Rasanch \ A Quarterly Journal of Media Studies and Research
http//qjmn.farhang.gov.ir DOI: 10.22034/bmsp.2024.455646.2025
Research paper Received: 4/5/2024
Vol. 36, No. 1, Spring 2025, Issue 4 Accepted: 24/7/2024

Requirements for Determining Punishment for Computer Crimes in the Iranian Legal System

Mehdi Mozaffari Anari: PhD Student in Criminal Law and Criminology, Faculty of Law and Political Science, University of Tehran (Corresponding Author), Tehran, Iran. **email:** mahdi.mozafari@ut.ac.ir

Reza Zahravi: Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, University of Tehran, Tehran, Iran. **email:** rezazahravi@ut.ac.ir

Computer crimes are crimes unique to computer spaces and electronic data, which can also go beyond the borders of a country and find an extraterritorial and international description. This type of crime, while being committed in a limited space, may have irreparable effects and even target a country or several parts of the world. In order to effectively deal with this type of crime, the legislator passed the Electronic Commerce Law in 2003 and then the Computer Crimes Law in 2009. Considering the existing regulations, although such a measure itself was necessary and essential, determining punishment for computer crimes without scientific attention and consideration of all important and strategic requirements and principles will not be fruitful. The present study, which was written using an analytical-applied method and using library resources, seeks to present the requirements governing the determination of punishment for this type of crime, by separating negative from positive requirements, in such a way that the legislator, in the capacity of punisher, can take steps towards effectively combating computer crimes by taking these requirements into account and reducing the inefficiency of existing punishments. The purpose of this study is to attempt to formulate extra-legislative requirements that, with a more complete view and based on existing principles, objectives, and realities, improve the situation of punishment for crimes in this area.

Keywords: Computer Crimes, Computer, Determination of Punishment, Negative Requirements, Positive Requirements.

How to cite this paper: Mozafari Anari, M., & Zahravi, R. (2025) . Requirements for Determining Punishment for Computer Crimes in the Iranian Legal System. *Rasaneh*, 36(1), 123-145. **[In persian]**

رسانه / فصلنامه مطالعاتی و تحقیقاتی وسایل ارتباط جمعی
Rasanch
نوع مقاله: پژوهشی
DOI: 10.22034/bmsp.2024.455646.2025
http//qjmn.farhang.gov.ir
Vol. 36, No. 1, Spring 2025

الزامات تعیین کیفر در جرایم رایانه‌ای در نظام حقوقی ایران

نوشتهٔ
مهدی مظفری اناری*
رضا زهروی**

تاریخ دریافت: ۱۴۰۳/۰۲/۱۵
تاریخ پذیرش: ۱۴۰۳/۰۵/۰۳

چکیده

جرایم رایانه‌ای، جرایمی منحصر به فضاهای رایانه‌ای و داده‌های الکترونیکی به‌شمار می‌آیند که درعین‌حال می‌توانند از مرزهای یک کشـــور نیز فراتر رفته و وصفی فراســـرزمینی و بین‌المللی پیدا کنند. این‌گونه جرایم، در عین ارتکاب در فضایی محدود، ممکن اســـت آثار جبران‌ناپذیری به‌بار آورده و حتی یک کشور یا چندین نقطه از جهان را متوجه خود ســـازند. به‌منظور مقابلهٔ مؤثر با این‌گونه جرایم، قانون‌گذار در سال ۱۳۸۲ قانون تجارت الکترونیک و پس‌ازآن در ســـال ۱۳۸۸ قانون جرایم رایانه‌ای را به‌تصویب رســـانده است. با ملاحظهٔ مقررات موجود، هرچند نفس چنین اقدامی لازم و ضروری بوده اســـت، اما تعیین کیفر برای جرایم رایانه‌ای بـــدون توجـــه و ملاحظهٔ علمی همهٔ الزامات و اصول مهم و راهبـــردی، مثمرثمر نخواهد بود. پژوهش حاضر که با روش تحلیلی ـ کاربردی و با بهره‌گیری از منابع کتابخانه‌ای نگارش یافته‌اســـت، درصدد اســـت الزامات حاکـــم بر تعیین کیفر در این‌گونه جرایم را، با تفکیک الزامات ســـلبی از ایجابی، به‌گونه‌ای ارائه کند که مقنن بتواند در مقام کیفرگذاری، با عنایت به این الزامات، در مســـیر مقابلهٔ مؤثر با جرایم رایانه‌ای گام بردارد و از ناکارآمدی کیفرهای موجود بکاهد. هدف از این پژوهش، تلاش در جهت تدوین الزاماتی فراتقنینی است که بـــا نگاهی کامل‌تر و مبتنی بر اصول، اهداف و واقعیت‌هـــای موجود، وضعیت کیفرگذاری برای جرایم مطرح در این گستره را بهبود بخشد.

کلیدواژه: جرایم رایانه‌ای، رایانه، تعیین کیفر، الزامات سلبی، الزامات ایجابی.

* دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران (نویسندهٔ مسئول)، تهران، ایران Mahdi.mozafari@ut.ac.ir
** استادیار گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
Rezazahravi@ut.ac.ir

نحوهٔ اســـتناد به این مقاله: مظفری اناری، مهدی و زهروی، رضا (۱۴۰۴). الزامات تعیین کیفر در جرایم رایانه‌ای در نظام حقوقی ایران. رسانه، ۳۶(۱)، ۱۲۳-۱۴۵.

مقدمه

در عصر حاضر فناوری‌های دیجیتال در جای‌جای زندگی انسان نقش‌آفرینی کرده که شاهد ماشینی‌شدن ارتباطات و تعاملات شهروندان هستیم. «تسلط هژمونیک ابزارهای هوشمند بر زندگی افراد زمانی بیشتر خود را نشان می‌دهد که ازیک‌طرف شرکت‌های سازنده، جهت به‌دست‌آوردن سهم بازار خود، سالانه حجم انبوهی از تلفن همراه را تولید و روانهٔ بازار می‌کنند و ازطرف‌دیگر هرکدام از کاربران نیز در تکاپو برای خرید آن محصولات هستند» (شاملو و همکاران، ۱۴۰۳: ۹۲). در کنار آن باید گفت شبکه‌های اجتماعی بخش عمده‌ای از ارتباطات انسانی دنیای پیچیدهٔ امروز را تشکیل می‌دهند که در عین فراهم‌کردن فرصت‌های مغتنم برای ارتقای علمی و افزایش آگاهی‌های سیاسی، اقتصادی، فرهنگی و اجتماعی، آسیب‌های نوظهوری نیز داشته‌اند که از روابط زناشویی تا کسب‌وکار شهروندان را تحت تأثیر قرار داده است (نیازی و همکاران، ۱۴۰۳: ۵۹). جرایم ارتکابی در این فضا نیز به‌تبع متمایز بوده و در مقایسه با جرایم سنتی، ماهیت و ویژگی‌های منحصربه‌فردی دارند که قانون‌گذاری و تعیین کیفر در قبال آن‌ها را بسیار دشوار ساخته است. یکی از مهم‌ترین ویژگی‌های این دسته از جرایم، نوظهوربودن آن‌هاست. در واقع، عمر جرایم رایانه‌ای در سراسر جهان به بیش از ۳۰ سال نمی‌رسد (برنر[1]، ۲۰۰۴: ۸). این در حالی است که جرایم سنتی سابقه و پیشینهٔ طولانی‌تری دارند و قوانین و رویکردهای مدون و شناخته‌شده‌ای برای مقابلهٔ با آن‌ها وجود دارد. عامل دیگر که تحلیل حقوقی جرایم رایانه‌ای را بسیار دشوار کرده است، سرعت شگفت‌انگیز تغییرات فناورانه در محیط دیجیتال است. همان‌گونه که اشاره شد، فناوری‌های دیجیتال با سرعتی بی‌سابقه در حال تحول هستند (کلاف[2]، ۲۰۱۵: ۶). این تغییرات مداوم، پیش‌بینی و تنظیم حقوقی را برای قانون‌گذار بسیار دشوار ساخته است، به‌طوری‌که بسیاری از مفاهیم و مدل‌های متداول در حقوق کیفری سنتی در محیط دیجیتال کارایی ندارند و نیاز به بازتعریف دارند. (والدن[3]، ۲۰۱۶: ۲۳). علاوه‌بر موارد فوق، تفاوت ماهوی جرایم رایانه‌ای با جرایم سنتی نیز از دیگر عوامل دشواری تحلیل حقوقی این دسته از جرایم است. برای مثال، بسیاری از مفاهیم اساسی در حقوق کیفری هم‌چون "مکان ارتکاب جرم"، "آثار جرم" و "هویت مجرم" در جرایم رایانه‌ای به‌صورت متفاوتی تعریف می‌شوند (کلاف، ۲۰۱۵: ۴۲-۴۵). این تفاوت‌های ماهوی مانع از کارایی رویکردهای سنتی در قبال این دسته از جرایم است. با توجه به چالش‌های پیش‌گفته، اتکای صرف به رویکردها و مدل‌های متداول در حقوق کیفری سنتی برای قانون‌گذاری و تعیین کیفر در حوزهٔ جرایم رایانه‌ای چندان مناسب نیست. در این

1. Brenner
2. Clough
3. Walden

راســتا، ضرورت اتخاذ رویکردی نوین و خلاقانه احساس می‌شــود که مبتنی‌بر شناخت دقیق ابعاد و ماهیت این دســته از جرایم باشــد (والدن، ۲۰۱۶: ۱۵). قانون‌گذار باید با بررســی دقیق ویژگی‌های منحصربه‌فرد جرایم رایانه‌ای، نســبت‌به طراحی و تدوین مقررات و سازوکارهای حقوقی کارآمد و منطبق با این حوزه اقدام کند. این امر می‌تواند شامل ایجاد نهادهای تخصصی، تدوین قوانین پویا و انعطاف‌پذیر و هم‌چنین ارائهٔ مجازات‌های کیفری متناسب با این دسته از جرایم باشد (وال[1]، ۲۰۰۷: ۸۷-۹۲).

در نظــام حقوقی ایران مســتند جرم‌انگاری جرایم رایانه‌ای در قالــب خاصی به نام قانون جرایم رایانه‌ای نهادینه شــده است که البته سابقهٔ توجه به این مقولهٔ مهم از سال ۱۳۸۰ هجری شمســی در نظام حقوقی ایران مدنظر مقنن قرارگرفته اســت. این جرایم بنا به اقتضای خود که لازم است در بستر فضای رایانه‌ای ارتکاب یابند، شرایط و کیفیت خاصی داشته و به‌همین‌جهت پاسخ‌شناســی کیفری و مقابلهٔ مؤثر با آن نیز می‌بایســت متناســب با اقتضائات خاص این‌گونه جرایم مدنظر قرار گیرد که در واقع امر، شاهد خلأ توجه به این موضوع هستیم. پژوهش حاضر درصدد آسیب‌شناســی کیفرگذاری در جرایم رایانه‌ای بــوده و الزامات حاکم بر تعیین کیفر در این‌گونه جرایم موردبررســی و تدوین قرار می‌گیرد؛ امری که در برخی پژوهش‌های ســابق تا حدود قابل‌ملاحظه‌ای مغفول مانده است.

در ادامه، نخست به مفهوم‌شناسی و مبانی نظری مرتبط با جرایم رایانه‌ای پرداخته می‌شود. ســپس به تبیین جرایم رایانــه‌ای در نظام حقوقی ایران خواهیم پرداخــت و در انتها با نگاهی آسیب‌شناسانه به ارائهٔ الزامات حاکم‌بر تعیین کیفر در این جرایم اشاره می‌شود.

مفهوم‌شناسی و مبانی نظری جرایم رایانه‌ای

به‌منظور آسیب‌شناسی مؤثر کیفری در جرایم رایانه‌ای لازم است مفهوم‌شناسی اجمالی از جرم رایانه‌ای در نظام حقوقی ایران صورت پذیرد و به مبانی نظری مرتبط با موضوع پرداخته شــود تا تعیین الزامات حاکم بر تعیین کیفر، متناسب، کارآمد و هدفمند باشند. به همین منظور در این بخش به تعاریف ناظر بر جرایم رایانه‌ای، فراســرزمینی بودن جرایم رایانه‌ای، شناخت تفاوت جرایم رایانه‌ای با سایر اصطلاحات و در نهایت انواع کیفر در این جرایم پرداخته می‌شود.

تعریف جرایم رایانه‌ای

جرایم رایانه‌ای، جرایمی مقید به فضا و ابزار خاص به‌شمار می‌روند که به‌ضرورت می‌بایست در فضــای رایانه و از طریق داده‌های الکترونیکی ارتکاب یابند. تحولات فناوری و گســترش ارتباطات در فضای رســانه‌ای و مجازی، ســهولت وقوع جرم را نیز دوچندان کرده و مرتکبان،

1. Wall

فضایی مناسب جهت تحقق‌بخشیدن به انگیزه‌های مجرمانهٔ خویش می‌یابند. برای جرایم رایانه‌ای تعاریف متعددی به چشم می‌خورد؛ در تعریفی جرم رایانه‌ای به هر جرم و جنایتی گفته می‌شود که از رایانه و شبکه به‌عنوان ابزاری جهت انجام آن جرم استفاده شده است (مور[1]، ۲۰۰۵: ۳۲). در تعریف دیگری نیز ارتکاب جرم در یک محیط الکترونیکی برای منافع اقتصادی یا آسیب‌رساندن به دیگران، جرم رایانه‌ای نامیده شده است (ساموئل[2]، ۲۰۰۸: ۱۶). در یک‌کلام می‌توان جرایم رایانه‌ای را هرگونه رفتار مجرمانه‌ای دانست که بنا به اقتضای خاص خود قابلیت ارتکاب در فضای رایانه‌ای را داشته باشد و باید در این فضا رقم خورد؛ چراکه برخی جرایم در اصل قابلیت ارتکاب در فضایی غیر از فضای حقیقی را نخواهند داشت؛ جرایمی چون قتل، آدم‌ربایی، ترک انفاق و سقط‌جنین نمونهٔ این جرایم به‌شمار می‌روند. در همین خصوص لازم است به تعاریف مضیق و موسع جرم رایانه‌ای پرداخته شود.

تعریف مضیق جرم رایانه‌ای

در تعریف مضیق جرم رایانه‌ای، این جرم تنها شامل جرایمی می‌شود که رفتار تعریف شده در رکن مادی آن‌ها مقید به‌وسیلهٔ رایانه است و یا به‌طور حتم در محیط مجازی رایانه‌ای ارتکاب می‌شود مانند دسترسی غیرمجاز یا شنود غیرمجاز؛ به‌عبارت‌بهتر هر جرمی که مقنن در تعریف رکن مادی آن، رایانه را موضوع یا وسیلهٔ ارتکاب جرم دانسته باشد.

تعریف موسع جرم رایانه‌ای

در تعریف موسع حتی اگر رایانه در فرایند ارتکاب جرم نقشی (هرچند کوچک و اتفاقی بدون ملازمهٔ عقلی یا قانونی) داشته باشد و بتوان مصادیقی از آن جرم را بدون رایانه نیز مرتکب شد، جرم رایانه‌ای رقم می‌خورد که از این لحاظ جرایم عادی هم‌چون جعل و کلاهبرداری نیز می‌توانند رایانه‌ای تلقی شوند. به‌نظر می‌رسد قانون‌گذار در قانون جرایم رایانه‌ای از تعریف موسع دنباله‌روی کرده است.

تفاوت جرایم رایانه‌ای، کامپیوتری، اینترنتی و سایبری

در نوشتگان حقوقی مرتبط با رایانه و در منابع آموزشی و پژوهشی، در کنار اصطلاح جرم رایانه‌ای، با اصطلاحاتی چون جرم کامپیوتری، اینترنتی یا سایبری نیز برخورد کرده‌ایم که این‌ها در مقام نظری تفاوت‌هایی دارند. البته باید گفت که دو اصطلاح رایانه و کامپیوتر از منظر لغوی معادل هم به‌شمار آمده و اولی فارسی و دومی انگلیسی است و بنابراین از این

1. Moore
2. Samuel

حیث تفاوت آشـکاری ندارند. هرچند در برخی موارد رایانه تنها به کامپیوتر اطلاق نمی‌شـود بلکـه هر ابـزاری که پردازش داده‌ها را انجام می‌دهد، رایانه خواهد بود و بنابراین رابطهٔ عموم و خصوص مطلق برقرار می‌گردد هم‌چون تلفن همراه.

سـایبر نیز فضای ناشـی از اینترنت و اتصال رایانه‌های مختلف به هم خواهد بود؛ به تعبیر بهتر سـایبر محصول اینترنت و اینترنت محصول ارتباط رایانه‌ها با یکدیگر است. براین‌اساس تفاوت جرایم رایانه‌ای از سـایبری بازشـناخته می‌شـود؛ جرایم سـایبری فقط در بستر شبکهٔ جهانـی اینترنت و اتصـال رایانه‌ها به هم قابل تحقق‌اند اما جرایـم رایانه‌ای لزومی به اتصال شـبکهٔ اینترنت ندارند هم‌چون تولید یا انتشـار نرم‌افزارهایی برای ارتکاب جرم که به‌صورت بـدون خط نیز قابل انجام اسـت (موضوع مـادهٔ ۷۵۳ قانون تعزیرات). براین‌اسـاس در اینجا نیـز با رابطهٔ عمـوم و خصوص مطلق مواجه خواهیم بود هرچند مصادیق مشـترکی نیز وجود دارد و به‌عنوان نمونه عدم پالایش محتوای مجرمانه از ناحیهٔ ارائه‌دهندگان خدمات دسترسـی و میزبانـی فقط در بسـتر اینترنت مطرح اسـت (موضوع مواد ۷۴۹ و ۷۵۱ قانـون تعزیرات). (حبیـب‌زاده، ۱۳۹۵: ۱) بااین‌همه قانون‌گذار در سـال ۱۳۸۸ از اصطلاح جرایم رایانه‌ای برای عنوان قانون مرتبط با این حوزه نام برده اسـت اما لازم است تفاوت‌ها و وجوه افتراق سایبر و رایانه بازشناخته شود تا خلط مبحث صورت نپذیرد.

فراسرزمینی بودن جرایم رایانه‌ای

جرایـم رایانـه‌ای با عنایت به اتصال شـبکهٔ جهانی اینترنت و پیوسـتگی آن در سراسـر دنیا، جرایمی از دو حیثیت فراسرزمینی قلمداد می‌شوند: از حیث ثبوتی و اثباتی.

۱. ثبوتی یعنی از حیث محل وقوع رکن مادی جرم؛ امروزه مجرمین رایانه‌ای می‌توانند فارغ از مرزهای ملی یک کشـور، به ارتکاب جرم بپردازند. از این‌رو جرایم رایانه‌ای به‌راحتی در مقیاس بین‌المللی ارتکاب می‌شوند.

۲. اثباتی یعنی از حیث ادلهٔ وقوع جرم؛ ازطرف‌دیگر امروزه ادلهٔ جرایم نیز در بسیاری از موارد از نوع ادلهٔ اینترنتی هستند که در شبکه‌های دادهٔ خارجی ذخیره می‌شوند. در نتیجه تعقیب این جرایم و انجام تحقیقات کیفری پیرامون آن‌ها مستلزم دسترسی به داده‌های فراسرزمینی است. از این‌رو دولت‌ها برای دسترسی به داده‌های فرامرزی ناگزیر از همکاری با یکدیگر از طریق معاضدت قضایی متقابل هستند (عبدی‌پور و همکاران، ۱۳۹۹: ۱۵۸).

خصلت فراسرزمینی این جرایم می‌تواند دو اثر بسیار مهم را در روند مطالعه و بررسی آن ایجاب کند؛ اول این‌که رسیدگی به این‌گونه جرایم نیازمند همکاری و تعاون قضایی بین‌المللی و انعقاد موافقت‌نامه‌های همکاری متقابل بین کشورهاسـت تا در عرصهٔ مقابلهٔ مؤثر با باندها و شـبکه‌های گسـتردهٔ ارتکاب جرایم رایانه‌ای، اقدام متناسبی صورت پذیرد و بزهکاران به‌زعم

خویــش فضای رایانه‌ای را محیطی امــن جهت ارتکاب اعمال مجرمانهٔ خــود قلمداد نکنند. دوم این‌که فراســرزمینی بودن این اثر را خواهد داشــت که قانون‌گذاران کشورهای مختلف از تجربیات و دســتاوردهای یکدیگر بهره برده و در روند پاسخ‌شناســی و مقابلهٔ کیفری مؤثر از دیدگاه‌ها و آموزه‌های کیفری سایر ملل دنیا نیز استفاده کنند. در حقیقت در باب جرایم رایانه‌ای می‌تــوان قائل به لزوم وحدت حقوقی بــود و هرقدر قوانین و مقررات ناظر بر جرایم رایانه‌ای در عرصهٔ بین‌المللی نزدیکی و وحدت یابند، امکان برخورد و پیشگیری مؤثر از جرایم به نحو بارزی افزایش پیدا می‌کند.

انواع کیفر در جرایم رایانه‌ای

هنگامی‌که جرم به‌عنوان رفتاری ضداجتماعی ارتکاب می‌شــود، حاکمیت عمومی وظیفه دارد با توســل به شــیوه‌های مناسب و مؤثر، ضمن پیشــگیری از وقوع و تکرار جرم در آینده، لزوم احترام به احکام و دستورات خود را به شهروندان گوشزد کند. هشدار مقامات عمومی به حفظ نظم عمومی و رعایت مقررات و حقوق جامعه بیان گوناگونی دارد که صورت مؤکد آن اجرای مجازات است (اردبیلی، ۱۳۹۹، ج ۳: ۱۷). بنابراین در ارتکاب یک رفتار خلاف قانون کیفری، پاســخ و مقابلهٔ کیفری در کنار ســایر پاســخ‌ها ضرورت پیدا می‌کند. این گزاره خود واجد دو مفهوم ایجابی و سلبی است. ایجابی ازاین‌جهت که هر جرمی می‌بایست مورد واکنش اجتماعی (مجازات یا اقدامات تأمینی و تربیتی) قرار گیرد و ســلبی ازاین‌جهت که نمی‌توان اعمال کیفر را بیش‌ازحد تناسب و ضرورت و در معنای موسع خود به‌کار برد که این تأثیر معکوس داشته و آسیب‌ها بر مزایا فزونی پیدا می‌کند. در جرایم رایانه‌ای نیز بدون شک کیفر رکنی رکین به شمار می‌رود. در حقیقت جرم و مجازات وابستگی تنگاتنگی باهم داشته و تا برای رفتاری مجازاتی تعریف و اعلام نشــود، آن رفتار در قلمرو کنترل دولتی قهرآمیــز قرار نمی‌گیرد (منصورآبادی، ۱۳۹۹: ۲۶۷). در خصوص جرایم رایانه‌ای با عنایت به جرم‌انگاری در قانون کیفری، بی‌درنگ مجازات نیز موردتوجه قرارگرفته و در رابطه با هر یک از عناوین مجرمانه، تعیین کیفر صورت پذیرفته اســت. نکتهٔ حائز اهمیت این اســت که فارغ از لزوم تعیین کیفر برای جرایم رایانه‌ای، تناســب و توجه بــه اوصاف خاص و کیفیات مختصهٔ هر عنــوان مجرمانه مدنظر مقنن نبوده و کیفرهــا به‌طــور عمده از وصفی واحد و نزدیک به هم تبعیــت کرده‌اند. چنان‌که حبس و جزای نقــدی دو مجــازات عمده و اصلی در قانون جرایم رایانه‌ای به‌شــمار می‌آیند؛ به‌عنوان‌مثال در مــادهٔ ۷۳۶ قانون تعزیرات بخش جرایم رایانه‌ای، مجازات جرم تخریب و اخلال در داده‌ها یا ســامانه‌های رایانه‌ای و مخابراتی حبس از شــش ماه تا دو ســال یا جزای نقدی از بیست‌وپنج میلیون تا صد میلیون ریال یا هر دو مجازات پیش‌بینی شده است و یا در مادهٔ ۷۴۲ همین قانون در خصوص انتشار، توزیع، معامله، ذخیره یا نگهداری محتویات مستهجن به‌وسیلهٔ سامانه‌های

رایانــه‌ای یا مخابراتی یا حامل‌های داده، مجازات حبس از نودویک روز تا دو ســال یا جزای نقدی از پانزده میلیون تا صد میلیون ریال یا هر دو مجازات پیش‌بینی شــده است. این ملاحظهٔ اجمالــی حکایت از ایــن دارد که تعیین کیفر، بدون توجه به ماهیت جــرم و فضای ارتکابی و اقتضائات خاص این فضا، مدنظر قرارگرفته است. حتی در جرایم علیه عفت و اخلاق عمومی در فضای حقیقی مجازاتی کمتر از این جرم در فضای مجازی مقرر بوده اســت؛ که این امر در برخی موارد قابل‌نقد به‌نظر می‌رســد، البته فقط در مواردی که گسترهٔ آثار جرم رایانه‌ای گسترده نبوده و محدود به چند فرد حقیقی بزرگسال باشد وگرنه در مواردی که گستره موسع باشد کیفر اشــد به‌طور طبیعی منطقی و قابل‌دفاع است، به‌عنوان نمونه در مادهٔ ۶۴۰ قانون تعزیرات همین رفتارهای مجرمانه با مجازات ســه ماه تا یک‌سال حبس و جزای نقدی از بیست تا صد میلیون ریال و تا (۷۴) ضربهٔ شــلاق یا یک یا دو مجازات مذکور روبرو شــده است. این نگاه در موارد محــدود بــه اثر مضیق، نگاهی تشــدیدگرایانه بوده و نگرش قانون‌گذار بــدون توجه به فضای ارتکابی و شــرایط خاص و تناسب‌بخشی بین پاسخ کیفری و جرم ارتکابی، فاقد توجیه بوده و لــزوم دقت‌نظر در تعیین کیفر در این عرصه را دو چندان می‌کند. چنان‌که در پژوهش حاضر در پی تعیین الزامات کیفرگذاری در این‌گونه جرایم هستیم.

الزامات کیفرگذاری در جرایم رایانه‌ای

به‌طورکلی، پاســخ قانونی به‌مقولهٔ جرم در چارچوب مشــخص و مدون کیفر نامیده می‌شــود. چنان‌که عنصر قانونی هر جرمی ناگزیر از دو رکن اساســی تعریف جرم و تعیین ضمانت اجرا (کیفر) است. به‌عبارت‌دیگر «بدون وجود گونه‌ای سازوکار برای الزام در به‌کارگیری هنجارهای قانونی، به‌سختی می‌توان سخن از نظام قانونی به میان آورد» (الهام و برهانی، ۱۳۹۸، ج ۲: ۱۵). در حقیقت کیفر نقشــی کلیدی و تعیین‌کننده به‌عنوان برنده‌ترین و آماده‌ترین سلاح حکومت‌ها در مبارزهٔ مؤثر و قاطع با جرایم در سطح داخلی و بین‌المللی دارد (صفاری، ۱۳۹۸: ۷). بنابراین به‌منظور جامهٔ عمل پوشــاندن به این مهم در نظام عدالت کیفری، جرم‌انگاری عناوین مجرمانه لازم است همگام با کیفرگذاری متناسب صورت پذیرد. در واقع مقنن در محل جرم‌انگاری لازم است مبتنی‌بر اصول و معیارهایی که دارد، کیفر مناسب و مقتضی برای عنوان مجرمانه برگزیند که این فرآیند انتخاب و تعیین کیفر را در اصطلاح کیفرگذاری می‌نامند (پیوندی، ۱۳۹۲: ۱۸). در جرایم رایانه‌ای با عنایت به مطالب پیش‌گفته ضرورت نگاه علمی و کارشناسانه به مقولهٔ تعیین کیفر دوچندان بوده و نیازمند دقت نظر و تأملی درخور اســت. به همین منظور الزامات ســلبی و ایجابی ناظر بر کیفرگذاری در این‌گونه جرایم موردبررســی قرار گرفته تا مقنن در پرتوی این الزامات، در تعیین کیفر متناسب و کارآمد نقش خویش را به‌درستی ایفا کند.

الزامات سلبی

در این قسمت از نوشتار مبتنی‌بر آسیب‌شناسی وضع موجود، الزامات سلبی ناظر بر کیفرگذاری جرایم رایانه‌ای مورد پیشنهاد قرار گرفته و کاربست این الزامات به قانون‌گذار توصیه می‌شود.

پرهیز از اتخاذ رویکرد سخت‌گیرانه و مطلق‌گرا در تعیین کیفر

رفتارهای مجرمانه در جرایم رایانه‌ای اقتضا دارد که رویکرد خاصی نسبت‌به این‌گونه جرایم صورت گیرد. بنابراین قانون‌گذار نمی‌بایست در قبال این‌گونه جرایم، رویکردی سخت‌گیرانه و مطلق‌گرا اتخاذ کند. این دسته از جرایم ماهیتی پیچیده و ظریف دارند و نیازمند برخورد هوشمندانه و متوازن هستند (برنر، ۲۰۰۴: ۴۵-۴۸). در نروژ، قانون جرایم سایبری ۲۰۱۳ با رویکردی متوازن و هوشمندانه تدوین شده است. این قانون ضمن تأکید بر پیشگیری و آموزش، مجازات‌های متناسب را برای جرایم سایبری در نظر گرفته است (برنر، ۲۰۰۴: ۴۷). هم‌چنین در کشور کانادا، قانون جرایم رایانه‌ای ۲۰۱۵ از رویکرد سخت‌گیرانه اجتناب کرده و بر اصول تناسب و فردی‌سازی مجازات تأکید دارد. در نظام حقوقی ایران در قانون جرایم رایانه‌ای به‌طورمعمول شاهد توجه بیش‌ازپیش مقنن به حبس به‌عنوان مصداق اَجلای رویکرد سخت و مطلق‌گرا هستیم. در حقیقت بسیاری از رفتارها از دسترسی غیرمجاز گرفته تا سرقت داده‌ها و ... با مجازات حبس روبه‌رو شده‌اند و هیچ‌گونه تمایزی به‌چشم نمی‌خورد. در نکوهش مجازات حبس توجیهات بسیاری وجود دارد؛ از نگاه نظریهٔ برچسب‌زنی در جرم‌شناسی مجازات حبس تأثیرات نامطلوبی بر مجرم زندانی داشته و در انطباق او با انگ مجرمانه می‌افزاید. اساس این نظریه را باید در دیدگاه‌های اِدمینگ لی‌مرت تحت عنوان "آسیب‌شناسی اجتماعی" جست‌وجو کرد. لی‌مِرت مبتنی‌بر دیدگاه انحراف ثانوی معتقد بود که عده‌ای از مرتکبین جرم به لحاظ برخوردهای نهادهای مسئول اداره و مبارزه علیه جرم، پس از تحمل مجازات دوباره به دنیای جرم و دستگاه عدالت کیفری بازمی‌گردند. برخوردهای اعمال کنترل اجتماعی موجب می‌شود که انحراف با جرم نزد این افراد نقش بندد و تبدیل به رفتار ثابت آن‌ها شود (نجفی ابرندآبادی، ۱۳۷۴: ۲۰۰). قانون‌گذار باید از این رویکرد اجتناب کرده و با اتخاذ رویکردی متوازن و هوشمندانه، به ماهیت پیچیدهٔ این جرایم پاسخ دهد تا هم به اصل فردی‌کردن کیفرها توجه شود و هم مقابلهٔ مؤثری با مجرمان رایانه‌ای صورت گیرد. اگر مجازات‌های یکسان و با رویکرد سخت‌گیرانه و مطلق مکفی بود، شاهد افزایش تکرار این‌گونه جرایم نبودیم.

اجتناب از تفکیک مطلق حوزه‌های فیزیکی و مجازی

تفکیک کامل حوزه‌های فیزیکی و مجازی در کیفرگذاری در حوزهٔ جرایم رایانه‌ای امری ناپسند است. با توجه به تأثیرپذیری متقابل این دو حوزه از یکدیگر، قانون‌گذار باید رویکردی یکپارچه و منسجم در نظر داشته باشد (والدن، ۲۰۱۶: ۵۶-۵۸). در فرانسه، قانون امنیت

دیجیتال مصوب سال ۲۰۱۶ با رویکردی یکپارچه به حوزه‌های فیزیکی و مجازی به‌صورت توأمان پرداخته است. این قانون، مقررات و الزامات امنیتی را برای هر دو حوزه تعیین کرده است (والدن، ۲۰۱۶: ۵۷). در اسپانیا، قانون جرایم فناوری اطلاعات ۲۰۱۰ نیز رویکردی یکپارچه در قبال جرایم فضای فیزیکی و مجازی اتخاذ کرده است.

در نظام حقوقی ایران، تا حدودی شاهد تفکیک کامل حوزه‌های فیزیکی و مجازی هستیم. قانون‌گذار باید با رویکردی یکپارچه و منسجم، به ارتباط تنگاتنگ این دو حوزه توجه کرده و قوانین مربوطه را تدوین کند. گاهی اوقات وقوع یک جرم در فضای مجازی تأثیرات بسیاری در فضای حقیقی جامعه به‌دنبال دارد و گاهی نیز جرایم ارتکابی در فضای فیزیکی، مقدمه‌ای برای ارتکاب جرایم در فضای مجازی خواهند بود. بنابراین به جهت تأثیر و تأثر متقابل حوزهٔ فیزیکی و مجازی نسبت‌به یکدیگر و نزدیکی آن در عصر فناوری اطلاعات لازم است کیفرگذاری برای این‌گونه جرایم متناسب با ارتباط متقابل این دو فضا صورت گیرد. برای نمونه در بسیاری موارد ارائه‌دهندگان سرویس‌های اینترنت تسهیلگر وقوع جرایم برای مجرمان رایانه‌ای هستند و فضا و بستر جرم را برای آنان فراهم می‌کنند. در قوانین موجود تکلیف نظارت و پایش برای این‌گونه اشخاص پیش‌بینی نشده است و حال آن‌که لازم است کیفرگذاری به سمت این‌گونه اشخاص که مقدمهٔ ایجاد جرم در فضای مجازی را مهیا می‌سازند، صورت پذیرد.

عدم اتکای صرف به مفاهیم و مدل‌های سنتی حقوق کیفری

همان‌گونه که پیشتر اشاره شد، بسیاری از مفاهیم و مدل‌های متداول در حقوق کیفری سنتی در محیط دیجیتال کارآیی ندارند. قانون‌گذار نباید تنها بر این مفاهیم و مدل‌ها تکیه کند، بلکه باید نسبت به ارائهٔ تعاریف و مدل‌های نوین متناسب با ویژگی‌های جرایم رایانه‌ای اقدام کند (کلاف، ۲۰۱۵: ۴۲-۴۵). در ایتالیا، قانون جرایم سایبری ۲۰۰۸ با تعاریف و مفاهیم نوینی هم‌چون "داده‌های مجرمانه" و "ورود غیرمجاز به سیستم‌های رایانه‌ای" تدوین شده است (کلاف، ۲۰۱۵: ۴۳). در سوئیس، قانون جرایم سایبری ۲۰۱۲ از مفاهیم سنتی حقوق کیفری فاصله گرفته و به ارائهٔ تعاریف جدید متناسب با ماهیت جرایم حوزهٔ دیجیتال پرداخته است. قوانین موجود در ایران به‌طور عمده بر مفاهیم و مدل‌های سنتی حقوق کیفری مبتنی هستند. قانون‌گذار باید با ارائهٔ تعاریف و مدل‌های نوین متناسب با ویژگی‌های جرایم رایانه‌ای، از به‌کارگیری صرف این مفاهیم سنتی اجتناب کند. در حوزهٔ کیفرگذاری برای این‌گونه جرایم نیز اغلب نقطهٔ اتکای مقنن بر کیفرهای سنتی و متداول بوده است؛ به‌گونه‌ای جز مجازات حبس و جزای نقدی، مجازات مؤثر دیگری یافت نمی‌شود. حال آن‌که بهتر بود در این‌گونه جرایم، کیفرها نیز به فراخور اقتضائات جرایم رایانه‌ای باشند. برای نمونه محرومیت از دسترسی به خدمات اینترنتی برای مدت معین، ردیابی اینترنتی مجرم در فضای مجازی، الزام مجرم

به احصا و تعیین خلأهای نظارتی موجود در شبکه‌های دسترسی و سرویس‌های خدمات رایانه‌ای و مواردی از این قبیل می‌بایست موردتوجه مقنن قرار گیرد.

پرهیز از توسل بی‌قیدوشرط به مجازات‌های مالی در جرایم رایانه‌ای

امروزه مجازات‌های محرومیت از دارایی تحت‌عنوان کلی مجازات‌های مالی بسیار مورد توسعه و کاربرد نظام‌های مختلف حقوقی قرارگرفته است. این مجازات‌ها با توجه به تغییرات نرخ تورم و تحولات اقتصادی کشورها، اثرات زیادی بر مجرمین داشته و حتی بازدارندگی برجسته‌ای ایجاد می‌کند. اما اعمال بی‌حدوحصر آن بر عموم مجرمان شاید نتواند آثار مطلوب آن را به‌دنبال آورد. در واقع می‌توان امروزه حسب آمار چنین گفت که در نظام حقوقی ایران بعد از مجازات‌های بدنی و سالب آزادی، مجازات‌های مالی و به‌خصوص جزای نقدی در ردیف سوم قرار دارند (همتی، ۱۳۹۱: ۱۷۷). مجازات‌های مالی شاید بتوانند گزینهٔ اول و مطلوبی برای اشخاص حقوقی تلقی شوند اما در جرایم اشخاص حقیقی نمی‌توان در همهٔ موارد چنین مطلوبیتی را انتظار داشت. در واقع جزای نقدی به‌عنوان گونهٔ رایج مجازات‌های مالی به‌جهت محدودیت اجرای بسیاری از مجازات‌های دیگر بر اشخاص حقوقی و هم به دلیل مزایای نسبی، رایج‌ترین مجازات قابل‌اعمال برای این اشخاص است. شرکت‌ها به‌دنبال کسب حداکثر سود مالی هستند بنابراین اگرچه شرکت‌های خیلی بزرگ جزاهای نقدی کم‌مقدار را هزینه‌های عادی فعالیت‌های تجاری خود قلمداد می‌کنند لیکن چنانچه هزینهٔ مجازات مورد انتظار به سود مورد انتظار غلبه یابد، باعث بازدارندگی شرکت از جرم خواهد بود (موسوی مجاب و رفیع‌زاده، ۱۳۹۴: ۱۹۰). در رابطه با جرایم رایانه‌ای نگاه قانون‌گذار نشئت گرفته از نحوهٔ برخورد با اشخاص حقوقی است، بنابراین در عمدهٔ عناوین مجرمانهٔ این قانون، جزای نقدی امری انکارناپذیر بوده است. حال آن‌که ممکن است مرتکبان این‌گونه جرایم از قشر جوان و نوجوان جامعه بوده باشند که هیچ‌گونه منبع درآمدی نداشته و با هدف کسب سود و منفعت مالی و یا دستیابی به اطلاعات و داده‌ها از طریق غیرمجاز اقدام به ارتکاب این جرایم کنند. این‌گونه مجازات‌ها نه‌تنها آن را از ورطهٔ انحراف و بزهکاری دور نمی‌کند، بلکه حتی برای پرداخت این مبالغ نیز ممکن است دست به تکرار چنین جرایمی زنند. بنابراین اصل تناسب و فردی‌کردن مجازات‌ها این‌گونه ایجاب می‌کند که در مقام تعیین کیفر، وضعیت شخصی مجرم، اوضاع‌واحوال ارتکاب جرم و شرایط و کیفیت خاص نوع جرم ارتکابی (جرایم رایانه‌ای) مدنظر مقنن قرار گیرد. در پایان خاطرنشان می‌شود که مجازات‌های مالی اثرات قابل‌قبولی در جایگزینی با مجازات‌هایی چون حبس دارند، اما این به معنای عمومیت و اثربخشی یکسان آن‌ها در همه جرایم نیست و لازم است مقید به شرایط و اصولی نسبت‌به تعیین این‌گونه کیفرها اقدام کرد. در واقع در گسترهٔ جرایم رایانه‌ای اگر باندها و شبکه‌های فراسرزمینی با

هدف سرقت و کلاهبرداری رایانه‌ای اقدام به ارتکاب کرده‌اند و یا حتی افرادی یقه‌سفید و متمول دست به ارتکاب چنین جرایمی زده‌اند، می‌توان مجازات‌های مالی را اقدامی متناسب برای آنان با لحاظ شرایط و کیفیت هر عمل مجرمانه قلمداد کرد اما در صورت ارتکاب فردی و شرایط اقتصادی ضعیف مرتکب و با انگیزه‌های غیرمادی و یا نیازهای ضروری خویش، این‌گونه مجازات‌ها راه به جایی نبرده و نامتناسب است.

الزامات ایجابی

پس از بررسی الزامات سلبی که لازم است مقنن عنایت ویژه‌ای در این خصوص مدنظر داشته باشد، نوبت به الزامات ایجابی کیفرگذاری در جرایم رایانه‌ای می‌رسد. در واقع همان‌طور که لازم است از برخی مؤلفه‌ها پرهیز کرد، می‌بایست برخی موارد را نیز در اهم اولویت‌های تقنینی دانست. در ادامه مهم‌ترین این الزامات مورد بررسی قرار می‌گیرند.

تعیین مجازات‌های متناسب و خلاقانه مبتنی‌بر فناوری اطلاعات

اصل تناسب بین نوع جرم و مجازات تعیینی از اصول اساسی حقوق کیفری به‌شمار می‌رود. در حقیقت مجازات زمانی تأثیر مطلوب را خواهد داشت که با نوع و ویژگی‌های خاص جرم ارتکابی تناسب و هم‌خوانی داشته باشد. جرایم رایانه‌ای اقتضائات خاصی داشته و در بستر فضای رایانه و اینترنت تحقق پیدا می‌کند که از حیث قلمروی مکانی متفاوت از دیگر جرایم است. هم‌چنین مرتکبان این‌گونه جرایم نیز توانمندی و استعداد خاصی در حوزه‌های مرتبط با فضای مجازی دارند که متمایز با دیگر مجرمان هستند. ازطرف‌دیگر آثار جرایم رایانه‌ای نیز ممکن است گستردگی زیادی داشته و حتی علاوه‌بر بزه‌دیدگان مستقیم، جامعهٔ محلی و حتی سراسر کشور نیز تحت‌تأثیر آن جرم قرار گیرد. بنابراین قانون‌گذار باید نسبت‌به طراحی و اجرای مجازات‌های نوین و خلاقانه‌ای هم‌چون محرومیت از دسترسی به فضای مجازی، ضبط و پاک‌سازی داده‌های مجرمانه و جریمه‌های مالی هوشمند اقدام کند (کلاف، ۲۰۱۵: ۳۲۵-۳۳۰). در آلمان، قانون جرایم سایبری ۲۰۰۷ در کنار مجازات‌های سنتی، مجازات‌هایی هم‌چون محرومیت از دسترسی به اینترنت و ضبط تجهیزات رایانه‌ای را پیش‌بینی کرده است (کلاف، ۲۰۱۵: ۳۲۶). در بریتانیا، قانون جرایم دیجیتال ۲۰۱۵ امکان جریمه‌های مالی هوشمند را برای جرایم سایبری فراهم ساخته است. در قوانین کنونی ایران، مجازات‌های کیفری متعارف بر جرایم رایانه‌ای حاکم است. قانون‌گذار باید با ارائهٔ مجازات‌های نوین و خلاقانه‌ای هم‌چون محرومیت از دسترسی به فضای مجازی و جریمه‌های مالی هوشمند، به ماهیت متمایز این دسته از جرایم پاسخ مناسبی ارائه دهد. به‌عنوان نمونه لازم است در خصوص هر گونهٔ خاصی از جرایم رایانه‌ای، کیفری متناسب تعیین شود و از کیفرگذاری کلی اجتناب شود. برای مثال در جرایمی چون هتک حیثیت و نشر اکاذیب رایانه‌ای بهتر است مقنن به محرومیت‌های اجتماعی

مجـرم از خدمـات الکترونیکی نیز در تعیین کیفر توجه داشـته باشـد و تنها مجازات حبس یا جزای نقدی ملاک عمل قرار نگیرد. هم‌چنین در جرایمی چون نشـر دسترسـی غیرمجاز و یا شنود رایانه‌ای می‌توان از کیفرهایی چون لزوم بررسی و احصاء خلأها و نواقص سرویس‌ها و سامانه‌های رایانه‌ای در مواجهه با جرایم احتمالی استفاده کرد.[1]

کیفرگذاری پویا و انعطاف‌پذیر در جرایم رایانه‌ای

جرایـم رایانـه‌ای به جهت متکی‌بودن به فضای سـایبر و ارتباط تنگاتنگ آن با دسـتاوردهای فناوری اطلاعات، در بسـتر زمان متحول و دگرگون می‌شـوند و مجرمان آن نیز به شـیوه‌های جدیدی برای ارتکاب دسـت می‌یابند. به همین منظور قانون‌گذار می‌بایسـت در تدوین کیفر از رویکردی انعطاف‌پذیر و پویا بهره گیرد. این امر به معنای اجتناب از تدوین قوانین سـخت و غیرقابـل انطباق با تغییرات فناورانه اسـت (والـدن، ۲۰۱۶: ۴۶-۴۴). قوانین باید به‌گونه‌ای طراحی شـوند که امکان بازنگری و به‌روزرسـانی مداوم آن‌ها وجود داشـته باشد. در اتحادیهٔ اروپا، دسـتورالعمل ۴۰/۲۰۱۳ در خصوص حمله به سیسـتم‌های اطلاعاتی به تصویب رسید. این دستورالعمل به‌گونه‌ای تدوین شده که امکان بازنگری و به‌روزرسانی مداوم آن وجود دارد (والدن، ۲۰۱۶: ۴۵). در اسـترالیا، قانون جرایم سـایبری ۲۰۰۱ دارای ساختاری انعطاف‌پذیر است و به‌طور مرتب موردبازنگری و اصلاح قرار می‌گیرد. با اندکی تأمل در نظام حقوقی ایران درمی‌یابیم قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ بوده و از آن سال تاکنون هیچ‌گونه تغییری در وضعیـت کیفرهای تعیینی در آن صورت نپذیرفته اسـت. به‌روزرسـانی عناوین مجرمانه و کیفرهای متناسب با آن امری مهم و ضروری در مقابلهٔ مؤثر با ناقضان قانون در فضای مجازی است اما امروزه هم‌چنان جرم و مجازات جرایم رایانه‌ای هم‌چون سایر جرایم سنجیده می‌شود و به خصلت‌های خاص این حوزه توجه وافری نشده است. به‌عنوان نمونه لازم است در انتهای جرایم رایانه‌ای ماده‌ای جانمایی شـود و شیوهٔ بازنگری در کیفرهای تعیینی را پس از یک بازهٔ دو و یا سه‌سـاله پیش‌بینی کند. ازطرف‌دیگر اگر کیفرهای تعیینی به‌تناسـب سـن و جنسیت و شـغل مرتکبان جرایم رایانه‌ای شخصی‌سازی شـود نیز تأثیر بهتری خواهد داشت. استفاده از ظرفیت مجرمان جوان رایانه‌ای نسبت‌به افراد مسن به‌عنوان یک کیفر می‌تواند نمونه‌ای از این موضوع باشد.

۱. منظور از لزوم بررسـی و احصا خلأها و نواقص سـرویس‌ها و سـامانه‌های رایانه‌ای آن است که مرتکب جرم به‌واسـطه شـناخت دقیق فضای مجازی نسبت به تعیین نقاط آسیب‌پذیر در این فضا پیشنهادهایی ارائه دهد تا هم متولیان امر، نظارت خود بر این منافذ را بالا ببرند تا از تکرار این‌گونه جرایم اجتناب شـود و هم مرتکب فعلی با تحمیل این مجازات، متنبه شود و بتواند در مسیر اجرای مجازات خویش نفعی به جامعه نیز برساند.

تأسیس نهادهای تخصصی تعقیب و رسیدگی برای مقابله با جرایم رایانه‌ای

خصلت خاص جرایم رایانه‌ای ایجاب می‌کند تا قانون‌گذار نسبت‌به ایجاد نهادها و سازمان‌های تخصصی در حوزهٔ جرایم رایانه‌ای اقدام کند. این نهادها می‌توانند با حضور متخصصان حوزه‌های فنی، حقوقی و جرم‌شناسی به شناسایی، پیشگیری و مقابله با این دسته از جرایم بپردازند (وال، ۲۰۰۷: ۹۷-۱۰۰). در کشور انگلستان، پلیس سایبری ملی[1] در سال ۲۰۱۳ تأسیس شد. این نهاد متشکل از متخصصان فنی، حقوقی و جرم‌شناسی است و وظیفهٔ شناسایی، پیشگیری و مقابله با جرایم سایبری را برعهده دارد (وال، ۲۰۰۷: ۱۰۰). در ایالات‌متحدهٔ آمریکا، بخش جرایم سایبری[2] در سازمان اف‌بی‌آی فعالیت می‌کند که مسئولیت مشابهی را برعهده دارد.

در نظام حقوقی ایران، هنوز نهاد تخصصی مستقلی برای مقابله با جرایم رایانه‌ای ایجاد نشده است و تنها کمیتهٔ تعیین مصادیق مجرمانه و شوراهایی چون شورای عالی فضای مجازی در کشور شکل گرفته است. بنابراین اگر نهادی تخصصی با حضور متخصصان حوزه‌های فنی، حقوقی و جرم‌شناسی شکل بگیرد تا در تعیین کیفر و مقابلهٔ مؤثر با مجرمان رایانه‌ای گام بردارد تأثیر شایانی بر کاهش نرخ این‌گونه جرایم خواهد داشت. نگاه سنتی پلیس و قضات به جرایم رایانه‌ای هم‌چون سایر جرایم نمی‌تواند مقابلهٔ مؤثری با این‌گونه جرایم به‌دنبال آورد. به‌عنوان نمونه می‌توان نسبت‌به تأسیس پلیس ویژهٔ جرایم رایانه‌ای و هم‌چنین محاکم اختصاصی ویژهٔ جرایم رایانه‌ای اقدام کرد تا هم پیشگیری و مقابلهٔ سریع و مؤثری صورت گرفته و هم تعقیب و رسیدگی متناسب و تخصصی در محاکم اختصاصی انجام گیرد.

بهره‌گیری از دستاوردهای علم اخلاق و رویکردهای اقناعی مجرمان در استفاده از رایانه

هرچند مرز اخلاق و حقوق طی نظریات مختلفی قابل‌تمایز است و اختلاف‌نظرات بنیادی در این حوزه می‌تواند به نتایج متفاوتی منجر شود و تمام بایدونبایدهای حقوق کیفری اسلامی را از گرایشات سکولار آن متمایز کند[3]، با این وصف بنا بر معنایی عرفی و غیرمصطلح اخلاق مجموعهٔ قواعدی است که رعایت آن‌ها لازمهٔ نیکوکاری و رسیدن به کمال است. احترام به این قواعد ریشه در ضمیر و نهاد آدمی دارد و بدون نیاز به دخالت دولت، انسان در وجدان خویش آن‌ها را محترم می‌داند (کاتوزیان، ۱۳۷۷: ۵۴۶ به نقل از وروایی و همکاران، ۱۳۹۳: ۳۷).

1. National Cyber Crime Unit
2. Cyber Crime Division
۳. برای مطالعه نظر مخالف در این خصوص بنگرید به محمودی جانکی، فیروز (۱۳۸۳). حمایت کیفری از اخلاق، علوم جنایی (مجموعه مقالات در تجلیل از استاد دکتر محمد آشوری)، ۷۵۶-۸۰۰ و برای نقد تفصیلی آن بنگرید به زهروی، رضا (۱۳۹۹). مرز اخلاق و حقوق؛ نقدی بر نظریهٔ نفی ورود حقوق به گسترهٔ حجاب (مطالعهٔ تطبیقی اسلام، ایران، و اروپا)، پژوهش‌نامه انتقادی متون و برنامه‌های علوم انسانی، ۲۰(۱۱)، ۲۷۰.
https://criticalstudy.ihcs.ac.ir/article_6011.html

اخلاق‌گرایی و تقید شهروندان یک جامعه به پایبندی به آن، ضامن پیشرفت و توسعهٔ آن اجتماع و کاهش آسیب‌ها و جرایم احتمالی است. از منظر جرم‌شناسی و از دیدگاه نظریهٔ کنترل اجتماعی، باورهای اخلاقی یکی از چهار عامل مهم پیوند اشخاص با جامعه و به‌تبع آن دوری از انحراف و جرم به‌شمار می‌رود.[1] در پیشگیری از وقوع جرم نیز نگرهٔ رشد اخلاقی حائز اهمیت است؛ از دیدگاه لارنس کلبرگ[2]:

> اخلاقی رفتارکردن با به دست‌آوردن باورها و معیارها از رهگذر الگوبرداری و همانندسازی در پیوند است. در پرتو نگرهٔ فوق، تحولات و رشد اخلاقی افراد صورت می‌پذیرد و براین‌اساس آنان با معیارهای اخلاقی مانند عدالت، حقیقت و درست‌کاری آشنا شده و آن‌گاه که این رشد و دگرگون‌شدن در دسته‌ای با درنگ همراه شود، زمینهٔ گرایش به بزهکاری رقم خواهد خورد. به همین منظور در چارچوب پیشگیری فردمدارانه با رشد نگره‌های اخلاقی به شناسایی روش‌های مناسب برای تقویت جنبه‌ها و مهارت‌های شناختی افراد و درست سپری‌شدن سطح رشد و تحولات اخلاقی می‌توان دست یافت (نیازپور، ۱۴۰۰: ۱۰۶-۱۰۷).

قطعنامهٔ شمارهٔ ۴۵/۱۲۱ در هشتمین کنگرهٔ سازمان ملل متحد با موضوع "پیشگیری از جرم و اصلاح مجرمان (توصیه‌های مرتبط با جرایم سایبری)" نیز، دولت‌ها را به مطالعه و همکاری با سازمان‌های ذی‌نفع در زمینهٔ اخلاق استفاده از رایانه و اقدام به تدوین مواد درسی و آموزشی به‌منظور ارتقای سطح آگاهی جامعه توصیه کرده است (قدیر و کاظمی فروشانی، ۱۳۹۸: ۲۶۰). مبتنی‌بر موارد پیش‌گفته، ضرورت دارد مقنن با نگاه اخلاق‌گرایانه و توجه به اقناع وجدانی مجرمان، در تعیین کیفر در جرایم رایانه‌ای به مقولهٔ آموزش و تعلیم و اقناع آنان توجه ویژه‌ای مبذول دارد؛ برای نمونه الزام به گذراندن دوره‌های اخلاق حرفه‌ای کار با رایانه، دوره‌های آموزش سواد رسانه‌ای و فضای سایبری می‌تواند به‌عنوان کیفر جبران‌کنندهٔ خلأ آموزش‌های انجام نشدهٔ فرد مجرم در دوران کودکی و نوجوانی باشد.

اهتمام قانون‌گذار به اولویت پیشگیری وضعی قبل از تعیین کیفر

پیشگیری از جرم همواره موردتوجه نظام‌های مختلف حقوقی بوده و در جایگاهی برتر نسبت به کیفر قرار دارد. پیشگیری‌های غیرکیفری (کنشی) در این زمینه نسبت به پیشگیری از طریق اعمال مجازات (واکنشی) اولویت داشته و آثار و نتایج مطلوب‌تری به‌دنبال دارند. یکی از توصیه‌های مندرج در قطعنامهٔ شمارهٔ ۴۵/۱۲۱ هشتمین کنگرهٔ سازمان ملل متحد در خصوص

۱. چهار عامل دل‌بستگی و داشتن عاطفه و حساسیت نسبت‌به دیگران، پایبندی و سرمایه‌گذاری عقلانی فرد در جامعه، درآمیختگی و اشتغال فکری و جسمی و درنهایت باورهای اخلاقی، عناصر پیوند شخص به اجتماع و دوری از انحراف و جرم در نظریه کنترل اجتماعی است (رایجیان اصلی، ۱۳۹۸: ۱۶۴-۱۶۵).

2. Lawrence Kohlberg

پیشـــگیری از جرم و اصلاح مجرمان نیز تقویت و ایجاد سازوکارهای پیشگیرانه و امنیتی برای هرگونه اســتفاده از رایانه با در نظر گرفتن حریم خصوصی کاربران و آزادی‌های مشــروع افراد بوده است (قطعنامهٔ شمارهٔ ۴۵/۱۲۱ سال ۱۹۹۸).

از مهم‌ترین گونه‌های پیشگیری، پیشگیری وضعی به‌شمار می‌رود. پیشگیری وضعی درصدد شناســایی عوامل زمینه‌ای موجود در محیط ارتکاب جرم و خنثی‌سازی و کم‌اثرکردن آنان و رفع فرصت‌های جرم‌زاست. این رویکرد به شکل دقیقی منطبق با نظریهٔ فرصت در جرم‌شناسی است.

> تفکر حاکم بر این نظریه آن است که به‌صرف وجود بزهکار و بزه‌دیده، جرم واقع نمی‌شود، بلکه باید فرصت و موقعیت مناســب و مهیایی برای ارتکاب نیز فراهم باشــد. این همان امری است که در فلسفه به‌عنوان فراهم‌بودن مقتضیات و فقدان موانع می‌شناسیم (محمدنسل، ۱۳۸۶: ۲۹۴).

در حقیقت اکثریت جرایم را می‌توان موقعیت‌مدار دانست؛ چراکه در فرصت‌ها و موقعیت‌های مناســب و بدون حفاظ ارتکاب آن‌ها ســهل‌الوصول بوده و مانعی بر سر راه مرتکب نیست. در این مفهوم فرصت‌مداری بدین معنی اســت که ارتــکاب جرم در کنار وجود مرتکب مصمم به وجــود یک آمــاج بدون دفاع یا محافظ نیــاز دارد. (بابایی و نجیبیــان، ۱۳۹۰: ۱۵۵) در جرایم رایانــه‌ای موقعیــت مهیا جهت ارتکاب جــرم فضای رایانه‌ای و داده‌های الکترونیکی اســت. وجود این فضای خاص موجب شــده اســت مرتکب با خیالی آســوده و بدون هرگونه دغدغهٔ خاطر وارد آن شــده و به عملی ســاختن قصد مجرمانهٔ خویش بپردازد. بنابراین اینجاســت که پیشــگیری وضعی به نحو بارزی می‌تواند این انگیزهٔ مصمم را در وی و سایر مجرمان بالقوه از بیــن بــرد. در حقیقت هم می‌توان حذف و یا محدودکــردن فرصت‌های مجرمانه را ضمن کیفر برای مجرم مذکور تعیین کرد و هم به‌طور مستقل از کیفر برای سیاست‌گذاری‌های پیشگیری از جرم آن را مدنظر دانست. به‌عنوان نمونه در عموم جرایم رایانه‌ای در قانون مصوب سال ۱۳۸۸ هیچ‌گونه اشاره‌ای به حذف فرصت‌های مجرمانه و یا محدودکردن فضای ارتکابی نشده است. از باب مثال می‌توان در جرمی چون شنود غیرمجاز (موضوع مادهٔ ۷۳۰ قانون تعزیرات) ضمن محکومیــت مجرم، وی را به محرومیت موقت یا برای مدت طولانی از دسترســی به فضاهای رایانه‌ای و داده‌های الکترونیکی محکوم کرد و یا حتی برای اشتراک اینترنت وی نیز محدودیت قائل شد. علاوه‌برآن در موارد جزئی نیز می‌توان با تعیین نظارت نوبه‌ای این محدودیت را برای استفادهٔ مجرم از فضاهای مذکور مقرر داشت. بنابراین پیوند میان آموزه‌های پیشگیری وضعی و تعیین کیفر در جرایم رایانه‌ای امری ضروری اســت و لازم اســت قبل از تعیین کیفر مدنظر مقنن و سیاســت‌گذاران کیفری قرار گیرد، هرچند ایرادات پیشــگیری وضعی نیز در این حوزه باید مورد آسیب‌سنجی قرارگرفته و خنثی شود[1] (زهروی، ۱۳۹۳).

۱. بــرای تفصیــل بنگرید به زهــروی، رضا (۱۳۹۳). پیشــگیری از جرایم و تخلفات در پرتــو خودپایی (نظارت همگانی مردمی)، نظارت و بازرسی، ۲۹. https://www.magiran.com/paper/2070854

تأکید بر مجازات‌های اجتماعی در قالب ارائهٔ خدمات رایگان رایانه‌ای

مجازات‌های اجتماعی امروزه مجازات‌هایی با منفعت اجتماعی و عام‌المنفعه به‌شمار می‌روند. هـر جامعه اقتضائات خاص خـود را دارد و جرم در یک زمینهٔ اجتماعی و فرهنگی رخ می‌دهد کـه لازم اسـت در تدویـن و تعیین مجـازات به آن‌ها توجه شـود. تعیین مجازات با نگرشـی جامعه‌شـناختی و با تأکید بر سـرمایه‌های افراد و ویژگی‌های خاص مجرم، زیان‌دیده، نوع جرم و شـرایط جامعه می‌تواند موجب انطباق بیشـتر این مجازات‌ها با واقعیات جامعه و کارآمدی بیشـتر آن‌ها و دستگاه قضایی شود (پرچمی و درخشان، ۱۳۹۷: ۵۵). مجازات‌های اجتماعی یا اجتماع‌محور به‌طورمعمول در راستای تأمین نیازهای اجتماعی صورت گرفته و از ظرفیت مجرم برای رفع نیازهای جامعه و افراد کم‌برخوردار استفاده می‌شود. مجرمان رایانه‌ای افرادی به‌شمار می‌روند که از سـطح متوسـط به بالایی واجد سـواد رایانه‌ای بوده و این آشـنایی همان‌طورکه موجب ارتکاب جرم شـده اسـت، می‌تواند در مسیر خدمت‌رسـانی به مردم صورت گیرد. در واقع این اطلاعات و دانش رایانه‌ای شمشـیری دو لبه است که هم‌زمان می‌تواند آسیب‌آفرین و مزیت‌بخش باشـد. در وضعیت موجود، در قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ هیچ‌گونه اشاره‌ای به مجازات‌های اجتماعی در قالب خدمت‌رسانی رایانه‌ای صورت نگرفته است و این ظرفیتی مغفول مانده اسـت که بهره‌وری از آن نه‌تنها مفید به حال جامعه بوده بلکه در بازسـازی اجتماعی مرتکب و احساس مفیدبودن وی نیز تأثیرگذار است. در واقع امروزه به جهت گسترش نوآوری رسانه و محوریت اکثریت امور و خدمات دولتی و عمومی در فضای رایانه‌ای، افرادی که از سـواد لازم برخوردار نبوده و آشـنایی کافی ندارند، به‌ناچار می‌بایست با پرداخت هزینه و صرف وقت امورات خویش را به انجام رسـانند، حال اگر چنین مجرمانی که از سـواد مطلوب در حوزهٔ رایانه‌ای برخوردارند، در این مسـیر به کار گمارده شـوند و با نظارت‌های سازمانی و متمرکز، به انجام امور رایانه‌ای نیازمندان بپردازند، هم در رفع مشکلات عمومی جامعه مؤثر بوده و هم در ترمیم شخصیت مجرم و بازسازی بیش‌ازپیش وی مؤثر است.

وحدت حقوقی در تعیین کیفر مبتنی‌بر رویکردهای حقوق بین‌الملل

در سـال‌های اخیر گسـترش روزافـزون تبادلات و ارتباطات کشـورهای مختلـف و ارتقای فناوری‌هـای نوین مجازی و رسـانه‌ای، دنیای معاصر را به یک دهکـدهٔ کوچک جهانی مبدل سـاخته اسـت؛ به‌گونه‌ای که هر نوع فرهنگ و هنجاری که در گوشـه‌ای از جهان ارزش تلقی شـود به‌سـرعت به دیگر نقـاط انتقال می‌یابـد. ازطرف‌دیگر جرم نیز در یـک فضای متمرکز، می‌تواند رسـوخ و نفـوذ یافته و ماهیتی فراسـرزمینی یابد. جرایم رایانه‌ای از این قسـم بوده که در شـبکهٔ گسـترده و سراسـری اینترنت و داده‌های الکترونیکی قابلیتی فراسرزمینی یافته و می‌تواند بزه‌دیدگانی خارج از محدودهٔ سـرزمینی یک کشـور را مورد هجمه قرار دهد. در این

زمینــه نیازمنــد یک وحدت رویه در برخورد متقابل با جرایم رایانه‌ای بین اکثریت کشــورها و یا دســت‌کم وحدت حقوقی منطقه‌ای هســتیم. در واقع در مقام مبارزهٔ مؤثر با این‌گونه جرایم که حدومرز ســرزمینی نمی‌شناســد نمی‌توان به پاســخ‌های کیفری داخلی تمسک جست و از رویکردها و آورده‌های کشــورهای دیگر غافل بود. برای نمونه کشور کانادا اولین کشوری بوده اســت که در ســال ۱۹۸۳ در قانون فدرال خود، به‌طور مشــخص به جرم رایانه‌ای اشاره کرد و قوانینی برای آن به تصویب رســاند (کیســی[1]، ۲۰۰۴: ۲۶). در کشور آمریکا نیز در کنگرهٔ قوانین فدرال، جرایم رایانه‌ای در ســال ۱۹۸۴ تصویب شــد که شــامل قوانینی جهت کلاهبرداری و سوءاســتفاده رایانه‌ای بود (ویلیامز[2]، ۲۰۰۶: ۱۴). در حال حاضر نمونهٔ موفقی از همکاری‌های بین‌المللی در حوزهٔ جرایم رایانه‌ای را می‌توان در کنوانســیون جرایم ســایبری مصوب ســال ۲۰۰۱ میلادی بوداپســت شــاهد بود. فصل ســوم این کنوانســیون به همکاری‌های بین‌المللی اختصاص یافته است که در مادهٔ ۲۳ آن با عنوان "اصول کلی" راجع‌به همکاری‌های بین‌المللی مقررشده است:

> اعضای کنوانسیون باید بر اساس مقررات این فصل و از طریق اجرای اسناد بین‌المللی مربوط به همکاری بین‌المللی در موضوعات کیفری، ترتیبات توافق شــده راجع‌به قانون‌گذاری متحدالشکل یا متقابل و قوانین داخلی و برای رســیدن به وسیع‌ترین حوزهٔ پی‌جویی یا رسیدگی قضایی راجع به جرایم مرتبط با سیســتم‌های رایانه‌ای و داده‌ها یا جمع‌آوری ادلهٔ الکترونیک در جرایم، با یکدیگر همکاری کنند (گروه کارشناسان، ۱۳۸۴: ۲۷).

این کنوانســیون مبنای عمل کشــورهای شــورای اروپا در مقابلهٔ مؤثر با جرایــم فضای رایانه اســت که وحدت حقوقی و اتخاذ تدابیری واحد و منسجم و کارآمد را میسر می‌سازد. بنابراین به‌منظور کســب تجارب کشــورهای مختلف در حوزهٔ مقابله با جرایم رایانه‌ای و پیشگیری از تکرار جرم در این عرصه، می‌توان با انعقاد موافقت‌نامه‌های قضایی منطقه‌ای و یا بین‌المللی، به تدوین قواعد مشترکی در این عرصه پرداخت و با احصاء کامل عناوین مجرمانه و کیفرگذاری مبتنی بر وحدت حقوقی در این عرصه گامی بلند در مبارزهٔ مؤثر با جرایم رایانه‌ای برداشت.

نتیجه‌گیری و پیشنهادها

قانــون تجارت الکترونیک مصوب ســال ۱۳۸۲ و قانون جرایم رایانه‌ای که در ســال ۱۳۸۸ به تصویب رســیده است، مســتندات مهم جرایم رایانه‌ای در نظام حقوقی ایران به شمار می‌آیند که نشــانگر رویکرد قابل‌تحســین مقنن به فضای سایبر و رایانه است. این‌گونه جرایم به جهت گســترش فضای اینترنــت در جای‌جای عرصهٔ پهناور هســتی، خصلتی فراســرزمینی یافته و

1. Casey
2. Williams

نمی‌تـوان آن را در محدودهٔ سـرزمینی خاص محصور کرد. رویکـرد قانون‌گذار در تعیین کیفر برای این‌گونه جرایم، تبعیت از کیفرگذاری در عموم جرایم بوده که نه‌تنها نمی‌تواند آثار مطلوبی فراهم آورد، بلکه به‌واسـطهٔ کسب تجارب ارزشمند توسط مجرمان از فضای جرایم رایانه‌ای، امکان تکرار آن در آینده دور از انتظار نیسـت. پژوهش حاضر در مقام احتراز از وضع موجود و آسـیب‌های متصـوره از کیفرگذاری جرایم رایانه‌ای، اقدام به تدویـن الزامات تعیین کیفر با محوریت الزامات سلبی و ایجابی در این‌گونه جرایم کرده است و کوشش شده است با نگاهی منحصربه‌فرد، خاص و درعین‌حال فراسرزمینی به این‌گونه جرایم نگریسته و الزامات مذکور را به رشتهٔ تحریر درآورد. در الزامات سلبی تعیین کیفر، لازم است مقنن از تدابیر سخت‌گرایانه و مطلق‌گـرا در تعیین کیفر در این جرایم بپرهیزد و با نگاهی منعطف و مبتنی بر واقعیت این‌گونه جرایم نسـبت به کیفرگذاری اقدام کند. مسئلهٔ دیگری که همواره حائز اهمیت است این است که مقنن در این‌گونه جرایم بین فضای فیزیکی و مجازی تفکیک قائل شـده اسـت حال آن‌که این دو فضا وابسـته و متلازم یکدیگرند و کیفرگذاری در آن باید مبتنی‌بر ارتباط دوسـویهٔ این فضاها باشد. علاوه‌برآن تکیه کردن به مدل‌های سنتی در تعیین کیفر آسیبی بزرگ در کیفرگذاری جرایم رایانه‌ای اسـت که لازم است نسبت به روزآمدسـازی و بهره‌گیری از اقتضائات فضای دیجیتال در تعیین کیفر برای این جرایم اهتمام لازم صورت گیرد. در آخر نیز می‌طلبد از توسل بی‌قیدوشـرط به مجازات‌هـای مالی به‌خصوص جزای نقدی بدون توجـه به نتیجه‌مندی آنان پرهیز شود تا شاهد آثار ناگوار تکرار جرم در این قبیل موارد نباشیم. در حوزهٔ الزامات ایجابی نیز می‌بایسـت مقنن نسبت به تعیین مجازات‌های متناسب و خلاقانه مبتنی‌بر فناوری اطلاعات همت گمارد. هم‌چنین در کیفرگذاری برای جرایم رایانه‌ای لازم است پویایی و انعطاف وجود داشته باشد تا امکان بازنگری و تغییر و تحول در کیفرهای تعیینی پس از سپری‌شدن دوره‌های دو و یا سه‌سـاله وجود داشته باشـد. تأسیس نهادهای تخصصی تعقیب و رسیدگی برای مقابله با مجرمان رایانه‌ای نیز از دیگر الزامات این حوزه اسـت که مقابلهٔ مؤثری را به‌دنبال می‌آورد. ازطرف‌دیگر بهره‌گیری از دسـتاوردهای علم اخلاق و رویکردهای اقناعی مجرمان در استفاده از رایانـه نیز می‌تواند بسـان راهکاری مطلوب در عین کیفر مجـرم، زمینهٔ هنجارپذیری وی و قانون‌مداری او را به‌دنبال آورد. هم‌چنین توجه به آموزه‌های پیشـگیری وضعی و حذف منافذ جرم‌زا و محدودیت در اسـتفادهٔ از فضای مجرمانهٔ موصوف، می‌تواند راهگشا و کارآمد باشد. در کنار آن تأکید بر مجازات‌های اجتماعی در قالب ارائهٔ خدمات رایگان رایانه‌ای به جامعه نیز هم در منفعت‌بخشـی به اجتماع و رفع نیازهای عمومی تأثیرگذار بوده و هم در تسـهیل ارتباط مجـرم با جامعه و حفـظ موقعیت وی به‌عنوان عنصری فعال و کنشـگری پویا مطلوبیت دارد. در آخـر نیز اهتمام به وحدت حقوقی و انعقـاد موافقت‌نامه‌های قضایی منطقه‌ای و بین‌المللی در جهـت اتخـاذ رویکردهای نزدیک به هم در مبارزهٔ مؤثر بـا جرایم رایانه‌ای و تعیین کیفر بر

مبنـای آورده‌های نوین دنیای معاصر امری لازم به‌شـمار می‌رود که مورد توصیهٔ کنوانسـیون جرایم سـایبر مصوب سال ۲۰۰۱ میلادی در بوداپسـت نیز بوده است. بنابراین از مقنن انتظار مـی‌رود چه در قانون تجارت الکترونیک و چه در قانون جرایم رایانه‌ای بازنگری شایسـته‌ای در کیفرهای موجود کند؛ چنان‌که این امر مورد تأکید قطعنامهٔ شـمارهٔ ۴۵/۱۲۱ هشـتمین کنگرهٔ سـازمان ملل متحد در خصوص پیشـگیری از جرم و اصلاح مجرمان به دولت‌های عضو بوده اسـت که نسبت‌به روزآمدکردن قوانین و دادرسی‌های کیفری ملی اهتمام ویژه‌ای کنند. بنابراین پیشـنهاد می‌شـود قانون‌گذار مبتنی‌بر ناکارآمدی کیفر حبس، تنها در موارد ضرورت به انتخاب این نوع کیفر بسـنده کند و در سـایر موارد با نگاه فردی و با عنایت به مقتضیات خاص جرایم رایانه‌ای به تعیین کیفر شایسته بپردازد. به نقش کیفرهای خدمات اجتماعی رایگان بیشتر توجه کرده و همگام‌شـدن با رویهٔ جهانی و وحدت حقوقی در حوزهٔ مقابله با جرایم رایانه‌ای را در دستور کار خود قرار دهد. امید است کاربست این تدابیر سلبی و ایجابی، گامی در جهت مقابلهٔ مؤثر با جرایم رایانه‌ای و پیشـگیری از تکرار آن در آینده باشـد و مقنن را در مسـیر رسیدن به وضع مطلوب در کنترل نرخ جرم در فضای مجازی یاری رساند.

منابع

اردبیلی، محمدعلی (۱۳۹۹). حقوق جزای عمومی. جلد سوم، چاپ بیستم. تهران: نشر میزان.

الهام، غلامحسـین و برهانی، محسـن (۱۳۹۸). درآمدی بر حقوق جزای عمومی. جلـد دوم، چاپ پنجم، تهران: نشر میزان.

بابایـی، محمدعلی و نجیبیـان، علی (۱۳۹۰). چالش‌های پیشـگیری وضعی از جرم. مجله حقوقی دادگسـتری، ۷۵(۷۵)، ۱۴۷-۱۷۲. https://doi.org/10.22106/jlj.2011.11079

پرچمـی، داوود و درخشـان فاطمه (۱۳۹۷). بررسـی مجازات‌هـای اجتماعی جایگزین حبـس و کاهش جرم. مطالعات جامعه شناسی، ۱۱(۴۰)، ۴۹- ۶۸.

پیونـدی، غلامرضـا (۱۳۹۲). اصـول و معیارهای کیفرگذاری از منظـر مکاتب حقوقی در مقایسـه با آموزه‌های اسلامی، پایان‌نامهٔ دکتری فقه و حقوق جزا. مدرسهٔ عالی شهید مطهری.

حبیب‌زاده، طاهر (۱۳۹۵). تفاوت چهار اصطلاح رایانه‌ای، کامپیوتری، اینترنتی و سـایبری، تارنمای رسمی دکتر طاهر حبیب‌زاده. http://drhabibzadeh.com/question/

رایجیان اصلی، مهرداد (۱۳۹۸). درآمدی بر جرم شناسی. چاپ سوم. تهران: انتشارات سمت.

شـاملو، کاظم؛ افشـانی، سـیدعلیرضا، روحانی، علی و مزیدی، علی‌محمد (۱۴۰۳). تلفن همراه؛ دروازه ورود به زیست شبکه‌ای: ارائهٔ یک نظریه زمینه‌ای. رسانه، ۳۵(۳) ۸۱- ۱۰۵.

https://doi.org/10.22034/bmsp.2023.400003.1886

صفاری، علی (۱۳۹۸). کیفرشناسی. چاپ سی و سوم. تهران: انتشارات جنگل.

عبدی‌پور کشاور، مهدی؛ انصاری، عباس‌قلی و ششگل، حمید (۱۳۹۹). هستی‌شناسی جرایم رایانه‌ای با توجه به قانون جرایم رایانه‌ای. تحقیقات حقوق بین‌المللی آزاد، ۱۳(۴۷)، ۱۶۹-۱۸۹.

https://doi.org/10.30495/alr.2020.671461

قدیر، محسن و کاظمی فروشانی، حسین (۱۳۹۸). بررسی تطبیقی حقوق کیفری ایران با اسناد بین المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری. مجله حقوقی بین‌المللی، ۳۶(۶۰) ۲۳۷- ۲۶۷.
https://doi.org/10.22066/cilamag.2019.35084
گروه کارشناسان (۱۳۸۴). کنوانسیون جرایم سایبر و گزارش توجیهی آن. گزارش تخصصی. تهران: گروه ارتباطات و فناوری های نوین مرکز پژوهش های مجلس شورای اسلامی.
محمدنسل، غلامرضا (۱۳۸۶). اصول و مبانی نظریه فرصت جرم. مطالعات حقوق خصوصی، ۳۷(۳)، ۲۹۳- ۳۲۲.
https://dor.isc.ac/dor/20.1001.1.25885618.1386.37.3.8.2
منصورآبادی، عباس (۱۳۹۹). مختصر حقوق جزای عمومی. چاپ اول. تهران: نشر میزان.
موسوی مجاب، سید درید و رفیع‌زاده، علی (۱۳۹۴). ضمانت اجراهای جرایم اشخاص حقوقی در قانون مجازات اسلامی مصوب. دیدگاه‌های حقوق قضائی، ۲۰(۶۹)، ۱۸۵-۲۰۶.
نجفی ابرندآبادی، علی‌حسین (۱۳۷۴). تقریرات درس جرم‌شناسی (نظریه‌های جرم‌شناسی). تهیه و تنظیم: فاطمه قناد، گروه حقوق جزا و جرم شناسی، دانشگاه شهید بهشتی.
نیازپور، امیرحسن (۱۴۰۰). پیشگیری از جرم. چاپ اول. تهران: نشر دادگستر.
نیازی، محسن؛ ذوالفقاری، اکبر، ذوالفقاری، اکبر و رضایی، الهام (۱۴۰۳). فراترکیب طراحی مدل ابعاد آسیب های رسانه‌های اجتماعی مجازی. رسانه، ۳۵(۱)، ۵۵-۸۱. https://doi.org/10.22034/bmsp.2023.370077.1805
وروایی، اکبر؛ سعادتی، رضا و هاشمی، حمید (۱۳۹۳). تاثیر اخلاق در جرم‌انگاری و جرم‌زدایی در نظام حقوق کیفری اسلامی ایران. پژوهش حقوق کیفری، ۳(۸)، ۳۳- ۶۲.
همتی، مریم (۱۳۹۱). اجرای احکام محکومیت جزای نقدی در حقوق کیفری ایران و انگلستان، پژوهش های حقوقی، ۱۱(۲۱)، ۱۷۷- ۱۹۱. http://jlr.sdil.ac.ir/article_34431.html

Abdipour Keshavarz, M., Ansari, A. Gh., & Sheshgol, H. (2020). Ontology of Computer Crimes According to the Computer Crimes Law. *International Legal Research*. 13(47), 169 – 89 **[In Persian]**. https://doi.org/10.30495/alr.2020.671461
Ardebili, M. A. (2020). *General Criminal Law*. Volume 3, 20th Edition, Tehran: Mizan Publishing. **[In Persian]**
Babaei, M. A., & Najibian, A. (2011). Hallenges of Situational Crime Prevention. *Justice Legal Journal*, 75(75), 147–152. **[In Persian]** https://doi.org/10.22106/jlj.2011.11079
Brenner, S.W. (2004). *Cybercrime: Re-thinking crime control strategies*. In Crime online .12-46. Routledge.
Casey, E. (2004). *Digital evidence and computer crime: forensics science, Computer and the internet, 2nded*. Amsterdam: Elsevier academic press.
Clough, J. (2015). *Principles of cybercrime*. Cambridge:Cambridge University Press.
Elham, Gh., & Borhani, M. (2019) . *Introduction to General Criminal Law*. Volume 2, Fifth Edition, Tehran: Mizan Publishing. **[In Persian]**
Ghadir, M., & Kazemiforoushani, H.(2019). Comparative Study of Iranian Criminal Law with International Documents in the Field of Countering and Preventing Cyberterrorism. *International Law Review*, 36(60). 237 – 267. **[In Persian]** https://doi.org/10.22066/cilamag.2019.35084
Group of Experts (2005). Group of Experts (2005). Cybercrime Convention and its Explanatory Report. Specialized Report. Tehran: Communications and New Technologies Group, Research Center of the Islamic Consultative Assembly. **[In Persian]**
Habibzadeh, T. (2016). Difference between the four terms computer, computerized, internet and cyber, Dr. Taher Habibzadeh's official website. http://drhabibzadeh.com/question/. **[In Persian]**
Hemmati, M. (2012). Enforcement of Fine Sentences in Iranian and English criminal law. *Legal*

Research, 11(21) 177 – 191. **[In Persian]** http://jlr.sdil.ac.ir/article_34431.html
Mansour Abadi, A. (2020). *Summary of General Criminal Law*. First Edition, Tehran: Mizan Publishing. **[In Persian]**
MohammadNasl, Gh. (2007). Principles and Foundations of the Theory of Opportunity of Crime. *Private Law Studies*, 37(3), 293 – 322. **[In Persian]** https://dor.isc.ac/dor/20.1001.1.25885618.1386.37.3.8.2
Moore, R .(2005). *Cybercrime: investigating high-technology computer crime*. Anderson publishing co.
Mousavi Mojab, S. D., & Rafizadeh, A. (2015). Sanctions of Artificial Persons Crimes in the Islamic Penal Code Approved in 2013. *Judicial Law*, View 20(69). 185 – 206. **[In Persian]**
Najafi Abrand Abadi, A. H. (1995). Criminology Course Notes (Criminology Theories). prepared and edited by: Fatemeh Ghanad, Department of Criminal Law and Criminology. Shahid Beheshti University. **[In Persian]**
Niazi, M., Zolfaghari, A., Zolfaghari, A., & Rezaei, E. (2024). Meta-composition of the design of the model of the dimensions of the harms of virtual social media . *Media*, 35(1), 55- 81. **[In Persian]** https://doi.org/10.22034/bmsp.2023.370077.1805
Niazpour, A. H. (2021). *Crime Prevention*. first edition. Tehran: Dadgostar Publishing. **[In Persian]**
Parchami, D., & Derakhshan, F. (2018), Investigation of social punishments as alternatives of imprisonment and crime reduction. *Sociological Studies*, 11(49), 49 – 68. **[In Persian]**
Peyvandi, Gh. (2013). Principles and Criteria of Punishment from the Perspective of Legal Schools in Comparison with Islamic Teachings, PhD Thesis in Jurisprudence and Criminal Law. Shahid Motahari High School. **[In Persian]**
Raijian Asli, M. (2019). *An Introduction to Criminology*. Third Edition, Tehran: Samt Publications. **[In Persian]**
Resolutions45/121 .(1998). United Nations.
Saffari, A. (2019). *Penology*. 33rd edition, Tehran: Jangal Publications. **[In Persian]**
Samuel, M. (2008). *Computer crime and Information Technology Misuse*. Commonwealth publishers.
Shamloo, K., Afshani, S. A. R., Rouhani, A., & Mazidi, A. M. (2024), Mobile Phone; Gateway to Networked Life: Presenting a Grounded Theory. Media, 35(3), 81 - 105. **[In Persian]** https://doi.org/10.22034/bmsp.2023.400003.1886
Varvaei, A., Saadati, R., & Hashemi, H. (2014), The Effect of Morality on Criminalization and Decriminalization in the Islamic Criminal Law System of Iran. *Criminal Law Research*, 3(8), 33 - 62. **[In Persian]**
Walden, I. (2016). *Computer crimes and digital investigations*. Oxford: Oxford University Press.
Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age (Vol. 4)*. Polity. https://ssrn.com/abstract=1066922
Wiliams, M .(2006). *Virtually criminal: Crime, Devian and regulation online*. London: Routledge.