Insights of Intellectual Property Law in Islamic Countries
Online ISSN: 3060-5997
https://diplic.qom.ac.ir

Implementation of Situational Crime Prevention Against Cyber Fraud in Iranian Law: A Comparative Study with English Law Based on Clarke's Situational Crime Prevention Model

Adnan Omrani Far [1], **Ruhollah Amiri** [2]

1. Ph.D. Graduate in Criminal Law and Criminology, University of Tehran, Tehran, Iran (Corresponding Author), Email: omrani.far@ut.ac.ir
2. Faculty Member, Department of Criminal Law and Criminology, Payame Noor University, Lorestan Province, Iran, dr.alicrime@gmail.com Email:

Abstract

Received: 19/05/2026
Revised: 01/08/2026
Accepted: 25/08/2026
Published online: 23/09/2026

Cyber fraud has emerged as one of the most sophisticated and rapidly evolving forms of cybercrime, posing significant threats to economic security, public trust, and the integrity of electronic transactions. The distinctive characteristics of cyber fraud including its transnational nature, offender anonymity, rapid execution, and constantly evolving methods have diminished the effectiveness of traditional punitive criminal justice responses. Consequently, preventive approaches, particularly situational crime prevention, have become increasingly important in contemporary criminal policy. This study adopts a descriptive-analytical methodology combined with a comparative legal approach to examine the implementation of situational crime prevention strategies against cyber fraud in the Iranian legal system, with reference to English law. The findings reveal that Ronald Clarke's situational crime prevention model, comprising five principal strategies—increasing the effort required to commit crime, increasing the risks of detection, reducing the rewards of offending, reducing provocations, and removing excuses for criminal conduct—offers an effective framework for limiting criminal opportunities in cyberspace. Although Iranian legislation has taken important steps toward enhancing cybersecurity and combating cybercrime, the effectiveness of these measures remains constrained by fragmented preventive policies, inadequate public awareness, insufficient institutional coordination, and limited cooperation with the private sector. By contrast, the English legal framework demonstrates that integrating legal, technological, educational, and collaborative measures significantly strengthens the prevention of cyber fraud. The study concludes that reinforcing preventive criminal policy through the systematic implementation of situational crime prevention strategies can substantially improve cybersecurity, reduce cyber victimization, and enhance public confidence in digital services within the Iranian legal system.

Keywords: Cyber Fraud; Situational Crime Prevention; Criminal Policy; Iranian Law; English Law; Ronald Clarke's Model.

How To Cite: Omrani Far,A. & Amiri, R (2026). Implementation of Situational Crime Prevention Against Cyber Fraud in Iranian Law: A Comparative Study with English Law Based on Clarke's Situational Crime Prevention Model, *Insights of Intellectual Property Law in Islamic Countries*, 2(3), 80-105. https://www.doi.org/10.22091/diplic.2026.16970.1055

Published by: University of Qom **© The Author(s)** **Article type: Research**

آموزه‌های حقوق مالکیت فکری کشورهای اسلامی
https://diplic.qom.ac.ir
شاپا الکترونیکی: ۳۰۶۰-۵۹۹۷

پیاده‌سازیِ پیشگیری وضعی در قبال کلاهبرداری سایبری در حقوق ایران با نگاهی به حقوق انگلستان (با تکیه بر اُلگوی کلارک)

عدنان عمرانی فر[۱]، روح الله امیری[۲]

۱. دانش‌آموخته دکتری تخصصی حقوق کیفری و جرم‌شناسی، دانشگاه تهران، تهران، ایران (نویسنده مسئول)، رایانامه: omrani.far@ut.ac.ir
۲. روح‌الله امیری عضو هیئت علمی، گروه حقوق کیفری و جرم‌شناسی، دانشگاه پیام نور، استان لرستان، ایران. رایانامه: dr.alicrime@gmail.com
۳.

چکیده

کلاهبرداری سایبری به‌عنوان یکی از پیچیده‌ترین و پرشتاب‌ترین اشکال جرائم نوظهور، با بهره‌گیری از فناوری‌های اطلاعاتی و ارتباطی، امنیت اقتصادی، اعتماد عمومی و سلامت مبادلات الکترونیکی را با چالش‌های جدی مواجه ساخته است. واکنش صرف کیفری در برابر این دسته از جرائم به دلیل ویژگی‌هایی نظیر فراملی بودن، ناشناس بودن مرتکبان، سرعت ارتکاب و تحول مداوم شیوه‌های مجرمانه، از کارآمدی کافی برخوردار نیست؛ ازاین‌رو، بهره‌گیری از رویکردهایِ پیشگیرانه به‌ویژه پیشگیری وضعی، ضرورتی اجتناب‌ناپذیر محسوب می‌شود. پژوهش حاضر با روش توصیفی‌تحلیلی و با رویکرد تطبیقی به بررسی نحوه پیاده‌سازی راهبردهای پیشگیری وضعی از کلاهبرداری سایبری در حقوق ایران با نگاهی به حقوق انگلستان پرداخته است. یافته‌های پژوهش نشان می‌دهد که الگوی پنج‌گانه رونالد کلارک شامل افزایش دشواری ارتکاب جرم، افزایش خطر شناسایی، کاهش منافع حاصل از جرم، کاهش عوامل تحریک‌کننده و حذف بهانه‌های ارتکاب، ظرفیت بالایی برای کنترل فرصت‌های مجرمانه در فضای سایبری دارد. هرچند قوانین ایران در سال‌های اخیر گام‌هایی در جهت حمایت از امنیت سایبری و مقابله با جرائم رایانه‌ای برداشته‌اند، اما ضعف در اجرای منسجم سیاست‌های پیشگیرانه، کمبود آموزش عمومی، فقدان مشارکت مؤثر بخش خصوصی و نبود هماهنگی نهادی، اثربخشی این تدابیر را محدود ساخته است. در مقابل تجربه حقوق انگلستان بیانگر آن است که تلفیق اقدامات حقوقی، فنی، آموزشی و مشارکتی نقش مهمی در کاهش فرصت‌های ارتکاب کلاهبرداری سایبری ایفا کرده است. ازاین‌رو، تقویت سیاست جنایی پیشگیرانه و بهره‌گیری از الگوی پیشگیری وضعی می‌تواند زمینه ارتقای امنیت فضای سایبری و کاهش بزه‌دیدگی در نظام حقوقی ایران را فراهم آورد.

واژگان کلیدی: کلاهبرداری سایبری، پیشگیری وضعی، سیاست جنایی، حقوق انگلستان، الگوی کلارک.

تاریخ دریافت: ۱۴۰۵/۰۲/۲۹
تاریخ اصلاح: ۱۴۰۵/۰۵/۱۰
تاریخ پذیرش: ۱۴۰۵/۰۶/۰۳
تاریخ انتشار برخط: ۱۴۰۵/۰۷/۰۱

استناد: عمرانی فر، عدنان و امیری، روح‌الله (۱۴۰۵). پیاده‌سازی پیشگیری وضعی در قبال کلاهبرداری سایبری در حقوق ایران با نگاهی به حقوق انگلستان (با تکیه بر اُلگوی کلارک)، آموزه‌های حقوق مالکیت فکری کشورهای اسلامی، ۲(۳)، ۱۰۵-۸۰.
https://www.doi.org/10.22091/diplic.2026.16970.1055

ناشر: دانشگاه قم © **نویسندگان** **نوع مقاله: پژوهشی**

مقدمه

گسترش فناوری اطلاعات و ارتباطات، توسعه خدمات الکترونیکی، بانکداری دیجیتال، تجارت الکترونیکی و شبکه‌های اجتماعی، ضمن ایجاد فرصت‌های گسترده برای رشد اقتصادی و تسهیل تعاملات اجتماعی زمینه ظهور گونه‌های جدیدی از بزهکاری را نیز فراهم ساخته است. در میان این جرائم، کلاهبرداری سایبری به دلیل اتکای گسترده به فناوری، قابلیت ارتکاب در مقیاس وسیع، سرعت بالا، فراملی بودن و دشواری شناسایی مرتکبان، به یکی از مهم‌ترین تهدیدهای امنیت اقتصادی و اجتماعی دولت‌ها تبدیل شده است. امروزه مجرمان سایبری با بهره‌گیری از روش‌هایی نظیر فیشینگ، جعل هویت دیجیتال، ایجاد درگاه‌های پرداخت جعلی، مهندسی اجتماعی، بدافزارها و سوءاستفاده از اطلاعات شخصی، خسارات مالی و روانی گسترده‌ای به اشخاص حقیقی، شرکت‌ها و نهادهای عمومی وارد می‌کنند. این وضعیت نشان می‌دهد که مقابله با کلاهبرداری سایبری صرفاً از طریق پاسخ‌های کیفری سنتی امکان‌پذیر نیست و اتخاذ سیاست‌های پیشگیرانه، به‌ویژه پیشگیری وضعی، ضرورتی انکارناپذیر یافته است.

پیشگیری وضعی که بر مبنای نظریه انتخاب عقلانی و کنترل فرصت‌های مجرمانه شکل گرفته، بر آن است که با تغییر شرایط محیطی، افزایش هزینه ارتکاب جرم، کاهش منافع مورد انتظار، افزایش احتمال شناسایی و حذف زمینه‌های مساعد ارتکاب، فرصت وقوع جرم را کاهش دهد. در این رویکرد به جای تمرکز صرف بر شخصیت بزهکار، محیط ارتکاب جرم و عوامل تسهیل‌کننده آن مورد توجه قرار می‌گیرد. ازاین‌رو، طراحی سامانه‌های ایمن، تقویت احراز هویت کاربران، توسعه نظارت هوشمند، آموزش عمومی، ارتقای سواد دیجیتال و مشارکت فعال نهادهای دولتی و خصوصی، از مهم‌ترین ابزارهای تحقق پیشگیری وضعی در فضای سایبری محسوب می‌شوند.

در نظام حقوقی ایران قانون جرائم رایانه‌ای و قانون تجارت الکترونیکی و سایر مقررات مرتبط چارچوب‌هایی برای مقابله با جرائم سایبری ایجاد کرده‌اند، اما بخش عمده سیاست جنایی همچنان بر واکنش کیفری پس از وقوع جرم متمرکز است. در مقابل، تجربه حقوق انگلستان نشان می‌دهد که اتخاذ سیاست‌های جامع پیشگیرانه، همراه با بهره‌گیری از فناوری‌های نوین، آموزش مستمر شهروندان، همکاری مؤسسات مالی، شرکت‌های فناوری، پلیس تخصصی و نهادهای امنیت سایبری، توانسته است نقش مؤثری در کاهش میزان موفقیت کلاهبرداری‌های سایبری ایفا کند. ازاین‌رو، مطالعه تطبیقی این دو نظام حقوقی می‌تواند ظرفیت‌ها و کاستی‌های موجود را آشکار ساخته و زمینه بهره‌گیری از تجارب موفق را فراهم آورد.

مسئله اصلی این پژوهش آن است که راهبردهای پیشگیری وضعی تا چه اندازه قابلیت پیاده‌سازی در نظام حقوقی ایران را دارند و تجربه حقوق انگلستان چه آموزه‌هایی برای ارتقای سیاست جنایی ایران درزمینهٔ مقابله با کلاهبرداری سایبری ارائه می‌دهد؟ فرضیه تحقیق بر این مبنا استوار است که اجرای هماهنگ راهبردهای پنج‌گانه پیشگیری وضعی، همراه با توسعه همکاری میان نهادهای دولتی، بخش خصوصی و کاربران، می‌تواند به‌طور معناداری فرصت‌های ارتکاب کلاهبرداری سایبری را کاهش دهد و کارآمدی سیاست جنایی ایران را افزایش بخشد.

پژوهش حاضر با روش توصیفی‌تحلیلی و بهره‌گیری از منابع کتابخانه‌ای، قوانین، اسناد، دکترین حقوقی و مطالعات تطبیقی انجام شده است. نوآوری پژوهش در آن است که الگوی پنج‌گانه پیشگیری وضعی کلارک را به‌صورت منسجم در حوزه کلاهبرداری سایبری تحلیل کرده و ضمن مقایسه تطبیقی حقوق ایران و انگلستان، راهکارهایی عملی برای تقویت سیاست جنایی پیشگیرانه ارائه می‌دهد. نتایج این پژوهش می‌تواند برای قانون‌گذار، قوه قضائیه، پلیس فتا، بانک‌ها، شرکت‌های فناوری، ارائه‌دهندگان خدمات دیجیتال و سایر نهادهای مسئول در حوزه امنیت سایبری، مبنایی مناسب برای اصلاح سیاست‌های پیشگیرانه و کاهش مخاطرات ناشی از کلاهبرداری سایبری فراهم آورد.

۱. پیشینه پژوهش

بررسی پیشینه پژوهش نشان می‌دهد که مطالعات انجام‌شده درباره کلاهبرداری رایانه‌ای و سایبری در حقوق ایران و انگلستان، عمدتاً بر ابعاد کیفری، جرم‌انگاری و عناصر تشکیل دهنده جرم متمرکز بوده‌اند و کمتر به پیشگیری وضعی به‌عنوان راهبردی مؤثر در کنترل فرصت‌های مجرمانه پرداخته‌اند. ازاین‌رو، هرچند این پژوهش‌ها در تبیین ماهیت حقوقی جرم و تحلیل واکنش کیفری ارزشمند هستند، اما در ارائه الگوی عملی برای پیشگیری از وقوع کلاهبرداری سایبری با محدودیت مواجه‌اند.

در این زمینه، هادی‌تبار و رضایی (۱۳۹۴) با مطالعه تطبیقی حقوق ایران و انگلستان، به بررسی جرم‌انگاری کلاهبرداری اینترنتی و تحولات قانون‌گذاری در دو نظام حقوقی پرداخته‌اند. نتایج پژوهش آنان نشان می‌دهد که گسترش فناوری اطلاعات موجب پیچیده‌تر شدن شیوه‌های ارتکاب جرم و ضرورت بازنگری در قوانین کیفری شده است. با وجود این، تمرکز پژوهش بر سیاست کیفری واکنشی بوده و نقش تدابیر پیشگیرانه، به‌ویژه پیشگیری وضعی مورد توجه قرار نگرفته است.

همچنین نجفی توانا و کریمی در پژوهش خود با عنوان «سیاست پیشگیری و مبارزه با جرم کلاهبرداری

اینترنتی»، سیاست‌های تقنینی، قضایی، اجرایی و مشارکتی را بررسی کرده‌اند. اگرچه این پژوهش نسبت به مطالعات پیشین نگاه جامع‌تری به پیشگیری دارد، اما چارچوب نظری مشخصی برای تحلیل اقدامات پیشگیرانه ارائه نکرده و به ظرفیت الگوهای جرم‌شناختی، ازجمله الگوی پیشگیری وضعی رونالد کلارک، نپرداخته است. افزون بر آن، مطالعه تطبیقی با نظام‌های موفق، به‌ویژه انگلستان در این پژوهش محدود است.

از سوی دیگر، اعتمادی (۱۴۰۴) و روشندل (۱۴۰۲) با رویکرد تطبیقی، عناصر قانونی و مادی و معنوی کلاهبرداری رایانه‌ای را در حقوق ایران و انگلستان تحلیل کرده‌اند. یافته‌های این دو پژوهش، ضمن تبیین تفاوت‌های تقنینی و کاستی‌های مقررات ایران، عمدتاً بر اصلاح جرم‌انگاری و ضمانت اجراهای کیفری تأکید دارند. درنتیجه، پیشگیری از جرم از طریق مدیریت فرصت‌های مجرمانه، ارتقای امنیت سامانه‌ها، آموزش کاربران و مشارکت نهادهای عمومی و خصوصی، جایگاه برجسته‌ای در تحلیل آنان ندارد.

تحلیل انتقادی پژوهش‌های پیشین بیانگر آن است که خلأ اصلی ادبیات موجود، فقدان پژوهشی است که پیشگیری از کلاهبرداری سایبری را بر پایه نظریه‌های نوین جرم‌شناسی، به‌ویژه الگوی پنج‌گانه پیشگیری وضعی کلارک مورد بررسی تطبیقی قرار دهد. پژوهش حاضر با فاصله گرفتن از رویکرد صرفاً کیفری، می‌کوشد ظرفیت‌های پیشگیری وضعی را در حقوق ایران با بهره‌گیری از تجربه حقوق انگلستان تحلیل کند و نشان دهد که ترکیب تدابیر حقوقی، فنی، آموزشی و مشارکتی، در کنار کاهش فرصت‌های ارتکاب جرم، می‌تواند اثربخشی سیاست جنایی ایران را در مقابله با کلاهبرداری سایبری به نحو چشمگیری افزایش دهد. بدین ترتیب، نوآوری پژوهش حاضر در تلفیق رویکرد جرم‌شناختی و حقوق تطبیقی و ارائه راهکارهای عملی برای پیاده‌سازی الگوی کلارک در نظام حقوقی ایران است.

۲. فلسفهٔ پیشگیری وضعی در قبال کلاهبرداری سایبری

۲-۱. مبانی مشروعیت پیشگیری وضعی

پیشگیری وضعی از کلاهبرداری سایبری، پیش از آنکه یک راهبرد جرم‌شناختی یا سیاست جنایی تلقی شود، بر مبانی فلسفه حقوق در خصوص مشروعیت مداخله دولت برای حمایت از نظم عمومی و حقوق بنیادین شهروندان استوار است. از منظر فلسفه حقوق، دولت صرفاً پس از وقوع جرم مسئول واکنش کیفری نیست، بلکه در حدود اصل تناسب و ضرورت، مکلف است از تحقق رفتارهای زیان‌بار نیز پیشگیری کند (غنی و دیگران، ۱۴۰۴: ۲۸).

در فضای سایبری که ویژگی‌هایی چون ناشناس بودن، سرعت انتقال داده‌ها و فرامرزی بودن تعاملات، فرصت‌های ارتکاب جرم را افزایش داده است، محدود ساختن این فرصت‌ها با بهره‌گیری از تدابیر وضعی، از منظر نظریه‌های عدالت و خیر عمومی قابل توجیه است. مشروعیت این مداخله زمانی تحقق می‌یابد که اقدامات پیشگیرانه به جای تحدید ناموجه آزادی‌های فردی، صرفاً بر کاهش فرصت‌های مجرمانه و ارتقای امنیت زیرساخت‌های دیجیتال متمرکز باشد. بر همین اساس پیشگیری وضعی نه به معنای گسترش کنترل کیفری، بلکه بیانگر تغییر جهت سیاست جنایی از واکنش پسینی به مدیریت عقلانی مخاطرات است. بنابراین، فلسفه حقوق پیشگیری وضعی بر این اندیشه استوار است که تأمین امنیت عمومی و حمایت از حقوق اشخاص، از طریق ایجاد محیطی ایمن و کاهش زمینه‌های ارتکاب جرم، با الزامات دولت قانون‌مدار سازگار بوده و در چارچوب اصول ضرورت، تناسب و منفعت عمومی قابل توجیه است.

۲-۲. نسبت پیشگیری وضعی با کرامت انسانی و آزادی‌های فردی

یکی از مهم‌ترین مباحث فلسفه حقوق در حوزه پیشگیری وضعی، نسبت میان امنیت عمومی و آزادی‌های بنیادین شهروندان است. هرگونه مداخله دولت برای پیشگیری از جرم، هنگامی مشروع خواهد بود که به کرامت انسانی، حریم خصوصی و آزادی‌های مشروع افراد احترام بگذارد. در کلاهبرداری سایبری، بسیاری از تدابیر پیشگیرانه همچون احراز هویت چندمرحله‌ای، پایش تراکنش‌های مشکوک، ثبت داده‌های ترافیکی و ارتقای استانداردهای امنیتی، ممکن است در نگاه نخست محدودکننده برخی آزادی‌ها تلقی شوند؛ اما از منظر فلسفه حقوق، این محدودیت‌ها زمانی موجه‌اند که بر اساس قانون، با هدف حمایت از حقوق دیگران، متناسب با خطر موجود و فاقد جنبه تبعیض‌آمیز باشند (قدسی و دیگران، ۱۴۰۰: ۳۴).

اصل کرامت انسانی اقتضا می‌کند که کاربران فضای سایبری نه صرفاً موضوع کنترل، بلکه صاحبان حق امنیت، حریم خصوصی و دسترسی ایمن به خدمات دیجیتال محسوب شوند. ازاین‌رو، پیشگیری وضعی باید به‌گونه‌ای طراحی شود که ضمن کاهش فرصت‌های ارتکاب کلاهبرداری، از تبدیل شدن به ابزاری برای نظارت گسترده و غیرضروری بر شهروندان جلوگیری کند. بدین ترتیب، فلسفه حقوق میان آزادی و امنیت رابطه‌ای تقابلی برقرار نمی‌کند، بلکه هر دو را ارزش‌های مکمل می‌داند که تحقق هر یک در گرو رعایت حدود و قیود دیگری است.

۲- ۳. پیشگیری وضعی و عدالت پیشگیرانه در سیاست جنایی معاصر

تحولات سیاست جنایی معاصر نشان می‌دهد که عدالت کیفری صرفاً به واکنش پس از وقوع جرم محدود نیست، بلکه به سوی الگوی «عدالت پیشگیرانه» حرکت کرده است. این تحول ریشه در مبانی فلسفه حقوق دارد که هدف نظام حقوقی را تنها مجازات بزهکار نمی‌داند، بلکه حمایت از حقوق شهروندان، کاهش آسیب‌های اجتماعی و تضمین امنیت عمومی را نیز از کارکردهای اساسی آن برمی‌شمارد (Garofalo, 2020: 72).

در حوزه کلاهبرداری سایبری، خسارت‌های مالی، روانی و اجتماعی ناشی از جرم غالباً به‌گونه‌ای است که حتی اعمال شدیدترین ضمانت اجراهای کیفری نیز قادر به جبران کامل آن نیست. ازاین‌رو، عدالت اقتضا می‌کند که نظام حقوقی پیش از وقوع جرم نیز با مدیریت فرصت‌های مجرمانه، از تحقق زیان جلوگیری کند. این رویکرد مجازات را آخرین ابزار حمایت از جامعه می‌داند و بر طراحی محیط‌های ایمن، مسئولیت‌پذیری ارائه دهندگان خدمات دیجیتال، ارتقای سواد سایبری و مشارکت نهادهای عمومی و خصوصی در کاهش مخاطرات تأکید دارد. بر همین مبنا، پیشگیری وضعی نه جایگزین عدالت کیفری، بلکه مکمل آن است و می‌تواند میان امنیت، آزادی و عدالت تعادل برقرار سازد. درنتیجه، از منظر فلسفه حقوق، مشروعیت سیاست جنایی در عصر دیجیتال بیش از آنکه به شدت مجازات‌ها وابسته باشد، به میزان موفقیت آن در پیشگیری از نقض حقوق افراد و کاهش بزه‌دیدگی بستگی دارد.

۳. الزامات دخالت پیشگیری وضعی در قبال کلاهبرداری سایبری

۳-۱. الزام‌سنجی در حقوق ایران

تحولات شتابان فناوری اطلاعات و ارتباطات، در کنار توسعه خدمات الکترونیکی، زمینه ارتکاب جرائم اقتصادی به‌ویژه کلاهبرداری سایبری را نیز گسترش داده است. گسترش بانکداری الکترونیکی، تجارت دیجیتال و خدمات برخط، امکان بهره‌گیری مجرمان از شیوه‌هایی مانند فیشینگ، جعل هویت دیجیتال، درگاه‌های پرداخت جعلی، مهندسی اجتماعی، بدافزارها و سوءاستفاده از داده‌های شخصی را افزایش داده است. در چنین شرایطی، اتکای صرف به پاسخ‌های کیفری پس از وقوع جرم، به دلیل ویژگی‌های فرامرزی فضای سایبری، ناشناس ماندن مرتکبان و دشواری کشف و تعقیب آن‌ها کارآمد نیست؛ ازاین‌رو، پیشگیری وضعی به‌عنوان یکی از مؤثرترین رویکردهای جرم‌شناختی، جایگاه ویژه‌ای در سیاست جنایی ایران یافته است

(رستمی، ۱۳۹۸: ۶۰). ضرورت پیشگیری وضعی، نخست از ماهیت فرصت‌مدار کلاهبرداری سایبری ناشی می‌شود. برخلاف جرائم سنتی، این جرم عمدتاً بر ضعف سامانه‌های الکترونیکی، کاستی‌های امنیتی و خطاهای انسانی استوار است و مرتکب می‌تواند با کمترین هزینه و در کوتاه‌ترین زمان، افراد بسیاری را هدف قرار دهد. بر اساس نظریه انتخاب عقلانی و الگوی کلارک، هرچه فرصت ارتکاب جرم محدودتر، هزینه ارتکاب بیشتر و احتمال موفقیت کمتر باشد، انگیزه بزهکار نیز کاهش می‌یابد. ازاین‌رو، پیشگیری وضعی با تمرکز بر کاهش فرصت‌های مجرمانه، مکمل سیاست کیفری بوده و امکان جلوگیری از وقوع جرم پیش از مداخله نظام عدالت کیفری را فراهم می‌سازد (آگنج و همکاران، ۱۴۰۲: ۱۹۱).

ضرورت دیگر، به محدودیت‌های ذاتی نظام کیفری ایران در مقابله با جرائم سایبری بازمی‌گردد. اگرچه قانون جرائم رایانه‌ای، قانون تجارت الکترونیکی و مقررات بانکداری الکترونیکی، چارچوب قانونی مناسبی برای مقابله با این جرائم ایجاد کرده‌اند، اجرای آن‌ها با چالش‌هایی همچون دشواری کشف جرم، کمبود ادله دیجیتال، ناشناس بودن مرتکبان، استفاده از سرورهای خارجی و پیچیدگی همکاری‌های بین‌المللی مواجه است. درنتیجه پیشگیری وضعی با تأکید بر ارتقای امنیت سامانه‌ها، احراز هویت مطمئن، نظارت مؤثر، طراحی ایمن خدمات الکترونیکی و آموزش کاربران، می‌تواند خلأهای نظام کیفری را تا حد زیادی جبران کند.

گسترش دولت الکترونیک و خدمات مالی دیجیتال نیز اهمیت این رویکرد را دوچندان کرده است. ارائه گسترده خدمات بانکی، مالیاتی، قضایی، بیمه‌ای و تجاری از طریق سامانه‌های برخط، امنیت سایبری را به بخشی از سیاست جنایی پیشگیرانه تبدیل کرده است. در این میان ضعف در طراحی سامانه‌ها، فقدان احراز هویت چندمرحله‌ای، هشدارهای امنیتی ناکافی و آموزش نامناسب کاربران، فرصت ارتکاب جرم را افزایش می‌دهد؛ ازاین‌رو، پیشگیری مؤثر مستلزم مشارکت قانون‌گذار، نهادهای اجرایی، بانک‌ها، شرکت‌های فناوری و ارائه‌دهندگان خدمات دیجیتال است (ابراهیمی، ۱۳۹۷: ۷۷) .

ویژگی‌های بزه‌دیدگان کلاهبرداری سایبری نیز ضرورت اتخاذ تدابیر پیشگیرانه را آشکار می‌سازد. بسیاری از قربانیان، به دلیل آگاهی فنی محدود، اطلاعات محرمانه خود را در اختیار مجرمان قرار می‌دهند و در این موارد، حتی شدیدترین ضمانت اجراهای کیفری نیز قادر به جبران کامل خسارات مالی و روانی نیست. ازاین‌رو، آموزش عمومی، هشدارهای امنیتی، طراحی ساده و ایمن سامانه‌ها و کاهش آسیب‌پذیری کاربران، از مهم‌ترین ابزارهای حمایت از بزه‌دیدگان بالقوه به شمار می‌رود. افزون بر این، کلاهبرداری سایبری

با کاهش اعتماد عمومی به تجارت الکترونیکی، بانکداری دیجیتال و خدمات برخط، هزینه‌های اقتصادی گسترده‌ای بر دولت و بخش خصوصی تحمیل می‌کند؛ بنابراین سرمایه‌گذاری در ارتقای امنیت سامانه‌ها، پایش هوشمند تراکنش‌ها، توسعه فناوری‌های احراز هویت و آموزش کاربران، در مقایسه با هزینه‌های ناشی از وقوع جرم، راهکاری پایدار و مقرون‌به‌صرفه محسوب می‌شود.

در مقام جمع‌بندی باید اذعان نمود ضرورت پیشگیری وضعی از تحول سیاست جنایی معاصر نیز ناشی می‌شود. سیاست جنایی نوین، به جای اتکا به واکنش کیفری پس از وقوع جرم، بر مدیریت خطر، کاهش فرصت‌های مجرمانه و مشارکت نهادهای دولتی و غیردولتی در پیشگیری از جرم تأکید دارد. ازاین‌رو، مقابله مؤثر با کلاهبرداری سایبری مستلزم آن است که پیشگیری وضعی به‌عنوان یکی از ارکان سیاست جنایی ایران، در طراحی خدمات الکترونیکی، تنظیم مقررات، ارتقای امنیت سایبری و آموزش عمومی نهادینه شود؛ رویکردی که می‌تواند ضمن کاهش فرصت‌های ارتکاب جرم، امنیت فضای تبادل اطلاعات، اعتماد عمومی به خدمات دیجیتال و کارآمدی نظام حقوقی را به نحو مؤثرتری تضمین کند.

۳-۲. الزام‌سنجی در حقوق انگلستان

حقوق انگلستان ازجمله نظام‌های حقوقی پیشرو در مواجهه با جرائم سایبری محسوب می‌شود که در دهه‌های اخیر، همگام با گسترش اقتصاد دیجیتال، رویکرد خود را از اتکای صرف به واکنش کیفری پس از وقوع جرم به سوی مدیریت پیشگیرانه مخاطرات سایبری سوق داده است. افزایش وابستگی اشخاص حقیقی، مؤسسات مالی، شرکت‌های خصوصی و نهادهای عمومی به فناوری اطلاعات، موجب شده است که کلاهبرداری سایبری به یکی از مهم‌ترین تهدیدهای امنیت اقتصادی و اجتماعی این کشور تبدیل شود. بر اساس گزارش‌های سالانه نهادهای مسئول مبارزه با جرائم اقتصادی، بخش قابل توجهی از جرائم ثبت‌شده در انگلستان را انواع کلاهبرداری، به‌ویژه کلاهبرداری‌های مبتنی بر فضای سایبری تشکیل می‌دهد (Cabinet Office, 2009: 19). این واقعیت نشان داده است که برخورد کیفری با مرتکبان هرچند ضروری است، اما به تنهایی قادر به کاهش پایدار این دسته از جرائم نیست؛ زیرا ویژگی‌های فضای سایبری، ازجمله ناشناس بودن کاربران، فرامرزی بودن بستر ارتکاب جرم، سرعت انتقال داده‌ها و پیچیدگی فناوری‌های مورد استفاده مجرمان، کارآمدی شیوه‌های سنتی کشف و تعقیب را محدود می‌کند. از همین رو، پیشگیری وضعی به‌عنوان یکی از ارکان اصلی سیاست جنایی انگلستان در مقابله با کلاهبرداری سایبری مورد توجه قانون‌گذار،

دستگاه قضایی و نهادهای اجرایی قرار گرفته است (McGuire & Dowling, 2013: 27).

نخستین ضرورت پیشگیری وضعی در حقوق انگلستان، ماهیت فرصت‌محور کلاهبرداری سایبری[۱] است. مطالعات جرم‌شناختی انجام شده در این کشور نشان می‌دهد که بسیاری از کلاهبرداری‌های اینترنتی نه حاصل برنامه‌ریزی پیچیده مجرمان حرفه‌ای، بلکه نتیجه وجود ضعف‌های امنیتی در سامانه‌های مالی، خطاهای انسانی، طراحی نامناسب خدمات دیجیتال و فقدان کنترل‌های مؤثر است (Home Office, 2013: 15). بر همین اساس، سیاست جنایی انگلستان بر این فرض استوار شده که کاهش فرصت‌های ارتکاب جرم،[۲] اثربخش‌تر و کم‌هزینه‌تر از افزایش صرف مجازات‌ها خواهد بود. این رویکرد با مبانی نظری پیشگیری وضعی کلارک هماهنگ است؛ زیرا هدف اصلی آن، دشوار کردن ارتکاب جرم، افزایش احتمال کشف، کاهش منافع حاصل از جرم و محدود ساختن فرصت‌های مجرمانه است.

ضرورت دیگر پیشگیری وضعی در حقوق انگلستان، حفظ اعتماد عمومی به اقتصاد دیجیتال است. وابستگی گسترده این کشور به تجارت الکترونیکی، بانکداری اینترنتی و خدمات مالی برخط، موجب شده است که افزایش کلاهبرداری‌های سایبری علاوه بر تحمیل خسارت به بزه‌دیدگان، اعتماد شهروندان و سرمایه‌گذاران را تضعیف، هزینه‌های امنیتی را افزایش و رقابت‌پذیری بازارهای دیجیتال را کاهش دهد. ازاین‌رو، پیشگیری وضعی در انگلستان صرفاً یک راهبرد کیفری نیست، بلکه بخشی از سیاست‌های اقتصادی، امنیتی و حکمرانی دیجیتال به شمار می‌رود (Atkinson & McKay, 2007: 14). از سوی دیگر، سیاست جنایی انگلستان بر مسئولیت مشترک دولت و بخش خصوصی در مدیریت مخاطرات سایبری استوار است. برخلاف رویکردهای سنتی، بانک‌ها، مؤسسات مالی، شرکت‌های فناوری، اپراتورهای مخابراتی، ارائه‌دهندگان خدمات اینترنتی و پلتفرم‌های دیجیتال نیز در پیشگیری از جرم نقش فعال دارند. این نهادها با رعایت استانداردهای امنیتی، توسعه سامانه‌های هوشمند شناسایی رفتارهای مشکوک، ارائه هشدارهای امنیتی و واکنش سریع به فعالیت‌های غیرعادی، در کاهش فرصت‌های ارتکاب جرم مشارکت می‌کنند؛ امری که نشان‌دهنده ماهیت مشارکتی پیشگیری وضعی در این نظام حقوقی است (Chohan, 2021: 9). همچنین،

---

۱. ماهیت فرصت‌محور کلاهبرداری سایبری به این معناست که مرتکبان این جرم بیش از آنکه به زور یا اجبار متوسل شوند، از فرصت‌ها، آسیب‌پذیری‌های فنی، ضعف‌های امنیتی و خطاهای انسانی برای ارتکاب جرم بهره می‌برند. گسترش فناوری‌های اطلاعاتی، افزایش استفاده از خدمات آنلاین و امکان ناشناس‌ماندن در فضای مجازی، فرصت‌های متعددی را برای کلاهبرداران فراهم کرده است. ازاین‌رو، وقوع کلاهبرداری سایبری تا حد زیادی به وجود بسترهای مناسب، ضعف تدابیر امنیتی و بی‌احتیاطی کاربران وابسته است. این ویژگی، پیشگیری از جرم را بیش از هر چیز به ارتقای امنیت سایبری، آموزش کاربران و کاهش فرصت‌های مجرمانه وابسته می‌سازد.

2. Reducing opportunities to commit crime.

تجربه عملی انگلستان نشان می‌دهد که بسیاری از کلاهبرداری‌های سایبری بر پایه خطاهای شناختی و روان‌شناختی کاربران و از طریق مهندسی اجتماعی، پیام‌ها و وبگاه‌های جعلی یا تماس‌های فریبکارانه انجام می‌شوند. ازاین‌رو، افزایش آگاهی عمومی، آموزش مستمر شهروندان، اطلاع‌رسانی درباره شیوه‌های نوین کلاهبرداری، هشدارهای هوشمند هنگام تراکنش‌های مالی و ارتقای سواد امنیت سایبری، از مهم‌ترین ابزارهای کاهش آسیب‌پذیری بزه‌دیدگان بالقوه به شمار می‌روند (Crimm & Majoor, 2019: 364).

افزون بر این، همگرایی سیاست‌های تقنینی و استانداردهای فنی از دیگر ضرورت‌های پیشگیری وضعی در انگلستان است. در این نظام حقوقی مقررات علاوه بر جرم‌انگاری رفتارهای متقلبانه، مؤسسات مالی و ارائه‌دهندگان خدمات دیجیتال را به رعایت الزامات امنیتی، حفاظت از داده‌های کاربران، مدیریت مخاطرات سایبری و گزارش‌دهی سریع رخدادهای امنیتی ملزم می‌کنند. این هماهنگی میان حقوق و فناوری، پیشگیری از کلاهبرداری سایبری را از مرحله واکنش قضایی به مرحله طراحی ایمن خدمات دیجیتال یا «امنیت از طریق طراحی» منتقل کرده و نقش مؤثری در کاهش فرصت‌های ارتکاب جرم ایفا کرده است (Europol, 2021: 128).

در سال‌های اخیر، حقوق انگلستان درزمینهٔ مقابله با کلاهبرداری‌های سایبری، به‌ویژه کلاهبرداری‌های پرداخت مجاز فریب‌خورده،[1] از رویکردی صرفاً واکنشی به سوی سیاستی پیشگیرانه و حمایت‌محور حرکت کرده است. مهم‌ترین نمود این تحول، اجرای رژیم الزام‌آور جبران خسارت قربانیان کلاهبرداری‌های از سال ۲۰۲۴ به ابتکار نهاد تنظیم‌گر نظام‌های پرداخت[2] است. بر اساس این نظام ارائه‌دهندگان خدمات پرداخت در صورت تحقق شرایط مقرر، مکلف به جبران خسارت قربانیان هستند؛ مگر آنکه رفتار مشتری مصداق بی‌احتیاطی فاحش یا استثناهای قانونی باشد. این تحول مسئولیت پیشگیری را از کاربران به مؤسسات مالی نیز تسری داده و بانک‌ها را به ارتقای سامانه‌های احراز هویت، پایش هوشمند تراکنش‌ها، شناسایی پرداخت‌های پرخطر و ارائه هشدارهای مؤثر به مشتریان ملزم کرده است (زارعی‌نژاد و دیگران، ۱۴۰۵: ۱۲).

از منظر پیشگیری وضعی، این رویکرد بیانگر انتقال بخشی از مسئولیت کنترل فرصت‌های ارتکاب جرم به نهادهای مالی و ارائه‌دهندگان خدمات پرداخت است. به بیان دیگر، قانون‌گذار انگلستان با ایجاد مسئولیت مالی برای بانک‌ها، انگیزه لازم را برای سرمایه‌گذاری در تدابیر پیشگیرانه، توسعه سامانه‌های کشف تقلب و

1. Authorised Push Payment Fraud – APP Fraud.
2. Payment Systems Regulator.

تقویت سازوکارهای مدیریت ریسک فراهم کرده است. درنتیجه، پیشگیری از کلاهبرداری سایبری دیگر صرفاً بر تعقیب و مجازات مرتکبان استوار نیست، بلکه از طریق کاهش فرصت‌های ارتکاب جرم، افزایش احتمال کشف، محدود کردن منافع حاصل از جرم و ارتقای امنیت زیرساخت‌های پرداخت تحقق می‌یابد؛ رویکردی که با مبانی پیشگیری وضعی کلارک نیز همخوانی دارد. این تجربه می‌تواند در اصلاح سیاست جنایی ایران، به‌ویژه در حوزه مسئولیت مؤسسات مالی و تقویت تدابیر پیشگیرانه در نظام پرداخت الکترونیکی، مورد توجه قانون‌گذار قرار گیرد.

در مقام جمع‌بندی نویسنده بر این باور است ضرورت پیشگیری وضعی در حقوق انگلستان، ریشه در تحول سیاست جنایی این کشور از عدالت کیفری واکنشی به مدیریت پیشگیرانه خطر دارد. در این رویکرد، موفقیت سیاست جنایی صرفاً با تعداد محکومیت‌های کیفری سنجیده نمی‌شود، بلکه میزان کاهش فرصت‌های ارتکاب جرم، افزایش امنیت کاربران، ارتقای تاب‌آوری زیرساخت‌های دیجیتال و کاهش خسارت‌های اقتصادی ناشی از کلاهبرداری نیز از شاخص‌های اصلی ارزیابی محسوب می‌شوند. به همین دلیل، حقوق انگلستان پیشگیری وضعی را نه یک راهکار فرعی، بلکه یکی از مؤلفه‌های بنیادین مقابله با کلاهبرداری سایبری تلقی کرده و از طریق تلفیق ابزارهای حقوقی، مدیریتی، فنی و آموزشی کوشیده است محیط ارتکاب جرم را برای بزهکاران پرهزینه، پرخطر و کم‌منفعت سازد. این تجربه می‌تواند برای نظام حقوقی ایران نیز الگوی مناسبی در جهت تقویت سیاست جنایی پیشگیرانه و کاهش آسیب‌های ناشی از کلاهبرداری‌های سایبری باشد.

۴. پیاده‌سازی پیشگیریِ وضعی در حوزه جرائم سایبری در مدل مطلوب

۴-۱. سخت نمودن ارتکاب کلاهبرداری سایبری برای بزهکاران

یکی از مهم‌ترین راهبردهای پیشگیری وضعی در الگوی رونالد کلارک، افزایش تلاش لازم برای ارتکاب جرم[1] است. این راهبرد بر مبنای نظریه انتخاب عقلانی استوار بوده و فرض می‌کند که بزهکار پیش از ارتکاب جرم، هزینه‌ها و منافع آن را ارزیابی می‌کند؛ بنابراین، هرچه ارتکاب جرم مستلزم زمان، مهارت، تجهیزات و هزینه بیشتری باشد، احتمال انصراف مرتکب افزایش می‌یابد (Clarke & Eck, 2003: 25). در کلاهبرداری سایبری نیز که غالباً بر ضعف تدابیر امنیتی، سهولت دسترسی به سامانه‌های اطلاعاتی و امکان فریب سریع

1. Increasing the effort required to commit a crime.

بزه‌دیدگان متکی است، افزایش موانع فنی و امنیتی می‌تواند فرصت ارتکاب جرم را به نحو مؤثری کاهش دهد (مجیدی، ۱۴۰۰: ۲۵۰).

در حقوق ایران، اگرچه قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و سایر مقررات مرتبط، چارچوب کیفری مقابله با کلاهبرداری سایبری را فراهم کرده‌اند، این مقررات عمدتاً ماهیتی واکنشی داشته و کمتر بر پیشگیری فنی و موقعیتی تأکید دارند. در مقابل حقوق انگلستان با اتکا بر رویکردی پیشگیرانه، علاوه بر مقرراتی مانند قانون سوءاستفاده از کامپیوتر ۱۹۹۰ و قانون کلاهبرداری ۲۰۰۶، از طریق استانداردهای امنیت سایبری مرکز ملی امنیت سایبری (NCSC)، سازمان‌ها را به استقرار تدابیری نظیر احراز هویت چندمرحله‌ای، مدیریت دسترسی، رمزنگاری اطلاعات، پایش مستمر سامانه‌ها و آزمون‌های نفوذ ترغیب یا ملزم می‌کند. بدین ترتیب، سیاست جنایی این کشور از تمرکز بر مجازات پس از وقوع جرم به سمت دشوارسازی شرایط ارتکاب آن سوق یافته است (Marion & Twede, 2020: 85). از منظر جرم‌شناختی نیز، تحقق کلاهبرداری سایبری حاصل تعامل میان انگیزه مجرمانه و فرصت ارتکاب جرم است. هرچند انگیزه‌هایی مانند کسب منفعت مالی، انتقام‌جویی، رقابت تجاری یا کسب اعتبار در میان هکرها می‌توانند زمینه‌ساز رفتار مجرمانه باشند، اما بدون وجود فرصت مناسب، این انگیزه‌ها به ارتکاب جرم منتهی نمی‌شوند. ازاین‌رو، پیشگیری وضعی با تمرکز بر کاهش فرصت‌های مجرمانه و اصلاح محیط جرم‌زا، حتی در صورت وجود انگیزه، امکان تحقق جرم را محدود می‌سازد؛ رویکردی که برخلاف دیدگاه‌های سنتی، به جای تمرکز بر ویژگی‌های شخصیتی مرتکب، بر کنترل شرایط و موقعیت‌های تسهیل‌کننده جرم تأکید دارد (Zhang, 2021: 15).

یکی از مهم‌ترین مصادیق افزایش تلاش برای ارتکاب کلاهبرداری سایبری، تقویت امنیت آماج جرم[1] است. آماج جرم در فضای سایبری، صرفاً رایانه یا تلفن همراه نیست، بلکه داده‌ها، حساب‌های کاربری، سامانه‌های بانکی، درگاه‌های پرداخت، شبکه‌های اجتماعی و سایر زیرساخت‌های دیجیتال را نیز در بر می‌گیرد. هر اندازه این آماج‌ها از طریق تدابیری نظیر احراز هویت چندعاملی[2] استفاده از گذرواژه‌های پیچیده، رمزنگاری داده‌ها، محدودسازی سطح دسترسی کاربران، ثبت وقایع امنیتی سامانه‌های تشخیص

---

۱. آماج جرم به شخص، مال، حق یا منفعتی گفته می‌شود که رفتار مجرمانه مستقیماً متوجه آن است و جرم علیه آن ارتکاب می‌یابد. به بیان دیگر، آماج جرم همان موضوعی است که مرتکب قصد آسیب رساندن، تعرض یا نقض آن را دارد. آماج جرم بسته به نوع بزه می‌تواند یک فرد، اموال، امنیت عمومی، نظم اجتماعی یا سایر ارزش‌های مورد حمایت قانون باشد. شناسایی آماج جرم در تحلیل ارکان مادی و معنوی جرم، تعیین عنوان مجرمانه و تشخیص آثار حقوقی و کیفری آن اهمیت فراوانی دارد.

2. Multi-Factor Authentication.

نفوذ و کنترل دسترسی مبتنی بر نقش (آر. بی. ای.سی)[1] تقویت شوند، امکان موفقیت بزهکار در اجرای عملیات متقلبانه کاهش می‌یابد. درواقع، این اقدامات مصداق بارز تکنیک «سخت کردن هدف» در نظریه کلارک محسوب می‌شوند.

در این زمینه، تفاوت رویکرد ایران و انگلستان قابل توجه است. در ایران بخش عمده مسئولیت حفاظت از اطلاعات بر عهده کاربران قرار گرفته و الزامات قانونی مشخصی برای بسیاری از ارائه‌دهندگان خدمات دیجیتال در خصوص رعایت حداقل استانداردهای امنیتی وجود ندارد (صبح‌خیز، ۱۳۹۴: ۱۲۵). در مقابل در انگلستان، علاوه بر مسئولیت کیفری مرتکبان، ارائه‌دهندگان خدمات مالی و دیجیتال نیز مکلف به رعایت استانداردهای امنیتی و مدیریت مخاطرات سایبری هستند. به همین دلیل، وقوع بسیاری از حملات فیشینگ یا کلاهبرداری‌های اینترنتی صرفاً از منظر مسئولیت کیفری مرتکب بررسی نمی‌شود، بلکه میزان رعایت استانداردهای امنیتی از سوی مؤسسات مالی و شرکت‌های ارائه‌دهنده خدمات نیز مورد ارزیابی قرار می‌گیرد. این رویکرد، نمونه‌ای از انتقال بخشی از مسئولیت پیشگیری از اشخاص به نهادهای ایجادکننده فرصت است (Gercke, 2009: 95).

به‌زعم نویسنده تلاش برای ارتکاب جرم صرفاً به تقویت سامانه‌های فنی محدود نمی‌شود، بلکه کنترل ابزارهای ارتکاب جرم نیز اهمیت اساسی دارد. مقصود از کنترل ابزارها، محدودسازی امکان استفاده مجرمانه از تجهیزات و خدماتی است که معمولاً در ارتکاب کلاهبرداری سایبری مورد استفاده قرار می‌گیرند؛ ازجمله سرورهای ناشناس، نرم‌افزارهای مخرب، حساب‌های کاربری جعلی، سیم‌کارت‌های بی‌هویت و درگاه‌های پرداخت فاقد احراز هویت کافی. البته این کنترل نباید به معنای نظارت فراگیر و نامحدود بر کاربران یا محدودسازی غیرضروری دسترسی آنان به اینترنت تلقی شود؛ زیرا چنین رویکردی با اصل تناسب، حریم خصوصی و آزادی‌های بنیادین در تعارض است. تجربه حقوق انگلستان نشان می‌دهد که کنترل ابزارهای جرم باید به جای کنترل همگانی کاربران مبتنی بر مدیریت ریسک، نظارت هدفمند و همکاری میان نهادهای انتظامی، قضایی، بانک‌ها و ارائه‌دهندگان خدمات اینترنتی باشد. از منظر فنی نیز انجام ارزیابی‌های امنیتی مستمر، آزمون‌های نفوذ، به‌روزرسانی نرم‌افزارها، مدیریت آسیب‌پذیری‌ها و استفاده از سامانه‌های هوشمند شناسایی حملات، نقش مؤثری در افزایش هزینه ارتکاب کلاهبرداری سایبری دارد. هرچند هیچ سامانه‌ای

[1]. کنترل دسترسی مبتنی بر نقش (RBAC) یکی از روش‌های استاندارد و پیشرفته برای مدیریت دسترسی به منابع اطلاعاتی و داده‌ها در سازمان‌ها است.

از امنیت مطلق برخوردار نیست، اما افزایش سطح امنیت موجب می‌شود که بزهکار برای دستیابی به هدف ناگزیر از صرف زمان، تخصص و منابع بیشتری باشد. درنتیجه، بسیاری از مرتکبان، به‌ویژه مجرمان فرصت‌طلب، اهداف آسان‌تر را انتخاب خواهند کرد. این دقیقاً همان منطق پیشگیری وضعی با موقعیت‌مدار است که به جای حذف کامل انگیزه مجرمانه، بر کاهش فرصت و افزایش دشواری ارتکاب جرم تمرکز دارد.

بر این اساس، می‌توان نتیجه گرفت که سیاست جنایی ایران درزمینهٔ مقابله با کلاهبرداری سایبری، بیش از آنکه بر توسعه تدابیر پیشگیرانه وضعی استوار باشد، همچنان بر واکنش کیفری پس از وقوع جرم تأکید دارد. درحالی‌که تجربه حقوق انگلستان نشان می‌دهد تلفیق مقررات کیفری با الزامات امنیت سایبری، استانداردهای فنی، مسئولیت‌پذیری ارائه‌دهندگان خدمات و ارتقای مستمر امنیت زیرساخت‌های دیجیتال، کارآمدترین شیوه برای افزایش تلاش لازم جهت ارتکاب جرم و کاهش نرخ موفقیت کلاهبرداری‌های سایبری است.

۴-۲. افزایش خطر کشف و دستگیری و کاهش فرصت‌های بزه‌دیدگی در کلاهبرداری سایبری

یکی از مهم‌ترین مبانی نظری پیشگیری وضعی، نظریه انتخاب عقلانی است که توسط رونالد کلارک و درک کورنیش در جرم‌شناسی توسعه یافته است. بر اساس این نظریه، ارتکاب جرم حاصل ارزیابی عقلانی مرتکب از منافع، هزینه‌ها و احتمال دستگیری است؛ ازاین‌رو، هر اقدامی که خطر کشف، شناسایی یا ناکامی عملیات مجرمانه را افزایش دهد، محاسبات بزهکار را تغییر داده و انگیزه ارتکاب جرم را کاهش می‌دهد (Newman & Marongiu, 2016: 145). این مبنا در کلاهبرداری سایبری اهمیت ویژه‌ای دارد؛ زیرا ناشناس ماندن نسبی کاربران، فرامرزی بودن ارتباطات و دشواری شناسایی هویت، احتمال تعقیب کیفری را در ذهن مرتکبان کاهش می‌دهد. در مقابل بهره‌گیری از فناوری‌های نوین، ثبت و نگهداری داده‌های ترافیکی، سامانه‌های هوشمند کشف تقلب، تحلیل رفتار کاربران، احراز هویت چندمرحله‌ای، تبادل اطلاعات میان بانک‌ها و نهادهای انتظامی و واکنش سریع به حملات سایبری با افزایش احتمال شناسایی مرتکب، مصداق تکنیک «افزایش خطر دستگیری» در الگوی پیشگیری وضعی کلارک محسوب می‌شود.

در حقوق ایران هرچند قانون جرائم رایانه‌ای سازوکارهایی برای جمع‌آوری ادله الکترونیکی، حفظ داده‌های ترافیکی و شناسایی مرتکبان پیش‌بینی کرده است، محدودیت‌های فنی، استفاده از ابزارهای

ناشناس‌ساز، سرورهای خارجی و پیچیدگی همکاری‌های بین‌المللی، کارآمدی این تدابیر را کاهش داده است. در مقابل سیاست جنایی انگلستان با تکیه بر همکاری میان نهادهای انتظامی، مؤسسات مالی، ارائه‌دهندگان خدمات اینترنتی، مرکز ملی امنیت سایبری و واحدهای تخصصی مقابله با تقلب، همراه با استفاده از سامانه‌های تحلیل تراکنش‌های مشکوک و نظام‌های گزارش‌دهی سریع، احتمال کشف و توقف کلاهبرداری‌های سایبری را به‌طور محسوسی افزایش داده است (Marshall & Saulawa, 2015: 45).

پیشگیری وضعی علاوه بر بزهکار، بر کاهش آسیب‌پذیری بزه‌دیدگان بالقوه نیز تمرکز دارد. بخش قابل‌توجهی از کلاهبرداری‌های سایبری از خطاهای انسانی، اعتماد بی‌مورد یا بی‌توجهی کاربران به الزامات امنیتی ناشی می‌شود؛ ازاین‌رو، آموزش عمومی و ارتقای سواد دیجیتال و آگاهی‌بخشی درباره شیوه‌های نوین کلاهبرداری از مهم‌ترین ابزارهای محدودسازی فرصت‌های مجرمانه به شمار می‌رود (اصلانی و رنجبریان، ۱۳۹۴: ۲۶۵). رعایت اصولی مانند استفاده از گذرواژه‌های قوی، احراز هویت دومرحله‌ای، پرهیز از ورود اطلاعات بانکی در شبکه‌های ناامن، بررسی اصالت درگاه‌های پرداخت، اجتناب از کلیک بر پیوندهای ناشناس و به‌روزرسانی مستمر نرم‌افزارها، احتمال موفقیت مرتکبان را کاهش داده و فرآیند ارتکاب جرم را دشوارتر می‌کند.

در انگلستان نیز افزایش تاب‌آوری کاربران بخش مهمی از سیاست پیشگیری را تشکیل می‌دهد. نهادهایی مانند مرکز ملی امنیت سایبری، بانک‌ها و پلیس تخصصی مقابله با تقلب، از طریق انتشار مستمر هشدارهای امنیتی، دستورالعمل‌های آموزشی و کمپین‌های آگاهی‌بخشی، شهروندان را نسبت به شیوه‌های نوظهور کلاهبرداری، ازجمله فیشینگ، مهندسی اجتماعی، جعل هویت دیجیتال و کلاهبرداری‌های مبتنی بر هوش مصنوعی آگاه می‌سازند. تجربه این کشور نشان می‌دهد که آموزش عمومی، در کنار تدابیر کیفری و فنی، از مؤثرترین ابزارهای کاهش فرصت‌های ارتکاب جرم است (Rowland et al, 2017: 215).

با وجود این، پیشگیری وضعی با محدودیت‌هایی نیز مواجه است. این رویکرد عمدتاً در برابر مجرمان فرصت‌طلب که رفتار آنان تابع محاسبات هزینه و فایده است، اثربخش‌تر بوده، اما مجرمان حرفه‌ای و سازمان‌یافته معمولاً با بهره‌گیری از دانش فنی و منابع بیشتر، موانع امنیتی را دور می‌زنند. بنابراین، پیشگیری وضعی باید در کنار سیاست‌های کیفری، توسعه همکاری‌های بین‌المللی، ارتقای توان فنی ضابطان، استقرار سامانه‌های هوشمند کشف تقلب و همکاری مستمر میان بخش عمومی و خصوصی اجرا شود. مقایسه حقوق ایران و انگلستان نشان می‌دهد که هر دو نظام حقوقی اصل افزایش احتمال کشف جرم را پذیرفته‌اند، اما

انگلستان با بهره‌گیری گسترده‌تر از فناوری‌های نوین، مسئولیت‌پذیری بیشتر مؤسسات مالی و سرمایه‌گذاری مستمر در آموزش عمومی، در تغییر محاسبات عقلانی بزهکاران و کاهش فرصت‌های ارتکاب کلاهبرداری سایبری موفق‌تر عمل کرده است؛ تجربه‌ای که می‌تواند در اصلاح سیاست جنایی ایران و تقویت پیشگیری وضعی در این حوزه مورد استفاده قرار گیرد.

۴-۳. کاهش دستاوردهای ناشی از کلاهبرداری سایبری

یکی از مهم‌ترین راهبردهای پیشگیری وضعی در الگوی رونالد کلارک، کاهش منافع حاصل از جرم[1] است. این راهبرد بر این فرض استوار است که هرچه امکان بهره‌برداری مرتکب از عواید جرم محدودتر شود، انگیزه ارتکاب آن نیز کاهش می‌یابد (عمرانی‌فر و بیرنگ، ۱۴۰۵: ۲۹۰). در کلاهبرداری سایبری که هدف اصلی آن کسب منافع مالی، اطلاعات ارزشمند یا داده‌های هویتی است، اقداماتی مانند انسداد سریع حساب‌های بانکی، رهگیری وجوه، مسدودسازی کیف‌پول‌های الکترونیکی، توقف تراکنش‌های مشکوک، استرداد اموال بزه‌دیدگان و بی‌اثر کردن داده‌های سرقت شده، با کاهش سود مورد انتظار، محاسبات عقلانی بزهکار را تغییر داده و مصداق تکنیک «کاهش پاداش جرم» در پیشگیری وضعی محسوب می‌شوند (Marion & Twede, 2020: 85).

در حقوق ایران هرچند توقیف اموال، انسداد حساب‌ها و استرداد عواید ناشی از جرم پیش‌بینی شده است، این اقدامات غالباً پس از وقوع جرم و در جریان رسیدگی قضایی اعمال می‌شوند. درنتیجه، مرتکبان در بسیاری از موارد با انتقال سریع وجوه، استفاده از حساب‌های واسطه یا تبدیل دارایی‌ها به ارزهای دیجیتال، منافع حاصل از جرم را از دسترس مراجع تعقیب خارج می‌کنند؛ امری که نشان‌دهنده غلبه رویکرد واکنشی و ضعف سازوکارهای پیشگیرانه در محروم‌سازی مجرمان از عواید جرم است.

در مقابل حقوق انگلستان با اتخاذ رویکردی پیشگیرانه، از طریق همکاری مستمر میان بانک‌ها، مؤسسات مالی، نهادهای نظارتی و پلیس تخصصی مقابله با تقلب، امکان شناسایی سریع تراکنش‌های غیرعادی، تعلیق پرداخت‌های مشکوک، انسداد فوری حساب‌ها و بازیابی بخش قابل توجهی از وجوه را فراهم کرده است. همچنین، بهره‌گیری از سامانه‌های هوشمند تحلیل تراکنش‌های مالی موجب شده است که بسیاری از عملیات متقلبانه پیش از تکمیل شناسایی و متوقف شوند؛ رویکردی که نمونه‌ای عملی از راهبرد «کاهش

1. Reducing the proceeds of crime.

منافع جرم» در پیشگیری وضعی به شمار می‌رود (Xiao et al, 2018: 6).

علاوه بر این تدابیر فنی نظیر دیوار آتش، سامانه‌های تشخیص و جلوگیری از نفوذ، رمزنگاری داده‌ها، مدیریت دسترسی، پشتیبان‌گیری و پایش مستمر امنیت شبکه، نه‌تنها احتمال موفقیت حملات سایبری را کاهش می‌دهند، بلکه ارزش اقتصادی داده‌ها و دارایی‌های مورد هدف را نیز برای مجرمان محدود می‌سازند (کاوه و بارانی، ۱۴۰۴: ۱۹۸). همچنین اقداماتی مانند محدودسازی سقف تراکنش‌های اینترنتی، استفاده از رمزهای یک‌بارمصرف، احراز هویت چندمرحله‌ای، اعمال دوره انتظار برای انتقال مبالغ کلان و امکان توقف فوری تراکنش‌های مشکوک، حتی در صورت موفقیت اولیه مرتکب، بهره‌برداری از منافع مالی جرم را دشوار می‌کند.

با وجود این، کاهش منافع جرم به‌تنهایی برای مقابله با کلاهبرداری‌های سایبری کافی نیست؛ زیرا مجرمان حرفه‌ای و شبکه‌های سازمان‌یافته فراملی با بهره‌گیری از فناوری‌های نوین، هویت‌های جعلی، حساب‌های اجاره‌ای و ارزهای رمزنگاری‌شده، پیوسته درصدد دور زدن تدابیر امنیتی هستند. ازاین‌رو، اثربخشی این راهبرد مستلزم همکاری مستمر میان مراجع قضایی، ضابطان، بانک‌ها، ارائه‌دهندگان خدمات پرداخت، شرکت‌های فناوری و نهادهای بین‌المللی است. در مجموع، مقایسه حقوق ایران و انگلستان نشان می‌دهد که هر دو نظام حقوقی اصل محروم‌سازی مجرم از منافع حاصل از جرم را پذیرفته‌اند، اما درحالی‌که حقوق ایران عمدتاً بر مصادره و استرداد اموال پس از کشف جرم تکیه دارد، حقوق انگلستان با توسعه سازوکارهای پیشگیرانه، بهره‌گیری از فناوری‌های هوشمند، مدیریت ریسک در نظام بانکی و همکاری میان بخش‌های عمومی و خصوصی، در تحقق عملی راهبرد «کاهش دستاوردهای جرم» موفق‌تر عمل کرده است. این تجربه می‌تواند در جهت اصلاح سیاست جنایی ایران و تقویت پیشگیری وضعی از کلاهبرداری‌های سایبری مورد بهره‌برداری قرار گیرد.

۴-۴. کاهش عوامل تحریک‌کننده کلاهبرداری سایبری

چهارمین راهبرد پیشگیری وضعی در الگوی رونالد کلارک، کاهش عوامل تحریک‌کننده ارتکاب جرم[1] است. برخلاف راهبردهایی که بر دشوارسازی ارتکاب جرم، افزایش خطر دستگیری یا کاهش منافع ناشی از جرم تمرکز دارند، این رویکرد بر مدیریت عوامل روانی، اجتماعی و محیطی مؤثر بر تصمیم‌گیری بزهکار

1. Reducing factors that provoke crime.

استوار است. بسیاری از جرائم سایبری، ازجمله کلاهبرداری سایبری، صرفاً حاصل برنامه‌ریزی قبلی نیستند، بلکه تحت تأثیر عواملی مانند تنش، هیجانات لحظه‌ای، انتقام‌جویی، رقابت‌های ناسالم، احساس ناشناس بودن در فضای مجازی، کسب اعتبار در میان گروه‌های مجرمانه و تأثیرپذیری از شبکه‌های اجتماعی شکل می‌گیرند. ازاین‌رو، کاهش این محرک‌ها می‌تواند احتمال تبدیل انگیزه مجرمانه به رفتار مجرمانه را کاهش دهد (شمسی و همکاران، ۱۴۰۴: ۲۱۸).

در این چارچوب، سیاست جنایی نباید صرفاً بر واکنش کیفری پس از وقوع جرم متمرکز باشد، بلکه باید شرایطی را که ارتکاب کلاهبرداری سایبری را از منظر روانی و اجتماعی تسهیل یا توجیه می‌کند، مدیریت کند. در این زمینه، حقوق انگلستان نسبت به حقوق ایران رویکردی پیشگیرانه‌تر اتخاذ کرده و با اجرای برنامه‌های آموزشی، انتشار هشدارهای امنیتی، ارتقای فرهنگ استفاده ایمن از خدمات دیجیتال، آموزش اخلاق حرفه‌ای در حوزه فناوری اطلاعات و افزایش سواد سایبری، درصدد کاهش عوامل محرک ارتکاب جرائم سایبری برآمده است (Calzavara et al, 2015: 12).

یکی از مهم‌ترین تکنیک‌های کلارک، کاهش استرس‌ها و ناکامی‌های زمینه‌ساز رفتار مجرمانه است. بخشی از جرائم سایبری، به‌ویژه در محیط‌های سازمانی، ناشی از اختلافات شغلی، احساس بی‌عدالتی یا تعارضات شخصی است؛ ازاین‌رو، ایجاد سازوکارهای مؤثر برای مدیریت تعارضات، رسیدگی به شکایات کارکنان و تقویت عدالت سازمانی می‌تواند زمینه ارتکاب این جرائم را کاهش دهد. همچنین کاهش برانگیختگی‌های هیجانی از طریق طراحی ایمن سامانه‌ها، ایجاد تأخیر در تراکنش‌های پرخطر، نمایش هشدارهای امنیتی، الزام به تأیید مجدد عملیات مالی و اطلاع‌رسانی درباره شیوه‌های رایج کلاهبرداری، از تصمیم‌گیری‌های هیجانی و ارتکاب جرم پیشگیری می‌کند (Kuhlhorn, 2005: 78-79).

از سوی دیگر، خنثی‌سازی فشارهای اجتماعی و فرهنگی نیز از مؤلفه‌های مهم این راهبرد است. در برخی گروه‌های مجازی، ارتکاب جرائم سایبری به‌عنوان نشانه‌ای از مهارت فنی یا موفقیت تلقی می‌شود و می‌تواند به‌ویژه نوجوانان و کاربران کم‌تجربه را به رفتارهای مجرمانه ترغیب کند. آموزش اخلاق حرفه‌ای، ترویج مسئولیت‌پذیری دیجیتال، معرفی الگوهای رفتاری مثبت و آگاه‌سازی نسبت به پیامدهای کیفری و اجتماعی کلاهبرداری‌های سایبری، نقش مؤثری در کاهش این فشارها دارد. افزون بر این تبیین شفاف مقررات، مسئولیت‌های قانونی کاربران و الزامات استفاده ایمن از خدمات الکترونیکی، احتمال ارتکاب رفتارهای مجرمانه ناشی از ابهام یا ناآگاهی را کاهش می‌دهد. در حقوق انگلستان نیز انتشار مستمر هشدارهای امنیتی

و دستورالعمل‌های استفاده ایمن از خدمات دیجیتال، بخشی از سیاست پیشگیری وضعی و ابزاری برای کاهش تحریکات محیطی به شمار می‌رود (Fisher, 2016: 145).

با وجود این، کاهش عوامل تحریک‌کننده جایگزین ضمانت اجراهای کیفری نیست، بلکه مکمل آن‌هاست و بیشترین کارآمدی را در برابر مجرمان فرصت‌طلب و رفتارهای ناشی از هیجان یا موقعیت دارد. ازاین‌رو همانند تجربه انگلستان، اجرای مؤثر این راهبرد مستلزم همکاری مستمر میان مراجع قضایی، ضابطان، مؤسسات مالی، ارائه‌دهندگان خدمات دیجیتال، مراکز آموزشی و رسانه‌هاست. مقایسه حقوق ایران و انگلستان نشان می‌دهد که موفقیت در پیشگیری از کلاهبرداری سایبری مستلزم تلفیق تدابیر کیفری با سیاست‌های آموزشی، فرهنگی و محیطی است؛ رویکردی که زمینه تحقق سیاست جنایی پیشگیرانه و شهروندمحور را فراهم می‌سازد.

۴-۵. حذف بهانه‌های ارتکاب کلاهبرداری سایبری

پنجمین راهبرد پیشگیری وضعی در الگوی رونالد کلارک، حذف بهانه‌های ارتکاب جرم[1] است. این راهبرد بر این فرض استوار است که بخشی از جرائم، به‌ویژه در فضای سایبری، نه از انگیزه‌های مجرمانه ریشه‌دار، بلکه از ابهام در قواعد رفتاری، ضعف آگاهی حقوقی، عادی‌انگاری برخی رفتارها یا برداشت نادرست از قانون ناشی می‌شوند. ازاین‌رو، شفاف‌سازی مقررات، تبیین مسئولیت‌های کاربران و گسترش آموزش‌های عمومی، امکان توجیه رفتار مجرمانه و استناد به جهل یا سوءبرداشت از قانون را کاهش داده و به‌عنوان یکی از ابزارهای مهم پیشگیری وضعی عمل می‌کند (Gardner & Anderson, 2009: 325).

در حوزه کلاهبرداری سایبری، توسعه خدمات مالی الکترونیکی و تجارت دیجیتال، ضمن ایجاد فرصت‌های گسترده اقتصادی، زمینه ارتکاب جرائمی همچون فیشینگ، جعل هویت دیجیتال و سوءاستفاده از داده‌های شخصی را نیز فراهم کرده است. ویژگی‌های فضای سایبری، ازجمله فرامرزی بودن، سرعت انتقال اطلاعات و سهولت دسترسی، موجب شده است که همه کاربران در معرض این تهدیدها قرار گیرند. در چنین شرایطی، آموزش مستمر درباره شیوه‌های ارتکاب کلاهبرداری، حقوق و تکالیف قانونی کاربران و روش‌های حفاظت از اطلاعات شخصی، نقش مهمی در کاهش فرصت‌های مجرمانه دارد (Slapper & Kelly, 2010: 98).

1. Eliminating excuses for committing crimes.

از منظر جرم‌شناختی، آموزش عمومی با افزایش آگاهی کاربران نسبت به مخاطرات فضای سایبری، احتمال بزه‌دیدگی را کاهش می‌دهد. همچنین، اطلاع‌رسانی درباره ضمانت اجراهای قانونی و پیامدهای کیفری کلاهبرداری سایبری، محاسبات مرتکبان بالقوه را تحت تأثیر قرار داده و امکان توجیه رفتارهایی مانند «ناشناس ماندن در فضای مجازی» یا «فقدان ممنوعیت قانونی» را محدود می‌سازد. بدین ترتیب، آموزش هم‌زمان کاربران و بزهکاران بالقوه، دو کارکرد مکمل در چارچوب پیشگیری وضعی ایفا می‌کند (خادم‌پور و دیگران، ۱۴۰۳: ۱۰). در حقوق ایران، اگرچه اسناد بالادستی و قوانین مرتبط بر نقش آموزش و مشارکت عمومی تأکید دارند، برنامه‌های آگاهی‌بخشی در حوزه کلاهبرداری سایبری غالباً مقطعی، واکنشی و فاقد انسجام نهادی هستند و هماهنگی لازم میان دستگاه قضایی، پلیس، نظام آموزشی، رسانه‌ها و بخش خصوصی در این زمینه مشاهده نمی‌شود. درنتیجه، بخش قابل‌توجهی از شهروندان همچنان از تهدیدهای نوظهور فضای مجازی و شیوه‌های مقابله با آن‌ها آگاهی کافی ندارند.

در مقابل در حقوق انگلستان، آموزش عمومی یکی از ارکان اصلی سیاست پیشگیری از جرائم سایبری است. نهادهایی مانند مرکز ملی امنیت سایبری، پلیس تخصصی مقابله با تقلب، مؤسسات مالی و ارائه‌دهندگان خدمات دیجیتال، به‌طور مستمر از طریق راهنماهای آموزشی، هشدارهای امنیتی، دوره‌های برخط و کمپین‌های اطلاع‌رسانی، در جهت اصلاح رفتار کاربران، افزایش مسئولیت‌پذیری دیجیتال و کاهش زمینه‌های سوءاستفاده مجرمان اقدام می‌کنند. تجربه این کشور نشان می‌دهد که آموزش مستمر، به‌ویژه در حوزه بانکداری و خدمات مالی الکترونیکی، نقش مؤثری در کاهش موفقیت کلاهبرداری‌های سایبری داشته است (Schneider & Leung, 2022: 456).

حذف بهانه‌های ارتکاب جرم همچنین مستلزم شفاف‌سازی قواعد حقوقی و فنی است. ارائه هشدارهای روشن هنگام تراکنش‌های مالی، اطلاع‌رسانی مستمر درباره شیوه‌های جدید کلاهبرداری، تبیین مسئولیت‌های قانونی کاربران و تدوین شرایط استفاده از خدمات به زبان ساده، از مهم‌ترین مصادیق تکنیک‌های «تعیین قواعد» و «هشداردهی» در الگوی کلارک به شمار می‌روند و نقش مؤثری در پیشگیری از کلاهبرداری‌های سایبری دارند (عمرانی‌فر، ۱۴۰۳: ۸۸). افزون بر این، مشارکت رسانه‌ها، نظام آموزشی، دانشگاه‌ها، بانک‌ها، شرکت‌های فناوری و سازمان‌های مردم‌نهاد در ارتقای سواد دیجیتال، آموزش مسئولیت‌های حقوقی و اخلاقی، حفاظت از حریم خصوصی و امنیت اطلاعات، از الزامات سیاست جنایی پیشگیرانه است.

در مجموع، حذف بهانه‌های ارتکاب جرم آخرین حلقه زنجیره پیشگیری وضعی از کلاهبرداری سایبری است. هرچند این راهبرد به‌تنهایی در برابر مجرمان حرفه‌ای و سازمان‌یافته کفایت نمی‌کند، اما در پیشگیری از جرائم فرصت‌طلبانه و رفتارهای ناشی از ناآگاهی اثربخشی قابل‌توجهی دارد. مقایسه حقوق ایران و انگلستان نشان می‌دهد که هر دو نظام حقوقی بر اهمیت آموزش و آگاهی‌بخشی تأکید دارند، اما انگلستان با نهادینه‌سازی آموزش مستمر، مشارکت فعال بخش خصوصی، بهره‌گیری از هشدارهای هوشمند و تبیین شفاف مسئولیت‌های کاربران، در اجرای راهبرد «حذف بهانه‌های ارتکاب جرم» موفق‌تر عمل کرده است. ازاین‌رو، توسعه آموزش عمومی، ارتقای سواد دیجیتال و تقویت همکاری میان نهادهای دولتی، مدنی و ارائه‌دهندگان خدمات الکترونیکی، می‌تواند از مؤثرترین ابزارهای پیشگیری وضعی از کلاهبرداری سایبری در حقوق ایران باشد.

تحلیل تطبیقی	حقوق انگلستان	حقوق ایران	راهبرد پیشگیری وضعی
انگلستان با ترکیب مقررات، آموزش و استانداردهای فنی، توجیه جرم را بیشتر محدود کرده است.	هشدارهای مستمر، مسئولیت‌های شفاف و استانداردهای رفتاری اجرا می‌شود.	هشدارها و مقررات وجود دارد، اما شفافیت و انسجام کافی نیست.	حذف بهانه‌های ارتکاب جرم
انگلستان به عوامل فرهنگی و اجتماعی مؤثر بر پیشگیری توجه بیشتری دارد.	آموزش مستمر، کمپین‌های آگاهی‌بخشی و ارتقای سواد سایبری اجرا می‌شود.	آموزش و هشدارهای امنیتی پراکنده و فاقد سیاست منسجم است.	کاهش عوامل تحریک‌کننده
رویکرد انگلستان بر محروم‌سازی سریع مجرم از منافع اقتصادی استوار است.	انسداد فوری حساب‌ها، توقف تراکنش‌های مشکوک و بازیابی وجوه انجام می‌شود.	توقیف اموال و انسداد حساب‌ها عمدتاً پس از کشف جرم انجام می‌شود.	کاهش منافع حاصل از جرم
انگلستان از فناوری و همکاری نهادی گسترده‌تر برای کشف جرم بهره می‌برد.	همکاری پلیس، بانک‌ها و نهادهای امنیت سایبری با سامانه‌های هوشمند برقرار است.	پلیس فتا و ادله الکترونیکی فعال‌اند، اما چالش‌های فنی و بین‌المللی وجود دارد.	افزایش خطر کشف و دستگیری
هر دو بر افزایش هزینه ارتکاب جرم تأکید دارند، اما انگلستان رویکردی پیشگیرانه‌تر دارد.	امنیت از طریق طراحی، احراز هویت چندعاملی و استانداردهای فنی الزام‌آور اعمال می‌شود.	احراز هویت دومرحله‌ای و برخی الزامات امنیتی پیش‌بینی شده، اما استانداردهای جامع وجود ندارد.	سخت‌تر کردن ارتکاب جرم

جدول شماره ۱. جدول مقایسه تطبیقی راهبردهای پیشگیری وضعی از کلاهبرداری سایبری در حقوق ایران و انگلستان بر مبنای الگوی کلارک

مقایسه تطبیقی نشان می‌دهد که هرچند حقوق ایران و انگلستان در پذیرش اصول کلی پیشگیری وضعی و ضرورت کاهش فرصت‌های ارتکاب کلاهبرداری سایبری اشتراک دارند، تفاوت اساسی آن‌ها در فلسفه

مداخله و شیوه اجرای سیاست‌های پیشگیرانه است. در حقوق ایران، سیاست جنایی همچنان بر پاسخ کیفری پس از وقوع جرم و تعقیب مرتکبان متمرکز است؛ درحالی‌که در حقوق انگلستان پیشگیری وضعی به‌عنوان بخشی از حکمرانی امنیت سایبری، از مرحله طراحی زیرساخت‌های دیجیتال، تنظیم استانداردهای فنی، مسئولیت‌پذیری بخش خصوصی و آموزش مستمر شهروندان آغاز می‌شود. بنابراین، تجربه انگلستان نشان می‌دهد که کارآمدی پیشگیری وضعی در گرو تلفیق ابزارهای حقوقی، فنی، مدیریتی و آموزشی و مشارکت فعال نهادهای عمومی و خصوصی است؛ الگویی که می‌تواند در اصلاح سیاست جنایی پیشگیرانه ایران مورد بهره‌برداری قرار گیرد.

نتیجه‌گیری

پژوهش حاضر با هدف تبیین ظرفیت‌های پیشگیری وضعی در مقابله با کلاهبرداری سایبری و ارزیابی جایگاه آن در حقوق ایران با نگاهی تطبیقی به حقوق انگلستان انجام شد. بررسی‌ها نشان داد که با وجود توسعه روزافزون بسترهای ارتکاب کلاهبرداری‌های سایبری، پاسخ حقوق کیفری ایران همچنان عمدتاً بر واکنش‌های پسینی، جرم‌انگاری و مجازات مرتکبان استوار است؛ درحالی‌که پیشگیری وضعی، به‌عنوان یکی از مؤثرترین رویکردهای جرم‌شناختی، بر کاهش فرصت‌های ارتکاب جرم و افزایش هزینه و دشواری ارتکاب آن تمرکز دارد. ازاین‌رو، یافته اصلی پژوهش آن است که نظام حقوقی ایران هنوز نتوانسته است ظرفیت‌های پیشگیری وضعی را به صورت منسجم و نظام‌مند در سیاست جنایی تقنینی و اجرایی خود نهادینه کند. تحلیل الگوی پیشگیری وضعی کلارک نشان داد که بسیاری از تدابیر پنج‌گانه این نظریه، ازجمله افزایش دشواری ارتکاب جرم، افزایش خطر کشف، کاهش منافع حاصل از جرم، کاهش تحریکات و حذف بهانه‌های ارتکاب، قابلیت انطباق با جرائم سایبری را دارند. بااین‌حال، بررسی مقررات ایران بیانگر آن است که این اقدامات غالباً به صورت پراکنده و بدون چارچوب سیاستی مشخص در قوانین مختلف پیش‌بینی شده‌اند و فاقد سازوکار هماهنگ میان نهادهای قانون‌گذار، مراجع قضایی، ضابطان، بانک‌ها، ارائه‌دهندگان خدمات پرداخت و شرکت‌های فناوری هستند. بنابراین خلأ اصلی نه فقدان ظرفیت‌های قانونی، بلکه نبود سیاست جنایی پیشگیرانه مبتنی بر مدیریت فرصت‌های جرم است.

مطالعه تطبیقی حقوق انگلستان نشان داد که موفقیت این کشور در کنترل بخش قابل توجهی از جرائم سایبری صرفاً ناشی از شدت ضمانت اجراهای کیفری نیست، بلکه حاصل ترکیب مقررات الزام‌آور، استانداردهای امنیت سایبری، مسئولیت‌پذیری مؤسسات مالی و ارائه‌دهندگان خدمات دیجیتال، آموزش

مستمر کاربران و همکاری نزدیک میان بخش عمومی و خصوصی است. در این نظام، پیشگیری وضعی از مرحله سیاست‌گذاری تا اجرا در قالب الزامات فنی، نظارتی و مدیریتی دنبال می‌شود و همین امر موجب کاهش فرصت‌های ارتکاب کلاهبرداری سایبری شده است. مقایسه دو نظام حقوقی نشان می‌دهد که تفاوت اساسی ایران و انگلستان در سطح جرم‌انگاری نیست، بلکه در نوع سیاست جنایی است. درحالی‌که حقوق انگلستان از رویکردی پیشگیرانه، چندنهادی و مبتنی بر مدیریت ریسک بهره می‌گیرد، حقوق ایران همچنان رویکردی عمدتاً واکنشی و کیفری دارد. ازاین‌رو، توسعه پیشگیری وضعی مستلزم تغییر نگرش از «مجازات پس از وقوع جرم» به «کاهش فرصت‌های ارتکاب جرم پیش از وقوع» است.

بر این اساس، یافته‌های پژوهش از چند پیشنهاد تقنینی و اجرایی حمایت می‌کنند: نخست، تدوین مقررات جامع درباره الزامات امنیت سایبری برای بانک‌ها، مؤسسات مالی و سکوهای ارائه‌دهنده خدمات دیجیتال؛ دوم، الزام ارائه‌دهندگان خدمات پرداخت به استقرار سازوکارهای هوشمند کشف تقلب، احراز هویت چندمرحله‌ای و پایش مستمر تراکنش‌های پرخطر؛ سوم، ایجاد سازوکار قانونی برای تبادل سریع اطلاعات میان پلیس فتا، بانک مرکزی، بانک‌ها و شرکت‌های فناوری به منظور انسداد فوری بسترهای ارتکاب جرم؛ چهارم، توسعه آموزش عمومی و ارتقای سواد دیجیتال شهروندان به‌عنوان یکی از مؤلفه‌های حذف فرصت‌های جرم؛ و پنجم، پیش‌بینی مسئولیت‌های پیشگیرانه مشخص برای اشخاص حقوقی فعال در فضای سایبری در کنار مسئولیت کیفری مرتکبان.

در مجموع، پژوهش حاضر نشان می‌دهد که افزایش کارآمدی سیاست جنایی ایران در مقابله با کلاهبرداری سایبری، بیش از آنکه نیازمند جرم‌انگاری‌های جدید باشد، مستلزم گذار به سیاستی است که پیشگیری وضعی را به‌عنوان رکن اساسی حکمرانی امنیت سایبری به رسمیت بشناسد. بهره‌گیری هدفمند از تجربه حقوق انگلستان، با رعایت اقتضائات نظام حقوقی ایران، می‌تواند زمینه شکل‌گیری نظامی منسجم‌تر، کارآمدتر و آینده‌نگرتر برای کاهش فرصت‌های ارتکاب کلاهبرداری سایبری و ارتقای امنیت فضای تبادل اطلاعات را فراهم سازد.

فهرست منابع

ابراهیمی، شهرام (۱۳۹۷). **جرم‌شناسی پیشگیری**. جلد ۱. تهران: نشر میزان.

اصلانی، جبار و رنجبریان، امیرحسین (۱۳۹۴). «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل». **فصلنامه تحقیقات حقوقی**،دوره ۱۸، شماره ۷۱.

آگنج، مهرورز، شیخ الاسلامی، عباس و ولی پوری، معصومه (۱۴۰۲). «سیاست جنایی ایران و انگلیس در پیشگیری از وقوع جرائم سایبری». **فقه جزای تطبیقی**، دوره ۳، شماره ۳.

خادم‌پور مشهدی، مانا و نیک‌فرجام شیرازی، کاوه (۱۴۰۳). «فیشینگ و حقوق حریم خصوصی: بررسی تقابل امنیت دیجیتال با آزادی‌های فردی». **حقوق سایبری**، دوره ۱، شماره ۳.

رستمی، هادی (۱۳۹۸). «کلاهبرداری رایانه‌ای؛ تأملی بر ارکان جرم و آثار آن». **آموزه‌های حقوق کیفری**، دوره ۱۶، شماره ۱۸.

زارعی‌نژاد، فرهاد، ملکشاه، آرزو و رضی، پوریا (۱۴۰۵). «چالش‌های مسئولیت مدنی در فضای مجازی در حقوق ایران و انگلستان». **پژوهش‌های نوین در مطالعات علوم انسانی اسلامی**، دوره ۵، شماره ۹.

شمسی، رضا؛ حبیبی، سیده زهرا؛ گل‌خندان، سمیرا و رجبی، اکبر (۱۴۰۴). «میزان بهره‌گیری از آموزه‌های نظریه کنترل برای مقابله با جرائم رایانه‌ای در سیاست جنایی ایران». **فقه جزای تطبیقی**، دوره ۵، شماره ۲.

صبح‌خیز، رضا (۱۳۹۴). «چالش‌های حقوقی جرائم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران». **پژوهش‌های اطلاعاتی و جنایی**، دوره ۱۰، شماره ۳.

عمرانی‌فر، عدنان (۱۴۰۳). «بایسته‌های «ایراد اتهام» در حقوق انگلستان و امکان‌سنجی تأسیس آن در حقوق ایران». **فصلنامه علمی مطالعات حقوق بشر اسلامی**، دوره ۱۳، شماره ۳.

عمرانی‌فر، عدنان و بیرنگ، یگانه (۱۴۰۵). «پیشگیری وضعی از جرائم مرتبط با رمزارزها در حقوق ایران (با تأکید بر الگوی کلارک)». **مطالعات فقه و حقوق رسانه**، دوره ۸، شماره ۱.

غنی، مهرداد؛ حسینی، سید حسین و سیدزاده‌ثانی، سید مهدی (۱۴۰۴). «تحلیل نقش دولت و حاکمیت؛ جامعه مدنی و مشارکت مردمی در پیشگیری از جرائم اقتصادی». **پژوهش‌های جرم‌شناسی کاربردی**، دوره ۳، شماره ۸.

قدسی، ابراهیم؛ قلیزاده، بهروز و شیخ‌اسلامی، عاطفه (۱۴۰۰). «پیشگیری از تکرار جرم با حفظ کرامت انسانی بزهکار با نگاهی به آموزه‌های جرم‌شناختی». **پژوهش‌های حقوقی**، دوره ۲۰، شماره ۴۵.

کاوه، محمدهادی و بارانی، محمد (۱۴۰۴). «به‌کارگیری هوش مصنوعی برای مقابله با جرائم رایانه‌ای و بهبود عملکرد امنیت سایبری». **فقه جزای تطبیقی**، دوره ۵، شماره ۱.

مجیدی، سید محمود (۱۴۰۰). «آسیب‌شناسی سیاست کیفری ماهوی ایران در قبال بزه جاسوسی». **مجلس و راهبرد**، دوره ۲۸، شماره ۱۰۵.

Reference

Atkinson, R. D, & McKay, A. S (2007). Digital prosperity: Understanding the economic benefits of the information technology revolution. Information Technology and Innovation Foundation. SSRN.

Button, M, Lewis, C, & Tapley, J (2010). Fraud typology and victims of fraud. University of Portsmouth.

Cabinet Office (2009). Cyber security strategy of the United Kingdom. HM Government.

Calzavara, S, Tolomei, G, Casini, A, Bugliesi, M, & Orlando, S (2015). A supervised learning approach to protect client authentication on the web. ACM Transactions on the Web, 9(1), 1–30.

Chohan, U. W (2021). Cryptocurrency: A theoretical perspective. SSRN Electronic Journal.

Clarke, R. V, & Eck, J. E (2003). Become a problem-solving crime analyst in 55 steps. Jill Dando Institute of Crime Science, University College London.

Council of Europe (1990). Recommendation No. R(89)9 on computer-related crime. Strasbourg, France.

Derry v Peek, 14 App. Cas. 337 (H.L. 1889).

Fisher, J (2016). Fraud in civil and criminal law. In B. Rider (Ed.), Research handbook on international financial crime. Edward Elgar Publishing.

Gardner, T. J, & Anderson, T. M (2009). Criminal law (10th ed). Thomson Publishing.

Garofalo, J (2020). The role of social institutions in crime prevention: A crosscultural perspective. Journal of Crime and Justice Studies, 45(2), 65-85.

Gercke, M (2009). Understanding cybercrime: A guide for developing countries. International Telecommunication Union (ITU).

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

Junaidu Bello Marshall, E, & Saulawa, E. M. A (2015). Cyber attacks: The legal response. International Journal of International Law, 1(2).

Kuhlhorn, E (2005). Housing allowances in a welfare society. In R. V. Clarke (Ed.), Situational crime prevention: Successful case studies (2nd ed). Harrow and Heston.

Marion, N. E, & Twede, J (2020). Cybercrime: An encyclopedia of digital crime (1st ed). ABC-CLIO.

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

Newman, G, & Marongiu, P (2016). Situational crime prevention and the utilitarian theories of Jeremy Bentham. In G. Newman, R. V. Clarke, & S. G. Shoham (Eds.), Rational choice and situational crime prevention: Theoretical foundations. Routledge.

Rowland, D, Kohl, U, & Charlesworth, A (2017). Information technology law (5th ed). Routledge.

Schneider, F. M, & Leung, L (2022). Social media and communication: The changing dynamics of online interactions. New Media & Society, 24(3), 451–468.

Slapper, G, & Kelly, D (2010). The English legal system (11th ed). Routledge-Cavendish.

Xiao, R, et al (2018). Attacking network isolation in software-defined networks: New attacks and countermeasures. In Proceedings of the International Conference on Computer Communications and Networks (ICCCN).

Zhang, Z (2021). Research on legal risks of legal digital currency. Unpublished manuscript.