مجله حقوقی دادگستری

مقاله پژوهشی/ دوره ۸۹/ شماره ۱۳۰/ صفحات: ۱۴۲-۱۱۱
تاریخ دریافت: ۱۴۰۳/۰۷/۳۰ تاریخ پذیرش: ۱۴۰۳/۱۲/۲۳

تخریب کیفریِ رایانه‌ای در حقوق ایران، انگلستان و وِیلز

امیر اعتمادی[۱]

چکیده

در جرم تخریب سنتی، رفتار مجرمانه نسبت به اشیای منقول یا غیر منقولی انجام می‌گیرد که در عالم خارج محسوس و لمس‌پذیر است، ولی اعمال خراب‌کارانه‌ای که به تخریب اطلاعات رایانه‌ای یا از کار افتادن سامانه‌های رایانه‌ای یا مخابراتی منجر می‌شوند، صورت متفاوتی دارند که با شکل سنتی آن فرق می‌کند. در حقوق کیفری ایران، تخریب رایانه‌ای به دو شکل تخریب داده‌های رایانه‌ای و اخلال در سامانه‌های رایانه‌ای یا مخابراتی پیش‌بینی شده است. در مقابل، در حقوق انگلستان و وِیلز، جرم دست‌کاری غیر مجاز داده‌های رایانه‌ای در راستای مقابله با هرگونه عمل غیر مجازی که با قصد اخلال در کارکرد رایانه، مانع دسترسی به برنامه یا داده رایانه‌ای شدن و یا مختل کردن عملکرد برنامه یا اطمینان پذیری داده رایانه‌ای ارتکاب یابد، جرم‌انگاری شده است. مقایسه نظام‌های کیفری یاد شده روشن می‌سازد که برخی نقص‌ها در رویکرد قانون‌گذار ایرانی، از جمله بی‌توجهی به برخی پیشرفت‌های فناوری نظیر اینترنت اشیا و به رسمیت نشناختن بی‌پروایی کیفری وجود دارد که برطرف ساختن آن‌ها در مقابله مؤثرتر با تخریب‌گران رایانه‌ای و صدور آرای کیفریِ منسجم تأثیر مطلوبی خواهد داشت.

واژگان کلیدی: اخلال در سامانه‌های رایانه‌ای یا مخابراتی، تخریب کیفری رایانه‌ای، تخریب داده‌های رایانه‌ای، دست‌کاری غیر مجاز داده‌های رایانه‌ای.

---

۱. استادیار گروه حقوق کیفری و جرم شناسیِ دانشکده حقوقِ دانشگاه قم، ایران، قم.
am.etemadi@gmail.com

درآمد

ظهور اینترنت و شـــبکه جهانی وِب، ارتباط متقابـــل بین نظام‌های رایانه‌ای و اَبَرپیوند اطلاعات در سراسر شبکه که به انفجار بی‌سابقه محتوا، ارتباطات و اَبَرداده‌ها منجر می‌شود، نشان‌دهنده تغییر از جرم رایانه‌ای[1] به جرم سایبری[2] است. آدمی اکنون در دنیایی متفاوت از دو دهه پیش زندگی می‌کند. این امر با افزایش بی‌ســابقه قدرت رایانه‌ای به واســطه کوچک‌سازی ضمنیِ حامل‌های داده دیجیتال از یک سو و به هم پیوستگیِ بیش‌از حد معمول با تأثیرهای شبکه متعاقب آن از سوی دیگر، ارتباط دارد (Hildebrandt, 2020:166).

در این میان در جرائم تخریب سنتی، رفتار مجرمانه نسبـــت به اشیایی اعم از منقول یا غیر منقول انجام می‌گیرد که در عالم خارج لمس‌پذیر هستنـد، اما پیشرفت‌ها در حوزه فناوری اطلاعات[3] موجب شـــکل‌گیری داده‌های گوناگونی شـــده‌اند که در فضاهایی نظیر دیســـک‌های رایانه‌ای ذخیره می‌شـــوند. افزون بـــر این، انواع مختلفی از دســـتگاه‌های رایانه‌ای یا مخابراتی، از قبیل رایانه دســـتی، تبلت و تلفن هوشمند، وجود دارند که ممکن اســـت حاوی داده‌هـــای مهمی باشـــند. ناگفته پیدا است که اَعمال خرابکارانه‌ای که به تخریب اطلاعات رایانه‌ای و یا از کار افـــتادن سامانه‌های رایانه‌ای یا مخابراتی منجر می‌شـــوند، صورت متفاوتی دارند که با شـــکل سنتی آن فرق می‌کند. بر این اساس، پیش‌بینی تخریب کیفری رایانه‌ای[4] در راســـتای حمایت کیـــفری از داده‌ها و یا سامانه‌های رایانه‌ای یا مخابراتیِ متـــعلق به دیگری ضروری قلمداد می‌شـود.

در حقوق انگلســـتان و وِیلز، اگر چه قانـــون خاصی زیر عنوان قانون تخریب کیفری ۱۹۷۱ [5] وجود دارد، بند ۱ ماده ۱۰ آن بر اموال با ماهیت عینی تأکید دارد؛ لذا برنامه‌ها و داده‌های رایانه‌ای از شـــمول این قانون خارج هستند. بند ۵ ماده ۱۰ قانون مذکور (الحاق شده به موجب قانون پلیس و عدالت ۲۰۰۶ [6]) نیز اعلام می‌دارد که در

1. Computer crime.
2. Cybercrime.
3. Information Technology.
4. Computer criminal damage.
5. Criminal Damage Act 1971.
6. Police and Justice Act 2006.

راستای هدف‌های این قانون، دســـت‌کاری محتویات رایانه به مثابه ایراد خسارت به هرگونه رایانه یا ابزار ذخیره‌ســـازیِ رایانه‌ای تلقی نخواهد شد؛ مگر این‌که تأثیر آن بر رایانه یا ابزار ذخیره سازیِ رایانه‌ایِ مزبور، وضعیت فیزیکی آن را مختل کند[1].

در پرونـــده وایتلی (۱۹۹۱)[2]، متهم دسترســـی غیر مجاز به شـــبکه مشـــترکِ دانشـــگاهی (جَنِت)[3] پیدا کرد و جایگاه مدیر ســـامانه‌ها را برای خودش تعیین کرد. وی فایل‌هایـــی را حذف و اضافه نمود، رمزهای عبور را تغییر داد و فایل‌های ممیّزیِ ثبت‌کننده فعالیت‌هایش را حذف کرد. مرتکب بسیار ماهر بود و حتی برنامه خاصی که برای به دام انداختن او قرار داده شده بود را حذف نمود. فعالیت‌های او باعث اختلال شدیدی شـــد و به تخریب دیسک‌های رایانه‌ای محکوم شد. دادگاه تجدید نظر مقرر داشـــت که ارزش دیسک‌ها کاهش یافته است و درخواست تجدید نظرش را رد کرد. رئیـــس دادگاه تجدیدنظر، لُرد لِین[4] اظهار داشـــت که به موجب قانون تخریب کیفری ۱۹۷۱ لازم است مال عینی تخریب شده باشد، نه این‌که خسارت خودش عینی باشد. در این پرونده، محکومیت مبتنی بر این بود که وضعیت ذره‌های مغناطیسیِ دیسک‌ها تغییر یافته‌اند، لذا می‌توانست استدلال شود که حتی اگر این ذره‌ها رؤیت‌پذیر نباشند، عینی قلمداد می‌شوند.

بر این اســـاس، پرسش‌هایی که مطرح می‌شـــوند عبارت است از: قانون‌گذار ایرانی، انگلیســـی و وِیلزی نســـبت به تخریب کیفری رایانـــه‌ای چه رویکردی اتخاذ کرده‌اند؟ عنصرهای ســـازنده جرم یاد شـــده در نظام‌های کیفری ایران، انگلســـتان و وِیلز چه تفاوت‌ها و شـــباهت‌هایی دارند و در راســـتای مقابله مؤثرتر با تخریب‌گران رایانه‌ای، چه راهکارهایی می‌توان ارائه کرد؟ در پاســـخ به این پرسش‌ها، ابتدا عنصر قانون تخریب کیفری رایانه‌ای بررسی می‌شود و سپس، با تحلیل عنصر مادی و عنصر

1. Section 10 (5) of the Criminal Damage Act 1971(inserted by Police and Justice Act 2006) provides: "For the purposes of this Act a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition".
2. Whiteley (1991) 93 Cr App R 381.
3. Joint Academic Network (JANET).
4. Lord Lane.

روانی جرم مذکور به نتیجه‌گیری و ارائه راهکارها پرداخته خواهد شد.

۱. عنصر قانونی تخریب کیفری رایانه‌ای

قانون‌گذار ایران تخریب کیفری رایانه‌ای را به دو صورت پیش‌بینی کرده است. از یک طرف، ماده ۷۳۶ قانون مجازات اسلامی (تعزیرات) الحاقی ۱۳۸۸ درباره تخریب داده‌های رایانه‌ای اعلام می‌دارد: «هر کس به طور غیر مجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیر قابل پردازش کند، به حبس از شش ماه تا دو سال یا جزای نقدی از هشتاد و دو میلیون و پانصد هزار ریال تا سیصد و سی میلیون ریال[1] یا هر دو مجازات محکوم خواهد شد». از طرف دیگر، ماده ۷۳۷ قانون مذکور در مورد اخلال در سامانه‌های رایانه‌ای یا مخابراتی اشعار می‌دارد: «هر کس به طور غیر مجاز با اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دست‌کاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آن‌ها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از هشتاد و دو میلیون و پانصد هزار ریال تا سیصد و سی میلیون ریال[2] یا هر دو مجازات محکوم خواهد شد»[3].

مفاد مواد قانونی بالا روشن می‌سازد که رایانه یا شبکه‌های رایانه‌ای در جرم تخریب رایانه‌ای حسب مورد مکان یا آماج فعالیت مجرمانه[4] است، نه صرفاً ابزاری برای ارتکاب جرم[5]. به همین خاطر، تخریب کیفری رایانه‌ای عمدتاً در محیط دیجیتال ارتکاب می‌یابد و مستلزم به‌کارگیری سامانه رایانه‌ای و حداقل بعضی از مهارت‌های فناوری اطلاعات است. در مقابل، در انگلستان و ویلز، قانون‌گذار ماده ۳ قانون سوء استفاده رایانه‌ای مصوب ۱۹۹۰[6] جرم مستقلی در این زمینه پیش‌بینی کرده است که

---

۱. بنگرید به: تصویب‌نامه شماره ۵۶۲۶۱/ت۶۲۲۹۸ه هیأت وزیران در خصوص اصلاح میزان مبالغ مربوط به جرایم و تخلفات مندرج در قوانین مختلف مورخ ۱۴۰۳/۴/۱۴، پیوست ۱ـ جرائم، ردیف ۵.

۲. بنگرید به: همان، ردیف ۵.

۳. باید خاطرنشان کرد که مواد قانونی مورد بحث درواقع، مواد ۸ و ۹ از قانون جرائم رایانه‌ای ۱۳۸۸ بوده‌اند که با الحاق مواد ۱ تا ۵۴ قانون اخیر به ادامه قانون مجازات اسلامی (تعزیرات) ۱۳۷۵ به‌عنوان مواد ۷۲۹ تا ۷۸۲، شماره آن‌ها به ۷۳۶ و ۷۳۷ تغییر کرده است.

4. Place or target of criminal activity.

5. Instrument for committing an offence.

6. Computer Misuse Act 1990.

زیر عنوان دســـت‌کاری غیر مجازِ داده‌های رایانه‌ای[1] خوانده می‌شـــود. بندهای ۱ تا ۳ این ماده مقرر می‌دارد:

۱- شـــخص، مقصر به جرم است، اگر: الف- هرگونه عمل غیر مجازی را در ارتبـــاط با رایانه انجام دهد؛ ب- در زمانی کـــه عمل مورد نظر را انجام می‌دهد، آگاه باشد که غیر مجاز است؛ و پ- یا بند ۲ یا بند ۳ زیر مصداق داشته باشد؛

۲- این بند در صورتی اعمال می‌شـــود که شخص با انجام عمل مربوط قصد داشته باشد که: الف- کارکرد هر رایانه‌ای را مختل کند؛ ب- مانع دسترسی به هرگونه برنامه یا داده‌ی نگه داشـــته شده در هر رایانه‌ای شود یا آن را به تأخیر اندازد؛ یا؛ پ- عملکـــرد هرگونه از این چنین برنامه‌ای یا اطمینان پذیریِ هرگونه از چنین داده‌ای را مختل کند؛ یا ت- امکان این‌که هر یک از موارد مذکور در پاراگراف‌های الف تا (پ) بالا انجام گیرد را فراهم سازد.

۳- این بند مصداق دارد، هرگاه شـــخص در مـــورد این‌که آیا عمل مورد نظر برای هر یک موارد اشـــاره شـــده در پاراگراف‌های الف تا ت بند ۲ بالا کافی است یا خیر، بی‌پروا باشد ...»[2].

شایان ذکر اســـت که از پیش‌بینی جرم مورد بحث در اصل با موج تبلیغات و ترس پیرامون استفاده از ویروس‌های رایانه‌ای[3] و سایر بدافزارها[4]، هم‌چنین نگرانی در

---

1. Unauthorised modification of computer material
2. Section 3 of the Computer Misuse Act 1990 provides: "(1) A person is guilty of an offence if —
(a) he does any unauthorised act in relation to a computer;
(b) at the time when he does the act he knows that it is unauthorised; and
(c) either subsection (2) or subsection (3) below applies.
(2) This subsection applies if the person intends by doing the act —
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer; or
(c) to impair the operation of any such program or the reliability of any such data; or
(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.
(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above".
3. Computer viruses
4. Malware

مورد آن‌چه رایانه‌زن‌ها[۱] بعد از دسترسی به دستگاه مورد نظر انجام می‌دهند حمایت شد. افزون بر این، در خصوص ابزارهای حمل کردنیِ داده[۲] از قبیل دیسک رایانه‌ای[۳]، حذف داده‌ها تنها در صورتی طبق ماده ۳ قانون بالا جرم محسوب می‌شود که ابزار ذخیره سازی[۴] متصل به رایانه باشد و به محض این‌که برداشته شود، هرگونه تخریبِ متعاقب آن، مشمول قانون تخریب کیفری ۱۹۷۱ خواهد بود (Reed, 2011: 700)[۵].

در خصوص جرمِ ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ هم‌چنین اظهار شده که به طور خاص برای کسانی پیش‌بینی شده است که ویروس‌های رایانه‌ای را می‌نویسند و با استفاده از تکنیک‌های فیشینگ[۶] یا اسب تراوا[۷] منتشر می‌کنند تا اطلاعات هویتی[۸] یا هرگونه داده دیگری را از منبع غیر مجازی[۹] به دست آورند یا فایل‌های سیستم عامل و یا جنبه‌ای از عملکردهای رایانه را تعدیل کنند تا مانع کارکرد آن شوند و یا از دسترسی به هرگونه داده‌ای جلوگیری کنند؛ نابودی فایل‌ها یا ایجاد عمدیِ کُدهایی برای این‌که موجب خرابی کاملِ سامانه شوند، به همین منظور انجام می‌گیرد (Wild & Weinstein, 2013: 663). در هر حال، قانون‌گذار انگلیسی و ویلزی در اصلاحاتی که مطابق با قانون پلیس و عدالت ۲۰۰۶ در قانون سوء استفاده رایانه‌ای ۱۹۹۰ اعمال کرده است، عنوان گذاری ماده ۳ قانون اخیر را به اعمال غیر مجاز با قصد اخلال در کارکرد رایانه و غیره یا بی‌پروایی در خصوص اخلال آن[۱۰] تغییر داده است.

۲. عنصر مادی تخریب کیفری رایانه‌ای

با بررسی مواد ۷۳۶ و ۷۳۷ از قانون مجازات اسلامی (تعزیرات) ۱۳۷۵ (الحاقی

---

۱. اصطلاح رایانه‌زن/داده‌زن که برگردان واژه‌ی انگلیسی Hacker به فارسی است، از کلمه راهزن ساخته شده است (محمدی‌فر، ۱۳۹۱: ۲۸۲).

2. Removable data media
3. Computer disk
4. Storage medium
5. See also, s 17 (6) of the Computer Misuse Act 1990.
6. Phishing techniques.
7. Trojan horse.
8. Identity data.
9. An unauthorised source.
10. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

۱۳۸۸) معلوم می‌شود که عنصر مادی جرائم تخریب رایانه‌ای زمانی تحقق می‌یابد که همه اجزای زیر ثابت شوند.

۱ـ۲. رفتار مجرمانه

در حقـــوق کیفری ایران، در ارتباط با تخریب داده‌های رایانه‌ای، برخی عقیده دارند کـــه رفتارهای مقرر در ماده ۷۳۶ قانون مجازات اســـلامی (تعزیرات) (الحاقی ۱۳۸۸) شـــامل حذف، تخریب، مختل و یا غیر قابل پردازش کردن می‌شود (عالی‌پور، ۱۳۹۵: ۲۱۹). هم‌چنین اظهار شـــده است که رفتار مجرمانه در این مصداق از تخریب کیفریِ رایانه‌ای دربرگیرنده یکی از رفتارهای یاد شـــده است؛ این جرم مقید به نتیجه است و رفتار مرتکب باید به حذف، تخریب، مختل یا غیر قابل پردازش کردن داده‌ها منجر شـــود (حیـــدری، ۱۳۹۶: ۱۳۰-۱۳۱). پذیرش دیدگاه اول موجب می‌شـــود که تخریب داده‌های رایانه‌ای به مثابه جرمی مطلق در نظر گرفته شود؛ چراکه قانون‌گذار غیـــر از آن‌چه نقطه نظر مورد بحث به عنوان رفتـــار مجرمانه تلقی کرده، از نتیجه‌ای سخن نگفته است، اما نظرگاه دوم نیز پذیرفتی نیست؛ به این دلیل که اجزای واحدی که ســـازنده بخشـــی از عنصر مادیِ جرمی باشند، ممکن نیست که هم به عنوان رفتار مجرمانه و هم نتیجه محسوب شوند.

در این میان، باید گفت که حذف، تخریب، مختل و یا غیر قابل پردازش کردن داده‌های رایانه‌ای در واقع امر نتیجه ممنوعه در ماده ۷۳۶ قانون مذکور هســـتند؛ زیرا تحقـــق هر یک از آن‌ها بر اثر رفتارهای مختلفی متصور اســـت. شـــخصی که با دادن فرمانی به سیستم عامل یک رایانه باعث حذف داده‌های ذخیره شده روی آن می‌شود؛ کسی با نصب برنامه‌ای که کرم رایانه‌ای[1] را در یک سامانه رایانه‌ای یا مخابراتی پخش می‌کند، سبب می‌شود که اطلاعات موجود در آن سامانه آسیب ببینند یا از بین بروند؛ فردی که با انتشـــار باکتریوم[2] (نوعی ویروس رایانه‌ای) روی یک حامل داده موجب می‌گـــردد که داده‌های ذخیره شـــده در آن مختل یا غیر قابل پردازش شـــوند؛ ممکن است به خاطر تخریب داده‌های رایانه‌ای تعقیب شود. در این نمونه‌ها، رفتار مجرمانه که به ترتیب دادن فرمان به سیســـتم عامل، نصب برنامه حاوی کرم رایانه‌ای و انتشار

1. Computer worm.
2. Bacterium.

باکتریوم است، از نتیجه حاصله تفکیک‌پذیر می‌باشند.

بر این اســـاس باید پذیرفت هر رفتاری که ســـبب یکی از نتایج ممنوعه مقرر شـــود، به مثابه رفتار مجرمانه در تخریب داده‌های رایانه‌ای به حســـاب می‌آید. چنین رفتاری ممکن اســـت به صورت ایجابی (فعل) یا سلبی (ترک فعل) باشد[۱]. مثال‌هایی که پیش‌تر بیان شدند، انعکاس‌دهنده رفتار مجرمانه از گونه ایجابی هستند، اما نمونه‌ای از رفتار مجرمانه از نوع سلبی دربرگیرنده جایی است که یک مهندس رایانه به موجب قراردادی عهده‌دار نصب سیســـتم عامل و برنامه ضد ویروس روی رایانه‌های شرکت خصوصی‌ای می‌شود، ولی عامدانه از نصب برنامه ضد ویروس روی بعضی از رایانه‌ها خودداری می‌کند و همین ترک فعل باعث مختل یا غیر قابل پردازش شـــدن داده‌های ذخیره شده در آن‌ها می‌شود.

در حقوق کیفری انگلســـتان و ویلز، قســـمت الف بند ۱ ماده ۳ قانون ســـوء اســـتفاده رایانه‌ای ۱۹۹۰ از انجام هرگونه عمل غیر مجازی[۲] در ارتباط با رایانه سخن گفته اســـت؛ لذا رفتار مجرمانه دست‌کاری غیر مجاز داده‌های رایانه‌ای محدود به نوع خاصی از رفتار نیست. اظهار شـــده که جرم ماده ۳ قانون مزبور پیش‌بینی شده است تا شـــامل فعالیت‌های دربرگیرنده ویروس‌های رایانه‌ای، اســـب‌های تراوا و کرم‌های رایانه‌ای، هم‌چنین خرابکاری در وب‌ســـایت‌ها[۳] یا دسترســـی به کانال‌های تلویزیونی کابلی با حق اشـــتراک بدون پرداخت حق عضویت[۴] شـــود. چنین رفتارهایی متفاوت از اعمالی هســـتند که در مواد ۱ و ۲ از قانون بالا به آن‌ها پرداخته شـــده‌اند. در اینجا، جرم پیش‌بینی شده مربوط به اشکالی از خرابکاری الکترونیکی[۵] است که چه‌بسا بدون دسترسی غیر مجاز[۶] که در سایر جرائم لازم است، انجام شود (Fafinski, 2009: 41).

در پرونده لیندزی (۲۰۰۱)[۷] متهم به سه فقره دست‌کاری غیر مجاز در داده‌های

---

۱. بـــرای ملاحظه دیدگاه مخالف، مبنی بر این‌که تحقق جرم تخریب داده‌های رایانه‌ای مســـتلزم این است که رفتار مرتکب به صورت فعل باشد؛ بنگرید به: صالح احمدی، ۱۳۹۸: ۶۳.

2. Any unauthorised act.

3. Interference with websites; See R v. Lindesny [2002] 1 Cr App R (S) 370 (CA).

4. Accessing subscription cable television channels without paying the subscription; See R v. Parr-Moore [2003] 1 Cr App R (S) 425 (CA).

5. Electronic sabotage.

6. Unauthorised access.

7. Lindesay [2001] EWCA Crim 1720.

رایانه‌ای اظهار تقصیر کرد. وی طراح و توسعه‌دهنده مستقلِ نرم‌افزار بود که تجربه و شهرت درخور توجهی داشت. اگر چه او قرارداد کوتاه مدتی با یک شرکت رایانه‌ای منعقد کرده بود، ولی به دلیل این‌که شرکت از کارش راضی نبود، برکنار شد. در خصوص پولی که گفته می‌شد که شرکت به او بدهکار است، اختلاف نظر وجود داشت و در حدود یک ماه بعد، متهم از حساب کاربریِ اینترنتی‌اش برای دسترسی غیر مجاز به سه مشتریِ شرکت رایانه‌ای که با آن اختلاف داشت، استفاده کرد. وی با گذرواژه‌هایی که در زمان کار برای شرکت مورد نظر از آن‌ها استفاده می‌کرد، برخی محتویات وب‌سایت‌های مشتریان را حذف نمود و بعضی از آن‌ها (برای مثال، دستورالعمل‌های وب‌سایت سوپرمارکت) را تغییر داد. متهم هم‌چنین ایمیل‌هایی برای مشتریان این سوپرمارکت ارسال کرد و مدعی شد که قیمت‌ها افزایش پیدا می‌کند. کُل هزینه تصحیح امور نه هزار پوند تخمین زده شد. مرتکب به نه ماه حبس محکوم شد و قاضی دادگاه اظهار به تقصیر او، صراحتش در برابر پلیس و پشیمانی‌اش را در نظر گرفت.

در مقابل، قسمت ابتدایی ماده ۷۳۷ قانون مجازات اسلامی (تعزیرات) ۱۳۷۵ (الحاقی ۱۳۸۸) حکایت از این دارد که رفتار مجرمانه اخلال در سامانه‌های رایانه‌ای یا مخابراتی شامل اَعمالی هم‌چون وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دست‌کاری یا تخریب داده‌ها و یا امواج الکترومغناطیسی یا نوری می‌شود. استفاده از عبارت «از قبیل» پیش از ذکر رفتارهای مورد بحث روشن می‌سازد که همگی آن‌ها جنبه تمثیلی دارند، نه حصری. وجه مشترک اعمال تمثیلی مذکور این است که تمامی آن‌ها با داده‌ها یا امواج الکترومغناطیسی یا نوری[1] پیوند ناگسستنی دارند؛ چراکه داده‌ها یا امواج که پس از ذکر اعمال مورد نظر آمده‌اند، در واقع، به همه آن‌ها برمی‌گردد. به نظر می‌رسد که ویژگی اخیر باید در مورد هر عمل دیگری

---

۱. موج (wave) به حرکت سیگنال گفته می‌شود که در حین طی مسیر از طریق یک وسیله ارتباطی به طور متناوب بالا و پایین می‌رود (Collin, 2004: 262). بر این اساس باید دانست که امواج الکترومغناطیسی (electromagnetic waves) ناظر بر امواج الکترونیکی هستند که به وسیله یک فیلتر الکترواستاتیک و مغناطیس با قدرت گوناگون پخش می‌شود و سرعت آن ۱۸۶/۳۰۰ مایل در ثانیه است (نیوتن، ۱۳۸۷: ۲٤٦)؛ و امواج نوری (light waves) تشعشع الکترومغناطیسی می‌باشند که طیف نوری را پوشش می‌دهند، یعنی طول موجی بین تقریباً ۰/۳ میکرومتر و ۳ میکرومتر (Mazda & Mazda, 1999: 370).

که ممکن اســـت باعث از کار افتادن یا مختل شـــدن کارکرد ســـامانه‌های رایانه‌ای یا مخابراتی شود نیز احراز گردد، به این دلیل که هرچند اعمال مجرمانه پیش‌گفته جنبه تمثیلی دارند، همه آن‌ها در فضای ســـایبری[1] انجام می‌گیرند و لذا اعمال مشـــابه نیز باید همین خصیصه را داشـــته باشـــند؛ وگرنه هر نحو اتلاف یا از کار انداختن اشیای منقول یا غیر منقول دیگری، از جمله ســـامانه‌های رایانه‌ای یا مخابراتی متعلق به غیر که در دنیای واقعی[2] صورت گیرد، زیر عنوان تخریب کیفری ســـاده (ماده ٦٧٧ قانون مجازات اسلامی (تعزیرات) اصلاحی ۱۳۹۹) تعقیب شدنی است.

پیش‌بینی جرم اخلال در ســـامانه‌های رایانه‌ای یا مخابراتی به طور مســـتقل به نوعی مؤید دیدگاه بالَا است؛ زیرا چنین رویکردی حاکی از ویژگی متمایزِ جرم مورد نظر اســـت. از این رو چنان‌چه کسی با دســـت‌کاری باد بزن‌های نصب شده در کنار سخت‌افزارهای یک سامانه رایانه‌ای موجب افزایش حرارت آن‌ها شود؛ به طوری که سامانه رایانه‌ای هم از کار بیفتد، عمل ارتکابی تخریب کیفری ساده محسوب می‌شود؛ به این دلیل که در دنیای واقعی انجام شـــده است، اما کسی که ایمیلی حاوی ویروس اسب تراوا برای دیگری ارسال می‌دارد و زمانی که گیرنده ایمیل آن را مشاهده می‌کند، کارکرد رایانه‌اش مختل می‌شـــود، مرتکب به علت اخلال در ســـامانه‌های رایانه‌ای یا مخابراتی ممکن اســـت تعقیب و محاکمه شود؛ چراکه عمل ارتکابی در فضای سایبر انجام گرفته است.

در هـــر حال، اعمال مجرمانه تمثیلی که در ماده ۷۳۷ قانون مجازات اســـلامی (تعزیرات) الحاقی ۱۳۸۸ آمده‌اند، در زیر توضیح داده می‌شوند:

وارد کـــردن داده‌ها یا امواج الکترومغناطیســـی یا نوری[3] ناظر بر جایی اســـت که اطلاعات برای پردازش یا امواج الکترومغناطیســـی یا نوری به واســـطه یک قطعه الکترونیک یا مغناطیس وارد سامانه رایانه‌ای یا مخابراتی شوند؛ به طوری که پردازش اطلاعات به وسیله سامانه یا انرژی الکترومغناطیسی یا نوری موجب اخلال در سامانه مورد نظر گردد. برای نمونه، شـــخصی که اطلاعاتی ماننـــد برخی اعداد و ارقام را با اســـتفاده از صفحه کلید وارد رایانه رومیزی متعلق به دیگری می‌کند و ســـبب ایجاد

1. Cyber space.
2. Real world.
3. Input of data or electromagnetic/light waves.

اختلال در کارکرد آن می‌شود، دست به ارتکاب این عمل مجرمانه زده است.

انتقـــال دادن داده‌ها یـــا امواج الکترومغناطیســـی یا نوری[1] به معنای ارســـال اطلاعات و یا امواج از یک دســـتگاه به دســـتگاه دیگر یا از یک مکان به مکان دیگر اســـت؛ لذا فرایند انتقال ممکن است در داخل سامانه و یا بین یک دستگاه خارجی و ســـامانه مورد نظر صورت گیرد. عمل مذکور هم‌چنین ارسال اطلاعات روی یک خط ارتباطی یا یک مدار الکترونیکی تعریف شـــده است (Blanton, 2003: 268). برای مثال، فردی که با متصل کردن حافظه پایدارِ[2] ویروســـی شده به رایانه دستی دیگری، داده‌های ویروسی به دیسک سخت آن منتقل می‌کند و در نتیجه موجب از کار افتادن رایانه می‌شـــود، مرتکب رفتار مجرمانه مورد بحث شده است. به همین ترتیب کسی که با استفاده از یک مغناطیس الکتریکی امواج الکترومغناطیسی را به سامانه مخابراتی دیگری منتقل می‌کند، به نحوی که ســـامانه مختل می‌شود، رفتار مجرمانه یاد شده را انجام داده است.

پخش داده‌ها یا امواج الکترومغناطیسی یا نوری[3] عبارت است از انتشار داده‌ها یا امواج الکترومغناطیســـی یا نوری از یک منبع به یک یـــا چند مقصد دیگر. در این رفتار مجرمانه، داده‌ها ممکن اســـت از یک محل انبار داده‌ها[4] روی یک یا چند پایگاه داده[5] پخش شـــوند. چنین کاری باعث اشغال پایگاه داده یا مقصد مورد نظر می‌گردد و در نتیجه کارکرد ســـامانه رایانه‌ای یا مخابراتی مربوط مختل می‌شود؛ بنابراین فردی که یک پایگاه وب را با پخش داده‌ها به نحوی درگیر کند که قسمت اعظم پهنای نوار آن اشـــغال گردد و کاربران اصلی دیگر نتوانند وارد پایگاه شـــوند، مرتکب این رفتار مجرمانه شده است.

حذف کردن داده‌ها یا امواج الکترومغناطیســـی یـــا نوری[6] نوعی تخریب و از بین بُردن داده‌های ذخیره شده و یا امواج الکترومغناطیسی یا نوریِ در جریان در یک سامانه رایانه‌ای یا مخابراتی است؛ اعم از این‌که کلی یا جزئی باشد. این عمل مجرمانه

1. Transmission of data or electromagnetic/light waves.
2. Flash memory.
3. Propagation of data or electromagnetic/light waves.
4. Data warehouse.
5. Database.
6. Deletion of data or electromagnetic/light waves.

احتمال دارد با استفاده از صفحه‌کلیدِ سامانه مورد نظر یا دادن فرمانی به سیستم عامل آن انجام گیرد. از این رو، کسی که با فرمت کردن دیسک سخت نصب شده در رایانه دیگریْ اطلاعات ذخیره شـــده در آن را پـــاک کند و موجب اختلال در کارکرد رایانه شود؛ یا شخصی که با به‌کارگیری یک دستگاه مغناطیس‌زدا امواج الکترومغناطیسیِ در جریان در یک سامانه مخابراتی را خنثی کند؛ به طوری که سامانه از کار بیفتد، دست به رفتار مجرمانه مورد بحث زده است.

متوقـــف کردن داده‌ها یا امواج الکترومغناطیســـی یا نوری[1] یعنی جلوگیری از انتقال و تبادل اطلاعات یا امواج یاد شـــده در ســـامانه رایانه‌ای یـــا مخابراتی. برای نمونه، شخصی برنامه‌ای را روی ســـامانه رایانه‌ای یا مخابراتی دیگری نصب می‌کند کـــه عملکرد اصلـــی آن خاموش کردن ســـامانه در خلال پـــردازش داده‌ها و جریان امواج الکترومغناطیسی است. در این فرض، هرگاه متوقف ساختن داده‌ها یا امواج به صورت مذکور باعث از کار افتادن ســـامانه رایانه‌ای یا مخابراتی و یا ایجاد اختلال در کارکرد آن شود، رفتار مجرمانه مذکور انجام گرفته است.

دســـت‌کاری یا تخریب داده‌ها یا امواج الکترومغناطیســـی یا نوری[2]، هرگونه تغییر، تبدیل، کم و زیاد کردن و یا محو اطلاعات یا امواج اســـت. در این زمینه، یکی از روش‌های مشـــهور، اســـتفاده از برنامه‌های منهدم کننده است که با استفاده از آن‌ها می‌توان در مدت کوتاهی حجم زیادی از داده‌ها را محو کرد. چنین برنامه‌هایی ممکن اســـت از نوع چندکاره، خود ساخته و یا اسب تروا باشـــند که به برنامه‌های اجرایی یا سیســـتم عامل نفوذ می‌کنند (زیبر، ۱۳۹۰: ٤٠ -٤١). افزون بر این، رایانه‌زنی که به طور غیر مجاز وارد شـــبکه رایانه‌ای دیگری می‌شـــود و با تغییر در داده‌های ذخیره شـــده در آن، سبب اختلال در کارکرد شبکه می‌شود، یا نوعی خرابی در جریان امواج الکترومغناطیسی آن ایجاد می‌کند و به این وسیله موجب از کار افتادن شبکه رایانه‌ای می‌شود، مرتکب رفتار مجرمانه مورد بحث شده است.

شـــایان ذکر است که ارتکاب یکی از رفتارهای مجرمانه بالا یا هر عملی که به یکی از نتایج ممنوعه مقرر انجامد، برای تحقق جرمِ اخلال در ســـامانه‌های رایانه‌ای یا

1. Suppression of data or electromagnetic/light waves.
2. Alteration or damage of data or electromagnetic/light waves.

مخابراتی کافی اســـت؛ لذا این جرم مشابه با تخریب داده‌های رایانه‌ای در زمره جرائم ســـاده[1] قرار می‌گیرد؛ ضمن این‌که تحقق جرائم تخریب رایانه‌ای مستلزم تداوم رفتار مجرمانه در زمان نیست، لذا جرائم آنی[2] به شمار می‌آیند. افزون بر این، اگر چه اعمالی مانند حذف یا تخریب داده‌ها در هر دو ماده ۷۳۶ و ۷۳۷ از قانون مجازات اســـلامی (تعزیرات) الحاقی ۱۳۸۸ مورد توجه قـــرار گرفته‌اند، دادرس مجاز به اعمال ضوابط تعدد عنوانیِ جرم نیســـت؛ زیرا در مواردی که مجموع جرائم ارتکابی در قانون عنوان مجرمانه خاصی (اخلال در ســـامانه رایانه‌ای یا مخابراتی) داشته باشد، مقررات تعدد جرم اعمال نمی‌گردد و مرتکب به مجازات مقرر در قانون محکوم می‌شود[3].

۲ـ۲. شرایط پیرامونی

در نظام کیفری ایران، عنصر مادی تخریب کیفری رایانه‌ای زمانی تحقق یافتنی است که شرایط زیر رفتار مجرمانه مرتکب را احاطه کرده باشند:

نخســـت، موضوع تخریب، داده‌های متعلق به دیگری باشـــد (ماده ۷۳۶ قانون مجازات اسلامی (تعزیرات) الحاقی ۱۳۸۸)؛

دوم، مـــکان فعالیتِ خرابکارانه باید ســـامانه‌های رایانه‌ای یـــا مخابراتی و یا حامل‌های داده باشد (ماده ۷۳۶ همان قانون)؛

سوم، موضوع اخلال، سامانه‌های رایانه‌ای یا مخابراتی دیگری است (ماده ۷۳۷ قانون مذکور)؛

چهارم، عمل مرتکب به طور غیر مجاز انجام گرفته باشـــد (مواد ۷۳۶ و ۷۳۷ از قانون بالا).

در خصوص شـــرط نخست باید دانست که به موجب قســـمت ابتدایی ماده ۷۳۶ قانون مجازات اســـلامی (تعزیرات) ۱۳۷۵ (الحاقی ۱۳۸۸)، آن‌چه رفتار مجرمانه تخریب داده‌های رایانه‌ای نســـبت به آن انجام می‌گیرد، همانا داده‌های دیگری است. عبارت اخیر در واقع، متضمن دو جزء اســـت: داده بـــودن و تعلق به غیر. داده‌ها[4] به معنای هر شـــکل از اطلاعات می‌باشـــند که برنامه‌های رایانه‌ای روی آن‌ها پردازش

1. Simple offences.
2. Immediate offences.
۳. بنگرید به: بند د ماده ۱۳٤ قانون مجازات اسلامی ۱۳۹۲ (اصلاحی ۱۳۹۹)
4. Data

می‌کنند. در این مفهوم، داده‌ها ممکن است یک فایل متنی، صوتی، تصویری و یا ترکیبی از آن‌ها باشند (Butterfield and Ekembe Ngondi, 2016: 610). ازاین‌رو، هرگاه کسی با انتخاب گزینه حذف، برخی فایل‌های پی‌دی‌اف متعلق به دیگری که حاوی یادداشت‌های شخصی او هستند و روی تبلت‌اش ذخیره کرده است را پاک کند؛ یا فردی با دادن دستوری به سیستم عاملِ رایانه دستی دیگری، عکس‌ها و فیلم‌های مراسم فارغ‌التحصیلی او از دانشگاه محل تحصیلش را غیر قابل پردازش کند؛ حسب مورد داده‌های متعلق به غیر را حذف و یا غیر قابل پردازش کرده است.

در موارد اخیر، چنان‌چه صاحب داده‌ها نسخه پشتیبان از آن‌ها داشته باشد یا وی بتواند داده‌های حذف یا غیر قابل‌پردازش شده را با استفاده از برنامه‌های رایانه‌ای بازیابی یا بازسازی کند، تأثیری در اصل جرمی که پیش‌تر واقع شده است، ندارد، اما بدیهی است که اگر شخصی اعمال مشابهی را نسبت به داده‌های متعلق به خودش انجام دهد، با توجه به قید دیگری در ماده مذکور، مرتکب جرمی نشده است. ناگفته نماند که قید اخیر در ماده ۷۳۶ قانون مزبور دربرگیرنده هر شخص حقیقی یا حقوقی غیر از مرتکب است. البته تعلق سامانه رایانه‌ای یا مخابراتی و یا حامل داده به دیگری شرط نیست؛ پس اگر کسی حافظه پایداری را از دوست خود به عاریه گرفته، اطلاعاتی روی آن ذخیره کرده باشد و شخص ثالثی اطلاعات ذخیره شده را با انجام عملی حذف یا غیر قابل پردازش کند، بدون این‌که آسیبی به حافظه پایدار وارد آورد، رفتار ارتکابی هم‌چنان بر طبق ماده مذکور تعقیب شدنی است. از این گذشته، هرچند اطلاق عبارت داده‌های دیگری دلالت بر این دارد که داده‌های مورد تخریب اعم از داده‌ها با ارزش مالی نظیر فایل‌های صوتی مربوط به سخنرانی علمی، یا بدون ارزش مالی هم‌چون عکس‌های مستهجن است، ولی در صورتی که ضابطه اصلی برای تشخیص ارزش مالیِ چیزی همانا معیار شرعی باشد (اعتمادی، ۱۴۰۳: ۴۴-۴۷)، حداقل باید پذیرفت که هرگاه صاحب داده‌هایی که به لحاظ شرعی مالیت ندارند، مسلمان باشد، از بین بردن آن‌ها زیر عنوان تخریب داده‌های رایانه‌ای تعقیب شدنی نیست[1]؛ به ویژه از آن رو که حمایت کیفریِ قانون‌گذار ایرانی از چنین

۱. برای ملاحظه دیدگاهی که تمامی داده‌ها شامل داده‌های مستهجنِ دیگری را مشمول ماده ۷۳۶

داده‌های رایانه‌ای امری لغو است و باعث تشویق افراد به نگه‌داری آن‌ها در پرتو ضمانت اجرای کیفری برای تخریب داده‌ها می‌شود. به طور استثنایی، در مواردی که صاحب داده‌های مورد بحث نامسلمان باشد، با توجه به عرف نامسلمانان، می‌توان گفت که مرتکبِ تخریب آن‌ها تعقیب شدنی است.

درباره شرط دوم باید متذکر شد که عبارت از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده‌ها در قسمت ابتدایی ماده ۷۳۶ قانون موردبحث حاکی از این است که فعالیت مجرمانه باید در چنین فضاهایی انجام گیرد. سامانه رایانه‌ای[1] مجموعه‌ای مستقل از تجهیزات رایانه‌ای متشکل از یک رایانه، یا احتمالاً چندین رایانه، همراه با نرم‌افزار وابسته است که برای تأمین نیازهای خاصی طراحی می‌شود (Dain-tith & Wright, 2006: 43)، از قبیل رایانه رومیزی[2]. در واقع، سامانه رایانه‌ای هر پیکربندی است که شامل تمامی اجزای عملیاتیِ رایانه و سخت‌افزار وابسته به آن باشد (Haynes, 2002: 121). دستگاه‌های جنبی مانند مودم[3] نیز در مفهوم سامانه‌های مذکور گنجانده می‌شود؛ زیرا سخت‌افزاری وابسته به رایانه هستند. نرم‌افزار به طور معمول بخشی از سامانه رایانه‌ای تلقی نمی‌شود؛ گر چه سیستم عامل[4] که سخت‌افزار را فعال می‌کند، معروف به نرم‌افزارِ سیستم[5] است، اما سامانه مخابراتی[6] که سیستم ارتباطی نیز خوانده شده، مجموعه‌ای از عنصرهای مرتبط است که روی هم رفته یک کارکرد ارتباطی را انجام می‌دهد (محمدی‌فر، ۱۳۹۱: ۱۲۲)؛ از قبیل تلفن همراه و اینترنت[7]. سامانه‌های یاد شده ترکیبی از سخت‌افزار و نرم‌افزار هستند تا کاربرها

قانون مجازات اسلامی (تعزیرات) الحاقی ۱۳۸۸ می‌داند؛ بنگرید به: عالی‌پور، ۱۳۹۵: ۲۱۹.

1. Computer system

۲. بند ب آیین‌نامه نحوه استفاده از سامانه‌های رایانه‌ای یا مخابراتی ۱۳۹۵ نیز در تعریف سامانه رایانه‌ای اِعلام می‌دارد: «مجموعه‌ای از نرم‌افزارها و سخت‌افزارهای مرتبط که از طریق یک شبکه رایانه‌ای جهت اجرای فرایندهای کار مشخصی، به یکدیگر متصل‌اند».

3. Modem.

4. Operating system.

5. System software.

6. Communications system.

۷. بند پ آیین‌نامه نحوه استفاده از سامانه‌های رایانه‌ای یا مخابراتی ۱۳۹۵ نیز در تعریف سامانه مخابراتی مقرر می‌دارد: «هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله قراردادهایی که برای گیرنده قابل فهم و تفسیر باشد».

بتوانند حسب مورد عملیات رایانه‌ای یا ارتباطی را با آن‌ها انجام دهند. در تبیین مفهوم سامانه‌های اخیر هم‌چنین آمده است که هر سیستمی که از طریق آن منبع اطلاعات قادر باشد که اطلاعات را با رعایت دقیقِ کارآیی و اطمینان پذیری به مقصدی انتقال بدهد؛ چنین سیستمی ممکن است دارای بیش از یک منبع و یا بیش‌تر از یک مقصد باشد که در این صورت، شبکه ارتباطی[1] خوانده می‌شود (Butterfield and Ekem-be Ngondi, 2016: 540). بالاخره، حامل داده[2] هرگونه وسیله‌ای است که داده‌های رایانه‌ای روی آن ذخیره شدنی باشد، هم‌چون انواع لوح‌های فشرده، حافظه‌های پایدار و یا دیسک‌های سخت خارجی که قابلیت حمل نیز دارند.

بر این اساس، هرگاه شخصی با قصد تخریب داده‌ها مبادرت به شکستن یا آتش زدن سخت‌افزار سامانه رایانه‌ای یا مخابراتی دیگری کند، یا حامل داده متعلق به غیر را در آتش بیندازد و یا با ضربه چکش روی آن تکه‌تکه کند، مرتکب تخریب کیفری ساده شده است، نه تخریب کیفریِ رایانه‌ای؛ چراکه مکان فعالیت مجرمانه، دنیای واقعی است، نه فضای داخلیِ سامانه‌های مذکور یا حامل‌های داده. البته، در مواردی که سامانه مورد نظر یا حامل داده متعلق به خود مرتکب و داده‌ها متعلق به دیگری باشد، تخریب کیفری ساده محقق نمی‌شود؛ زیرا اگر قرار باشد که قضیه زیر عنوان جرم اخیر قرار گیرد، رفتار ارتکابی به دلیل تعلق سامانه یا حامل داده به مرتکب تعقیب‌شدنی نیست[3].

در مورد شرط سوم باید خاطر نشان کرد که طبق قسمت میانی ماده ۷۳۷، عمل مجرمانه مرتکب باید روی سامانه‌های رایانه‌ای یا مخابراتی دیگری، اعم از شخص حقیقی یا حقوقی، واقع شود. مفهوم این سامانه‌ها پیش‌تر تبیین شد، ولی در اینجا درخور ذکر است که اگر کسی با ارتکاب عملی موجب از کار افتادن سامانه متعلق به خودش شود، یا کارکرد آن را مختل کند، به علت اخلال در سامانه‌های رایانه‌ای یا مخابراتی، به عنوان مصداقی از تخریب کیفریِ رایانه‌ای، تعقیب و محاکمه نخواهد شد.

در ارتباط با شرط چهارم باید در نظر داشت که مطابق با قسمت ابتدایی مواد

1. Communication network.
2. Data carrier.
۳. بنگرید به: مواد ٦٧٦ و ٦٧٧ از قانون مجازات اسلامی (تعزیرات) ۱۳۷۵

۷۳۶ و ۷۳۷ از قانون مجازات اسلامی (تعزیرات) الحاقی ۱۳۸۸، تحقق عنصر مادی تخریب کیفریِ رایانه‌ای هم‌چنین مستلزم این است که عمل مرتکب به طور غیر مجاز صورت گرفته باشد. اصطلاح اخیر ناظر بر رفتاری است که توسط مالک یا اداره کننده تأیید نگردیده یا مجاز شمرده نشده باشد (Gattiker, 2004: 340). اصطلاح اخیر در ارتباط با جرائمی که مستلزم دسترسی غیر مجاز می‌باشند[1]، هم‌چنین به این معنا آمده است که شخص یا اشخاصی که حق کنترلِ دسترسی به داده‌های مورد نظر را دارند، رضایت یا اجازه استفاده از اطلاعات یا بخشی از آن‌ها را به دیگری نداده باشند[2]. در شرایطی که رضایت یا اجازه استفاده از داده‌ها به طور شفاهی داده شده باشد، گر چه ممکن است از لحاظ اثباتی مشکل آفرین باشد، ولی در صورتی که دادرس آن را احراز کند، می‌باید عمل ارتکابی را مجاز به حساب آورد؛ به ویژه از آن رو که اطلاق عبارت بالا حاکی از این است که کتبی بودنِ اجازه شرط نیست؛ بنابراین هرگاه شخصی رضایت صاحب داده‌ها را برای حذف، تخریب، مختل و یا غیر قابل پردازش کردن داده‌ها، یا اذن صاحب سامانه رایانه‌ای یا مخابراتی را جهت از کار انداختن و یا ایجاد اختلال در کارکرد آن نداشته باشد، عمل ارتکابی‌اش به طور غیر مجاز انجام گرفته است، اما چنان‌چه کسی که درصدد فروش رایانه دستی‌اش برمی‌آید، از دیگری بخواهد که دیسک سخت داخلی آن را فرمت کند، به طوری که بازیابی داده‌های ذخیره شده روی آن دیگر امکان‌پذیر نباشد؛ در صورتی که شخص مورد نظر اقدام به این کار کند، به خاطر تجویز صاحب داده‌ها، مرتکب جرمی نشده است. به همین ترتیب، اگر فردی که می‌خواهد سامانه مخابراتی‌اش را از دور خارج کند، از یک مهندس رایانه درخواست نماید که با دست‌کاری داده‌ها یا امواج الکترومغناطیسی آن، سامانه را از کار بیندازد، در صورتی که مهندس یاد شده مبادرت به چنین عملی کند، رفتار غیر مجاز نبوده؛ چراکه با اذن صاحب سامانه بوده است.

در نظام کیفری انگلستان و ویلز نیز با توجه به قسمت الف بند ۱ ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ شرط است که عمل انجام شده در ارتباط با رایانه غیر مجاز[3] باشد. اصطلاح اخیر در بند ۸ ماده ۱۷ همان قانون تبیین شده است. به موجب

1. Offences of unauthorised access.
2. See, e.g. Clause 1 (3) of the Computer Crime (Scotland) Bill.
3. Unauthorised.

بند مذکور، عملی که در ارتباط با رایانه انجام می‌گیرد، در صورتی غیر مجاز است که شـــخصِ انجام دهنده عمل (یا کسی که سبب انجام آن می‌شود): الف) خودش فردی نباشد که در قبال رایانه مسئولیت دارد و مُحق باشد که تعیین کند، آیا عمل مورد نظر مجاز اســـت که انجام گیرد یا خیر؛ و ب) رضایت نســـبت به عمل مربوط را از چنین شخصی نداشته باشد.

در پرونده دادســـتان کُل علیه لِنون (۲۰۰۶)[1]، دادگاه بخش[2] مقرر داشـــت که جرم ماده ۳ قانون بالا در شرایطی که کارمند سابقِ شرکتی از روی کینه توزی کارکرد رایانَه شرکت مورد نظر را با استفاده از برنامه‌ای جهت ایجاد و ارسال ۵ میلیون ایمیل به شـــرکت مختل کرده، ارتکاب یافته است. دادگاه استدلالِ دفاعی به موجب قسمت ب بند ۸ ماده ۱۷ قانون مذکور، مبنی بر این‌که صاحب رایانه اقدام به دریافت ایمیل‌ها نموده؛ لذا باید فرض شـــود که رضایت به ارسال ایمیل‌ها داشته است را رد کرد؛ زیرا چنین رضایت ضمنی‌ای بدون محدودیت نبوده و این‌که مالک نمی‌توانسته فرض شود که رضایت به ارســـال شـــدن ایمیل‌های متعدد به منظور خراب کردن سامانه رایانه‌ای خود داشته است.

در مواردی که مرتکب اجازه اســـتفاده از رایانه را داشته باشد؛ حتی اگر سوابق رایانه‌ای[3] را به منظور پنهان ساختن فعالیت مجرمانه[4] یا بدنام کننده دیگری تغییر دهد، به دلیل احراز نشـــدن شـــرط مورد بحث، تحقق جرم دست‌کاری غیر مجازِ داده‌های رایانه‌ای زیر ســـؤال می‌رود. در پرونده سینها (۱۹۹۵)[5]، پزشکی در یک مطبَ به قتل غیر عمد[6] و جرم تلاش برای تحریف جریان عدالت[7] متهم شد. بیمار زنِ سی ساله‌ای که از تنگی نفسَ رنج می‌برد، به پزشـــک مراجعه و او دارویی تجویز کرد که موجب حمله کشـــنده تنگی نفس شد. پزشک بعدها ســـوابق رایانه‌ای مرتبط با این بیمار را تغییـــر داد تا ارجاع‌ها به ابتلای بیمار به تنگی نفـــس را حذف کند. اگر چه ارجاع‌ها

1. DPP v Lennon (2006) 170 JP 532.
2. Divisional Court.
3. Computer records.
4. Criminal activity.
5. Sinha [1995] Crim LR 68.
6. Manslaughter.
7. Offence of attempting to pervert the course of justice.

دیگر نمایش داده نمی‌شدند، ولی هم‌چنان امکان بازیابی آن‌ها از دیسک رایانه وجود داشـــت. اتهامی به موجب ماده ۳ قانون سوء اســـتفاده رایانه‌ای ۱۹۹۰ به جریان افتاد، در حالی که پزشـــک اجازه اســـتفاده از رایانه و دسترسی به سوابق بیمارها را داشت. در نتیجه اثبات این‌که آیا دست‌کاری سوابق مورد نظر از جانب پزشک غیر مجاز بود یا خیر، با دشـــواری مواجه می‌شـــد. در این زمینه، اتهام تحریف جریان عدالت بیشتر اطمینان پذیر بود و نسبت به انهدام یا اخفای ادله[1] مصداق داشت.

۳ـ۲. نتیجه جرم

در حقـــوق ایران، تخریب کیفـــریِ رایانه‌ای از جرائم مقید به شـــمار می‌آید؛ چراکـــه از یک طرف، ماده ۷۳۶ قانون مجازات اســـلامی (تعزیرات) الحاقی ۱۳۸۸ بر لزوم حـــذف، تخریب، مختل و یا غیر قابل پردازش کردن داده‌ها از ســـوی مرتکب و از طـــرف دیگر، ماده ۷۳۶ همان قانون بر ضـــرورت از کار انداختن یا مختل کردن سامانه‌های رایانه‌ای یا مخابراتی از جانب شخص تأکید کرده است. مفهوم بیش‌تر این نتایج ممنوعه پیش‌تر به مناسبت تبیین شد، ولی درباره مختل کردن داده‌ها[2] یا غیر قابل پردازش کردن آن‌ها باید گفت که شـــامل هرگونه دست‌کاری خرابکارانه در اطلاعات می‌شود که در امکان پردازش آن‌ها به وسیله سامانه رایانه‌ای یا مخابراتی اختلال ایجاد کند. در این راســـتا، باید توجه داشـــت که پردازش[3] مجموعه‌ای از دستورالعمل‌هایی اســـت که رایانه در سیســـتم عاملِ چند وظیفه‌ای اجرا می‌کند. بسیاری از پردازش‌ها به طور هم زمان اجرا می‌شـــوند و از نظر کاربر، پردازش‌ها ممکن اســـت برنامه‌ها یا بخش‌هایی از برنامه‌ها باشـــند، مانند روال عـــادیِ ویرایش و چاپ در یک واژه پرداز کـــه ممکن اســـت در حین ویرایش چاپ کنـــد (Downing et. al. 2009: 380). به طور مشـــابهی، مختل کردن ســـامانه[4] در بر گیرنده هر نوع از دست‌کاری سایبری در سخت‌افزار یا نرم‌افزارِ ســـامانه رایانه‌ای یا مخابراتی است که باعث ایجاد اختلال در عملکرد آن مثلاً در پردازش یا انتقال داده‌ها شـــود. برای نمونه، حمله‌ها از نوع انکار

1. Destruction or concealment of evidence
2. Data interference
3. Process
4. System interference

خدمات[1] ممکن است سبب مختل شدن سامانه رایانه‌ای شوند. انکار خدمات وضعیتی است که سامانه مورد نظر تعداد زیادی از فرمان (بیش از ظرفیت پردازش) دریافت می‌کند و قادر نیست که به آن‌ها پاسخ دهد. گاهی اوقات در حمله‌های امنیتی به شبکه‌های رایانه‌ای تعداد بسیار زیادی فرمان از چند نقطه مختلف ارسال می‌کنند تا سامانه به حالت انکار خدمات برود و از کار بیفتد (محمدی‌فر، ۱۳۹۱: ۱۸۳). شکل دیگر از حمله‌های انکار خدمات شامل تخریب یا تغییر در اطلاعات پیکربندیِ سرویس دهنده (مانند اطلاعات مسیریابی یا دسترسی غیر مجاز به مؤلفه‌های فیزیکیِ یک سیستم و یا ارسال اطلاعات بسیار بزرگ و نادرست) است که سبب مختل شدن سامانه می‌شود (Blanton, 2003: 79).

از این رو، هرگاه کسی با ورود به سامانه رایانه‌ای یا مخابراتی دیگری و نصب برنامه‌ای در سامانه مذکور درصدد برآید که داده‌های متعلق به غیر را از بین ببرد، ولی درست در زمانی که می‌خواهد برنامه نصب‌شده را اجرا کند، صاحب داده‌ها مانع او شود؛ یا شخصی دیسک سخت خارجی که حاوی ویروس‌های رایانه‌ای است را به رایانه رومیزی متعلق به دیگری متصل کند تا ویروس‌ها را به رایانه او انتقال بدهد و به این وسیله، کارکرد آن را مختل نماید، اما پیش از آن‌که بتواند برنامه ضد ویروس رایانه موردنظر را غیر فعال کند تا امکان انتقال ویروس‌ها میسر شود، قطع برق مانع از ادامه عملیات مجرمانه‌اش گردد؛ وی به خاطر هیچ یک از مصادیق تخریب کیفریِ رایانه‌ای تعقیب و محاکمه نخواهد شد، به این دلیل که هنوز نتیجه موردنظر تحقق نیافته است. از لحاظ نظری، مرتکب در این فرض‌ها در مرحله شروع به جرم قرار دارد، ولی با توجه به اصل قانونی بودن جرائم و مجازات‌ها و این‌که ماده ۱۲۲ قانون مجازات اسلامی ۱۳۹۲ شروع به جرم را در جرائمی که مجازات قانونی آن‌ها حبس تعزیری درجه یک تا پنج باشد، مستوجب کیفر دانسته است، در حالی که مجازات قانونی تخریب کیفریِ رایانه‌ای تعزیر درجه شش به حساب می‌آید، شروع به تخریب کیفریِ رایانه‌ای[2] مجازات شدنی نیست.

در حقوق انگلستان و وِیلز نیز در بحث از جرمِ دست‌کاری غیر مجازِ داده‌های

1. Denial of service (DoS)
2. Attempted computer criminal damage.

رایانه‌ای از اصطلاحِ اخلال[1] یاد می‌شـــود و عنوان اصلاح شـــده‌ای هم که قانون‌گذار انگلیســـی و ویلزیِ برای ماده ۳ قانون سوء اســـتفاده رایانه‌ای ۱۹۹۰ برگزیده است، همان‌طور که پیش‌تر اشـــاره شـــد، اعمال غیر مجاز با قصد اخلال در کارکرد رایانه و غیره یا بی‌پروایی در خصوص اخلال آن است، اما اصطلاح مذکور تعریف نشده است و از قـــرار معلوم، معنای معمولِ خود را دارد. افـــزون بر این، برخی نگرانی‌ها درباره این‌که اصطلاح مزبور ممکن اســـت به طور گســـترده اعمال شود، ابراز شده است؛ به ویژه از آن رو که اخلال چه‌بسا موقتی باشد[2]. برای مثال، گروه‌های اعتراضِ سایبری[3] گاهی اوقات درصدد بستن وب‌سایت‌ها برای مدت کوتاهی برمی‌آیند. در مواردی که چنین معترضانی به ســـادگی با استفاده از مرورگرهای استاندارد وارد صفحه‌های وِب می‌شـــوند، خطرهای درخور توجهی در ایجاد چارچوبی برای جرم‌انگاری رفتارشان وجـــود دارد (Clough, 2010: 115). بـــا وجـــود این، جرمِ دســـت‌کاری غیر مجازِ داده‌هـــای رایانه‌ای از جرائم مطلق[4] به حســـاب می‌آید؛ به این دلیـــل که مفاد ماده ۳ قانون بالا، به ویژه بندهای ۱ تا ۳ آن، حاکی از این اســـت که تحقق عملیِ آن‌چه متهم قصد می‌کند یا در خصوص آن بی‌پروا اســـت، لازم نیست. به عبارت دیگر، ضرورتی ندارد که اخلال در کارکرد رایانه و غیره در عمل محقق شود و همین‌که متهم با قصد یا بی‌پروایی لازم اقدام کند، کافی خواهد بود. آن‌چه این دیدگاه را تقویت می‌کند، این اســـت که در عنوان‌گذاری ماده مورد بحث بر قصد اخلال در کارکرد رایانه و غیره یا بی‌پروایی در خصوص اخلال آن تأکید شده است، نه تحقق عملی آن.

۳. عنصر روانی تخریب کیفری رایانه‌ای

در ایـــران، اگر چه مـــواد ۷۳۶ و ۷۳۷ از قانون مجازات اســـلامی (تعزیرات) الحاقی ۱۳۸۸ از عنصر روانی جرائم پیش‌بینی شـــده در آن‌ها سخن نگفته‌اند، با توجه به اصل عمدی بودن جرائم باید دانســـت که تخریب کیفریِ رایانه‌ای در زمره جرائم عمدی قرار می‌گیرد. به موجب ماده ١٤٤ قانون مجازات اسلامی ۱۳۹۲، عنصر روانی

1. Impairment.

۲. شـــایان ذکر اســـت که به موجب قسمت (پ) بند (۵) ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ م. مختـــل کردن، جلوگیری از چیزی و یا به تأخیر انداختن آن در قانون مذکور دربرگیرنده انجام آن به طور موقت می‌شود.

3. Cyber-protest groups.

4. Conduct offences.

این جرم مشتمل بر دو جزء قصد عام و قصد خاص است. احراز قصد عام در تخریب کیفریِ رایانه‌ای مستلزم اثبات این است که مرتکب با علم به شرایط پیرامونی در ارتکاب رفتار مجرمانه‌اش عمد داشته باشد؛ بنابراین هرگاه دو نفر دانشجو اطلاعات تحقیقاتی خود را روی رایانه رومیزی موجود در اتاق خوابگاهشان ذخیره کرده باشند، ولی یکی از آن‌ها به اشتباه اطلاعات دیگری را متعلق به خودش قلمداد و حذف کند؛ فردی رایانه دستی‌اش را برای تعویض سیستم عامل به کسی بدهد که خدمات رایانه‌ای ارائه می‌کند و شخص مورد نظر بدون پشتیبان گرفتن از داده‌های ذخیره شده روی قسمتی از دیسک سخت داخلی رایانه که سیستم عاملِ پیشین روی آن نصب بوده است، مبادرت به فرمت کردن قسمت مربوط کند؛ در حالی که تصور می‌کرده که صاحب رایانه نسبت به این کار برای تعویض سیستم عامل رضایت داشته است؛ حسب مورد به دلیل نداشتن علم به موضوع تخریب یا غیر مجاز بودن عمل ارتکابی‌اش، قصد عامِ مرتکب احراز نمی‌شود.

در مقابل، قصَد خاص در تخریب کیفریِ رایانه‌ای عبارت است از قصد حذف، تخریب، مختل و یا غیر قابل پردازش کردن داده‌ها (در جرم تخریب داده‌های رایانه‌ای) و قصد از کار انداختن یا مختل کردن کارکرد سامانه‌های رایانه‌ای یا مخابراتی (در جرم اخلال در سامانه‌های رایانه‌ای یا مخابراتی). بر این اساس چنان‌چه یک مهندس کامپیوتر عهده‌دار پارتیشن بندی (قسمت بندی)[1] دیسک سخت داخلی بعضی از رایانه‌های شرکتی خصوصی و نصب برنامه‌های کاربردی روی آن‌ها، هم‌چنین عیب‌یابی برخی رایانه‌های دیگر در آن شرکت شده باشد، اما در جریان انجام پارتیشن بندی برحسب اتفاق باعث مختل یا غیر قابل پردازش شدن بعضی از داده‌های ذخیره شده روی دیسک سخت داخلیِ رایانه‌ها گردد، یا در حین عیب‌یابی رایانه‌های دیگر از روی سهل‌انگاری موجب ایجادِ اختلال در کارکرد آن‌ها شود، قصد خاص او ثابت نمی‌شود؛ چراکه به ترتیب قصد پارتیشن بندی دیسک سخت داخلی و یا عیب‌یابی رایانه‌ها را داشته است، نه قصد خاص به شرح بالا. بدیهی است که اگر مهندس مذکور علم به وقوع نتیجه داشته باشد، هم‌چنان قصد خاص او احراز

۱. پارتیشن (Partition) قسمتی از دیسک است که برای راحتی کاربربه وسیله سیستم عامل به عنوان دیسک مستقل تعریف و نام‌گذاری می‌شود. برای نمونه، یک دیسک ۵۰۰ گیگابایتی ممکن است به دو پارتیشن ۲۵۰ گیگابایتی به نام‌های C و D تقسیم و نام‌گذاری شود.

شدنی است.

در انگلستان و ویلز، به موجب قسمت ب بند ۱ ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ مرتکب در زمان ارتکاب عمدیِ رفتار مجرمانه‌اش باید آگاه باشد که عملش غیر مجاز است و قصد خاص یا بی‌پروایی او در چارچوب بندهای ۲ و ۳ از ماده یاد شده احراز گردد. توضیح بیش‌تر این‌که طبق بند ۲ ماده مورد بحث، مرتکب باید قصد خاص هم‌چون قصد اخلال‌گری در کارکرد رایانه، ایجاد مانع برای دسترسی به هرگونه برنامه یا داده نگه داشته شده در رایانه و یا مختل ساختن عملکرد هرگونه از این‌چنین برنامه‌ای یا اطمینان پذیریِ هرگونه از چنین داده‌ای را داشته باشد؛ بنابراین، ارسال داده‌های صحیح ممکن نیست بر اطمینان پذیریِ هرگونه داده نگه داشته شده در رایانه تأثیر بگذارد، اما هرگاه داده‌ها ناصحیح باشند، چنین تأثیری خواهند داشت. چنان‌چه هرگونه نادرستی در نتیجه اشتباه صادقانه از جانب فرستنده باشد، آنگاه، هرچند اطمینان پذیری داده‌ها ممکن است مختل شود، ارسال کننده داده‌ها نمی‌تواند از قصد لازم برای تأثیرگذاری بر اطمینان پذیری داده‌ها برخوردار باشد. در واقع، حتی اگر اطمینان پذیری داده‌ها[1] تحت تأثیر قرار گیرد، کارکرد رایانه مختل شود و یا دسترسی به برنامه‌ها یا داده‌ها مورد ممانعت یا تأخیر قرار گیرد، دادستان هم‌چنان باید عنصر روانیِ لازم را اثبات کند و بی‌دقتی کافی نیست. در مواردی که دست‌کاری به شکل ویروس، بمب زمانی[2] و یا بمب منطقی[3] باشد، استنباط قصد لازم ممکن است به راحتی صورت گیرد، مشروط بر این‌که بتوان ثابت کرد که متهم آن را از روی

1. Reliability of data

۲. بمب زمانی (Time-bomb) برنامه مخربی است که به نحوی طراحی شده است تا در زمان خاصی منفجر شود و ویروسی را در سامانه یا شبکه رایانه منتشر کند؛ بنگرید به: HIMSS, 2019: 199.

۳. بمب منطقی (Logic-bomb) که بمب خوشه‌ای (Fork bobd) هم نامیده می‌شود، برنامه یا قسمتی از آن است که موجب راه‌اندازی نرم‌افزار کاربری یا سیستم عامل در زمانی می‌شود که رویداد منطقیِ خاصی واقع گردد. برنامه مورد نظر ممکن است به کار گرفته شود تا رونوشت‌هایی از خودش را به‌طور بازگشتی به وجود آورد و به این وسیله، در نهایت همه ورودی‌های جدول فرایند را نابود و به طور مؤثر سامانه مربوط را قفل کند. تاریخ معین، ترکیب کلیدی و یا شمارگر داخلی از متداول‌ترین عامل‌هایی هستند که تأثیرهایی را ایجاد می‌کنند؛ از نمایشگرهای روی صفحه گرفته تا مسدودسازی سامانه یا حذف فایل‌ها و برنامه‌ها. برای مثال، برنامه مذکور ممکن است هر روز در ساعت ۱۷ پیامی را به ده آدرس از پایگاه داده آدرسِ ایمیل شخص ارسال کند؛ برای مطالعه بیش‌تر، بنگرید به: Gattiker, 2004: 198.

عمد در رایانه قرار داده اســت. پس شــخصی که از روی بی‌توجهی[1] پیوست ایمیل حاوی ویروس را بدون اطلاع از وجود آن بازفرست می‌کند، قصدش احراز نمی‌گردد (Bainbridge, 2004: 397). در دسامبر ۱۹۹۳ پرستاری رایانه یک بیمارستان را هک کرد و نســخه‌های دارویی بیماران را به نحوی تغییر داد که به طور بالقوه کشنده بود. وی به خاطر دو جرم طبق ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ مقصر شناخته و به دوازده ماه حبس محکوم شد. احتمال داشت که اتهام شروع به قتل عمد[2] و یا قتل غیر عمد در چنین شــرایطی مناسب باشد، ولی اثبات قصد لازم[3] دشوار بود، در حالی که قصد در جرم ماده مزبور تنها باید به ســمت رایانه یا برنامه‌ها و یا داده‌های ذخیره شــده در آن هدایت شده باشــد (Bainbridge, 2004: 398)، اما در صورتی‌که قصد خاص به شــرح مذکور احراز نگردد، به موجب بند ۳ مــاده ۳ قانون بالا، بی‌پروایی دربــاره این‌که آیا عمل مورد نظر باعث هــر یک از موارد مندرج در بند ۲ همان ماده می‌شود یا خیر، کافی خواهد بود. البته قصد یا بی‌پروایی به شرح مقرر در بندهای ۲ و ۳ از ماده ۳ قانون مزبور لازم نیســت مرتبط با رایانه خاص، برنامه یا داده معینی و یا برنامه یا داده‌ای از هر نوع خاص باشد. در پرونده ززف و یاریماکا علیه رئیس زندان علیاحضرت بریکستون (۲۰۰۲)[4] مقرر شد که جرم ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ در جایی که متهم ایمیل ساختگی را روی فایل‌های رایانه شخص دیگری قرار داده، ایمیلی که به ظاهر از طرف شــخصی آمده که آن را ارسال نکرده، ارتکاب یافته است. لازم نیست ثابت شود که متهم هرگونه رایانه، برنامه یا داده خاصی را آماج قرار داده اســت. در چنین شرایطی، اطمینان پذیری رایانه مختل می‌گردد؛ زیرا که از رایانه برای ثبت اطلاعات به این عنوان که از شــخص معینی نشأت یافته، استفاده شده، در حالی که در واقع امر از شخص دیگری سرچشمه می‌گرفته است.

پرونده اخیر تبیین کننده اصطلاح اطمینان پذیری[5] در قســمت پ بند ۲ ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ نیز هست. بر این اساس، هرگاه رایانه اطلاعاتی را

1. Inadvertently.
2. Attempted murder.
3. Required intention.
4. Zezev and Yarimaka v Governor of HM [Her Majesty's] Prison Brixton [2002] 2 Cr App R 515.
5. Reliability.

ثبت کند که نشان می‌دهد که از جانب شخصی آمده است؛ در حالی که در واقع امر از طرف شخص دیگری آمده باشد، به وضوح اطمینان پذیری آن تحت تأثیر قرار گرفته است. قرار دادن ایمیل ساختگی در فایل‌های رایانه، چیزِ اضافه شده غیر مجازی به داده‌ها است که اطمینان پذیری آن‌ها را مختل می‌کند.

٤. مجازات تخریب کیفری رایانه‌ای

در حقوق کیفری ایران، به موجب قسمت انتهایی مواد ۷۳٦ و ۷۳۷ از قانون مجازات اسلامی (تعزیرات) ۱۳۷۵ (الحاقی ۱۳۸۸)، هر کس مرتکب تخریب کیفریِ رایانه‌ای، اعم از تخریب داده‌های رایانه‌ای یا اخلال در سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از شش ماه تا دو سال یا هشتاد و دو میلیون و پانصد هزار ریال تا سیصد و سی میلیون ریال یا هر دو مجازات محکوم خواهد شد. با توجه به ماده ۱۹ قانون مجازات اسلامی ۱۳۹۲ و با ملاک قرار دادن کیفر حبس در مواد یاد شده باید دانست که مجازات تعزیری مقرر برای جرائم تخریب رایانه‌ای تعزیر درجه شش محسوب می‌شود. افزون بر این، استفاده از حرف ربط یا در میان مجازات‌های پیش‌بینی شده حاکی از این است که قاضی دادگاه از صلاح‌دید تعیین کیفر و نیز تحمیل یک مجازات یا هر دو مجازات در چارچوب حداقل و حداکثر مقرر با لحاظ ضوابط قانونی و اوضاع و احوال پرونده برخوردار است، اما در شرایطی که کسی با قصد به خطر انداختن امنیت، آسایش و امنیت عمومی مرتکب جرائم مذکور در مواد ۷۳٦ و ۷۳۷ از قانون پیش گفته علیه سامانه‌های رایانه‌ای و مخابراتی شود که برای ارائه خدمات ضروریِ عمومی، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری به کار می‌روند، طبق ماده ۷۳۹ قانون مجازات اسلامی (تعزیرات) الحاقی ۱۳۸۸ به حبس از سه تا ده سال (تعزیر درجه چهار) محکوم می‌شود. عبارت از قبیل در ماده اخیر روشن می‌سازد که خدمات ضروریِ عمومی که برشمرده شده‌اند، جنبه تمثیلی دارند، لذا اخلال در سامانه‌های رایانه‌ای و مخابراتی مربوط به شبکه‌های فاضلاب، آتش‌نشانی و یا مراکز دانشگاهی نیز تحت شمول قرار می‌گیرند.

در هر حال، از آنجا که اخلال در سامانه‌های رایانه‌ای و مخابراتیِ ارائه دهنده خدمات ضروریِ عمومی با قصد خاص به شرح پیش گفته جرمی امنیتی به شمار

می‌آیـــد، دادرس بایـــد محدودیت‌ها و ممنوعیت مرتبط با جرائم علیه امنیت کشـــور را در خصـــوص آن در نظـــر گیرد کـــه از جمله آن‌ها می‌توان بـــه محدودیت تعلیق اجرای مجازات و ممنوعیت تعویق صدور حکم در چارچوب ماده ٤٧ قانون مجازات اسلامی ۱۳۹۲ (اصلاحی ۱۳۹۹)[1] اشاره کرد.

در حقوق کیفری انگلستان و وِیلز، مجازات دست‌کاری غیر مجاز در داده‌های رایانه‌ای در بند ٦ ماده ۳ قانون ســـوء اســـتفاده رایانه‌ای ۱۹۹۰ پیش‌بینی شـــده است. مطابق با این بند، شخصی که به خاطر جرم یاد شده مجرم شناخته شود، در محکومیت اختصاری مشـــمول حبس برای مدتی که متجاوز از دوازده ماه نباشد، یا جزای نقدی که از حداکثر قانونی بیش‌تر نشـــود و یا هر دو مجازات می‌شـــود، اما در محکومیت برحســـب کیفرخواست متحمل حبس برای مدتی که از ده سال تجاوز نکند، یا جزای نقدی و یا هر دو مجازات خواهد شـــد. این مطلب روشن می‌سازد که جرم بالا از دو جهت محاکمه شدنی است.

در پرونـــده گولدِن (۱۹۹۲)[2] به عنوان نخســـتین تعقیب کیفـــریِ اصلی که به موجـــب ماده ۳ قانون مذکور به جریان افتاد، متهم بســـته نرم‌افزاریِ امنیتی‌ای را روی ایستگاه کاریِ اَپِل[3] برای یک شرکت چاپ به نام اَمپرسَند[4] نصب کرد. این بسته شامل تسهیلاتی برای جلوگیری از دسترسی بدون استفاده از رمز عبور[5] می‌شد. متهم از این تسهیلات به منزله بخشی از ادعای خود برای هزینه‌هایی به مبلغ ۲/۲۷۵ پوند استفاده کرد. شرکت اَمپرسَند در نتیجه ماهیت رایانه‌ای شده عملیات چاپ خود نتوانست برای مدت چند روز کار کند. شـــرکت مذکور ادعا کرد که سی و شش هزار پوند کسب و کارش، ازجمله هزار پوند برای متخصصی جهت لغو حفاظت از دسترسی را به خاطر اقدام‌های متهم از دســـت داده است. دادگاه آزادی مشـــروط[6] دوساله و ۱/٦٥۰ پوند جزای نقدی برای متهم تعیین کرد. قاضی دادگاه در اظهار نظر تعجب برانگیزی اظهار داشت که اقدام‌های متهم در پایین‌ترین حد از شدت بوده است!

---

۱. بنگرید به: ماده ۷ قانون کاهش مجازات حبس تعزیری ۱۳۹۹.

2. Goulden (1992) The Times, 10 June 1992.

3. Apple workstation.

4. Ampersand.

5. Access without use of a password.

6. Conditional discharge.

ناگفتـــه نماند که بـــه موجب قانون جرم شـــدید ۲۰۱۵ [1] بعضی از مقرره‌های قانون ســـوء استفاده رایانه‌ای ۱۹۹۰ اصلاح شده و برخی مواد قانونی نیز به آن الحاق گردیده‌انـــد. یکی از این موارد، ایجاد جرمی اســـت که از آن زیـــر عنوان اعمال غیر مجازی که موجب خســـارت شدید می‌شـــوند یا خطر آن را ایجاد می‌کنند[2] یاد شده است[3]. جرم مورد بحث که با انجام هرگونه عمل غیر مجاز در ارتباط با رایانه ارتکاب می‌یابد[4]، در مواردی که باعث خسارت شدید به امنیت ملی[5] یا رفاه بشری[6] به صورت ایراد لطمه به حیات انســـان[7] و یا بیماری یا صدمه آدمی[8] شود، یا خطر درخور توجه آن را به وجود آورد، در محکومیت برحسب کیفرخواست ممکن است مجازات حبس ابد را در پی داشـــته باشد[9]؛ این در حالی اســـت که هرگاه خسارت به محیط‌زیست[10] یـــا اقتصاد[11] وارد آید، یا خطر درخور توجـــه آن ایجاد گردد، حداکثر مجازات حبس در همان نوع از محکومیت متجاوز از چهارده ســـال نخواهـــد بود[12]. البته قصد ایراد خسارت شدید به یکی از شکل‌های مذکور یا بی‌پروایی در مورد این‌که چنین خسارت وارد می‌آید یا خیر، باید احراز شود[13].

1. Serious Crime Act 2015.
2. Unauthorised acts causing, or creating risk of, serious damage.
3. See SZA of the Computer Misuse Act 1990, inserted by s 41 of the Serious Crime Act 2015.
4. SZA (1) (a) of the Computer Misuse Act 1990.
5. National security.
6. Human welfare.
7. Loss to human life.
8. Human illness or injury.
9. SZA (7) of the Computer Misuse Act 1990.
10. Damage to the environment.
11. Damage to the economy.
12. SZA (6) of the Computer Misuse Act 1990.
13. SZA (1) (d) of the Computer Misuse Act 1990. For further reading, See Rowland, et al. 2017: 304.

برآمد

۱ـ بررسی عنصرهای سازنده تخریب کیفری رایانه‌ای در نظام‌های حقوقی ایران، انگلستان و ویلز حکایت از آن دارد که با وجود جرم‌انگاری این عمل از سوی قانون‌گذار، برخی نقص‌ها در رویکرد اتخاذی در راستای مقابله با تخریب‌گران رایانه‌ای یافت می‌شوند که تلاش برای رفع آن‌ها، به ویژه در جهت صدور آرای کیفری منسجم، تأثیر مطلوبی خواهد داشت. بر این اساس قانون‌گذار ایران لازم است در قوانین مربوط به موضوع بازنگری کند.

۲ـ قانون‌گذار ایرانی در تخریب داده‌های رایانه‌ای تنها از حذف، تخریب، مختل و یا غیر قابل پردازش کردن داده‌های رایانه‌ای سخن گفته است. با توجه به این‌که تحقق هر یک موارد یاد شده به واسطه رفتارهای گوناگونی متصور است، مناسب بود که قانون‌گذار، همانند آن‌چه در عنصر قانونی اخلال در سامانه‌های رایانه‌ای یا مخابراتی پیش‌بینی کرده است، مقرره مربوط را به نحوی وضع می‌کرد که باعث اختلاف در تلقی حقوق‌دانان و قضات از تخریب داده‌های رایانه‌ای به مثابه جرمی مقید یا جرمی مطلق نشود. ناگفته پیدا است که این امر صرفاً یک بحث نظری نیست؛ چراکه اثبات اجزای سازنده عنصر مادی جرائم مطلق و به تبع آن، صدور حکم محکومیت در این جرائم مطلق؛ به دلیل عدم لزوم احراز جزء نتیجه، آسان‌تر است.

۳ـ لحن قانون‌گذار در مقررات کنونی، به ویژه تأکید بر برخی اصطلاح‌های رایانه‌ای متداول، موجب می‌شود که صدور رأی در خصوص اعمال ارتکابی در حوزه فناوری‌های نوین با دشواری مواجه شود. برای نمونه، امروزه اینترنت اشیا[1] با سرعت در حال رشد است و ممکن است بعضی از دستگاه‌های خانگی از قبیل تلویزیون و دوربین‌های امنیتی، در معرض حمله سایبری قرار گیرند و تخریب داده‌ها یا اختلال در سامانه‌های رایانه‌ای را در پی داشته باشند. در این موارد، مقررات کنونی که عمدتاً بر تخریب داده‌ها روی رایانه‌ها و یا سرورها تمرکز دارند، به طور کامل شامل این نوع از تهدیدها نمی‌شوند. به همین ترتیب، تأکید بر حامل‌های داده (و به خصوص قابلیت حمل وسیله مورد نظر) دربرگیرنده فضای ذخیره‌سازی ابری[2] نیست. از این

1. Internet of Things (IoT)
2. Cloud Data Storage

رو، گنجاندن مسائل جدید مرتبط با فناوری‌های نوین در مقررات مربوط به تخریب کیفری رایانه‌ای ضروری است.

٤ـ در حقوق انگلستان و وِیلز، بی‌پروایی نوعی از حالت ذهنی است که در مرز بین تقصیر جزایی و قصد مجرمانه در حقوق ایران قرار گرفته است. ایده ورای بی‌پروایی این است که متهم خطر صدمه (نتیجه ممنوعه) را پیش‌بینی کرده و با این حال، پیش رفته و تن به آن داده است؛ این در حالی است که در حقوق ایران چنین حالت ذهنی‌ای به رسمیت شناخته شده است. در راستای مقابله مؤثرتر با مرتکبان تخریب کیفریِ رایانه‌ای، لازم است در خصوص جرمِ دست‌کاری غیر مجازِ داده‌های رایانه‌ای، قانون‌گذار ایرانی نیز حالت ذهنی پیش گفته را به طور مستقل در قانون منعکس سازد.

۵ـ با در نظر گرفتن این‌که حدود دو سوم از مفاد عنصر قانونی جرائم تخریب داده‌های رایانه‌ای و اخلال در سامانه‌های رایانه‌ای یا مخابراتی یکی است؛ از جمله این‌که نوع و میزان مجازات‌های مقرر برای آن‌ها کاملاً یکسان پیش‌بینی شده است، قانون‌گذار ایرانی در راستای جلوگیری از تورم مواد قانون کیفری می‌تواند دو ماده ۷۳٦ و ۷۳۷ قانون مجازات اسلامی (تعزیرات) الحاقی ۱۳۸۸ را ادغام کند. چنین رویکردی در جرم ماده ۳ قانون سوء استفاده رایانه‌ای ۱۹۹۰ (در نظام کیفری انگلستان و وِیلز) جلوه‌گر شده است؛ هر چند که از حیث قلمرو شمول محدود و دارای نقص است. افزون بر این، عبارت «قصد به خطر انداختن امنیت، آسایش و امنیت عمومی» که در ماده ۷۳۹ همان قانون به منزله عامل مشدده جرائم پیش‌گفته به کار رفته است، از لحاظ نگارشی مناسب نیست و لازم است با عبارتی مانند «قصد به خطر انداختن امنیت و آسایش عمومی» جایگزین شود.

فهرست منابع

الف. فارسی

* اعتمادی، امیر (۱۴۰۳)، **حقوق کیفری اختصاصی، جرائم مالی**، جلد دوم: سرقت، چاپ دوم، تهران: میزان.

* حیدری، علی‌مراد (۱۳۹۶)، **جرائم علیه اموال و مالکیت**، چاپ نخست، قم: دانشگاه حضرت معصومه.

* زیبر، اولریش (۱۳۹۰)، **جرائم رایانه‌ای**، برگردان: محمدعلی نوری و دیگران، چاپ دوم، تهران: گنج دانش.

* صالح احمدی، سحر (۱۳۹۸)، **جرائم رایانه‌ای در نظم حقوقی کنونی**، چاپ نخست، تهران: کتاب آوا.

* عالی‌پور، حسن (۱۳۹۵)، **حقوق کیفری فناوری اطلاعات**، چاپ چهارم، تهران: خرسندی.

* محمدی‌فر، محمدرضا (۱۳۹۱)، **فرهنگ فناوری اطلاعات و ارتباطات**، چاپ نخست، تهران: فرهنگ معاصر

* نیوتن، هری (۱۳۸۷)، **فرهنگ تشریحی مخابرات، فیبر نوری و بی‌سیم**، برگردان: محمدحسن مهدوی، چاپ دوم، تهران: خانه نشر هزاره

* هِرینگ، جاناتان (۱۴۰۳)، **مقدمات حقوق کیفری**، برگردان: امیر اعتمادی، چاپ نخست، تهران: میزان

ب. انگلیسی

* Bainbridge, David (2004), **Introduction to Computer Law**, Fifth Edition, Harlow, Pearson Education Limited.

* Blanton, Alex (Ed) (2003), **Microsoft Internet & Networking Dictionary**, Washington, Microsoft Press

* Butterfield, Andrew and Ekembe Ngondi, Gerard (Eds) (2016), **A Dictionary of Computer Science**, Seventh Edition, Oxford, Oxford University Press.

* Collin, S.M.H. (2004), **Dictionary of ICT**, Fourth Edition, London,

Bloomsbury Publishing Plc.

❋ Clough, Jonathan (2010), **Principles of Cybercrime**, New York, Cambridge University Press, First Published.

❋ Daintith, John and Wright, Edmund (2006), **The Facts On File Dictionary of Computer Science**, Revised Edition, New York, Facts On File, Inc.

❋ Downing, Douglas A. et. al. (2009), **Dictionary of Computer and Internet Terms**, Tenth Edition, Hauppauge, Barron's Educational Series, Inc.

❋ Fafinski, Stefan (2009), **Computer Misuse: Response, Regulation and the Law**, Devon, Willan Publishing, First Published.

❋ Gattiker, Urs E. (2004), **The Information Security Dictionary**, Boston, Kluwer Academic Publishers.

❋ Haynes, Sandra (Ed) (2002), **Microsoft Computer Dictionary**, Fifth Edition, Washington, Microsoft Press.

❋ Hildebrandt, Mi.reille (2020), **Law for Computer Scientists and Other Folk**, First Edition, Oxford, Oxford University Press

❋ HIMSS (2019), **HIMSS Dictionary of Health Information and Technology Terms, Acronyms and Organizations**, Fifth Edition, Boca Raton, CRC Press.

❋ Mazda, Xerxes C. and Mazda, Fraidoon F. (1999), **The Focal Illustrated Dictionary of Telecommunications**, Oxford, Focal Press, First Published.

❋ Reed, Chris (Ed) (2011), **Computer Law**, Seventh Edition, Oxford, Oxford University Press.

❋ Rowland, Diane et al. (2017), **Information Technology Law**, Fifth Edition, London, Routledge.

❋ Wild, Charles and Weinstein, Stuart (2013), **Smith & Keenan's**

English Law: Text and Cases, Seventeenth Edition, Harlow, Pearson Education Limited.

- Cases

❋ DPP v Lennon (2006) 170 JP 532.

❋ Goulden (1992) The Times, 10 June 1992.

❋ Lindesay [2001] EWCA Crim 1720.

❋ R v. Lindesny [2002] 1 Cr App R (S) 370 (CA).

❋ R v. Parr-Moore [2003] 1 Cr App R (S) 425 (CA).

❋ Sinha [1995] Crim LR 68.

❋ Whiteley (1991) 93 Cr App R 381.

❋ Zezev and Yarimaka v Governor of HM [Her Majesty's] Prison Brixton [2002] 2 Cr App R 515.