری اطلاعات می‌توانند به‌صورت هدفمند انجام شوند.مختل کردن رقابت‌های اقتصادی به‌ویژه در صنایع استراتژیک مانند انرژی و فناوری، حملات سایبری به‌منظور آسیب رساندن به رقبا یا جلوگیری از پیشرفت اقتصادی آن‌ها می‌تواند انجام شود.این نوع از حملات،که به‌طور ویژه در راستای منافع اقتصادی دولت‌ها صورت می‌گیرد،می‌تواند در نهایت به تضعیف رقابت و قدرت اقتصادی کشورها منجر شود.

۲- بازنمایی کیفری در حقوق کیفری ایران و فرانسه

جرایم سایبری، به‌ویژه آنهایی که زیرساخت‌های حساس مانند انرژی‌های نو را هدف قرار می‌دهند،با چالش‌های حقوقی متعددی روبه‌رو هستند.این چالش‌ها نه‌تنها به دلیل پیچیدگی‌های ماهوی این نوع جرایم،بلکه به‌ویژه به‌خاطر ویژگی‌های منحصر به‌فرد فضای سایبر و زیرساخت‌های فنی مرتبط با آن،از جمله انرژی‌های نو،مطرح می‌شوند.یکی از مهم‌ترین مشکلات،تعیین محل ارتکاب جرم است.در فضای سایبر،برخلاف فضای

فیزیکی،مرزهای جغرافیایی به‌طور واضح قابل شناسایی نیستندواین باعث می‌شودکه شناسایی مرجع صالح برای رسیدگی به این‌گونه جرایم دشوار و پیچیده باشد.به‌ویژه هنگامی که حملات سایبری از یک کشور به کشور دیگر منتقل می‌شود و اثرات آن به زیرساخت‌های حیاتی و انرژی‌های نو که حیاتی برای عملکرد کشورها هستند،وارد می‌شود.علاوه بر این،مسأله صلاحیت قضائی بین‌المللی در جرایم سایبری مطرح است.زمانی که جرم در فضای سایبر رخ می‌دهد،ممکن است از مرزهای یک کشور فراتر برود، به‌ویژه در جرایم مرتبط با انرژی‌های نوکه می‌توانند ابعاد فرامرزی داشته باشند.در این شرایط،کشمکش‌های حقوقی و اختلافات میان کشورها در خصوص اعمال صلاحیت قضائی می‌تواند منجر به بی‌اثری یا عدم اجرای مؤثر احکام قضائی شود.در این راستا،به‌روزرسانی و تکمیل قوانین داخلی و بین‌المللی در خصوص صلاحیت قضائی و نحوه رسیدگی به این‌گونه جرایم ضروری به نظر می‌رسد.

۱-۲رویارویی با جرایم سایبری علیه زیر ساخت‌های انرژی در حقوق ایران و فرانسه

در بررسی ویژگی‌های بزه‌های فضای مجازی و تمایزات آن‌ها با بزه‌های دنیای واقعی،به‌وضوح قابل درک است که الگوهای ارتکاب جرم در فضای دیجیتال با جرایم سنتی تفاوت‌های قابل توجهی دارند.این تمایزات،همراه با تحولات ناشی از پیدایش فضای سایبر، باعث می‌شود که سیستم کیفری سنتی نتواند به‌طور مؤثر با جرایم فضای مجازی مقابله کند.بنابراین،تبیین رویکرد افتراقی در قلمرو جرایم سایبری ضروری به نظر می‌رسد.

نظام کیفری سنتی بیشتر به دوره‌ای تعلق دارد که فناوری در مراحل ابتدایی خود قرار داشت،اما امروزه با رشد و پیشرفت فناوری‌های دیجیتال،استفاده از منابع انسانی سازمان‌یافته و امکانات متمرکز برای مقابله با بزهکاران فضای مجازی دشوار شده است.اگرچه صنایع مختلف مانند حمل‌ونقل و ارتباطات نیز بزهکاری‌های خاص خود را به‌دنبال داشته‌اند،اما از آنجا که این تغییرات عمدتاً جنبه کمی داشتند،نظام عدالت

کیفری توانسته است با سرعت بیشتری خود را با الزامات این تحولات تطبیق دهد.در حالی که جرایم فضای مجازی به‌ویژه از نظر پیچیدگی،گستردگی و ویژگی‌های خاص،نیازمند رویکردی جدید و تخصصی هستند که قادر به پاسخگویی به چالش‌های نوین این عرصه باشد(صبح خیز،۱۳۹۸:۱۲۱).

نظریه انتخاب عقلانی یکی از تئوری‌های بنیادین در جرم‌شناسی است که رفتارهای مجرمانه را به‌عنوان تصمیمات عقلانی افراد برای دستیابی به منافع شخصی و رفع نیازهای خود تحلیل می‌کند.بر اساس این نظریه،فرد مجرم به‌طور عقلانی موقعیت‌ها و فرصت‌های ارتکاب جرم را ارزیابی کرده و تصمیم می‌گیردکه آیا ارتکاب جرم برای او سودمند است یا خیر. این فرآیند شامل بررسی خطرات و منافع حاصل از عمل مجرمانه است و فرد معمولاً تصمیم می‌گیرد که با ارزیابی نسبت سود به ضرر، وارد عمل شود(شاه محمدی و تاهو، ۱۳۹۳: ۱۰۱).نظریه انتخاب عقلانی به‌ویژه در تحلیل جرایم سایبری و به‌طور خاص جرایم سایبری علیه زیرساخت‌های انرژی‌های نوپدید می‌تواندکاربرد قابل‌توجهی داشته باشد.(علیوردی‌نیا و صالح نژاد،۱۳۹٤:۲۱).

بر اساس این نظریه،فرد مجرم با تحلیل محیط و بررسی عواملی همچون هزینه و منفعت، تصمیم می‌گیرد که به ارتکاب جرم بپردازد یا از آن اجتناب کند.در فضای سایبری، جرایم علیه انرژی‌های نوپدید نیز از این قاعده مستثنی نیستند.به‌طور کلی،دو عامل مهم که در اتخاذ تصمیمات مجرمانه در فضای سایبری نقش دارند عبارتنداز:دردسترس بودن و جذابیت هدف.به عبارت دیگر،هنگامی که زیرساخت‌های انرژی‌های نوپدید به راحتی قابل نفوذ باشند و جذابیت بالایی برای مجرمان داشته باشند،احتمال ارتکاب جرم در این فضا بیشتر خواهد بود(گودرزی،۱٤۰۰:٤۳).

ماده L. 323-1 قانون کیفری فرانسه:دسترسی غیرمجاز به سیستم‌های اطلاعاتی:این ماده به‌طور کلی به جرم‌انگاری دسترسی غیرمجاز به

سیستم‌های اطلاعاتی پرداخته و این نوع اقـدامات را بـرای تهدیـد امنیـت ملی،به‌ویژه در بخش‌های حساس مانند انرژی،جرم محسوب می‌کند.

ماده L. 1332-1 قانون امنیت ملـی فرانسـه (Code de la défense) حفاظت از زیرساخت‌های حیاتی:این ماده به‌طور کلی بر اهمیت حفاظـت از زیرساخت‌های حیاتی کشور از جمله سیستم‌های انرژی تأکید می‌کند و به دولت اجازه می‌دهد که تدابیر ویژه‌ای بـرای جلـوگیری از تهدیـدات و حملات به این زیرساخت‌ها اتخاذ کند.

ماده ۳٤ قانون حمایت از داده‌هـای شخصـی فرانسـه[۲]امنیـت اطلاعـات و داده‌ها:این ماده به‌طور خاص به امنیت اطلاعات پرداخته و موظف می‌کنـد که هر سازمانی، به‌ویژه در زمینه‌های حساس همچون انرژی، تدابیر امنیتی لازم برای محافظت از داده‌ها را اتخاذ کند[۳].در زمینه امنیت انرژی،این ماده به‌ویژه برای شرکت‌های فعال در بخش انرژی تجدیدپذیر و یا شبکه‌هـای هوشمند انرژی که اطلاعات حساس را پردازش می‌کنند،از اهمیت بـالایی برخوردار است.در قانون کیفری فرانسه[٤] جرایم خاصی به‌طور غیرمسـتقیم به تهدیدات علیه امنیت انرژی پرداخته است. این جرایم می‌تواننـد شـامل فعالیـت‌هـایی باشـند کـه امنیـت ملـی یـا تأسیسـات انـرژی را بـه خطـر می‌اندازند.ماده L. 223-1 قانون کیفـری فرانسـه–خرابکـاری و تخریـب عمدی تأسیسات انرژی:این ماده به‌طور خاص به تخریب وخرابکـاری در تأسیسات حیاتی کشور،از جمله تأسیسات انرژی،پرداخته است.

۲-۲ انفعال قوانین کیفری در حوزه جرایم سایبری علیـه انـرژی‌هـای نوپدید

با گسترش سریع فناوری‌های دیجیتال و وابستگی بیشتر به زیرساخت‌های شبکه‌ای،جرایم سایبری به یکی از تهدیدات جدی در عرصه انـرژی‌هـای نوپدید تبـدیل شـده‌انـد.انرژی‌هـای تجدیدپـذیر و نوپدیـد نظیـر انـرژی

---

[2] -Loi Informatique et Libertés

[۳]متن ماده ۳٤:

«هر نهادی که داده‌های شخصی را پردازش می‌کند، باید تدابیر فنی و سازمانی لازم را برای جلوگیری از دسترسی غیرمجاز به این داده‌ها اتخاذ کند.»

[4] -Code pénal

خورشیدی،بادی،بیوماس،و هیدروژن در حال تبدیل شدن بـه بخـش‌هـای حیـاتی و اسـتراتژیک در کشـورها هسـتند.این در حـالی اسـت کـه زیرساخت‌های مرتبط با این انرژی‌ها،بـه‌ویـژه در مراحـل اولیـه توسـعه و گسترش،به دلیل ویژگی‌های فناورانه،پیچیدگی‌ها و نیـاز بـه نـوآوری‌هـای مستمر،در برابر تهدیدات سایبری آسیب‌پذیر هستند.

۳-۲ضرورت توسعه قوانین کیفری برای مقابله با جرایم سایبری علیـه انرژی‌های نوپدید

حوزه انرژی به‌دلیل اهمیت حیاتی آن برای کشـورهای مختلـف،از جملـه تأسیسات و منابع انرژی کـه بـه‌عنـوان ارکـان زیرسـاختی در هـر کشـور محسوب می‌شود،به‌طور مداوم در معرض تهدیدات مختلـف قـرار دارد.از جمله این تهدیدات،جرایم سایبری است که به یکی از معضلات جدی در حوزه انرژی تبـدیل شـده اسـت.در دنیـای امروز،بـا پیشـرفت فنـاوری و افزایش وابستگی به سیستم‌های دیجیتال،آسیب‌پذیری تأسیسات انرژی در برابر حملات سایبری به شدت افزایش یافتـه اسـت.از همـین رو، تـدوین یک قانون کیفری جداگانه برای حوزه انرژی،با توجـه بـه پیچیـدگی‌هـا و ویژگی‌های خاص جرایم این حوزه،به‌ویژه جرایم سایبری،امری ضـروری به نظر می‌رسد.

انفعال یا کمبود قوانین کیفری در حوزه جرایم سایبری علیـه انـرژی‌هـای نوپدید،چالش‌های قابل توجهی را برای کشـورهای مختلـف ایجـاد کـرده است.یکی از دلایل عمده این مسئله،سرعت پیشرفت فناوری‌ها در عرصـه انرژی‌های نوپدید است که ممکن است قوانین موجود نتواننـد بـه‌سـرعت تغییرات و تهدیدات جدید را شناسایی و پاسخ دهنـد.(آمری و همکـاران، ۱۳۹۹:۵٦).

٤-۲انفعال قوانین بر امنیت انرژی‌های نوپدید

بـا گسـترش فنـاوری‌هـای نـوین و افـزایش وابسـتگی بـه سیسـتم‌هـای دیجیتـال،یکی از چـالش‌هـای اساسـی در حقـوق کیفـری در بسـیاری از کشورها،به‌ویژه در ایران و دیگر کشورهای در حال توسـعه،انفعال قـوانین کیفری در حوزه جرایم سایبری علیه انرژی‌های نوپدید اسـت.انرژی‌هـای

نوپدید شامل انرژی‌های تجدیدپذیر و پاکی مانند انرژی خورشیدی،بادی،زیستی،و سایر فناوری‌های نوین انرژی هستند که به‌طور فزاینده‌ای در حال تبدیل به بخش‌های حیاتی زیرساخت‌های ملی می‌باشند.

بیشتر قوانین موجود در حوزه جرایم سایبری،به‌ویژه در حقوق کیفری ایران،عمدتاً بر روی زیرساخت‌های انرژی سنتی متمرکز هستند و به‌طور خاص به تهدیدات سایبری علیه انرژی‌های نوپدید نمی‌پردازند.این موضوع باعث ایجاد چالش‌هایی در زمینه حفاظت قانونی از زیرساخت‌های انرژی‌های تجدیدپذیر می‌شود.انرژی‌های نوپدید معمولاً از سیستم‌های پیچیده و هوشمند استفاده می‌کنند که تهدیدات سایبری علیه این سیستم‌ها،به‌ویژه با استفاده از فناوری‌هایی مانند اینترنت اشیا و شبکه‌های برق هوشمند،می‌تواند آسیب‌های گسترده‌ای به سیستم‌های انرژی و حتی اقتصاد کشور وارد کند.با این حال،قوانین موجود به‌طور کامل قادر به پاسخگویی به این تهدیدات نیستند و بسیاری از جرایم سایبری علیه انرژی‌های نوپدید به‌ویژه در چارچوب‌های قانونی ناشناخته یا بی‌پاسخ باقی می‌مانند(عباسی کلیمانی،اکبری، ۱۳۹٤:۳۲).

یکی از مهم‌ترین چالش‌های موجود در این زمینه،کمبود قوانین خاص در رابطه با انرژی‌های نوپدید است.در اکثر نظام‌های حقوقی،به‌ویژه در ایران،توجه به قوانین خاص در مورد تهدیدات سایبری علیه انرژی‌های تجدیدپذیر وجود ندارد.به همین دلیل،بسیاری از حملات سایبری که به زیرساخت‌های انرژی‌های نوپدید وارد می‌شود،بدون پاسخ می‌مانند. در سطح جهانی نیز،حملات سایبری به سیستم‌های انرژی‌های نوپدید در حال افزایش است.سیستم‌هایی مانند انرژی خورشیدی و توربین‌های بادی که در بسیاری از کشورها به‌طور گسترده‌ای استفاده می‌شوند،می‌توانند هدف حملات سایبری قرار گیرند.این حملات می‌توانند شامل دستکاری در داده‌ها،اختلال در عملکرد سیستم‌ها یا حتی آسیب به تجهیزات حساس باشند.

برای مقابله با این تهدیدات،کشورها نیاز دارند تا قوانین و مقررات خاصی را برای حفاظت از سیستم‌های انرژی‌های نوپدید وضع کنند.این قوانین باید شامل مجازات‌های مشخص برای حملات سایبری علیه این سیستم‌ها و همچنین اقدامات پیشگیرانه برای شناسایی و مقابله با تهدیدات باشد.(سعیدی،۱۳۹٦:۲۹).

در حقوق ایران و فرانسه،قوانین موجود برای مقابله با تهدیدات سایبری علیه زیرساخت‌های حیاتی،از جمله انرژی‌های نوپدید،به‌طور کلی وجود دارند اما با کاستی‌هایی مواجه هستند که نیاز به اصلاح و به‌روزرسانی دارند.ایران،قانون جرایم رایانه‌ای به تهدیدات سایبری علیه سامانه‌های حیاتی عمومی اشاره دارد،اما هیچ مقرره خاصی برای انرژی‌های نوپدید مانند انرژی‌های خورشیدی و بادی وجود ندارد.همچنین،مفهوم"زیرساخت‌های حیاتی"در این قانون به‌طور دقیق تعریف نشده و ممکن است شامل برخی سیستم‌های انرژی نوپدید نشود.علاوه بر این،ضعف در مکانیزم‌های نظارتی و همکاری‌های بین‌المللی در مقابله با تهدیدات سایبری،یکی دیگر از چالش‌های موجود است.در فرانسه، قانون امنیت سایبری تلاش‌هایی برای تقویت حفاظت از زیرساخت‌ها به‌ویژه در برابر تهدیدات سایبری انجام داده،اما هنوز پوشش کاملی برای انرژی‌های نوپدید و تهدیدات سایبری پیچیده این حوزه‌ها وجود ندارد.قوانین موجود به سیستم‌های هوشمند انرژی و اینترنت اشیا در این بخش به‌طور کافی نمی‌پردازند و نیاز به همکاری‌های بین‌المللی بیشتر و اجرای نظارت‌های مستمر برای مقابله با حملات پیچیده احساس می‌شود.(صبح خیز،۱۳۹۸:۱۲٤).

۵-۲لزوم بازنگری در قوانین کیفری و تدوین مقررات جدید

برای مقابله مؤثر با جرایم سایبری علیه انرژی‌های نوپدید،لازم است که کشورهای مختلف،به‌ویژه ایران،اقدام به بازنگری در قوانین کیفری و تدوین مقررات جدید کنند.این قوانین باید به‌طور خاص به مسائل مربوط به تهدیدات سایبری علیه زیرساخت‌های انرژی‌های نوپدید توجه داشته باشند.در راستای مقابله با چالش های حوزه انرژی و به ویژه تهدیدات

سایبری،چندین قانون و آیین‌نامه در ایران به تصویب رسیده‌اند که به‌طور مستقیم یا غیرمستقیم به مسائل حقوقی و کیفری مرتبط با این حوزه پرداخته اند.قانون اصلاح الگوی مصرف انرژی(۱۳۸۹)با هدف کاهش اتلاف انرژی و بهینه‌سازی مصرف آن تصویب شد.قانون توسعه انرژی‌های تجدیدپذیر(۱۳۹۵)نیز به حمایت از تولید و استفاده از انرژی های پاک پرداخته و هدف آن ارتقاء تولید انرژی های تجدیدپذیر همچون انرژی خورشیدی و بادی به منظور کاهش وابستگی به منابع غیرقابل تجدید است.این قانون در کنار سایر قوانین،زمینه ساز تحولی اساسی در تأمین انرژی به صورت پایدار و در راستای حفظ محیط زیست است.

در مجموع،این قوانین و آیین‌نامه‌ها در کنار هم یک چارچوب حقوقی جامع برای حمایت از انرژی های تجدیدپذیر، بهینه سازی مصرف انرژی و حفاظت از زیرساخت‌های حیاتی ایجاد کرده‌اند،که در کاهش تهدیدات و چالش های این حوزه، به‌ویژه جرایم سایبری،مؤثر خواهد بود.زیرساخت های بخش انرژی به خاطر داشتن ارزش اقتصادی بالا همواره مورد توجه دولت‌ها و عوامل خصوصی بوده است.چنین افزایشی در تعداد بازیگران و مرتکبان حملات سایبری باعث می‌گردد حجم حملات سایبری به زیرساخت‌های بخش انرژی افزایش یابد و اگر دولت‌ها نتوانند اقدامات احتیاطی و حفاظتی را برای حفاظت از زیرساخت‌ها و تأسیسات این حوزه مانند آب،برق،نفت،گاز و سایر حوزه‌های مرتبط انجام دهند،در آینده به دلیل گسترش در تعداد حملات سایبری و مرتکبان این حملات،شاهد ناامنی و برهم خوردن امنیت زیرساخت‌های این حوزه خواهند بود.(مجیدی، ۷۶:۱۳۹۳).

این دلیلی است که هدایت‌کنندگان این حملات به انجام آن‌ها تمایل دارند و هر روز شاهد افزایش این حملات در سطح جهان هستیم در نهایت، انفعال قوانین کیفری در حوزه جرایم سایبری علیه انرژی‌های نوپدید به‌ویژه در کشورهای در حال توسعه،از جمله ایران، می‌تواند تهدیدات قابل توجهی را به همراه داشته باشد.بنابراین، تدوین قوانین ویژه و جامع

در این زمینه،تقویت همکاری‌های بین‌المللی،و به‌روز رسانی سیستم‌های امنیتی و نظارتی از الزامات اساسی برای مقابله با این چالش‌های نوظهور به‌شمار می‌روند.(جلالی فراهانی، ۴۵:۱۳۹۵)در مقابله با جرایم سایبری باید از یک رویکرد توصیفی و توصیه‌ای برای شناسایی و تدوین سیاست‌های کیفری استفاده کرد.در این راستا،علاوه بر بازنگری در قانون جرائم رایانه‌ای مصوب ۱۳۸۸،توجه به نیازهای جدید نظام کیفری ایران و تطابق آن با چالش‌های نوین جرایم سایبری ضرورت دارد.

۶-۲چالش‌ها و موانع پیشگیری از جرایم سایبری در حوزه انرژی

بسیاری از کشورها با کمبود متخصصان سایبری در حوزه انرژی روبه‌رو هستند،که این می‌تواند به کاهش توانایی در تشخیص و مقابله با تهدیدات سایبری منجر شود.هماهنگی ناکافی میان سازمان‌های دولتی،شرکت‌های خصوصی و نهادهای بین‌المللی می‌تواند منجر به ضعف در پاسخگویی به تهدیدات سایبری و مشکلات اجرایی شود.با پیشرفت سریع فناوری‌ها و تغییرات دائمی در تهدیدات سایبری،بسیاری از کشورها و شرکت‌ها قادر به حفظ هم‌پایی با این تغییرات نیستند و این می‌تواند خطرات امنیتی جدیدی ایجاد کند.این نظریه به‌ویژه در زمینه پیشگیری از جرایم سایبری علیه انرژی‌های نوپدید و کاهش آسیب‌پذیری زیرساخت‌ها در دنیای دیجیتال می‌تواند مفید باشد.بر اساس این دیدگاه،اتخاذ تمهیدات پیشگیرانه برای کاهش جذابیت اهداف مجرمانه و دشوارتر کردن ارتکاب جرم می‌تواند موثر واقع شود.(حیدری نژاد، ۳۴:۱۳۹۷).برای پیشگیری از جرایم سایبری علیه زیرساخت‌های انرژی‌های نوپدید و کاهش آسیب‌پذیری این شبکه‌ها،می‌توان راهکارهایی مبتنی بر نظریه انتخاب عقلانی اتخاذ کرد.این راهکارها شامل مواردی همچون افزایش سطح امنیت سامانه‌ها، تقویت نظارت بر فعالیت‌های آنلاین،آموزش کاربران و توسعه زیرساخت‌های حفاظتی هوشمند هستند.با استفاده از این اقدامات،می‌توان جذابیت اهداف مجرمانه را کاهش داد و به‌طور کلی،فرصتی را برای ارتکاب جرم از مجرمان سایبری سلب کرد.(خانعلی‌پور واجارگاه، ۱۲۴:۱۳۹۰).همچنین،در راستای کاهش

فرصت‌های ارتکاب جرم در فضای مجازی،باید توجه ویـژه‌ای بـه ایجـاد موانع و سدهای امنیتی داشت کـه دسترسـی بـه شـبکه‌هـای انـرژی‌هـای تجدیدپذیر و دیگر زیرساخت‌های حیـاتی را دشـوار و زمـان‌بـر کنـد.این اقدام نه تنها می‌تواند باعث کاهش میزان حمـلات سـایبری شـود،بلکه بـه ارتقاء امنیت کلی در دنیای دیجیتال نیز کمک خواهد کرد.استفاده از نظریه انتخاب عقلانی در تحلیل و پیشگیری از جرایم سایبری علیه انـرژی‌هـای نوپدید،نشان می‌دهد که درک دقیق‌تر رفتار مجرمان و ملاحظـات عقلانـی آن‌ها در فضای سایبری،می‌تواند به ارائه راهکارهای مؤثر در مقابله با ایـن جرایم کمک کند.

٦-٢-١تدابیر پیشگیرانه در حقوق ایران

ماده ۱۰ قانون جرایم رایانه ای (۱۳۸۸)این ماده به طور خاص بـه جـرایم سایبری علیه سامانه‌های رایانه‌ای و مخابراتی اشاره دارد که برای خـدمات عمومی ضروری مانند برق، آب،گاز و مخابرات استفاده می‌شـود. هرگونـه حمله سایبری به این سیستم‌ها با مجازات حـبس از ۳ تـا ۱۰سـال مواجـه می‌شود.

ماده ۱:در این ماده،جرایم رایانـه‌ای بـه‌طـور کلـی تعریـف شـده اسـت و هرگونه دستکاری،تغییر،خرابکاری یا ایجاد اختلال در سامانه‌های رایانه‌ای که باعث آسیب به امنیت اطلاعات یا زیان مـالی شـود،جرم‌انگـاری شـده است.

ماده ۱۲:این ماده مربوط به اعمال مجازات‌ها برای اقدامات خرابکارانـه در شـبکه‌هـای رایانـه‌ای و زیربنـای حیـاتی اسـت کـه مـی‌توانـد شـامل زیرساخت‌های انرژی‌های نوپدیـد شـود.(الهـی مـنش،۱۳۹۱:١٦٥).قـانون مدیریت داده‌ها و اطلاعات ملی مصوب ١٤٠١این قانون برای حفاظـت از اطلاعات و امنیت سـامانه‌هـای اطلاعـاتی کشـور طراحـی شـده اسـت و تدابیری برای پیشگیری از نفوذ سایبری به سـامانه‌هـای حیـاتی کشـور،از جمله زیرساخت‌های انرژی،در نظر گرفتـه اسـت.در ایـن قـانون بـه‌طـور غیرمستقیم به تهدیدات سایبری علیـه سـامانه‌هـای انـرژی اشـاره شـده و مکانیسم‌هایی برای ارتقاء امنیت این سامانه‌ها وضع شده است.

٦-٢-٢تدابیر پیشگیرانه در حقوق فرانسه

با استفاده از قانون امنیت سایبری فرانسه (۲۰۱۹)در ماده:L1332-1 می-توان دریافت که این ماده تحت قانون امنیت سایبری فرانسه،به محافظت از زیرساخت‌های حیاتی کشور در برابر حملات سایبری اشاره دارد و نهادهای مختلف را ملزم به ارتقای امنیت سایبری در این زیرساخت‌ها می‌کند.زیرساخت‌هایی مانند شبکه‌های هوشمند برق، انرژی خورشیدی و توربین‌های بادی نیز در این قانون در نظر گرفته شده‌اند.همچنین ماده :L111-1این ماده تأکید دارد که تمامی نهادهای عمومی و خصوصی که در حوزه‌های زیرساخت‌های حیاتی فعالیت می‌کنند،باید اقدامات پیشگیرانه و امنیتی مناسبی را برای مقابله با تهدیدات سایبری اتخاذ کنند.این اقدامات می‌توانند شامل ارزیابی ریسک، شناسایی آسیب‌پذیری‌ها و تدوین برنامه‌های اضطراری باشند.قانون دفاع و امنیت ملی فرانسه(۲۰۱۳)در ماده:L1132-1 بیان می‌دارد که به اقدامات خاص دفاعی در برابر حملات سایبری به زیرساخت‌های حیاتی مانند زیرساخت‌های انرژی می‌پردازد.قانون امنیت ملی فرانسه مسئولیت‌های مختلفی را برای دولت و نهادهای امنیتی در مقابله با تهدیدات سایبری به عهده می‌گذارد و از جمله،بر لزوم نظارت مستمر بر شبکه‌های انرژی تأکید دارد.(گودرزی،۱٤۰۰:۵۲).ماده ۳ قانون امنیت اطلاعات فراوان (Loi n° 2013-1168)این ماده به تأسیس و تقویت مراکز امنیت سایبری برای نظارت و محافظت از سیستم‌های اطلاعاتی حیاتی اشاره دارد.به‌ویژه در بخش‌هایی مانند انرژی‌های نوپدید که به فناوری‌های پیچیده و اینترنت اشیا وابسته هستند،تدابیر امنیتی ویژه‌ای برای محافظت از داده‌ها و زیرساخت‌ها در نظر گرفته شده است(دشتی،۱٤۰۰:٤۲).

قانون همکاری‌های بین‌المللی فرانسه در زمینه امنیت سایبری(۲۰۱٦)این قانون به همکاری‌های بین‌المللی برای مقابله با حملات سایبری در سطح جهانی می‌پردازد و تأکید دارد که فرانسه به عنوان عضو اتحادیه اروپا و سایر سازمان‌های بین‌المللی باید در مبارزه با تهدیدات سایبری،از جمله تهدیدات علیه انرژی‌های نوپدید،همکاری داشته باشد.تشکیلات

طراحی‌شده برای مبارزه با تروریسم در فرانسه از سازمان‌دهی بالایی برخوردار است.یکی از نتایج این سازمان‌دهی همه‌جانبه بودن تلاش‌ها برای مبارزه با تروریسم است.در این راستا لازم به ذکر است که بخش‌های مختلف امنیتی،اطلاعاتی،قضایی و حتی تأمین اجتماعی با یکدیگر هماهنگ شده‌اند و در سطوح امنیتی،فرهنگی،توسعه،تکنولوژی و حتی منابع مالی با معضل تروریسم مبارزه شده است و نیز اینکه هم در سطح ملی و هم در سطح اتحادیه اروپا تلاش شده تا هماهنگی‌های لازم به عمل آید. چهارم،هم به جنبه‌های نظامی و هم به جنبه‌های غیرنظامی پرداخته‌شده است.(غفاریون اصفهانی،۱٤۰۱:۱٦۹).

چالش‌های پیشگیری از جرایم سایبری علیه زیرساخت‌های انرژی در ایران و فرانسه عمدتاً به مسائل حقوقی،فناوری، انسانی و بین‌المللی باز می‌گردد.کمبود قوانین خاص برای انرژی‌های نوپدید،محدودیت‌های منابع،آسیب‌پذیری‌های تکنولوژیکی و تهدیدات فرامرزی از جمله مهم‌ترین چالش‌هایی هستند که هر دو کشور با آن مواجه‌اند.برای حل این مشکلات،نیاز به توسعه قوانین جدید،آموزش گسترده،همکاری‌های بین‌المللی و سرمایه‌گذاری در زیرساخت‌های امنیت سایبری وجود دارد.

۷-۲الزامات فنی و تخصصی جرایم سایبری و چالش‌های دادرسی-های کیفری آن

با توجه به رشد فناوری‌های اطلاعات و ارتباطات،این جرایم به شدت پیچیده‌تر و فراگیرتر شده‌اند.از این رو،به‌روزرسانی قوانین و دادرسی‌های کیفری در پاسخ به این تهدیدات ضروری است.قوانین کیفری سنتی به‌طور معمول به‌طور کامل نمی‌توانند تهدیدات و جرایم سایبری را پوشش دهند.در نتیجه،کشورها باید قوانینی خاص برای مقابله با این نوع جرایم تصویب کنند.این قوانین باید تعریف واضح‌تری از جرایم سایبری داشته باشند،مجازات‌های خاص و کارآمد برای جرایم سایبری تعیین کنند و سازوکارهای جدید دادرسی برای رسیدگی به این جرایم ارائه دهند.یکی از چالش‌های مهم در دادرسی جرایم سایبری،کشف و اثبات

جرم است.پیچیدگی‌های فنی و عدم حضور فیزیکی مجرم در موقعیت وقوع جرم باعث می‌شود که ارائه شواهد در دادگاه دشوارتر شود.برای مواجهه با این چالش‌ها باید مقامات قضائی از تخصص فنی و کارشناسان حوزه فناوری اطلاعات بهره‌مند شوند،شواهد دیجیتال به‌طور قانونی جمع‌آوری و ذخیره شوند تا در محاکم قابل قبول باشند و دادگاه‌ها و قضات آموزش‌های ویژه‌ای در خصوص فناوری‌های نوین و چگونگی بررسی پرونده‌های سایبری دریافت کنند(مجیدی،۱۳۹۹:۳۸).

از آنجا که بسیاری از جرایم سایبری مرزها را در می‌نوردند و به‌راحتی از یک کشور به کشور دیگر منتقل می‌شوند،همکاری بین‌المللی در زمینه مبارزه با جرایم سایبری از اهمیت بالایی برخوردار است.سازمان‌ها و کنوانسیون‌های بین‌المللی نظیر کنوانسیون بوداپست به ایجاد چارچوب‌هایی برای همکاری بین کشورها در زمینه رسیدگی به جرایم سایبری کمک کرده‌اند. این همکاری‌ها باید در راستای اجرای قوانین،تسهیل استرداد مجرمان و تبادل اطلاعات در خصوص تهدیدات سایبری گسترش یابد.فناوری‌های جدید می‌توانند نقش مهمی در بهبود فرآیند دادرسی جرایم سایبری ایفا کنند.از آنجا که بسیاری از کاربران اینترنت از تهدیدات سایبری آگاهی ندارند،دولت‌ها باید برنامه‌های آگاهی‌سازی عمومی در خصوص خطرات سایبری و حقوق شهروندان در فضای مجازی را اجرا کنند.پیشگیری از جرایم سایبری،از طریق آموزش،اطلاع‌رسانی و تشویق به استفاده از سیستم‌های امنیتی مانند رمزنگاری و نرم‌افزارهای ضدویروس،می‌تواند تأثیر زیادی در کاهش وقوع این نوع جرایم داشته باشد. همچنین باید قوانینی برای جرم‌انگاری فعالیت‌هایی مانند انتشار بدافزار،حملاتDOS[5] و کلاهبرداری‌های اینترنتی ایجاد شود.(کتانچی و پور قهرمانی،۱۳۹۸:٤۹).

یکی از زیرساخت‌های حساس که بیشتر در معرض تهدیدات سایبری قرار دارد،بخش انرژی است.حملات سایبری به شبکه‌های انرژی می‌تواند عواقب جبران‌ناپذیری برای امنیت ملی و اقتصاد یک کشور به‌دنبال داشته

[5] - Denial of Service

باشد.به‌روزرسانی قوانین کیفری برای مقابلـه بـا جـرایم سـایبری در ایـن حوزه،شـامل جـرم‌انگـاری حمـلات بـه سیسـتم‌هـای انـرژی و ایجـاد مسئولیت‌های کیفری برای افرادی اسـت کـه از ابزارهـای سـایبری بـرای آسیب رساندن به این زیرساخت‌ها استفاده می‌کنند.(دشتی، ۱٤۰۰:۱٥٤).

نتیجه گیری

آنالیز و مدل‌های نظری رفتارهای دیجیتال،ارتباطات آنلاین و ساختار فضای مجازی نشان می‌دهد که این نظریه‌ها چگونه رفتارهای مجرمانه را در این محیط تحلیل می‌کنند.در زمینه جرایم سایبری علیه انرژی‌های نوپدید،این تحلیل‌ها می‌توانند به ما کمک کنند تا عواملی را که منجر به وقوع جرایم سایبری علیه زیرساخت‌های انرژی می‌شوند،شناسایی کنیم.فضای مجازی با ویژگی‌های خاص خود از جمله سهولت دسترسی،فرامرزی بودن و ناشناخته بودن مجرمان،زمینه‌ای را فراهم می‌آورد که مجرمان سایبری به راحتی می‌توانند به زیرساخت‌های انرژی‌های تجدیدپذیر و شبکه‌های هوشمند انرژی نفوذ کرده و آسیب‌های عمده‌ای به این زیرساخت‌ها وارد کنند.درک عمیق‌تری از عوامل مؤثر در تکوین جرم در فضای مجازی، به‌ویژه در ارتباط با جرایم سایبری علیه انرژی‌های نوپدید،به ما این امکان را می‌دهد که آسیب‌پذیری‌های این حوزه را شناسایی و مدیریت کنیم.از این رو،توجه به ابعاد جرم‌شناختی در پیشگیری از جرایم سایبری و ایجاد امنیت در فضای دیجیتال و شبکه‌های انرژی‌های تجدیدپذیر از اهمیت بالایی برخوردار است.ارائه راهکارهایی مبتنی بر دیدگاه‌های جرم‌شناختی،به‌ویژه در حوزه‌های آموزش،نظارت،و تأمین امنیت آنلاین در سیستم‌های انرژی،می‌تواند به پیشگیری از تهدیدات سایبری علیه این زیرساخت‌ها کمک کند.در این زمینه،پژوهش‌های بیشتر و توسعه مدل‌های جرم‌شناسی در راستای مقابله با جرایم سایبری علیه انرژی‌های نوپدید ضروری است.این پژوهش‌ها باید بر تحلیل دقیق‌تر رفتارهای مجرمانه در فضای مجازی،به‌ویژه در ارتباط با نفوذ به سامانه‌های انرژی‌های تجدیدپذیر و هک کردن شبکه‌های هوشمند انرژی، متمرکز شوند.از طریق استفاده از الگوهای رفتاری و فرآیندهای شناختی،می‌توان به نقش عواملی نظیر انگیزه‌ها،ادراکات و محیط فردی در شکل‌گیری این جرایم پی برد.

بهره‌برداری از ساختارهای مناسب و اقدامات پیشگیرانه در سیستم‌های دیجیتال و شبکه‌های اجتماعی می‌تواند به مقابله با این تهدیدات کمک

کند.امنیت شبکه‌های انرژی‌های نوپدید به‌ویژه در کشورهای در حال توسعه که به‌طور فزاینده‌ای به انرژی‌های تجدیدپذیر و هوشمند وابسته هستند،اهمیت ویژه‌ای دارد.از این جهت، توسعه پژوهش‌های بیشتر در این زمینه، با محوریت‌های مورد توجه قرار گرفته،می‌تواند به ارتقاء دانش ما از رفتارهای مجرمانه در فضای مجازی و جرایم سایبری علیه زیرساخت‌های انرژی کمک کند.به‌طور کلی،برای پیشگیری از جرایم سایبری علیه انرژی‌های نوپدید و حفظ امنیت انرژی در دنیای دیجیتال،لازم است که رویکردهای جرم‌شناختی نوین در کنار فناوری‌های پیشرفته امنیت سایبری به کار گرفته شوند تا شبکه‌های انرژی‌های تجدیدپذیر در برابر تهدیدات سایبری ایمن بمانند.در فرانسه، قوانین خاصی برای مقابله با تهدیدات علیه زیرساخت‌های انرژی و حفاظت از اطلاعات حساس در این بخش‌ها وجود دارد.یکی از مهم‌ترین قوانین در این زمینه،قانون امنیت سایبری است که به‌طور خاص بر امنیت سیستم‌های اطلاعاتی و حفاظت از داده‌ها متمرکز است. ماده L 323-1 قانون کیفری فرانسه،به جرم‌انگاری دسترسی غیرمجاز به سیستم‌های اطلاعاتی پرداخته و آن را برای تهدید امنیت ملی، به‌ویژه در بخش‌های حساس مانند انرژی، جرم محسوب می‌کند.در این راستا،هرگونه تلاش برای نفوذ به سیستم‌های کنترل انرژی یا دستکاری داده‌ها می‌تواند طبق این ماده مجازات شود.همچنین، قانون حفاظت از زیرساخت‌های حیاتی به‌طور خاص بر اهمیت حفاظت از تأسیسات حیاتی کشور تأکید دارد.این قانون به دولت اجازه می‌دهد که تدابیر ویژه‌ای برای جلوگیری از تهدیدات و حملات به زیرساخت‌ها اتخاذ کند.در فرانسه، در مواجهه با تهدیدات سایبری، به‌ویژه در زمینه انرژی‌های نو و زیرساخت‌های انرژی،قوانین گسترده‌ای برای حفاظت از اطلاعات و سیستم‌های حساس در نظر گرفته شده است.

در ایران،حقوق کیفری نیز قوانینی مشابه در زمینه مقابله با جرایم علیه امنیت انرژی و زیرساخت‌های حیاتی دارد،اما از آنجا که فضای قانونی و اجرایی ایران در این زمینه هنوز در حال تکامل است،چالش‌هایی در

مواجهه با تهدیدات جدید مانند حملات سایبری و امنیت انرژی وجود دارد.در ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸، به‌طور خاص به حفاظت از داده‌ها و سیستم‌های اطلاعاتی پرداخته است.این قانون،دسترسی غیرمجاز به سیستم‌های رایانه‌ای،هک و سرقت داده‌ها را جرم‌انگاری می‌کند.در زمینه امنیت انرژی، این قانون می‌تواند برای مقابله با حملات سایبری به تأسیسات انرژی و شبکه‌های توزیع انرژی به‌کار گرفته شود.ماده ۷۳٦ الی ۷۳۹ قانون مجازات اسلامی نیز به جرم‌انگاری تخریب عمدی تأسیسات عمومی و زیرساخت‌های حیاتی کشور پرداخته و آن را مشمول مجازات‌های شدید می‌کند.

یکی از شباهت‌های عمده بین حقوق کیفری ایران و فرانسه در زمینه جرایم علیه امنیت انرژی،تأکید بر امنیت سایبری است. هر دو کشور به‌طور جدی به مقابله با تهدیدات سایبری پرداخته‌اند و در این راستا، قوانینی برای حفاظت از سیستم‌های اطلاعاتی و تأسیسات حیاتی در نظر گرفته‌اند.در ایران، اگرچه قانون جرایم رایانه‌ای وجود دارد،اما در عمل چالش‌هایی از قبیل ناهماهنگی بین دستگاه‌های اجرایی و ضعف در اجرای دقیق مقررات، وجود دارد. این در حالی است که در فرانسه، نهادهایی مانند[٦] ANSSI مسئول نظارت و اجرای سیاست‌های امنیت سایبری هستند و تدابیر امنیتی ویژه‌ای برای محافظت از تأسیسات انرژی به‌ویژه در مقابل حملات سایبری در نظر گرفته شده است.در زمینه قانون‌گذاری در خصوص حملات تروریستی علیه تأسیسات انرژی،در فرانسه، ماده ٤٢١-٢ قانون کیفری به‌طور خاص به حملات تروریستی علیه زیرساخت‌ها و تأسیسات انرژی پرداخته و آن را به‌عنوان یک عمل تروریستی تلقی می‌کند.این نوع تهدیدات به‌ویژه در زمینه تأسیسات انرژی و دیگر زیرساخت‌های حیاتی کشور،تهدیدات جدی محسوب می‌شوند و هرگونه خرابکاری عمدی در این زمینه می‌تواند مجازات‌های سنگینی به همراه داشته باشد.مشابه این نوع جرم‌انگاری در ایران نیز در ماده ٦٨٧

[6]- Agence nationale de la sécurité des systèmes d'information

قانون مجازات اسلامی و برخی مقررات دیگر در زمینه حفاظت از تأسیسات انرژی وجود دارد.

در حقوق ایران و فرانسه،تدابیر پیشگیرانه برای مقابله با جرایم سایبری علیه زیرساخت‌های انرژی عمدتاً از طریق قوانین امنیت سایبری و حفاظت از زیرساخت‌های حیاتی پیش‌بینی شده‌اند.این تدابیر شامل مجازات‌های سخت‌گیرانه برای حملات سایبری به سامانه‌های انرژی،ارزیابی ریسک‌ها و آسیب‌پذیری‌ها، و همچنین تقویت همکاری‌های بین‌المللی در زمینه امنیت سایبری است.در حقوق ایران، قوانین مثل قانون جرایم رایانه‌ای و قانون حفاظت از اطلاعات به این مسئله پرداخته‌اند،در حالی که در فرانسه،قوانین خاص مانند قانون امنیت سایبری و قانون امنیت ملی اقدامات پیشگیرانه‌تری را در نظر گرفته‌اند تا از تهدیدات سایبری علیه انرژی‌های نوپدید و سایر زیرساخت‌های حیاتی جلوگیری کنند.با توجه به این موارد، می‌توان گفت که گرچه فرانسه و ایران در زمینه جرم‌انگاری و مقابله با جرایم علیه امنیت انرژی شباهت‌هایی دارند،اما تفاوت‌های مهمی در جزئیات اجرایی و ساختار قانونی هر یک از این کشورها مشاهده می‌شود.فرانسه به‌ویژه در زمینه نظارت و اجرای مقررات امنیت سایبری و مدیریت بحران‌های انرژی توانسته است گام‌های مؤثری بردارد،در حالی که ایران همچنان در مراحل ابتدایی تقویت زیرساخت‌های قانونی و اجرایی در این زمینه قرار دارد.اعمال هک‌های دولتی و حملات سایبری به زیرساخت‌های فنی و انرژی در راستای دفاع از منافع اقتصادی دولت‌ها،به‌ویژه در دنیای امروز که رقابت‌های اقتصادی و فناوری به اوج خود رسیده است،یکی از مسائل پیچیده و مهم در حقوق بین‌الملل و حقوق ملی است.این حملات،که به‌ویژه در زمینه‌هایی همچون انرژی، فناوری اطلاعات و رقابت‌های تجاری صورت می‌گیرند،نیازمند چارچوب‌های قانونی دقیق و مؤثر برای مقابله با آن‌ها هستند.کشورهای مختلف باید برای مقابله با این تهدیدات،قوانینی نوین و نهادهایی کارآمد برای شناسایی، پیگیری و مجازات چنین حملاتی ایجاد کنند،با توجه به تهدیدات فزاینده در دنیای

دیجیتال و وابستگی روزافزون به انرژی‌های نو،همکاری‌های بین‌المللی و تقویت ظرفیت‌های داخلی در زمینه حقوق کیفری و حفاظت از زیرساخت‌های انرژی در هر دو کشور ضروری به نظر می‌رسد.

منابع

۱.اردبیلی، محمدعلی(۱٤۰۱).حقوق جزای عمومی.تهران: میزان.

۲.ارشدی،علی یار؛بقایی،بهزاد و همکاران(۱٤۰۰)کتاب قوانین برق(تمامی قوانین در یک قانون جامع).تهران :انتشارات پژوهشگاه نیرو

۳.افتخار جهرمی،گودرز،اسلامی،ابراهیم (۱۳۹٤).نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرائم فضای مجازی.حقوقی دادگستری,(۸۸)، ۳۷-٦۳.

٤.انصاری،باقر(۱۳۹٦).حقوق ارتباط‌جمعی. تهران:سمت.

۵.آمری، محمدعلی، ملک‌زاده،سلیمان،مقیمی،مهدی،موسوی، سید رحیم (۱۳۹۹).پیشگیری از جرائم سایبری(سیاست‌ها و راهبردهای بین‌المللی).تهران:پژوهشگاه علوم انتظامی و پیشگیری ناجا.

٦.بهره‌مند،حمید،کوره‌پز،حسین محمد،سلیمی،احسان(۱۳۹۳).راهبردهای وضعی پیشگیری از جرائم سایبری.آموزه‌های حقوق کیفری,(۷)،۱٤۷-۱۷٦.

۷.بیگی،جمال،خوشیار،رزاق(۱۳۹۰).جرائم رایانه‌ای و مقابله با آن در اسناد بین‌المللی.همایش منطقه‌ای چالش‌های جرائم رایانه‌ای در عصر امروز, ۱-۱۵.

۸.جلالی فراهانی، امیرحسین(۱۳۹۵).درآمدی بر آیین دادرسی کیفری جرائم سایبری. تهران: خرسندی.

۹.حیدری نژاد،نصرالله (۱۳۹۷).پیشگیری وضعی در جرائم سایبری از منظر حقوق کیفری ایران و جهان.قانون یار, ۲(٦)، ۲۹-٤٤.

۱۰.حیدریان دولت‌آبادی،محمدجواد، آرش پور،علی‌رضا (۱۳۹۷).نگاهی نوین به مقوله نیابت قضائی بین‌المللی از دیدگاه حقوق عمومی ایران. دومین کنفرانس بین‌المللی نوآوری و تحقیق در علوم انسانی،مدیریت و معارف اسلامی, ۱-۱۵.

۱۱.خـــانعلی‌پـــور واجارگاه،ســـکینه (۱۳۹۰).پیشـــگیری فنـــی از جرم.تهران:میزان.
۱۲.دشتی، بیتا(۱٤۰۰).مطالعات تطبیقی جرائم سایبری در حقـوق ایـران و بین‌الملل.تهران:کهکشان علم.
۱۳.سعیدی،رحمان (۱۳۹٦).حقوق بین‌الملل ارتباطات سایبری.تهران:مجد.
۱٤.سلیمی،صادق(۱٤۰۱).سازوکار تضمین حقوق بشـری افـراد در پلـیس بین‌الملل. پژوهش‌های جرم شناختی پلیس, (٦)، ۲-۲٦.
۱۵.شاه‌محمدی،غلام‌رضا،تاهو،منصور(۱۳۹۳).بررسی شیوه‌های پیشـگیری از جرائم سایبری؛مبتنی بر فنـاوری اطلاعـات. پـژوهش‌هـای اطلاعـاتی و جنایی, ۹(۳)، ۹۹-۱۲۰.
۱٦.صبح خیز،رضا (۱۳۹۸).چالش‌های حقـوقی جـرائم سـایبری در نظـام حقوق بین‌الملل و نظام حقوقی ایران.پـژوهش‌هـای اطلاعـاتی و جنـایی, (۳۹)، ۱۱۷-۱۳۷.
۱۷.عباسی کلیمانی،عاطفه،اکبری،عاطفه(۱۳۹٤).جرائم سایبری.تهران:مجد.
۱۸.علیوردی‌نیا،اکبر.،صالح نـژاد، صـالح.، (۱۳۹٤)،"کاربسـت نظریـه‌هـای گزینش عقلانی در تبیین جرایم و ارائه دلالت‌های سیاسی برای پیشـگیری از جرم"،فصلنامه کارآگاه،شماره۲۵: ۹-
۱۹.غفاریون اصفهانی،محمدرضا (۱٤۰۱).همکاری‌های قضـائی در عرصـه بین‌الملل در مواجهه با انتقال محکومان.قانون یار, ٦(۲٤)، ۱٦۱-۱۸۰.
۲۰.کتانچی،الناز؛بابک پورقهرمانی(۱۳۹۸).«سیاست هـای نمـادین معاهـدۀ جرایم سایبری شورای اروپـا».فصـلنامۀ مطالعـات بـین‌المللـی، شـمارۀ ۲، ص۴۷-۳۱ DOI:10.22034/ISJ.2019.99238 .
۲۱.گـودرزی بروجردی،محمدرضـا ؛مقـدادی،لیال،(۱٤۰۰)،«درآمـدی بـر قانون مجازات فرانسه»،چاپ دوم،انتشارات خرسندی
۲۲.مجیدی،سید محمود (۱۳۹۳).جرایم علیه امنیت. چاپ دوم، تهران،نشر میزان.
۲۳.مجیدی،سید محمود، (۱۳۹۹)،«حقوق کیفری اختصاصی تطبیقی جرایم علیه امنیت»،چاپ چهارم،انتشارات میزان، تهران

٢٤.موسی زاده،رضا (١٤٠٠).بایسته‌های حقوق بین‌الملل عمومی. تهران:میزان.
٢٥.موسی زاده،رضا (١٤٠١).حقوق سازمان‌های بین‌المللی.تهران:میزان.
٢٦.میر خلیلی،سید محمود،عبداللهی،معاذ (١٣٩٧).مبانی اخلاقی-روان‌شناختی ضرورت جرم‌انگاری جرائم دولتی با تأکید بر مدل‌های حکومتی.پژوهش‌های اخلاقی, (٣٣)، ١٢٣-١٣٨.
٢٧.میر محمدصادقی،حسین (١٤٠١).حقوق جزای بین‌الملل.تهران:میزان.