نوع مقاله: **پژوهشی**

تاریخ دریافت: ۱۴۰۰/۱۰/۰۱
تاریخ پذیرش: ۱۴۰۱/۱۲/۰۶
صفحه: ۱۰۵ الی ۱۲۷

International Legal Research
تحقیقات حقوقی بین المللی

Volume 15, Issue 56, summer 2022

Received: 2021/12/22
Date of Acceptance: 2022/02/25
Pages: 105-127

System: alr.iauctb.ac.ir doi: 10.30495/ALR.2022.1949604.2258 Article Type: **Research**

دوره ۱۵ / شماره ۵۶ / تابستان ۱۴۰۱

Evaluation of the legal criminal policy of Iran and the European Union in relation to computer crimes

Navid Deylami Moazi[1], Mehdi Esmaili✉[2], Hassan Haji Tabar Firouzjaei[3]

Abstract

Field and Aims: The development and expansion of computer science and the increasing desire to use it, apart from creating a technological revolution in the world, has also provided a favorable environment for the emergence of crimes in cyberspace, and its expansion has caused various damages in communities have become. The present research is aimed at preventing and dealing with these crimes and the damages caused by them and how to develop criminal policies around computer crimes in the two platforms of the legislative criminal policy of Iran and the European Union, in order to consider the pioneering role of this Union in fighting against crimes. The cyber space and the development of an efficient criminal policy system should benefit from their experiences in eliminating the weaknesses and gaps in the country's criminal policy in dealing with computer crimes.

Method: The present research was carried out using a descriptive-analytical method.

Finding and Conclusion: The research shows that the strength and correlation of the range of criminal policies adopted in the European Union is greater and deeper than the criminal system of Iran, considering the history and age of legislation and dealing with crimes in the cyber space. The legal criminal policy of Iran is based on the criminal policy and distancing itself from non-criminal preventive measures and not adopting social and situational preventive measures against crime and the lack of proper understanding of the law about such crimes or the inability to predict the types of emerging crimes in the future and the existence of a culture of misuse of space. Cyber is one of the main causes of the ineffectiveness of Iran's criminal policy.

Keywords: computer crimes, legislative criminal policy, Supreme Council of Cyberspace, European Union.

❋Citation (APA): Deylami Moazi, N., Esmaili, M., Haji Tabar Firouzjaei, H. (2022). Evaluation of the legal criminal policy of Iran and the European Union in relation to computer crimes. *International Legal Research*, 15(56), 105-127.
https://alr.ctb.iau.ir/article_689413.html?lang=en

---

1. PhD student in Criminal Law and Criminology, Department of Law, Ayatollah Amoli Unit, Islamic Azad University, Amol, Iran. Email: naviddeilami@gmail.com
2. Assistant Professor, Department of Law, Central Tehran Branch, Islamic Azad University, Tehran, Iran. (Author). Email: Dresmaeli@yahoo.com
3. Assistant Professor, Department of Law, Qaimshahr Branch, Islamic Azad University, Qaimshahr, Iran.Email: hajitabar@yahoo.com

Volume 15, Issue 56, Summer 2022
Received: 2021/12/22
Date of Acceptance: 2022/02/25
Pages: 105-127

تحقیقات حقوقی بین المللی
International Legal Research

نوع مقاله: **پژوهشی**
تاریخ دریافت: ۱۴۰۰/۱۰/۰۱
تاریخ پذیرش: ۱۴۰۱/۱۲/۰۶
صفحه: ۱۰۵ الی ۱۲۷

Article Type: **Research** doi: 10.30495/ALR.2022.1949604.2258 **سامانه:** alr.iauctb.ac.ir

دوره ۱۵ / شماره ۵۶ / تابستان ۱۴۰۱

ارزیابی سیاست جنایی تقنینی ایران و اتحادیه اروپا در قبال جرایم رایانه‌ای

نوید دیلمی معزی[۱]، مهدی اسماعیلی ✉[۲]، حسن حاجی تبارفیروزجائی[۳]

چکیده

زمینه و هدف: توسعه و گسترش علوم رایانه‌ای و تمایل روزافزون به استفاده از آن، گذشته از ایجاد تحول یا انقلاب فناوری در جهان، شرایط و بستری مساعد برای ظهور جرایم در فضای مجازی را نیز فراهم آورده است و گسترش آن سبب ایجاد خسارات گوناگون در جوامع گردیده است. پژوهش حاضر بر آن است در جهت پیشگیری و مقابله با این جرایم و خسارات ناشی از آنها و چگونگی تدوین سیاست‌های جنایی پیرامون جرائم رایانه‌ای در دو بستر سیاست جنایی تقنینی ایران و اتحادیهٔ اروپا بپردازد تا با عنایت به پیشگامی این اتحادیه در مبارزه با جرایم فضای سایبر و تدوین یک نظام کارآمد سیاست کیفری از تجربیات آنان نیز در رفع ضعف‌ها و خلأهای موجود در سیاست جنایی کشور در برخورد با جرایم رایانه‌ای بهره ببرد.

روش: پژوهش حاضر به روش توصیفی- تحلیلی انجام شده است.

یافته‌ها و نتایج: پژوهش بیانگر آن است که قوت و همبستگی طیف سیاست‌های کیفری اتخاذ شده در اتحادیهٔ اروپا با توجه به سابقه و قدمت تقنین و مقابله با جرایم فضای سایبر، نسبت به فضای نظام کیفری ایران بیشتر و عمیق‌تر است. سیاست جنایی تقنینی ایران با تکیه بر سیاست کیفری و فاصله گرفتن از تدابیر پیش‌گیرندهٔ غیرکیفری و اتخاذ نکردن تدابیر پیش‌گیرندهٔ وضعی و اجتماعی از جرم و عدم درک صحیح قانون از این‌گونه جرایم یا عدم توان پیش‌بینی انواع جرایم نوظهور در آینده و وجود فرهنگ استفاده غلط از فضای سایبری از علل اصلی ناکارآمدی سیاست جنایی ایران می‌باشد.

کلیدواژه‌ها: جرایم رایانه‌ای، سیاست جنایی تقنینی، شورای عالی فضای مجازی، اتحادیهٔ اروپا.

❋ استناددهی (APA): دیلمی معزی ، نوید؛ اسماعیلی، مهدی؛ حاجی تبارفیروزجائی، حسن. (۱۴۰۱). ارزیابی سیاست جنایی تقنینی ایران و اتحادیه اروپا در قبال جرایم رایانه‌ای. *تحقیقات حقوقی بین‌المللی*، ۱۵(۵۶)، ۱۲۷-۱۰۵.
https://alr.ctb.iau.ir/article_689413.html

۱. دانشجوی دکتری حقوق کیفری و جرم‌شناسی، گروه حقوق، واحد آیت الله آملی، دانشگاه آزاد اسلامی، آمل، ایران.
رایانامه: naviddeilami@gmail.com

۲. استادیار گروه حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول).
رایانامه: Dresmaeli@yahoo.com

۳. استادیار گروه حقوق، واحد قائمشهر، دانشگاه آزاد اسلامی، قائمشهر، ایران. رایانامه: hajitabar@yahoo.com

مقدمه

جرایم رایانه‌ای حوزه بسیار گسترده‌ای دارند و به فعالیتی گفته می‌شود که در آن کامپیوترها یا شبکه‌های ارتباطی ابزار، مقصد یا محل اجرای یک فعالیت مجرمانه و غیر قانونی می‌باشند. در هر عصر که علم جدیدی کشف می‌شود، مجرمین نیز از جلوه‌های نوین آن علم جهت ارتکاب جرم بهره‌برداری می کنند. تسهیل و تسریع در پیدا کردن کیفر برای جرایم جدید، پیدا کردن سابقهٔ جرم، ردپای جرایم مرتبط و زنجیرهٔ بازداشت، آموزش از اهداف اصلی هستی‌شناسی جرایم رایانه‌ای می‌باشد (عبدی پور کشاورز، انصاری و ششگل، ۱۳۹۹: ۱۴۹).

درست است که ایران و اتحادیهٔ اروپا هر دو از جرایم رایانه‌ای رنج می‌برند و ایران در قبال مبارزه با جرایم رایانه‌ای گام‌های مؤثری برداشته است، ولی با توجه به قراردادی بودن جرایم رایانه‌ای به دلیل پیشرفت تکنولوژی، هنوز خلأهایی احساس می گردد که موارد مذکور در بررسی تطبیقی با سیاست جنایی اتحادیهٔ اروپا نمایان می گردد. اهداف مقابله با جرایم سایبر مستلزم تبیین گونه‌ای از رویکرد کیفری است که لزوماً با اصول و مبانی رویکرد کیفری متعارف همسانی ندارد. بیان ویژگی‌های جرایم سایبر بایستگی تدوین چنین رویکردی را روشن‌تر می‌سازد (جوان جعفری، ۱۳۸۹: ۱۷۵).

به لحاظ امکان وجود سوء استفاده در محیط مجازی و رایانه‌ای، یکی از مسائل مهم در قلمرو سیاست جنایی، مقابله با جرایم رایانه‌ای است که ضروری است مورد توجه قرار گیرد. به عبارتی باید گفت که در مقابله با جرایم رویکردهای مختلفی در جوامع اتخاذ شده است که برخی از این رویکردها سنتی بوده است و توسل به نهادهای قهرآمیز مانند پلیس و واکنش‌های سرکوبگرانه می‌باشد که این رویکردها بر اساس آمارهای جنایی به تنهایی نمی‌تواند جلوه‌های گوناگون بزهکاری را مهار کند؛ از این‌رو به دلیل ناموفق بودن ابزارهای واکنشی (کیفری/ مجازات) برای کاهش بزهکاری، استفاده از ابزارهای کنشی (غیر کیفری) را به منظور پیشگیری از وقوع جرم توجه جرم‌شناسان و به‌تبع آن سیاست‌گذاران جنایی را به خود جلب کرده است (پورقهرمانی، ۱۳۹۵: ۱۷۹). بر این اساس در این مقاله ابتدا سیاست جنایی تقنینی واکنشی علیه جرایم رایانه‌ای در ایران و اتحادیهٔ اروپا مورد ارزیابی قرار می گیرد و سپس سیاست جنایی تقنینی کنشی علیه جرایم رایانه‌ای در ایران و اتحادیهٔ اروپا مطالعه می گردد.

۱. ارزیابی سیاست جنایی تقنینی واکنشی علیه جرایم رایانه‌ای در ایران و اتحادیهٔ اروپا

سیاست جنایی تقنینی واکنشی، مجموعه‌ای از تدابیر مبارزه با بزهکاری به صورت تعیین و تشدید مجازات را دربر می گیرد که در قانون متجلی شده است و ضمانت اجرای مطمئنی چون ضمانت

اجرای قانونی دارد. در این قسمت این نوع سیاست جنایی تقنینی واکنشی در ایران و اتحادیهٔ اروپا مورد بررسی قرار می‌گیرد.

۱-۱. نقاط مثبت

بعد از بیان تعاریف و تشریح سیاست جنایی تقنینی واکنشی، نوبت به بررسی و ارزیابی این سیاست در برخورد با جرایم رایانه‌ای در ایران و اتحادیهٔ اروپا می‌رسد. لذا در این گفتار ابتدا به ارزیابی سیاست جنایی تقنینی واکنشی علیه جرایم رایانه‌ای در ایران و سپس اتحادیهٔ اروپا پرداخته می‌شود.

۱-۱-۱. ارزیابی سیاست جنایی تقنینی واکنشی علیه جرایم رایانه‌ای در ایران

به نظر می‌رسد تنها سیاست جنایی تقنینی واکنشی ایران در خصوص جرایم رایانه‌ای، «قانون جرایم رایانه‌ای» مصوب ۱۳۸۸ می‌باشد. در قانون مذکور مصادیق استفاده مجرمانه از سامانه‌های رایانه‌ای و مخابراتی و تعیین مجازات متناسب با آنها ذکر شده است که می‌توان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی، شنود غیرمجاز، جاسوسی رایانه‌ای و ... را نام برد. یکی از نوآوری‌های قانون‌گذار در خصوص مقابله با جرایم رایانه‌ای، پیش‌بینی «کمیته تعیین مصادیق محتوای مجرمانه» است که مبنای تعیین چنین کمیته‌ای را باید در ویژگی قراردادی جرایم رایانه‌ای جستجو نمود. طبق مادهٔ ۲۲ قانون مذکور: «قوهٔ قضائیه موظف است ظرف یک ماه از تاریخ تصویب این قانون کمیته تعیین مصادیق محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. وزیر یا نمایندهٔ وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر نمایندهٔ مجلس شورای اسلامی به انتخاب کمیسیون حقوقی و قضایی و تأیید مجلس شورای اسلامی اعضای کمیته را تشکیل خواهند داد. ریاست کمیته به عهدهٔ دادستان کل کشور خواهد بود.

تبصره ۱- جلسات کمیته حداقل هر پانزده روز یک‌بار و با حضور هفت نفر عضو دارای حق رأی رسمیت می‌یابد و تصمیمات کمیته با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره ۲- کمیته موظف است به شکایات راجع به مصادیق پالایش شده رسیدگی و نسبت به آنها تصمیم‌گیری کند. رأی کمیته قطعی است.

تبصره ۳- کمیته موظف است هر شش ماه گزارشی در خصوص روند پالایش محتوای مجرمانه را به رؤسای قوای سه‌گانه و شورای عالی امنیت ملی تقدیم کند.

در عمل کمیته مذکور، فهرستی ارائه داد که در پنج فصل در بخش‌های «محتوی خلاف عفت و اخلاق عمومی، محتوی علیه مقدسات، محتوی علیه امنیت و آرامش عمومی، محتوی علیه

مقامات و نهادهای دولتی و عمومی و محتوایی که برای ارتکاب جرایم رایانه‌ای و سایر جرایم» تهیه شده بود. بخشی از این فهرست به مواردی اشاره دارد که در قانون مجازات اسلامی نیز آمده است، ولی در برخی موارد مصادیق ارائه شده تازگی دارد.

نقاط مثبت سیاست جنایی تقنینی واکنشی ایران را می‌توان در موارد ذیل خلاصه کرد:

۱) با ملاحظه قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و مفاد کنوانسیون بین‌المللی بوداپست مصوب ۲۰۰۱ می‌توان نتیجه گرفت که قانون‌گذار ایران در نگارش و تدوین قانون مذکور از مفاد این کنوانسیون الهام گرفته است که این امر نقطه قوت این قانون است.

۲) ضابطه‌مند کردن اقدامات شکلی و توجه به «جمع‌آوری ادلهٔ الکترونیکی»[1] و «استناد پذیری ادلهٔ الکترونیکی» و رفع خلأهای احتمالی با ارجاع نمودن آن به قوانین آیین دادرسی کیفری.

۳) توجه قانون‌گذار به جدیدترین جنبه‌های ماهوی حقوق کیفری فناوری اطلاعات و ارتباطات.

۴) پذیرش مسئولیت کیفری اشخاص حقوقی یکی دیگر از نقاط مثبت در قانون جرایم رایانه‌ای است؛ زیرا «نظام کیفری کشور ما تا قبل از تصویب قانون جرایم رایانه‌ای هیچ‌گاه به‌صراحت و طی فصلی مجزا مسئولیت کیفری اشخاص حقوقی را پیش‌بینی نکرده بود؛ زیرا طبع فردمدارانه حقوق کیفری مانع از آن بود که تکالیف مقرر در قانون به گروه یا جمعی واحد تسری پیدا کند. به همین ترتیب در رویهٔ قضایی (کیفری) نیز هر جا سخن از «شخص» یا «کس» به میان آمده، مخاطبان قانون‌گذار، انسان‌های طبیعی (حقیقی) هستند. البته جابه‌جا و در برخی موارد، مقنن گاه به‌صراحت و روشنی و گاه به‌طور ضمنی با مسئولیت کیفری اشخاص حقوقی برخورد کرده و غالباً همان شخص حقوقی را مسئول پاسخ‌گویی دانسته است» (پاک‌نهاد و سدره‌نشین، ۱۳۹۰: ۲۷).

۱-۱-۲. ارزیابی سیاست جنایی تقنینی واکنشی علیه جرایم رایانه‌ای در اتحادیهٔ اروپا

از آنجا که جوامع اروپایی بیشتر بر اطلاعات و فناوری تکیه می‌کنند، به‌طور فزاینده‌ای در معرض خطر جرایم سایبری قرار می‌گیرند. کنوانسیون بوداپست در مورد جرایم سایبری نه تنها در اروپا بلکه در سراسر جهان پاسخی به این خطر می‌دهد: شورای اروپا از طریق برنامهٔ خود در زمینهٔ جرایم سایبری کمک‌های فنی به کشورهای جهان می‌کند.

شورای اروپا همچنین تهدیدات دیگر مربوط به شبکه را برطرف می‌کند. کنوانسیون پیشگیری از تروریسم[2] (۲۰۰۵) شامل مفاهیمی است که استخدام و آموزش تروریست‌ها از طریق اینترنت را

---

۱. از قبیل نحوه نگهداری داده‌ها و حفظ و ارائه آنها، تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی و شنود محتوای ارتباطات رایانه‌ای.

2. Convention on the Prevention of Terrorism

به‌عنوان یک جرم تروریستی تبدیل می‌کند. کنوانسیون لانزاروت[1] (۲۰۰۷) به سوء استفاده‌های جنسی و سوء استفاده از کودکان می‌پردازد، همچنین محیط آنلاین را نیز در برمی‌گیرد. در این کنوانسیون اقداماتی برای محافظت از کودکان در برابر استثمار و سوءاستفاده جنسی آنلاین پیش‌بینی شده است. کنوانسیون شورای اروپا در مورد حمایت از کودکان در برابر استثمار جنسی و سوء استفاده جنسی که با عنوان «کنوانسیون لانزاروت» نیز شناخته می‌شود، مستلزم جرم‌انگاری کلیهٔ انواع تخلفات جنسی علیه کودکان است. این قانون تصریح می‌کند که کشورها در اروپا و فراتر از آن باید قوانین خاصی را اتخاذ کنند و برای جلوگیری از خشونت جنسی، برای محافظت از کودکان قربانی و پیگرد قانونی مجرمین اقدامات لازم را انجام می‌دهند[2]. کنوانسیون محافظت از داده‌ها[3]نیز جمع‌آوری و استفاده غیرقانونی از داده‌های شخصی را تضمین می‌کند.

شورای اروپا کنوانسیون بوداپست را برای افزایش اثربخشی متون بین‌المللی موجود در زمینهٔ مبارزه با تروریسم اتخاذ کرده است. این هدف برای تقویت تلاش کشورهای عضو برای جلوگیری از تروریسم از دو طریق ذیل است[4]:

۱) با جرم‌انگاری برخی از اعمال، ممکن است منجر به ارتکاب جرایم تروریستی، یعنی تحریک عمومی، استخدام و آموزش شوند.

۲) تقویت همکاری در زمینهٔ پیشگیری، هم در داخل کشور (سیاست‌های پیشگیری ملی) و هم در سطح بین‌المللی (اصلاح دستورالعمل‌های استرداد و کمک‌های متقابل و ابزارهای دیگر).

علاوه بر این، کنوانسیون مذکور شامل مفاد حمایت و جبران قربانیان تروریسم است. یک روند مشاوره برای اطمینان از اجرای مؤثّر و پیگیری برنامه‌ریزی شده است. کنوانسیون سایبری (۲۰۰۱) تنها ابزار الزام‌آور بین‌المللی در این زمینه است. این برنامه به‌عنوان یک دستورالعمل برای هر کشوری است که مایل به تدوین قانون جامع برای مقابله با جرایم سایبری می‌باشد و به عنوان چهارچوبی برای همکاری بین کشورهای عضو خود عمل می‌کند. این پروتکل در مورد اِکسونوفوبیا[5] (تنفر از مردم کشورهای دیگر) و نژادپرستی انجام شده از طریق سیستم‌های رایانه‌ای (۲۰۰۳) تکمیل شده است. این کنوانسیون رفتار را به جای فناوری تعریف می‌کند و اطمینان می‌دهد که با تکامل فناوری، قوانین و رویه‌ها معتبر خواهند ماند. این پیمان از سوی کمیتهٔ کنوانسیون سایبری حمایت می‌شود که نظارت بر اجرای آن دارد و یک دفتر برنامه‌ریزی مقابله با جرایم سایبری در بخارست رومانی که از کشورهای جهان از طریق برنامه‌های ظرفیت‌سازی مانند

1. Lanzarote Convention
2. Council of Europe. 2020. Childrents Rightd. Available from: https://www.coe.int/en/web/children/lanzarote-convention
3. The Data Protection Convention
4 . Council of Europe. 2020. Council of Europe Action against Cybercriame Available from: https://www.coe.int/en/web/portal/coe-action-against-cybercrime
5. Xenophobia

پروژهٔ «اقدام جهانی علیه جرایم سایبری»[1] در زمینهٔ اقدام جهانی علیه جرایم سایبری پشتیبانی می‌کند[2].

سیاست تقنینی اتحادیهٔ اروپا در مقابل جرایم رایانه‌ای که توسط شورای جرایم سایبری اتحادیهٔ اروپا انجام می‌گیرد، به شرح ذیل است:

۱) تلاش در جهت جرم‌انگاری اقدامات ضد محرمانگی، یکپارچگی و در دسترس بودن داده‌ها و سیستم‌های رایانه‌ای، جرایم مربوط به رایانه، جرایم مربوط به محتوا (هرزه‌نگاری کودک، نژادپرستی و زنوفوبی) و جرایم مربوط به نقض کپی‌رایت و حقوق مرتبط.

۲) تلاش در جهت اتخاذ روش‌هایی که تحقیقات را کارآمدتر کند.

۳) فراهم کردن مبنای قانونی برای همکاری‌های بین‌المللی بین کشورهای عضو این کنوانسیون، از جمله تبادل اطلاعات خودبه‌خود، استرداد و کمک‌های متقابل بین‌المللی.

دستاوردهای اتحادیهٔ اروپا در زمینهٔ سیاست تقنینی را می‌توان به شرح ذیل نام برد:

۱) بسیاری از کشورها قوانین خود را با استفاده از کنوانسیون جرایم سایبری به عنوان یک دستورالعمل یا «قانون نمونه»[3] تقویت می‌کنند.

۲) با تصویب قوانین مشابه، همکاری بین ذی‌نفعان و بازیگران اصلی تقویت شده است که شامل همکاری و مشارکت‌های عمومی و خصوصی می‌شود.

۳) کنوانسیون‌ها، دستورالعمل‌هایی برای تقویت همکاری بین مقامات مجری قانون (انتظامی)[4] ارائه دهندگان خدمات اینترنت، در بررسی جرایم سایبری تحت عنوان پروژه جرایم سایبری (۲۰۰۸)[5] هستند. این دستورالعمل‌ها اکنون در چندین کشور اعمال می‌شود و اتحادیهٔ اروپا نیز از آنها استفاده می‌کند.

۴) اتحادیه‌ی اروپا در زمینه استرداد مجرمین رایانه‌ای، همکاری‌های مؤثّری با یکدیگر دارند.

۱-۲. چالش‌ها و محدودیت‌ها

پس از بیان نقاط قوت، سیاست تقنینی واکنشی در خصوص مبارزه با جرایم رایانه‌ای دارای چالش‌ها و محدودیت‌هایی در حقوق ایران و اتحادیهٔ اروپا است. لذا در این قسمت به این موارد اشاره می‌گردد.

1 . GLACY (Global Action on Cybercrime)
2 . Council of Europe. 2020. Council of Europe Action against Cybercriame Available from: https://www.coe.int/en/web/portal/coe-action-against-cybercrime
3. model law
4. law enforcement authorities
5. Project on Cybercrime

۱-۲-۱. چالش‌های سیاست تقنینی واکنشی در قانون جرایم رایانه‌ای ایران

از چالش‌های سیاست تقنینی واکنشی در قانون جرایم رایانه‌ای ایران، می‌توان به موارد ذیل اشاره نمود:

۱) متأسفانه ایران تاکنون به هیچ یک از اسناد بین‌المللی مربوط به جرایم رایانه‌ای از جمله کنوانسیون بین‌المللی جرایم سایبری بوداپست ۲۰۰۱ ملحق نشده است که پیگیری جرایم رایانه‌ای و همکاری و معاضدت‌های بین‌المللی برای جمع‌آوری دلایل الکترونیکی و رهگیری ارتباطات سایبری را با مشکلاتی اساسی مواجه می‌سازد و این امر یکی از نقاط ضعف می‌باشد.

۲) در قانون جرایم رایانه‌ای، تنها مجازات‌های اصلی، «حبس» و «جزای نقدی» است که به‌تنهایی و بدون به‌کارگیری ابزارهای غیر کیفری (اداری، اجتماعی، مدنی و...) مورد قبول حقوقدانان و کارشناسان فناوری اطلاعات و ارتباط نیست» (پاک‌نهاد و سدره‌نشین، ۱۳۹۰: ۳۰).

۳) مادۀ ۷۵۵ (۲۷) قانون جرایم رایانه‌ای چندان کارایی نخواهد داشت و با واقعیات امروز همخوانی ندارد. ماده مذکور مقرر می‌دارد: «در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنۀ مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند...». علت این امر آن است که افراد محروم از خدمات مذکور، می‌توانند به‌راحتی از طریق دوستان و بستگان خود خدمات مذکور را انجام دهند.

۴) در بند «د» مادۀ ۷۵۴ (۲۶) قانون جرایم رایانه‌ای به «جرایم سازمان‌یافته» اشاره نموده است که هنوز قوانین و مقررات شکلی و ماهوی مدونی در رابطه با جرایم مذکور در ایران به تصویب نرسیده است.

۵) در قانون جرایم رایانه‌ای، ضابطان خاصی برای جمع‌آوری، مداخله، تفتیش، توقیف و حفظ و نگهداری داده‌ها از سامانه‌های رایانه‌ای و مخابراتی مشخص نشده است. بهتر بود مأموران پلیس سایبری (فتا) به‌عنوان مقام صلاحیت‌دار در قانون نام برده می‌شدند؛ زیرا باید ضابطان دادگستری به نحو دقیق و شایسته‌ای با شیوه صحیح در اختیار گرفتن داده‌ها و سامانه‌های مذکور آشنا باشند. بهتر بود قانون‌گذار دلایل مشخصی را به‌عنوان مصداق برای توجیه صدور مجوّز قضایی تفتیش و توقیف سامانه‌های رایانه‌ای و مخابراتی نام می‌برد تا از تعرّض‌های احتمالی بی‌مورد، به حقوق اشخاص و حق خلوت آنان جلوگیری شود. همچنین مدّت اعتبار مجوّزهای مذکور نیز در قانون مشخص نشده است (پاک‌نهاد و سدره‌نشین، ۱۳۹۰: ۳۹-۳۸).

۶) از نظر سیاست جنایی، مقنن قانون جرایم رایانه‌ای به جبران خسارت معنوی[1] توجه آن چنانی نداشته است، به نحوی‌که در برخی موارد به صرف جرم‌انگاری اعمالی که علیه حیثیت افراد است

1. Immaterial restitution

(با ضمانت اجراهای نسبتاً ضعیف حبس یا جزای نقدی) اکتفا شده است (مواد ۱۸-۱۶) و به جبران ضرر و زیان معنوی ناشی از بزه‌دیدگی جرایم مذکور توجه خاصی نشده است و صرفاً در مادهٔ ۷۴۶ (۱۸) قانون جرایم رایانه‌ای، آن هم به صورت مردد بر جبران خسارات معنوی «... افزون بر اعاده حیثیت (در صورت امکان) ...» در نظر گرفته شده است (پورقهرمانی، ۱۳۹۶: ۲۳).

۷) غفلت قانون‌گذار ایران از برخی جرایم مانند:

- جاسوسی صنعتی که جنگ پیشرفت و فناوری در عرصهٔ اقتصاد می‌باشد، از نظر مقنن دور نگه داشته شده است؛

- عدم جرم‌انگاری حملات سایبری به دیگر کشورها برای مقاصدی از قبیل دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، تخریب و اخلال در داده‌ها یا سامانه‌ها؛

- قانون در مورد سرقت هویت و یا داده‌های هویتی اشخاص در فضای سایبر ساکت است؛

- عدم جرم‌انگاری آزاررسانی و به ستوه‌آوری اشخاص در بستر فضای سایبر؛

- دسترسی غیرمجاز به سامانه‌هایی که با تدابیر امنیتی حفاظت نشده‌اند، مورد توجه قانون‌گذار قرار نگرفته است (با لحاظ اینکه امنیت سامانه، یک مفهوم نسبی است)؛

- عدم توجه به افشای داده های غیرسرّی که ممکن است به امنیت کشور یا منافع ملّی لطمه وارد کند؛

- سرقت زمان سامانه‌های رایانه‌ای و مخابراتی مورد تصریح قانون‌گذار قرار نگرفته است؛

۸) عدم رویکرد افتراقی از رهگذر کیفرگذاری تشدیدی در مورد هرزه‌نگاری کودکان نسبت به بزرگسالان و سیاست پاسخ‌دهی غیر حمایتی و غیراختصاصی اعمال شده است.

۲-۲-۱. چالش‌های سیاست تقنینی واکنشی در خصوص جرایم رایانه‌ای اتحادیهٔ اروپا

چالش‌های پیش‌رو در سیاست جنایی تقنینی واکنشی به شرح ذیل است:

۱) در خصوص اتحادیهٔ اروپا، یک راه حل برای حل و پیشگیری از مشکلات پیش‌رو، غلبه بر اصطکاکی است که قوانین ملی با جرایم سایبری روبه‌رو هستند. همگرایی قوانین در بین اروپا (و سایر کشورها) ممکن است راه حل فنی برای بسیاری از مشکلات مربوط به چهارچوب فعلی همکاری‌های بین‌المللی ارائه دهند (کالدرونی، ۲۰۱۰).

۲) ظهور و پیشرفت فناوری اطلاعات و تهدیدات جدید رایانه‌ای، فراتر از تدوین و اجرای قوانین اتحادیهٔ اروپا است. قوانین و رویه‌های اتحادیهٔ اروپا با توجه به عصر دیجیتال کافی نبوده و توسعه رویه‌های نوآورانه و انعطاف‌پذیر برای تضمین یک سیاست و چارچوب قانونی مناسب با هدف پیش‌بینی بهتر و شکل دادن به آینده، یک اولویت اساسی است (دادگاه اروپایی حسابرسان، ۲۰۱۹: ۱۸).

۳) نهادهای قانون‌گذاری بالأخص در سطح جوامع محلی ناتوان از وضع قوانین قدرتمند و قاطع در مبارزه با جرایم رایانه‌ای می‌باشد که در ماورای مرزهای جغرافیایی آنان رخ می‌دهد. در این خصوص کمبود نیرو و بودجه نیز بر خلأ موجود دامن می‌زند (توماس[1]، ۲۰۱۸: ۱۴۳).

۲. ارزیابی سیاست جنایی تقنینی کنشی در قبال جرایم رایانه‌ای در ایران و اتحادیهٔ اروپا

سیاست جنایی تقنینی کنشی، مجموعه‌ای از تدابیر مبارزه با بزهکاری به صورت پیشگیری را در بر می‌گیرد که در قانون متجلی شده است. در این قسمت این نوع سیاست جنایی تقنینی کنشی در ایران و اتحادیهٔ اروپا مورد بررسی قرار می‌گیرد.

۲-۱. نقاط مثبت

۲-۱-۱. ارزیابی سیاست جنایی تقنینی کنشی در قبال جرایم رایانه‌ای در ایران

در خصوص ارزیابی سیاست جنایی تقنینی کنشی در قبال جرایم رایانه‌ای در ایران، می‌توان به قانون پیشگیری از وقوع جرم مصوب ۱۳۹۵، مصوبات شورای عالی فضای مجازی و اساسنامه مرکز ملی فضای مجازی اشاره نمود که در این گفتار به آنها پرداخته می‌شود.

۲-۱-۱-۱. قانون پیشگیری از وقوع جرم

قانون پیشگیری از وقوع جرم نمونه‌ای از سیاست جنایی تقنینی کنشی است که می‌توان در حوزهٔ مبارزه با جرایم رایانه‌ای نیز از آن استفاده نمود. مادهٔ ۳ قانون مذکور در خصوص تشریح وظایف شورای عالی پیشگیری از وقوع جرم می‌باشد که بند سوم آن «بررسی و تصویب برنامه‌های کلان برای گسترش فرهنگ، ایجاد زمینه‌های مشارکت مردم و نهادهای دولتی و غیردولتی در امر پیشگیری از وقوع جرم و حمایت از آنها» به‌عنوان یکی از وظایف شورای مذکور برشمرده است.

مادهٔ ۵ قانون پیشگیری از وقوع جرم به وظایف دبیرخانه شورای عالی در قوهٔ قضاییه اشاره دارد که بند دوم و سوم آن بر جلب مشارکت نهادهای مردمی و دانشگاهی تأکید نموده و انجام تحقیقات و پژوهش‌های مورد نیاز برای آسیب‌شناسی علل وقوع جرم و راه‌های پیشگیری از آن از طریق نهادهای تحقیقاتی در قوای سه‌گانه و مراکز پژوهشی دانشگاهی و در صورت نیاز انجام تحقیقات مذکور به‌صورت مستقل و تهیه و انتشار گزارش‌های آماری ادواری و سالانه و شناسایی راه‌های جلب مشارکت مردمی و حمایت از سازمان‌های مردم‌نهاد و نهادهای غیردولتی در امر پیشگیری از وقوع جرم در چهارچوب قوانین و مقررات و مصوبات شورا را از وظایف دبیرخانه شورای عالی پیشگیری از وقوع جرم در قوهٔ قضاییه نام برده است.

1. Thomas

با توجه نقص‌های قانون پیشگیری از جرم مصوب ۱۳۹۴ و ناکارآمدی آن و نگرش مثبت و ایجابی در تدوین استراتژی پیشگیرانه و توجه به توانمندسازی جامعه در مواجهه با آسیب‌های فضای مجازی می‌توان به تدوین و تصویب پیش‌نویس استراتژی پیشگیری از آسیب‌های فضای مجازی در ایران نیز گام برداشت (کرامتی معز، ۱۳۹۹: ۱۲۷).

۲-۱-۱-۲. مصوبات شورای عالی فضای مجازی

اولین نهاد تأسیس شده در رابطه با فضای مجازی، شورای عالی فضای مجازی است که در ۱۷ اسفند ماه ۱۳۹۰ به وجود آمد. این شورا فرا قوه‌ای می‌باشد و این بدان معنا است که وابسته به هیچ نهاد یا قوه‌ای نیست (منصورآبادی، میرخلیلی و کرامتی معز، ۱۴۰۰: ۳۷).

در ادامه به برخی مصوبات این شورا اشاره می‌گردد:

در مصوبه این شورا با موضوع توسعه فضای مجازی سالم، مفید و امن به شماره ۹۴/۱۰۰۱۵۱ش مصوب ۱۳۹۴/۱/۳۰ به تعریف فضای مجازی ایمن پرداخته شده است. در این مصوبه آمده است: «فضای ایمن، فضایی است متشکل از شبکه‌های ارتباطی که در آن، محتوا و خدمات مفید در چهارچوب مبانی و ارزش‌های اسلامی و مقررات کشور ارائه می‌شود و کاربران می‌توانند بر اساس ویژگی‌های جمعیتی از قبیل سن، جنس، شغل و تحصیلات از محتوا و خدمات مورد نیاز بهره‌مند شوند و حتی‌الامکان در برابر محتوا و رفتارهای آسیب‌زا محفوظ بمانند».

در عنوان این مصوبه هرچند به توسعه فضای مجازی سالم، مفید و ایمن پرداخته شده است، اما در تعریفی که از فضای ایمن ارائه شده، به نظر می‌رسد فضای ایمن به لحاظ محتوایی مد نظر بوده؛ یعنی فضایی که محتوای آن در چهارچوب مبانی اسلامی باشد. به عبارت بهتر در این مقرره قانون‌گذار صرفاً به پالایش محتوا توجه داشته در حالی‌که پالایش یک اقدام حفاظتی محسوب نمی‌شود (فضلی، ۱۳۹۶: ۱۱۱). دلیل این امر این است که پالایش همواره از سوی مقامات دولتی و برای پاک‌سازی یک وب‌سایت یا سایت از اطلاعاتی که به لحاظ مضمون با مبانی اخلاقی و اسلامی ناسازگارند به‌کار رفته و جنبهٔ حفاظتی ندارد؛ در حالی‌که آنچه در حفاظت از اطلاعات مالی مد نظر است، این است که از اطلاعات مالی حفاظت به عمل آید تا این اطلاعات، افشاء، تخریب، محو و ... نشوند که این حفاظت می‌تواند هم از سوی اشخاص حقیقی و هم حقوقی باشد.

مصوبهٔ دیگر، تحت عنوان «سیاست‌های ساماندهی خدمات پیامکی ارزش‌افزوده و پیامک انبوه در شبکه‌های ارتباطی» به شماره ۹۳/۱۰۶۶۸۱ش مورخ ۱۳۹۳/۱۱/۱ از سوی شورای مذکور صادر شده است که در بند ۴ این مصوبه آمده است: «به منظور حفظ و صیانت از اطلاعات خصوصی مخاطبان پیام و بر اساس قوانین به ویژه قانون جرایم رایانه‌ای، ارائه‌دهندگان خدمات

ارتباطی و ارائه‌دهندگان خدمات محتوایی، حق واگذاری، فروش و یا در اختیار قرار دادن این اطلاعات به دیگران را ندارند». در این مصوبه نیز هرچند به حفاظت و حراست از اطلاعات اشاره شده، اما تنها به حفاظت از اطلاعاتی که مربوط به حریم خصوصی شهروندان است، پرداخته شده و به اطلاعات مالی به‌طور خاص توجهی نشده است (جاویدنیا، ۱۳۹۱: ۵). دلیل این امر چندان مشخص نیست، اما به نظر می‌رسد یا وصف اطلاعات مالی برای مقنن ناشناخته بوده و از این‌رو حمایتی از این اطلاعات به عمل نیاورده و یا اطلاعات مالی را نیز بخشی از اطلاعات شخصی افراد قلمداد نموده و آنها را همانند اطلاعات شخصی مشمول حمایت قرار داده است. به این استدلال این خدشه وارد می‌شود که اولاً از اطلاعات مالی اشخاص حقوقی در این قالب نمی‌توان حفاظت نمود؛ ثانیاً اقداماتی هم که جهت حفاظت از اطلاعات شخصی به عمل آمده، تدابیر واسطه‌ای هستند. این تدابیر، تدابیری هستند که در پی تنظیم مقررات مناسب برای حفاظت از اطلاعات‌اند (وطنی و اسدی، ۱۳۹۵: ۱۱۲).

مصوبهٔ دیگر این شورا در خصوص «شرح وظایف، اختیارات و اعضای کمیسیون عالی امنیت فضای مجازی کشور» می‌باشد که شورای عالی فضای مجازی در نهمین جلسه مورخ ۱۳۹۱/۷/۲۲، براساس مادهٔ ۹ اساسنامه مرکز ملی فضای مجازی، شرح وظایف و اختیارات کمیسیون مذکور را تصویب نمود. این وظایف و اختیارات به شرح ذیل است:

ـ فراهم آوردن شرایط لازم برای دستیابی فضای مجازی کشور به بالاترین سطح از امنیت و سلامت برای آحاد مردم، نظام و کلیهٔ نقش‌آفرینان در فضای مجازی در چهارچوب مصوبات شورای عالی.

ـ ایجاد آمادگی لازم در عالی‌ترین سطح به منظور صیانت از زیرساخت‌های حیاتی در برابر حملات اینترنتی و دفاع مناسب در برابر هرگونه حمله در چهارچوب مصوبات شورای عالی.

ـ تقسیم‌کار ملی، هماهنگی و هم‌افزایی در فضای مجازی کشور در ابعاد امنیتی، انتظامی و دفاعی در چهارچوب مصوبات شورای عالی.

ـ پایش و رصد عالمانه، نظام‌مند و مستمر تهدیدهای فضای مجازی برای کشور و تدابیر لازم برای مواجهه به‌موقع و مبتکرانه با آنها در چهارچوب مصوبات شورای عالی.

ـ ساماندهی امنیت فضای مجازی کشور در شرایط عادی و بحرانی و همچنین تهیه و تصویب ضوابط، آیین‌نامه‌ها و دستورالعمل‌های مورد نیاز در این عرصه و نظارت مستمر بر حسن اجرای آنها در چهارچوب مصوبات شورای عالی.

ـ مدیریت تشخیص حملات سایبری به کشور و همچنین دفاع از زیرساخت‌های حیاتی در برابر حملات سایبری از داخل و خارج کشور در چهارچوب مصوبات شورای عالی.

ـ تهیه و تصویب دستورالعمل‌ها و پیوست‌های امنیتی پروژه‌ها و طرح‌های فضای مجازی کشور در چهارچوب مصوبات شورای عالی.

تبصره ۱- هر دستگاه و یا نهادی که در حوزهٔ امنیت و دفاع فضای مجازی فعالیت می‌نماید ملزم به فعالیت با هماهنگی و در چهارچوب مصوبات این کمیسیون می‌باشد».

مصوبهٔ دیگر این شورا، «سیاست‌های حاکم بر برنامه‌های رایانه‌ای» نام دارد و مصوبه جلسه بیست و ششم مورخ ۲۵/۰۹/۱۳۹۴ شورای عالی فضای مجازی با موضوع «سیاست‌های حاکم بر برنامه ملّی بازی‌های رایانه‌ای»، که به استحضار مقام معظم رهبری (مدظله‌العالی) رسیده است، طی نامه شماره ۱۰۳۵۵۷/۹۴/ش در تاریخ ۱۰/۱۲/۱۳۹۴ توسط دبیر شورای عالی فضای مجازی ابلاغ شد.

در بند ۱۰ سیاست مذکور، به «اصلاح و تنقیح قوانین مرتبط از جمله قانون جرایم رایانه‌ای در جهت افزایش بازدارندگی، کاهش تکرار تخلفات و جرایم، حفظ حریم خصوصی و حقوق مصرف‌کننده» اشاره شده است. ظاهراً تدابیر پیش‌بینی شده در این بند تنها ناظر به حفظ حریم خصوصی است و اطلاعات مالی اشخاص حقوقی، تحت شمول این مقرره قرار نمی‌گیرند، ولی به نظر می‌رسد حمایت از حقوق مصرف‌کننده می‌تواند شامل حمایت از اطلاعات مالی مشتریان نیز شود که این مشتریان، هم می‌توانند اشخاص حقوقی و هم اشخاص حقیقی باشند.

در مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه مصوب ۱۳۸۰ قانون‌گذار در بند «ب» مادهٔ ۶ به استفاده از تدابیر فنی جهت صیانت از شبکه‌ها و اطلاعات تصریح کرده است. در این بند آمده: «سیستم بارو[1] مناسب به منظور صیانت شبکه‌ها از تخریب، فریب و سرقت اطلاعات به کار می‌رود».

در این مقرره، قانون‌گذار به امنیت اطلاعات به‌طور صریح پرداخته است. اطلاعات به‌کار رفته در این متن مطلق می‌باشد و شامل اطلاعات مالی و غیرمالی می‌گردد. در این مقرره تنها به حفاظت از اطلاعات در برابر سرقت، تخریب و فریب اشاره شده؛ در حالی‌که بهتر بود مقنن به حفاظت از اطلاعات در برابر تهدیدات به نحو مطلق اشاره می‌کرد.

مرجعی باید خود را مسئول حاکمیت ایران بر اینترنت بداند تا بتواند در این امر مهم، بین کلیه نهادها، سازمان‌ها، وزارتخانه‌ها، بخش خصوصی و قوانینی که با هم، همپوشانی یا تعارض دارند، هماهنگی لازم را ایجاد نماید. فرصت‌ها و تهدیدهای این فضا را رصد نموده و تصمیمات مقتضی را برای وضعیت فعلی و آینده بگیرد. اختصاص شورای عالی فضای مجازی بر انجام این مهم، می‌تواند تصمیم مناسبی باشد؛ اگر در طراحی نظام حقوق فضای مجازی مرجعی نظیر شورای عالی فضای مجازی برای یکسان‌سازی قوانین و نظارت بر مراجع و نهادهای کثیری که بر فضای اینترنت

1. Firewall

قانون‌گذاری می‌کنند، ایجاد شود، امر سیاست‌گذاری، قانون‌گذاری و هماهنگی در اداره این فضا، وضعیت مطلوب‌تری را خواهد داشت؛ بنابراین، نقش شورای عالی فضای مجازی در راستای تدابیر نظارتی در محور پیشگیری از جرایم رایانه‌ای کلیدی و مهم است (منصورآبادی، میرخلیلی و کرامتی معز، ۱۴۰۰: ۴۱-۴۰).

۲-۱-۱-۳. اساسنامه مرکز ملی فضای مجازی

در مادۀ ۲ اساسنامه مرکز ملی فضای مجازی «به مقابله با تهدیدات فضای مجازی از نظر فنی و محتوایی» پرداخته شده است. یکی از مهم‌ترین تهدیدات در حوزۀ سایبر، تهدیداتی است که علیه محرمانگی و اصالت اطلاعات مالی صورت می‌گیرد. در بند ۱ مادۀ ۲ اساسنامه مذکور، «مواجهه فعال و مبتکرانه با فضای مجازی در سطح ملی و جهانی و توسعه آن به میزان آمادگی قطعی نظام (از نظر فنی و محتوایی) برای استفاده از فرصت‌ها و مقابله با تهدیدات آن» به عنوان یکی از سیاست‌ها و اهداف مرکز ملی فضای مجازی شمرده شده است.

بر اساس اساسنامه فوق در بند چهار ماده دوم، یکی از اهداف و سیاست‌های مرکز «آموزش عمومی[1] و فرهنگ‌سازی در جهت بالا بردن سواد اینترنتی، هشیارسازی مردم در مورد مخاطرات فضای سایبری و انگیزه دادن به مردم برای مقابله با مخاطرات آن در زندگی فردی و اجتماعی» برشمرده شده است (مهدوی ثابت و عبدالهی، ۱۳۹۹: ۲۱-۲۰).

مصوبۀ دیگر این شورا «تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه سال ۱۳۹۳» است. مصوبات جلسه پانزدهم مورخ ۳۰/۱۰/۱۳۹۲ شورای عالی فضای مجازی با موضوع «تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه سال ۱۳۹۳ مرکز ملی فضای مجازی» که به استحضار مقام معظم رهبری (مدظله‌العالی) رسیده است، طی نامۀ شماره ۱۰۲۴۶۸/۹۲/ش در تاریخ ۱۳۹۲/۱۱/۱۲ توسط دبیر شورای عالی فضای مجازی ابلاغ شد. در بند چهارم مصوبۀ دوم به «شبکه‌ای با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضا دیجیتالی به کلیۀ کاربران» پرداخته شده است. در این مقرره، قانون‌گذار تنها به امنیت شبکه توجه داشته و اشاره‌ای به امنیت اطلاعات نکرده است. امنیت شبکه به فرآیند ایمن‌سازی گفته می‌شود که طی آن یک شبکه با استفاده از استانداردهای امنیتی در مقابل انواع مختلف تهدیدات اعم از داخلی و خارجی امن می‌شود؛ به عبارت دیگر، امنیت شبکه ناظر به حفاظت از شبکه در مقابل حملات است که گاه این حملات منجر به تخریب کل شبکه و گاه منجر به دسترسی غیرمجاز به

---

۱. خوشبختانه، وزارت آموزش و پرورش با احیای ششم ابتدایی گام مثبتی را در این راستا برداشته است و در مقطع ششم ابتدایی درسی را با عنوان «کار و فناوری»، با محتوای فناوری اطلاعات و ارتباطات گنجانده است که در نوع خود قابل تحسین است که می‌تواند نقش بسزایی در تربیت و آموزش کودکان از تخلفات و جرایم رایانه ای باشد (کرامتی معز و میرخلیلی، ۱۳۹۹: ۱۰).

منابع و اطلاعات می‌شود. با این حال در امنیت شبکه، متخصصان بیشتر بر عملکرد صحیح سیستم کامپیوتری تمرکز دارند؛ در حالی‌که در امنیت اطلاعات، بیشتر، تأکید بر حفاظت از اطلاعات خصوصاً اطلاعات با ارزش اشخاص است تا در پرتو این حفاظت بتوان از ضررهای هنگفتی که ممکن است در اثر رفتارهای مخرب به اشخاص وارد آید، جلوگیری نمود. سایر تدابیر پیشنهاد شده در مصوبهٔ دوم که مربوط به الزامات حاکم بر تحقق شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباط فضای مجازی کشور است، عبارت است از:

۱) شبکه‌ای متشکل از زیرساخت‌های ارتباطی با مدیریت مستقل کاملاً داخلی؛

۲) شبکه‌ای کاملاً مستقل و حفاظت شده نسبت به دیگر شبکه‌ها (از جمله اینترنت) با امکان تعامل مدیریت شده با آنها؛

۳) شبکه‌ای با امکان عرضهٔ انواع محتوا و خدمات ارتباطی سراسری برای آحاد مردم با تضمین کیفیت از جمله قابلیت تحرک؛

۴) شبکه‌ای با قابلیت عرضهٔ انواع خدمات امن اعم از رمزنگاری و امضای دیجیتالی به کلیهٔ کاربران؛

۵) شبکه‌ای با قابلیت برقراری ارتباطات امن و پایدار میان دستگاه‌ها و مراکز حیاتی کشور؛

۶) شبکه‌ای پرظرفیت، پهن‌باند و با تعرفهٔ رقابتی شامل مراکز داده و میزبانی داخلی.

الزامات پیش گفت، در جهت خدمت‌رسانی امن به کاربران تدوین شده و همگی در قالب تدابیر پیشگیری فنی‌اند. در این مصوبه، تنها به تدابیر فنی از جمله رمزنگاری و امضای دیجیتال اشاره شده است و هدف مصوبهٔ مذکور، حفظ و ارتقای شبکه ملی ارتباطات از لحاظ فنی می‌باشد. شبکه ملی اطلاعات، به‌عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است به صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود.

۲-۱-۲. ارزیابی سیاست جنایی تقنینی کنشی در قبال جرایم رایانه‌ای در اتحادیهٔ اروپا

امروزه قوانین و مقرراتی در سطح اتحادیهٔ اروپا برای مقابله با حملات علیه سیستم‌های اطلاعاتی توسط کشورهای عضو تعیین شده است. طبق قوانین جدید، دسترسی غیرقانونی، مداخله در سیستم یا رهگیری جرایم جنایی در سراسر اتحادیهٔ اروپا جرم‌انگاری شده است. سازندگان به اصطلاح «بات نت»[1]، شبکه‌های رایانه‌ای آلوده که مجرمان می‌توانند از سوء استفاده‌های خود استفاده کنند،

1.Botnets

با تحریم‌های کیفری روبه‌رو هستند، همانند نویسندگان انواع دیگر بدافزارها. دستورالعمل حمله به سیستم‌های اطلاعاتی همچنین قوانین جدیدی را برای تقویت همکاری سریع بین مقامات اجرای قانون کشورهای عضو وضع کرده است. دستورکار اروپا در زمینهٔ امنیت، جرایم سایبری را یکی از سه اولویت اصلی دستور فعلی کمیسیون اروپا در حوزهٔ امنیت قرار می‌دهد. «مجرمان سایبری حقوق اساسی شهروندان اتحادیهٔ اروپا را نقض می‌کنند و به اقتصاد ما آسیب می‌رسانند. کاربران حق دارند به صورت آنلاین احساس امنیت کنند و عاملان نباید احساس کنند که می‌توانند با مصونیت از مجازات عمل کنند. برای تقویت اعتماد به خدمات آنلاین که برای تک بازار دیجیتال ضروری است. اجرای این دستورالعمل گامی اساسی در جهت همکاری نزدیک‌تر در سراسر اتحادیهٔ اروپا است»[1].

در خصوص سیاست تقنینی کنشی اتحادیهٔ اروپا می‌توان به موارد ذیل اشاره نمود:

۲-۱-۲-۱. نهاد نظارتی MONEYVAL

مطالعهٔ تایپولوژی[2] در مورد «گردش مالی کیفری»[3] در اینترنت توسط پروژهٔ جهانی جرایم سایبری به‌صورت مشترک با MONEYVAL و به رهبری فدراسیون روسیه انجام گرفته است. MONEYVAL یک نهاد نظارت دائمی شورای اروپا است که وظیفهٔ ارزیابی انطباق قوانین و مقررات با معیارهای اصلی بین‌المللی در مقابله با پول‌شویی و تأمین مالی تروریسم و اثربخشی اجرای آنها و همچنین وظیفهٔ ارائهٔ توصیه به مقامات ملی را به عهده دارد. با توجه به پیشرفت‌های لازم در سیستم‌هایشان، این سازمان قصد دارد ظرفیت‌های مقامات ملی را برای مبارزه با پول‌شویی و تأمین مالی تروریسم به‌طور مؤثر بهبود بخشد. MONEYVAL که سابقاً (PC-R-EV) نام داشت، در سال ۱۹۹۷ تأسیس شد و عملکرد آن با مفاد کلی قطعنامه 47 (2005) Res در مورد کمیته‌ها و نهادهای تابعه، شرایط مرجع آنها و روش‌های کاری تنظیم می‌شد. هیات وزیران در جلسه خود در تاریخ ۱۳ اکتبر ۲۰۱۰ قطعنامه 12 (2010) CM Res را در مورد اساسنامه کمیتهٔ خبرگان ارزیابی اقدامات ضد پول‌شویی و تأمین مالی تروریسم (MONEYVAL) تصویب کرد. اساسنامه از ۱ ژانویه ۲۰۱۱ به MONEYVAL این امکان را داد تا یک مکانیسم نظارت مستقل در شورای اروپا باشد که مستقیماً در برابر کمیتهٔ وزرا پاسخ‌گو است. اساسنامه MONEYVAL در

1. European Commission. 2015. Combating Cybercrime: EU-wide rules against cyber attacks come into force. Available at: https://ec.europa.eu/home-affairs/what-is-new/news/news/2015/20150904_1.

۲. نوع شناسی مجموعه ای از دسته‌های مورد استفاده برای طبقه بندی است.

3. criminal money flows

سال ۲۰۱۳ توسط قطعنامه CM / Res (2013) 13 و در سال ۲۰۱۷ توسط قطعنامه CM / Res 19 (2017) اصلاح شد[1].

۲-۱-۲-۲. همکاری و آموزش

ظرفیت‌های قوی‌تر برای تحقیقات بین‌المللی از طریق ایجاد نقاط تماس ۷/۲۴، آموزش مقامات برای همکاری قضایی و همکاری نزدیک‌بین شورای اروپا، اینترپل، یوروپول و زیر گروه جرایم فناوری پیشرفته G8.

۱) از طریق برنامهٔ مقابله با جرایم سایبری به ایالات کمک می‌شود. این پروژه شامل پروژه‌های مشترک با اتحادیهٔ اروپا و پروژهٔ جهانی در زمینهٔ جرایم سایبری (با بودجه استونی، ژاپن، موناکو، رومانی، انگلستان، مایکروسافت، مک آفی و ویزای اروپا) است.

۲) هر ساله شورای اروپا کنفرانس اختاپوس در مورد جرایم سایبری را برگزار می‌کند که متخصصان سراسر دنیا را برای تبادل دانش و تجربه جمع می‌کنند. کنفرانس اختاپوس که هر ۱۲ تا ۱۸ ماه توسط شورای اروپا برگزار می‌شود، یکی از بزرگ‌ترین و بهترین سکوهای تبادل نظر در زمینهٔ تجمع متخصصان جرایم سایبری از ۸۰ کشور، سازمان‌های بین‌المللی، بخش خصوصی و دانشگاه‌ها است. هر کنفرانس اختاپوس تمرکزی خاص است که به جدیدترین موضوع جرایم سایبری مرتبط می‌باشد. کنفرانس Octopus 2019 در تاریخ ۲۰-۲۲ نوامبر ۲۰۱۹ برگزار می‌شود[2].

۲-۱-۲-۳. دفتر برنامه‌ریزی جرایم سایبری شورای اروپا (C-PROC)[3]

۲-۱-۲-۳-۱. مبنا و پایه

این دفتر در بخارست (پایتخت کشور رومانی) قرار دارد و وظیفهٔ کمک به کشورهای سراسر جهان در راستای تقویت ظرفیت سیستم‌های حقوقی‌شان برای پاسخ‌گویی به چالش‌های ناشی از جرایم سایبری و ادلهٔ الکترونیکی بر اساس استانداردهای کنوانسیون بوداپست نسبت به جرایم سایبری را بر عهده دارد. جامعه بین‌الملل در زمینهٔ ایجاد ظرفیت به عنوان یک رویکرد مؤثر برای کمک به جوامع در مواجهه با چالش رو به رشد جرایم سایبری، به توافق گسترده‌ای رسیده است. شورای اروپا از سال ۲۰۰۶ تاکنون در اجرای کنوانسیون بوداپست از طریق طیف وسیعی از پروژه‌ها به جوامع سراسر جهان کمک می‌کند. تأسیس C-PROC زیرساخت‌های شورای اروپا را فراهم می‌کند تا به‌طور مؤثر به تقاضای رو به رشد برای پاسخ‌گویی بپردازند. هم‌اکنون کلیهٔ فعالیت‌های ظرفیت‌سازی در زمینهٔ جرایم سایبری شورای اروپا در سراسر جهان از این اداره، مدیریت می‌شود.

---

4. Council of Europe. 2020. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. Available from: https://www.coe.int/en/web/moneyval
1. Council of Europe. 2020. Octopus Conferences. Available from: https://www.coe.int/en/web/cybercrime/octopus-conference
2. The Cybercrime Programme Office of the Council of Europe

۲-۱-۲-۳-۲. اساس قانونی

علاوه بر پیشنهاد دولت رومانی، در اکتبر ۲۰۱۳، کمیتهٔ وزیران شورای اروپا تصمیم به ایجاد دفتر برنامه‌ریزی گرفت. در ۱۵ اکتبر ۲۰۱۳، دولت رومانی و شورای اروپا تفاهم‌نامه‌ای را برای این منظور امضا کردند. قانون تصویب این تفاهم‌نامه در پارلمان رومانی در مارس ۲۰۱۴ تصویب و در روزنامهٔ رسمی ۲ آوریل ۲۰۱۴ منتشر شد. تفاهم‌نامه در تاریخ ۷ آوریل ۲۰۱۴ لازم‌الاجرا گردید و بنابراین C-PROC در آن روز عملیاتی شد. C-PROC بخش مهمی از واکنش بین‌المللی به جرایم سایبری است و بخشی از کمک‌ها شامل موارد ذیل می‌شود[1]:

۱) تقویت قانون در مورد جرایم سایبری و شواهد الکترونیکی در راستای استانداردهای قوانین حقوقی و حقوق بشر (از جمله حفاظت از داده‌ها)؛

۲) آموزش قضات، دادستان‌ها و مأموران انتظامی؛

۳) ایجاد واحدهای تخصصی جرایم سایبری و پزشکی قانونی و بهبود همکاری‌های بین سازمانی؛

۴) ارتقاء همکاری‌های عمومی/ خصوصی؛

۵) محافظت از کودکان در برابر خشونت جنسی به صورت آنلاین؛

۶) تقویت اثربخشی همکاری‌های بین‌المللی.

C-PROC با کارکرد ظرفیت‌سازی خود، کار کمیتهٔ کنوانسیون سایبری جرم (T-CY)[2] را تکمیل می‌کند که از طریق آن دولت‌های عضو از اجرای کنوانسیون بوداپست پیروی می‌کنند.

دفتر برنامه‌های جرایم سایبری شورای اروپا (C-PROC) در آوریل ۲۰۱۴ عملیاتی شد. فضای اداری توسط دولت رومانی تحت تفاهم‌نامه امضا شده در اکتبر ۲۰۱۳ به شورای اروپا اجاره داده می‌شود. دبیرخانه کمیتهٔ کنوانسیون جرایم سایبری (T-CY) در استراسبورگ دایر است و هدف این دفتر اطمینان از اجرای پروژه‌های ظرفیت‌ساز در زمینهٔ جرایم سایبری شورای اروپا در کلیه مناطق جهان می‌باشد که شامل موارد زیر است:

– تشخیص هویت نیاز به ظرفیت‌سازی در زمینهٔ جرایم سایبری، مشاوره، پشتیبانی و هماهنگی در برنامه‌ریزی، مذاکره و اجرای به موقع فعالیت‌های هدفمند شورای اروپا در زمینهٔ جرایم سایبری از جمله برنامه‌های مشترک با اتحادیهٔ اروپا و سایر اهداکنندگان دارد؛

– ایجاد مشارکت در برابر جرایم سایبری با سازمان‌های بخش دولتی و خصوصی؛

– همکاری با مقامات رومانی در زمینه‌های مربوط به جرایم سایبری؛

– فعالیت‌های تأمین مالی برای پروژه‌ها و برنامه‌های خاص C-PROC.

---

1. Council of Europe. 2020. Cybercrime Programme Office. Available from: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc
2. Cybercrime Convention Committee

۲-۲. نقاط ضعف

در سیاست‌های جنایی تقنینی کنشی ایران، نهادهای مستقلی برای نظارت بر اجرای قوانین مربوط به جرایم رایانه‌ای دیده نمی‌شود و به نظر می‌رسد این امر از نقاط ضعف سیاست جنایی ایران باشد. در خصوص اتحادیهٔ اروپا و با توجه به آمارهای ارائه شده، به نظر می‌رسد هنوز هم جرایم سایبری، هزینه‌های قابل توجهی برای اقتصاد اتحادیهٔ اروپا ایجاد می‌کند که با رشد اعتماد به خدمات اینترنتی افزایش می‌یابد. نگرانی کاربران در مورد امنیت اینترنت در سال‌های گذشته افزایش یافته است و به عنوان جدیدترین گزارش، اکثریت قریب به اتفاق کاربران اینترنت (۸۵ درصد) احساس می‌کنند خطر قربانی شدن جرایم سایبری در حال افزایش است. اکثریت نیز اظهار داشتند که آنها نگران هستند که اطلاعات شخصی آنلاین آنها توسط وب سایت‌ها امن نباشد (۷۳ درصد). هنگام استفاده از اینترنت برای بانکداری آنلاین یا خرید، ۴۲ درصد از کاربران نگران امنیت پرداخت‌های آنلاین هستند. به دلیل نگرانی‌های امنیتی، ۱۳ درصد از کاربران، تمایل کمتری به خرید کالا به‌صورت آنلاین و ۱۲ درصد تمایل کمتری نسبت به «آنلاین- بانک» دارند. متأسفانه نرخ قربانی شدن نیز افزایش یافته است. ۱۴ درصد از کاربران اینترنت به دلیل حملات سایبری نتوانسته‌اند به خدمات آنلاین دسترسی پیدا کنند، ۱۲ درصد آنها رسانه‌های اجتماعی یا ایمیلشان هک شده است و ۱۶ درصد از کاربران اینترنت که می‌گویند کالاهای آنلاین یا خدمات آنلاین می‌خرند، کلاهبرداری آنلاین را تجربه کرده‌اند. در سراسر اتحادیهٔ اروپا، ۸ درصد از کاربران اینترنت قربانی بدافزار شده‌اند، بدافزارهایی که یک دستگاه را ربوده و فقط در مقابل پرداخت «هزینه» حذف می‌شوند. ۸ درصد می‌گویند که قربانی کارت اعتباری یا کلاهبرداری بانکی به صورت آنلاین شده‌اند، ۷ درصد می‌گویند سرقت هویت را تجربه کرده‌اند و ۷ درصد نیز گفتند که به طور اتفاقی با پورنوگرافی کودکان به صورت آنلاین مواجه شده‌اند[1].

بحث و نتیجه‌گیری

رعایت چهارچوب و ابعاد سیاست جنایی اتحادیهٔ اروپا می‌تواند در رفع چالش‌های مربوط به سیاست جنایی ایران در مبارزه با جرایم رایانه‌ای نقش اثرگذاری داشته باشد. نخست آنکه یکی از رویکردهای مهم در سیاست جنایی در نظام کیفری اتحادیهٔ اروپا کاهش اختلاف در قوانین مربوط به جرایم سایبری در میان کشورها و به عبارت دیگر همانندسازی قوانین است. این عامل با حذف ناسازگاری بین سیستم‌های دادرسی کیفری با موانع سرکوب این پدیده مبارزه می‌نمایند. در همین راستا اتحادیهٔ اروپا همواره بر لزوم گسترش تحقیقات و همکاری‌های بین‌المللی در مقابله با جرائم فضای سایبر تأکید می‌نماید. از دیگر سو اتحادیهٔ اروپا با اتخاذ استراتژی انعطاف‌پذیر و نوآورانه و

1. European Commission. 2015. Combating Cybercrime: EU-wide rules against cyber attacks come into force. Available from:
https://ec.europa.eu/home-affairs/what-is-new/news/news/2015/201509041

تأکید بر لزوم انطباق با نیازهای روز خلأ موجود مابین رشد فناوری و اقدامات کیفری را کمتر نموده است. همچنین از جمله تدابیر بسیار موثّر در تدوین سیاست‌های جنایی در حیطه جرایم رایانه‌ای در بستر اتحادیهٔ اروپا توجه خاص به اقشار آسیب‌پذیر و نیازمند حمایت‌های خاص مانند زنان و کودکان در فرآیندهای سیاست جنایی پیشگیرانه، تقنینی و قضایی است. نظارت بر اجرای قوانین مربوط به جرایم رایانه‌ای در اتحادیهٔ اروپا بر عهده نهادهای خاص و مستقلی است که حسن اجرای قوانین را تضمین می‌نمایند.

علت اصلی ناکارآمدی سیاست جنایی ایران در قبال جرایم رایانه‌ای را می‌توان به این نکته کلیدی مرتبط دانست که اگر قرار است سیستم‌های عدالت کیفری به‌طور مؤثر با مشکلات مربوط به جرایم سایبری برخورد کنند، باید قوانین و سیستم‌های اجرای قانون خود را در جایی که این افراد قادر به مقابله با تحقیقات و پیگرد قانونی پدیده نیستند، به‌روز کنند. در اتحادیهٔ اروپا، توافق‌نامه‌های بین‌المللی در صدد حل این مسائل هستند؛ زیرا هماهنگ‌سازی قوانین میان کشورها، باعث به‌روز شدن قوانین گردیده و از برخوردهای متفاوت نیز جلوگیری می‌نماید.

مهم‌ترین چالش فراروی سیاست جنایی ایران در مبارزه با جرایم رایانه‌ای، بدین شرح است. در حیطه سیاست جنایی تقنینی، انجام تحقیقات جدید و شناخت و آشنایی بیشتر با جنبه‌های فنی می‌تواند به تدوین سیاست جنایی متناسب حاکم بر جرایم رایانه‌ای به ویژه سیاست جنایی تقنینی کمک شایانی نماید. حملات سایبری، به معضل بزرگی برای کشورهای اروپایی تبدیل شده است و به همین لحاظ این کشورها تلاش می‌کنند تا اقدامات جدیدی را برای افزایش آمادگی برای مقابله با این‌گونه حملات صورت دهند. به عنوان نمونه طرح «رمز دوم پویا» برای انتقال وجه در زمینهٔ کاهش کلاهبرداری و سرقت اینترنتی بسیار مؤثر بوده است. همچنین در چهارچوب ماهیت پیشگیرانه سیاست جنایی، ناکافی بودن میزان آگاهی مردم و مدیران ارگان‌های مختلف هنگام مواجهه با جرایم رایانه‌ای و موارد مشکوک یا نحوهٔ وقوع آنها، ناشی از کم‌توجهی نهادهای مسئول در فضای سیاست جنایی ایران ملموس می‌باشد.

پیشنهادها

– در بستر سیاست تقنینی جمهوری اسلامی ایران نیز رشد همانندسازی قوانین در داخل کشور و پرهیز از تشتت در قانون‌نگاری به‌همراه یکسان‌سازی قوانین با الگوهای جهانی موجود و استفاده از تجارب بین‌المللی با بهره‌گیری از تحقیقات و ظرفیت همکاری‌های بین‌المللی مورد پیشنهاد است. قانون‌گذاران باید همکاری متقابل منطقه‌ای و تقویت همکاری‌های بین‌المللی در زمینهٔ تدوین تا اجرای قوانین، کشف، جمع‌آوری دلایل الکترونیکی، تعقیب، استرداد مجرمین و رسیدگی قضایی را مورد توجه قرار دهند تا علاوه بر تسهیل و تسریع در روند رسیدگی به جرایم سایبر، امکان رسیدگی هرچه بهتر دیگر جرایمی که ادلهٔ الکترونیک در آنها نقش دارند نیز فراهم گردد و این امر را به‌طور جدی و فوری در دستور کار خود قرار دهند. با توجه به ماهیت و ویژگی‌های جرایم رایانه‌ای که آیین‌نامه و تشریفات خاصی را می‌طلبد، ارجاع قانون‌گذار به مواد قانون آیین دادرسی کیفری در راستای پر کردن خلأ ناشی از مواد شکلی قانون جرایم رایانه‌ای نیز به‌تنهایی نمی‌تواند راهگشای تمامی مسایل مربوط باشد.

– یکی از نقاط مبهم در قانون جرایم رایانه‌ای مصوب ۱۳۸۸، مشخص نبودن ارتباط این قانون با قوانین پیشین است. در مادهٔ ۵۶ آمده است: «قوانین و مقررات مغایر با این قانون ملغی است». در اینجا لازم بود مقنن به صراحت منظور خود را در رابطه با نسخ یا عدم نسخ مواد قانونی مرتبط با قانون جرایم رایانه‌ای بیان نماید تا از تشتت آرای حقوق‌دانان و محاکم دادگستری جلوگیری شود. پیشنهاد می‌گردد در این خصوص تدبیری اندیشیده شود.

– پیشنهاد می‌گردد در خصوص تناسب میان جرایم و مجازات‌ها برای مثال مجازات حبس در جرایم «جعل رایانه‌ای» و «کلاهبرداری رایانه‌ای»، ۱ تا ۵ سال و در «جاسوسی رایانه‌ای» که جرمی مهم‌تر به‌شمار می‌رود، ۱ تا ۳ سال است! (میزان جزای نقدی نیز به همین صورت است). با توجه به ویژگی‌های خاص این جرایم انتظار می‌رود، قانون‌گذار محترم جهت تعیین ضمانت‌های اجرایی متناسب با آن محیط در راستای حمایت از بزه‌دیدگان جرایم رایانه‌ای دقت نظر خاصی داشته باشد.

– الحاق قانون خاص (حاوی جنبه‌های ماهوی و شکلی) به قانون مجازات اسلامی (عام و ماهوی) که امری نامتعارف است و حتی استقلال شمارهٔ مواد این قانون، از جمله مباحثی است که پیشنهاد می‌گردد قانون‌گذار ایران در آینده در صدد اصلاح و بازنگری آن برآید.

– در کشور ایران در خصوص تعارض صلاحیت‌ها راجع به جرایم سایبری، قانون جرایم رایانه‌ای و دیگر مقررات جاری ایران در مورد حالتی که چند کشور به دنبال اعمال صلاحیت نسبت به یک جرم سایبری باشند، راه حلی ارائه نداده‌اند. لذا پیشنهاد می‌گردد با پیش‌بینی اصولی قابل قبول و مطلوب در ایجاد ارتباط میان جرم، مجرم، بزه‌دیده و ابزار جرم با کشور مدعی اعمال

صلاحیت مشکل حل شود و یا با فراهم شدن الحاق کشورها به کنوانسیون جرایم سایبری به رفع تعارض‌ها در زمینهٔ صلاحیت اقدام گردد.

– مادهٔ ۷۴۱ قانون تعزیرات (مادهٔ ۱۳ قانون جرایم رایانه‌ای ایران)، مادهٔ کاملی برای مبارزه با کلاهبرداری اینترنتی نیست و نیاز است قانون‌گذار محترم نسبت به رفع این مشکل اقدام نماید و این اقدام می‌تواند با بهره‌گیری از سوابق دیگر کشورها در قانون‌گذاری باشد تا بتوانیم قانونی کامل و متناسب با کشور خودمان داشته باشیم. دربارهٔ پیشگیری از کلاهبرداری اینترنتی نیز ایرادهایی مانند نبود برنامه‌های مشخص و منسجم، وارد است که رفع این ایرادها نیز نیازمند برنامه‌ای جامع، مشخص و اجراشدنی است.

– از خلأهای موجود در فصل جرایم رایانه‌ای مصوب خرداد ۱۳۸۸ الحاقی به قانون مجازات اسلامی بر خلاف قوانین سایر کشورها و کنوانسیون ۲۰۰۱ بوداپست می‌توان به عدم طبقه‌بندی داده‌های محرمانه از جمله به‌کلی محرمانه، محرمانه، غیر محرمانه و عدم تأثیر میزان حساسیت و اهمیت‌های خاص هر طبقه از داده‌ها در میزان مسئولیت متهم اشاره کرد که باید این نقیصه‌ها برطرف شود و در نتیجه میزان مجازات کسی که به عنوان مثال با استفاده از ویروس «استاکس نت» داده‌های محرمانه با اهمیت نه چندان زیاد را فاش می‌کند تفاوت وجود داشته باشد.

– ایراد دیگر که فصل جرایم رایانه‌ای به نظر می‌رسد دارد، عدم حمایت این قانون از اطلاعات و حریم شخصی افراد جامعه است. با توجه به وظیفه‌ای که حقوق جزا در قبال صیانت از حریم اشخاص دارد باید در این مورد نیز اصلاحاتی جهت حمایت از اطلاعات شخصی و سایت افراد صورت بگیرد. همان‌طور که در سایر کشورها از جمله انگلیس، استرالیا و آمریکا قوانین خاص علیه تجاوزات به حقوق فردی به تصویب رسیده است.

منابع

- پاک‌نهاد، امیر؛ سدره‌نشین، ابوالفضل. (۱۳۹۰). بررسی قانون جرایم رایانه‌ای از دیدگاه موازین حقوق کیفری فناوری اطلاعات. *کاراگاه*، ۵(۱۷)، ۴۳-۲۴.
http://det.jrl.police.ir/article_10497.html
- پورقهرمانی، بابک. (۱۳۹۶). مطالعه تطبیقی سازکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست. *حقوق کیفری*، ۸(۱۵)، ۳۶-۷.
https://jol.guilan.ac.ir/article_2286.html
- پورقهرمانی، بابک. (۱۳۹۵). *سیاست جنایی ایران در قبال جرایم رایانه‌ای (مطالعه تطبیقی با اسناد بین‌المللی)*. چاپ اول. موسسه مطالعات و پژوهش‌های حقوقی شهر دانش.
- جاویدنیا، جواد. (۱۳۹۱). *جرائم تجارت الکترونیکی*. چاپ سوم. خرسندی.
- جوان جعفری، عبدالرضا. (۱۳۸۹). جرائم سایبر و رویکرد افتراقی حقوق کیفری. *دانش و توسعه*، ۱۷(۳۴)، ۱۹۳-۱۶۹.
https://danesh24.um.ac.ir/article_27350.html
- عبدی‌پور کشاورز، مهدی؛ انصاری، عباسقلی؛ ششگل، حمید. (۱۳۹۹). هستی‌شناسی جرائم رایانه‌ای با توجه به قانون جرائم رایانه‌ای. *تحقیقات حقوقی بین‌المللی*، ۱۳(۴۷)، ۱۶۸-۱۴۹.
http://alr.iauctb.ac.ir/article_671461.html
- فضلی مهدی. (۱۳۹۶). *مسئولیت کیفری در فضای سایبر*. چاپ سوم. خرسندی.
- کرامتی معز، هادی. (۱۳۹۹). *بزه دیده‌شناسی کودکان در شبکه‌های مجازی*.چاپ اول. دادگستر.
- کرامتی معز، هادی؛ میرخلیلی، سید محمود. (۱۳۹۹). پیشگیری رشدمدار از بزه‌دیدگی کودکان در شبکه‌های اجتماعی مجازی (مطالعه موردی معلمان منطقه پنج شهر تهران. *مطالعات پیشگیری از جرم*، ۱۵(۵۶)، ۲۲-۱.
http://cps.jrl.police.ir/article_95006.html
- منصورآبادی، عباس؛ میرخلیلی، سید محمود. (۱۴۰۰). پیشگیری از بزه‌دیدگی کودکان در شبکه‌های اجتماعی مجازی با تأکید بر نقش شورای عالی فضای مجازی و پلیس فتا. *مطالعات بین المللی پلیس*، ۱۲(۴۶)، ۵۲-۳۰.
http://interpol.jrl.police.ir/article_95912.html
- مهدوی ثابت، محمدعلی؛ عبدالهی، سامان. (۱۳۹۹). ایمن‌سازی کودکان از آسیب‌ها و تهدیدات فضای سایبر (با تأکید بر اقدامات پلیس بین الملل). *مطالعات پلیس بین‌الملل*، ۱۱(۴۳)، ۳۷-۹.
http://interpol.jrl.police.ir/article_94520.html
- وطنی، امیر؛ اسدی، حمید. (۱۳۹۵). سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم. *حقوق اسلامی*، ۱۷(۴۴)، ۱۲۶-۹۹.
https://ilr.journals.isu.ac.ir/article_1959.html
-Thomas, J. H. (2018). Regulating Cybercrime through Law Enforcement and Industry Mechanisms. *ANNALS, AAPSS*, 679: 140-157.
https://journals.sagepub.com/doi/abs/10.1177/0002716218783679