شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

تمدن حقوقی

دوره ۹ - شماره ۲۷ - بهـار ۱۴۰۵

بار اثبات دعوا در داوری تجاری بین المللی
همایون مافی، مائده اصغرزاده
تحلیل رویه احراز صلاحیت دیوان کیفری بین‌المللی جهت رسیدگی به ازدواج اجباری
محمدحسین رمضانی قوام‌آبادی، پوریا ابراهیم زاده
بازاندیشی حقوقی در استفاده از هوش مصنوعی برای اجرای مجازات حبس در ایران و نظام های حقوقی مختلف
امیررضا محمودی، آنوشا ظفری کوره تاش
حقوق فدراسیونی در فوتبال: رویکرد نظام‌های حقوقی ایران، فرانسه، انگلستان، آرژانتین، برزیل، اسپانیا و کلمبیا
بهنام نورزاده
تعارض آیین نامه ماده سوم قانون الزام به ثبت رسمی معاملات اموال غیرمنقول با قوانین و اصول حقوقی
اکبر ایمان پور، سهند نجادی ایجادکار
شخصیت مجرمانه و رابطه آن با مجازات موثر
مریم بهمئی، مصطفی کرمی پور
چالش‌ها و موانع تفسیر قراردادها در حقوق ایران
فرزین یزدان پناه، محمدرضا نصیری
تدابیر پیشگیری از فساد مالی در نظام بانکی
علیرضا درائی، سیدابراهیم مرتضوی، امیرحسن ابوالحسنی
طلاق به درخواست زن در نظام حقوقی ایران
محمد احمدی، حلما سادات ذریه کرمانشاهی
ماهیت کیفری قرعه کشی های آنلاین در حقوق ایران
محمدحسین حاجب، زهرا ربانی، رویا آسیایی
قرارداد بیع متقابل در نظام حقوقی ایران
صادق محبی، محمدعلی جهانی
ویژگی ها و خصوصیات جرائم سایبری در نظام کیفری ایران
سیده الهه بابونکی
بررسی حق اشتغال زنان در حقوق بین الملل
حبیب اله عبداله پور، سما خدایاری
اثرگذاری اقدامات تأمینی و تربیتی در بازاجتماعی شدن بزهکاران نوجوان؛ نمونه پژوهی مجتمع قضایی شهید فهمیده
لیلا احدی
مقابله به مثل در قرآن کریم و جایگاه آن در سیاست کیفری اسلامی
رژین مسعودی، جمال رضایی حسین آبادی
واکاوی حقوقی ساختار نظارتی بازار غیرمتشکل پولی در ایران: از ابهامات مفهومی تا چالش‌های تقنینی و اجرایی
علی بابایی
تاثیر نهادهای مستقل بین المللی بر کارآمدی تحریم ها در حقوق تجارت بین الملل
الهه قربان کریمی
بر مدار مصلحت عالیه کودک؛ تحلیل حضانت با رویکرد حقوقی، فقهی و روان‌شناختی تا شناخت خلاهای تقنینی
مونا کمیلی
بازپروری حقوق بشرمدار و محدودیت های آن در نظام کیفری ایران
امین رضا بهار فلامرزی
تحلیلی بر مسئولیت محض مدنی در حوادث صنایع شیمیایی؛ مطالعه موردی واحدهای تولید متانول ایران
محمد جوکار، ساسان وزین پور
آسیب شناسی مجازات سالب حیات در حقوق کیفری ایران
محمدرضا رضائی
اجرای مقررات ملی شدن اراضی در خصوص اراضی وقفی با تاکید بر رویه قضایی
اسماعیل چوگانی
سیاست کیفری بین‌المللی در قبال نسل کشی: تحلیل تطبیقی در دادگاه‌های کیفری بین‌المللی
علی هادیان حقیقی، صابر سیاری زهان
تحلیل جرم شناختی کولبری در مناطق مرزی ایران و مقایسه آن با قاچاق کالا
مرتضی هاشم پور
چالش ها و آسیب های حقوقی موسسات اعتباری غیرمجاز در نظام پولی ایران
امین امینی نژاد
تاثیر اختلال کارکرد قشر پیش‌پیشانی بر مسئولیت کیفری در جرم قتل عمدی
حمید غیاثی، مهدی شعبان زاده
هوش مصنوعی و حق بر محاکمه عادلانه در پرتو قانون اساسی ایران
پوریا ژولیده
تأثیر مخارج و بدهی دولت بر رشد بازار سهام در ایران
راضیه حجتی نژاد
جایگاه نهاد طرف معامله مرکزی در معاملات فرامرزی و تأثیر آن بر اصل نسبی بودن قراردادها در حقوق ایران، اروپا و ایالات متحده آمریکا
عارفه قاسم زاده ده آبادی
راهکارهای پیشگیری و مقابله با جرائم سایبری
احمد پدیدار

تمدن حقوقی
دوره ۹، شماره ۲۷، بهار ۱۴۰۵
صفحات: ۷۲۰-۷۰۱
نوع مقاله: پژوهشی

Legal Civilization
Vol. 9, No. 27, Spring 2026
Pages: 701-720
Article Type: Original Research
https://www.pzhfars.ir/article_242791.html
doi: 10. 22034/lc. 2026. 579299. 1765

راهکارهای پیشگیری و مقابله با جرائم سایبری

Strategies to Combat and Deal with Cybercrime

احمد پدیدار
کارشناس ارشد حقوق کیفری و جرم‌شناسی، دانشگاه تابناک، لامرد، ایران
ahmadpadidar6@gmail.com

Ahmad Padidar
Master of Criminal Law and Criminology, Tabnak University, Lamerd, Iran

چکیده

جرائم سایبری به یکی از چالش‌های اساسی جوامع بشری در عصر حاضر تبدیل شده است که با گسترش روزافزون فناوری اطلاعات و ارتباطات، ابعاد پیچیده‌تری به خود گرفته‌اند. این جرائم که طیف وسیعی از فعالیت‌های غیرقانونی در فضای مجازی را دربرمی‌گیرند، از جرائم سازمان‌یافته فراملی گرفته تا کلاهبرداری‌های فردی و هتک حیثیت امنیت فردی، اجتماعی و حتی امنیت ملی را به‌طور جدی تهدید می‌کنند. در این پژوهش، با رویکردی تحلیلی-توصیفی، به بررسی جامع راهکارهای پیشگیری و مقابله با جرائم سایبری در نظام کیفری ایران پرداخته می‌شود. ابتدا، مفاهیم کلیدی مرتبط با جرائم سایبری و انواع رایج آن‌ها تشریح گردیده و سپس چهارچوب قانونی موجود برای مقابله با این جرائم مورد ارزیابی قرار می‌گیرد. در ادامه، راهکارهای پیشگیرانه در سطوح مختلف اعم از فنی، حقوقی، فرهنگی و آموزشی مورد بحث و بررسی واقع شده و اثربخشی آن‌ها در کاهش وقوع جرائم سایبری تبیین می‌گردند. همچنین، چالش‌ها و موانع موجود در مسیر پیاده‌سازی مؤثر این راهکارها از جمله خلأهای قانونی، ضعف زیرساخت‌های فنی، کمبود آموزش‌های تخصصی و همکاری‌های بین‌المللی‌شناسایی و تحلیل می‌شوند. در نهایت، با ارائه پیشنهاداتی کاربردی در جهت اصلاح و تکمیل قوانین، تقویت زیرساخت‌های فنی و قضایی، ارتقاء فرهنگ حقوقی شهروندان و توسعه همکاری‌های منطقه‌ای و بین‌المللی گامی مؤثر در جهت ایجاد محیطی امن و پایدار در فضای مجازی برداشته خواهد شد.

واژگان کلیدی: جرائم سایبری، علت‌شناسی، پیشگیری.

Abstract

Cybercrime has become one of the fundamental challenges of human societies in the present era, which has become more complex with the increasing expansion of information and communication technology. These crimes, which include illegal activities in cyberspace, from transnational organized crimes to individual fraud and defamation, seriously threaten individual, social and even national security. In this study, with an analytical-descriptive approach, a comprehensive study of the strategies for preventing and combating cybercrimes in the Iranian criminal system is conducted. First, the key concepts related to cybercrimes and their common types are explained, and then the existing legal framework for combating these crimes is evaluated. Next, preventive strategies at various levels, including technical, legal, cultural, and educational, are discussed and examined, and their effectiveness in reducing the occurrence of cybercrimes is explained. Also, challenges and obstacles in the path of effective implementation of these solutions, including legal gaps, weak technical infrastructure, lack of specialized training, and international cooperation, are identified and analyzed. Finally, by providing practical suggestions for amending and supplementing laws, strengthening technical and judicial infrastructure, promoting citizens' legal culture, and developing regional and international cooperation, an effective step will be taken towards creating a safe and sustainable environment in cyberspace.

Keywords: Cybercrime, Pathology, Prevention.

دریافت مقاله: ۱۴۰۵/۰۱/۲۲ - بازنگری مقاله: ۱۴۰۵/۰۲/۰۶ - پذیرش مقاله: ۱۴۰۵/۰۳/۱۰

Received: 2026/04/11 - Review: 2026/04/26 - Accepted: 2026/05/31

ارجاع:
پدیدار، احمد؛ (۱۴۰۵)، راهکارهای پیشگیری و مقابله با جرائم سایبری، شماره ۲۷.

مقدمه

پیدایش فضای مجازی در چند دهه اخیر یکی از بزرگ‌ترین نمادهای تحول جهانی است. رخدادی که تأثیرات شگرف آن هر روز در ابعاد فرهنگی، اجتماعی، اقتصادی، سیاسی، امنیتی و دفاعی در عرصه ملی و بین‌المللی نمود بیشتری پیدا می‌کند. هرگونه تغییر و تحول در دنیای کنونی به دلیل پیچیدگی فعالیت‌های انسانی، خواه ناخواه آثار و پیامدهایی به همراه خواهد داشت. به گونه‌ای که با اختراع وسیل‌های جدید، در کنار استفاده صحیح و مشروع از آن، همواره امکان سوءاستفاده از آن‌ها وجود دارد. در این راستا علم حقوق، به‌عنوان حامی عدالت و موجد توازن در جامعه انسانی، هر آن چه را که کوچک‌ترین خدشه‌ای به این توازن وارد نماید، تحت پوشش قرار داده و سعی در رفع یا پیشگیری از آثار نامطلوب آن می‌نماید. فضای سایبر که ماحصل پیشرفت‌های علمی و صنعتی در قرون اخیر است، از این قاعده مستثنی نبوده و آثاری به‌صورت مثبت و منفی در زندگی بشر وارد نموده است که ضرورت مطالعه آن را انکارناپذیر می‌نمایاند (امیریان فارسانی و همکاران، ۱۳۹۹، ۱۹۵).

گسترش لجام‌گسیخته فضای مجازی و نفوذ فناوری‌های نوین در تاروپود زندگی روزمره، ضمن ایجاد فرصت‌های بی‌شمار برای توسعه و تسهیل ارتباطات، بستری مساعد برای ظهور و گسترش جرائم سایبری نیز فراهم آورده است. این جرائم که با ویژگی‌هایی چون پیچیدگی فنی، قابلیت انکار،

فراملی بودن و دشواری کشف و اثبات همراه هستند نظم عمومی، امنیت اقتصادی، حریم خصوصی افراد و حتی اقتدار دولت‌ها را به‌طور جدی مورد تهدید قرار می‌دهند.

با وجود تلاش‌های صورت گرفته در تدوین قوانین و اتخاذ تدابیر امنیتی، نظام حقوقی و ساختارهای اجرایی کشور همچنان با چالش‌های جدی در زمینه پیشگیری مؤثر و مقابله قاطع با این پدیده نوظهور و رو به تزاید مواجه است. خلأهای قانونی، عدم تناسب برخی مجازات‌ها با شدت و گستردگی جرائم، ضعف زیرساخت‌های فنی و قضایی برای‌شناسایی و رهگیری مجرمان، کمبود آگاهی عمومی و تخصصی درباره مخاطرات فضای سایبری و شیوه‌های مقابله با آن و همچنین موانع همکاری‌های بین‌المللی در استرداد مجرمان و تبادل اطلاعات از جمله مهم‌ترین این چالش‌ها به شمار می‌روند. لذا، ضرورت بازنگری و اصلاح رویکردها، تدوین راهکارهای جامع و عملیاتی و تقویت همکاری‌های میان‌بخشی و بین‌المللی در زمینه پیشگیری و مقابله با جرائم سایبری، امری حیاتی و اجتناب‌ناپذیر است. این پژوهش درصدد است تا با تبیین جامع راهکارهای موجود وشناسایی نقاط ضعف و قوت نظام حقوقی ایران در این حوزه، به ارائه چهارچوبی مؤثر برای مقابله با جرائم سایبری بپردازد.

۱- علت‌شناسی جرائم سایبری

جرم‌شناسی قانون جرائم رایانه‌ای به مطالعه عوامل ایجاد جرم در فضای مجازی و تأثیرات آن بر دنیای حقیقی و راهکارهای پیشگیری از حدوث این گونه جرائم می‌باشد. مطالعات عینی پرونده‌های جرائم رایانه‌ای نشان می‌دهد ایجاد شخصیت جرائم فضای مجازی با ذهنیت عدم‌شناسایی و البته سهولت و گستردگی ارتکاب برخی بزه‌ها در این فضا بستر مناسبی را برای بروز خلاءهای شخصیتی و روانی فراهم می‌سازد. لذا ما بر این باور هستیم که شخصیت واقعی یک بزهکار رایانه‌ای را باید در همان شخصیت مجازی وی جست‌وجو کرد. به دیگر سخن، شخصیت مجازی که بزهکار رایانه‌ای از خود ساخته است در واقع همان خود واقعی او است که به دلایل مختلف امکان بروز آن در دنیای حقیقی را نداشته است (امیریان فارسانی و همکاران، ۱۳۹۹، ۱۹۷). جرائم سایبری، پدیده‌ای نوظهور و پیچیده، ریشه در تلاقی

عوامل سنتی جرم‌زا و ویژگی‌های منحصربه‌فرد فضای مجازی دارند. جرم‌شناسی معاصر، در تلاش برای فهم عمیق این پدیده، علل وقوع جرائم سایبری را در سه دسته کلی فردی، اجتماعی و اقتصادی و همچنین خصوصیات محیطی فضای سایبر را مورد بررسی قرار می‌دهد. این عوامل، ضمن تأثیرپذیری از یکدیگر، بستری مساعد برای ارتکاب تخلفات در گستره دیجیتال فراهم می‌آورند.

۱-۱- عوامل فردی و شخصیتی

در سطح فردی، خصوصیات روان‌شناختی و ویژگی‌های شخصیتی نقش تعیین‌کننده‌ای ایفاء می‌کنند. عواملی چون خودشیفتگی، حرص و طمع مالی، کینه‌توزی، پرخاشگری، حس انتقام‌جویی و میل به قدرت‌نمایی در فضای مجازی به دلیل کاهش موانع بازدارنده، سهولت اجرای بزه و امکان ناشناس ماندن تشدید یافته و راحت‌تر به بروز رفتارهای مجرمانه منجر می‌شوند. سن نیز در این میان متغیر مهمی است؛ درحالی‌که جرائم مالی سایبری غالباً توسط افراد در سنین بالاتر و باتجربه‌تر ارتکاب می‌یابد، جرائم مرتبط با هتک حیثیت، انتشار محتوای غیراخلاقی و آزار و اذیت در میان نوجوانان و جوانان شیوع بیشتری دارد. فضای مجازی با تسهیل دسترسی به محتوای آسیب‌زا و ایجاد بستری برای ارتباطات پنهانی، می‌تواند تأثیرات مخرب دوران بلوغ و نوجوانی را تشدید بخشد (وروایی و مومنی‌پور، ۱۳۹۱، ۹).

۱-۲- عوامل اجتماعی و فرهنگی

عوامل اجتماعی، از جمله ساختار خانواده، هنجارهای فرهنگی، تأثیر گروه همسالان و عملکرد رسانه‌ها، در شکل‌گیری ذهنیت و رفتار مجرمانه در فضای سایبری نقش دارند. ضعف در نهادهای تربیتی، ناکارآمدی نظام‌های نظارتی اجتماعی و عدم پایبندی به ارزش‌های اخلاقی بستر را برای پذیرش هنجارشکنان در محیط‌های مجازی فراهم می‌سازند. گروه همسالان در محیط‌های مجازی می‌توانند نه‌تنها به‌عنوان منبع انگیزه و تشویق، بلکه به‌عنوان تأمین‌کننده دانش فنی، ابزار و حتی توجیهات اخلاقی برای ارتکاب جرائم سایبری عمل کنند.

۱-۳- عوامل اقتصادی و محرومیت

شرایط نامساعد اقتصادی مانند فقر، بیکاری، تورم شدید، شکاف طبقاتی و احساس محرومیت نسبی، به‌عنوان یکی از قدرتمندترین محرک‌های ارتکاب جرم، در فضای سایبری نیز نمود پیدا می‌کنند. در جوامعی که ارزش‌های مادی و موفقیت مالی به‌شدت تبلیغ می‌شوند، اما راه‌های مشروع دستیابی به این اهداف محدوداند، افراد به سمت جرائم مالی سایبری مانند کلاهبرداری، فیشینگ و سرقت اطلاعات سوق داده می‌شوند. فضای سایبر با ارائه امکان دستیابی سریع و گاه پنهانی به منافع مالی، این انگیزه‌ها را تقویت می‌کند.

۲- ویژگی‌های محیطی فضای سایبر

ماهیت خود فضای سایبر، عاملی کلیدی در تسهیل ارتکاب جرائم است. انعطاف‌پذیری بی‌نظیر در زمان و مکان، امکان ناشناس ماندن نسبی یا کامل کاربران، گستردگی جهانی و نامحدود بودن بستر جرم و دسترسی آسان به اطلاعات و ابزارهای لازم همگی از عواملی هستند که ریسک ارتکاب جرم را کاهش داده و جذابیت آن را برای افراد با انگیزه‌های مجرمانه افزایش می‌دهند. این محیط، حس گمنامی و کاهش احساس مسئولیت‌پذیری را در فرد تقویت کرده و او را به سمت رفتارهای پرخطر سوق می‌دهد (جلالی فراهانی و باقری اصل، ۱۳۸۷، ۱۵۲).

علت‌شناسی جرائم سایبری، درک یکپارچه‌ای از تعامل پیچیده میان فرد، جامعه، اقتصاد و محیط دیجیتال را می‌طلبد. مقابله مؤثر با این پدیده، نیازمند اتخاذ رویکردهای چندوجهی است که ضمن تقویت عوامل بازدارنده فردی و اجتماعی به اصلاح شرایط اقتصادی و همچنین ارتقاء سواد و امنیت سایبری در جامعه توجه ویژه دارد.شناسایی و تحلیل این عوامل، گامی اساسی در جهت طراحی راهکارها و سیاست‌های پیشگیرانه اثربخش محسوب می‌شوند.

۳- پیشگیری از جرائم سایبری

مبحث حاضر با تمرکز بر رویکردهای جرم‌شناختی به پیشگیری از جرائم سایبری، به تبیین مفهوم

پیشگیری، تقسیم‌بندی انواع آن و تحلیل ظرفیت‌ها و چالش‌های هر رویکرد می‌پردازد. در چهارچوب جرم‌شناسی، پیشگیری مجموعه‌ای از اقدامات سازمان‌یافته و غیرخشونت‌آمیز است که هدف آن کنترل بزهکاری، کاهش وقوع جرم و مداخله در علل و زمینه‌های بزه‌زای آن است. در مورد تعریف پیشگیری، دیدگاه‌های متعددی ارائه شده است. موریس کوسن، جرم‌شناس نامدار کانادایی، آن را این‌گونه تعریف می‌کند: «مجموعه‌ای از اقدامات و استراتژی‌های غیرخشونت‌آمیز که با هدف کنترل بزهکاری، کاهش احتمال وقوع جرم و مهار آن از طریق ریشه‌یابی و مقابله با علل پدیده جنایت، به کار گرفته می‌شوند» (ابراهیمی، ۱۴۰۳، ۳۸). بر این اساس، دو نوع کلی پیشگیری در اسناد علمی و حقوقی برجسته شده است: پیشگیری کیفری و پیشگیری غیرکیفری.

۳-۱- پیشگیری کیفری

پیشگیری کیفری قدیمی‌ترین شیوه مقابله با بزهکاری است و بر استفاده از ضمانت‌اجراهای کیفری شامل مجازات‌ها و اقدامات تأمینی و تربیتی و همچنین کارکرد مجموعه نظام عدالت کیفری متکی است. این نوع پیشگیری در دو سطح عمومی و خصوصی عمل می‌کند:

پیشگیری عمومی با اتکاء به تهدید قانونی، هشدار نسبت به نتایج ارتکاب جرم و تقویت احساس نظارت و کشف‌پذیری تلاش می‌کند احتمال ورود افراد عادی به ورطه بزه را کاهش دهد. پیشگیری خصوصی با اعمال مجازات بر مجرمان، آنان را از تکرار رفتار مجرمانه بازمی‌دارد.

کارآمدی این رویکرد مبتنی‌بر اصولی چون حتمیت، قطعیت و تناسب مجازات‌ها است؛ اصولی که تخطی از آن‌ها کارکرد ارعابی و بازدارنده حقوق کیفری را تضعیف می‌کند. در حوزه جرائم سایبری، قانون‌گذار ایران با تصویب قوانینی مانند قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹، قانون تجارت الکترونیک مصوب ۱۳۸۲ و در قانون جامع جرائم رایانه‌ای مصوب ۱۳۸۸ تلاش کرده بستر حقوقی این نوع پیشگیری را تقویت کند (فضلی، ۱۳۸۹، ۱۲۴). بااین‌حال، پیشگیری کیفری در فضای سایبری با محدودیت‌های ساختاری مواجه است: رمزنگاری و

امکان حذف سریع داده‌ها، ناشناس‌بودن مجرمان، گستردگی شبکه‌ها، حجم عظیم اطلاعات و ضعف تخصصی بخشی از ضابطان و قضات همگی موجب می‌شود اتکای صرف به ابزار کیفری ناکافی و در مواردی ناکارآمد باشد.

۳-۲- پیشگیری غیرکیفری

در برابر محدودیت‌های رویکرد کیفری، پیشگیری غیرکیفری که بر اصل پیشگیری بهتر از درمان است استوار است به‌ویژه در دهه‌های اخیر اهمیت روزافزونی یافته است. این رویکرد به جای واکنش‌های قهرآمیز، بر مداخله در علل جرم‌زا و نیز دشوارسازی شرایط ارتکاب جرم تمرکز دارد. دو گونه مهم این شیوه عبارت‌اند از: پیشگیری اجتماعی: که با ارتقای آگاهی عمومی، آموزش، تقویت فرهنگ استفاده صحیح از فناوری و کاهش عوامل اجتماعی آسیب‌زا بر تغییر رفتارهای پرخطر تمرکز دارد. پیشگیری وضعی: که با به‌کارگیری تدابیر فنی و ساختاری مانند افزایش امنیت سامانه‌ها، کنترل دسترسی، بهبود معماری شبکه و کاهش فرصت‌های ارتکاب جرم وقوع رفتار مجرمانه را دشوار، پرهزینه یا پرخطر می‌سازد. اهمیت این نوع پیشگیری نه‌تنها در ادبیات علمی بلکه در اسناد بین‌المللی نیز مورد تأکید قرار گرفته است؛ از جمله قطعنامه[۱] مجمع عمومی سازمان ملل متحد که خواستار تقویت همکاری‌ها و اقدامات پیشگیرانه برای مقابله با جرائم سایبری است.

برآیند تحلیل‌ها نشان می‌دهد که پیشگیری کارآمد از جرائم سایبری مستلزم ترکیبی از رویکردهای کیفری و غیرکیفری است. با توجه به ماهیت فرامکانی، پیچیدگی فنی و سرعت تحولات فضای سایبری توفیق در کنترل بزهکاری سایبری در گرو مشارکت هم‌زمان نظام عدالت کیفری، ساختارهای فنی، نهادهای اجتماعی و کاربران است؛ امری که نیازمند سیاست‌گذاری جامع، ارتقای تخصص‌ها و بازنگری مداوم در شیوه‌های پیشگیری است.

۱- شماره ۴۵/۱۲۱

۴- محورهای اصلی مقابله و پیشگیری از جرائم سایبری

برای غلبه بر محدودیت‌های موجود و افزایش اثربخشی پیشگیری وضعی از جرائم سایبری، می‌توان به چند محور اصلی توجه نمود:

اول- توسعه تدریجی خودکفایی فنی سرمایه‌گذاری هدفمند در تولید ابزارها و سامانه‌های بومی امنیت سایبری باید به یک اولویت راهبردی تبدیل شود. دوم- ایجاد استاندارد و چهارچوب واحد اجرایی تدوین و الزام‌آور کردن یک استاندارد ملی برای تنظیمات فیلترینگ، پایش ترافیک و اعمال محدودیت‌های وضعی که همه ارائه‌دهندگان خدمات موظف به رعایت آن باشند. این چهارچوب باید شامل فهرست به‌روز و شفاف مصادیق محتوای مجرمانه، معیارهای فنی دقیق برای مسدودسازی و مکانیزم اعتراض و بازنگری سریع در موارد خطا[۲] باشد. سوم- تقویت خودتقنینی مسئولانه پلتفرم‌ها، هدایت قانونی پلتفرم‌های داخلی و ارائه‌دهندگان خدمات به سمت خودتقنینی هوشمند که هم امنیت را تأمین کند و هم به حریم خصوصی و آزادی مشروع دسترسی لطمه نزند. چهارم- آموزش و فرهنگ‌سازی عمومی امنیت سایبری پیشگیری وضعی بدون افزایش آگاهی کاربران ناقص است. برنامه‌های آموزش عمومی، کارگاه‌های امنیت برای کسب‌وکارها، دروس اجباری امنیت سایبری در مدارس و دانشگاه‌ها و کمپین‌های رسانه‌ای می‌توانند حجم زیادی از جرائم مبتنی‌بر خطای انسانی[۳] را کاهش دهند. پنجم- تعادل میان امنیت، حریم خصوصی و آزادی اطلاعات هرگونه گسترش دامنه فیلترینگ یا نظارت وضعی باید همراه با تضمین‌های قانونی قوی، لزوم مجوز قضایی برای اقدامات نظارتی هدفمند، شفافیت در معیارها و فهرست‌های مسدودسازی، وجود مکانیزم‌های مستقل رسیدگی به شکایات شهروندان و گزارش‌دهی دوره‌ای عملکرد به نهادهای نظارتی و عمومی باشد.

پیشگیری وضعی از جرائم سایبری در ایران، هم از منظر فنی[۴] و هم از منظر حقوقی و اجرایی[۵] با

۲- سایت‌های علمی و رسمی به اشتباه مسدود شده

۳- فیشینگ، افشای اطلاعات، کلیک روی لینک‌های مخرب و مانند آن

۴- وابستگی به فناوری خارجی و سرعت بالای تغییر تهدیدها

چالش‌های جدی مواجه است. بااین‌حال، تشکیل شورای عالی فضای مجازی، ابلاغ دستورالعمل‌های شورای عالی انقلاب فرهنگی و تلاش برای توسعه فناوری بومی، نشان‌دهنده حرکت تدریجی به سمت سامان‌دهی بهتر این حوزه است. موفقیت پایدار در پیشگیری وضعی نیازمند ترکیبی از سرمایه‌گذاری جدی در خودکفایی فنی، ایجاد چهارچوب قانونی و اجرایی شفاف و یکپارچه، تقویت آموزش عمومی و فرهنگ امنیت سایبری و حفظ تعادل دقیق میان امنیت، حریم خصوصی و آزادی‌های مشروع می‌باشد که بدون توجه هم‌زمان به این ابعاد، اقدامات صرفاً فنی یا صرفاً محدودکننده، نمی‌توانند به نتیجه مطلوب و پایدار دست یابند (فهیمی، ۱۳۸۰، ۱۳۶).

۴-۱- نقش نهادها و اشخاص در پیشگیری

۱-۴-۱- نقش و جایگاه قانون‌گذار

قانون‌گذار در حوزه جرائم سایبری با چالش‌های بنیادین و متفاوتی نسبت به جرائم سنتی مواجه است. مجرمان سایبری معمولاً برای حقوق فردی، مرزهای جغرافیایی، قوانین ملی، مقررات ایمنی و تعهدات بین‌المللی احترام چندانی قائل نیستند. از این رو قانون‌گذار با مشکلات ماهیت مجازی و فراملی جرم، امکان حضور یا هدایت جرم از خارج از مرزهای کشور، دشواری شدید درشناسایی هویت واقعی مرتکب، ضرورت هماهنگی قضایی و پلیسی بین‌المللی برای تعقیب و استرداد، پیچیدگی اثبات عناصر جرم در فضای دیجیتال و نیاز به تعاریف دقیق فنی و حقوقی از مفاهیم نوظهور روبرو می‌شود. به همین دلیل، یکی از مهم‌ترین وظایف قانون‌گذار تدوین تعاریف روشن، دقیق و قابل اجرا از اصطلاحات کلیدی است تا از تفسیرهای متفاوت قضایی و ایجاد خلأهای قانونی جلوگیری شود.

سه دسته‌بندی رایج از جرائم رایانه‌ای در ادبیات حقوقی: جرائم علیه خود رایانه یا سامانه مانند نفوذ غیرمجاز، رمزشکنی، تخریب داده‌ها، سابوتاژ سامانه و انتشار بدافزار. جرائم با واسطه بودن رایانه مانند کلاهبرداری آنلاین، قمار اینترنتی، فیشینگ، اخاذی دیجیتال و پولشویی سایبری. جرائم سنتی

۵- عدم شفافیت چهارچوب‌ها، ناهماهنگی ارائه‌دهندگان خدمات، تعارض با حریم خصوصی و آزادی اطلاعات

که رایانه فقط صحنه یا ابزار ذخیره‌سازی است مانند نمایش آگهی غیرقانونی در سایت برای جذب مشتری به تجارت غیرمجاز، ذخیره اسناد مجرمانه در سرور و استفاده از رایانه برای برنامه‌ریزی جرم سنتی (فهیمی، ۱۳۸۰، ۱۰۳).

رمزنگاری و چالش‌های آن یکی از پیچیده‌ترین موضوعات برخورد قانون با فناوری رمزنگاری است. رمزنگاری هم برای حفاظت مشروع اطلاعات خصوصی و تجاری ضروری است و هم توسط مجرمان برای مخفی‌سازی فعالیت‌های غیرقانونی استفاده می‌شود. قانون‌گذار باید تعادلی ایجاد کند که حق استفاده مشروع از رمزنگاری قوی حفظ شود و امکان دسترسی قانونی دستگاه‌های قضایی[۶] در موارد جرم سنگین فراهم باشد (شیرزاد، ۱۳۸۸، ۱۱۴). قانون‌گذار باید تعاریف دقیق و به‌روز از مفاهیم فنی و حقوقی ارائه دهد، خلأهای قانونی راشناسایی و رفع کند، تعادل میان امنیت ملی، حریم خصوصی، آزادی بیان و توسعه اقتصاد دیجیتال برقرار سازد، هماهنگی بین‌المللی را در دستور کار قرار دهد، چهارچوب‌های اجرایی شفاف برای پیشگیری وضعی، نظارت و خودتقنینی پلتفرم‌ها تدوین کند و به‌روزرسانی مستمر قانون را تضمین نماید که بدون قانون‌گذاری دقیق، به‌روز و جامع نه پیشگیری وضعی مؤثر خواهد بود، نه تعقیب قضایی کارآمد و نه اعتماد عمومی به فضای سایبر کشور حفظ خواهد شد.

۲-۴-۱- مراقبت از سامانه‌های اطلاعاتی حساس کشور

در هر جامعه‌ای، برخی زیرساخت‌ها و خدمات حیاتی وجود دارند که تداوم عملکرد صحیح آن‌ها برای حفظ امنیت، نظم و آرامش عمومی ضروری است. هرگونه خدشه، اختلال یا نفوذ به اطلاعات و سامانه‌های این بخش‌ها می‌تواند به‌سرعت آرامش جامعه را به خطر اندازد و حتی اثرات دومینویی گسترده‌ای ایجاد کند. از مهم‌ترین سامانه‌های اطلاعاتی حساس کشور می‌توان به مرکز کنترل ترافیک و راه‌های کشور، مرکز کنترل شبکه برق سراسری و نیروگاه‌ها، شبکه ملی مخابرات و زیرساخت‌های

۶- با رعایت تشریفات و مجوز قضایی

ارتباطی اصلی، سامانه‌های بهداشت، درمان و اورژانس، سامانه‌های دفاعی و نظامی، شبکه بانکی و پرداخت الکترونیکی، سامانه‌های گمرکی، مالیاتی و تجاری الکترونیک و زیرساخت‌های انرژی و حمل‌ونقل هوشمند اشاره کرد.

در کشورهای پیشرفته، معمولاً نهادی تخصصی تحت عنوان مرکز مراقبت از سامانه‌های اطلاعاتی حساس یا مشابه آن مسئولیت دارد. در ایران نیز این موضوع در سال‌های اخیر در قالب حفاظت از زیرساخت‌های اطلاعات ملی و شبکه ملی اطلاعات مورد توجه قرار گرفته و مسئولیت‌های مرتبط عمدتاً به شورای عالی فضای مجازی، وزارت ارتباطات، پلیس فتا و سازمان پدافند غیرعامل واگذار شده است (فهیمی، ۱۳۸۰، ۱۰۸).

۳-۴-۱- نیروهای واکنش سریع سایبری

امروزه حملات سایبری به‌عنوان عرصه پنجم جنگ شناخته می‌شوند. بسیاری از کشورها واحدهای تخصصی تحت عنوان مرکز واکنش سریع سایبری ایجاد کرده‌اند که وظایف اصلی آن‌ها عبارت است از رصد وشناسایی تهدیدهای نوظهور سایبری در لحظه، هشدار سریع به سازمان‌های دولتی و زیرساخت‌های حیاتی، پاسخ فوری به حوادث سایبری، ابداع و آزمایش روش‌های نوین دفاعی و تهاجمی سایبری، هماهنگی ملی و بین‌المللی در زمان بحران سایبری بزرگ. این مراکز معمولاً از بودجه وزارت دفاع، نیروهای مسلح و پلیس تأمین مالی می‌شوند و از متخصصان بسیار سطح بالا تشکیل شده‌اند. در ایران، پلیس فتا[۷] به‌عنوان نهاد اصلی عهده‌دار نقش واکنش سریع سایبری در سطح ملی است. این پلیس علاوه بر وظایف انتظامی و قضایی، مسئولیت رصد تهدیدها، پاسخ به حوادث، هشدار به نهادها و هماهنگی در زمان حملات سایبری گسترده را نیز بر عهده دارد (شیرزاد، ۱۳۸۸، ۱۱۷).

۴-۴-۱- نقش تأمین کنندگان خدمات اطلاعاتی

بخش قابل توجهی از جرائم سایبری از طریق شبکه جهانی اینترنت و زیرساخت‌های ارتباطی کشور

۷- پلیس فضای تولید و تبادل اطلاعات

انجام می‌شود. به همین دلیل، ارائه‌دهندگان خدمات اینترنت[۸] نقش بسیار کلیدی در پیشگیری و مقابله با جرائم سایبری دارند. در بررسی هر حادثه سایبری، معمولاً دو دسته اطلاعات از ارائه‌دهندگان خدمات اینترنت مورد نیاز استک ابتدا اطلاعات حساب کاربری[۹] و نیز اطلاعات ترافیک و جلسات ارتباط. [۱۰] محققان بین‌المللی در پرونده‌های جرائم سایبری، معمولاً فهرستی متشکل از حدود چهارده مورد اطلاعات ترافیک جلسه و بیست و یک مورد اطلاعات حساب مشترکین را به‌عنوان حداقل اطلاعات ضروری مورد نیاز دادستانی و پلیس فهرست کرده‌اند (فهیمی، ۱۳۸۰، ۱۰۶). ارائه‌دهندگان خدمات اینترنت در ایران موظف‌اند این اطلاعات را طبق ماده ۳۲ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ نگهداری کرده و در صورت درخواست مقام قضایی صالح، سریعاً ارائه دهند.

۵-۴-۱- نقش دولت در مقابله و پیشگیری از اشاعه جرائم سایبری

دولت به‌عنوان تنظیم‌گر اصلی، نقش محوری در ایجاد فرهنگ امنیت سایبری و همکاری بین بخش دولتی و خصوصی دارد. وظایف اصلی دولت در این زمینه عبارتند از: تبیین جایگاه امنیت سایبری در سیاست‌های کلان و استراتژی همکاری دولت و بخش خصوصی. مشارکت بخش خصوصی در تدوین قوانین و آیین‌نامه‌ها تا قوانین واقع‌بینانه‌تر و دارای ضمانت اجرایی بالاتر باشند. انتقال دانش تهدیدهای نوظهور به تولیدکنندگان سخت‌افزار، نرم‌افزار و تجهیزات مخابراتی کشور و بالعکس و آگاه‌سازی نهادهای امنیتی از روندهای جدید فناوری. ارزیابی مستمر آمادگی بخش خصوصی در برابر حملات سایبری و تدوین استانداردهای ملی امنیت سایبری. ترویج فرهنگ اخلاق سایبری و امنیت اطلاعاتی در جامعه. اجبار یا تشویق به اجرای تدابیر پیشگیرانه وضعی در سازمان‌های حساس. اشاعه بهترین شیوه‌های مدیریتی امنیتی در حوزه‌های پرخطر مانند بانکداری الکترونیک، فروشگاه‌های

۸- ISP

۹- مشخصات مشترک، شماره قرارداد، اطلاعات هویتی ثبت‌شده، شماره تلفن، آدرس و...

۱۰- زمان دقیق اتصال، آدرس‌ای پی اختصاص یافته، حجم ترافیک، سایت‌ها و سرویس‌های مورد استفاده، مقصد و مبدأ ارتباط، مدت زمان جلسه و...

آنلاین، بیمه الکترونیک و خدمات پرداخت (شیرزاد، ۱۳۸۸، ۱۱۸).

جمع‌بندی نقش دولت و نهادها پیشگیری و مقابله مؤثر با جرائم سایبری در ایران نیازمند هماهنگی گسترده میان نهادهای زیر است: شورای عالی فضای مجازی[۱۱]، پلیس فتا[۱۲]، وزارت ارتباطات و فناوری اطلاعات[۱۳]، قوه قضاییه[۱۴]، سازمان پدافند غیرعامل[۱۵]، وزارتخانه‌های تخصصی[۱۶] و بخش خصوصی.[۱۷]

۶-۴-۱- نقش مردم در پیشگیری از وقوع جرائم سایبری

بسیاری از افراد به‌دلیل عدم آشنایی کافی با اصول ایمنی در فضای مجازی، ناخواسته دسترسی به اطلاعات شخصی خود را برای متخلفان سایبری فراهم می‌کنند. از جمله این رفتارها می‌توان به افشای داده‌های خصوصی در شبکه‌های اجتماعی، برقراری گفت‌وگو با افراد ناشناس بدون تأیید هویت و وارد کردن رمز کارت‌های بانکی در سایت‌های غیرمعتبر هنگام انجام خریدهای اینترنتی اشاره کرد. چنین اقداماتی زمینه‌ساز سوءاستفاده مالی و دسترسی غیرمجاز به حساب‌های بانکی می‌شود.

برای پیشگیری از این خطرات، لازم است پس از انجام هر تراکنش الکترونیکی مانند پرداخت قبوض یا شهریه رمزهای ذخیره‌شده در مرورگر به‌صورت دستی حذف گردند. همچنین، نصب و به‌روزرسانی منظم نرم‌افزارهای ضدویروس و ضدجاسوس‌افزار از راهکارهای مؤثر برای مقابله با بدافزارها است؛ چرا که بسیاری از این برنامه‌های مخرب پس از نفوذ به سیستم، ابتدا موانع امنیتی را غیرفعال کرده و سپس اقدام به سرقت و انتقال اطلاعات کاربر به مهاجم می‌کنند.

۱۱- سیاست‌گذاری کلان

۱۲- واکنش سریع، تعقیب و پیشگیری انتظامی

۱۳- زیرساخت و الزامات فنی ارائه‌دهندگان خدمات اینترنت

۱۴- تعریف جرم، صدور مجوز نظارت و رسیدگی قضایی

۱۵- حفاظت از زیرساخت‌های حساس

۱۶- صنعت، اقتصاد، بهداشت، آموزش و...

۱۷- ارائه‌دهندگان خدمات اینترنت، پلتفرم‌ها و شرکت‌های فناوری

۷-۴-۱- طراحی و اجرای نقشه طرح ملی آموزش عمومی امنیت سایبری

در عصر دیجیتال، رعایت اصول اخلاقی و مسئولیت‌پذیری فردی در استفاده از فناوری اطلاعات از اهمیت بالایی برخوردار است؛ به‌گونه‌ای که حتی یک اقدام نادرست در سطح فردی می‌تواند در مدت زمان بسیار کوتاهی در سراسر جهان گسترش یابد. به‌عنوان نمونه، ویروس عشق که در سال ۲۰۰۰ میلادی از فیلیپین منتشر شد، خسارتی بالغ بر ده میلیارد دلار به بخش‌های گوناگون اقتصادی وارد کرد و داده‌های بسیاری از سازمان‌های بین‌المللی را از بین برد. مطالعه الگوهای موفق در کشورهای پیشرفته نشان می‌دهد که آگاه‌سازی جامعه در حوزه امنیت و اخلاق دیجیتال تنها در قالب برنامه‌های ملی یکپارچه و با همکاری چندبخشی قابل تحقق است. این برنامه‌ها با همراهی نهادهای سیاست‌گذار، اجرایی، قضایی، رسانه‌های عمومی و بخش خصوصی طراحی و پیاده‌سازی می‌شوند. توجه به این نکته ضروری است که موفقیت طرح‌های ملی فناوری اطلاعات و مقابله با جرائم سایبری مستلزم مشارکت فعال بخش خصوصی است؛ رویکردی که در تمام کشورهای پیشرو دنیا مورد تأکید قرار گرفته است.

۴-۲- نقش دستگاه قضایی در پیشگیری

۱-۴-۲- نقش دادستان و مقامات قضایی کشور برای پیشگیری از وقوع جرائم سایبری

با توجه به واقعیت‌های موجود، باید پذیرفت که دسترسی به بسیاری از ابزارهای پیشگیرانه در حوزه امنیت سایبری محدود است؛ زیرا این فناوری عمدتاً مبتنی‌بر واردات بوده و کشور در جریان یک‌طرفه‌ای از تولید و توسعه آن قرار گرفته است. این شرایط در بسیاری از ابعاد، امکان اعمال اراده ملی در کنترل کامل این فضا را محدود ساخته است. بااین‌حال، راهکارهایی مانند فیلترینگ به‌عنوان یک اقدام دفاعی می‌تواند تا حدی نقش بازدارندگی ایفاء کند. بر این اساس، مصوبه شورای عالی انقلاب فرهنگی[۱۸]، کمیته‌ای را با عنوان «کمیته تعیین مصادیق پایگاه‌های اطلاع‌رسانی رایانه‌ای غیرمجاز» تشکیل داد تا ضمن بررسی فعالیت‌های نامشروع در فضای سایبری، زمینه اعمال فیلترینگ

۱۸- شماره ۵۹ مورخ دهم مهر ۱۳۸۱

را با در نظر گرفتن جنبه‌های فرهنگی، امنیتی و حقوقی فراهم آورد.

۲-۴-۲- جایگاه قضایی در تصمیم‌گیری‌های مربوط به فیلترینگ

اگرچه کمیته مذکور از آن‌جایی که ذاتاً نهادی قضایی نیست، نمی‌تواند مستقیماً منجر به اعطای یا سلب حق از افراد شود، اما لازمه قانونی فیلتر یا رفع فیلتر هر سایت، صدور مجوز توسط مقام قضایی ذیصلاح است. در مقررات مربوط به پالایش محتوا، چهارده عنوان مجرمانه از جمله توهین به مقدسات، اشاعه فحشا، نشر اکاذیب و توهین به علما و مسئولان تعریف شده است. همچنین، ماده‌های ۶۳۹ و ۶۴۰ قانون مجازات اسلامی (کتاب پنجم تعزیرات) مصوب ۱۳۷۵ به جرائم مرتبط با فضای مجازی پرداخته است. هرچند کنترل‌های قضایی، امنیتی و پلیسی هر کدام مبانی قانونی جداگانه‌ای دارند، اما از دیدگاه قضایی، دادسرا به‌عنوان نهاد کشف و تعقیب جرم، مسئولیت اولیه را بر عهده دارد؛ یعنی باید با پیگیری گزارش‌های ثالث یا درخواست نظر کارشناسان، روند قضایی را آغاز کند. در مواردی که جرم دارای جنبه عمومی باشد مانند محتوایی که در فضای سایبری در معرض دید میلیون‌ها نفر قرار می‌گیرد دادستان به‌عنوان مدعی‌العموم، موظف است به نیابت از جامعه از حقوق عمومی صیانت نماید.

۳-۴-۲- نقش محوری دادستان در پیشگیری از جرائم سایبری

با توجه به ماهیت ترکیبی جرائم سایبری که دربرگیرنده ابعاد فنی، حقوقی و قضایی است رسیدگی به آن‌ها مستلزم همکاری متخصصان حوزه‌های مختلف است. در این میان، جایگاه دادستان به‌عنوان نهاد مسئول صیانت از حقوق عمومی و تعقیب جرائم، از اهمیت کلیدی برخوردار است. این نقش با تکیه بر بند پنجم اصل یکصد و پنجاه و ششم قانون اساسی جمهوری اسلامی ایران که پیشگیری از وقوع جرم را یکی از وظایف قوه قضاییه می‌داند، تقویت می‌شود. همچنین، رویه قضایی و اختیارات واگذارشده از سوی رئیس قوه قضاییه، این مسئولیت را به‌طور خاص به دادستان کل کشور به‌عنوان مدعی‌العموم با صلاحیت سراسری محول کرده است. این جایگاه، دادستان کل کشور را به مقام

ذیصلاح برای سامان‌دهی فضای سایبری و پیشگیری از جرائم در این حوزه تبدیل می‌کند. علاوه بر این، نظارت دادستان کل کشور بر حسن اجرای امور قضایی در سطح کشور که در اصل یکصد و شصت و یکم قانون اساسی جمهوری اسلامی ایران پیش‌بینی شده، این جایگاه را تثبیت می‌کند.

۴-۳- ضرورت آمادگی جامع در برابر گسترش جرائم سایبری

با توجه به گسترش فزاینده اینترنت و نفوذ آن در تمام ابعاد زندگی بشر، جرائم سایبری در کشورهای پیشرفته به یکی از دغدغه‌های اصلی تبدیل شده‌اند. ازاین‌رو، در کشورهای در حال توسعه مانند ایران که با سرعت در مسیر دیجیتالی‌شدن گام برمی‌دارند، ضروری است تا پیش از فراگیر شدن این جرائم با بهره‌گیری از تجربیات بین‌المللی، زیرساخت‌های لازم از جنبه‌های فنی، تکنولوژیک و حقوقی و قضایی فراهم آید تا بتوان در برابر این تهدیدات به‌صورت مؤثر ایستاد (شیرزاد، ۱۳۸۸، ۱۲۰).

۱-۴-۳- نقش و جایگاه پلیس در پیشگیری از جرائم سایبری

بررسی ساختار واحدهای تخصصی جرائم سایبری در پلیس کشورهای مختلف جهان نشان می‌دهد که این واحدها معمولاً در بخش‌های اصلی حمایت از کودکان و نوجوانان در فضای مجازی، دریافت و پیگیری شکایت‌های ثبت‌شده از طریق اینترنت، برخورد با تخلفات تجاری و اقتصادی در بستر دیجیتال، مقابله با جاسوسی اطلاعاتی در حوزه‌های صنعتی و تجاری[۱۹]، انجام عملیات تخصصی از مرحله‌شناسایی تا محاکمه و ایجاد آزمایشگاه‌های قضایی تخصصی برای بررسی شواهد دیجیتال فعالیت می‌کنند.

۲-۴-۳- فعالیت‌های آموزشی و آگاه‌سازی عمومی

در حوزه ترویج فرهنگ ایمنی سایبری، پلیس با همکاری نهادهای آموزشی، رسانه‌ای و تجاری، برنامه‌های گسترده‌ای را اجرا می‌کند. از جمله آن‌ها می‌توان به موارد زیر اشاره نمود: برگزاری کارگاه‌ها و سخنرانی‌های آموزشی برای دانش‌آموزان، معلمان و والدین، ارسال هشدارهای ویژه به

۱۹- شامل تخلفات مخابراتی، سرقت سخت‌افزار و نرم‌افزار

کاربران دارای پهنای باند بالا که در معرض خطرات بیشتری قرار دارند، طراحی و توزیع بروشور، پوستر و برچسب‌های آموزشی در مدارس و مراکز عمومی، همکاری با ارائه‌دهندگان خدمات اینترنتی برای ارسال اخطار به کاربران ناقض قوانین شبکه، مشارکت با وزارت آموزش و پرورش در تدوین محتوای امنیتی برای کتاب‌های درسی و طرح درس فناوری اطلاعات، برگزاری جلسات آموزشی برای کارکنان و مدیران شرکت‌ها و بنگاه‌های اقتصادی، گنجاندن ماده‌های قانونی مرتبط با جرائم رایانه‌ای در منابع آموزشی رسمی و حضور فعال در همایش‌ها و نمایشگاه‌های تخصصی امنیت اطلاعات با هدف ارتقای سطح آگاهی عمومی.

۳-۴-۳- فرایند کشف و اثبات جرم در فضای سایبری

کشف و اثبات جرائم سایبری مستلزم طی کردن مسیری پیچیده و تخصصی توسط کارشناسان پلیس است. این فرایند با بهره‌گیری از فناوری‌های روز و تجهیزات پیشرفته سخت‌افزاری و نرم‌افزاری، باید قادر باشد چهار وظیفه اصلی را ایفاء کند:شناسایی مجرم، تحلیل روش‌های به‌کاررفته توسط وی، ارائه راهکارهای پیشگیرانه و مقابله‌ای و مستندسازی دقیق شواهد برای ارائه در دادگاه. یکی از چالش‌های اساسی در این حوزه، امکان دستکاری آسان اطلاعات مربوط به زمان و مکان وقوع جرم توسط متخلفان است. برای غلبه بر این چالش، مأموران اجرای قانون از روش‌های تخصصی مانند منجمد کردن اطلاعات استفاده می‌کنند؛ روشی که با بهره‌گیری از ابزارهای خاص امکان ثبت و حفظ شواهد دیجیتال را از راه دور فراهم می‌آورد (شیرزاد، ۱۳۸۸، ۱۸۸).

۴-۴-۳- نقش پلیس فضای تولید و تبادل اطلاعات

هم‌زمان با توسعه و گسترش روزافزون استفاده از رایانه و سیستم‌های رایانه‌ای، جرائم رایانه‌ای هم به وجود آمدند. گسترش جرائم رایانه‌ای در سطح دنیا موجب شد تا قوانین تخصصی جدیدی برای مقابله با آن به کار گرفته شود و هم‌زمان نیاز به وجود پلیس تخصصی نیز احساس می‌شود. با توجه به دانش فنی مورد نیاز برای مقابله با این جرائم بسیاری از کشورهای توسعه‌یافته اقدام به ایجاد رده‌های

تخصصی پلیس مبارزه با جرائم سایبری نمودند. در ایران نیز از سال ۱۳۸۱ با تشکیل اداره کل جرائم رایانه‌ای در پلیس آگاهی فراجا این موضوع در دستور کار قرار گرفت. هم‌زمان به منظور ایجاد رویه قضایی و قانونی متناسب، کمیته‌ای در قوه قضاییه تحت عنوان کمیته مبارزه با جرائم رایانه‌ای تشکیل شد و به دنبال آن فرایند تدوین قانون جرائم رایانه‌ای آغاز گردید. یک رکن تخصصی نیروی انتظامی جمهوری اسلامی ایران که نام مختصر «فتا» است که مقابله با جرائم اینترنتی و ایجاد نظم و امنیت در فضای مجازی، جعل و کلاهبرداری در فضای سایبر و حفاظت از اسرار ملی بر روی شبکه اینترنت وظیفه و هدف آن است (گل محمدی، ۱۳۹۳، ۵۰).

مأموریت اصلی این نهاد تخصصی، فراهم‌آوردن بستری امن برای فعالیت‌های علمی، اقتصادی و اجتماعی در جامعه اطلاعاتی است تا شهروندان بتوانند بدون ترس از مخاطرات دیجیتال، از امکانات فضای مجازی بهره‌مند شوند. در این راستا، پلیس فتا بر حفظ هویت ملی و دینی جامعه تأکید دارد و با رصد مستمر فضای تولید و تبادل اطلاعات، از تبدیل این فضا به ابزاری برای هماهنگی و اجرای برنامه‌های غیرقانونی جلوگیری می‌کند. همچنین، این واحد مسئولیت مقابله با انواع جرائم سایبری از جمله جرائم اخلاقی و جرائم اقتصادی تا اشکال مدرن تروریسم دیجیتال را بر عهده دارد و درعین‌حال از تعرض به ارزش‌ها و هنجارهای جامعه در بستر مجازی جلوگیری می‌نماید.

نتیجه

در پرتو بررسی‌های انجام شده در این پژوهش، آشکار گردید که جرائم سایبری، پدیده‌ای پیچیده و چندوجهی‌اند که ابعاد مختلف امنیت فردی، اجتماعی و ملی را به چالش کشیده‌اند. نظام کیفری ایران، اگرچه گام‌هایی را در جهت جرم‌انگاری برخی از این جرائم و تعیین مجازات برای مرتکبین برداشته است، اما با چالش‌های متعددی در زمینه پیشگیری مؤثر و مقابله قاطع با این تهدیدات روبرو است.

یافته‌های این پژوهش نشان دادند که راهکارهای پیشگیرانه، اعم از تدابیر فنی، حقوقی، آموزشی و فرهنگی نقشی حیاتی در کاهش وقوع جرائم سایبری ایفاء می‌کنند.

بااین‌حال، اثربخشی این راهکارها مستلزم رفع خلأهای قانونی موجود، به‌روزرسانی مستمر قوانین متناسب با تحولات فناوری، تقویت زیرساخت‌های فنی و قضایی برای کشف وشناسایی جرائم و مجرمان و همچنین ارتقاء سطح آگاهی عمومی و تخصصی در جامعه است. به‌طور خاص، ضعف در همکاری‌های بین‌المللی، دشواری در استرداد مجرمان و تبادل اطلاعات و همچنین عدم تناسب برخی مجازات‌ها با عمق آسیب‌های ناشی از جرائم سایبری، از موانع جدی در مسیر تحقق عدالت کیفری در این حوزه محسوب می‌شوند. در نهایت، مقابله مؤثر با جرائم سایبری، نیازمند یک عزم ملی و همکاری مستمر میان تمامی ذینفعان، از جمله دولت، بخش خصوصی، دانشگاهیان و آحاد جامعه است تا بتوان فضایی امن، پایدار و پویا را در پهنه گسترده فضای مجازی تضمین نمود.

پیشنهاد

بر این اساس، پیشنهاد می‌شود رویکردی جامع‌نگر و چندبعدی در پیشگیری و مقابله با جرائم سایبری اتخاذ گردد که شامل موارد زیر است: تکمیل و اصلاح قوانین: بازنگری در قوانین موجود، جرم‌انگاری رفتارهای جدید در فضای سایبری و تعیین مجازات‌های بازدارنده و متناسب با شدت جرائم. تقویت زیرساخت‌های فنی و قضایی: سرمایه‌گذاری در فناوری‌های نوین کشف جرم، آموزش نیروهای متخصص در حوزه جرائم سایبری و تسریع فرایندهای قضایی مرتبط. ارتقاء فرهنگ حقوقی و سواد سایبری: افزایش آگاهی عمومی از طریق رسانه‌ها، نظام آموزشی و برنامه‌های فرهنگی به منظور توانمندسازی شهروندان در برابر تهدیدات فضای مجازی. توسعه همکاری‌های بین‌المللی: تقویت تعاملات با سایر کشورها در زمینه تبادل اطلاعات، همکاری در تحقیقات مشترک و تدوین معاهدات دوجانبه و چندجانبه برای مقابله با جرائم سایبری فراملی. ایجاد نهاد هماهنگ‌کننده ملی: تشکیل یا تقویت نهادی متمرکز برای هماهنگی میان دستگاه‌های مختلف دولتی و خصوصی در حوزه امنیت سایبری و مقابله با جرائم سایبری.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و

ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

- ابراهیمی، شهرام، ۱۴۰۳، **جرم‌شناسی پیشگیری**، چاپ هشتم، تهران، انتشارات میزان.
- امیریان فارسانی، امین؛ عبدالصمدی، راضیه؛ حیدری فارسانی، فاطمه، ۱۳۹۹، علت‌شناسی ارتکاب جرائم سایبری و سازوکارهای پیشگیری از آن، **فصلنامه علوم خبری**، شماره ۳۵.
- جلالی فراهانی، امیرحسین و باقری اصل، رضا، ۱۳۸۷، پیشگیری اجتماعی از جرائم و انحرافات سایبری، **فصلنامه مجلس و پژوهش**، شماره ۵۵.
- شیرزاد، کامران، ۱۳۸۸، **جرائم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل**، چاپ اول، تهران، انتشارات بهینه فراگیر.
- فضلی، مهدی، ۱۳۸۹، **مسئولیت کیفری در فضای سایبر**، چاپ اول، تهران، انتشارات خرسندی.
- فهیمی، مهدی، ۱۳۸۰، جرائم رایانه‌ای و روش‌های مقابله و پیشگیری از آن، **فصلنامه دیدگاه‌های حقوقی**، شماره ۲۳.

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.27- Spring 2026

Burden of Proof and Admissibility and of Evidence in International Commercial Arbitration
Homayoun Mafi, Maedeh Asgharzadeh
Analysis the Practice of Determining the Jurisdiction of the International Criminal Court to Adjudicate Forced Marriage
Mohammad Hossein Ramezani Ghavamabadi, Pouria Ebrahimzadeh
Legal Rethinking of the Use of Artificial Intelligence for the Enforcement of Punishment
Amirreza Mahmoudi, Anusha Zafari Kore Tash
Federative Rights in Football: Approaches of the Legal Systems of Iran, France, England, Argentina, Brazil, Spain and Colombia
Behnam Noorzadeh
Conflict of the Regulation of the Third Article of the Mandatory Formal Registration of Immovable Properties with Laws and Legal Principles
Akbar Iman Poor, Sahand Nejadi Ijadkar
Criminal Personality and Its Relationship with Effective Punishment
Maryam Bahmai, Mostafa Karamipour
Challenges and Obstacles to Interpreting Contracts in Iranian Law
Farzin Yazdan Panah, Mohammadreza Nasiri
Measures to Prevent Financial Corruption in the Banking System
Alireza Deraei, Sayyed Ebrahim Mortazavi, Amirhasan Abolhasani
Divorce at the Request of the Woman in the Iranian Legal System
Mohammad Ahmadi, Helma Sadat Zorrieh Kermanshahi
Assessing the Criminal Nature of Online Lotteries in Iranian Law
Mohammadhossein Hajeb, Zahra Rabbani, Roya Asiaei
Mutual Sale Contract in the Iranian Legal System
Sadegh Mohebbi, Mohammadali Jahani
Features and Characteristics of Cybercrimes in the Iranian Criminal System
Seyedeh Elaheh Babonaki
Studying the Right to Employment of Women in International Law
Habibolah Abdolah Poor, Sama Khodayari
The Effectiveness of Security and Educational Measures in the Resocialization of Juvenile Delinquents; A Case Study of Shahid Fahmideh Judicial Complex
Leila Ahadi
Retaliation in the Quran and its Place in Islamic Penal Policy
Rojin Masoudi, Jamal Rezaei Hossein Abadi
a Legal Analysis of the Regulatory Structure of the Unorganized Monetary Market in Iran: from Conceptual Ambiguities to Legislative and Executive Challenges
Ali Babaei
The Impact of Independent International Institutions on the Effectiveness of Sanctions in International Trade Law
Elahe Ghorban Karimi
Based on the Best Interests of the Child; an Analysis of Custody with a Legal, Jurisprudential and Psychological Approach to Identifying Legislative Gaps
Mona Komeyli
Human Rights-Based Rehabilitation and Its Limitations in the Iranian Penal System
Amin Reza Bahar Falamarzi
an Analysis of Strict Civil Liability in Chemical Industry Accidents; a Case Study of Iranian Methanol Production Units
Mohammad Jokar, Sasan Vazin Pour
Pathology of Lethal Punishment in Iranian Criminal Law
Mohammadreza Rezaei
Implementing Regulations on Land Nationalization, Especially Endowment Lands, with Emphasis on Judicial Practice
Esmaeil Chogani
International Criminal Policy Against Genocide: A Comparative Analysis in International Criminal Tribunals
Ali Hadian Haghighi, Saber Sayyari Zohan
Criminological Analysis of Kolbari in the Border Areas of Iran and its Comparison with the Kalba
Morteza Hashem Pour
Legal Challenges and Harms of Unauthorized Accredited Institutions in the Iranian Monetary System
Amin Amini Nezhad
The Impact of Prefrontal Cortex Dysfunction on Criminal Responsibility in the Crime of Intentional Murder
Hamid Ghiasi, Mehdi Shaban Zadeh
Artificial Intelligence and the Right to a Fair Trial in Light of the Iranian Constitution
Pouria Zhoulideh
Impact of Government Expenditure and Debt on Stock Market Growth in Iran
Razeih Hojjati Nezhad
the Position of the Central Counterparty Institution and Its Impact on the Principle of Privity of Contracts in Cross Border Transactions in the Legal Systems of Iran, Europe and the United States of America
Arefeh Ghasem Zadeh Dehabadi
Strategies to Combat and Deal with Cybercrime
Ahmad Padidar