شناسه دیجیتال (DOI): 10.22106/JLJ.2018.32738

# گونه‌شناسی جرایم سایبری با نگاهی به قانون جرایم رایانه‌ای و آمار پلیس فتا

**روح‌الدین کردعلیوند***
**محمد میرزایی****

## چکیده

بزهکاری سایبری از پویایی خیره‌کننده‌ای برخوردار است. رفتارهای مجرمانه در این نوع بزهکاری متنوع و پویا هستند؛ برخی ازآنها کاملاً نو و برخی دیگر همان جرایم متداولی هستند که در بستر سامانه و شبکه‌های اطلاعاتی به شکلی دیگر ارتکاب پیدا می‌کنند. در گونه‌شناسی جرایم سایبری از معیارهای مختلفی چون نقش سامانه و شبکه‌های اطلاعاتی در پیدایش و گسترش جرایم (به عنوان پشتوانه و یا وسیله ارتکاب جرم)، موضوع و محتوای جرایم سایبری و یا تلفیقی از این معیارها استفاده می‌شود. با توجه به این معیارها و نیز با تکیه بر قانون جرایم رایانه‌ای مصوب ۱۳۸۸، نویسندگان این مقاله نخست به تبیین دو گونه‌شناسی از جرایم سایبری می‌پردازند و سپس وضعیت بزهکاری سایبری در کشور ایران، بر اساس آمار ارائه شده توسط پلیس فضای تولید و تبادل اطلاعات (فتا) برای سال‌های ۱۳۹۱ تا ۱۳۹۵ را بررسی می‌کنند.

**کلیدواژه‌ها**: گونه‌شناسی، دسترسی غیرمجاز، هرزه‌نگاری کودکان، باج‌افزار، تخریب داده‌ها.

* عضو هیأت علمی گروه حقوق دانشگاه دامغان (نویسنده مسئول) R.kordalivand@du.ac.ir
** کارشناس ارشد مبارزه با جرایم سایبری پلیس فتا Mirzaei_mail@yahoo.com
تاریخ دریافت: ۹۵/۰۳/۲۳ تاریخ پذیرش: ۹۵/۰۷/۰۳

## مقدمه

هر گونه پیشرفت در فناوری تحول حقوق را بـه دنبـال دارد.[۱] بـی‌تردیـد فنـاوری اطلاعات و پیدایش شبکه‌ها فضایی جدید از آزادی را در برابر انسان گشوده اسـت ولـی این آزادی مطلق نیست. رفتارهای ارتکـاب‌یافتـه در بسـتر ایـن فنـاوری، آنگـاه کـه بـه ارزش‌های بنیادین جوامع بشری، به‌ویژه به کرامت انسـانی، آسـیب برسـانند، از طریـق جرم‌انگاری‌های مناسب سرکوب می‌شوند. این همان چیزی اسـت کـه مبنـای سیاسـت جنایی مبارزه با بزهکاری سایبری[۲] را تشکیل می‌دهد.

اصطلاح بزهکاری سایبری هنوز موضوع تعریفی رسمی، چه در اسناد بین‌المللی و چه در قوانین بسیاری از کشورها، قرار نگرفته است. این متـون بـا تکیـه بـر رویکـردی کاربردی ترجیح می‌دهند به جای ارائه تعریفی قانونی محتوای ایـن بزهکـاری را تبیـین کرده، جرایم تشکیل‌دهنده آن را دسته‌بندی کننـد. البتـه از سـال۱۹۸۳ کـه نخسـتین تعریف از جرم سایبری از سوی سازمان همکاری و توسعه اقتصادی اروپـا منتشـر شـد[۳] تاکنون تعریف‌های زیادی از جرم سایبری ارائه شده است.[۴] رهیافت‌های اتخـاذ شـده در این تعریف‌ها یا گسترده و یا محدود بوده، ممکن است همه مصادیق پیش‌بینی شـده در قوانین کیفری را شامل نشود و یا با توصیف‌های مضیق حقوقی تطابق نداشته باشد.[۵]

وجه مشترک تعریف‌های مختلف از بزهکاری سایبری مربوط به ارتباط جـرایم آن با سامانه، اینترنت یا شبکه است. شیوه ارتکاب ایـن جـرایم معمـولا بـا فاصـله و بـدون ارتباط جسمی مستقیم با بزه‌دیده است. به طور کلی می‌توان گفت که جـرایم سـایبری شامل تمام جرایمی می‌شود که با کمک سامانه‌ها و شبکه‌های اطلاعاتی و یا علیـه آنهـا ارتکاب به وقوع می‌پیوندند.[۶] فهرست این جرایم به نـوع خاصـی از رفتارهـای مجرمانـه محدود نمی‌شود و همه حوزه‌های جنایی را در بر می‌گیرد.

۱. رنه ساواتیه از جمله نویسندگانی بود که در سال 1959 بـه گونـه‌ای پـیش‌دسـتانه بـه تـأثیر دگرگـونی‌هـای اجتماعی، اقتصادی و فناورانه در تحول حقوق پرداخت:
- Savatier, R., Les métamorphoses économiques et sociales du droit privé d'aujourd'hui, Dalloz, 1959.

2. Cybercrime; Cybercriminalité.

۳. بر اساس این تعریف جرم رایانه‌ای عبارت است از هـر عمـل غیرقـانونی، غیراخلاقـی یـا غیرمجـاز نسـبت بـه پردازش خودکار و یا انتقال داده‌ها. در این زمینه، ر.ک: زیبر، اولـریش، جـرایم رایانـه‌ای، چـاپ دوم، ترجمـه محمدعلی نوری و دیگران، تهران، گنج دانش، ۱۳۹۰، ص. ۱۸.

۴. در زمینه تعریف‌های مختلف از جرم رایانه‌ای، ر.ک: عالی‌پور، حسن، حقوق کیفـری فنـاوری اطلاعـات، چـاپ چهارم، معاونت حقوقی و توسعه قضایی قوه قضاییه، مرکز مطالعات توسعه قضایی، ۱۳۹۵، صص. ۱۲۵-۱۲۰.

۵. در این زمینه، ر.ک: خرم‌آبادی، عبدالصمد، «تاریخچه، تعریـف و طبقـه‌بنـدی جـرم‌هـای رایانـه‌ای»، در: مجموعـه مقـالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی، انتشارات سلسبیل، ۱۳۸۴، ص. ۲۹.

6. Chopin, F., «Cybercriminalité», Répertoire de droit pénal et de procédure pénale, Dalloz, 2017, p. 2.

بزهکاری سایبری افزون بر نو بودن از قابلیت بالای تحول‌پذیری و تحول‌بخشی در برخوردار است. این تحول تنها مربوط به جرایمی که با پیدایش شبکه پا به عرصه وجود گذاشته‌اند نیست؛ پیشرفت فناوری اطلاعات شیوه ارتکاب بسیاری از جرایم سنتی نیز متحول ساخته است.[1] به عنوان مثال می‌توان به تحول جرم راهزنی دریایی، به عنوان یکی از قدیمی‌ترین جرایم بین‌المللی، از راهزنی سنتی به راهزنی سایبری اشاره کرده که امروزه یکی از چالش‌های امنیتی برای دولت‌هاست.[2] جلوه‌ای دیگر از این تحول را می‌توان در تجاری‌سازی فعالیت‌های مجرمانه سایبری[3] و ایجاد ارتباط شبکه‌ای میان بزهکاران مشاهده کرد. بزهکاران سایبری فعالیت‌های خود را به خدماتی حرفه‌ای تبدیل کرده و با استفاده از ابزارهای ارتباطی آنها را در معرض فروش قرار می‌دهند. این ویژگی‌ها تنوع و پویایی رفتارهای مجرمانه را همواره بیشتر می‌کند.

پاسخ‌دهی کیفری به بزهکاری سایبری باعث ایجاد جرم‌انگاری‌های متعددی شده است که شمار آنها همواره در حال افزایش است. برخی از این جرم‌انگاری‌های کاملاً نوین بوده و واژگان خاصی را وارد ادبیات حقوق کیفری کرده است (جرایم علیه محرمانگی داده‌ها). برخی دیگر ساختاری تلفیقی دارند؛ تلفیقی از ساختار جرایم سنتی و عناصر مربوط به ارتکاب آن در فضای سایبری (کلاهبرداری رایانه‌ای به عنوان مثال). در بیشتر موارد نیز قانون‌گذار با افزودن عنصر «استفاده از سامانه و شبکه‌های اطلاعاتی»، به عنوان کیفیت مشدده در جرم انگاری‌های رایج آنها را در شمار جرایم رایانه‌ای قرار می‌دهد. گاهی نیز هیچ‌گونه اشاره‌ای در ساختار جرم‌انگاری به شیوه ارتکاب سایبری رفتارها نشده است اما با توجه به قابلیت ارتکاب آنها در فضای سایبر ممکن است به عنوان مصداق جرم رایانه‌ای در نظر گرفته شوند. از نظر بستر قانونی جرم‌انگاری، افزون بر قوانین خاص ناظر بر جرایم رایانه‌ای (همانند قانون جرایم رایانه‌ای ایران مصوب ۱۳۸۸) جرایم سایبری در قوانین متعددی دیگری نیز پیش‌بینی شده‌اند. با توجه به این پیچیدگی و نیز در نظر گرفتن فقدان تعریف قانونی از بزهکاری سایبری چگونه می‌توان جرایم سایبری را دسته‌بندی کرد؟ بر اساس چه

۱. حقوق کیفری نیز به دنبال این تحولات دستخوش تغییر اساسی شده است. در این زمینه ر.ک: حاجی ده آبادی، احمد؛ سلیمی، احسان، «اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرائم رایانه‌ای)»، فصلنامه مجلس و راهبرد، شماره ۸۰، ۱۳۹۳، ص. ۶۲.

۲. برای نشان دادن ضعف‌های امنیتی سامانه دریانوردی، یک گروه تحقیقاتی در دانشگاه تگزاس آمریکا در سال ۲۰۱۳ در جریان یک تجربه آزمایشی، کنترل یک کشتی مسافرتی را، با منحرف کردن سامانه دریانوردی GPS آن، در دست گرفتند بی آنکه سکان‌دارن این کشتی متوجه شوند یا اینکه زنگ‌های هشدار کشتی به صدا درآیند. به نقل از:
Rouiai, A. «La piraterie moderne, d'une mer à l'autre», Carto, n°41, 2017, p.44.

3. Manky, D., «Cybercrime As A Service: A very Modern Business.», Computer Fraud & Security, n°6, 2008, p. 9.

معیارهایی می‌توان یک گونه‌شناسی از جرایم سایبری ارائه کرد؟ چه فایده‌ای بر این گونه‌شناسی مترتب است؟

گونه‌شناسی عبارت است از مطالعه و تحلیل ویژگی‌های مشخص‌کننده اشکال متعدد یک واقعیت پیچیده جهت درک بهتر و دسته‌بندی افراد تشکیل‌دهنده این واقعیت. در زمینه بزهکاری سایبری، گونه‌شناسی‌های متعددی را می‌توان در نوشته‌های نویسندگان این حوزه جستجو کرد. این دسته‌بندی‌ها یا بر اساس متعددی چون زمینه و فرصتی که فضای سایبری برای ارتکاب جرایم فراهم آورده است؛[1] نقشی که سامانه‌ها در ارتکاب جرم ایفا می‌کنند؛[2] محتوای این جرایم (فریبکاری، سرقت، هرزه‌نگاری، خشونت، جرایم علیه دولت و...)، ارزش‌های مورد حمایت و یا تلفیقی از آنها صورت گرفته است. از لحاظ قانون‌گذاری، گونه‌شناسی و دسته‌بندی جرایم افزون بر کارکرد اعلامی (اعلام ارزش‌های مورد حمایت قانون‌گذار) می‌تواند به ایجاد یک سیاست جنایی منسجم کمک کند. گونه‌شناسی جرایم امکان شناسایی ماهیت جرایم، نوع و شدت رفتارهای تشکیل‌دهنده و نیز ویژگی‌های مشترک آنها را فراهم می‌آورد. گونه‌شناسی همچنین کمک می‌کند تا آمار و اطلاعات مربوط به جرایم سایبری از شفافیت بیشتری برخوردار شود و بدین‌تربیت امکان بهتری برای تجزیه و تحلیل آنها فراهم شود. البته هیچ دسته‌بندی عاری از نقص نیست و حقوق‌های کیفری همیشه در دسته‌بندی‌های خود از جرایم موفق نبوده‌اند و در مواردی عدم استحکام معیارهای دسته‌بندی زمینه آشفتگی و سردرگمی در حقوق کیفری را به وجود آورده است.[3] در مقررات قانون جرایم رایانه‌ای[4] مصوب ۱۳۸۸/۳/۵، با الهام از کنوانسیون جرایم سایبری (بوداپست ۲۳ نوامبر ۲۰۰۱،[5] تلاشی برای ارائه یک گونه‌شناسی از جرایم صورت گرفته است. کارگروه تعیین مصادیق مجرمانه می‌تواند به ارائه فهرستی از جرایمی که می‌تواند مصداق جرم رایانه‌ای باشد.

هدف نخست که در این مقاله دنبال می‌شود ارائه نوعی گونه‌شناسی از جرایم سایبری بر اساس دو معیار زیر است: تأثیر فضای سایبری در پیدایش و یا گسترش جرایم؛ نقش سامانه‌ها و شبکه‌های اطلاعاتی در ارتکاب جرم. هدف دوم این مقاله

1. Wall, D.S. «The internet as a conduit for criminal activity», in: Pattavina, A. (Ed.), Information technologie and Criminal Justice System, Thousand Oaks, CA: Sage publication, 2005/2015, p. 80.
2. Leman-Langlois, S., «Le crime comme moyen de contrôle du cyberspace commercial», Criminologie, 39,9 (1), 2006, pp. 66-67.

۳. عالی‌پور، حسن، منبع پیشین، صص. ۱۴۴-۱۴۲.

۴. از این پس، این گونه به این قانون اشاره می‌شود: ق.ج.ر.

۵. در زمینه این کنوانسیون، ر.ک: فراهانی، امیرحسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، انتشارات خرسندی، ۱۳۹۵.

گزارشی مختصر از سیمای بزهکاری سایبری در ایران بر اساس آمار پلیس فتا در سال‌های بین ۱۳۹۱تا ۱۳۹۵ است.

## ۱. گونه‌شناسی مبتنی بر تأثیر فضای سایبری در پیدایش یا گسترش جرایم

پیدایش اینترنت و شبکه طلاعات، بی‌تردید، زمینه ارتکاب فعالیت‌های مجرمانه نوینی که تحقق آنها پیش از ایجاد شبکه ممکن نبوده را به وجود آورده است؛ جرایمی همانند دسترسی غیرمجاز به داده‌ها، جاسوسی رایانه‌ای. همه جرایم سایبری از این دست نیستند؛ بسیاری از رفتارهایی که تحت عنوان جرایم سایبری دسته‌بندی شده‌اند، پیش از آغاز عصر اینترنت جرم‌انگاری شده‌اند و پیدایش شبکه تنها بستر ارتکاب آنها را متفاوت ساخته است. گاهی از این جرایم با عنوان جرایم کلاسیک با توصیف رایانه‌ای نامبرده می‌شود.[1] جرایمی همانند کلاهبرداری رایانه‌ای یا نشر اکاذیب ازین دسته هستند. فضای سایبری نسبت به پیدایش و یا گسترش برخی دیگر از جرایم (جدید یا سنتی) نقش جانبی دارد (جرایم انتخاباتی). جدول زیر بر اساس رابطه بین پیدایش سامانه‌ها و شبکه‌ها اطلاعاتی، پیدایش جرایم جدید و یا گسترش جرایم سنتی را نشان می‌دهد.

| نقش سامانه‌ها و شبکه‌ها | زمان جرم‌انگاری رفتارها | |
|---|---|---|
| | جرایم سنتی | جرایم جدید |
| آغازگر | - | حملات سایبری، تولید یا توزیع یا در دسترس‌گذاری یا معامله نرم افزارهای مجرمانه، جرایم علیه محرمانگی داده‌ها، دسترسی غیرمجاز |
| گسترش‌دهنده | هرزه‌نگاری کودکان، تقلب‌ها؛ کلاهبرداری، سرقت، نشر اکاذیب | ایمیل‌های تقلبی، باج‌گیری اینترنتی از طریق باج افزار، جرایم علیه مالکیت معنوی |
| جانبی | جرایم انتخاباتی | حمایت از تروریسم |

**جدول شماره ۱ [2]ـ نقش سامانه‌ها و شبکه‌های اطلاعاتی در پیدایش یا گسترش جرم‌انگاری**

## ۲. گونه‌شناسی مبتنی بر نقش سامانه و شبکه‌ها و محتوای جرایم سایبری

جرم‌انگاری رفتارهای زیان‌بار در فضای سایبری، همانند جرم‌انگاری جرایم سنتی، بر این مبنا صورت گرفته است که همگی به ارزش‌های مورد حمایت قانون‌گذار آسیب وارد می‌کنند. بزهکاران جرایم سایبری نه تنها تمامیت و امنیت خود سیستم‌ها و

۱. عباسی کلیمانی، عاطفه؛ اکبری، عاطفه، جرایم سایبری، تهران انتشارات مجد، ۱۳۹۴، ص. ۳۷.
۲. منبع:.Leman-Langlois, S., op.cit., p. 63.

شبکه‌های اطلاعاتی و مخابراتی را در معرض خطر قرار می‌دهند بلکه با استفاده از سیستم‌ها و شبکه‌های اطلاعاتی، چه به عنوان پشتوانه و چه به عنوان وسیله ارتکاب، ارزش‌های بنیادین جوامع انسانی را نیز مورد حمله و آسیب قرار می‌دهند. جدول زیر گونه‌شناسی دیگری از جرایم سایبری را نشان می‌هد که بر اساس رابطه بین استفاده از شبکه‌ها و نقش آنها در آسیب به ارزش‌های مورد حمایت قانون‌گذار تهیه شده است. رفتارهای زیان‌باری که جرایم سایبری را تشکیل می‌دهند، صرف‌نظر از تفاوت آنها، همه دارای این ویژگی مشترک هستند که سیستم‌ها و شبکه‌های اطلاعاتی را چه به عنوان موضوع جرم، چه به عنوان پشتوانه جرم و چه به عنوان وسیله ارتکاب جرم مورد استفاده قرار می‌دهند.

| سامانه و شبکه‌های اطلاعاتی | جرایم |
|---|---|
| موضوع جرم | جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی: تخریب و اخلال در داده‌ها |
| پشتوانه جرم | جرایم علیه اشخاص و شخصیت معنوی افراد همانند هرزه‌نگاری، هتک حیثیت، انتشار تصاویر خشونت‌آمیز، جرایم مطبوعاتی، قاچاق انسان، ترغیب به روسپیگری |
| وسیله ارتکاب جرم | جرایم علیه اموال همانند سرقت و کلاهبرداری، اخاذی از طریق باج‌افزارها، جرایم علیه مالکیت معنوی، جرایم علیه امنیت همانند تروریسم |

**جدول شماره ۲ ـ گونه‌شناسی جرایم بر اساس رابطه بین سامانه‌ها و شبکه‌های اطلاعاتی و محتوای جرایم سایبری**

### ۲ـ۱. سامانه و شبکه‌های اطلاعات: موضوع جرم

حفظ تمامیت و صحت سامانه و شبکه خود ارزش و منفعتی مستقل است که قانون‌گذار به دنبال پشتیبانی از آن در برابر خطرات ناشی از فضای سایبری است. به پیروی از کنوانسیون بوداپست، بسیاری از حقوق‌های کیفری داخلی رفتارهای که خود سامانه و داده‌ها را موضوع جرم واقع قرار می‌دهند را جرم‌انگاری کرده‌اند. دو دسته از جرایم در این زمینه پیش‌بینی شده‌اند: جرایم علیه محرمانگی داده‌ها و سامانه‌ها و جرایم علیه صحت و تمامیت داده‌ها و سامانه‌ها. در حقوق کیفری ایران این جرایم در فصل نخست و دوم ق.ج.ر پیش‌بینی شده‌اند.

زیر عنوان جرایم علیه محرمانگی داده‌ها و سامانه‌ها رفتارهای مختلفی مورد جرم‌انگاری واقع شده‌اند: نخستین رفتار مجرمانه مربوط به دسترسی غیرمجاز به داده‌هاست. دسترسی غیرمجاز به داده‌ها به طور عام در ماده ۱ ق.ج.ر و به طور خاص

در ماده ۴ همین قانون تحت عنوان جاسوسی رایانه‌ای جرم‌انگاری شده است. جاسوسی رایانه‌ای هر چند در مبحث جداگانه‌ای جرم‌انگاری شده است ولی از لحاظ رفتار مادی تفاوت خاصی با آنچه در ماده یک قانون آمده است ندارد. موضوع جرم جاسوسی رایانه‌ای تنها سامانه‌هایی است که داده‌های سری در آن نگهداری می‌شود. مرتکب جرم افزون بر قصد نقض تدابیر امنیتی برای دسترسی به سامانه، باید قصد خاص دسترسی به داده‌های سری را نیز داشته باشد.[۱]

دومین رفتار مجرمانه مربوط به شنود غیرمجاز است که در ماده ۲ ق.ج.ر پیش‌بینی شده است. حفاظت از داده‌های شخصی در مقابل ورود دولت‌ها و مداخله‌گران غیر دولتی در زندگی خصوصی یکی از دغدغه‌های مهم افراد در جوامع امروزی است. به همین خاطر در سطح بین‌المللی یا داخلی مقرراتی[۲] در این زمینه تصویب شده‌است و نهادهایی برای فعالیت در این زمینه برقرار شده اند.[۳] با توجه به آنکه امروزه به بهانه مقابله با تروریسم و دیگر جرایم امنیتی استفاده از شنود تلفنی و رهگیری اطلاعات و داده‌ها یکی از برجسته‌ترین راه‌های کنترل شهروندان تبدیل شده است حمایت شهروندان نسبت به دسترسی غیرمجاز به داده‌های شخصی آنان اهمیتی بیش از پیش پیدا کرده است. شنود رایانه‌ای هم می‌تواند نسبت به ارتباطات تلفنی صورت گیرد و هم نسبت به محتوای دیداری و نوشتاری. آنچه که این جرم را از جرم دسترسی غیرمجاز به داده‌ها متمایز می‌سازد مربوط به موضوع آن، محتوای در حال انتقال، است.[۴]

دسته دیگر از جرایمی که سامانه و شبکه اطلاعات رایانه‌ای را هدف قرار می‌دهد مربوط به جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی است. به منظور حفاظت از صحت و تمامیت داده‌ها قانون‌گذار کشورمان شش رفتار را جرم‌انگاری کرده است: جعل رایانه‌ای[۵] و استفاده از سند مجعول (موضوع مواد ۶ و ۷ ق.ج.ر)، تخریب داده‌ها[۶] و سامانه‌های رایانه‌ای و مخابراتی (موضوع مواد ۸ و ۹ ق.ج.ر)؛

۱. عالی‌پور، حسن، منبع پیشین، ص. ۱۶۲.

۲. به عنوان نمونه می‌توان به کنوانسیون حمایت از حقوق افراد در زمینه پردازش خودکار داده‌های شخصی» مصوب ۱۹۸۱ شورای اروپا اشاره کرد:
Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg, 1981, Avaible from URL: www.conventions.coe.int/treaty/.

۳. کمیسیون اطلاعات و آزادی‌ها (CNIL) در فرانسه از جمله این نهادهاست. این نهاد از اختیار صدور و اعمال ضمانت اجراهایی، به ویژه آنهایی که جنبه مالی دارند، برخوردار می‌باشد.

۴. عالی‌پور، حسن، منبع پیشین، ص. ۱۶۲.

۵. در زمینه جعل رایانه‌ای، ر.ک: قناد، فاطمه، جعل در بستر فناوری‌های اطلاعات و ارتباطات، دوفصلنامه علمی پژوهشی آموزه‌های حقوق کیفری، شماره ۲، ۱۳۹۰، صص. ۸۸-۶۳.

۶. قانون تجارت الکترونیکی مصوب ۱۳۸۲ و قانون جرایم رایانه‌ای مصوب ۱۳۸۸. ماده ۵۸ فصل سوم قانون تجارت الکترونیکی با عنوان حمایت از داده پیام‌های شخصی، شرایط قانونی ذخیره، پردازش و توزیع

ممانعت از دسترسی به داده‌ها (ماده ۱۰ ق.ج.ر) و درنهایت اخلال در سامانه‌های مورد استفاده برای ارائه خدمات ضروری به قصد به خطر انداختن آسایش و امنیت عمومی (ماده ۱۱ق.ج.ر). ماده اخیر اخیر به طور ضمنی یک اقدام تروریستی سایبری را مورد سرکوب قرار می‌دهد.

### ۲ـ۲. سامانه و شبکه‌های اطلاعات: پشتوانه ارتکاب جرم

بر کسی پوشیده نیست که امروزه فناوری اطلاعات و مخابرات بیش از پیش در خدمت ارتکاب جرایم قرار می‌گیرند. اینترنت بستری را برای ارتکاب برخی از جرایم فراهم آورده است که تا پیش از آن اساساً با استفاده از مطبوعات نوشتاری یا رسانه‌های صدا و سیمایی ارتکاب پیدا می‌کردند. امکانات متنوعی که اینترنت با شکل‌های مختلف ایجاد می‌کند پشتوانه محکمی برای ارتکاب برخی از جرایم فراهم می‌آورد. سامانه‌ها و شبکه‌هایی رایانه‌ای پشتوانه جرایمی برای ارتکاب جرایمی متعددی همانند هرزه‌نگاری و به ویژه هرزه‌نگاری کودکان، ترغیب کودکان به روسپیگری، جرایم علیه حریم خصوصی، ارتکاب جرایم مطبوعاتی، برخی از جرایم علیه شخصیت معنوی افراد است. قانون جرایم رایانه‌ای در دو فصل چهارم و پنجم زیر عناوین جرایم علیه عفت عمومی و اخلاق عمومی و هتک حیثیت و نشر اکاذیب به سرکوب برخی از رفتارهایی پرداخته است که سامانه و شبکه اطلاعات پشتوانه ارتکاب آنهاست.

قانون‌گذار جرایم رایانه‌ای، زیر عنوان جرایم علیه عفت اخلاق عمومی، سه دسته از رفتارها را جرم‌انگاری کرده است:[1] رفتارهای مرتبط به محتویات مستهجن (ماده ۱۴ ق.ج.ر) و معاونت در دسترسی به محتویات مستهجن (بند الف ماده ۱۵ ق.ج.ر) و دستیاری افراد در ارتکاب برخی از جرایم علیه اشخاص و یا آموزش دادن بزه به این افراد (بند ب ماده ۱۵ ق.ج.ر). دو رفتار نخست در واقع زیر بنای جرم هرزه‌نگاری را تشکیل می‌دهند که قانون‌گذار ایران عناوین سنتی جرایم علیه عفت و اخلاق عمومی و محتویات مستهجن را بر آن ترجیح داده است. محتویات مستهجن بر اساس تبصره ۴ ماده ۱۴ همین قانون شامل «تصویر، صوت، یا متن واقعی یا غیر واقعی، یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان» است. ماده ۱۴ ق.ج.ر دو دسته رفتار را سرکوب می‌کند: دسته نخست مربوط به انتشار، توزیع یا معامله محتویات مستهجن، صرف‌نظر از قصد مرتکب در انجام این امور،

داده‌پیام‌های شخصی را مشخص ساخته است؛ با این توضیح که مصادیق مورد نظر در این قانون تنها ناظر به داده‌های شخصی حساس است.

۱. قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیر مجاز می‌نمایند مصوب ۱۳۷۲ و اصلاحی سال ۱۳۸۶.

می‌باشد و دسته دوم تولید، ذخیره و نگهداری این محتویات به قصد تجارت یا افساد را شامل می‌شود. بند ماده ۱۵ این قانون معاونت در دسترسی به محتویات مستهجن را به صورت مستقل جرم‌انگاری کرده است (تحریک، ترغیب، تهدید یا تطمیع افراد به منظور دستیابی آنها به محتویات مستهجن).

بند ب ماده ۱۵ از محدوده هرزه‌نگاری فراتر می‌رود و یک جرم‌انگاری گسترده را تشکیل می‌دهد. بر اساس این ماده تحریک یا ترغیب یا تهدید، دعوت، فریب افراد به ارتکاب جرایم منافی عفت، استعمال مواد مخدر یا روانگردان، خودکشی، انحرافات جنسی اعمال خشونت‌آمیز، تسهیل ارتکاب و یا آموزش ارتکاب آنها، جرم محسوب می‌شود. هر چند که سرکوب استفاده از سامانه و شبکه رایانه‌ای برای ارتکاب جرایم امری ضروری است با این حال سرکوب این استفاده با استناد به عناوینی مانند انحرافات جنسی که موضوع تعریف و جرم‌انگاری دقیقی قرار نگرفته‌اند شایسته اصل دقت و خوانا بودن قوانین کیفری نیست. همچنین بهتر بود در این ماده به جرایمی همانند قاچاق انسان نیز اشاره می‌شد در آن بزهکاران از سامانه‌ها و شبکه‌های رایانه‌ای برای فریب افراد و یافتن قربانیان احتمالی خود استفاده می‌کنند.

در زمینه جرایم علیه شخصیت افراد رفتارهای متعددی در حقوق‌های کیفری مورد جرم‌انگاری قرار گرفته است. هدف این جرم‌انگاری‌ها حمایت افراد در برابر خطراتی چون آسیب به حریم خصوصی افراد، نقض محرمانگی مکاتبات افراد، افترا، غصب هویت افراد و غیره است. قانون جرایم رایانه‌ای در فصل پنجم خود شخصیت افراد را در مقابل سه رفتار مجرمانه مورد حمایت قرار گرفته است: رفتار نخست بر تغییر یا تحریف یک محتوای مربوط به دیگری (فیلم، صوت، تصویر) یا انتشار عالمانه محتوای تحریف شده مبتنی است (ماده ۱۶ ق.ج.ر)؛ رفتار دوم به انتشار اسرار یا داده‌های با محتوای خصوصی یا خانوادگی یا خصوصی، بدون رضایت افراد ذی‌نفع، مربوط می‌شود (ماده ۱۷.ق.ج.ر).[1] رفتار سوم به عنوان نشر اکاذیب جرم‌انگاری شده است (ماده ۱۸ ق.ج.ر). لازم به یادآوری است که این جرم دارای کارکردی دوگانه است. از یک طرف به دنبال تضمین امنیت همگانی است (انتشار اکاذیب و یا در دسترسی دیگران قرار دادن آنها به قصد اضرار یا تشویش اذهان عمومی یا مقامات رسمی) و از طرف دیگر از حیثیت افراد حمایت می‌کند (نسبت دادن اعمال بر خلاف حقیقت به شخص حقیقی یا حقوقی با همان مقاصد).

۱. قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیر مجاز می‌نمایند (مصوب۱۳۸۶) نیز به حمایت از حریم خصوصی شهروندان توجه داشته است. بندهای ب و ج ماده ۵ به ترتیب به رفتارهای مجرمانه زیر اختصاص یافته است: تهیه فیلم یا عکس از محله‌هایی که اختصاصی بانوان بوده و آنها فاقد پوشش مناسب می‌باشند مانند حمام‌ها و استخرها و یا تکثیر و توزیع آن؛ تهیه مخفیانه فیلم یا عکس مبتذل از مراسم خانوادگی و اختصاصی دیگران و تکثیر و توزیع آن.

### ۲ـ۳. سامانه و شبکه‌های اطلاعات: وسیله ارتکاب جرم

تحول فناوری رایانه‌ای و مخابراتی باعث گسترش جرایمی شده است که قبل از پیدایش شبکه در قوانین کیفری مورد جرم‌انگاری قرار گرفته‌اند. سامانه‌ها و شبکه‌های اطلاعاتی وسیله‌های ارتکاب این جرایم را افزایش داده و متعدد ساخته‌اند. جرایم علیه اموال، جرایم علیه مالکیت معنوی، قماربازی‌های اینترنتی و یا تبلیغات دروغین و فریبنده از جمله این دسته از جرایم می‌باشند.

در زمینه گسترش جرایم مالی قابل ارتکاب در فضای سایبر باید گفت که امروزه بیشتر مبادلات تجاری با پشتوانه سیستم‌ها و شبکه‌های اطلاعاتی صورت می‌گیرد. ورود اینترنت به این حوزه از یک طرف باعث تسهیل مبادلات تجاری و بانکی شده و از طرف دیگر فرصت‌های مجرمانه جدیدی به ویژه در زمینه تقلب نسبت به کارت‌های بانکی[۱] را ایجادکرده است. برخی از جرایم سنتی همانند سرقت، کلاهبرداری، خیانت در امانت و جرایم شبیه به آن نیز قابلیت اعمال بر رفتارهای ارتکاب‌یافته از طریق اینترنت را پیدا کرده‌اند. به عنوان نمونه در زمینه خیانت در امانت در حقوق فرانسه پرسشی در سال‌های اخیر مطرح شد مبنی بر اینکه آیا استفاده شخصی از وسایل رایانه‌ایی که کارفرما برای استفاده کاری در اختیار کارمند خود قرار می‌دهد خیانت در امانت محسوب می‌شود؟ شعبه اجتماعی دیوان عالی کشور فرانسه در این زمینه چنین اظهار نظر کرد: «بازدیدهای کارمند از پایگاه‌های اینترنتی در زمان انجام کار و با استفاده از ابزار رایانه‌ای که کارفرما، در راستای انجام وظایف کاری، در اختیار وی قرار داده است کارکرد حرفه‌ای دارد به گونه‌ای که کارفرما می‌تواند، خارج از حضور کارمند، آن پایگاه‌ها را مرور کند.[۲] همین شعبه در رأی جدید خود اعلام کرده است که بازدید از پایگاه‌های اینترنتی در بردارنده تصاویر جنسی تخلف انظباطی مهمی از جانب کارمند محسوب می‌شود و اخراج وی را به خاطر این تخلف مهم موجه می‌سازد.[۳]

قانون جرایم رایانه‌ای مصوب ۱۳۸۸ در فصل سوم خود دو نوع از مهم‌ترین جرایم مالی (سرقت و کلاهبرداری) را مورد توجه قرار داده است و ارتکاب آنها از طریق رایانه را جرم‌انگاری کرده است (مواد ۱۲ و ۱۳ ق.ج.ر). جرم سرقت رایانه‌ای بر ربایش غیرمجاز داده‌های دیگری، چنانچه عین داده‌ها در اختیار صاحب آن باشد، مبتنی است. این ربایش که به معنای دست‌اندازی به داده‌های دیگری است در عمل از طریق

۱. در کشور فرانسه قانون مصوب ۱۵ نوامبر ۲۰۰۱ راجع به امنیت روزمره مرکزی با عنوان دیده‌بان تامین امنیت کارت‌های پرداختی ایجاد کرد. یکی از فعالیت‌های این مرکز رصد کردن تقلب‌های جدید نسبت به این کارت‌هاست.

2. Soc-45.9 juill.2008, n°06-45.800.

3. Soc.21 sept.2011, n°10-14.869.

روگرفتن (کپی) یا برش (کات) داده‌ها صورت می‌گیرد.[1] رفتارهای تشکیل‌دهنده جرم کلاهبرداری[2] باید در بستر سامانه‌های رایانه‌ای و مخابراتی صورت گیرند. جرم کلاهبرداری رایانه‌ای بر تحصیل غیرمجاز وجه، مال، یا منعت یا خدمات یا امتیازات مالی برای خود یا دیگری از سامانه‌های رایانه‌ای و مخابراتی از طریق اعمالی که در ماده ۱۷ ق.ج.ر به طور تمثیلی احصاء شده‌اند (واردن کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها با مختل کردن سامانه) مبتنی است.

استفاده از ابزارهای سایبری به عنوان وسیله ارتکاب جرم به طور خاص در ماده ۲۵ قانون جرایم رایانه‌ای. ماده ۲۵ ق.ج.ر جرم‌انگاری شده است. این ماده سه دسته از رفتارهای مجرمانه راسرکوب می‌کند: دسته نخست شامل تولید، انتشار، توزیع، در دسترس‌گذاری و یا معامله داده‌ها یا نرم افزارها یا هر نوع ابزار الکترونیکی که صرفا به منظور ارتکاب جرایم رایانه‌ای بکار می‌رود (بند الف ماده ۲۵). بد افزارها از گوناگونی و پویایی خیره‌کننده‌ای برخوردارند و دارای قابلیت آسیب‌زایی بالایی هستند. باج افزارها[3] از جمله بدافزارهایی است که امروزه زمینه ارتکاب اخاذی‌های رایانه‌ای را فراهم آورده است؛ دسته دوم رفتارهای مجرمانه مربوط به فروش یا پخش یا در دسترس‌گذاری داده‌های رخنه‌گر است. منظور از داده‌های رخنه‌گر گذرواژه یا هر داده‌ای است که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌آورد. (بند ب ماده ۲۵)؛ دسته سوم از رفتارهای مجرمانه موضوع این ماده شامل پخش یا در دسترس قرار دادن محتویات آموزش جرایم رایانه‌ای (دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، تخریب و اخلال داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی (بند ج ماده ۲۵) می‌شود.

در زمینه دیگر جرایمی که در آن از سامانه و شبکه به عنوان وسیله ارتکاب مورد استفاده قرار می‌گیرند، همانند جرایم علیه مالکیت معنوی،[4] قانون جرایم رایانه مجازات

۱. عالی‌پور، حسن، منبع پیشین، ص. ۲۵۵.

۲. اصطلاح کلاهبرداری کامپیوتری نخست در قانون تجارت الکترونیکی مصوب ۱۳۸۲ مطرح شد. ماده ۶۷ این قانون به تبیین عنصرهای تشکیل‌دهنده آن پرداخته است. در زمینه کلاهبرداری رایانه‌ای ر.ک: میرمحمد صادقی، حسین؛ شایگان، محمدرسول، «بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازات‌های آن در نظام حقوقی ایران»، دیدگاه‌های حقوق قضایی، شماره ۵۱ و ۵۲، ۱۳۸۹، صص. ۱۶۲ـ۱۳۷.

۳. Ransomware: باج‌افزار نرم‌افزاری زیان‌آور است که به سامانه یک کاربر رخنه کرده، دسترسی کاربر به داده‌های خود را محدود یا غیرممکن می‌سازد و طراح این بدافزار برای برداشتن محدودیت و ممکن ساختن دسترسی به داده‌ها باج‌خواهی می‌کند.

۴. قوانینی که در این زمینه می‌توان بدانها مراجعه کرد عبارتند از: قانون حمایت از نشانه‌های جغرافیایی (مصوب ۱۳۸۳/۲/۱۸)؛ قانون تجارت الکترونیکی (۱۳۸۲/۱۱/۱۱)؛ قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری (مصوب ۱۳۸۶)؛ قانون حمایت از مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸؛ قانون حمایت از

خاصی پیش‌بینی نشده است و از روش ارجاع استفاده نموده است. ماده ۵۲ ق.ج.ر مقرر می‌دارد :«در مواردی که سامانه رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم به کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قوانین جزایی مربوط به عمل خواهد شد». روش ارجاع‌دهی پیش‌بینی شده در این ماده این امکان را برای کارگروه (کمیته) تعیین مصادیق مجرمانه پیش‌بینی شده در ماده ۲۲ ق.ج.ر را فراهم می‌آورد تا نسبت به تعیین مصادیق جرایم رایانه‌ای بر اساس قوانین دیگر، علاوه بر قانون جرایم رایانه‌ای، نیز اقدام نماید. در فهرستی که این کارگروه از مصادیق محتوای مجرمانه در درگاه اینترنتی خود قرار داده است[1] مصادیق متعددی تحت عناوین زیر به احصاء شده است: محتوا علیه عفت و اخلاق عمومی (۶ مصداق)؛ محتوای علیه مقدسات اسلامی (۷ مصداق)؛ محتوای علیه امنیت و آسایش عمومی (۱۶ مصداق)؛ محتوای علیه مقامات و نهادهای دولتی و عمومی (سه مصداق)؛ محتوا مرتبط با جرایم رایانه‌ای (محتوایی که برای ارتکاب جرایم رایانه‌ای به کار می‌رود) (۹ مصداق)؛ محتوایی که تحریک، ترغیب یا دعوت به ارتکاب جرم می‌کند (محتوای مرتبط با سایر جرایم) (۸ مصداق)؛ محتوا مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی (۴ مصداق)؛ محتوای مرتبط با انتخابات مجلس شورای اسلامی و مجلس خبرگان رهبری (۱۴ مصداق) و محتوای مجرمانه مرتبط با انتخابات ریاست جمهوری (۲۵ مصداق). این کارگروه همچنین فهرستی از قوانینی که در مصداق‌یابی خود در جرایم رایانه‌ای به آنها استناد کرده است را در پایان فهرست مصادیق مجرمانه معرفی نموده است.[2] فهرست تهیه شده از مصادیق جرایم سایبری توسط پلیس فتا برای کشف جرایم سایبری مورد استفاده قرار می‌گیرد.

## ۳. وضعیت بزهکاری سایبری بر اساس آمار پلیس فتا

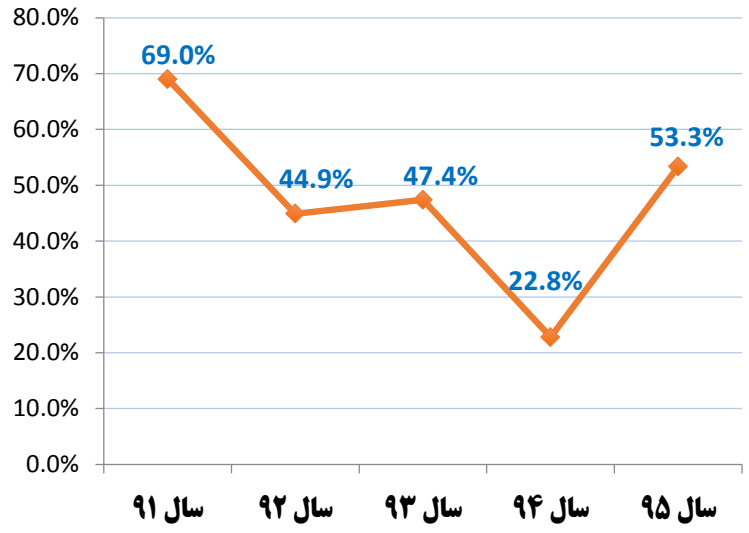
بررسی وضعیت جرایم سایبری در پنج سال اخیر (۱۳۹۵ ـ ۱۳۹۱) نشان می‌دهد که از مجموع پرونده‌های متشکله، حوزه اقتصادی ۴۷٪، حوزه اخلاقی و فرهنگی ۳۲٪،

نرم‌افزارهای رایانه‌ای؛ قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ۱۳۵۲؛ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز دارند مصوب ۱۳۸۶.

1. http://internet.ir/crime_index.html.

۲. در میان این قوانین علاوه بر قانون جرایم رایانه‌ای و قانون مجازات اسلامی مصوب ۱۳۹۲، به قوانین زیر استناد شده است: قانون مطبوعات مصوب ۱۳۷۹، قانون مجازات انتشار و افشای اسناد محرمانه و سرّی دولتی مصوب ۱۳۵۳، قانون بازار و اوراق بهادار مصوب ۱۳۸۴، قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵، قانون ممنوعیت به‌کارگیری تجهیزات دریافت ماهواره مصوب ۱۳۷۳، قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز دارند مصوب ۱۳۸۶، قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای مصوب ۱۳۷۹، قانون تجارت الکترونیکی مصوب ۱۳۸۲، قانون انتخابات مجلس شورای اسلامی مصوب ۱۳۷۸، قانون انتخابات ریاست جمهوری۱۳۶۴، قانون اخلال در نظام اقتصادی کشور مصوب ۱۳۶۹.

حـوزه اجتمـاعی ۱۴٪ و حـوزه سیاسـی ۷٪ از جـرایم را بـه خـود اختصـاص داده اسـت. بیشترین جرایم مربوط به جرم برداشت غیرمجاز از حساب‌هـای بـانکی بـا ۳۶/۵٪، هتـک حیثیت و نشر اکاذیب با ۹/۵٪ و کلاهبـرداری رایانـه‌ای بـا ۸/۸٪ مـی‌باشـد. گسـترش روز افزون خدمات مبتنی بر فناوری اطلاعات و ارتباطات در سال‌های گذشته موجـب گردیـده وقوع جرایم سایبری هر سال نسبت به سال قبل از آن افزایش پیدا کند. با تناسب فراگیـر شدن نوع خدمات در سطح جامعه، میزان ارتکاب جرایم در حوزه‌های مختلـف اجتمـاعی، اقتصادی و اخلاقی و فرهنگی نیز تغییر پیدا کرده است. نمودار زیر درصد رشـد جـرایم از سال ۹۱ تا سال ۹۵ (نسبت به مدت مشابه سال قبل در هر سال) را نشان می‌دهد:




در سال ۱۳۹۵ نیز ۴۳.۵٪ از پرونـده‌هـای متشـکله مربـوط بـه حـوزه اخلاقـی و فرهنگی، ۳۳.۱٪ حوزه اقتصادی، ۱۸٪ حـوزه اجتمـاعی و ۵.۴٪ نیـز مربـوط بـه حـوزه سیاسی بوده است. از بدو تاسیس پلیس فتا تـاکنون حـوزه اقتصـادی بیشـترین میـزان جرایم در هر سال را بـه خـود اختصـاص داده اسـت. در سـال ۹۵ بـه دلیـل گسـترش چشـمگیر اسـتفاده از شـبکه‌هـای اجتمـاعی و موبـایلی در بـین کـاربران و روی‌آوردن بزهکاران به استفاده از این وسیله‌ها، جرایم مـرتبط بـا حـوزه‌هـای اخلاقـی و فرهنگـی افزایش داشته است. اختصاص ۴۶.۴ درصدی کـل پرونـده‌هـای تشـکیل شـده در همـه حوزه‌ها و همچنین ۸۹ درصدی پرونده‌های حوزه اخلاقی به انواع اپلیکیشن‌های[1] OTT نشان‌دهنده این موضوع است.

1. Over the top application

در بین انـواع شـبکه‌هـای موبـایلی نیـز شـبکه اجتمـاعی، تلگـرام (Telegram) بیشترین سهم را در بین پرونده‌های سایبری داشته است. در سال ۹۵ بیشـترین میـزان پرونده‌های تشکیل‌شده به ترتیب مربوط به استان‌های تهران بـزرگ (۲۷.۳٪)، خراسـان رضـوی (۹.۵٪)، فـارس (۷.۹٪) و آذربایجـان شـرقی (۵.۵٪) بـوده اسـت. فیشـینگ درگاه‌های بانکی و نصب بدافزارهای جاسوسی، سوءاستفاده از اعتمـاد افـراد مهـم‌تـرین شگردهای فنی مورد استفاده برای ارتکاب جرایم حوزه اقتصادی را تشـکیل داده اسـت. در خصوص کلاهبرداری‌های رایانه‌ای اغفال بزه‌دیدگان (عمدتاً از طریق پیامـک) و اخـذ اطلاعات حساس نظیر شماره حساب و رمز دوم و نهایتـاً خریـد اینترنتـی از مهـم‌تـرین روش‌های مورد استفاده بزهکاران سایبری است. بیشترین فراوانی وقوع جـرایم سـایبری در کشور در شش سال اخیر به ترتیب مربوط به تهران بزرگ با ۲۸/۵٪، خراسان رضوی با ۷/۹٪، فارس با ۷/۴٪ و آذربایجان شرقی با ۵/۷٪ بوده است.

سیمای بزه‌دیدگان جرایم سایبری در شش سال اخیر نشان مـی‌دهـد کـه مـردان ۶۵٪ و زنان ۳۵٪ از مجموع شاکیان را تشکیل داده‌انـد. سـطح تحصـیلات شـاکیان بـه صورت زیر بوده است: ۱۴٪ از تحصیلات زیر دیپلم، ۳۵٪ دیپلم، ۹٪ فـوق دیـپلم، ۳۲٪ لیسانس، ۷٪ فوق لیسانس و ۳٪ دکترا. از مجمـوع متهمـان دسـتگیر شـده حـدود ۸۴ درصد مرد و بقیه زن بوده‌اند که از میان آنها ۶٪ زیر ۱۷ سال، حدود ۳۳ درصد بین ۱۸ تا ۲۶ سال و مابقی بالای ۲۷ سال سن داشته‌اند. در خصوص میزان تحصیلات متهمـان دستگیر شده بررسی‌های انجام شده بر روی پرونده‌های تشـکیل شـده از بـدو تاسـیس پلیس فتا نشان می‌دهد که ۴۵٪ از متهمین دارای مدرک تحصـیلی دیـپلم، ۱۱٪ فـوق دیپلم، ۲۳٪ کارشناسی، ۴٪ کارشناسی ارشد، ۱٪ دکترا و بالاتر و ۱۶٪ نیـز زیـر دیـپلم بوده‌اند. از بسترهای مورد استفاده برای ارتکاب جرایم در شبکه‌های اجتماعی اپلیکیشن تلگرام با ۶۰٪ بیشترین سهم را داشـته و نقـش اینسـتاگرام ۱۷٪ بـوده اسـت. افـزایش استفاده کاربران شبکه‌های اجتماعی تلگرام و اینستاگرام باعث تغییر رویکـرد بزهکـاران سایبری شده است؛ آنان بیش از پیش برای ارتکاب جرایم مرتبط با محتوا (نظیر جـرایم حوزه اخلاقی و فرهنگی) و کلاهبرداری‌های رایانه‌ای به اسـتفاده از ایـن رسـانه‌هـا روی آورده‌اند. بدیهی است که بهره‌گیری صحیح از خدمات فناوری اطلاعات در بین کـاربران مستلزم ارتقای سطح آگاهی و دانش استفاده‌کنندگان از این خدمات بوده کـه ایـن امـر خود همکاری همه دستگاه‌های مرتبط با این حوزه را می‌طلبد.

## نتیجه‌گیری

گونه‌شناسی بزهکاری سایبری نشان می‌دهد که این بزهکاری دو دسته از جرایم را در برمی‌گیرد: گونه نخست از جرایمی خاص و جدید تشکیل شده است که علیه خود سامانه‌ها و شبکه‌های اطلاعاتی صورت می‌گیرد و یا اینکه بدون وجود این سامانه‌ها قابلیت ارتکاب ندارند؛ گونه دوم که تعداد آنها بسیار زیاد است شامل جرایم رایج و متداولی است که بیش از پیش در بستر فناوری اطلاعات ارتکاب پیدا می‌کنند. فن‌آوری اطلاعات یا وسیله ارتکاب این جرایم قرار می‌گیرد و یا اینکه به عنوان پشتوانه ارتکاب آنها را تسهیل می‌کند. قانون جرایم رایانه‌ای با پیروی از کنوانسیون جرایم سایبری بوداپست به طور کلی از این الگو پیروی کرده است، هر چند از لحاظ معرفی جرایم تا حدودی دچار پراکندگی شده است. از لحاظ عملی، کارگروه مصادیق مجرمانه یک گونه‌شناسی محتوایی از جرایم سایبری ارائه کرده است. این کارگروه با تکیه بر قوانین، مقررات و آیین‌نامه‌های مختلف فهرستی از جرایم را احصاء کرده است که ارتکاب آنها در بستر سامانه‌های اطلاعاتی امکان‌پذیر است. این فهرست مورد استفاده پلیس فتا نیز می‌باشد. پیشنهاد می‌شود با همکاری این دو نهاد این فهرست به گونه‌ای دقیق‌تر تکمیل شود و در آن دو دسته از جرایم طبقه‌بندی شود: دسته نخست شامل جرایمی باشد که به طور ویژه ماهیتی سایبری دارند، بدین معنی که چه از لحاظ موضوع و چه از لحاظ شیوه ارتکاب ارتباط آنها با فضای سایبری در قانون تصریح شده است؛ دسته دوم جرایمی را در برگیرد که ارتباط آنها با فضای سایبری به صراحت مورد اشاره قانون‌گذار قرار نگرفته است اما مجریان قانون، در مقام کشف و تعقیب جرایم، چنین ارتباطی را تایید کرده‌اند. استفاده از یک فهرست طبقه‌بندی شده از جرایم سایبری توسط مجریان قانونی این امکان را فراهم می‌آورد تا وضعیت آماری این بزهکاری به گونه‌ای دقیق‌تر و جامع‌تر معرفی شود. با تکیه بر ارزیابی وضعیت تحول این بزهکاری در جامعه و نیز با شناخت بهتر تأثیر فناوری‌های نوین در پیدایش و گسترش بزهکاری است که قانون‌گذار کیفری می‌تواند سیاسی کیفری خود در مقابله با این بزهکاری را به‌روز سازد.

## منابع


- جاویدنیا، جواد، جرایم تجارت الکترونیکی (جرایم رایانه‌ای در بستر تجارت الکترونیکی)، انتشارات خرسندی، ۱۳۹۱.
- حاجی ده آبادی، احمد؛ سلیمی، احسان، «اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرائم رایانه‌ای)»، فصلنامه مجلس و راهبرد، شماره ۸۰، ۱۳۹۳.
- خرم‌آبادی، عبدالصمد، «تاریخچه، تعریف و طبقه‌بندی جرم‌های رایانه‌ای»، در: مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی، انتشارات سلسبیل، ۱۳۸۴.
- داوری دولت‌آبادی، مجید، امنیت در پایگاه‌های داده، انتشارات پلیس فضای تولید و تبادل اطلاعات ناجا (فتا)، ۱۳۹۲.
- رهامی، محسن؛ پرویزی، سیروس، «جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین‌المللی آن»، فصلنامه حقوق، مجله دانشکده حقوق و علوم سیاسی، شماره ۳، سال ۱۳۹۱.
- زیبر، اولریش، جرایم رایانه‌ای، چاپ دوم، ترجمه محمدعلی نوری و دیگران، تهران، گنج دانش، ۱۳۹۰.
- صادقیان، داود، «کالبدشناسی جرائم سایبری در ایران»، دادرسی، شماره ۸۸، ۱۳۹۰.
- عباسی کلیمانی، عاطفه؛ اکبری، عاطفه، جرایم سایبری، تهران انتشارات مجد، ۱۳۹۴.
- عالی‌پور، حسن، حقوق کیفری فناوری اطلاعات، چاپ چهارم، معاونت حقوقی و توسعه قضایی قوه قضاییه، مرکز مطالعات توسعه قضایی، ۱۳۹۵.
- فراهانی، امیرحسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، انتشارات خرسندی، ۱۳۹۵.
- قناد، فاطمه، «کلاهبرداری الکترونیکی در بستر فناوری‌های اطلاعات و ارتباطات»، فصلنامه پژوهش حقوق و سیاست، شماره ۲۵.
- میرمحمد صادقی، حسین؛ شایگان، محمدرسول، «بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازات‌های آن در نظام حقوقی ایران»، دیدگاه‌های حقوق قضایی، شماره ۵۱ و ۵۲، ۱۳۸۹.
- یاسمی‌نژاد، عرفان؛ آزادی سرابله، اکرم، مبانی امنیت در اینترنت، انتشارات پلیس فضای تولید و تبادل اطلاعات ناجا (فتا)، ۱۳۹۲.

- Cazki, M., Combattre la cybercriminalité, édition de Saint Amans, Perpignan, 2009.
- Chopin, F., «Cybercriminalité», Répertoire de droit pénal et de procédure pénale, Dalloz, 2017.
- Leman-Langlois, S., «Le crime comme moyen de contrôle du cyberspace commercial», Criminologie, 39,9 (1), 2006.
- Kim-Kwang, R. C., «Organised crime groups in cyberspace: a typology.», Trends Organ Crim, n°11, 2008.
- Manky, D., «Cybercrime As A Service: A very Modern Business.», Computer Fraud & Security, n°6, 2008.
- Rouiai, A. «La piraterie moderne, d'une mer à l'autre», Carto, n°41, 2017.
- Savatier, R., Les métamorphoses économiques et sociales du droit privé d'aujourd'hui, Dalloz, 1959.
- Wall, D.S. «The internet as a conduit for criminal activity», in: Pattavina, A. (Ed.), Information technologie and Criminal Justice System, Thousand Oaks, CA: Sage publication, 2005/2015.