Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 3, Issue 3, 2023

Iran and the UK Criminal Policy in Preventing Cyber Crime

Mehrvarz Aganj[1], Abbas Sheikhol Eslami[2*], Masoume Valipouri[3]

1. PhD Student, Criminal Law and Criminology, Mashhad Branch, Islamic Azad University, Mashhad, Iran.
2. Associate Professor, Department of Law, Mashhad Branch, Islamic Azad University, Mashhad, Iran. (Corresponding Author)
3. Assistant Professor, Faculty of Law, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

ARTICLE INFORMATION

Type of Article: ***Original Research***
Pages: ***185-194***

Corresponding Author's Info
ORCID: *0000-0003-3975-6844*
TELL: *+ 989153148848*
Email: *heikholeslami.abbas.law@gmail.com*

Article history:
Received: *09 May 2023*
Revised: *27 Jul 2023*
Accepted: *29 Agu 2023*
Published online: *23 Sep 2023*

Keywords:
Criminal Policy, Prevention, Cybercrime.

ABSTRACT

The issue of crime and its prevention has always been a challenge in every community and state. The emergence and advancement of information and communication technology has brought tremendous changes and great achievements. Nowadays, most economic, social and cultural activities are somehow dependent on computers and online communication networks, and consequently, the areas of criminal behavior have also changed more widely and varied. This paper which has been written by descriptive and analytical method has concluded that in Iran and the UK, criminal policy in preventing cybercrime is often focused on legislative criminal policy and preventive measures are mainly concerned with situational prevention of these crimes.

How to Cite This Article: Aganj, M; Sheikhol Eslami, A & Valipouri, M (2023). "Iran and the UK Criminal Policy in Preventing Cyber Crime". *Journal of Comparative Criminal Jurisprudence*, 3(3): 185-194.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
انجمن علمی فقه جزای تطبیقی ایران
فصلنامه فقه جزای تطبیقی

دوره سوم، شماره سوم، پاییز ۱۴۰۲

سیاست جنایی ایران و انگلیس در پیشگیری از وقوع جرایم سایبری

مهرورز آگنج[۱]، عباس شیخ‌الاسلامی*[۲]، معصومه ولی‌پوری[۳]

۱. دانشجوی دکتری تخصصی، حقوق جزا و جرم‌شناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران.

۲. دانشیار، گروه حقوق جزا و جرم‌شناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. (نویسنده مسؤول)

۳. استادیار، دانشکده حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱۸۵-۱۹۴

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۳-۳۹۷۵-۶۸۴۴

تلفن: +۹۸۹۱۵۳۱۴۸۸۴۸

ایمیل: heikholeslami.abbas.law@gmail.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۲/۰۲/۱۹

تاریخ ویرایش: ۱۴۰۲/۰۵/۰۵

تاریخ پذیرش: ۱۴۰۲/۰۶/۰۷

تاریخ انتشار: ۱۴۰۲/۰۷/۰۱

واژگان کلیدی:

سیاست جنایی، پیشگیری، جرایم سایبری.

چکیده

مسأله جرم و پیشگیری از آن همواره یکی از چالش‌های موجود در هر اجتماع و دولتی بوده است. پیدایش و رشد بی‌نظیر فناوری اطلاعات و ارتباطات، تحولات شگرف و دستاوردهای بزرگی را به‌همراه داشته است، به‌گونه‌ای‌که امروزه اغلب فعالیت‌های اقتصادی، اجتماعی و فرهنگی به نوعی وابسته به رایانه و شبکه‌های ارتباطیِ برخط شده است و به تبع آن، زمینه‌های بروز رفتارهای مجرمانه نیز گسترده و متنوع‌تر و متناسب با شرایط موجود تغییر یافته است. این مقاله که با روش توصیفی ـ تحلیلی نگارش شده است، به این نتیجه رسیده که در ایران و انگلستان، سیاست جنایی در پیشگیری از جرایم سایبری غالباً متمرکز در سیاست جنایی تقنی بوده و تدابیر پیشگیرانه، عمدتاً ناظر بر پیشگیری وضعی از این جرایم است.

مقدمه

در سال‌های اخیر، انقلاب فناوری اطلاعات و ارتباطات، کمتر عرصه‌ای از حیات بشر را بدون تغییر رها کرده است. تأثیرات این فناوری در ابعاد مختلف زندگی بشر آنچنان گسترده بوده که بعید نیست در آینده همچون پیدایش خط، تاریخ تمدن بشر به دو دوره پیش از پیدایش فناوری اطلاعات و پس از پیدایش آن تفکیک شود. این فناوری بزرگ که در ابتدا برای آسایش و رفاه هرچه بیشتر انسان‌ها مورد بهره‌برداری قرار می‌گرفت، به‌تدریج به ابزاری برای مجرمان، جهت نیل به آمال مجرمانه نیز تبدیل شد. به دیگر سخن، فعالیت بزهکارانه عمومی، دیگر منحصر به دنیای حقیقی نمانده است، بلکه به موازات گسترش فعالیت‌ها و ارتباطات در فضای سایبر، بخشی از بزهکاران نیز فعالیت مجرمانه خود را به فضای سایبر منتقل کرده‌اند یا از رهگذر چنین فضایی، مرتکب جرم می‌شوند.

این فضای جدید به گونه‌ای حقوق جزای سنتی را دستخوش تحولات بنیادین کرده است که تعریف از جرایم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری از موارد متفاوت است. به‌نظر می‌رسد جرم‌شناسی و علت‌شناسی این جرایم نیز تا حدودی متفاوت از جرایم کلاسیک باشد، چراکه در بستر این فناوری، نه‌تنها بزهکاران به شیوه جدیدِ ارتکاب جرم توانمند شده‌اند، بلکه افرادی که پیش‌تر منحرف نبودند نیز به رفتارهای مجرمانه تمایل پیدا کرده‌اند و رقم بزه سایبری در کنار ارقام سیاه و خاکستری این دسته از جرایم با سرعت در حال رشد است.

وابستگیِ فزاینده جامعه به فناوری‌های اطلاعاتی و ارتباطی و ناتوانی دولت‌ها در تعقیب و شناسایی بزهکاران این جرایم، دولت‌ها را به کاربست تدابیر و برنامه‌های پیشگیرانه واداشته است. مطالعه حاضر مقدم بر ورود به موضوع اصلی خود، یعنی مطالعه تطبیقی سیاست جنایی تقنینی دو کشور ایران و انگلیس، نیازمند طرح مباحثی درخصوص فضای سایبر، جرایم سایبری و درنهایت برنامه‌های پیشگیرانه است، چون تا ابتدا گزاره‌های قبلی مورد توجه قرار نگیرد، هرگونه طرح و برنامه پیشگیرانه بی‌ثمر است.

پیشگیری از وقوع جرم یکی از راه‌هایی است که از دیرباز برای جلوگیری از جرم، مورد توجه بشر بوده است، اما به‌صورت علمی، بررسی این موضوع، پیشینه طولانی ندارد. جرم‌شناسی در قرن ۱۹ میلادی، به‌عنوان علمی نوظهور در عرصه علوم مختلف مطرح شد. در اوایل دهه هفتاد میلادی بود که «جرم‌شناسی پیشگیری» به‌عنوان یک رشته خاص، داخل مباحث جرم‌شناسی نظری مطرح گردید (ابراهیمی، ۱۳۹۱: ۱۳). به‌نظر می‌رسد مهم‌ترین دلیل توجه به روش‌های پیشگیری از جرم از یک‌سو «ناکامی پاسخ‌های نظام عدالت کیفری» و از سوی دیگر «افزایش آمار جرایم و نگرانی‌های عمومی» باشد (جوان جعفری و سیدزاده ثانی، ۱۳۹۱: ۲۵۷).

۱- مفهوم جرم سایبری

کلمه سایبر، از لحاظ ریشه‌ای به‌معنای سکاندار است و از نظر مفهومی دلالت بر «خودکارشدن، کنترل مصنوعی و رایانه‌ای شدن» دارد. برخی فضای سایبر را «فضای خیالی» می‌دانند. برخی دیگر معتقدند که فضای سایبر دور از واقعیت است، اما گروهی دیگر معتقدند که فضای سایبر واقعی و حاضر است و آن را با ذخیره و انتقال الکترونیکی اطلاعات برابر گرفته‌اند. برخی نیز آن را با ارتباطات در شبکه‌های رایانه‌ای یکسان پنداشته‌اند. بنابراین می‌توان دید که رویکردهای مفهومی به فضای سایبر متفاوت و گاه متعارض است. با این حال، نگاهی به ادبیات پژوهشی و اسناد کشورهای مختلف جهان به‌ویژه اسناد راهبردی امنیت سایبری کشورهایی همچون آمریکا، کانادا و انگلستان حاکی از آن است که مفهوم فضای سایبر در قلمرو ادبیات پژوهشی جامعه‌شناسی و جرم‌شناسی مفهومی برابر در سطح جهانی یافته است.

در هر حال، فضای سایبر پدیده فراگیر امروز جامعه بشری است که با سرعت و قلمرویی فزاینده در حال درگیرساختن همه ساحات زندگی بشر در تمامی ابعاد و لایه‌ها است. پدیده‌ای منحصربه‌فرد که از عناصر، ابعاد، متغیرها و فرامتغیرهای فراوانی تشکل یافته است و همین ساحت گسترده و قدرتمند است که تعریف و تشخیص جرم سایبری را مهم می‌نماید.

از زمان پیدایش رایانه تاکنون، می‌توان از سه نسل جرایم مرتبط با رایانه سخن گفت. تا اواخر دهه ۸۰ میلادی جرایم رایانه‌ای نسل اول که بیشتر جرایم علیه حریم خصوصی رایانه بود را شامل می‌شد. در دهه ۹۰ میلادی نسل دوم جرایم رایانه‌ای موسوم به جرایم علیه داده‌ها پا به عرصه وجود گذاشت. طی دوران اول و دوم، سازمان همکاری و توسعه اقتصادی جرم سایبری را به‌عنوان «هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار یا انتقال داده‌ها» معرفی نمود (سلیمی، ۱۳۹۳: ۲۵).

با ظهور و رواج اینترنت و پیدایش گونه‌های جدید جرم با ویژگی‌های کاملاً متفاوت با جرایم سابق، اعم از جرایم علیه داده یا سامانه و جرایم کلاسیک، در مفهوم و مصادیق جرایم مرتبط با رایانه یک دگردیسی اساسی صورت گرفت و سخن از جرمی با ویژگی‌های کاملاً متفاوت به میان آمد که می‌توان از آن به‌عنوان جرایم نسل سوم یاد کرد.

برخلاف جرایم نسل اول و دوم که افتراق آن‌ها در موضوع آن‌ها نسبت به جرایم کلاسیک، یعنی داده بود، جرایم نوین مرتبط با رایانه موضوع متفاوتی نسبت به جرایم کلاسیک نداشتند، بلکه روش و بستر ارتکاب آن‌ها متفاوت بود، زیرا این جرایم در سامانه‌های شبکه‌ای جهان‌گستر، یعنی در دنیای جدید اینترنت واقع می‌شود.

به این ترتیب، نسل سوم این جرایم، شامل بزه‌هایی می‌شود که فناوری‌های برخط نظیر اینترنت در آن‌ها نقش اصلی را بازی می‌کنند. از آنجا که ادبیات حقوقی و جرم‌شناختی مربوط به جرایم سایبری در ایران، برآمده از ترجمه پژوهش‌های گذشته و به‌ویژه کنوانسیون‌های جهانی و منطقه‌ای است، غالب مترجمان و پژوهشگران بدون توجه به دگردیسی‌های صورت‌گرفته در جرایم مرتبط با رایانه، تعریف صحیحی از جرایم سایبری ارائه نمی‌دهند و بین جرایم رایانه‌ای و جرایم سایبری در عمل تفاوتی قائل نمی‌شوند.

۱-۱- رویکرد مقنن ایرانی به جرایم سایبری

قانون‌گذار ایران در سردرگمی‌های آغازین مقابله با جرایم سایبری با اقتباس از کنوانسیون بوداپست که محصول سال ۲۰۰۱ و پیش از درک اهمیت کارکرد و خطر مضاعف سامانه‌های شبکه‌ای جهان گستر است، پنج دسته جرم را با عنوان «جرایم رایانه‌ای» شناسایی نموده است.

با مروری بر محتوای کنوانسیون مذکور و قانون جرایم رایانه‌ای مشخص می‌شود که جرم‌انگاری‌های صورت‌گرفته غالباً متوجه نسل اول و دوم این جرایم، یعنی جرایم رایانه‌ای می‌شود و جرایم سایبری یا اینترنتی علی‌رغم خطر مضاعف، کمتر مورد توجه قرار گرفته‌اند.

شاهد سخن آنکه ملاک و محور شناسایی جرم در کنوانسیون و قانون مذکور، موضوع این جرایم، یعنی «داده و سامانه» است و با همین ملاک تقریباً در اغلب مواد قانونی داده و سامانه به‌عنوان موضوع جرم مطرح شده‌اند و رفتار مجرمانه درصورتی‌که بر روی آن‌ها صورت گیرد، جرم محقق شده است.

تنها درخصوص برخی جرایم این قانون نظیر جرایم علیه عفت و اخلاق (مواد ۷۴۲ و ۷۴۳)، هتک حیثیت و نشر اکاذیب (۷۴۴، ۷۴۵ و ۷۴۶)، جرم کلاه‌برداری موضوع ماده ۷۴۱ جرم سایبری، یعنی جرمی که از طریق یا به‌وسیله سامانه‌های شبکه‌ای به‌هم‌پیوسته جهان‌گستر روی می‌دهد، مورد شناسایی قرار گرفته است.[۱]

---

[۱]- برای تفهیم بهتر موضوع مقایسه نص مواد ۷۴۰ و ۷۴۲ جالب توجه است، درحالی‌که ماده ۷۴۰ داده‌های رایانه‌ای را موضوع جرم معرفی نموده، ماده ۷۴۲ بر طریقیت سامانه‌های رایانه‌ای تأکید دارد. در هر حال امروزه این نقد جدی بر قانون مذکور وارد است که در اغلب مواد این قانون، از یک‌سو مقنن سیاست کیفری افتراقی را متوجه جرایمی ساخته که جز در موضوع جرم، یعنی آنچه جرم بر آن واقع می‌شود، تفاوتی با دیگر جرایم ندارند؛ به‌طور نمونه اگر موضوع تخریب داده یا سامانه باشد، مرتکب به‌جای ماده ۶۷۷ بخش تعزیرات به ماده ۷۳۶ قانون جرایم رایانه‌ای محکوم می‌گردد. از سوی دیگر قانون‌گذار از برخی جرایم کلاسیک که با ابزار اینترنت در فضاهای سایبر واقع می‌شوند و ویژگی‌های جرایم سایبری همچون گستردگی خسارت و سهولت ارتکاب و... را به‌همراه دارد، نظیر تروریسم سایبری، قمار و شرطبندی سایبری، پول‌شویی سایبری و ... نامی به میان نیاورده است و در سیاست کیفری تشدیدی ـ افتراقی، جایگاهی برای آن‌ها شناسایی ننموده است. منشأ این خطا به کنوانسیون جهانی جرایم سایبری بوداپست (۲۰۰۱) بازمی‌گرددکه قانون‌گذار ایرانی، حتی در بیان و دسته‌بندی نیز از آن تبعیت نموده است.

بنابر آنچه گفته شد، آنچه جرم سایبری یا اینترنتی را از جرایم رایانه‌ای و جرایم کلاسیک متمایز می‌سازد، روش ارتکاب و کاربست قابلیت‌های ارتباطاتی نوین برای انجام جرم و نه موضوع جرم است. به این ترتیب در تعریف جرم سایبری می‌توان گفت: «ارتکابِ فعل یا ترک فعلِ خلاف قانون، با به‌کارگیری سامانه‌ها و شبکه‌های ارتباطی و مخابراتی به‌هم‌پیوسته برخط جهان‌گسترِ که به‌موجب قانون برای آن مجازات تعیین شده باشد.»

ناگفته پیدا است که موضوع این رفتارهای مجرمانه، اعم از اشخاص حقیقی یا حقوقی، اشیا یا داده‌ها و سامانه‌ها است و به دسته‌ای خاص محدود نمی‌شود، لذا هم‌سو با نظر برخی صاحب‌نظران، بزهکاری سایبری از یک‌سو، شامل جرایم متعارفی مانند کلاه‌برداری، جاسوسی، افترا، هرزه‌نگاری، پولشویی و تروریسم که در فضای سایبر و به کمک فناوری‌های نوین اطلاعات و ارتباطات ارتکاب می‌یابند، می‌شود و از سوی دیگر به جرایمی اطلاق می‌شود که موضوع آن اقدام علیه امنیت سامانه‌ها، شبکه‌ها و داده‌های سایبری و انفورماتیکی است (ابرندآبادی، ۱۳۹۰: ۱۲-۱۱).

به این ترتیب برخلاف تصور غالب، همان‌گونه که می‌توان جرم کلاسیک سایبری نظیر قمار سایبری را تصور نمود، می‌توان جرم رایانه‌ای سایبری را نیز تصور کرد و منظور از آن جرمی است که علیه داده از طریق شبکه‌های ارتباطی به‌هم‌پیوسته روی دهد. به‌عنوان نمونه جرم موضوع ماده ۷۲۹ که علیه محرمانگی داده‌ها است، در مواردی که از طریق شبکه‌های ارتباطی به‌هم‌پیوسته محقق شود، مصداق جرم رایانه‌ای سایبری است. اگر این تلقی از جرایم سایبری پذیرفته شود، می‌توان ویژگی‌هایی مشترکی برای این جرایم برشمرد که به خطر مضاعف آن‌ها منجر شده است؛ در غیر این صورت سخن از ویژگی‌هایی خاص برای جرایم رایانه‌ای چندان با مسمی نخواهد بود.

۱-۲- رویکرد مقنن انگلیس به جرایم سایبری

جرایم تعریف‌شده در حقوق انگلیس جهت حمایت از محرمانگی، تمامیت و دسترس‌پذیری و سیستم‌ها یا داده‌های رایانه‌ای پیش‌بینی شده‌اند و فعالیت‌های مشروع و معمول طراحی شبکه‌ها یا فعالیت‌های تجاری را دربر نمی‌گیرند (میرزایی، ۱۳۹۷: ۲۳۱).

در حقوق انگلستان، «دسترسی غیرقانونی» شامل جرمی می‌شود که تهدیدهای خطرناک و تعرض‌ها علیه امنیت (یعنی محرمانگی، تمامیت و دسترس‌پذیری) سیستم‌ها و داده‌های رایانه‌ای را دربر می‌گیرد. نیاز به حفاظت، منافع سازمان‌ها و افراد در مدیریت، اجرا و کنترل سیستم‌هایشان را بدون وجود مزاحمت و ممانعت بازتاب می‌دهد. صرف تعرض غیرمجاز، یعنی «هک‌کردن»، «کرک‌کردن» یا «ورود به عنف رایانه»، اصولاً و فی‌نفسه باید غیرقانونی تلقی شود. این جرایم می‌توانند موانعی برای کاربران مشروع سیستم‌ها و داده‌ها ایجاد کنند و تغییرها یا تخریب‌هایی را با هزینه‌های زیاد بازسازی به‌وجود آورند. چنین تعرض‌هایی می‌تواند باعث دسترسی به داده‌های محرمانه (نظیر گذرواژه‌ها، اطلاعات راجع به سیستم‌های هدف) و اسرار برای استفاده از سیستم بدون پرداخت پول یا حتی تشویق نفوذگرها به ارتکاب اشکال خطرناک‌تری از جرایم مرتبط با رایانه، نظیر کلاه‌برداری یا جعل مرتبط با رایانه شود (قاسمی و باقرزاده، ۱۳۹۴: ۲۳۰).

«دسترسی» شامل ورود به تمام یا بخشی از سیستم رایانه‌ای می‌شود (سخت‌افزار، اجزای آن، داده‌های ذخیره در سیستم نصب‌شده، شاخه‌ها، داده‌های ترافیک و داده‌های مرتبط با محتوا). با این حال، صرف ارسال یک رایانامه و یا فایل به آن سیستم را دربر نمی‌گیرد. «دسترسی» شامل ورود به سیستم رایانامه‌ای دیگری به وسیله شبکه‌های مخابراتی عمومی یا ورود به سیستم رایانه‌ای همان شبکه است (عرب‌پور، ۱۳۹۰: ۲۸).

همچنین این عمل باید «بدون حق» انجام شود. به این معنا که دسترسی مجاز شمرده‌شده از سوی مالک یا ذی‌حق دیگر به سیستم یا بخشی از آن جرم محسوب نمی‌شود (مانند دسترسی با هدف ارزیابی مجاز یا حفاظت از سیستم رایانه‌ای مورد نظر)، به‌علاوه، دسترسی به سیستم رایانه‌ای که برای عموم آزاد و رایگان است نیز جرم نیست.

داشتن یک وب‌سایت عمومی، رضایت ضمنی دارنده را برای دسترسی هر کاربر وب نشان می‌دهد. به‌کارگیری ابزارهای استاندارد تهیه‌شده بر پایه پروتکل‌ها و برنامه‌های ارتباط مشترک، به‌خودی‌خود «بدون حق» نیست، به‌ویژه درجایی‌که فرض می‌شود صاحب حق سیستم دسترسی یافته، این‌گونه بهره‌برداری را پذیرفته و برای مثال نصب مقدماتی کوکی‌ها را رد و آن‌ها را پاک نکرده است (میرزایی، ۱۳۹۷: ۳-۲).

۲- سیاست جنایی ایران در پیشگیری از جرایم سایبری

۲-۱- سیاست جنایی تقنین ایران

به‌طور کلی، پیشگیری از جرم در ایران «اساسی‌سازی[۱]» شده است و مورد تصریح قانون اساسی گرفته است. علاوه‌بر این، قانون پیشگیری از جرم، نهایتاً در سال ۱۳۹۴ توسط مجمع تشخیص مصلحت نظام، با اصلاحات موافق مصلحت نظام دانسته شده است. در قوانین مختلف دیگر هم یا به پیشگیری از جرم تصریح شده است یا مقرره‌هایی به اصول، ضوابط و کیفیت برنامه‌های پیشگیری از جرم پرداخته‌اند. درخصوص پیشگیری از جرایم سایبری به‌طور مشخص، مقرره‌ها یا دستورالعمل‌های اندکی وجود دارد. به‌عنوان مثال صرفاً درخصوص موضوع فیلترینگ مواد ۷۴۹ تا ۷۵۱ قانون مجازات به این موضوع پرداخته است.

بنابر تصریح ماده ۷۴۹ فهرستی از سوی کمیته تعیین مصادیق محتوای مجرمانه، تعیین شده است. همچنین پلیس فتا در یک بخشنامه ۲۱ ماده‌ای به دفاتر خدمات اینترنت (کافی‌نت‌ها) وظایفی را محول نموده که بیشتر در راستای تدابیر نظارتی است که در عرصه پیشگیری وضعی و پالایش محتوا قابل بررسی است.

لازم است تأکید شود که درخصوص برخی از مصادیق جرایم سایبری و بسیاری از شیوه‌های جرم سایبری، اقدام پیشگیرانه خاصی اعم از وضعی یا پالایش محتوا یا اجتماعی یا ... انجام نمی‌شود.

۲-۲- برنامه‌های پیشگیری وضعی

برنامه‌های پیشگیری وضعی از جرایم سایبری یا ماهیتاً یک اقدام نظارتی یا محدودساز هستند و یا اقدامی هستند که با تقویت آماج از جرایم سایبری پیشگیری می‌نمایند. قطع نظر از درصد اندکی از کاربران یا شهروندان ایرانی فضای سایبر که برنامه‌های پیشگیری وضعی از جرم را به‌صورت فردی مورد توجه قرار می‌دهند و سالانه هزینه‌هایی برای این برنامه‌ها نظیر آنتی‌ویروس‌ها، برنامه‌های فیلترینگ کودک و ... پرداخت می‌کنند، غالباً پیشگیری از جرم سایبری در ایران یک وظیفه دولتی تلقی می‌شود.

قطع نظر از اقداماتی که توسط کاربران انجام می‌شود پالایش محتوا/ فیلترینگ، استفاده الزام به ثبت کانال‌ها و گروه‌های شبکه‌های اجتماعی، استفاده از نرم‌افزار ضد پول‌شویی (aml)، الزام کافی‌نت‌ها به ثبت هویت مشتریان، گشت سایبری و دام‌گستری سایبری، مهم‌ترین اقداماتی است که توسط دولت در راستای پیشگیری از جرم سایبری انجامی شود.

در میان تمام گزینه‌های ممکن برای پیشگیری وضعی از جرم سایبری، فیلترینگ یا پالایش محتوا و تدابیر نظارتی، بیشترین کاربرد را در ایران دارند. واقعیت آن است که حجم سرمایه‌گذاری و تمرکزی که بر برنامه‌های پیشگیری وضعی از جرم سایبری به‌ویژه تدبیر فیلترینگ می‌شود، با مجموع روش‌های دیگر قابل مقایسه نیست. در ادامه به‌ترتیب پالایش محتوا و تدابیر نظارتی به‌صورت جداگانه مورد بررسی قرار می‌گیرد.

۲-۲-۱- پالایش محتوا

پالایش محتوا در زمره معدود برنامه‌های پیشگیری از جرایم سایبری است که مقنن درصدد برآمده تا شیوه و کیفیت اجرای آن را مشخص سازد. در ایران، اِعمال فیلترینگ یا پالایش محتوا معمولاً به‌وسیله ارائه‌دهندگان خدمات دسترسی و میزبانی در اینترنت انجام می‌شود، ولی تعیین سطح، مصادیق و سیاست‌های فیلترینگ با کمیته تعیین مصادیق

---

[۱]- اساسی‌سازی یا اساسی‌گرایی حقوق، یک جنبش حقوقی است که از سده هجدهم میلادی به‌صورت نظام‌یافته و برای صیانت از حق‌ها و آزادی‌های بنیادین شهروندان در برابر قدرت عمومی وارد گستره حقوق شده است تا به هنجارهای عادی ارزش و اعتبار هنجار اساسی داده شود (گرجی، ۱۳۹۳: ۹۸۸). همچنین واردشدن یک مقوله حقوقی یا گونه‌ای از حقوق و آزادی‌های شهروندان در پهنه قانون اساسی، آن پدیده حقوقی را اساسی می‌کند (تقی‌زاده، ۱۳۸۶: ۱۳۰).

محتوای مجرمانه است. مستند قانونی پالایش فضای مجازی در ایران مواد ۷۴۹، ۷۵۰ و ۷۵۱ از قانون مجازات اسلامی بخش جرایم رایانه‌ای است.

مطابق با ماده ۷۵۱ از قانون مذکور، کارگروه تعیین محتوای مصادیق مجرمانه که دارای ۱۲ عضو حقیقی و حقوقی بوده و با حضور حداقل ۷ عضو رسمیت می‌یابد، به ریاست دادستان کل کشور تشکیل جلسه می‌دهد. این کارگروه دو دسته از محتواهای ناشی از جرایم رایانه‌ای و محتواهایی که برای جرایم رایانه‌ای به‌کار می‌روند را شناسایی می‌نماید.

ماده ۷۴۹ ارائه‌دهندگان خدمات دسترسی و ماده ۷۵۱ ارائه‌دهندگان خدمات میزبانی را به‌عنوان متصدیان اجرایی اِعمال فیلترینگ معرفی می‌نماید که موظف‌اند فهرستی را که توسط کارگروه تعیین مصادیق محتوای مجرمانه تهیه می‌شود، پالایش نمایند. به این ترتیب قانون‌گذار درصدد است که اولاً با سلب دسترسی و ثانیاً با سلب میزبانی، پالایش فضای مجازی را به‌طور کامل محقق سازد.

مطابق با تبصره ۲ از ماده ۷۵۱ شکایت و اعتراض نسبت به مصادیق پالایش‌شده توسط کارگروه مذکور رسیدگی می‌شود. همچنین مطابق با تبصره ۲ از ماده ۷۴۹ برخی پالایش‌های موردی که در راستای حمایت از شاکی خصوصی صورت می‌گیرد، به دستور مقام قضایی رسیدگی‌کننده به پرونده و پس از احراز مجرمیت یا حداقل محکومیت (اعم از حقوقی یا جزایی) صورت می‌گیرد.

درخصوص شیوه‌های پالایش محتوا در فضای مجازی به‌طور کلی در ایران چند شیوه خاص برای پالایش محتوای فضای مجازی به‌کار گرفته شده است:

در روش اول، فیلترینگ از طریق آدرس آی‌پی انجام می‌شود. در این روش آدرس آی‌پی چهار بخشی مربوط به سروری که سایت ممنوعه در آن قرار دارد، فیلتر می‌شود. اشکال اصلی این روش این است که اکثر سایت‌های اینترنتی از سرویس میزبانی اشتراکی استفاده می‌کنند. در این حالت اگر هزار سایت روی یک سرور قرار داشته باشند و فقط یک سایت جزء سایت‌های ممنوعه باشد با فیلترشدن آی‌پی دسترسی به هر هزار سایت غیرممکن خواهد بود. این روش در سال‌های اول فیلترینگ در ایران، انجام می‌شد و به‌جهت مکانیسم خود بعضاً موجب فیلترشدن صفحه‌های دولتی نیز شده است؛ باتوجه به درصد خطای بالای آن و اعتراضات فراوان کارشناسان و کاربران متوقف شده است.

روش دوم، فیلترینگ از طریق فهرست سیاه است. فیلترینگ مرکزی که هم‌اکنون در ایران استفاده می‌شود، از نوع فیلترینگ فهرست سیاه است. در فیلترینگ براساس فهرست سیاه، یک فهرست از آدرس‌هایی وجود دارد که شامل نشانی وبگاه‌هایی که دسترسی به آن‌ها مجاز نیست، می‌شود.

در روش سوم که فیلترینگ از طریق کلیدواژه‌ها است، فهرستی از کلمات کلیدی ممنوعه تهیه می‌شود و شناسایی کلیدواژه‌های مجرمانه به‌وسیله نرم‌افزارهای فیلترینگ انجام می‌شود. نرم‌افزار فیلترینگ بر این اساس عمل می‌کند که اگر کلمه ممنوعه در آدرس لینک صفحه درخواستی کاربر باشد یا توسط کاربر در موتورهای جستجو وارد شود، با پیغام خطا مواجه می‌شود.

۲-۲-۲- تدابیر نظارتی

تدابیر نظارتی، به‌معنای کلیه اقدامات پایشی و مراقبتی است که با هدف ایجاد امنیت در فضاهای سایبر انجام می‌شود. این اقدامات به دو دسته تدابیر نظارتی فعال و تدابیر نظارتی منفعل قابل تقسیم است. در تدابیر نظارتی فعال، مأموران کشف جرم با سلسله اقداماتی در قالب عملیات‌های پلیسی که اصطلاحاً دام‌گستری نامیده می‌شود، اقدام به پیشگیری از جرم و کشف جرم می‌نمایند.

در تدابیر نظارتی منفعل، مأموران و متصدیان پیشگیری، با اقدامات پایشی در جهت کشف و شناسایی به هنگامِ جرم تلاش می‌کنند. مهم‌ترین این اقدامات شامل گشت‌های پلیسی در فضای سایبر نظیر چت‌روم‌ها و شبکه‌های اجتماعی، نظارت‌های متصدیان بانک‌ها برای پیشگیری از پول‌شویی سایبری و مراقبت‌های متصدیان کافی‌نت‌ها و مراکز عمومی می‌شود.

بخشنامه پلیس فتا به کافی‌نت‌ها را می‌توان ازجمله تدابیر نظارتی به‌شمار آورد. مواد ۸، ۱۱ و ۱۷ این بخشنامه ارتباط بیشتری با تدابیر نظارتی پیشگیری از جرم دارند. ماده ۸ این بخشنامه مقرر می‌دارد: «**دفاتر خدمات اینترنت موظفند اطلاعات هویتی کاربران را با دریافت مدارک شناسایی معتبر (ترجیحاً کارت ملی) ثبت و از ارائه خدمات به مراجعه‌کنندگانی که مدارک شناسایی ارائه نمی‌کنند، خودداری کنند.**» ماده ۱۰ مقرر می‌دارد: «**دفتر خدمات اینترنت موظفند علاوه‌بر اطلاعات هویتی کاربران، سایر اطلاعات کاربری شامل روز و ساعت استفاده، آی‌پی اختصاص‌یافته و فایل لاگ وبسایت‌ها و صفحات رؤیت‌شده را ثبت و حداقل تا شش‌ماه نگهداری کنند.**» ماده ۱۷ هم نصب دوربین مداربسته داخلی با قابلیت ضبط تمام وقت، نگهداری تصاویر و امکان بازبینی تا شش‌ماه را الزامی می‌نماید.

۳- سیاست جنایی انگلستان در پیشگیری از جرایم سایبری

توسعه اینترنت و فناوری‌های دیجیتال در انگلستان دنیای تجارت را در این کشور متحول کرده و ابزارهای جدیدی برای ارتباطات روزمره پیشنهاد کرده است. فعالیت‌های اینترنتی و آنلاین در حال حاضر به یکی از ارکان اساسی زندگی روزمره مردم در انگلستان تبدیل شده است. با این حال، اینترنت فرصتی نیز در اختیار مجرمان اینترنتی قرار می‌دهد. ماهیت برخی از انواع سنتی جرم و جنایت با استفاده از رایانه و دیگر فناوری‌های ارتباطی اطلاعات دگرگون شده است و تبعاتی را برای جنبه‌های مختلف زندگی اجتماعی به‌همراه داشته است.

با توسعه اینترنت و دسترسی به آن، اشکال جدیدی از فعالیت‌های مجرمانه، ازجمله هدف قراردادن امنیت رایانه‌ها و شبکه‌های کامپیوتری از طریق گسترش نرم‌افزارهای مخرب و هک‌کردن نیز پدید آمدند. تهدیدهای مذکور نه‌تنها افراد و کسب و کار، بلکه امنیت و زیرساخت‌های ملی را نیز تهدید کرده است.

تحولات سیاست پیشگیری از جرم در انگلیس به بهترین شکل در مقاله **دنیل گیلینگ** با عنوان «پیشگیری از جرم چندنهادی در بریتانیا: مشکل ترکیب راهبردهای وضعی و اجتماعی» ارائه شده است. **گیلینگ** در این مقاله بر این بحث تأکید دارد که «سیاست پیشگیری از جرم بین دهه ۱۹۵۰ و ۱۹۹۰ در راهبرد مرکزی سیاست پیشگیری از وقوع جرم شکل گرفت که در آن حمایت احزاب پارلمان بریتانیا مشهود بود» (Gilling, 2000: 25).

در امر پیشگیری از جرم و بالاخص پیشگیری از جرایم سایبری، چند سند قانونی در انگلستان قابل بررسی است. یکی از آن‌ها گزارش مجلس عوام با موضوع «روش دولت در مبارزه با جرم و جنایت» در سال ۱۰-۲۰۰۹ می‌باشد که روند پیشرفت در کاهش جرم را مطرح می‌نماید. دولت **دیوید کامرون**، در ده‌سال اول پیشرفت مطلوبی در عرصه‌های مختلف پیشگیری از جرم داشته است. سند دیگر که در ماه مارس سال ۲۰۱۳ به تأیید سلطنت بریتانیا رسید، «قانون رفتار ضداجتماعی، جرم و حفاظت» است. این قانون قدرت‌های مؤثر در مبارزه با رفتار ضداجتماعی و حفاظت بیشتر از بزه‌دیدگان و جوامع را معرفی می‌کند (Home Office, 2013).

در زمینه مبارزه با جرایم سایبری، «استراتژی جرایم سایبری» سندی است که روشی منسجم در مبارزه با تهدیدات اینترنتی و تکنولوژی مربوطه را مطرح می‌نماید. یکی از بخش‌های مهم این استراتژی «راهبرد توسعه دستیابی» است که به مبارزه با جرایم جدی سازمان‌یافته‌ای مانند جرایم مرتبط با فضای سایبری پرداخته است.

استراتژی امنیت ملی انگلستان، تهدیدهای سایبری را «تهدید درجه یک» برای امنیت ملی و هم ردیف با تروریسم بین‌المللی به‌حساب می‌آورد و بیشترین اولویت را در پیگیری به آن اختصاص داده است. به همین منظور، آژانس ملی جرم (NCA) در سال ۲۰۱۳ با راه‌اندازی واحد ملی جنایت سایبری (NCCU) به اجرای قوانین تخصصی به‌منظور بررسی برخی از جدی‌ترین اشکال جرایم اینترنتی پرداخته است. استراتژی جدید جرایم جدی و سازمان‌یافته، در کنار راه‌اندازی NC، چهارچوب و روش مقابله که شامل جرایم اینترنتی می‌شود را معرفی کرد.

در انگلستان آنچه خارج از فضای اینترنت غیرقانونی می‌باشد، در فضای سایبری هم غیرقانونی تلقی می‌شود. جرایم خاص

که معمولاً با جرایم سایبری همراه هستند، مانند هک‌کردن و ایجاد یا توزیع نرم‌افزارهای مخرب که در قانون سوءاستفاده از کامپیوتر در سال ۱۹۹۰ و جرم سایبری تعریف شده است، اصطلاحی جامع می‌باشد که دو جرم مجزا، اما کامل را شرح می‌دهد: ۱- جرایم وابسته به اینترنت؛ ۲- جرایم از طریق اینترنت (Cabinet Office, 2009).

جرایم وابسته به اینترنت، جرایمی هستند که ارتکاب آنان تنها با استفاده از یک کامپیوتر، شبکه‌های کامپیوتری و یا شکل دیگری از ICT امکان‌پذیر است. این اعمال عبارت‌اند از گسترش ویروس و دیگر برنامه‌های مخرب، هک و حملات لغو سرویس گسترده (DDoS)، مانند حمله اطلاعاتی به سرویس‌دهنده‌های اینترنت جهت مختل‌کردن زیرساخت‌های شبکه و یا وب‌سایت‌ها.

جرایم وابسته به اینترنت در درجه اول فعالیت‌هایی را دربر می‌گیرند که علیه کامپیوترها و یا منابع شبکه صورت می‌گیرند، اگرچه ممکن است نتایج ثانویه مانند کلاه‌برداری را نیز در پی داشته باشند.

جرایم از طریق اینترنت دسته‌ای از جرایم سنتی می‌باشند که مقیاس و بُردشان با استفاده از کامپیوتر، شبکه‌های کامپیوتری و یا سایر ICT افزایش می‌یابند. برخلاف جرایم وابسته به اینترنت، این گروه از جرایم بدون استفاده از ICT هم روی می‌دهند. جهت روشن‌شدن منظور و هدف در اینجا سه نوع از آن‌ها معرفی می‌شوند:

۱- کلاه‌برداری، ازجمله کلاه‌برداری‌های انبوه در سطح بازار، ایمیل‌های فیشینگ و دیگر تقلب‌های ایمیلی، کلاهبرداری‌های بانکداری آنلاین و تجارت الکترونیکی؛ ۲- سرقت، شامل سرقت اطلاعات شخصی و داده‌های شناسایی؛ ۳- تخلفات جنسی علیه کودکان، ازجمله گرومینگ و در اختیارداشتن، ایجاد و/یا توزیع تصاویر جنسی (McGuire & Dowling, 2013: 23).

اقدامات دولت انگلستان جهت پیشگیری از جرایم سایبری و ایجاد شرایطی امن‌تر در تجارت، از قرار زیر است:

– راه‌اندازی واحد ملی جرایم سایبری در سازمان ملی جرم و جنایت در سال ۲۰۱۳ که واحد پلیس سایبری و آژانس جرایم پراهمیت سازمان‌یافته (SOCA) را ادغام نموده است.

– ارائه مشاوره امنیت سایبری به شرکت‌های تجاری ازقبیل انتشار کتابچه «۱۰ قدم به سوی امنیت سایبری» و «راهنمای مناسب شرکت‌های کوچک».

– برقراری همکاری با شرکت‌های تجاری از طریق امنیت سایبری اشتراک اطلاعات که به دولت و صنعت اجازه می‌دهد تا در یک فضای مطمئن به تبادل اطلاعات در مورد تهدیدات اینترنتی بپردازند.

– توافق با صنعت در مورد اصول هدایت‌کننده ارائه‌دهندگان خدمات اینترنت، تعیین بهترین روش کمک به اطلاع‌رسانی، آموزش و حمایت از مشتریان در مقابل تهدیدات آنلاین.

– توسعه یک استاندارد سازمانی ارجح برای امنیت سایبری، تا از طریق آن چهارچوب روشنی برای مقابله با خطرات امنیت سایبری در اختیار صنعت قرار گیرد.

– معرفی یک سیستم گزارش‌دهی مجزا برای مردم تا از آن طریق بتوانند جرایم اینترنتی با انگیزه‌های مالی (تحت قانون تخلف و کلاه‌برداری) را گزارش دهند. در این راستا مرکز شبانه‌روزی گزارش جرایم سایبری بریتانیا به ضبط تقلبات پرداخته، اشتراک و تحلیل اطلاعات مربوط به جرایم سایبری را میسر ساخته و عملیات اجرایی در پیشگیری را هدفمندتر می‌سازد (McGuire & Dowling, 2013: 23).

نتیجه‌گیری

فناوری اطلاعات و ارتباطات که در ابتدا برای آسایش و رفاه هرچه بیشتر انسان‌ها مورد بهره‌برداری قرار می‌گرفت، به‌تدریج به ابزاری برای مجرمان، جهت نیل به آمال مجرمانه تبدیل شد. این فضای جدید به‌گونه‌ای حقوق جزای سنتی را دستخوش تحولات بنیادین کرده است که تعریف از جرایم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری از موارد متفاوت است. وابستگیِ فزاینده جامعه به فناوری‌های اطلاعاتی و ارتباطی و ناتوانی دولت‌ها در تعقیب و شناسایی بزهکاران این جرایم، دولت‌ها را به

کاربست تدابیر و برنامه‌های پیشگیرانه واداشته است. نتیجه حاصل از این پژوهش آن است که در ایران و انگلستان، سیاست جنایی در پیشگیری از جرایم سایبری غالباً متمرکز در سیاست جنایی تقنینی بوده و تدابیر پیشگیرانه، عمدتاً ناظر بر پیشگیری وضعی از این جرایم است.

ملاحظات اخلاقی: در این پژوهش، تمامی ملاحظات اخلاقی رعایت شده است.

تعارض منافع: نگارش این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: در این پژوهش، نویسندگان مشترکاً اقدام نموده‌اند.

تشکر و قدردانی: لازم است از تمامی کسانی که در تدوین این مقاله، ما را یاری رسانده‌اند، قدردانی نماییم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین مالی انجام گرفته است.

منابع و مآخذ

الف. منابع فارسی و عربی

– ابراهیمی، شهرام (۱۳۹۱). *جرم‌شناسی پیشگیری*. جلد اول، تهران: نشر میزان.

– تقی‌زاده، جواد (۱۳۸۶). «مسأله اساسی‌سازی نظم حقوقی». *مجله پژوهش‌های حقوقی*، ۱۱: ۱۲۹–۱۶۲.

– جوان جعفری، عبدالرضا و سیدزاده ثانی، سید مهدی (۱۳۹۱). *رهنمودهای علمی پیشگیری از جرم*. تهران: نشر میزان.

– سلیمی، احسان (۱۳۹۳). *بزه‌دیدگی زنان در فضای سایبر*. پایان‌نامه کارشناسی ارشد، به راهنمایی محمدجواد فتحی، قم: پردیس دانشگاه تهران.

– عرب‌پور، حمزه (۱۳۹۰). *جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای در نظام حقوقی ایران و اسناد بین‌المللی*. پایان‌نامه کارشناسی ارشد، اصفهان: دانشگاه اصفهان.

– قاسمی، غلامعلی و باقرزاده، سجاد (۱۳۹۴). «جایگاه حقوق بشر در مبارزه با سایبرتروریسم». *مجله حقوقی بین‌المللی*، ۳۲(۵۲): ۲۲۷–۲۵۴.

– گرجی، علی‌اکبر (۱۳۹۳). *در تکاپوی حقوق عمومی*. تهران: انتشارات جنگل.

– میرزایی، مریم (۱۳۹۷). «بررسی جرایم منافی عفت سایبری در حقوق انگلستان». *پژوهش‌های حقوقی قانون یار*، ۱(۳): ۲۲۹–۲۵۰.

– نجفی ابرندآبادی، علی‌حسین (۱۳۹۰). *از جرم‌شناسی حقیقی تا جرم‌شناسی مجازی*. تهران: انتشارات میزان.

ب. منابع انگلیسی

- Cabinet Office (2009). *Cyber Security Strategy of the United Kingdom*

- Gilling, D (2000). "Multi-Agency Crime Prevention in Britain: The Problem of Combinig Situational and Social Strategies". *Applied Social Studies*, 231-248.

- Home Office (2013). *Anti-social Behaviour, Crime and Policing Act*. Retrieved from GOV.UK: https://www.gov.uk/government/collections/anti-social-behaviour-crime-and-police-bill

- McGuire, M & Dowling, S (2013). *Cyber crime: A review of the evidence*. London: Home Office.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf