

هستی‌شناسی جرائم رایانه‌ای با توجه به قانون جرائم رایانه‌ای

مهدی عبدی پور کشاورز،^۱ عباسقلی انصاری*^۲، حمید ششگل^۳

چکیده:

با رشد روز افزون فن آوری اطلاعات و خدمات اینترنت، فعالیت‌های مجرمانه نیز در فضای مجازی افزایش می‌یابند. چالشی که سازمان قضایی با آن مواجه است، تعیین مجازات و کیفر برای مجرمان می‌باشد؛ زیرا قوانین جرایم رایانه‌ای متناسب با رشد فن آوری اطلاعات به‌روزرسانی نمی‌شوند و در نتیجه پس از وقوع جرم جدید، تعیین کیفر برای آن جرم توسط قانونگذار، کاری زمانبر و دشوار است. قوانین جرایم رایانه‌ای باید طوری تدوین شوند که همه شمول بوده و خلأ و حفره‌های قوانین را پوشش دهد. راستا در سال ۱۳۸۸ قانون جرائم رایانه‌ای به تصویب و اجرا درآمد و مشکل خلأ تقنینی در مورد عنصر قانونی جرائم مذکور را در نظام حقوق کیفری مرتفع ساخت. جرایم رایانه‌ای حوزه بسیار گسترده‌ای دارند و به فعالیتی گفته می‌شود که در آن کامپیوترها یا شبکه‌های ارتباطی ابزار، مقصد یا محل اجرای یک فعالیت مجرمانه و غیر قانونی می‌باشند. در هر عصر که علم جدیدی کشف می‌شود، مجرمین نیز از جلوه‌های نوین آن علم جهت ارتکاب جرم بهره‌برداری می‌کنند. تسهیل و تسریع در پیدا کردن کیفر برای جرایم جدید، پیدا کردن سابقه‌ی جرم، ردپای جرایم مرتبط و زنجیره‌ی بازداشت، آموزش از اهداف اصلی هستی‌شناسی جرایم رایانه‌ای می‌باشد. این هستی‌شناسی می‌تواند در سازمان‌های قضایی و انتظامی مورد استفاده قرار بگیرد.

واژگان کلیدی: هستی‌شناسی، جرایم رایانه‌ای، حقوق، قوانین کیفری.

* دانشجوی دکتری حقوق کیفری و جرم‌شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران.

** استادیار گروه حقوق واحد تاکستان، دانشگاه آزاد اسلامی، تاکستان، ایران. (نویسنده مسئول)

ansari@gmail.com

*** استادیار گروه حقوق واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران.

مقدمه

به دلیل ماهیت جرم رایانه‌ای و تفاوت استفاده از فن‌آوری اطلاعات توسط کاربران و تفاوت دیدگاه حقوقدانان و نظام حقوق کیفری کشورها، تعاریف متعددی از جرم رایانه‌ای ارائه شده است ولی تاکنون در سطح بین‌المللی، توافق بر سر تعریف جامعی از جرم رایانه‌ای صورت نگرفته است؛ دلیل این امر، آن است که روزافزون به گستره‌ی جرائم رایانه‌ای افزوده می‌شود و محدودی‌ی جرائم مشخص نمی‌باشد.

در جرم‌شناسی، چهار پدیده وجود دارد که در بررسی‌های جرم‌شناسی، همواره تکیه‌گاه این علم محسوب شده، اصول جرم‌شناسی نامیده می‌شود. زیرا به طور مداوم و در همه مباحث، وسیله و واسطه بحث‌ها و تجزیه و تحلیل‌های تحقیقات می‌باشد. علت، عامل، انگیزه و شرط پدیده‌هایی هستند که هریک دارای معنا و مفهومی دقیق منطقی و فلسفی هستند. گاه در اثر عدم توجه به مفاهیم مذکور، یکی از این پدیده‌ها در معنای دیگری به کار می‌رود و گاه مفهوم اصلی خود را از دست داده و مسیر تحقیق را نیز تغییر می‌دهد. شناخت این اصول، جرم‌شناس را در نیل به اهداف تحقیقاتی خود موفق می‌نماید (کی‌نیا، ۱۳۷۰: ۵۴).

ظهور و گسترش ابزارهای اطلاعاتی که طی چندین سال اخیر روند رو به رشد فوق‌العاده‌ای داشته است، تمامی شئون و جنبه‌های زندگی انسانی را به شدت تحت تاثیر قرار داده است. این تاثیر آنچنان عمیق و شگرف بوده که به اعتقاد بسیاری از اندیشمندان دوران نوینی از زندگی بشری را که از آن به عنوان جامعه اطلاعاتی یاد می‌شود موجب گشته است. جامعه کنونی جهان، جامعه‌ای است که به سرعت به سوی این جامعه ارتباطی و اطلاعاتی در حال حرکت است؛ جامعه‌ای که به اعتقاد برخی از اندیشمندان نظیر آلون تافلر، آنقدر پراهمیت است که سومین جریان و رویکرد کلی زندگی بشری را از ابتدا تا کنون و پس از گذر از جوامع کشاورزی و صنعتی رقم زده است. نمادین‌ترین محصول سیر تحول جوامع انسانی از صنعتی به اطلاعاتی در هزاره سوم شبکه‌های رایانه‌ای و خصوصا اینترنت است که از فضای بوجود آمده از ارتباط آنها به عنوان سایبر یاد می‌شود. واژه رایانه‌ای از نظر لغوی به معنای مجازی و غیر ملموس و مترادف لغت انگلیسی Virtual می‌باشد. سایبر از لغت یونانی Kybernetes به معنای سکاندار یا راهنما مشتق شده است. به عبارتی، رایانه‌ای به مطالعه ساز و کارهای مورد استفاده در کنترل و تنظیم سیستم‌های پیچیده اعم از انسان یا ماشین اطلاق می‌شود. اصطلاح فضای رایانه‌ای یا دنیای مجازی آنلاین نخستین بار توسط ویلیام گیسون در زمانی با عنوان نیو رومانس در سال ۱۹۸۴ مورد استفاده قرار گرفت (اسلامی، ۱۳۹۵: ۱۲).

جرم به فعل یا ترک فعلی گفته می‌شود که قانون‌گذار برای آن مجازاتی در نظر گرفته است

و برای آنکه جرم تلقی شود باید عنصر قانونی، عنصر مادی و عنصر روانی یا معنوی جرم فراهم باشد. کلاهبرداری رایانه ای به لحاظ خلاقیت مرتکب آن و سهولت و کثرت ارتکابش مهمترین و شایع ترین جرم اقتصادی فضای مجازی رایانه و اینترنت محسوب می شود هر چند به ظاهر در ارتکاب این جرم رایانه در حد وسیله جرم ظاهر می شود اما رایانه و اینترنت کلاهبرداری را توأم با کیفیات و شرایط غیر قابل انکاری می کنند که قانون گذاران ناگزیر به شناسایی جدید در کنار کلاهبرداری سنتی هستند. کلاهبرداری رایانه ای چون در دنیای جدید به نام دنیای مجازی رایانه و اینترنت با امکانات بیشماری تحقق می یابد فقط علیه انسان نیست و بلکه غالباً سیستم رایانه ای و نرم افزارهای آن است و بنابراین شرط فریب قربانی در آن تا مرز حذف شدن تضعیف می شود. موضوع جرم کلاهبرداری رایانه ای نیز فراتر از مال یا وسیله تحصیل مال است و شامل خدمات و امتیازات مالی و حتی داده های رایانه ای و دارای ارزش مالی نیز می شود (انصاری دوست، ۱۳۹۶:۱۴۲).

قوانین جرایم رایانه ای باید با رشد جرایم رایانه ای به روز شوند. تعیین کیفر مناسب برای جرایم رایانه ای جدید یک روند قانونی است که نیاز به بررسی جرم و آنچه در ایجاد جرم نقش داشته اند، دارد. هدف این مقاله ارائه روشی است تا باعث تسهیل کار قانونگذار در روند تعیین کیفر شود و به دنبال وقوع جرم، جرایم احتمالی که پیش از آن صورت گرفته شده اند را جستجو کرد و منشأ اصلی جرم را شناسایی کرد. در روش پیشنهادی می خواهیم فعالیت هایی که در فضای مجازی صورت میگیرد و منجر به نقض حقوق افراد میشود را شناسایی کرده و به تعریف جرایم رایانه ای پردازیم.

با ایجاد هست شناسی متکی بر جرایم رایانه ای و حقوق میتوان جرایم رایانه ای که در قانون جرایم رایانه ای ایران به صراحت ذکر نشده است را تعریف کرده و به هستی شناسی جرایم افزود. اگر فعالیتی در فضای مجازی منجر به پایمال شدن حقی از افراد شود، میتوان در صورت عدم وجود جرم متناظر، جرم جدیدی را متناظر با این عمل نافی حقوق تعریف نمود. همچنین هنگامیکه جرمی صورت گیرد به بررسی حقوق نقض شده پرداخته میشود. در صورتیکه حقی وجود داشته باشد و آن حق در هستی شناسی حقوق یافت نشود، حق جدید در صورت صحت به هستی شناسی حقوق افزوده میشود. با افزودن حق جدید میتوان با استفاده از حقوق مشابه به آن حق، جرایم جدیدی را تعریف نمود.

تاریخچه و چارچوب نظری در پیدایش جرم رایانه ای

با پیشرفت فناوری اطلاعات و ارتباطات، تحولاتی اساسی در زیست انسانی صورت گرفته است. آن دسته از رفتارهای انسانی که به شکل سنتی جرم تلقی میشد، امروز به شکل ترجمه ایده های مجرمانه به زبان خاص رایانه و یا از طریق فضای مجازی تحقق می یابد (افتخار جهرمی،

تاریخچه مشخصی از پیدایش جرم رایانه ای وجود ندارد ولی به هر حال این دسته از جرایم نتیجه فناوری اطلاعات دانست. کارشناسان رایانه بر این باورند که منشأ پیدایش جرم رایانه ای و اینترنتی به قضیه رویس^۱ باز می‌گردد. این شخص که بعد از بی‌مهری مسئولان یک شرکت فروش عمده میوه و سبزی به عنوان حسابدار آنها انتخاب شده بود از طریق رایانه اقدام به حسابرسی کرد و با تغییر قیمت‌ها و تنظیم درآمد جنس، مبلغی از مرجع آن را کاهش می‌داد و به حساب دیگری واریز می‌کرد. رویس با ظرافت خاصی قیمت‌ها را تغییر می‌داد، بعد از آن با نام هفده شرکت محل قرار داد، چک‌های جعلی صادر و از آن حساب برداشت می‌کرد به طوری که در کمتر از شش سال به بیش از یک میلیون دلار رسید، اما به علت نداشتن مکانیزمی برای توقف این روند، رویس خودش را به محاکم قضایی معرفی کرد و به ده سال زندان محکوم شد. به این ترتیب کارشناسان رایانه می‌گویند بر اساس مطالعات صورت گرفته زمینه پیدایش جرم رایانه ای این گونه به وجود آمده است.

بر اساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپ‌خانه و یک دانشجوی رایانه اقدام به جعل چک‌های تضمینی مسافرتی کردند و بعد از این بود که گروه‌های هکر جرم‌های دیگری را مرتکب شدند، مواردی چون جعل اسکناس، اسناد و بلیت‌های شرکت اتوبوسرانی، جعل اسناد دولتی از قبیل گواهی‌نامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک‌های مسافرتی و عادی بخشی از این جرایم رایانه‌ای هستند. مون^۲ و مک^۳ کلووسکی بیان می‌کند که جرایم رایانه‌ای به یک مسئله جهانی تبدیل شده است و همچنان به سرعت در حال رشد است. با این حال مطالعات کمی در مورد نظریه جرم و جنایت صورت گرفته است با استفاده از این مطالعه که از ۲۷۵۱ جوان کره‌ای صورت گرفت بررسی کردند که آیا خودکنترلی می‌تواند به عنوان یک چارچوب نظری برای کاهش جنایات رایانه‌ای مؤثر واقع شود یا خیر؟ نتایج مطالعات نشان داد که دانلود غیر قانونی نرم‌افزارها و استفاده غیر قانونی از هویت شخصی دیگران تا حدودی به خودکنترلی مربوط می‌شود. مطابق پیش‌بینی این نظریه‌ها متغیرهای فرصتی چون ساعات استفاده از رایانه به این پیش‌بینی کمک کرده است. هیگینس^۴ و فل با استفاده از یک نمونه مورد مطالعه از ۳۱۶ دانشجوی کالج نشان داد که بین خودکنترلی کم و دزدی نرم‌افزار یک رابطه مثبت وجود دارد. بر اساس گفته آدل^۵ و

1 - Theorem Rois

2 - Moon

3 - Mc Clasky

4- Higgins

5 - Audal

رومان^۱ رایانه و فناوری های مربوط با آن ابزاری ضروری هستند که جنبه های مختلف قابل توجهی از زندگی اجتماعی و شخصی از قبیل آموزش، کسب و کار، فرهنگ و فعالیت های اوقات فراغت را تحت تأثیر قرار می دهد. با استفاده گسترده از رایانه های شخصی و اینترنت با سرعت بالا انحرافات مربوط به رایانه و رفتارهای جنایی از قبیل هک کردن، بار گذاری موسیقی به صورت غیر قانونی و برنامه های نرم افزاری، سرقت رمز عبور دیگران و... به صورت قابل توجهی افزایش پیدا کرده است. با توجه به اهمیت موضوع تعداد فزاینده ای از مطالعات در سالهای اخیر به بررسی جنایات رایانه ای پرداخته اند. یار^۲، هیگنس و فوستر^۳ با تمرکز بر علت انحرافات رایانه ای و نظریه های جرم شناسی سنتی، از قبیل خود کنترلی، نظریه یادگیری اجتماعی - عقلانی و نظریه انتخاب توانستند انحرافات رایانه ای را مورد مطالعه و بررسی قرار دهند.

به طور کلی یافته های تجربی شواهدی را در ارتباط با توانایی نظریه های جرم شناسی سنتی در توضیح انواع مختلفی از جرایم مربوط به رایانه فراهم می کند. مک کواد^۴ بیان می کند که اگر چه مطالعات تجربی به بهبود درک درستی از جرایم رایانه ای کمک کند، اما محدودیت هایی نیز دارند. از جمله اینکه تعداد محدودی از مطالعات تجربی نظریه عمومی جرم را انحرافات رایانه ای را مورد بررسی قرار داده اند. با وجود ادعای این نظریات عدم خود کنترلی علت اصلی بسیاری از رفتارهای مجرمانه است. یک نظرسنجی که ویاسون و پاترسون در سازمان کسب و کار در ایالت متحده انجام داده اند متوجه شدند که ۶۴ درصد از کسب و کارهای منتشر شده حداقل از یک حادثه امنیتی رایانه زیان مالی دیده اند. با توجه به اهمیت موضوع تعداد فزاینده ایی از مطالعات انجام شده در سال های اخیر به بررسی انحرافات رایانه ای با تمرکز بر علت این انحرافات پرداخته اند.

دیدگاههای نظری در تقسیم بندی جرایم رایانه ایی

سه دیدگاه کلی در مورد تقسیم بندی جرایم رایانه ای و جرایم الکترونیکی وجود دارد. دیدگاه اول در نظر گرفتن طبقه بندی خاص و متمایز از جرایم سنتی است. دیدگاه دوم در نظر گرفتن طبقه بندی کلی جرایم سنتی این جرایم است؛ به این معنا که این جرایم را به جرایم علیه اشخاص، جرایم علیه اموال، جرایم علیه امنیت و آسایش عمومی تقسیم نموده و در یک قانون خاص با ذیل عناوین قوانین سنتی، هر جرم را ذیل یکی از عناوین جای می دهیم. دیدگاه سوم هم قائل به ظهور منافع جدید نیازمند حمایت (سخت افزار، نرم افزار، داده ها، حقوق خصوصی و فردی) در کنار منافع سنتی حمایت شده در حقوق جزا (اشخاص، اموال، امنیت و آسایش عمومی) می باشد.

1 - Roman

2 - Yar

3- Foster

4 - Me Quade

برخی از منتقدان به شدت با دیدگاه اول مخالف بوده و در نظر گرفتن یک طبقه بندی خاص برای جرائم رایانه‌ای را ناشی از آن می‌دانند که غالباً متخصصان رایان و نه حقوق دانان به تدوین مقررات مربوط پرداخته‌اند و حقوق دانان، که آشنایی کافی به این مقوله جدید نداشتند به حاشیه رانده شده‌اند. این عده معتقدند می‌بایست جایگاه جرائم رایانه‌ای نسبت به جرائم کاملاً شفاف باشد، تا از حیث سیاست جنایی بتوان در مورد جرایمی که منافع معینی را هدف خود قرار می‌دهند، واکنش یکسان نشان داد. به عنوان مثال جاسوس رایانه‌ای که امنیت عمومی کشور را خدشه دار می‌کند، می‌بایست از سیاست جنایی سایر جرائم علیه امنیت پیروی کند؛ در حالی اگر جرائم رایانه‌ای یک طبقه خاص در کنار طبقه بندی سنتی جرائم فرض کنیم که لزوماً از یک سیاست خاص جنایی تبعیت خواهند کرد، این امر محقق نخواهد شد. از سوی دیگر در نظر گرفتن یک طبقه خاص برای پاره‌ای از جرائم فقط به لحاظ اینکه از حیث وسیله ارتکاب جرم مشترکند، بدعتی جدید محسوب می‌شود و مستلزم آن است که قانونگذار کلاً طبقه بندی قبلی جرائم سنتی را که به کناری نهاده و یک طبقه بندی جدیدی مبنی بر وسیله ارتکاب جرم برای کلیه جرائم ارائه دهد. یکی از این منتقدین می‌نویسد: «هرچند عده‌ای جرائم مذکور را در تقسیمات مجزا جای داده و مرز تفکیک آنها را مشخص کرده‌اند، لیکن باید جایگاه هر یک از آنان را در حقوق جزا مشخص نماییم. این کار بدون شک از عهده متخصصین حقوق جزایی بر خواهد آمد که با علوم رایانه نیز تا حد کافی آشنا هستند (جاویدنیا، ۱۳۸۷: ۱۴۱). برای این کار می‌توان از دو روش استفاده کرد. در روش اول می‌توان جرائم مذکور را همانند جرائم علیه اموال یا جرائم علیه اشخاص، به عنوان یک سرفصل جدید قرار داد. عناوین مجرمانه‌ای که ممکن است از آنها واقع شود را در دوران این سرفصل‌ها قرار داد. در روش دوم می‌توان با توجه بیشتر، ابتدا جرائم داخل در هر عنوان را شناسایی و سپس هر یک را در سرفصل‌هایی که هم‌اکنون نیز وجود دارد، تزریق کرد. برای مثال در این روش شاید بتوان عمل هکرا در زمره اعمالی دانست که باعث تخریب اموال غیر یا اموال عمومی می‌گردد. به تبع این تقسیم بندی مرسوم در حقوق جزا، جرائم کامپیوتری نیز در طول دهه‌های اخیر بر حسب زمینه‌های اصلی جرم مورد مطالعه قرار گرفته‌اند و به همین لحاظ در مجموعه‌های قوانین کیفری کشورها عناوینی همچون جرائم اقتصادی کامپیوتری یا جرائم علیه حقوق خصوصی و فردی به چشم می‌خورد... آنچه مسلم است، در کنار منافع قضایی حمایت شده مرسوم در حقوق جزا، انواع جدیدی از روشها به وجود آمده است که نیازمند حمایت حقوقی‌اند و به همین جهت علاوه بر اشخاص اموال امنیت و آسایش عمومی بایستی داده‌ها، اطلاعات برنامه‌های کامپیوتری و به طور کلی سیستم‌های کامپیوتری از لحاظ صحت و درستی، قابلیت دسترسی و قابلیت اطمینان یا محرمانه بودن، از سوی مقررات کیفری

مورد ضمانت واقع شوند؛ بر همین مبنا می توان چنین نتیجه ای گرفت که دسته بندی جرایم از یک سو شامل جرایم علیه اشخاص، جرایم علیه اموال و جرایم علیه امنیت و آسایش عمومی و از سوی دیگر، شامل جرایم علیه سخت افزار، جرایم علیه نرم افزار، جرایم علیه داده ها و جرایم علیه حقوق خصوصی و فردی می باشد. در جمع بندی و مقایسه این سه دیدگاه می توان گفت، شیوه مطلوب در جرم انگاری، همان است که کشورهای توسعه یافته از جمله فرانسه، آلمان و... پیش گرفته اند و از جرم انگاری های پراکنده خودداری می کنند و با در نظر گرفتن یک مجموعه قوانین جزایی واحد با شماره بندی خاص مواد، که افزودن مواد جدید را در آن جای می دهند و به صورت هماهنگ با پیشرفت و تحول جامعه، آن مواد را الحاق یا اصلاح می کنند.

اقسام طبقه بندی نظری جرایم رایانه ای

محققان طبقه بندی های مختلفی را برای جرایم رایانه ای در نظر گرفته اند که هر کدام در جای خود مفید و قابل استفاده است در ادامه به برخی از این طبقه بندی ها اشاره می کنیم.

الف. بر اساس منافع مورد حمله

پروفسور اولریش زیبر، بر اساس منافع مورد حمایت قوانین سنتی یک تقسیم بندی به شرح ذیل

ارائه داده است

الف- جرائم رایانه ای علیه اموال و مالکیت (جرائم اقتصادی):

الف-۱- کلاهبرداری رایانه ای از طریق دستکاری رایانه ای و سیستمهای پردازش شده

الف-۲- جاسوسی رایانه ای و سرقت نرم افزار

الف-۳- خرابکاری رایانه ای

الف-۴- سرقت خدمات

الف-۵- دسترسی غیر مجاز به سیستمهای پردازش داده ها

الف-۶- جرایم اقتصادی سنتی به کمک پردازش داده ها (تغییر صورت درآمدها و داراییهای

که در رایانه نگهداری می شوند برای فرار مالیاتی)

ب: جرایم رایانه ای علیه حقوق فردی و خصوصاً حریم خصوصی

ب-۱- دستکاری و حذف داده های شخصی توسط اشخاص غیر مجاز

ب-۲- جمع آوری، پردازش و انتشار داده های شخصی کاذب توسط دارنده قانونی آنها

ب-۳- جمع آوری و ذخیره غیر قانونی داده های صحیح

ب-۴- افشای غیر قانونی و سوءاستفاده از داده ها

ب-۵- نقض تشریفات قانونی حمایت از داده های شخصی

ج- جرایم رایانه ای علیه منافع جمعی:

- ج- ۱- جرایم علیه امنیت ملی
ج- ۲- جرایم علیه تمامیت جسمانی اشخاص
ج- ۳- جرایم علیه کنترل فرامرزی داده‌ها
ج- ۴- جرایم علیه تمامیت رویه‌های رایانه‌ای و شبکه‌های داده‌ای ارتباطی
ج- ۵- جرایم علیه مشروعیت دموکراتیک مصوبات پارلمان در مورد رایانه (نوری، ۱۳۸: ۲۰).

ب. بر اساس جایگاه رایانه در ارتکاب جرم

بر این اساس جرایم رایانه‌ای به سه دسته تقسیم می‌شوند:

الف: جرایم رایانه‌ای که در آنها رایانه هدف و موضوع جرم واقع شوند:

نفوذگری

خرابکاری رایانه‌ای

سرقت اطلاعات یا خدمات رایانه‌ای

ب: جرایم رایانه‌ای که در آنها رایانه وسیله جرم واقع می‌شود:

ب- ۱- جرایمی که رایانه تنها وسیله ارتکاب و جزء عنصر مادی آنها است:

کلاهبرداری رایانه‌ای

جعل رایانه‌ای

۲- جرایمی که رایانه وسیله منحصر به فرد ارتکاب و جزء عنصر مادی آنها نیست:

هرزه‌نگاری کودکان

توهین

ج: جرایم رایانه‌ای که در آنها رایانه مستقیم هدف یا وسیله جرم واقع نشده است؛ بلکه اطلاعات غیر مجاز حاصل از جرم در رایانه ذخیره یا پردازش یا منتقل شده است. مانند ذخیره سازی تصاویر هرزه‌نگاری کودکان در یک رایانه.

ج. بر اساس فلسفه نیاز به قانونگذاری

بر این اساس جرایم رایانه‌ای بر دو دسته اند:

الف: جرایم رایانه‌ای سنتی؛ جرایم رایانه‌ای قابل مجازات با قوانین مربوط به جرایم کلاسیک:

الف- ۱- جرایم رایانه‌ای علیه اشخاص؛ مانند قتل نفس (از طریق دستکاری رایانه بیمارستان)،

ایراد ضرب و جرح عمدی از طریق (طراحی ناقص یک محصول رایانه‌ای به صورت عمدی)،

توهین و نشر اکاذیب

الف- ۲- جرایم رایانه‌ای علیه اموال؛ مانند کلاهبرداری سنتی (از طریق تبلیغات موهوم در

اینترنت)، و تخریب (با اختلال در برنامه زمان بندی و مسیر حرکت هواپیما و یا قطار)،

الف - ۳- جرایم علیه امنیت و آسایش عمومی

الف - ۴- جرایم علیه عصمت و عفت و اخلاق حسنه

الف - ۵- جرایم علیه خامواده (مانند فریب در ازدواج از طریق اینترنت)

ب: جرایم رایانه ای مدرن؛ جرایم رایانه ای غیر قابل مجازات با قوانین سنتی و نیازمند قانون گذاری جدید:

ب - ۱- جرایمی که قبل از پیدایش فناوری اطلاعات ارتکاب آنها متصور نبوده است؛ مانند جرایم علیه محرمانگی، تمامیت و قابلیت دسترسی داده ها و سیستمهای رایانه ای یا نقص حقوق پدیدآورندگان نرم افزار های رایانه ای

ب - ۲- جرایمی که تفاوت ماهیتی با نوع کلاسیک شان موجب جرم انگاری نوع رایانه ای آنها شده است، هرچند نام و نتیجه شان با نوع کلاسیک آنها یکسان است؛ مانند جعل و کلاهبرداری رایانه ای جرایمی که صرفاً خطرناکتر شدن آنها نسبت به نوع کلاسیک شان موجب جرم انگاری نوع رایانه ای، آنها شده است و در ماهیت، نام و نتیجه هیچ تفاوتی با نوع کلاسیک ندارند؛ مانند هرزه نگاری کودکان و اعمال دارای ماهیت نژاد پرستانه.

علل محیطی بزهکاری رایانه‌ای

خاستگاه توجه جرم‌شناسان و دانشمندان علوم جنایی به محیط و عوامل جامعه شناختی جرم، به قرن هجدهم بازمیگردد. با پیدایش گرایش‌های جامعه‌شناسانه، کانون توجه مطالعات جرم‌شناسی از بزهکار به محیط جغرافیایی و فیزیکی پیرامون وی معطوف شد. نخستین مکتب در زمینه جامعه‌شناسی جنایی و توجه به عوامل محیطی مؤثر در ارتکاب جرم، مکتب جغرافیای جنایی است که با نظریات گری و کیتل بر اساس مطالعات آماری مطرح شد. آنها بر این باور بودند که بزهکاری تابعی از نحوه استقرار شهرها، فصول و شرایط اقلیمی و آب‌وهوا است و با توجه به همین مطالعات قانون حرارتی بزهکاری را بنیان نهادند و به بررسی نقش آب و هوا و شرایط جوئی و تأثیر آن بر روی جرم و کیفیت ارتکاب جرم پرداختند. در همان دوره، به رابطه بین بحران اقتصادی و بزهکاری نیز توجه ویژه‌ای شد. فقر به عنوان یکی از جلوه‌های بارز بحران اقتصادی، به مثابه یکی از عوامل محیطی مؤثر در افزایش ارتکاب جرم و انحراف مطرح شد. صرفنظر از مردود انگاشته شدن این نظریه‌ها و استدلال‌های مربوط به آن، از آنجا که این نظریه‌ها نخستین گام در آغاز دوران جرم‌شناسی علمی و مبنایی برای شکل‌گیری مطالعات محیطی بودند، از اهمیت قابل توجهی برخوردارند (نجفی ابرندآبادی، ۱۳۷۵: ۳۳۴).

توجه به عوامل محیطی در آموزه‌های مکتب تحقیقی به اوج خود رسید و اگر تا پیش از این مطالعات محیطی بر پایه اصول فلسفی و اخلاقی صورت می‌گرفت، در این دوره رنگ علمی به خود

گرفت. به باور آنریکوفری، بنیانگذار جرم‌شناسی کاربردی و جامعه‌شناسی جنایی، در شناخت علل وقوع جرم از تأثیر محیط نباید غافل شد. به باور وی، محیط اجتماعی گاهی آنچنان وضع آسان-کننده‌های پدید می‌آورد که افراد سالم نیز دچار وسوسه میشوند و به ارتکاب جرم تن در میدهند (اردبیلی، ۱۳۸۳: ۹۶).

دلایل ماهیت فرامرزی جرایم رایانه‌ای و ادله اینترنتی

امروزه مجرمین رایانه‌ای می‌توانند فارغ از مرزهای ملی به ارتکاب جرم بپردازند. از اینرو جرایم رایانه‌ای به راحتی در مقیاسی بین‌المللی ارتکاب می‌یابند. از طرفی امروزه ادله دیگر جرایم نیز در بسیاری از موارد از نوع ادله اینترنتی هستند که در سرورهای خارجی ذخیره می‌شوند. در نتیجه تعقیب این جرایم و انجام تحقیقات کیفری پیرامون آن‌ها مستلزم دسترسی به داده‌های فرامرزیست. فرامرزی بودن ادله جرم موضوع اعمال فرامرزی قوانین داخلی را مطرح می‌نماید. با اینحال امور کیفری از جمله امور داخلی دولت‌ها هستند و اعمال فرامرزی قوانین کیفری داخلی در مغایرت با اصل حاکمیت سرزمینی دولت‌ها قرار دارد. از اینرو دولت‌ها برای دسترسی به داده‌های فرامرزی ناگزیر از همکاری با یکدیگر از طریق معاضدت قضایی مقابل هستند. استفاده فزاینده از رمزنگاری ارتباطات آنلاین موجب شده تا دسترسی دولت‌ها به داده‌های فرامرزی بیش از پیش اهمیت یابد. دسترسی به محتوای ارتباطات اینترنتی رمزنگاری شده به راحتی امکان‌پذیر نیست و مستلزم دسترسی به داده‌های ابرهای رایانه‌ای می‌باشد. اطلاعات ابرهای رایانه‌ای نیز اغلب در سرورهای خارجی ذخیره می‌شوند و دسترسی به آن‌ها از طریق معاضدت قضایی ممکن می‌باشد (اسویر^۱، ۲۰۱۲: ۲۰۰).

برای دهه‌ها تلفن فناوری ارتباطی اصلی به شمار می‌رفت و دولت‌ها می‌توانستند از شنود مکالمات تلفنی برای انجام تحقیقات کیفری استفاده نمایند. حتی پس از فراگیر شدن ارتباطات اینترنتی، دولت‌ها همچنان می‌توانستند از طریق شرکت‌های محلی ارائه خدمات اینترنتی به محتوای ارتباطات دسترسی یابند. با اینحال تهدیدات امنیتی و مقتضیات مربوط به حفظ حریم خصوصی در یک دهه اخیر شرکت‌های ارائه خدمات اینترنتی را به رمزنگاری ارتباطات اینترنتی واداشته است. امروزه تجارت الکترونیک بر رمزنگاری داده‌ها متکی می‌باشد. در چنین شرایطی دولت‌ها نمی‌توانند به سیاق سابق به محتوای ارتباطات اینترنتی دسترسی پیدا کنند. از اینرو دولت‌ها می‌باید پیش از رمزنگاری شدن داده‌ها توسط شرکت‌های ارائه خدمات اینترنتی به آن‌ها دسترسی یابند. در اینجاست که معاضدت قضایی متقابل اهمیت می‌یابد.

دشواری‌های موجود در تعقیب جرایم رایانه‌ای و ناکارآمدی همکاری‌های بین‌المللی در این زمینه دولت‌ها را بر آن داشته تا داده‌های کاربران داخلی را پیش از انتقال آن‌ها به سرورهای خارجی در داخل ذخیره نمایند تا در صورت لزوم به آن‌ها دسترسی مستقیم داشته باشند. به این منظور دولت‌ها شرکت‌های ارائه‌دهنده خدمات اینترنتی را ملزم می‌نمایند تا از سرورهای داخلی برای ارائه خدمات اینترنتی در قلمروی آن‌ها استفاده نمایند. داخلی سازی داده‌ها پیامدهای اقتصادی نامطلوبی خواهد داشت. امروزه تجارت اینترنتی بر ارتباط آسان با مشتریان بین‌المللی مبتنی است. شبکه جهانی اینترنت یافتن بازارهای بین‌المللی را ممکن ساخته است (اسویر^۱، ۲۰۱۷: ۷۱۳). داخلی سازی داده‌ها هزینه هنگفتی را بر تجارت اینترنتی تحمیل می‌نماید. همچنین مشکلات فنی بسیاری را برای شرکت‌های ارائه‌دهنده خدمات اینترنتی به وجود خواهد آورد و هزینه خدمات اینترنتی را افزایش خواهد داد. ذخیره سازی داخلی داده‌ها همچنین خطر نقض حریم خصوصی و حق آزادی بیان کاربران توسط دولت‌ها را افزایش می‌دهد. ناکارآمدی و کندی فرآیندهای معاضدت قضایی متقابل همچنین موجب گشته تا برخی از دولت‌ها درصدد اعمال فراسرزمینی قوانین خود برآیند. روشن است که تلاش دولت‌ها برای اجرای قوانین خود در ویرای مرزهایشان سبب به وجود آمدن اختلافات جدی بین‌المللی خواهد شد. به علاوه در چنین شرایطی شرکت‌های ارائه خدمات اینترنتی ناگزیر از رعایت قوانین کشورهای مختلف خواهند بود و که فعالیت‌های تجاری آنان را به شدت تحت تأثیر قرار خواهد داد. داخلی سازی داده‌ها و اعمال فراسرزمینی قوانین داخلی بزرگترین خطراتی هستند که امروزه اینترنت آزاد و ساختار جهانی آن را تهدید می‌نمایند و ناکارآمدی رژیم معاضدت قضایی بر دامنه این تهدیدات افزوده است. چنانچه دولت‌ها بتوانند از طریق معاضدت قضایی به نحو مؤثری برای تعقیب جرایم رایانه‌ای با یکدیگر همکاری نمایند انگیزه آن‌ها برای داخلی سازی داده‌ها و اعمال فرامرزی قوانین داخلی کاهش خواهد یافت (اسویر^۲، ۲۰۱۷: ۷۱۴).

اشکال معاضدت قضایی متقابل در زمینه جرایم رایانه‌ای

بین ۳۰ تا ۷۰ درصد جرایم رایانه‌ای دارای ابعاد فرامرزی هستند (دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد^۳، ۲۰۱۳: ۲۴). داده‌های رایانه‌ای می‌توانند فارغ از مرزهای ملی بر روی هر سیستم رایانه‌ای متصل به شبکه جهانی اینترنت ذخیره شوند. در نتیجه ممکن است داده‌های مربوط به یک جرم رایانه‌ای که در واقع ادله الکترونیکی آن جرم هستند در جایی خارج از قلمروی دولت تعقیب کننده جرم ذخیره شده باشند. بنابراین تعقیب مؤثر جرم مستلزم دسترسی فرامرزی

۱. Swire

۱. Swire

۱. UNODC

دولت تعقیب کننده به ادله مذکور خواهد بود. با این حال امور کیفری در انحصار مطلق دولت‌ها قرار دارد و مطابق اصول عدم مداخله و تساوی حاکمیت‌ها هیچ دولتی نمی‌تواند در قلمروی دولت دیگری به انجام تحقیقات کیفری بپردازد مگر به موجب معاهده یا شکل دیگری از اعلام رضایت آن دولت. مطابق حقوق بین‌الملل مأموران تحقیق بایستی در تحقیقات خود حاکمیت ملی سایر دولت‌ها را محترم بدانند (روت^۱، ۲۰۰۵: ۱). در نتیجه همکاری دولت‌ها برای تعقیب مؤثر جرایم رایانه‌ای ضروری و اجتناب‌ناپذیر می‌باشد. معاضدت قضایی متقابل سازگار است که در آن دولت‌ها از اختیارات شکلی خود برای کمک به تعقیب جرم توسط دولتی دیگر و دسترسی آن دولت به ادله فرامرزی استفاده می‌نمایند. ۷۰ درصد همکاری‌های بین‌المللی در زمینه جرایم رایانه‌ای در چارچوب معاضدت متقابل صورت می‌گیرد (دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد^۲، ۲۰۱۳: ۲۰۱). اجرای درخواست‌های معاضدت برای تعقیب جرایم رایانه‌ای تنها در صورتی ممکن خواهد بود که قوانین داخلی به نحو هماهنگی ابزارهای شکلی مناسب برای تعقیب این نوع جرایم را پیش‌بینی نموده باشند. از اینرو معاضدت متقابل مؤثر منوط به هماهنگی قوانین شکلی دولت‌های طرف همکاری است. به طور مثال چنانچه دولتی از اختیار قانونی برای حفاظت فوری از داده‌های رایانه‌ای برخوردار نباشد دیگر دولت‌ها نمی‌توانند انجام آن را از دولت مذکور درخواست نمایند. به عبارت دیگر اقداماتی که در چارچوب معاضدت متقابل قابل انجامند قانوناً همان اقداماتی هستند که دولت‌ها در تحقیقات کیفری داخلی مجاز به انجام آن‌ها می‌باشند.^۳ ادله الکترونیکی می‌توانند به صورت از راه دور در سرور و یا رایانه‌ای در آن سوی کره زمین ذخیره شوند.

این امکان است که از ساختار جهانی شبکه اینترنت ناشی می‌گردد. برخی از شرکت‌های تجاری داده‌های مربوط به شعبات و نمایندگی‌های خارجی را در مقر اصلی شرکت ذخیره می‌نمایند. به عنوان مثال با اینکه شرکت اینترنتی آمریکا آنلاین^۴ در ایالات متحده، اروپا و آسیا به ارائه خدمات اینترنتی می‌پردازد اما تمام داده‌های کاربران خود را در مقر خود در رستون^۵ ویرجینیا ذخیره می‌

۲. Roth

۳. UNODC

۴. در برخی موارد دولت‌ها انجام اقداماتی را از یکدیگر درخواست می‌نمایند که در قانون دولت مورد درخواست پیش‌بینی نشده‌اند. اسناد حاکم بر معاضدت قضایی متقابل به طور معمول صراحتاً دولت‌ها را ملزم به انجام چنین اقداماتی نمی‌نمایند. با اینحال مطابق بند ۱ ماده ۱۰ مقررات اروپایی تحقیقات (European Investigation Order) در صورتی که اقدام درخواست شده در قانون دولت مورد درخواست پیش‌بینی نشده باشد بایستی از اقدامات جایگزین استفاده گردد.

4. America Online

5. Reston, Virginia

نماید (سومن^۱، ۱۹۹۸: ۴۷۱) بنابراین چنانچه دو فرد در ژاپن از خدمات این شرکت برای نامه نگاری اینترنتی استفاده کنند تمام داده‌های مربوط به ارتباط اینترنتی آنان در ایالات متحده ذخیره می‌گردد. در نتیجه چنانچه مقامات ژاپنی به منظور تعقیب یک جرم رایانه‌ای در صدد کنترل ارتباط اینترنتی میان آن دو برآیند برای دسترسی به داده‌ها ناگزیر از جلب همکاری مقامات آمریکایی خواهند بود. گذشته از این ممکن است داده‌ها عمده^۲ در کشور دیگری ذخیره گردند تا دسترسی مقامات داخلی به آن‌ها میسر نباشد. با عمومیت یافتن استفاده از ابرهای رایانه‌ای^۳ مجرمان رایانه‌ای می‌توانند داده‌های خود را بر روی یک سرور اینترنتی خارجی ذخیره نمایند. از اینرو دولت‌ها برای دسترسی به داده‌های فرامرزی و بررسی آن‌ها بایستی تفتیش و توقیف داده‌های مذکور را از دولت محل ذخیره داده‌ها تقاضا نمایند.^۴ چنانچه داده‌های مورد نظر در معرض حذف یا دستکاری قرار داشته باشند تسریع در اجرای تقاضای توقیف داده‌ها حیاتی خواهد بود. معاضدت قضایی برای تفتیش و توقیف داده‌ها بیش از اقسام دیگر معاضدت قضایی برای تعقیب جرایم رایانه‌ای مورد استفاده دولت‌ها قرار می‌گیرد چرا که این نوع معاضدت دسترسی کامل به داده‌های فرامرزی و بررسی دقیق آن‌ها را میسر می‌سازد (Westmoreland, 2015, 230).

قسمت عمده زیرساخت‌های اینترنتی در کنترل شرکت‌های ارائه دهنده خدمات اینترنتی قرار دارد. از اینرو بخش اعظم داده‌های مربوط به ارتباطات اینترنتی در اختیار بخش خصوصی می‌باشد. استفاده مأموران تحقیق از اقدامات قهری نظیر تفتیش و توقیف در بیشتر موارد به دلیل حجم بالای پرونده‌ها، پیچیدگی‌های سیستم‌های رایانه‌ای، حجم بالای داده‌های ذخیره شده، عمومیت یافتن اقدامات امنیتی برای حفظ حریم خصوصی و نیز به دلیل ایجاد اخلاص در فعالیت‌های رایانه‌ای قانونی غیر ممکن می‌باشد (انگرز^۵، ۲۰۰۴: ۴۶). از اینرو ممکن است مأموران تحقیق نتوانند به داده‌های مورد نظر دست یابند. در این موارد دولت محل ذخیره داده‌ها بایستی بنا به درخواست دولت تعقیب کننده جرم حکمی موسوم به حکم ارائه داده‌ها^۶ را صادر نماید. به موجب حکم مذکور ارائه دهندگان خدمات اینترنتی و یا سایر اشخاصی که کنترل داده‌های رایانه‌ای مورد نظر را در اختیار دارند، با دستور مقامات ذی صلاح ملزم به جستجو، شناسایی و ارائه داده‌ها به مقامات

۳. Sussmann

۲. ابر رایانه‌ای به سیستمی متشکل از یک رایانه مرکزی اطلاق می‌شود که کاربران مختلف از سراسر جهان می‌توانند داده‌های خود را به وسیله شبکه اینترنت بر روی آن ذخیره کنند. این سیستم کاربران را قادر می‌سازد تا بدون نیاز به ذخیره‌سازی داده‌ها در رایانه‌های شخصی یا سازمانی، در هر زمان و هر مکان از طریق شبکه اینترنت به داده‌های مذکور دسترسی یابند.
۳. معاضدت متقابل برای تفتیش و توقیف داده‌های رایانه‌ای در ماده ۳۱ کنوانسیون بوداپست و ماده ۳۹ کنوانسیون اتحادیه عرب پیش‌بینی شده است.

۶. Westmoreland

۱. Angers

6. Production Order

می‌باشند، به صورتی که مقامات بتوانند از داده‌های ارائه شده به عنوان ادله استفاده نمایند. یکی از ویژگی‌های ادله الکترونیکی قابلیت دستکاری، انتقال و یا حذف فوری و آسان آن‌ها از راه دور است.^۱ ممکن است این تغییرات نتیجه اقدامات مرتکبین برای از بین بردن آثار و ادله جرم باشد و یا در نتیجه اقدامات معمول شرکت‌های ارائه دهنده خدمات اینترنتی از جمله حذف داده‌های ترافیکی^۲ به وجود آید. در هر صورت ممکن است ادله الکترونیکی حتی پیش از ارسال درخواست معاضدت از بین بروند. روش‌های سنتی جمع‌آوری ادله فرامرزی بسیار کند هستند چرا که طی شدن روندهای قانونی توسط دولت‌های خارجی و تکمیل فرآیندهای دیپلماتیک معمول بسیار زمانبر است. به علاوه ممکن است مأمورین تحقیق بلافاصله پس از ارتکاب یک جرم رایانه ای منشأ آن را شناسایی نمایند اما قادر به جمع‌آوری و ارائه فوری اطلاعاتی به دولت محل ذخیره داده‌ها نباشند. هر چه زمان بیشتری برای ارائه این اطلاعات مورد نیاز باشد احتمال از بین رفتن یا دستکاری ادله الکترونیکی بیشتر خواهد شد (کلی‌فورد و کلونی^۳، ۱۹۹۰: ۷۵). استفاده از روش‌های سنتی در رابطه با فناوری‌های نوین همیشه مؤثر و نتیجه‌بخش نیست. صدور حکم تفتیش و توقیف و یا صدور دستور ارائه داده‌ها فرآیند زمانبر است و ممکن است داده‌ها در خلال آن حذف یا دستکاری گردند. از اینرو مقامات دولت محل ذخیره داده‌ها بایستی بنا به درخواست دولت تعقیب‌کننده جرم، ارائه‌دهندگان خدمات اینترنتی را با صدور حکمی ملزم به ذخیره نمودن داده‌ها نمایند تا مانع از حذف یا دستکاری داده‌ها شوند. در غیر این صورت حذف و دستکاری داده‌ها ممکن است انجام تحقیقات کیفری را با مانع جدی مواجه سازد. حفاظت سریع از داده‌های رایانه‌ای ذخیره شده^۴ به مقامات امکان می‌دهد تا انتقال داده‌های مورد نظر توسط ارائه‌دهندگان خدمات اینترنتی را ردیابی نمایند.^۵ طبیعتاً دستور قضایی برای حفاظت سریع از داده‌های ذخیره شده دستوری موقتیست و تنها تا زمانی اجرا خواهد شد که دولت محل ذخیره داده‌ها در مورد درخواست تفتیش و توقیف داده‌ها تصمیم‌گیری نماید. به طور کلی استفاده از این اختیار شکلی

1. Kettle, M. & Bowcott, O., Computer Crime: The Age of Digital Sleuth, The Guardian, 12 December 1997.

۲. داده‌های ترافیکی داده‌هایی هستند که اینترنت و دیگر سیستم‌های ارتباط از راه دور از آن‌ها برای شناسایی و تعیین موقعیت مبدا و مقصد یک ارتباط استفاده می‌کنند و برقراری ارتباط و جابجایی داده‌های محتوایی را در مسیر میان مبدا و مقصد ارتباط میسر می‌سازند. مأموران تعقیب جرم از داده‌های ترافیکی برای ردیابی ارتباطات از راه دور و مدت و حجم آن استفاده می‌کنند.

۵. Clifford & Connolly

4 Expedited Preservation of Stored Computer Data

۵. معاضدت متقابل در زمینه حفاظت سریع از داده‌های رایانه‌ای در ماده ۱۷ کنوانسیون بوداپست و ماده ۲۴ کنوانسیون اتحادیه عرب پیش‌بینی شده است.

یک اقدام موقتی برای تضمین حفظ داده‌ها تا زمان صدور حکم قضایی مناسب است. حفاظت از داده‌ها را نباید با الزام به حبس داده‌ها^۱ یکسان دانست. حبس داده‌ها یک الزام قانونیست که به موجب آن ارائه‌دهندگان خدمات اینترنتی ملزم هستند تا داده‌های مربوط به همه کاربران را برای یک دوره زمانی مشخص جمع‌آوری و حفظ نمایند. هدف از حبس داده‌ها آنست که دسترسی به داده‌ها برای انجام تحقیقات کیفری امکان‌پذیر باشد. امروزه تعقیب جرم در بسیاری از موارد مستلزم ردیابی ارتباطات اینترنتی مظنونین است و تأخیر در آن موجب عدم موفقیت در تعقیب جرم خواهد شد. ردیابی ارتباطات اینترنتی نیز مستلزم دسترسی به داده‌های ترافیکیست. با اینحال ممکن است داده‌های ترافیکی هرگز ذخیره نشوند و در طی ارتباطات موقتی ایجاد شده و بلافاصله از بین بروند. داده‌های ترافیکی اغلب پس از مدت کوتاهی به صورت خودکار حذف می‌شوند چرا که این داده‌ها پس از اتمام فرآیند برقراری ارتباط اینترنتی دیگر مورد نیاز نیستند و شرکت‌های ارائه‌دهنده خدمات اینترنتی به دلایل اقتصادی آن‌ها را حذف می‌کنند. در نتیجه ردگیری ارتباطات اینترنتی مستلزم جلوگیری از حذف داده‌های ترافیکی مورد نظر می‌باشد. از اینرو چنانچه از خدمات یک شرکت خارجی برای برقراری ارتباط اینترنتی مورد نظر استفاده شده باشد دولت تعقیب کننده جرم بایستی از دولت متبوع آن شرکت درخواست نماید تا مانع از حذف داده‌های ترافیکی مورد نظر شود و آن‌ها را ذخیره نماید.^۲

از آنجا که ممکن است داده‌ها در مسیر انتقالشان از مبدا به مقصد از کشورهای متعددی عبور نمایند حفاظت از داده‌های ترافیکی باید در تمامی کشورهایی که در مسیر انتقال داده‌ها قرار دارند صورت پذیرد. از اینرو تقاضا از دولت محل ذخیره داده‌ها برای افشای سریع داده‌های ترافیکی ذخیره شده^۳ جهت شناسایی مسیر انتقال داده‌ها ضروری می‌باشد (کونکیل یا اروپا^۴، ۲۰۰۸: ۳).^۵ افشای داده‌های ترافیکی تنها تا حدی ضروریست که برای ردیابی ارتباطات اینترنتی کافی باشد.^۶ این اقدام یکی از ابزارهای مهم همکاریست چرا که امروزه شرکت‌های ارائه‌دهنده خدمات اینترنتی در حوزه‌های قضایی مختلف پراکنده‌اند و ردیابی موفقیت‌آمیز یک ارتباط اینترنتی معمولاً مستلزم همکاری تمامی ارائه‌دهندگان خدمات اینترنتی در زنجیره انتقال داده‌هاست. در مواردی که مأموران تحقیق از اطلاعات مبادله شده در ارتباطات اینترنتی مظنونین اطلاعی در دست ندارند

1. Data Retention

۲. معاضدت متقابل در زمینه جمع‌آوری آنی داده‌های ترافیکی در ماده ۳۳ کنوانسیون بوداپست و ماده ۴۱ کنوانسیون اتحادیه عرب پیش‌بینی شده است.

3. Expedited Disclosure of Preserved Traffic Data

۲. Council of Europe

۵. معاضدت متقابل در زمینه افشای داده‌های ترافیکی در بند ۱ ماده ۳۰ کنوانسیون بوداپست و ماده ۳۸ کنوانسیون اتحادیه عرب پیش‌بینی شده است.

۶. بند ۱ ماده ۳۰ کنوانسیون بوداپست

کنترل داده‌های محتوایی^۱ ابزار مهمی برای تعقیب جرم است. ازینرو دولت‌ها بایستی داده‌های محتوایی ارتباطات مذبور را بنا به درخواست دولت تعقیب کننده جرم کنترل نماید.^۲ کنترل داده‌های محتوایی^۳ اغلب در مورد جرایم مهمی ممکن است که در حقوق داخلی تعریف شده‌اند.^۴ بدیهیست که کنترل داده‌های محتوایی بیشتر از کنترل داده‌های ترافیکی و کنترل داده‌های مربوط به اشتراک اینترنتی،^۵ حریم خصوصی و حقوق فردی اشخاص را تهدید می‌نماید. بنابراین در برخی از کشورها صدور حکم کنترل داده‌های محتوایی قانوناً تنها در رابطه با جرایم خاصی که در قوانین فهرست شده‌اند و یا حد معینی از مجازات را در پی دارند ممکن می‌باشد (انگرس^۶، ۲۰۰۴: ۴۷). این کشورها بایستی رویکرد خود را مورد بازبینی قرار دهند چرا که کنترل داده‌های محتوایی اغلب باید به سرعت و پیش از آنکه مأموران تحقیق به قابل کنترل بودن ارتباط مورد نظر پی‌برند انجام گیرد و ممکن است در خلال مدتی که برای بررسی این موضوع لازم است فرصت کنترل داده‌ها از بین برود. یکی از مشکلاتی که مأموران تحقیق در کنترل داده‌های محتوایی با آن مواجه هستند استفاده مجرمان رایانه‌ای از فناوری رمزنگاریست. مرتکبان می‌توانند دسترسی مأمورین تحقیق به داده‌های محتوایی را با استفاده از این فناوری دشوار سازند چرا که رمزگشایی از داده‌ها بدون دسترسی به کلید رمز بسیار زمانبر خواهد بود. معاهدات معاضدت قضایی در زمینه جرایم رایانه‌ای بایستی ارائه خدمات رمزگشایی را نیز پیش‌بینی نمایند و دولت‌ها بایستی متعهد به ارائه این نوع خدمات به یکدیگر باشند. ممکن است داده‌هایی که در چارچوب معاضدت قضایی در دسترس مقامات یک دولت خارجی قرار می‌گیرد داده‌های رمزنگاری شده باشند. در این صورت داده‌های مذبور کارایی چندانی برای مقامات تحقیق خارجی نخواهند داشت و از آنجا که دولت محل ذخیره داده‌ها از موقعیت بهتری برای دستیابی به کلید رمز برخوردار است بایستی در زمینه رمزگشایی داده‌ها با مقامات خارجی همکاری نماید.

۱. داده‌های محتوایی داده‌هایی هستند که محتوای یک ارتباط اینترنتی را تشکیل می‌دهند.

۲. معاضدت متقابل در زمینه کنترل داده‌های محتوایی در ماده ۳۴ کنوانسیون بوداپست و ماده ۴۲ کنوانسیون اتحادیه عرب پیش‌بینی شده است.

3. Interception of Content Data

۴. بند ۱ ماده ۲۱ کنوانسیون بوداپست

۵. داده‌های مربوط به اشتراک اینترنتی داده‌هایی هستند که نشانی‌های اینترنتی را به اشخاصی که از آن‌ها استفاده می‌کنند مربوط می‌سازند. به وسیله این داده‌ها می‌توان به هویت کاربر خدمات اینترنتی، موقعیت جغرافیایی یا آدرس پستی وی، نوع خدمات و امکانات فنی مورد استفاده و مدت زمان آن پی برد.

نتیجه گیری

با رشد روزافزون فناوری اطلاعات و خدمات اینترنت، فعالیت های مجرمانه نیز در فضای مجازی افزایش می یابند. چالشی که سازمان قضایی با آن مواجه است، تعیین مجازات و کیفر برای مجرمان می باشد؛ زیرا قوانین جرایم رایانه ای متناسب با رشد فناوری اطلاعات به روزرسانی نمی شوند و در نتیجه پس از وقوع جرم جدید، تعیین کیفر برای آن جرم توسط قانون گذار، کاری زمان بر و دشوار است. قوانین جرایم رایانه ای باید طوری تدوین شوند که همه شمول بوده و خلأ و حفره های قوانین را پوشش دهد.

هدف از ایجاد هستی شناسی جرایم رایانه ای این است که زبانی مشترک برای بیان جرم بوجود آید و آنچه که در قانون جرایم رایانه ای مسکوت مانده است، نشان دهد و به کمک این هستی-شناسی بتوان جرایم رایانه ای که جدید هستند و در قانون جرایم رایانه ای به صراحت بیان نشده اند را پوشش دهد.

حقوق افراد هنگامی ضایع میشود که جرمی صورت گرفته باشد و در صورت وقوع جرم از سوی مجرم، آسیبی به قربانی وارد میشود. قربانی متشکل از یک فرد و یا افراد جامعه است و با صدمه ای که از وقوع جرم میبیند، حقی از او ضایع میشود. اگر حقوق نقض شده مصداق جرمی باشد که در قانون جرایم رایانه ای ذکر شده و برای آن کیفری در نظر گرفته شده باشد، مجازات قانونی مجرم مشخص است. در صورتیکه جرمی رخ دهد و برای آن جرم کیفری تعیین نشده باشد، در هستی شناسی به جستجوی جرایم مشابه قبلی پرداخته میشود که حق مزبور را نقض کرده باشد. سپس کیفر جرایم مشابه قبلی که از قبل مشخص شده است به عنوان کیفر پیشنهادی برای جرم جدید برگزیده می شود.

مجازات جرائم رایانه ای، علیرغم این که ارتکاب آن ها آسان تر و دارای ضرر اقتصادی بیشتری نسبت به جامعه و افراد هستند، سبکتر در نظر گرفته شده است که به نظر می رسد برای پیشگیری از این جرائم کافی نباشد. همان طور که جوامع با وقوع جرم در دنیای فیزیکی مقابله می کنند، ارائه راهکارهای مناسب در جهت مقابله و جلوگیری از وقوع جرم در محیط مجازی که از اوصاف و ویژگی های متفاوتی نسبت به محیط واقعی برخوردار است، امری ضروری است. علی رغم جرم انگاری شدن جرایم رایانه ای در حقوق داخلی ایران و همچنین وجود اسناد بین المللی مختلف از جمله کنوانسیون بوداپست در این زمینه، اما ارائه راهکارهای مقابله با جرایم رایانه ای بالاخص جرم کلاهبرداری رایانه ای در این قوانین و اسناد به چشم نمی خورد.

با ظهور رایانه و به تبع آن شبکه های اطلاعاتی و ارتباطی جهانی، یکی از تأثیرگذارترین عناصر بشر بوده است. در کنار این فناوری نوین سوءاستفاده هایی رخ داد که منجر به آسیب های اجتماعی شده است. از آن جا که قانون جرائم رایانه ای، اصلیتزین قانون مربوط به جرائم رایانه ای

است، ایجاب میکند حتی‌الامکان جامع اشکال مهم و پرخطر جرائم رایانه‌ای باشد؛ به گونه‌ای که برای مقابله با بعضی از جرائم رایانه‌ای با خلأ مواجه نباشیم، درحالی‌که قانون مذکور جرائمی نظیر؛ ارتشا، اختلاس، خیانت در امانت، اخاذی، پول شویی رایانه‌ای و مواردی از جرائم علیه مالکیت فکری نظیر؛ نقض اسرار و علائم تجاری و نیز جرائمی نظیر تبلیغات علیه نظام، تحریک به جنگ و کشتار، توهین به مقدسات و غیره را به طور کامل پوشش نمیدهد. از سوی دیگر، در قوانین جرائم رایانه‌ای تنها دو شکل از انواع ضمانت اجراها یا همان مجازات وجود دارد که جریمه نقدی و زندان میباشد. این مسئله نشان میدهد قانونگذار منطق قابل دفاعی در توجیه وضع ضمانت‌های اجرایی ندارد. از سوی دیگر، مرجع رسیدگی به برخی جرائم اینترنتی باید در زمینه فعالیت سایت خبری اینترنتی، مجازات و نحوه برخورد با آنها را در قلمرو قانون مطبوعات جستجو کند؛ زیرا قانونگذاران شبکه‌های اینترنتی خبری نوعی نشریه محسوب میکنند. لذا همه این موارد نیاز به اصلاح و بررسی مجدد دارد. از همین رو به موازات ایجاد اختیارات شکلی نوین برای تعقیب داخلی جرایم رایانه‌ای، اشکال نوینی از معاضدت قضایی نیز برای تعقیب بین‌المللی این جرایم به وجود آمده است. تفتیش و توقیف داده‌های رایانه‌ای، حفاظت سریع از داده‌های رایانه‌ای ذخیره شده، افشاء سریع داده‌های ترافیکی ذخیره شده، جمع‌آوری آنی داده‌های ترافیکی و کنترل داده‌های محتوایی اقداماتی هستند که در چارچوب معاضدت متقابل قابل ارائه می‌باشند. ارائه این نوع معاضدت‌ها مستلزم وضع قوانین شکلی هماهنگ در سطح داخلی است. همچنین هماهنگی قوانین کیفری ماهوی نیز برای تحقق شرط مجرمیت متقابل از اهمیت برخوردار است. همکاری بین‌المللی دولت‌ها کلید غلبه بر این مشکل است. این همکاری در زمره همکاری‌های بین‌المللی در امور کیفری قرار دارد و معاضدت قضایی متقابل مهمترین شکل آنست. باینحال ویژگی‌های منحصر به فرد محیط رایانه‌ای ابعاد خاصی به این نوع همکاری بخشیده و آن را از سایر معاضدت‌های قضایی متقابل در امور کیفری متمایز ساخته است. در واقع هیچ جرمی به اندازه جرایم رایانه‌ای موجب تحول حقوق کیفری بین‌المللی نشده است. اشکال خاص زمینه جرایم رایانه‌ای، مقتضیات قانونی و مشکلات آن موضوعیست که در این مقاله مورد بررسی قرار گرفته است.

تشکر و قدردانی

پژوهشگران، از عزیزانی که در فرآیند ویراستاری ادبی و صفحه‌آرایی این مقاله همکاری و راهنمایی داشتند، کمال تشکر و امتنان را دارند.

منابع

- اردبیلی، محمدعلی (۱۳۸۳). **حقوق جزای عمومی**، نشر میزان، چاپ پنجم.
- اسلامی، ابراهیم (۱۳۹۵). **جرم رایانه ای و بزه دیده رایانه ای**، تهران: افروز، چاپ اول.
- افتخار جهرمی، گودرز و اسلامی ابراهیم (۱۳۹۳). **نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرایم فضای مجازی**. *مجله حقوق دادگستری*، ۷۸(۸۸).
- انصاری دوست، شیما (۱۳۹۶). **جرایم رایانه ای در حقوق ایران**، چاپ اول.
- جاویدنیا، جواد (۱۳۸۷). **جرایم تجارت الکترونیکی**، انتشارات خرسندی، چاپ اول.
- کی‌نیا، مهدی (۱۳۷۰). **مبانی جرم‌شناسی**، تهران، نشر دانشگاه تهران، چاپ سوم.
- نجفی ابرندآبادی، علی‌حسین (۱۳۷۵). **جامعه‌شناسی جنایی**، دانشگاه تهران، چاپ دوم.
- نوری، محمد (۱۳۸۴). **جرایم رایانه ای**، انتشارات گنج دانش، چاپ دوم.

References:

- BR Roth (2005). **State Sovereignty, International Legality, and Moral Disagreement**.
- Clifford Stoll, Lawrence Berkeley Lab, Berkeley, CA (1990). **The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**, *Physics Today*, Vol. 43, issue 8.
- Council of Europe (2001). **Explanatory Report to the Council of Europe Convention**.
- Council of Europe (2009). **International Co-operation Under the convention on Cybercrime**.
- Kate Westmoreland, Gail Kent (2015). **International Law Enforcement Access to User Data: A Survival Guide and Call for Action**, *Canadian Journal of Law and Technology*, Vol. 13.
- Lucie, Angers (2004). **Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation**, In: *Crime and Technology: New Frontiers for Regulations. Law Enforcement and Research*, Chapter 4.
- Michael Sussmann (1998). **The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium**, *Duke Journal of Computer & International Law*, Vol. 9.
- Peter Swire, Justin Hemmings (2017). **Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program**, *New York Annual Survey of American Law*, Vol. 71.
- Peter Swire (2012). **From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud**, *International Data Privacy Law*, Vol. 2.
- United Nation Office on Drugs and Crime (2013). **Comprehensive Study on Cyber-Crime**.