مرکز وکلای قوه قضاییه خراسان رضوی

فصلنامه علمی تخصصی حقوق وکیل دعاوی

وابسته به مرکز وکلای قوه قضاییه خراسان رضوی

دوره ۱، شماره ۳، پاییز ۱۴۰۴، صص: ۳۹-۲۱

چالش‌های امنیت سایبری در برابر تهدیدات نوظهور و استراتژی‌های حفاظتی در فضای مجازی

نویسندگان:

کیارش غلامی خجسته

URL: https://www.vakildaavirazavi.ir/

DOI: https://doi.org/10.22034/vd.2026.2080798.1004

فصلنامه علمی تخصصی حقوق وکیل دعاوی

Journal of Vakil Daavi

دوره یک، شماره سوم، پاییز ۱۴۰۴، صص: ۳۹-۲۱

Vol 1, No 3, 2026, P: 21-39

چالش‌های امنیت سایبری در برابر تهدیدات نوظهور و استراتژی‌های حفاظتی در فضای مجازی

کیارش غلامی خجسته

دانش آموخته مقطع کارشناسی ارشد، گرایش حقوق جزا و جرم شناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران
Email: kiarashkhojaste1375@gmail.com

چکیده

در دهه‌های اخیر، فضای مجازی به بستری بی‌بدیل برای تعاملات فردی، اقتصادی، سیاسی و فرهنگی بدل شده است؛ اما در کنار این تحولات مثبت، تهدیدات نوظهور در فضای سایبری، ازجمله حملات شناختی، نفوذ به زیرساخت‌های حیاتی، بهره‌برداری از داده‌های شخصی و جنگ‌های ترکیبی سایبری، چالش‌های عمیقی برای امنیت ملی، حاکمیت داده و حقوق شهروندی ایجاد کرده‌اند. در چنین شرایطی، ضرورت بازاندیشی در ابزارها و سازوکارهای حقوقی و سیاست‌گذاری بیش‌ازپیش احساس می‌شود. پژوهش حاضر با رویکرد توصیفی - تحلیلی و بر پایه داده‌ها و منابع علمی معتبر داخلی و بین‌المللی، در پی شناسایی ابعاد تهدیدات نوین و ارائه راهبردهای کارآمد حفاظتی با تکیه‌بر تحلیل حقوقی و سیاستی است. یافته‌های تحقیق نشان می‌دهند که چارچوب‌های حقوقی موجود، ازجمله قانون جرائم رایانه‌ای مصوب ۱۳۸۸، پاسخگوی کامل تهدیدات جدید نیستند و فاقد نهادهای مستقل نظارتی، نظام منسجم حمایت از داده‌ها و رویه‌های شفاف مسئولیت‌پذیری نهادی‌اند. از سوی دیگر، سیاست‌گذاری سایبری ایران با خلأ هم‌افزایی نهادی، نبود مشارکت ذی‌نفعان خصوصی و عدم تبعیت از اصول حکمرانی دیجیتال مواجه است؛ بنابراین، پژوهش بر لزوم طراحی سیاست‌های پیش‌دستانه، به‌کارگیری چارچوب‌های چندلایه حفاظتی، الحاق به کنوانسیون‌های بین‌المللی همچون کنوانسیون بوداپست و تدوین قانون جامع امنیت سایبری مبتنی بر اصول شفافیت، مسئولیت‌پذیری و عدالت سایبری تأکید دارد. همچنین، ارتقاء سواد دیجیتال عمومی و تربیت نیروی انسانی متخصص، ازجمله الزامات بنیادین در مسیر تحقق حکمرانی اثربخش سایبری تلقی می‌شوند.

واژگان کلیدی: امنیت سایبری، تهدیدات نوظهور، حکمرانی دیجیتال، داده‌های شخصی، سیاست‌گذاری سایبری، مسئولیت حقوقی، نهادهای نظارتی

مقدمه

در عصر حاضر، فضای سایبری به‌عنوان یکی از بسترهای حیاتی تعاملات انسانی، اقتصادی، نظامی، فرهنگی و اجتماعی، جایگاه بی‌بدیلی در ساختارهای کلان جوامع یافته است. این فضا، متشکل از شبکه‌های گسترده دیجیتال، سامانه‌های اطلاعاتی، زیرساخت‌های ارتباطی و محیط‌های مجازی است که انسان‌ها و نهادها از طریق آن به تبادل اطلاعات، تصمیم‌سازی، مدیریت منابع و ایجاد روابط تجاری و سیاسی می‌پردازند. بااین‌حال، هم‌زمان با رشد شتابان فناوری اطلاعات و ارتباطات، تهدیداتی نوین نیز ظهور یافته‌اند که ماهیت آن‌ها با تهدیدات سنتی و شناخته‌شده امنیتی تفاوت بنیادین دارد. این تهدیدات که از آن‌ها تحت عنوان «تهدیدات نوظهور در فضای سایبری» یاد می‌شود، اغلب غیرخطی، پویا، نامتقارن و چندلایه‌اند؛ به این معنا که مرزهای جغرافیایی را درنوردیده، تابع قوانین کلاسیک نبوده و به‌صورت هوشمندانه در حال تکامل‌اند.

از عوامل کلیدی در بروز تهدیدات نوظهور، وابستگی شدید و روزافزون سازمان‌ها، دولت‌ها و حتی زندگی روزمره افراد به زیرساخت‌های سایبری است. این وابستگی، به‌ویژه در حوزه‌هایی نظیر بانکداری، خدمات درمانی، زیرساخت‌های انرژی، حمل‌ونقل هوشمند، دولت الکترونیک، امنیت ملی و حتی آموزش، فرصت‌هایی کم‌نظیر برای توسعه و بهره‌وری ایجاد کرده، اما درعین‌حال زمینه‌های آسیب‌پذیری عمیقی نیز فراهم ساخته است. به‌عنوان نمونه، نفوذ در سامانه‌های اطلاعاتی نیروگاه‌ها یا سامانه‌های کنترل ترافیک شهری، می‌تواند پیامدهایی فاجعه‌بار بر امنیت ملی و سلامت عمومی جامعه داشته باشد (رئوفی نیا، ۱۳۹۷).

تهدیدات نوظهور در فضای سایبری، معمولاً از فنونی بهره می‌گیرند که با پیشرفت‌های نوین فناورانه هم‌راستا هستند. به‌ویژه، کاربرد گسترده فناوری‌هایی چون هوش مصنوعی[1]، یادگیری ماشین[2]، رایانش ابری[3]، اینترنت اشیاء[4] و بلاک‌چین[5]، نه‌تنها موجب ارتقای کارایی خدمات دیجیتال شده‌اند، بلکه ابزارهای جدیدی برای حملات پیچیده سایبری فراهم کرده‌اند. از حملات مبتنی بر داده‌های جعلی و فیشینگ پیشرفته گرفته تا نفوذ به شبکه‌های عصبی مصنوعی و بهره‌برداری از حفره‌های امنیتی در سامانه‌های خودران، همگی گویای تحولی اساسی در ماهیت تهدیدات امنیتی در دوران معاصر هستند. این امر، لزوم بازنگری و طراحی مجدد در چارچوب‌های دفاع سایبری، استراتژی‌های پیشگیرانه و الگوهای پاسخ به تهدیدات را ضروری می‌سازد. مهم‌ترین چالش امنیت سایبری در برابر این تهدیدات نوظهور، درواقع دوگانه‌ای از «پیش‌بینی‌ناپذیری» و «سرعت انطباق مهاجمان» است. برخلاف گذشته که حملات عمدتاً مبتنی بر امضای بدافزارها و الگوهای شناخته‌شده بود، امروزه تهدیدات نوظهور از طریق

1. AI
2. ML
3. Cloud Computing
4. IoT
5. Blockchain

یادگیری و تحلیل رفتار سامانه‌ها، حملاتی هدفمند و تطبیق‌پذیر انجام می‌دهند که به‌راحتی قابل‌شناسایی و مهار نیستند. از سوی دیگر، نبود هماهنگی در سطح ملی و بین‌المللی در سیاست‌گذاری، فقدان استانداردهای یکپارچه و عقب‌ماندگی قانون‌گذاری سایبری از تحولات فنی، زمینه‌های مساعدی برای گسترش این تهدیدات ایجاد کرده است. در این میان، کشورهایی چون جمهوری اسلامی ایران که به‌طور روزافزون در معرض تهدیدات سایبری با منشأ خارجی و داخلی هستند، نیازمند شناختی علمی، ساختاری و فناورانه از ماهیت تهدیدات نوظهور و تدوین سیاست‌های دفاعی نوین می‌باشند (خداقلی، ۱۳۹۵). پژوهش حاضر درصدد است تا با تحلیل جامع این تهدیدات و بررسی دقیق‌ترین و کارآمدترین استراتژی‌های حفاظتی، ازجمله الگوریتم‌های هوشمند، مدل‌های پیش‌بینی رفتاری و سامانه‌های هشدار سریع، نقشه راهی علمی برای ارتقاء تاب‌آوری سایبری در سطح فردی، سازمانی و ملی ارائه نماید. لذا از این منظر، مسئله محوری این پژوهش آن است که: «ماهیت و ویژگی‌های تهدیدات نوظهور در فضای سایبری چیست و چه استراتژی‌های حفاظتی می‌توانند در سطح ملی و سازمانی برای مقابله با آن‌ها کارآمد واقع شوند؟»

تعاریف و مفاهیم پژوهش

در مسیر بررسی تهدیدات نوظهور و راهکارهای مقابله با آن‌ها در فضای سایبری، نخستین گام، تبیین دقیق مفاهیم بنیادین مورداستفاده در این پژوهش است. این مفاهیم، چارچوب تحلیلی تحقیق را شکل می‌دهند و بدون درک روشن آن‌ها، تحلیل ساختاری و راهبردی از چالش‌ها و فرصت‌های امنیتی ممکن نخواهد بود.

تهدیدات سایبری

تهدیدات سایبری به‌عنوان یکی از مهم‌ترین چالش‌های عصر دیجیتال، به هرگونه اقدام مخرب در فضای مجازی گفته می‌شود که هدف آن دسترسی غیرمجاز، تخریب، سرقت، تغییر یا دستکاری اطلاعات و یا ایجاد اختلال در کارکرد سامانه‌ها و زیرساخت‌های اطلاعاتی است. این تهدیدات نه‌تنها جنبه فنی دارند بلکه از ابعاد اقتصادی، اجتماعی، سیاسی و حتی فرهنگی نیز قابل تحلیل‌اند. تهدیدات سایبری می‌توانند از سوی بازیگران دولتی، گروه‌های تروریستی، مجرمان سایبری یا حتی کاربران ناآگاه رخ دهند. در جهان امروز، حملاتی نظیر نفوذ به سامانه‌های مالی، سرقت داده‌های دولتی، فیشینگ، بدافزارها، حملات اختلال در سرویس[1] و جاسوسی صنعتی تنها بخشی از مصادیق تهدیدات سایبری محسوب می‌شوند. این تهدیدات به دلیل ماهیت بی‌مرز فضای سایبری، ابعاد جهانی یافته‌اند و یک کشور نمی‌تواند بدون همکاری بین‌المللی به مقابله مؤثر با آن بپردازد. به‌بیان‌دیگر،

1. DDoS

تهدیدات سایبری نه‌فقط تهدیدی علیه یک سازمان یا کشور خاص، بلکه تهدیدی علیه ساختار نوین حکمرانی دیجیتال در سطح بین‌المللی به شمار می‌روند (مرادیان و همکاران، ۱۴۰۲).

تهدیدات نوظهور سایبری

تهدیدات نوظهور سایبری، گونه‌ای پیشرفته‌تر از تهدیدات دیجیتال سنتی‌اند که از دل فناوری‌های نوظهوری چون هوش مصنوعی[1]، اینترنت اشیاء[2]، بلاک‌چین، سامانه‌های خودران، متاورس و رایانش کوانتومی سر برآورده‌اند. این تهدیدات، به دلیل نوظهور بودنشان، عمدتاً از قابلیت شناسایی فوری و مکانیسم‌های مقابله کلاسیک فراتر رفته‌اند. به‌عنوان نمونه، استفاده از هوش مصنوعی در توسعه بدافزارهای خودآموز یا سامانه‌های جعل عمیق[3] که قادر به تولید محتوای صوتی و تصویری شبه واقعی‌اند، نه‌فقط تهدیدی علیه امنیت سایبری، بلکه تهدیدی علیه حقیقت و واقعیت اجتماعی است. همچنین استفاده از حس‌گرها و گجت‌های متصل به اینترنت در بستر اینترنت اشیاء، آسیب‌پذیری کاربران و زیرساخت‌ها را در برابر نفوذگران افزایش داده است (اسحاق و فرید، ۲۰۲۳). آنچه این تهدیدات را متمایز می‌سازد، سطح پیچیدگی، قدرت یادگیری و سرعت بالای انطباق آن‌ها با تغییرات محیطی است. در بسیاری از موارد، این تهدیدات از دید نهادهای حاکمیتی و تنظیم‌گر پنهان می‌مانند و واکنش به آن‌ها نیازمند سیاست‌گذاری‌های مبتنی بر آینده‌پژوهی و طراحی پیش‌دستانه است (غلام‌پور و هدایتی، ۱۴۰۳؛ داو و همکاران، ۲۰۲۳).

امنیت ملی در فضای سایبری

امنیت ملی در بستر فضای سایبری مفهومی پیچیده و چندلایه است که حفاظت از حاکمیت دیجیتال، زیرساخت‌های حیاتی اطلاعاتی، حریم خصوصی شهروندان و ظرفیت دفاعی کشور در فضای مجازی را دربر می‌گیرد. برخلاف گذشته که امنیت ملی بیشتر به مرزهای فیزیکی محدود می‌شد، امروز مفهوم امنیت ملی از طریق فناوری، وارد ساحت‌های اطلاعاتی، ارتباطی و سایبری شده است. تهدید به زیرساخت‌های انرژی، بانکداری، حمل‌ونقل، آب و برق و حتی رسانه‌های ملی، می‌تواند کل امنیت ملی کشور را در معرض خطر قرار دهد. از سویی دیگر، تهدیدات سایبری با تأثیرگذاری بر افکار عمومی، القای شایعات سازمان‌یافته، دستکاری اطلاعات و نفوذ در فرآیندهای انتخاباتی، کارکردهای اساسی یک نظام سیاسی را به چالش می‌کشد. بدین ترتیب، امنیت ملی سایبری، تنها به معنای حفظ اطلاعات و داده‌ها نیست بلکه به معنای حفظ ثبات حاکمیتی، مشروعیت سیاسی و امنیت

1. AI
2. IoT
3. Deepfake

روانی جامعه نیز است (شفیعی و جلالی، ۱۴۰۳).

تحولات فناورانه و تغییر منطق تهدید

تحولات فناوری اطلاعات طی دو دهه اخیر، نه‌فقط ساختار فنی زیرساخت‌های ارتباطی را تغییر داده‌اند، بلکه منطق تهدید و حفاظت را نیز دگرگون ساخته‌اند. امروزه فناوری‌هایی چون هوش مصنوعی، رایانش ابری، تحلیل کلان داده‌ها[1]، بلاک‌چین و اینترنت اشیاء، ماهیت محیط عملیاتی سازمان‌ها و دولت‌ها را تغییر داده‌اند. از سوی دیگر، همین فناوری‌ها به ابزارهایی برای مهاجمان سایبری نیز بدل شده‌اند (جواهری و همکاران، ۲۰۲۳). برای مثال، تحلیل داده‌های بزرگ، امکان تحلیل رفتارهای کاربری و نفوذ هدفمند به سامانه‌ها را فراهم می‌کند. همچنین فناوری بلاک‌چین که در ابتدا با هدف امنیت طراحی شد، امروزه با سوءاستفاده در معاملات غیرقانونی یا رمزگذاری مجرمانه مورداستفاده قرار می‌گیرد. در چنین شرایطی، نهادهای امنیتی نیازمند رویکردی هوشمندانه، انعطاف‌پذیر و فناورانه برای فهم و مقابله با این تغییرات هستند، چراکه دیگر تهدیدات، تنها فنی نیستند بلکه با حوزه‌های حقوقی، اقتصادی، فرهنگی و اجتماعی نیز درآمیخته‌اند (غلام‌پور و هدایتی، ۱۴۰۳).

این تعاریف، زمینه‌ساز ورود به مباحث نظری و تحلیلی پژوهش خواهند بود. در بخش بعدی، به پیشینه پژوهش و بررسی دستاوردهای علمی پیشین در این حوزه خواهیم پرداخت.

پیشینه پژوهش

نیکو منش و برخورداری (۱۳۹۷) در پژوهشی با عنوان «چالش‌های مجازی‌سازی روابط و تأثیر آن بر نهادهای خانواده» بر این باورند که اتکا به شبکه‌های اجتماعی باعث آسیب‌هایی مانند ازدواج‌های اینترنتی، طلاق و فروپاشی خانواده در بسیاری از کشورها می‌شود. جهان، ازجمله ایالات‌متحده و بریتانیا، رشد قابل‌توجهی داشته است. طبق آمار ایالات‌متحده، حداقل یکی از هر ۵۰ زوج متأهل در سال ۲۰۱۱ از طریق سایت‌های شبکه‌های اجتماعی با یکدیگر آشنا شده‌اند. درعین‌حال از هر ۵ وکیل طلاق در آمریکا ۴ نفر اعلام کردند که تعداد پرونده‌های طلاق مربوط به شبکه‌های اجتماعی افزایش‌یافته است. علاوه بر این، شبکه‌های اجتماعی فوق، همسر ناراضی را وسوسه می‌کند تا به دنبال افراد دیگری (دوستان، همکلاسی‌های سابق، دوستان نزدیک دوران کودکی یا دوستان جدید و غیره) باشد که ممکن است پتانسیل فریب همسر فعلی خود را داشته باشند. همچنین رضاییان و رئیسی (۱۳۹۶) در پژوهشی با عنوان «تأثیر جرائم به وقوع پیوسته در شبکه‌های اجتماعی بر سبک زندگی نسل چهارم» چنین تبیین می‌کند که هدف مقاله حاضر بررسی تأثیر شبکه‌های اجتماعی مجازی (تلگرام، اینستاگرام و توییتر) بر سبک زندگی

1. Big Data

نسل چهارمی‌ها یا متولدین دهه هشتاد است. در این پژوهش با رویکرد اثبات‌گرایی، از فن پیمایش استفاده‌شده است. جامعه آماری دانش‌آموزان مقطع متوسطه دوم شهر تهران بوده و سه منطقه ۱، ۷ و ۱۶ به‌عنوان مناطق نمونه انتخاب‌شده‌اند. تعداد نمونه بر اساس فرمول کوکران ۳۸۰ نفر که با روش نمونه‌گیری خوشه‌ای چندمرحله‌ای طبقه‌بندی تصادفی انتخاب شدند. یافته‌ها بیانگر آن است که بین میزان استفاده و نوع شبکه‌های اجتماعی مجازی و ابعاد سبک زندگی همبستگی مستقیمی وجود دارد، به‌گونه‌ای که هرچه میزان استفاده از شبکه‌های اجتماعی افزایش یابد، گرایش به سبک زندگی مدرن نیز، بالاتر می‌رود. همچنین، به میزان فاصله گرفتن از سبک زندگی سنتی، اعتماد اجتماعی کاهش ولی سرمایه فرهنگی افزایش‌یافته است. در پژوهشی دیگر، عاشور (۲۰۲۲) در پژوهشی با عنوان «مبنای قانونی جرم اخاذی الکترونیکی علیه زنان و کودکان و مصلحت در نظر گرفته‌شده برای آنان» بیان می‌کند که عکس مهم‌ترین وسیله در دست باج گیران و پس‌ازآن صدا است. یکی از عوامل باج‌خواهی، سهل‌انگاری برخی از دختران و زنان در ارسال تصاویر خود از طریق شبکه‌های اجتماعی و یا ذخیره تصاویر خود در حافظه موبایل است. گاهی دیده شده که حتی در هنگام فروش دستگاه، آن‌ها را حذف نمی‌کند، بنابراین باج‌گیر وقتی عکس یکی از آن‌ها را پیدا می‌کند متوسل به تهدید می‌شود تا به فرد فشار بیاورد و از وی اخاذی کند، در غیر این صورت او را با تصاویر یا صداهای خود افشا می‌کند.

چارچوب نظری پژوهش

در تحلیل تهدیدات نوظهور سایبری، نمی‌توان به الگوهای سنتی واکنش به جرم و پیشگیری از آن بسنده کرد؛ چراکه با پدیده‌ای مواجهیم که نه‌تنها در بستر زمان بلکه در متن تحولات فناورانه، فرهنگی و امنیتی بازتعریف می‌شود. چارچوب نظری این پژوهش بر پایه درک تعامل میان سه مؤلفه اصلی: ساختار جرم دیجیتال، آسیب‌پذیری نظام‌های اجتماعی و ناکارآمدی سیاست جنایی سنتی در عصر سایبری بناشده است. در این زمینه، نظریه «جامعه مخاطره‌آمیز» اولریش بک (۱۹۹۲) یکی از پایه‌های اصلی درک مفهوم تهدیدات نوظهور است. بر اساس این دیدگاه، مخاطرات برخاسته از فناوری مدرن نه‌تنها غیرقابل‌کنترل، بلکه فراگیر و چندبعدی‌اند؛ به‌گونه‌ای که نهادهای سنتی قانون‌گذاری، امنیتی و قضایی قادر به واکنش سریع، متناسب و پیش‌بینی‌پذیر به آن‌ها نیستند. همچنین از دیدگاه نیکلاس لومان[1]، نظام‌های اجتماعی مدرن، تحت‌فشار پیچیدگی‌های فناورانه، دچار گسست‌های ارتباطی و سازوکاری می‌شوند؛ این گسست‌ها دقیقاً همان گلوگاه‌هایی‌اند که تهدیدات سایبری از آن عبور می‌کنند. لومان، بر ضرورت خودتنظیمی ساختاری در نظام‌های اجتماعی برای بازآفرینی امنیت تأکید دارد. در این بستر، نظریه‌های نوین جرم‌شناسی سایبری نظیر «نظریه انتخاب عقلانی» و «نظریه سبک زندگی دیجیتال» به ما می‌آموزند که جرم

1. Niklas Luhmann

در فضای سایبری برخلاف جرائم سنتی، مبتنی بر محاسبات فرصت‌محور و طراحی کنش‌های زیرکانه توسط فاعلان سایبری است. در چارچوب مفهومی این پژوهش، تهدیدات سایبری نوظهور در سه سطح تحلیل می‌شوند:

الف) سطح فردی: تصمیم مجرمانه، انگیزه و توانایی فنی؛

ب) سطح نهادی: ضعف زیرساخت‌های تقنینی و قضایی در پاسخ به تهدید؛

ج) سطح ساختاری: تعامل قدرت، فناوری و سیاست بین‌المللی در تولید یا مهار تهدید.

برآیند این سطوح، نشان‌دهنده ضرورت بازتعریف سیاست جنایی تقنینی بر پایه الگوهای پاسخ سریع، تطبیق‌پذیر و چندلایه است که در آن نهادهای قانون‌گذاری، امنیتی و فناورانه در قالب یک معماری حکمرانی سایبری مشترک عمل کنند.

دیدگاه‌های حقوقی

از منظر حقوق عمومی و حقوق کیفری، تهدیدات سایبری نوظهور بستری برای به چالش کشیدن اصول بنیادین نظیر «قانونی بودن جرم و مجازات»، «صلاحیت سرزمینی» و «تناسب جرم و مجازات» فراهم کرده‌اند. یکی از بحران‌های بنیادی در حقوق کیفری، ناتوانی در تعریف دقیق، شفاف و جامع از جرائم سایبری است؛ زیرا بسیاری از این تهدیدات نه با نیت مجرمانه سنتی، بلکه با ترکیبی از اهداف اقتصادی، سیاسی، اطلاعاتی و گاهی صرفاً نمایشی صورت می‌پذیرند. به‌بیان‌دیگر، تفکیک روشن میان «نفوذ غیرمجاز»، «کنجکاوی فناورانه» و «حمله سازمان‌یافته» برای قانون‌گذار کلاسیک امری دشوار است. قوانین ایران نظیر قانون جرائم رایانه‌ای مصوب ۱۳۸۸، به‌رغم گام مثبت اولیه، در مواجهه با تهدیداتی چون باج‌افزارها، دستکاری الگوریتمی، نفوذ به زنجیره بلوکی، جاسوسی الگوریتمی و جنگ اطلاعات، دچار کاستی‌های تقنینی جدی‌اند. از منظر تطبیقی، کشورهایی چون ایالات‌متحده و اتحادیه اروپا تلاش کرده‌اند با تدوین قوانینی چون Cybersecurity Enhancement Act، Computer Fraud and Abuse Act و NIS2 Directive، ساختار پاسخ‌گویی تقنینی را مبتنی بر دو اصل پایه‌ای تنظیم کنند: نخست، اصل پویایی تقنین در برابر تهدیدات تغییرشکل‌یابنده؛ دوم، اصل هم‌پوشانی صلاحیت‌های فنی، قضایی و امنیتی. در این چارچوب، وظیفه جرم‌انگاری تنها بر دوش قانون‌گذار نیست، بلکه یک کنسرسیوم مشارکتی میان نهادهای تقنینی، جامعه فناوران، شرکت‌های داده محور و دستگاه قضا شکل می‌گیرد. حقوق کیفری ایران نیازمند نوسازی ساختاری در سه محور است:

الف) توسعه صلاحیت جهانی در جرائم سایبری؛

ب) پذیرش مقررات فراملی در زمینه جرائم سایبری بر پایه معاهدات؛

ج) طراحی نهاد مستقل «دادسرای جرائم سایبری پیشرفته» باصلاحیت ترکیبی حقوقی-فنی.

دیدگاه‌های جرم‌شناسی

از دیدگاه جرم‌شناسی، تهدیدات سایبری نوظهور در چارچوب سنتی تحلیل جرم نمی‌گنجند. این تهدیدات بر پایه ویژگی‌هایی چون فرازمانی، فرامکانی، فاقد هویت سنتی و دارای ساختار شبکه‌ای غیرمتمرکز تعریف می‌شوند. درنتیجه، دسته‌بندی‌های کلاسیکی مانند "مجرم"، "قربانی"، "صحنه جرم" و ابزار جرم، در زمینه فضای سایبری اغلب بی‌معنا یا تغییریافته‌اند. بر این اساس، جرم‌شناسانی چون «توماس هالت[1]، دیوید والت[2]» و در نظریات نوین خود بر ضرورت تأسیس جرم‌شناسی سایبری مستقل تأکید کرده‌اند که در آن، تحلیل جرم نه از زاویه فرد، بلکه از زاویه شبکه‌های ارتباطی، الگوریتم‌ها و ساختارهای نفوذ دیجیتال صورت می‌گیرد. بر مبنای این دیدگاه‌ها، مجرم سایبری، الزاماً فردی مجرم با نیت معطوف به شر نیست؛ بلکه می‌تواند بازیگری دولتی، شرکت فناوری، یا حتی نرم‌افزاری باشد که در شرایط خاص، ساختارهای مشروع را به خطر می‌اندازد. به‌ویژه در مواردی چون جاسوسی سایبری، دروغ‌پراکنی الگوریتمی، یا حمله به زیرساخت‌های حیاتی، کنش مجرمانه در بستر نابرابری اطلاعاتی و فناورانه میان کشورها و شرکت‌ها تکوین می‌یابد. در این میان، تحلیل «سبک زندگی دیجیتال قربانیان[3]» نیز اهمیت می‌یابد؛ چراکه بسیاری از قربانیان، به سبب استفاده ناآگاهانه، نبود سواد رسانه‌ای و عدم رعایت امنیت پایه‌ای، در معرض تهدیدات قرار می‌گیرند. اینجاست که نقش سیاست‌های آموزش محور، شفاف‌سازی و فرهنگ‌سازی پیش‌دستانه در قالب سیاست جنایی پیشگیرانه برجسته می‌شود.

مبادی تصوری پژوهش

در این بخش از پژوهش به ماهیت جرائمی که در فضای سایبری رخ می‌دهد از منظر جرم‌شناسی و دیگر روابطی و عللی که وجود دارد، اشاره خواهد نمود.

دیدگاه کلی قانونی در حوزه جرائم سایبری

جرم‌شناسی، شاخه‌ای از علوم جنایی است که با روش علمی و عینی به تحلیل علل و عوامل زیستی، روانی و اجتماعیِ پیدایش جرم و راهکارهای کنترل رفتار مجرمانه در فرد و جامعه، با هدفِ پیشگیری از وقوع جرم و اصلاح و درمان بزهکاران، می‌پردازد. ازاین‌رو، جرم‌شناسی به‌عنوان علم علل جرم تعریف‌شده و بر گفته از رویکردها و قرائت‌های مختلف از پدیده جنایی در جامعه است. در طی چند دهه اخیر، علاقه روزافزونی نسبت به بهره‌گیری از نتایج تحقیقات جرم‌شناسی در توسعه سیاست‌گذاری و برنامه‌ریزی در بخش‌های مختلف نظام عدالت کیفری به

1. Thomas Holt
2. David Wall
3. Digital Lifestyle of Victims

وجود آمده است؛ چراکه جرم نیز مانند دیگر پدیده‌ها دارای علت است و اگر علت یا علل آن مشخص گردد تا حد زیادی می‌توان از وقوع آن پیشگیری کرد (گتوندی، ۱۴۰۰). علم جرم‌شناسی در عمر یک صدساله خود همواره در پی کشف عوامل جرم‌زا و شرایط مؤثر در بروز رفتار جنائی بوده تا به مدد آن و البته بهره‌گیری از تمامی تخصص‌های علمی به روش‌های پیشگیری از حدوث جرائم و روش‌های درمان و اصلاح و تربیت بزهکاران دست یابد؛ اما نکته قابل‌توجه در این میان آن است که چنین تکاپویی تا اوایل دهه شصت و همزمان با پیدایش جرائم سایبری صرفاً در بستر دنیای حقیقی بوده است هرچند که نقاط مشترکی در مطالعات تطبیقی جرائم فضای حقیقی و مجازی وجود دارد لکن باید گفت جرائم سایبری مرزهای مطالعاتی جدیدی برای جرم‌شناسان ایجاد کرده است زیرا این جرائم در سیر تحول خود، نه‌تنها چالش مفهومی و مصداقی برای حقوق جزای سنتی ایجاد کرده بلکه ادبیات تخصصی خاص خود را نیز دارا هستند. هرچند برخی بر این باورند که اصلاح قوانین سنتی جزایی پاسخگوی نیازها در برابر جرائم سایبری است در مقابل عده‌ای معتقدند دنیای مجازی دنیایی جدید است و مجرمان سایبر ازلحاظ جرم‌شناسی از مجرمان عادی متفاوت‌اند و مجازات و درمان‌های متفاوتی را نیاز دارند. مطالعه علمی جرم در چارچوب رشته‌ای به نام جرم‌شناسی، در اواخر سده نوزدهم میلادی آغاز گردید. جرم‌شناسی تحت تأثیر وضعیت علوم و فرهنگ آن عصر، مطالعات خود را بر جرائمی متمرکز کرد که علیه تمامیت جسمانی، اخلاقی و مالی انسان در دنیای حقیقی- دنیایی که ملموس و فیزیکی است و شهروندان آن از نزدیک با یکدیگر ارتباط و دادوستد داشتند، ارتکاب می‌یافت. جرم‌شناسی، به‌موازات تحولات علمی، اقتصادی، فنی و اجتماعی نیمه دوم سده بیستم، خود نیز ازنظر روش‌شناسی، رویکردهای نظری و موضوع مطالعه، دستخوش دگرگونی شد و در این مقطع رفتارهایی را در مطالعات خود وارد کرد که به لحاظ نقض ارزش‌ها و مصالح جدید فنی و حقوق بشری، در حقوق کیفری جرم انگاری شده بودند. ویژگی اصلی این جرائم نیز، همچون جرائم اخلاقی که هسته اصلی بزهکاری را تشکیل می‌دهند، این است که همچنان در محیط یا فضای حقیقی به وقوع می‌پیوندند و بنابراین ازنظر حقوقی، مشمول اصول عمومی حقوقی کیفری «حقیقی» می‌شوند و ازنظر جرم شناختی نیز در چارچوب همان اصول، یافته‌ها و نظریه‌های جرم‌شناسی «حقیقی» موردمطالعه قرار می‌گیرند (گتوندی، ۱۴۰۰). ازجمله آثار پیشرفت‌های علمی و فناورانه اواخر سده بیستم، تولد دنیای جدیدی بود که از پیوندهای فناوری‌های اطلاعاتی و ارتباطی پدید آمده و فضای مجازی (سایبری) یا اطلاعاتی-ارتباطی نام گرفت و به فضاهای زمینی، دریایی و هوایی دنیای حقیقی افزوده شد. به دنبال این دگرگونی اساسی، بخش قابل‌توجهی از روابط و فعالیت‌های علمی، اجتماعی، اقتصادی انسان‌ها به این دنیای بی‌مرز و ناملموس منتقل گردید. هم‌اکنون، یکی از مظاهر این جهان به‌اصطلاح مجازی، یعنی شبکه جهانی اینترنت، بیش از یک میلیارد و نیم عضو و شهروند مجازی دارد و درواقع فعالیت و روابط خود را در دوجهان حقیقی و مجازی، همزمان دنبال می‌کنند. بدین ترتیب، انسان‌های آغاز هزاره سوم، دارای حقوق و تکالیف شهروندی دوگانه حقیقی و مجازی و به عبارتی زندگی دوم شده‌اند (سمسی، ۱۳۹۹). بااین‌حال، نباید تصور کرد که

فعالیت در دنیای مجازی، فاقد اعتبار و پیامدهای حقوقی است، بلکه به همان اندازه و در مواردی حتی بیشتر از نمونه‌های دنیای فیزیکی، آثار حقوقی به دنبال دارد. تعبیر مجازی بودن تنها ازاین‌جهت است که فناوری‌های اطلاعاتی و ارتباطی، قابلیت شبیه‌سازی و مجازی‌سازی دارند تا بتوانند امور فیزیکی را به‌طور مطلوب به نمایش و اجراگذارند. این قابلیت منحصربه‌فرد و بسیار سودمند به واقعی بودن فعالیت‌ها، روابط و دادوستد جاری در فضای سایبر خدشه‌ای وارد نمی‌سازد (سمسی، ۱۳۹۹). به‌موازات گسترش فعالیت‌ها و ارتباطات در فضای سایبر، بخشی از بزهکاران نیز فعالیت‌های مجرمانه خود را به فضای سایبری منتقل کرده‌اند یا از رهگذر چنین فضایی، مرتکب جرم یا جرائمی می‌شوند. ازاین‌پس گونه‌های بزهکاری متعارف در فضای سایبری، به‌وسیله این جلوه از فناوری جدید اطلاعات و ارتباطات ارتکاب می‌یابد. عده‌ای از بزهکاران، با ظهور فضای مجازی، ازجمله اینترنت درواقع از یکسو، فرصت‌ها و وسایل جدید برای ارتکاب اعمال مجرمانه متعارف و کلاسیک دنیای حقیقی و از سوی دیگر، گونه‌های بزهکارانه نوین مرتبط با ویژگی‌ها و ماهیت مجازی، پیداکرده‌اند؛ یعنی افزون بر ارتکاب جرائم متعارف، شاهد ظهور جرائم خاص رایانه‌ای یا مرتبط با رایانه و به‌طورکلی دنیای سایبری هستیم (حاجی ده آبادی و همکاران، ۱۳۹۷). در چنین فضایی وجود عاملی که بتواند نابهنجاری افراد و گروه‌های سازمان‌یافته را کنترل کند امری بدیهی است؛ اما پیشگیری ازاین‌گونه رفتارها خود اهمیت ویژه‌ای دارد و سیاست‌جنایی ایران در این راستا قابل‌تأمل است؛ چراکه پیشگیری را بهتر از درمان دانسته‌اند و پیشگیری به‌نوعی مقابله با بروز انواع جرائم در حوزه اینترنتی است (رایجیان اصل، ۱۳۹۳). ازجمله این موضوعات می‌توان به باج‌گیری براثر اغفال و فریب کاربران رایانه‌ای و مقیم در شبکه‌های اجتماعی اشاره کرد که همتای جرم در فضای فیزیکی است. لیکن، قانون‌گذاری و برخورد با چنین بزه‌هایی، رویکرد قطعی قانون خواهد بود (فرجیها، ۱۳۹۳).

چالش‌های محیط مجازی

شبکه جهانی، فضایی نامحدود و گسترده‌ای از حجم اطلاعات است که همگانی، بدون کنترل و مرکزیت واحد است؛ و بیش از صدها میلیون کاربر و صفحه اینترنتی وجود دارد که این روند روبه‌پیشرفت و ازدیاد است و همین روند روب رشد، چالش‌های زیادی را پدید آورده است (حسینی و همکاران، ۱۴۰۳). سهولت دسترسی یکی از الزامات سنتی ارتکاب جرم است. همین ویژگی با توسعه شبکه جهانی اینترنت، زمینه چالش‌های زیادی را فراهم کرده است. اگر تا چند وقت قبل نیاز به حضور فیزیکی مرتکب برای راه‌یابی به محیط رایانه‌ای و انجام عمل غیرقانونی بوده اما امروزه با پیشرفت شبکه جهانی اینترنت، فرد حتی از راه دور و بدون نیاز به حضور فیزیکی می‌تواند به سامانه‌ها دسترسی پیدا کند که این دسترسی اغلب به دلیل راهکارهای امنیت ضعیف است (خلیلی، ۱۴۰۳). چالش دیگر امکان ایجاد هویت جعلی است که این امکان را به کاربران می‌دهد تا به‌جای یک کاربر مجاز وارد سیستم شوند. چالش دیگر، گستردگی و فراگیر بودن قلمرو محیط مجازی است؛ که همین ویژگی باعث دستیابی به هرگونه

اطلاعاتی می‌شود که گاهی می‌تواند خصوصی‌ترین اطلاعات افراد باشد؛ و همین تنوع اطلاعات موجود در فضای مجازی باعث رسیدن برخی افراد به اهداف غیرقانونی می‌شود. گاهی یک هکر می‌تواند به‌راحتی کلیه اطلاعات موجود در پایگاه داده‌ی یک سازمان دولتی یا خصوصی را در دست بگیرد؛ و از این طریق سوءاستفاده کند. نکته و چالش دیگر که باعث بروز ارتکاب جرائم سایبری می‌شود بی‌مرز بودن این فضاست. در جهان فیزیکی هر فردی که قصد ارتکاب عمل غیرقانونی را داشته باشد ازنظر مکانی با محدودیت روبروست اما این محدودیت در فضای مجازی بی‌معناست؛ و همین امر باعث توسعه ارتکاب جرائم فراملی شده است. مواردی که اشاره شد تنها بخشی از ویژگی‌های بحران‌زای فضای مجازی بود که زمینه را برای ارتکاب هر چه آسان‌تر و کم‌هزینه‌تر بودن اعمال مجرمانه فراهم کرد.

تهدیدات نوظهور در فضای مجازی

فضای مجازی، با توجه به گسترش روزافزون فنّاوری‌های نوین، به محیطی پیچیده و خطرناک برای تهدیدات سایبری تبدیل‌شده است. این تهدیدات نه‌تنها ابعاد پیچیده‌ای دارند، بلکه به‌طور مداوم در حال تکامل و پیچیده‌تر شدن هستند. به همین دلیل، درک و شناسایی این تهدیدات به‌طور صحیح برای مقابله مؤثر ضروری است.

۱. باج‌افزارها[1]: تهدیدی در حال تحول

باج‌افزارها یکی از پررنگ‌ترین تهدیدات در فضای سایبری هستند که طی سال‌های اخیر به‌طور فزاینده‌ای در سطح جهانی گسترش‌یافته‌اند. باج‌افزارها معمولاً از طریق فیشینگ، نرم‌افزارهای آلوده، یا آسیب‌پذیری‌های نرم‌افزاری وارد سامانه‌های کامپیوتری می‌شوند و پس از قفل‌کردن داده‌ها یا سامانه‌ها، از قربانی درخواست پول به‌عنوان باج می‌کنند؛ اما این تهدید به‌مرورزمان پیچیده‌تر شده است. امروزه، حملات باج‌افزاری هدفمند به سازمان‌ها، مراکز دولتی، بیمارستان‌ها و حتی سامانه‌های زیرساختی حیاتی، به‌ویژه در کشورهای پیشرفته، افزایش‌یافته است. باج‌افزارهای جدید، مانند Conti و REvil، علاوه بر رمزگذاری داده‌ها، اطلاعات حساس را دزدیده و به‌عنوان تهدید به افشای عمومی قرار می‌دهند. این حملات نه‌تنها با سامانه‌های فناوری اطلاعات، بلکه با سامانه‌های صنایع حساس نیز درگیر می‌شوند که تهدید بزرگی برای صنایع حیاتی مانند انرژی، بهداشت و درمان و حمل‌ونقل به شمار می‌رود. به همین دلیل، این نوع تهدیدات به یکی از بزرگ‌ترین مشکلات امنیتی در فضای مجازی تبدیل‌شده‌اند (محمد و همکاران، ۲۰۲۳). لذا ویژگی برجسته حملات باج‌افزاری جدید این است که اغلب با

1. Ransomware

استفاده از حملات توزیع‌شده و سازمان‌دهی گروهی صورت می‌گیرند. به‌طورمعمول، گروه‌های مجرمانه در پس این حملات از ایجاد باج‌افزارهای سفارشی و گسترش شبکه‌های رباتیک[1] بهره می‌برند. علاوه بر این، مدیریت تهدیدات در سطح کلان با استفاده از هوش مصنوعی و یادگیری ماشینی برای پیش‌بینی و شناسایی الگوهای حملات باج‌افزاری و جلوگیری از حملات گسترده‌تر اهمیت دارد (الحسن[2] و همکاران، ۲۰۲۳).

۲. حملات مبتنی بر هوش مصنوعی

در سال‌های اخیر، هوش مصنوعی به‌طور گسترده‌ای در تولید تهدیدات سایبری به‌ویژه برای حملات فیشینگ و حملات هدفمند مورداستفاده قرارگرفته است. این نوع حملات، با استفاده از یادگیری ماشینی و الگوریتم‌های هوشمند، قادر به شبیه‌سازی رفتارهای انسانی و دستکاری دقیق‌تر سامانه‌های امنیتی هستند. به‌عنوان‌مثال، حملات فیشینگ با استفاده از چت‌بات‌های مبتنی بر هوش مصنوعی و پیام‌های سفارشی‌شده می‌توانند به‌طور مؤثری کاربران را فریب دهند. نمونه‌هایی از حملات هوش مصنوعی: هکرها با استفاده از الگوریتم‌های پردازش زبان طبیعی[3]، پیام‌های فیشینگ را به‌گونه‌ای طراحی می‌کنند که کاملاً شبیه به پیام‌های واقعی به نظر برسند. این نوع حملات به حدی پیشرفته شده‌اند که تشخیص آن‌ها برای سامانه‌های امنیتی و حتی کاربران بسیار دشوار شده است. در برخی موارد، این حملات از مدل‌های یادگیری عمیق برای شبیه‌سازی شخصیت‌های معتبر و حتی ایمیل‌های تقلبی استفاده می‌کنند (ژانگ و وانگ[4]، ۲۰۲۴). افزایش استفاده از هوش مصنوعی در حملات سایبری از جنبه‌های مختلفی نشان‌دهنده تهدیدی جدی است. افزایش هوش مصنوعی در تحلیل رفتار کاربران و همچنین شبیه‌سازی‌های پیشرفته موجب خواهد شد که این تهدیدات هر روز پیچیده‌تر و گسترده‌تر شوند. در این شرایط، پیگیری راهکارهای مقابله‌ای مانند آموزش خودکار سامانه‌های امنیتی و پایش پیشرفته رفتارهای مشکوک ضروری خواهد بود.

۳. حملات به زیرساخت‌های حیاتی[5]

یکی از دیگر تهدیدات نوظهور و بسیار مهم، حملات به زیرساخت‌های حیاتی مانند شبکه‌های برق، آب، حمل‌ونقل و سامانه‌های بانکی است. این نوع حملات معمولاً با هدف مختل کردن عملکرد سامانه‌های حیاتی صورت می‌گیرند و می‌توانند خسارات زیادی به زیرساخت‌های کشورها وارد کنند. نمونه‌ای از این حملات، حمله

1. Botnet
2. ALhassan
3. Natural Language Processing
4. Zhang, Wang
5. Critical Infrastructure Attacks

Stuxnet است که در سال ۲۰۱۰ به تأسیسات هسته‌ای ایران وارد شد. این نوع حملات به دلیل پیچیدگی فناوری و اعتماد به سامانه‌های صنعتی، می‌تواند پیامدهای فاجعه‌آمیزی داشته باشد. امروزه، با استفاده از دستگاه‌های متصل به اینترنت، حملات به اینترنت اشیاء به‌شدت گسترش‌یافته است. این دستگاه‌ها که شامل دوربین‌های مداربسته، ترموستات‌ها و تجهیزات کنترل صنعتی می‌شوند، به‌طور بالقوه به اهداف آسان برای حملات سایبری تبدیل‌شده‌اند. هکرها می‌توانند از این دستگاه‌ها برای ایجاد شبکه‌های Botnet استفاده کرده و حملات گسترده‌تری را اجرا کنند (سیمانتک، ۲۰۲۳). تهدیدات به زیرساخت‌های حیاتی به دلیل وابستگی روزافزون جامعه به فناوری‌های دیجیتال اهمیت بسیاری دارند. برای مقابله با این تهدیدات، استفاده از سامانه‌های نظارت و پایش پیشرفته، امنیت در سطح سخت‌افزار و استفاده از فناوری‌های مقاوم در برابر حملات سایبری ضروری است.

۴. تهدیدات مربوط به اینترنت اشیاء

یکی از بزرگ‌ترین تهدیدات در فضای مجازی که به‌سرعت در حال گسترش است، تهدیدات مرتبط با اینترنت اشیاء است. ازآنجاکه این دستگاه‌ها به‌طور فزاینده‌ای به اینترنت متصل می‌شوند، تهدیدات سایبری به‌ویژه در بخش‌های خانگی، صنعتی و تجاری گسترش‌یافته‌اند. دستگاه‌های اینترنت اشیاء معمولاً فاقد سطح مناسب امنیتی هستند و همین امر آن‌ها را به اهداف آسان برای حملات سایبری تبدیل می‌کند. لذا گسترش شبکه‌های اینترنت اشیاء تهدیدات جدیدی به‌ویژه در امنیت اطلاعات شخصی و نفوذ به زیرساخت‌های حساس ایجاد کرده است. استفاده از پروتکل‌های امنیتی استاندارد و آموزش کاربران برای محافظت از دستگاه‌های اینترنت اشیاء ازجمله الزامات اساسی برای مقابله با این تهدیدات به شمار می‌روند. فضای مجازی، با توجه به پیشرفت‌های فنّاورانه، شاهد ظهور تهدیدات جدید و پیچیده‌ای است. این تهدیدات نه‌تنها سامانه‌های فناوری اطلاعات، بلکه زیرساخت‌های حیاتی، اطلاعات شخصی و امنیت ملی را نیز در معرض خطر قرار می‌دهند. برای مقابله مؤثر با این تهدیدات، نیاز به استراتژی‌های حفاظتی پیچیده‌تر و پایش لحظه‌ای تهدیدات است. علاوه بر این، آموزش و آگاهی کاربران از خطرات موجود در فضای مجازی و همچنین ایجاد همکاری بین‌المللی برای مقابله با تهدیدات سایبری اهمیت زیادی دارد (اسحاق و فرید[1]، ۲۰۲۳).

استراتژی‌های حفاظتی در سایبر: از امنیت فناورانه تا حکمرانی حقوقی و سیاستی

در فضای مجازی، تهدیدات نوظهور دیگر تنها در قالب حملات سایبری کلاسیک، نظیر بدافزار، فیشینگ یا نفوذ به شبکه‌ها نمود نمی‌یابند؛ بلکه ابعاد پیچیده‌تری همچون حملات شناختی، جاسوسی سایبری سازمان‌یافته،

1. Isagh, Fareed

مداخله در افکار عمومی از طریق پلتفرم‌های هوش مصنوعی و آسیب به زیرساخت‌های حیاتی دیجیتال را نیز دربر می‌گیرند (انیسا[1]، ۲۰۲۳). به همین دلیل، استراتژی‌های حفاظتی نمی‌توانند صرفاً فنی باقی بمانند و باید در قالب سیاست‌های کل‌نگر، با تأکید بر حکمرانی سایبری، توسعه یابند (کلو، ۲۰۱۷). از منظر حقوقی، فضای مجازی یکی از پیچیده‌ترین حوزه‌ها برای اعمال حاکمیت است؛ چراکه در آن اصل صلاحیت سرزمینی[2] به‌واسطه ماهیت فراملی فضای مجازی تضعیف‌شده است (کوپس، ۲۰۱۴). همین امر موجب می‌شود که کشورها ناچار به تدوین قوانین داخلی برای صیانت از دارایی‌های دیجیتال، اطلاعات شخصی و زیرساخت‌های حیاتی باشند؛ اما در نبود توافقات بین‌المللی الزام‌آور، این قوانین اغلب با چالش مواجه‌اند (زوبوف، ۲۰۱۹). در ایران نیز، تصویب اسنادی مانند قانون جرائم رایانه‌ای (۱۳۸۸)، سند راهبردی افتا (۱۴۰۲) و پیش‌نویس لایحه حمایت از داده‌های شخصی، نشانه‌ای از تلاش برای استقرار سیاست‌های حفاظتی ملی است. بااین‌حال، مطالعات نشان داده‌اند که این اسناد هنوز از انسجام نهادی، ضمانت اجرای کافی و هماهنگی با الزامات بین‌المللی بی‌بهره‌اند (کیاسری، ۱۳۹۶). از منظر مسئولیت حقوقی، نهادهایی که در حفظ امنیت سایبری کوتاهی کنند، ممکن است مشمول مسئولیت مبتنی بر تقصیر یا در برخی موارد، مسئولیت محض ناشی از فعالیت‌های پرخطر فناورانه شوند (سولوو، ۲۰۲۰). در نظام‌های حقوقی پیشرفته، نظارت بر این موارد بر عهده نهادهای مستقل[3] نهاده شده است (گرینلیف[4]، ۲۰۱۸). در سطح سیاست‌گذاری، راهبردهای حفاظتی باید ناظر به چرخه پیشگیری، پاسخ، بازیابی و ارتقاء تاب‌آوری سازمانی باشند. همچنین، اصل مشارکت ذی‌نفعان مختلف – اعم از دولت، بخش خصوصی، دانشگاه و جامعه مدنی – به‌عنوان یکی از ارکان حکمرانی خوب سایبری در اسناد بین‌المللی، ازجمله گزارش گروه خبره سازمان ملل متحد[5](۲۰۲۱) تأکید شده است. از سوی دیگر، با پیشرفت هوش مصنوعی و کلان داده، مسئله بی‌طرفی الگوریتمی، تبعیض دیجیتال و مداخله در اراده سیاسی شهروندان به تهدیداتی جدید برای آزادی‌های بنیادین تبدیل‌شده‌اند که نیازمند رویکردهای حقوق بشری در حکمرانی داده و حفاظت از حقوق دیجیتال شهروندان است (میتلاستید[6]، ۲۰۱۶). در پایان، تأکید می‌شود که هیچ راهبرد حفاظتی‌ای در فضای سایبری بدون پشتیبانی حقوقی شفاف، سیاست‌گذاری داده محور، نظارت نهادینه و اعتماد عمومی پایدار نخواهد بود. حکمرانی سایبری باید تلفیقی از اصول امنیتی، حقوقی و مشارکتی باشد تا به‌جای تقویت اقتدارگرایی دیجیتال، عدالت دیجیتال را ارتقاء دهد (زوئیتر[7]، ۲۰۱۴).

1. Enisa
2. Territorial Jurisdiction
3. Data Protection Authorities یا Cybersecurity Oversight Committees
4. Greenleaf
5. UN GGE Report
6. Mittelstadt
7. Zwitter

نتیجه‌گیری

این پژوهش نشان داد که تهدیدات سایبری نوظهور مانند باج‌افزارها، فیشینگ پیشرفته، نقض داده‌ها و حملات مبتنی بر هوش مصنوعی، فضای مجازی ایران را به‌طورجدی تهدید می‌کنند و پیامدهای اقتصادی، اجتماعی و امنیتی گسترده‌ای دارند. استراتژی‌های حفاظتی پیشنهادی شامل بازنگری قانون جرائم رایانه‌ای با الگوبرداری از استانداردهای جهانی، سرمایه‌گذاری در فناوری‌های امنیتی پیشرفته مانند هوش مصنوعی، اجرای برنامه‌های آموزشی گسترده برای کاربران و کارکنان و ایجاد مراکز هماهنگی سایبری مانند CERT است. این استراتژی‌ها با شرایط بومی ایران (منابع محدود، زیرساخت‌های قدیمی) تطبیق داده‌شده‌اند و قابل‌اجرا هستند. این مطالعه چارچوبی جامع و بومی برای حفاظت از فضای مجازی ایران ارائه می‌دهد که می‌تواند به سیاست‌گذاران و سازمان‌ها در تقویت امنیت سایبری کمک کند. بدون اجرای این استراتژی‌ها، فضای مجازی ایران در برابر تهدیدات نوظهور آسیب‌پذیر باقی خواهد ماند. لذا چالش‌های امنیت سایبری در برابر تهدیدات نوظهور نیازمند رویکردی چندوجهی است که شامل اصلاح قوانین، تقویت همکاری بین‌المللی، افزایش آگاهی عمومی و استفاده از فناوری‌های پیشرفته باشد. از منظر جرم‌شناسی، تمرکز بر پیشگیری وضعی و کاهش فرصت‌های جرم می‌تواند نرخ جرائم سایبری را کاهش دهد. اجرای این راهکارها نه‌تنها امنیت فضای مجازی را تقویت می‌کند، بلکه اعتماد عمومی به‌نظام حقوقی و قضایی را افزایش می‌دهد. برای همین مسئله نیز می‌توان چند راهکار اراده داد:

- **تدوین و به‌روزرسانی قوانین جامع سایبری:**

الف: ایجاد قوانین خاص برای جرائم نوظهور مانند سوءاستفاده از هوش مصنوعی، دیپ‌فیک و حملات سایبری به زیرساخت‌های حیاتی.

ب: همگام‌سازی قوانین داخلی با کنوانسیون‌های بین‌المللی مانند کنوانسیون بوداپست (۲۰۰۱) برای تسهیل همکاری قضایی فراملی.

- **تقویت همکاری بین‌المللی:**

الف: امضای تفاهم‌نامه‌های قضایی با کشورهای دیگر برای تبادل اطلاعات و استرداد مجرمان سایبری.

ب: ایجاد یک پایگاه داده بین‌المللی برای ردیابی حملات سایبری و شناسایی گروه‌های مجرم.

- افزایش آگاهی عمومی و آموزش تخصصی: اجرای برنامه‌های آموزشی اجباری در مدارس و سازمان‌ها برای افزایش سواد سایبری.
- تقویت نظام قضایی و اجرای قانون: تأسیس دادگاه‌های تخصصی جرائم سایبری با قضات و کارشناسان آموزش‌دیده در حوزه فناوری.
- استفاده از فناوری‌های پیشرفته مانند تحلیل داده‌های بزرگ و هوش مصنوعی برای ردیابی و شناسایی مجرمان سایبری.

- حمایت از قربانیان و جبران خسارت: ایجاد صندوق جبران خسارت برای قربانیان جرائم سایبری، مشابه صندوق‌های جبران خسارت قربانیان جرائم سنتی.
- تشویق بخش خصوصی به ایفای نقش فعال: الزام شرکت‌های فناوری به پیاده‌سازی استانداردهای امنیتی بالا و گزارش دهی سریع حوادث سایبری.
- ارائه مشوق‌های مالیاتی به شرکت‌هایی که در توسعه فناوری‌های امنیتی سرمایه‌گذاری می‌کنند.

منابع

الف)فارسی

حاجی ده آبادی، محمدعلی، سلیمی، احسان، (۱۳۹۷). «علت‌شناسی بزه دیدگی زنان در شبکه‌های اجتماعی، مطالعه موردی شبکه اجتماعی فیس‌بوک». فصلنامه علمی و پژوهشی زن و جامعه. دوره ۹، شماره ۳۵، پاییز ۱۳۹۷، صفحه ۱۱۷-۱۴۲.

حسینی، س. ح؛ و احمدی بلوطکی، ا. (۱۴۰۳). «بررسی علت‌شناسی جرائم خلاف منافی عفت با تکیه‌بر فضای سایبری». نهمین اجلاس بین‌المللی فقه، حقوق و پژوهش‌های دینی.

خداقلی، زهرا. (۱۳۹۵). «جرائم رایانه‌ای». چاپ هفتم. تهران: ناقوس اندیشه.

خلیلی، م. (۱۴۰۳). «سیاست جنایی تقنینی ایران در قبال جرائم سایبری نوظهور». مجله حقوق فناوری اطلاعات، ۶(۱)، ۲۲-۵۰.

خلیلی، م. (۱۴۰۳). «بررسی جرم کلاهبرداری در بستر اینترنت از منظر قانون و رویه قضایی». نهمین کنفرانس بین‌المللی فقه، حقوق و پژوهش‌های دینی. بازیابی از

رایجیان اصلی، مهرداد. (۱۳۹۸). «درآمدی بر جرم‌شناسی». انتشارات سمت، چاپ چهارم.

رضاییان، عالیه، ادریسی، افسانه. (۱۳۹۶). «تأثیر شبکه‌های اجتماعی بر سبک زندگی نسل چهارم». فصلنامه علمی مطالعات میان فرهنگی. ۱۳(۳۴).

رئوفی نیا، کیارش. (۱۳۹۷). جرائم اینترنتی: ارکان و مصادیق. تهران: نشر قومس.

زارعی، ح؛ و اسماعیلی، ن. (۱۴۰۲). «تحلیل تهدیدات سایبری در پرتو جرم‌شناسی سایبری». فصلنامه حقوق جزا، ۱۸(۲)، ۴۱-۶۳.

سمسی، طیبه. (۱۳۹۹). «نقش شبکه‌های اجتماعی در کیفیت زندگی زنان تهرانی با تأکید بر جرائم حادث‌شده در اینستاگرام». پنجمین همایش بین‌المللی افق‌های نوین در علوم انسانی و مدیریت. کد COI مقاله: DH-CONF05_062.

شفیعی، ن؛ و جلالی، س. (۱۴۰۳). «بازتعریف امنیت ملی در بستر سایبری: رهیافت حکمرانی دیجیتال». پژوهشنامه سیاست دفاعی، ۸(۳)، ۶۶-۸۸.

عزیزی، س. (۱۴۰۱). «بررسی تطبیقی صلاحیت جهانی در جرائم سایبری». دوماهنامه حقوق تطبیقی، ۱۲(۱)، ۶۵-۸۹.

غلام پور، ر؛ و هدایتی، ع. (۱۴۰۳). «تأثیر فناوری‌های نوظهور بر ساختار امنیت ملی دیجیتال»، فصلنامه راهبرد دفاعی، ۱۲(۱)، ۱۴-۳۹.

کیاسری، نیلو. (۱۳۹۶). «بررسی جرائم مرتبط با فضای سایبری با محوریت خانواده ایرانی». پایان‌نامه کارشناسی ارشد قم: دانشگاه آزاد اسلامی.

گتوندی، ش. (۱۴۰۰). « بررسی جرم تروریسم سایبری از منظر حقوق کیفری». مجله حقوقی دانشگاه اصفهان، ۸(۱)، ۸-۲۵

محمودی، ج؛ و یوسفی، م. (۱۴۰۳). «ضرورت تحول ساختار حقوقی در پاسخ به تهدیدات فناورانه». پژوهش حقوق عمومی، ۹(۳)، ۸۷-۱۱۰.

مرادیان، س، حسین زاده، ع؛ و ملکی، م. (۱۴۰۲). «بررسی تهدیدات نوین سایبری و راهبردهای مقابله با آن»، فصلنامه امنیت ملی، ۲۳(۴)، ۳۱-۵۶.

ب) انگلیسی

Ashour, l. A. (2021). Electronic extortion and its impact on university female students. *Review of international geographical education online*, 11(10), 2246-2254.

Alhassan, I. et al. (2023). IoT Security Threats and Mitigation Strategies. *International Journal of Cybersecurity*, 22(1), 12-29.

Dave, R, Ullah, I. & Li, H. (2023). Emerging Cyber Threats: Taxonomy and Countermeasures. *ACM Computing Surveys*, 55(9), Article 181.

European Commission (2022). NIS2 Directive: EU Legislation on Cybersecurity. Retrieved from https://digital-strategy.ec.europa.eu

Holt, T. J. (2021). Cybercrime and Digital Forensics: An Introduction. Routledge.

Ishaq, M. & Fareed, S. (2023). Cybersecurity challenges and emerging threats in post-pandemic digital transformation. *Journal of Cyber Policy*, 8(2), 112–130.

Javaheri, N. Marimuthu, S. & Gupta, B. B. (2023). National Cybersecurity Strategy in the Era of AI and Big Data. *Computers & Security*, 130, 103246.

Mohammad, H. et al. (2023). Ransomware and Critical Infrastructure Security: Challenges and Countermeasures. *Journal of Cybersecurity Research*, 35(4), 99-112.

Symantec (2023). Global Threat Intelligence Report. Symantec Corporation.

United States Congress. (2015). Cybersecurity Enhancement Act. Public Law 113–274.

Wall, D. S. (2022). Crime, Security and Surveillance: Cybercrime and Cybersecurity in the 21st Century. Routledge.

Yar, M. (2020). Cybercrime and Society. SAGE Publications.

Zhang, H. & Wang, Y. (2024). Artificial Intelligence in Cybersecurity: A New Frontier. *Journal of Digital Security*, 21(2), 55-78.