به نام خدا

سیاست کیفری حاکم بر جرایم سایبری
با چشم‌انداز کیفرشناسی

مولف :

محسن صفاری فرد خوزانی

کارشناس حقوق

انتشارات ارسطو
(چاپ و نشر ایران)
۱۳۹۹

سرشناسه : صفاری‌فرد خوزانی، محسن، ۱۳۵۶-
عنوان و نام پدیدآور : سیاست کیفری حاکم بر جرایم سایبری با چشم انداز کیفر شناسی /مولف محسن صفاری‌فردخوزانی.
مشخصات نشر : مشهد: ارسطو، ۱۳۹۹.
مشخصات ظاهری : ۱۶۰ص.
شابک : ۳۵۰۰۰۰ریال: ۹-۴۳۲۴۲۲-۶۰۰-۹۷۸
وضعیت فهرست نویسی : فیپا
موضوع : جرایم کامپیوتری -- قوانین و مقررات
موضوع : Computer crimes -- Law and legislation
موضوع : جرایم کامپیوتری -- قوانین و مقررات-- ایران
موضوع : Computer crimes -- Law and legislation-- Iran
موضوع : جرایم کامپیوتری
موضوع : Computer crimes
رده بندی کنگره : KMH۸۰
رده بندی دیویی : ۳۴۳/۵۵۰۹۹۴۴
شماره کتابشناسی ملی : ۶۱۲۳۳۱۷

نام کتاب : سیاست کیفری حاکم بر جرایم سایبری با چشم انداز کیفر شناسی
مولف : محسن صفاری فرد خوزانی
ناشر : ارسطو (با همکاری سامانه اطلاع رسانی چاپ و نشر ایران)
صفحه آرایی، تنظیم و طرح جلد: پروانه مهاجر
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : اول - ۱۳۹۹
چاپ : مدیران
قیمت : ۳۵۰۰۰ تومان
فروش نسخه الکترونیکی - کتاب‌رسان :
https://chaponashr.ir/ketabresan
شابک : ۹-۴۲۲-۴۳۲-۶۰۰-۹۷۸
تلفن مرکز پخش : ۰۹۱۲۰۲۳۹۲۵۵
www. chaponashr. ir

انتشارات ارسطو
چاپ و نشر ایران
Chaponashr.ir

به پاس تعبیر عظیم و انسانی از کلمه ایثار و از خود گذشتگی

به پاس عاطفه سرشار و گرمای امیدبخش وجودش که در این سردترین روزگاران بهترین پشتیبان قلب است

به پـــاس قلب بزرگش که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می گراید

و به پاس محبـــت های بی دریغش که هرگز فروکش نکرده و نمی کند

این مجموعه را به روح پدر عزیزم تقدیم می کنم

فهرست مطالب

عنـوان | صفحـه

عنـوان | صفحـه

مقدمه

تحولات ساختاری ناشی از به‌کارگیری فناوری‌های نوین اطلاعات و ارتباطات، جوامع بشری را در تمامی عرصه‌های اجتماعی با چالش‌های نوینی مواجه نموده و حوزه‌ها و افق‌های جدیدی را فرا روی بشر گسترده است؛ به‌گونه‌ای که طراحان ساختارهای اجتماعی، اقتصادی، فرهنگی و حتی سیاسیِ نسل نوین ناگزیرند برای ایجاد مناسبترین بستر و پویاترین ابزار، در فضایی قاعده‌مند و قانون‌مدار، کلیه چارچوب‌ها و معیارهای موجود را روزآمد نمایند. به عبارت دیگر این تحولات، در عصر انقلاب فناوری اطلاعات و ارتباطات کلیه جوامع بشری را ناگزیر ساخته تا سیاست‌های مؤثر و کارآمدی را طراحی نمایند و عملکرد کاربران این فناوری را به‌ویژه در خصوص ارتکاب جرائم در عرصه مبادلات الکترونیکی و رایانه‌ای تحت پایش و مراقبت‌های جامع و سودمندی قرار دهند. (باستانی، ۱۳۸۸: ۳۳)

نکته مهم و اساسی درباره جرائم سایبری، ویژگی‌های انحصاری آنها در مقایسه با جرائم سنتی است. سرعت ارتکاب، کثرت، سهولت ارتکاب، ارزان بودن، بی‌مرز بودن، ناشناختگی، اتوماتیک بودن و...، در جرائم سایبر موجب ظهور گونه‌ای متمایز از جرائم نوین در کنار جرائم سنتی، شده است. در این نوع بزه، مرتکبان ناشناس در فضایی ناشناخته دست به اعمال مجرمانه می‌زنند. برخلاف جرم کلاسیک، جرم سایبری دارای فناوری برتر و وسایل پیشرفته‌تری است. مرتکبین این جرائم با استفاده از فناوری نوین و ابزارهای جدید به اهداف شوم خود دست پیدا می‌کنند بدون آنکه اثری همانند جرم کلاسیک از خود برجای بگذارند. ویژگی دیگر این دسته از جرائم نامشخص بودن هویت مجرمان و همچنین عدم‌تشخیص درست طیف بزه دیدگان است؛ زیرا افراد و سازمان‌های متعددی می‌توانند هدف این مجرمان قرار بگیرند. لذا جرم سایبری نشان‌دهنـده‌ی یک محـدوده‌ی

گسترده از مجرمیت یا بزه‌دیده‌ای نامشخص است. این موضوع نشان می‌دهد که مجرمین سایبری فارغ از زمان و مکان بوده و این نوع از جرائم هم‌اکنون جنبه فراملی و فراسرزمینی به خود گرفته است. فناوری‌هـــای نوین در این عرصه و پیشرفت تجهیزات ارتباطی، مخابراتی و الکترونیکی، سهولت ارتکاب جرم در فضای سایبر، مجرمان را قادر ساخته که فعالیت‌های خود را بدون داشتن ارتباطی خاص با یک محل معین و مشخص، انجام دهند. پرواضح است که با وقوع این نوع از جرائم، خطری جدی برای جامعه بین‌المللی و جامعه داخلی یک کشور رقم می‌خورد.

پیشگیری و واکنش کیفری شود. پژوهش پیش‌رو، تلاش دارد در مقام تبیین و تشریح سیاست کیفری متناسب جرائم سایبری، ضرورت‌های گزینش سیاست کیفری متمایز از جرائم سنتی، در این جرائم را تبیین نماید و با توجه به شرایط و اقتضائات نظام کیفری ایران، گونه‌های این سیاست کیفری افتراقی را در حوزه حقوق کیفری ماهوی اعم از جرم، مسئولیت کیفری و مجازات، و نیز حقوق کیفری شکلی به‌ویژه مرحله تحقیقات مقدماتی، ادله ارتکاب این جرائم و استناد پذیری آن، رسیدگی و صلاحیت محاکم، معرفی کند.

تبیین واکنش‌های کیفری در قوانین جزایی سنتی، عموماً از اصول و مبانی مشترکی پیروی می‌کنـــد. در تعیین این واکنش‌ها تعریف بزه، ارکان تشکیل‌دهنده آن، مبانی مسئولیت کیفری و قواعد حاکم بر مجازات‌ها به‌گونه‌ای عمل می‌شود که کاربردی کمابیش یکسان در مورد انواع بزه و بزهکاری داشته باشد. مثلاً همه جرائم از ارکان سه‌گانه برخوردار بوده و کیفیات مخففه و مشدده در همه جرائم کمابیش مشابه اعمال می‌شود. همین ویژگی‌های مشترک را در بعد شکلی نیز می‌توان مشاهده کرد. در این زمینه آیین‌های حاکم بر کشف بزه، تعقیب، محاکمه و اعمال مجازات علیه بزهکاران اشتراک بنیادین دارند. سیاست‌گذاران حوزه کیفر تلاش می‌کننـــد برای تحقق عدالت و حفظ حقوق و آزادی‌های فردی قواعدی‌نسبتاً یکسان را برای مقابله باهمه مصادیق بزه و بزهکاری به کاربندند. مثلاً قواعد مربوط به حقوق متهم، ادله اثبات بزه، جلب و احضار متهم، نحوه دادرسی و...تابعِ نُرم‌هایی مشابه‌اند. اما گاه ظهور و بروز مصالح و ارزش‌های نوین، ویژگی‌های خاص بزهکار و گستـــره‌ی بزه دیدگان و یا آثار گستـــرده‌ای که گونه‌ای خاص از بزه در جامعه دارد، باعث می‌شود که قانون‌گذار در موارد استثنایی، معیارها، ضوابط و قوانین متمایز ازمعیارها، ضوابط و قوانینِ متعارف حاکم بر بزه وضع نموده و یا به همین سبب آیین‌هایی متفاوت از شیوه‌هایی متداول دادرسی تعریف و تدوین نماید. (عالی پور، ۱۳۹۰: ۴۵)

توجه به ویژگی‌های و تمایزات بزه‌های فضای مجازی در مقایسه با بزه‌های‌ارتکابیِ‌دنیایِ واقعی، این امر را قابل درک می‌سازد که الگوهای ارتکاب جرم در این فضا با الگوهای جرائم سنتی تمایزات قابل توجهی دارند؛ و به‌واسطه‌ی این تحولات و تمایزات و عدم کارایی نظام کیفری سنتی در مقابله با جرائم سایبری است که تبیین رویکرد افتراقی را در قلمرو جرائم سایبر، ضروری می‌نماید. رویکرد کیفری سنتی موجود و متعارف، مربوط به زمانی است که‌فنّاوری، دوران طفولیت خود را سپری می‌کـرد؛ اما امروزه رشد و توسعه‌فنّاوری امکان استفاده از نیروهای انسانی سازمان‌یافته و منابع و امکانات متمرکز برای مقابله با بزهکاران فضای دیجیتال را سلب کرده است.

به نظر می‌رسـد تحولات ناشی از تولد فضای سایبر، متمایز از دگرگونی‌هایی است که در اثر گسترش سایر فناوری‌های پیچیده و مدرن پدید آمده است. درست است که‌مثلاً صنعت حمل‌ونقل، ارتباطات، و سایر صنایع و تکنولوژی‌ها بزهکاری‌های‌خاصِ خود را تولید کرده‌انـد، اما ازآنجاکه این دگرگونی‌هاعمدتاً جنبه کمی داشته‌اند، نظام عدالت کیفری توانسته است با سرعت بیشتری خود را با الزامات ناشی از ساختارهای نوین هماهنگ سازد. یعنی با استفاده از اصول و مبانی موجود حقوق جزا در بعد شکلی و ماهوی در پی مقابله با جرائم ناشی از تحولات جامعه‌ی صنعتی برآمده و توفیق نسبی کسب نموده است. اما ویژگی‌های و خصایص بزه‌های ارتکابی در فضای سایبر حامل این پیام است که حقوق جزا در ابعاد شکلی و ماهوی وارد مرحله جدیدی شده است؛ به‌طوری‌که تنها شرط مبارزه با این‌گونه جرائم، ارائه تحلیلی نو از نحـوه‌ی ارتکاب بزه سایبری و تدوین رویکرد کیفری متناسب برای مواجهه با آن، در ابعاد مختلف ماهوی و شکلی مرتبط با این جرائم، است.

فصل اول:

مبانی افتراقی شدن سیاست کیفری در جرم‌انگاری و کیفر گزینی

بستر ارتکاب جرائم رایانه‌ای، فضای سایبر یا فضای مجازی رایانه، اینترنت و مخابرات است و آنچه این فضا را دنیای جدید معرفی کرده، امکانات و قابلیت‌های متفاوت آن است؛ وگرنه این فضا از همان واژگان دنیایی که در آن زندگی می‌کنیم مانند شاهراه اطلاعات، کتابخانه مجازی، جریان اطلاعات و دهکده جهانی شکل گرفته است۱. بزه‌های سایبری در فضایی ارتکاب می‌یابند که به‌قدری تبادل اطلاعات در آن سریع است که مراحل سنتی ارتکاب جرم یعنی اراده و قصد، تدارک مقدمات و شروع به اجرا به چشم نمی‌آید و مسیرهای اطلاعاتی‌اش به‌قدری زیادند که نتیجه جرم در یک لحظه در مکان‌های گوناگونی حاصل می‌شود. بستری که برای ارتکاب جرم در فضای سایبر به‌ویژه زمانی که شخص داخل در شبکه، رفتار مجرمانه‌اش را ارتکاب می‌دهد، آنقدر با محیط بیرون متفاوت است که مفهوم و اوصاف سنتی جرم را از دو جهت به چالش کشیده است. یکی از جهت روش ارتکاب که فنی و مبتنی بر همکاری ماشین و انسان بوده و بنابراین جرم سایبری در یک لحظه واقع می‌شود و اگر در محیط بیرون جرم آنی را به تحقق لحظه‌ای رفتار فیزیکی جرم می‌شناسیم، در فضای سایبر نه‌تنها زمان همین یک لحظه بسیار کوتاه‌تر شده که کمتر می‌توان سراغی از بزه‌های مستمر گرفت. غیر از این، آنی بودن وقوع جرم فقط ناظر به رفتار فیزیکی، آن‌هم در یک مکان واحد نیست، بلکه در فضای سایبر، اجزای دیگر جرم مانند نتیجه مجرمانه آن‌هم همزمان در مکان‌های مختلف واقع می‌شود. از همه فراتر برخی از جرائم مانند نفوذ غیرمجاز به سیستم یا انتشار ویروس دارای آثار و نتایج مستمری هستند که به جرئت باید جرم سایبری را جرم سیال دانست و این، ماهیت پیچیدگی و فنی بودن فضای سایبر است. دوم، از جهت محیطی که خود ناشی از جنبه فنی و اطلاعاتی فضای سایبر است. جرم سایبری‌ماهیتاً جرمی بین‌المللی است

که گستـره‌ی آن، مرز و محدوده نمی‌شناسـد و محیطش پهنایی به بزرگی دنیا است که مرتکب، جرم را در نقطه‌ای از جهان انجام می‌دهـد و نتایج زیان‌بار را در هر جا که اراده می‌کنـد به نظاره می‌نشینـد، و به‌واسطه محدوده‌ی وسیع آن، آثار جرائم ارتکابی نیز به همان میزان گسترده و وسیع است؛ به همین دلیل است که بزه‌های سایبری ماهیتی جهانی داشته و باید کل یا بخش مهم رفتار تشکیل‌دهنده آن‌هـا در شبکه باز، یعنی زمانی که رایانه متصل به شبکه اینترنت باشد، ارتکاب یابد. (Zakalik, 2002: 269) در ادامه برای تبیین دقیقتر موضوع به تحلیل تفاوت‌های ماهیتی، شیوه‌ی ارتکاب و گستره جرائم سایبری در مقایسه با جرائم کلاسیک خواهیم پرداخت.

مبانی افتراقی جرم انگاری سایبری

تفکیک حمایت از داده

اصـل تفکیک بیانگـر دو موضوع است. نخست اینکه موارد مختلـف نقض حریم خصوصی در فضای سایبر نباید در یک مادهٔ کلی جرم‌انگاری شود و همچنین جرم‌انگاری رفتارها در فضای سایبر باید مبتنی بر معیارهای مادی و روانی مختلف باشد که موجب تغییر در اوصاف جرائم می‌شوند. اصل تقصیر (قابل مجازات بودن) مستلزم تفکیک میان این موارد بر طبق مصالح مربوط، اعمال ارتکابی، وضعیت مرتکب و دیگر عناصر روانی است (Sieber, 1994, p.190).

فضای سایبر زمینه‌ی ایجاد مشابهت در عنصر مادی جرائم ارتکابی در این قلمرو را فراهم نموده و عنصـر روانـی و سایر اوضـاع و احوال است که وصف مجرمانه این رفتارهـا را از یکدیگر متمایز می‌کند (دزیانی، ۱۳۸۴، ص۱۵). برای نمونه، تغییر داده چنانچه برای کسب منفعت اقتصادی انجام شـود، کلاه‌برداری رایانه‌ای؛ اگر در یک سنـد الکترونیکی قابل استناد در مراجع رسمی تحقق یابد، جعـل رایانه‌ای؛ و چنانچه روی داده‌های شخصی با هدف ایجـاد مزاحمت انجام شود، نقض حریم خصوصی اشخاص محسوب می‌شود. لذا این تفکیک و تمایز باید به‌دقت انجام شود.

همچنیـن عدالت ایجاب می‌کند حمایت قانونگذار از اشخاص و داده‌ها در فضای سایبر به‌تناسب میزان اهمیت و آسیب‌پذیری انجام شود. داده‌های شخصی افراد اهمیت یکسانی ندارند؛ برخی از آن‌ها اهمیت ویژه‌ای دارند و جمع‌آوری، پردازش، انتقال یا افشای آن‌ها ذاتاً حریم خصوصی اطلاعاتی افراد

را با چالش روبرو می‌سازد. این داده‌ها را داده‌های شخصی حساس[1] می‌نامند. انجمن بین‌المللی حقوق جـزا و شورای اروپا در راستای حمایت از داده‌های یادشده اصول و معیارهایی را پیشنهاد کرده‌اند که بـر اسـاس آن باید دولت‌ها مقررات جزایی قابل اجرا در زمینـه‌ی حقوق فردی را فقط در موارد مهم اعمـال کنند؛ به‌ویـژه مواردی که داده‌های رایانه‌ای بسیار حساس اسـت و جرم‌انگاری‌ها نیز باید به افعال عمدی محدود شود (Sieber, 1994, p.673)زیرا، اصولاً نقض حریم افراد و داده‌های آن‌ها در فضای سایبر در صورتی با مجازات همراه می‌شود که شخص به طور عمد مرتکب عمل شده باشد و لذا بر این مبنا جرم‌انگاری اعمال ناشی از بی‌مبالاتی مستلزم توجیه ویژه است

بر این اساس، کمیته‌ی حقوق بشر در تفسیر خود از مادۀ ۱۷ حقوق بشر اعلام می‌کند که هر فرد باید بتواند نهادهای دولتی و خصوصی را که بر اطلاعات شخصی او کنترل دارند، بشناسد (کدخدایی و حاجی‌ملا، ۱۳۹۳، ص۵۳۹).

کنوانسیـون جرائم سایبر با آنکـه برابر مفاد مقدمه ازجمله مـواد ۲،۳،۴،۵،۷ کنوانسیون یکی از اهـداف مهم این سند را حمایت از محرمانگی، حفظ تمامیت، دسترس بودن داده‌ها، به‌ویژه دادهای شخصی دانسته، لیکن هیچ‌گونه تقسیم‌بندی از اقسام داده‌های شخصی ارائه نکرده است. همچنین چگونگـی حمایت از داده‌های حساس اشخاص حقیقی و حقوقـی و تسری قواعد حمایت از داده‌ها به این دسته از اطلاعات را بر عهدۀ قانونگذاران ملی نهاده است. مطابعه تطبیقی نشان می‌دهد که ووانیـن مربوطه عموماً داده‌های اشخاص حقوقـی را شامل نمی‌شود (Personal Data protec-tionCode, 2003, p.1-10). ایـن مباحث هنگـام تنظیم رهنمودهای سازمان توسعه و همکاری اقتصـادی هم پیش آمد، ولی درنهایـت تمرکز بر حمایت از داده‌های اشخاص حقیقی قرار گرفت و تسـری آن به داده‌های اشخاص حقوقـی به کشورهای عضو واگذار شد (OECD, 1986, p.22). برخـی کشورهای عضو بر این باور بودنـد که شرکت‌های تجاری و انجمن‌ها باید تحت شمول این رهنمودها قرار گیرند، زیرا ممکن است نحوۀ اقدام‌های آن‌ها هدف حکومت‌ها را در حفظ بازار آزاد و رقابت موجود در ارائه‌ی خدمات دچار اختلال کند (Rustad&Koenhg, 2005, p.368).

بـر اساس دستورالعمل شمارۀ ۹۵/45/EC اتحادیه‌ی اروپا و کنوانسیون جرائم سایبر، در قوانین داخلـی قانون فدرال حمایت از داده را تصویب کرد. سپـس در مادۀ ۴ قانون فدرال حمایت از داده،

1. Sensitive personal Data

ضمـــن تبیین چگونگی جمع‌آوری و پردازش داده‌های شخصی، به صورت مطلق داده‌های شخصی را مورد حمایت قرار داده و در بند «الف» مادۀ ۴ شرط رضایت در قانونی دانستن پردازش داده‌های شخصـــی را تبیین ساخته است. همچنین در بند «ج» مـــادۀ ۴ نیز به موارد استثنایی همچون منافع عمومی، دعاوی حقوقی، حفاظت از منافع حیاتی موضوع داده پرداخته است که به‌موجب آن پردازش داده‌هـــا حتـــی در موارد ممنوع فراهم می‌شود. در نظام قانونگـــذاری آلمان میزان سختگیری قوانین دربـــارۀ داده‌های حســـاس به‌مراتب بیش از داده‌هـــای معمولی است و اصول پـــردازش این داده‌ها به‌خصـــوص اصل امنیت و شفافیت در مورد این داده‌ها سخت‌گیرانه اعمال می‌شوند و حتی‌الامکان حقوق اطلاعاتی فرد باید دقیقاً در آن رعایت شود (حسنی، ۱۳۸۹، ص۱۸).

قانونگذار ایران به‌طور خاص در مادۀ ۵۸ قانون تجارت الکترونیک مصوب ۱۳۸۲ش به موضوع داده‌پیام‌های شخصی پرداخته و قائل به تفکیک در حمایت از داده‌ها شده است. مادۀ۵۸ مقرر می‌دارد: ذخیـــره، پـــردازش و یا توزیع داده پیام‌هـــای شخصی بیانگر ریشه‌های قومی یـــا نژادی دیدگاه‌های عقیدتـــی، مذهبی، خصوصیـــات اخلاقی و داده‌پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است و به‌موجب مادۀ ۷۱ قانون یادشده نقض آن از سوی مرتکب، جرم و مشمول مجازات است.

مادۀ ۷۲ قانون تجارت الکترونیک نیز ارتکاب این جرائم را از جانب دفاتر خدمات صدور گواهی الکترونیکـــی و سایـــر نهادهای مسئول جرم‌انگاری نموده و هرگونـــه بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی را مشمول مجازات دانسته است.

مـــاده ۵۸ قانون مذکور مصادیق داده‌های مـــورد حمایت احصاء نموده، لیکن سخنی از داده‌های صنعتـــی و تجاری به میان نیاورده است و در مادۀ ۵۹ قانون تجارت الکترونیک، شرط جرم ندانستن رفتـــار را رضایت شخـــص دانسته است به اینکه الف) اهـــداف داده‌پیام‌های شخصی مشخص بوده، به‌طـــور واضـــح شرح داده شده باشند. ب) تنها به اندازۀ ضـــرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع داده‌پیام شرح داده شده است، جمع‌آوری و استفاده شود. ج) داده‌پیام صحیح و روزآمد باشد. د) شخص موضوع داده‌پیام بتواند به پرونده‌های رایانه‌ای حاوی داده‌پیام‌های شخصـــی مربوط به خـــود دسترسی داشته باشد و داده‌پیام‌های ناقص یـــا نادرست را محو یا اصلاح کند. قانونگذار ایران با اینکه در مقام بیان بوده، از موارد خاص و استثنایی که بنا به دلایل امنیتی و مصالح عمومی بتوان دست به پردازش داده‌ها زد، سخنی به میان نیاورده است.

مـواد قانونی اشاره‌شده سه عنـوان مجرمانه‌ی ذخیره، پردازش پیام‌های شخصی حساس و عدم رعایـت شرایط قانونی پیام‌های شخصی حساس، و جرائم غیرعمـد راجع به داده‌پیام‌های شخصی حسـاس را بیـان نموده است. به این ترتیب، ترک فعل در جرائـم پیش‌گفته نمی‌تواند عنصر مادی جـرم قـرار گیرد؛ زیرا افعالی که عنصر مـادی جرائم پیش‌گفته را تشکیـل می‌دهند، شامل ذخیره، پـردازش داده و توزیع داده‌پیام اسـت. بنابراین، قانونگذار ایران فقـط داده‌های شخصی حساس را حمایـت می‌کند و از مطلـق داده‌های شخصی، ازجمله داده‌های تجـاری و صنعتی، حمایت نکرده است. همچنین قانونگذار ایران موارد استثنایی جمع‌آوری و پردازش داده‌ها بدون رضایت اشخاص را پیش‌بینی نکرده است. به نظر می‌رسد نبود منابع اطلاعاتی دقیق و زیرساخت‌های مخابراتی متناسب و همچنیـن قوانین پایـه‌ای و تخصصی ازجمله قانون حمایـت از داده، ازجمله مهم‌ترین علت‌های تفاوت در رویکرد قانونگذاران دو کشور است

تفکیک حمایت از اشخاص آسیب‌پذیر

یکـی از سازوکارهای حمایت کیفـری در فضای سایبر، جرم‌انگاری افتراقـی رفتارهای آسیب‌زا نسبـت به اشخاص آسیب‌پذیر، به‌ویژه کودکان است. این امـر در سطح بین‌المللی بیشتر به حمایت از کودکـان در برابر سوءاستفادهٔ جنسی محدود می‌شود. کنوانسیون سازمان ملل متحد دربارهٔ حقوق کودک (UN Convention, 1989, P.1577)، کنوانسیون شورای اروپا راجع به حمایت از کودکان در برابر سوءاستفادهٔ جنسی (Council of Europe Treaty Series, 2007, (p.201 و یا چارچوب تصمیم‌گیری شورای اتحادیه‌ی اروپایی دربارهٔ حمایت از کودکان در برابر سوءاستفادهٔ جنسی (Convention Council of Europe,2001,p.20) همگـی بیانگر فرایند جهانی‌شدن حقوق کیفری در قلمـرو حمایت از کودکـان در برابر هرزه‌نگاری است. کنوانسیون جرائم سایبر نیز در مادهٔ ۹ با عنوان جرائـم مرتبط بـا محتوا، دولت‌های عضو را به جرم‌انگاری هرزه‌انگـاری اشخاص زیر ۱۸ سال ملزم ساخته است که بیانگر توافق بین‌المللی در مجرمانه بودن چنین رفتاری است. لیکن چگونگی اجرای ایـن مقـررات همواره با اختلاف نظرهایی همراه بوده است؛ نخسـت اینکه محدودهٔ سنی افراد مورد حمایت در کشورهای مختلف از ۱۴ تا ۱۸ سال متغیر است (Delmas Marty, 2008, p.155).

این قلمـرو حمایت در بیشتر کشورها با عنوان هرزه‌نگاری نـرم (Soft pornography) تلقی می‌شـود؛ بـه این معنا که توزیـع آن در میان بزرگسـالان مجاز و برای کودکـان ممنوع است. در

مقابل، دیدگاه دیگری با عنوان هرزه‌نگاری مطلق مطرح است؛ به این معنا که توزیع آن حتی میان بزرگسالان نیز ممنوع است (Delmas-Marty, 2008, p.157).

قانونگذار ایران در نحوهٔ حمایت، بین بزرگسالان و کودکان قائل به تمایز نشده و به این لحاظ نیز حمایت کیفری لازم را اعمال نکرده است؛ صرفاً در بند «د» مادهٔ ۲۸ که مربوط به صلاحیت دادگاه‌ها است مقرر می‌دارد: چنانچه جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب بزه دیده ایرانی یا غیر ایرانی باشد، دادگاه‌های ایران صالح به رسیدگی است. در تبصرهٔ ۳ مـادهٔ ۳ نیز نحوهٔ مجازات اشخاصـی که در امور سمعی و بصری فعالیت‌های غیرمجاز دارند، مقرر شـده است: استفاده از صغار برای نگهداری، نمایش، عرضه، فروش و تکثیر نوارها و لوح‌های فشردهٔ غیرمجاز موضوع این قانون موجب اعمال حداکثر مجازات مقرر برای عامل خواهد بود.

عـدم تفکیک در قانونگذاری سایبری به نظر می‌رسد بیشتـر ناشی از شتاب‌زدگی نظام کیفری ایـران در جرم‌انگاری تحت تأثیر حاکمیت فضای احساسی و اولویت یافتن ملاحظات سیاسی برای پاسخگویـی مقطعی و فوری به انتظارات عمومی در پـی بازتاب گستردهٔ رسانه‌ای این جرائم است. نمونـه‌ی این فرایند را می‌تـوان در طرح قانون نحوهٔ مجازات اشخاصی که در امور سمعی و بصری فعالیـت غیرمجاز دارند مشاهده کرد که به دور از دغدغه‌های علمی و کارشناسی به دلیل همسویی با دیدگاه‌های عوام‌گرایانه به‌سرعت در دستور کار قرار گرفت (فرجی‌ها و مقدسی، ۱۳۹۲، ص۱۴۷–۱۴۶)؛ موضوعی که شاید در آغاز کار از اهمیت چندانی برخوردار نباشد. اما واقعیت این است که تمام تلاش‌هـای قانونگذار در راستای تدوین قوانین مناسـب برای حمایت از اشخاص و داده‌ها در آنچه بـه نگارش درمـی‌آورد، بروز می‌یابد. شتاب‌زدگی و نگارش نادرسـت و تفسیر نابجا می‌تواند تمامی تلاش‌های پژوهشی ناشی از طی فرایند دشوار قانونگذاری را بی‌حاصل نماید، زیرا چگونگی انشای مواد قانونی به صورت ناخواسته می‌تواند تأثیرات ماهوی بر قوانین داشته باشد.

وضوح و دقت در تعریف جرائم سایبر

اصـل دقت در تعریف جرائم سایبر بیانگر این موضوع است کـه قانونگذار باید اعمال ممنوع را به‌تفصیـل بیان کرده، با ارائه‌ی تعاریف دقیـق از اعمال غیرقانونی و تعیین اوصاف حقوق ماهوی و محدودهٔ آن، از ابهام و کلی‌گویی خودداری نماید (حسنی، ۱۳۸۹، ص۱۸۱).

مـادۀ ۶ کنوانسیون جرائم سایبر در این خصوص مقـرر می‌دارد: قوانین مصوب در این باره باید تـا حد امکان با دقت و ظرافت خاصی نوشته شوند تا قابلیت پیش‌بینی مناسب نوع رفتاری را که به محکومیت کیفری منجر می‌شود، فراهم آورند. به‌موجب اصل قانونی بودن جرم و مجازات به‌عنوان یکـی از اصول حقوقی که مورد تأکیـد قانون اساسی است، قانونگذار بایـد عناصر قانونی، مادی و معنوی هر جرم را به‌طور واضح و شفاف و بدون هرگونه ابهام و کلی‌گویی به‌خصوص در امور کیفری اعلام نماید تا شهروندان قانون را بهتر درک کنند و درنتیجه اثر بازدارندگی قانون نیز افزایش یابد.

قانونگـذار ایران در مـادۀ ۲۱ قانون جرائم رایانه‌ای، ارائه‌دهندگـان خدمات دسترسی را موظف نمـوده طبـق ضوابط فنی و فهرست مقرر از سوی کارگروه تعیین مصادیق، محتوای مجرمانه را که در چارچـوب قانـون تنظیم شده است اعم از محتوای ناشـی از جرائم رایانه‌ای و محتوایی که برای ارتکـاب جرائم رایانه‌ای به کار مـی‌رود، پالایش نمایند و چنانچه عمداً از پالایش محتوای مجرمانه خودداری کنند، مجازات انحلال را پیش‌بینی نموده و مقرر داشته است: چنانچه از روی بی‌احتیاطی و بی‌مبالاتـی زمینه‌ی دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه‌ی نخست به جزای نقـدی و در صورت تکـرار به تعطیلی موقت محکوم خواهند شد. تدویـن و نگارش مادۀ ۲۱ قانون جرائـم رایانـه‌ای به گونه‌ای است کـه با توجه به معیار شفافیت در عمـل ممکن است با مشکلات زیادی روبرو شود:

نخسـت اینکـه بر اساس مادۀ یادشده گاهـی ارائه دهندۀ خدمات، فضـای لازم را برای ذخیرۀ اطلاعـات در اختیار گذاشته باشد و طبق قرارداد، مدیریت پردازش به عهدۀ کسی دیگر باشد که در این صورت طبق مادۀ یادشده ارائه‌کننده مسئول است و پردازش‌کننده مسئولیتی ندارد و این تحمیل مسئولیـت بـه نظر درست نمی‌آید به نظـر می‌رسد قانونگذار ایران در تدوین مـادۀ یادشده، مادۀ ۶ کنوانسیون جرائم سایبر را الگو قرار داده است، ولی تفاوت عمدۀ آن با مادۀ ۲۵ قانون جرائم رایانه‌ای شامل دو موضوع است که یکی از آن‌ها موضوع جرم می‌باشد که به‌موجب ش ق «الف» بند ۱ مادۀ ۶ کنوانسیـون، وسیله‌ای است که برای یکی از چهار جرمِ دستیابی غیرمجاز، شنود غیرمجاز، اخلال در داده و اخـلال در سیستم، طراحی و تنظیم شده است. لیکن به‌موجب بند «الف» مادۀ ۶ موضوع جرم، داده یا نرم‌افزار و هر نوع وسایل الکترونیکی (بدون توجه به نوع جرم) به‌کاررفته که عدم دقت در تدویـن مـادۀ ۲۵ موجب شده است توزیع، انتشار و معامله‌ی آن‌ها مشمول مادۀ ۱۴ و ۱۵ و ۱۶ و هـم مشمول مادۀ ۲۵ قرار گیرد. این در حالی اسـت که اگر قانونگذار ایران به تبعیت از کنوانسیون

جرائم سایبر، موضوع جرم را به وسایل ارتکاب یکی از چهار جرم دستیابی و شنود غیرمجاز و اخلال در داده و سیستم محدود می‌کرد، اشکال مورد نظر تحقق نمی‌یافت.

بـا توجه بـه اینکه بیشتر نرم‌افزارهای موجود ماهیتی دوگانه دارنـد، کنوانسیون جرائم سایبر در بنـد ۲ مادۀ ۶ و بنـد ۱ (الف)، تولید و فروش، تهیه به‌منظور استفاده، واردکردن، توزیع یا به هر نحو در دسترس قرار دادن دستگاه دارای برنامه‌ی رایانه‌ای را چنانچه طراحی یا سازگار شده باشد برای ارتکاب جرائم مندرج در مواد ۲ تا ۵ ممنوع کرده است. کنوانسیون به‌عنوان یک توافق معقول، حوزۀ عملکرد خود را به مواردی محدود کرده است که دستگاه‌ها در ابتدا به قصد ارتکاب جرم به صورت نوعی طراحی یا سازگار شده باشند. بر اساس این معیار دستگاه‌های دو منظوره از شمول ماده خارج می‌شوند و این در حالی است که قانونگذار ایران در موارد اشاره‌شده به این امر دقت لازم را نداشته اسـت و لذا در مادۀ ۲۵ قانون جرائم رایانه‌ای، فروش یـا انتشار یا در دسترس قرار دادن گذرواژه یا هـر دادهای کـه امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌هـای رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم نماید، جرم و قابل مجازات دانسته و این در صورتی است که رمز عبـور و کدهای دسترسی و داده‌های مشابـه ازجمله وسایلی هستند که دارای کاربردهای دوگانه‌اند. بـر همین اساس، مـادۀ ۶ کنوانسیون بیان می‌کند، در صورتی که انتشار و معامله و در اختیار نهادن به‌قصد ارتکاب جرم باشد، بایستی جرم‌انگاری شود؛ در حالی که در بند «ب» مادۀ ۲۵ صرف انتشار و در اختیار گذاردن را جرم تلقی نموده است. قانونگذار ایران با توجه به مشارکت نداشتن در نهادها و کنوانسیون‌هـای بین‌المللی همچون کنوانسیـون جرائم سایبر و پروتکل الحاقی و همچنین اولین تجربه‌ی قانونگذاری تخصصی در حوزۀ سایبر دقت لازم را در نگارش، ازجمله تعریف جرائم سایبر، اعمال نکرده است.

شفافیت در تعریف جرائم سایبر و عدم ارجاع

جرائـم فضای سایبـر معمولاً با واژگان و اصطلاحاتی تعریـف و توصیف می‌شوند که در جرائم فضای واقعی کاربرد دارند، مانند سرقت رایانه‌ای یا کلاه‌برداری سایبری و شنود داده‌های الکترونیکی؛ در حالـی که به لحاظ عنصر مادی و نحوۀ ارتکاب، تفاوت اساسی میان این دو وجود دارد. بنابراین، اعمـال جرم‌انگاری شده باید تا حد امکان به صورت واضح و روشن از سوی مقررات کیفری مربوط

تشریــح شوند. استفادۀ گسترده از روش ارجاع[1] مقــررات کیفری را مبهم و غیرشفاف می‌سازد و لذا بایــد از آن خــودداری شود (دزیانی، ۱۳۸۴، ص۲۱) و در مواردی کــه قانونگذار ناگزیر به استفاده از ارجاعــات صریــح یا ضمنی به مقررات کیفری می‌شود لازم است قانونگــذار ایران در مادۀ ۳ قانون جرائــم رایانه‌ای در خصوص دسترسی غیرمجاز و استفــاده از اسناد و داده‌های سری در حال انتقال یــا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مقرر می‌دارد، هر کس مرتکب اعمال زیر گردد، مشمول مجازات خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال؛ ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت؛ ج) افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها.

قانونگذار ایران در این ماده به مجازات جاسوسی رایانه‌ای پرداخته و در تبصرۀ ۱ داده‌های سری را تعریف کرده است، لیکن نحوۀ تعیین و تشخیص داده‌های سری و نیز چگونگی طبقه‌بندی و حفاظت آن‌ها را به تنظیم آیین‌نامه وابسته کرده که هنوز تصویب نشده است. اما این نکته را باید خاطرنشان کرد که در خصوص اسناد دولتی سری و محرمانه قانونگذار در سال ۱۳۵۳ش قانون مجازات انتشار و افشای اسناد محرمانه و سری را به تصویب رسانده و در خصوص اسناد اشاره شده تعیین تکلیف کرده اســت. در تعریــف اسناد دولتی و محرمانه در مادۀ ۱ این قانون آمده است: اسناد دولتی شامل هر نوع نوشته یا اطلاعات ثبت یا ضبط‌شده مربوط به وظایف و فعالیت‌های وزارتخانه‌ها و مؤسسات دولتی و وابسته به دولت و شرکت‌های دولتی از قبیل مراسلاتی است که در مراجع پیش‌گفته تهیه شده یا به آن رسیده باشد. اسناد دولتی سری را نیز شامل اسنادی دانسته است که افشای آن‌ها مغایر با مصالح دولت و یا مملکت باشد. اسناد دولتی محرمانه را شامل اسنادی دانسته است که افشای آن‌ها با مصالح خاص اداری سازمان‌های یادشده در این ماده مغایرت داشته باشد.

تعریــف جرائم خطیر و خاص مقرر می‌نماید: جرائم خطیــر و خاص معمولاً در صورتی به وقوع خواهنــد پیوست که مجــرم از مسئولیتی که بر اساس آن به حفاظت از اسرار دولتی ملزم شده است سوءاستفاده کند و به‌واسطه‌ی عمل مجرمانه‌ی او، آسیب جدی به امنیت خارجی وارد گردد. همانطور کــه مشاهــده شد، قانونگذار با بیــان جرائم خاص و خطیر در همان مادهای کــه به آن اشاره کرده

۱. روشی که مطابق آن فعالیتهایی که تحت حکومت کدهای غیرکیفری قرار دارند با ارجاع به مقررات کیفری جرم انگاشته شوند.

است و بدون ارجاع به سایر قوانین مصوب، حداکثر در یک مادهٔ دیگر در خود همان قانون اقدام به شفاف‌سازی کرده است. (حسنی، ۱۳۸۹، ص۱۸۹).

هرچـه جرم‌انگـاری بر مطالعات و تفکرات عمیق استوار باشد، نظـام کیفری را کارآمدتر خواهد ساخـت. بر این اساس، تدوین و اعلام معیارهای جرم‌انگـاری می‌تواند با ایجاد شفافیت در رویکرد قانونگـذار و ایجـاد چارچوبی علمی، مانع اشتباهات حاکم در تدویـن سیاست کیفری شود و حقوق شهرونـدان را تضمیـن کند. اینکـه چه داده‌هایی بایـد حمایت شوند و نیز مشخـص کردن حدود اختیـارات حکومت و حمایت‌های ویژه از شهروندان در برابر این اختیارات و تعیین اقشار آسیب‌پذیر و حمایت‌هـای مخصوص از این اقشار، هریک مؤلفه‌هایی هستند که به‌عنوان یک معیار بین‌المللی جرم‌انگاری در فضای سایبر مطرح می‌شوند.

دقـت در تفکیـک جرائم و همچنین تمایز نهادن در نحوهٔ حمایـت از داده‌ها برحسب اهمیت آن ازجملـه معیارهـای اساسی جرم‌انگاری در جرائـم سایبر است. برخی از داده‌هـای شخصی به دلیل حساسیت موضوع داده، باید از حمایت‌های ویژه‌ای برخوردار شوند و پردازش آن‌ها جز در موارد خاص و مصـرح مجاز نیست. قانونگذار آلمـان به‌طور مطلق از داده‌های شخصی حمایت کرده، لیکن موارد استثنایـی را نیز پیش‌بینی نموده است که جمع‌آوری، پردازش، افشای داده‌ها نیازمند رضایت شخص نیسـت. قانونگذار ایران نیز تنها داده‌های حساس اشخاص را در قبال پردازش، مشمول حمایت قرار داده است؛ با اینکه در مقام بیان موارد استثنا بوده، در خصوص موارد خاص و استثنایی که بنا به دلایل امنیتی و مصالح عمومی باید جمع‌آوری و پردازش شوند، سخنی به میان نیاورده است.

بیشتـر بیانگر قواعد بنیادیـن جرم‌انگاری مانند اصل مشروعیت، اصل ضـرورت، رعایت حریم خصوصـی، تناسب جرم و مجازات و توجه کامل به امکانات موجودِ دستگاه عدالت کیفری است در مورد همه مواردی که نیاز به جرم شمردن یک عمل هست باید رعایت شوند. در کنار این اصول به جهـت ویژگی‌های منحصربه‌فرد و بی‌نظیر فضای سایبر باید از اصولی سخن گفت که خاص جرائم سایبری است. در ادامه در دو بخش، ابتدا به برشمردن «اصول عام» جرم‌انگاری در خصوص جرائم سایبری و سپس به بیان «اصول خاص» جرم‌انگاری در جرائم سایبری پرداخته خواهد شد.

مبانی افتراقی کیفرگزینی سایبری

ماهیت فنیِ بزه‌های سایبری

پیشرفت‌های فنی و صنعتی، یک قاعده عام را پیش‌روی می‌نهد و آن اینکه هر فن یا صنعت جدید کارگشای بسیاری از مشکلات بشر است ولی در همان حال چالش‌هایی نیز به همراه دارد که برخی از این چالش‌ها جنبه انسانی داشته و از سوی ناقضان هنجارهای آن فن یا صنعت رخ می‌دهد. فضای سایبر نیز یک ابر نمونه فنی است که دارای اجزای مختلف بوده و هریک یا تمام این اجزا می‌تواند زمینه سوءاستفاده‌های بزهکاران سایبری گردد. فناوری اطلاعات خصوصاً اینترنت ابزاری قدرتمند برای بزهکاران است. آنچه ابتدا توسط وزارت دفاع آمریکا برای تقویت ارتش و بالا بردن قابلیت‌های تهاجمی ایجاد شده بود، اکنون برای همان مقاصد توسط بزهکاران استفاده می‌شود. تولیدات پیشرفته فناوری، قابلیت دستیابی گسترده و هزینه‌های کم، اینترنت را تبدیل به ابزاری کرده است که برای هر فردی قابل دسترسی است. این قابلیت دسترسی فزاینده به ارتباطات پیشرفته موجب شده است تا بزهکاران سایبری در رابطه با منابع، دیگر نیازی به حمایت دولت‌ها نداشته باشند. اینترنت در تمام نقاط جهان با یک مودم و یک رایانه قابل دسترسی است، اگرچه قابلیت دستیابی جهانی در بعضی مناطقی که تقریباً هیچ زیر ساختار ارتباطی ندارند، به نحو قابل توجهی متفاوت است. اینترنت ماهیتاً قلمرویی ایــده‌آل برای فعالیت‌های مجرمانه‌ی سایبری است و مزیت‌های برجسته‌ای را ارائه می‌کند از جمله: دسترسی آسان، نبودن یا حداقل بودن مقررات سانسور یا دیگر کنترل‌های حاکم، خیل عظیم و بالقوه‌ای از مخاطبین در سرتاسر جهان، ابهام هویت در ارتباطات، جریان سریع اطلاعات، ارتباطات تعاملی، کم‌هزینه بودن ایجاد و نگهداری حضور شبکه‌ای محیط چند رسانه‌ای (امکان ترکیب متن، تصویر، صوت و فیلم و امکان دانلود کردن فیلم، موسیقی، کتاب، پوستر و غیره توسط کاربران).

فضای سایبر علاوه بر مطلوبیت‌هایی که برای مجرمین دارد، مخاطرات و محدودیت‌هایی را نیز برای اقدامات مجرمانه دارد که این امر تصمیم‌گیری برای حضور بیشتر در فضای سایبر تأثیرگذار بوده است. پس بخشی از تحقق اقدامات مجرمانه‌ی سایبری، در گرو موقعیت فنی است؛ یعنی ارتکاب بزه سایبر، از طریق یا علیه امکانات فنی و پیچیده فضای سایبر، رخ می‌دهد. این پیچیدگی‌های فنی فضای سایبر خود گواه آن است که می‌تواند بستر ایجاد بزه‌های سایبری را

فراهم سازد. گاهی واقعیت فنی بزه‌های سایبری مبتنی بر وسیله است که بر اساس آن رایانه و مخابرات دو سامانه‌ای هستند که می‌توانند در خدمت هر اقدامی باشند و ازجمله اقدامات بزهکارانه و گاهی واقعیت فنی این پدیده مبتنی بر موضوع که همان اطلاعات و داده است، می‌باشد که بر اساس آن، اطلاعات، هسته و بن مایه رفتارهای بزهکارانه در فضای سایبر و از یک دید، هدف و سیبل آن خواهد بود. گاهی نیز واقعیت فنی‌های‌بزه سایبری بر پایه رفتارهای فنی و خاص است که در این میان هک و کرَک از همه برجسته‌تر است. این رفتارهای حرفه‌ای و خاص نشان‌دهنـــده این است که جرائم در فضای سایبر، چهره‌ای خاص ممتاز دارد. بدین ترتیب ماهیت فنی جرائم سایبری با سه محور وسیله، هدف و رفتار توجیه می‌شود:

محوریت رایانه و مخابرات

بزه‌های سایبری بدون تصور سیستم رایانه‌ای و سیستم مخابراتی امکان‌پذیر نیست. امروزه سیستم مخابراتی مبتنی بر نظام دیجیتال (صفر و یک) بوده و گزاف نیست که آنرا در دل سیستم رایانه‌ای جا دهیم. سیستم رایانه‌ای برگرفته از دو جزء سیستم و رایانه است که در بیشتر موارد به‌جای همدیگر به کار می‌روند اما با کنکاش در معنای این دو واژه می‌توان دریافت که سه واژه «سیستم»، «رایانه» و «سیستم رایانه‌ای» معنای یکسانی ندارند. سیستم (سامانه)، واژه‌ای است که در بیشتر دانش‌ها و نیز در بسیاری از امور و فعالیت‌های اجرایی و اداری بر زبان‌ها افتاده و برحسب جایگاه به‌کارگیری‌اش دارای معناهای ویژه مانند روش، چارچوب و هر چیز نظام‌مند است ولی در ارتباط با جهان انفورماتیک، مجموعه‌ای از عناصر است که برای انجام یک کنش با یکدیگر کار می‌کنند. یک سیستم سخت‌افزاری متشکل از یک ریزپردازنده، تراشه‌ها و مدارات مرتبط با آن، وسایل ورودی و خروجی، وسایل جانبی؛ یک سیستم‌عامل متشکل از مجموعه‌ای از برنامه‌ها و فایل‌های دادهـــای یا یک سیستم مدیریت بانک اطلاعاتی که برای پردازش انواع خاصی از اطلاعات مورد استفاده قرار می‌گیرد، نمونه‌هایی از یک سیستم هستند. (هیئت مؤلفان مایکروسافت، ۱۳۸۱: ۷۱۷)

رایانه هر وسیله‌ای است که قابلیت پردازش اطلاعات را جهت تولید و نتیجه موردنظر دارا باشد. بدون توجه به بزرگی یا کوچکی رایانه‌ها، آنها عموماً کارهای خود را در سه مرحله تعریف شده، انجام می‌دهند: ۱- پذیرش ورودی ۲- پردازش ورودی مطابق با قوانین از پیش تعریف شده (برنامه‌ها) ۳- تولید خروجی. (هیئت مؤلفان مایکروسافت، ۱۳۸۱: ۱۶۶)

در دو تعریف گفته شده، روشن است که نزد عرف متخصصین رایانه، منظور از سیستم همان رایانه است و رایانه هم یک سیستم است و ازاین‌رو، گاهی به‌جای هم به کار برده می‌شوند. تنها خوبیِ به کار گرفتن واژه «سیستم رایانه‌ای»، آوردن جنبه‌های نرم‌افـزاری و سخت‌افزاری در کنار یکدیگر است. (هیئت مؤلفان مایکروسافت، ۱۳۸۱: ۱۶۶) هم‌اکنون، واژه «سیستم رایانه‌ای» در نظام قانون‌گذاری ایران وارد شده که پیش‌بینی می‌شود این به‌کارگیری افزایش یابد ازجمله طبق بند «و» ماده ۲ قانون تجارت الکترونیکی، سیستم رایانه‌ای «هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری – نرم‌افـزاری است که از طریق اجرای برنامه‌های پردازش خودکار داده‌پیام عمل می‌کند.» با توجه به اینکه سیستم رایانه‌ای، به‌هرحال، افزار تراکنش اطلاعات است و نیز چون سیستم مخابراتی، بستر پیوند میان اشخاص را از رهگذر تلفن و دیگر افزارهای ارتباطی گفتاری و شنیداری فراهم می‌کند، به اولی سیستم اطلاعاتی و دومی سیستم ارتباطی نیز گفته می‌شود[۱].

تحولاتی که رایانه و سیستم رایانه‌ای در زندگی روزمره بشر ایجاد کرده به‌اندازهـای بیشمار و خیره‌کننده است که امروزه رایانه‌ای بودن، ویژگی همه امور شده است. در واقـع بشر امروزی برای روزآمدسازی یا آینده‌نگری بر سر هر واژه‌ای، تعبیر «رایانه‌ای» یا «سایبری» گذاشته و می‌کوشد تا به جنبه‌های جدید آن نیز بیاندیشد. مضاف بر اینکه سیستم رایانه‌ای و مخابراتی امکاناتی نیستند که بزهکاران بتوانند از کنار آنها بگذرند. ازاین‌رو، تردید در واقعیت فنی بزه‌های سایبری، تردید در قابلیت‌ها و توانایی‌های سیستم رایانه‌ای و مخابراتی است.

۱. دو اصطلاح سیستم اطلاعاتی و ارتباطی در نام ورازتخانه ارتباطات و فناوری اطلاعات نهفته است. این برداشت را به ویژه می‌توان از ماده ۲ قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات مصوب نوزدهم آذرماه ۱۳۸۲ فهمیده که مقرر می‌دارد: به منظور اعمال حاکمیت بر طیف فرکانس و حفاظت از حقوق رادیویی کشور در سطح منطقه و بین الملل و تمرکز امور سیاستگذاری، تدوین ضوابط و استانداردها و نظارت بر حسن اجرای آنها در بخش های مختلف ارتباطات پستی و مخابراتی نظیر خدمات جدید و متعارف پستی، مخابراتی، ارتباطات فضایی، ارتباطات رادیویی، انتقال داده‌ها، انتقال صدا و تصویر، سنجش از راه دور، ارتباطات رایانه‌ای و ایجاد بستر مناسب برای ارتباطات و آمایش و پردازش اطلاعات و روش‌های دورسنجی و پشتیبانی آنها و همچنین سیاستگذاری در زمینه توسعه امکانات و خدمات ارتباطی مذکور، هماهنگ با آخرین پیشرفت‌های علمی، تجربی و فناوری اطلاعات در جهان، در چارچوب سیاست‌های کلی نظام به موجب این قانون نام وزارت پست و تلگراف و تلفن به «وزارت ارتباطات و فناوری اطلاعات» تغییر می‌یابد و کلیه وظایف، اختیارات و مسئولیت‌های وزیر و وزارت پست و تلگراف و تلفن به وزیر و وزارت ارتباطات و فناوری اطلاعات تفویض می‌گردد.