حق ما

ما از عدالت سهمی داریم

سال هشتم، شماره ۲۲۰/ ۱۰ خرداد ۱۴۰۳/ ۳۰ می ۲۰۲۴

جرایم سایبری

IRAN HUMAN RIGHTS (IHRNGO)
سازمان حقوق بشر ایران

ما از عدالت سهمی داریم
دو هفته نامه الکترونیکی تخصصی حقوق بشر
صاحب امتیاز و مدیر مسئول: سازمان حقوق بشر ایران/ محمود امیری مقدم
سردبیر این شماره: مریم غفوری
تحریریه: طناز کلاهچیان، علی‌اصغر فریدی، سیروان منصوری
صفحه‌بندی: ماهور خوش‌قدم
تماس با مجله: mail@iranhr.net

حقوق ما در ویرایش مطالب آزاد است!

یادداشت هایی که از روزنامه‌نگاران و اشخاص دریافت می‌شود نظر شخصی آنان است و دیدگاه مجله حقوق ما نیست.

در این شماره می‌خوانید:

دسترسی آزاد به اطلاعات اشخاص و نیاز به وضع قوانین جدید

طناز کلاهچیان

از دیرباز بشر با شیوه‌های های مختلف سعی در برقراری ارتباط با هم نوع خود داشته است . شیوه هایی که با مدرن شدن زندگی، رنگ دیگری به خود گرفته و تغییرات چشمگیری داشته است. این تغییرات با شروع قرن ۲۱ و گسترش روزافزون علم و تکنولوژی، فضاهای مختلفی را برای برقراری ارتباطات ایجاد نموده و این امر نه تنها در حوزه ارتباطات دوستانه میان افراد که برای رفع نیازهایی همچون خرید مایحتاج از جمله البسه، مواد خوراکی، مسکن، خودرو و غیره بدون نیاز به حضور فیزیکی و تنها با ورود به سایت‌های مختلف در سراسر دنیا و پرداخت غیر نقدی به این فضا نیاز داشتند.

لیکن این فضا محدود به موارد پیش‌گفته نمی‌شد و برخی اوقات برای تبادل مبالغ ارزی راه‌گشا بود . به گونه‌ای که اشخاص (اعم از حقیقی و حقوقی) برای انجام مبادلات مالی خود با ورود به این شبکه‌ها بهره می‌بردند.

گسترش این فضا در سال‌های اخیر به گونه‌ای بود که حجم بالایی از شبکه‌های مجازی و رایانه‌ای ایجاد شد و شرکت‌های بزرگ سعی در تدوین مقررات مخصوص به خود کردند اما همین امر سبب بروز اختلاف میان سیستم قضایی آن کشور و متضررین شد.

در این میان جوامع مختلف بر آن شدند تا علاوه بر سامان دادن به این فضا و نگارش قوانین برای کاربران، حد و مرز مشخصی را برای آن تعریف کنند و عنوان مقررات رایانه‌ای یا سایبری را بر آن لحاظ نمایند.

شاید بهترین تعریف برای فضای سایبری مجموعه‌ای از ارتباطات افراد از طریق سامانه‌های مخابراتی و رایانه‌ای است که قدرت انتقال داده‌ها به سرعت میان افراد بدون توجه به مرزهای جغرافیایی مبادله می‌گردد، به گونه‌ای که افراد می‌توانند هم از این فضا برای لذت بردن و گذراندن اوقات خود از طریق تماس تصویری در هر لحظه در سراسر جهان، دیدن فیلم یا گوش دادن به موسیقی، یا حتی خرید و فروش بدون حضور فیزیکی بهره ببرند اما همین فضای لذت‌بخش می‌تواند توام با آسیب و ضرر معنوی و مالی باشد.

در کنار جنبه های مثبت این فضا، چنین راه‌های ارتباطی هیچگاه بدون خطر نبوده و همواره افراد سودجو در صدد ایجاد ناامنی در این حیطه هستند. کاربرانی با نام نامشخص یا ایجاد حساب کاربری ناامن قصد ایجاد ضرر و زیان معنوی یا مادی دارند. متاسفانه بسیار شنیده می‌شود که صفحه ای به نام شرکت یا شخص حقوقی در همین فضای سایبری ایجاد شده اما

با تحقیق مشخص می‌شود که تنها هدف آن سوء استفاده مالی از افراد و خالی نمودن حساب ارزی آنان یا ایجاد شبکه‌هایی برای انجام فعل مجرمانه است.

گسترش چنین فضای ارتباطی جوامع را بر آن داشت تا نسبت به این حوزه حساسیت ویژه قائل باشند و علت آن امر را شاید در ناشناخته بودن این فضا برای همگان و دسترسی آسان افراد بر این حیطه و همچنین وجود مجوز برای ناشناس ماندن افراد دانست. همین امر سبب گشت تا جوامع بشری به فکر تدوین و تصویب قوانین مختلف در جهت ایجاد محدودیت برای آن و آشنا نمودن افراد برای استفاده از چنین حوزه‌ای باشند.

دسترسی آزاد به اطلاعات اشخاص و سودجویی عده‌ای باعث گردید تا جوامع به این باور برسند که این قسم سوء استفاده کاربران در این فضا را در رده جرایم دانسته و برای آن قوانین مخصوص و بازدارنده تدوین نمایند. قوانینی که با اعمال بازدارندگی، فضای امنی را برای کابران ایجاد نموده تا به راحتی از آن بهره برند.

قوانین موضوعه ایران نیز از این امر مستثنا نبوده و با ظهور پدیده فضای آزاد اطلاعات، دست‌اندرکاران اجرایی و قانونی را بر آن داشت تا قانونی با تکیه بر همین اهداف تدوین نمایند و حاصل آن نگارش قانونی تحت عنوان قانون جرایم رایانه‌ای شد.

به گونه ای که در سال ۱۳۸۸ قانونگذار این فعل را مصداق بارز عمل مجرمانه دانست. از مواد ۷۲۹ لغایت ۷۵۵ از بخش پنجم قانون مجازات در بحث تعزیرات به این فعل مجرمانه اختصاص یافته است .

اما عناوین کلی جرم‌انگاری شده توسط قانونگذار در این مباحث خلاصه می گردد:

۱- جرائم علیه محرمانگی داده‌ها، سامانه‌های رایانه‌ای و مخابراتی؛ مربوط به دسترسی غیر مجاز شنود غیرمجاز و جاسوسی رایانه‌ای

۲- جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی مربوط به جعل تخریب و اختلال در سامانه

۳- سرقت و کلاهبرداری

۴- جرایم علیه عفت و اخلاق در این فضا

۵- هتک حیثیت و نشر اکاذیب

اقداماتی که برای هر یک از آنها مجازاتی اعم از جزای نقدی یا حبس در نظر گرفته است.

اما حجم رو به گسترش چنین فضایی که هر روز ابعاد تازه‌ای به خود می‌بیند و احتمال تداخل مقررات ما بین کشورها را افزایش می‌دهد. بدین‌سان که تصویب قوانین و مقررات داخلی برای هر کشور به خودی خود راه حل این مقیاس از جرائم سایبری نبوده و هر روز ابعاد تازه‌ای به خود می گیرد. در همین راستا و به دلیل همین گسترش روزافزون جرایمی که در این فضای ناشناخته در سطح بین‌المللی رخ می‌دهد، در سال ۲۰۲۱ کشورهای جهان را بر آن داشت تا بر سر یک معاهده واحد بین‌المللی برای مقابله با جرایم سایبری مذاکره نمایند تا شاید با تصویب این معاهده به عنوان اولین سند لازم الاجرا جهت پیشگیری از آسیب‌های مالی و معنوی که می‌تواند چندین کشور را در زمان واحد به خود مشغول سازد کمک شایانی نماید.

با نگاهی به سیر تحول این فضای ارتباطی در ایران و در سطح جهانی به طور قطع نیاز به وجود چنین قوانین داخلی و بین المللی و البته به روز در جلوگیری از این آسیب که هم حوزه خصوصی افراد و هم حیطه عمومی آن را نشانه می‌گیرد، نقش تعیین‌کننده‌ای خواهد داشت. کاربرانی که با سوء استفاده از این فضا سعی در نا امنی آن دارند توسط قانون شناسایی می‌گردند. به طور حتم وجود چنین قوانینی برای جلوگیری از آسیب‌های معنوی و ضررهای مالی می‌تواند قدری از آلام شخص آسیب دیده را بکاهد. هر چند اثبات این قبیل جرایم با توجه به گستردگی، به‌روز بودن و فضای ارتباطی آن، نیازمند داشتن سیستم قضایی مدرن و بودجه‌ای متناسب است که علاوه بر امکانات کافی، از آگاهی و دانش مدرن وامروزی نیز برخوردار بوده تا قضات دادگاه‌ها با استفاده از آن و تکیه بر قوانین نافع بتوانند احکام موجه و مستدلی صادر نمایند.

عناوین مجرمانه سایبری و انوع ساختار قانونی در سیستم کیفری ایران

علی‌اصغر فریدی

جرایم مطرح‌شده در قوانین مرتبط با امور سایبری، هم در باب جرایم علیه اموال، هم امور امنیتی، و هم جرایم علیه اشخاص که در ماده پانزدهم این قانون مصوب ۱۳۸۸ (هم اکنون به عنوان ماده هفتصد و چهل و سوم قانون تعزیرات) مطرح و جرم‌انگاری شده است. اما روش‌های مختلف قانون‌گذاری در این زمینه که بر اساس سیستم Common Law (حقوق عرفی) بر روند و یا رویه قضایی استوار است و یا روش قانون‌گذاری بر اساس سیستم "رومی-ژرمنی" که هدف آن تدوین، نگارش، اعمال و اجرای قوانین است را شامل می‌شود. همچنین کشورهایی وجود دارند که در زمینه مبارزه با بزه‌های رایانه‌ای و یا حتی پیشگیری از آن قوانین مناسب به روز و یا لازم را ندارند. به نظر می‌رسد که سیستم قانون‌گذاری ایران مانند جرایم مرتبط با امور سیاسی که در قانون جرایم سیاسی مصوب سال ۱۳۹۵ بیان شده است، در جرائم مرتبط با امور رایانه نیز تنها به بیان مصادیق آن پرداخته و متاسفانه تعریف مناسب با آن صورت نگرفته است. بنابراین می‌توان بیان داشت که مصادیق مطرح شده در قانون مذکور نیز به طور کامل و جامع بیان نشده است.

مجله حقوق ما در این باره با دکتر زهرا وهبی، حقوق‌دان، مصاحبه کرده است:

کدام مواد قانونی در ایران به جرایم سایبری دلالت دارد؟

در سیستم کیفری ایران، با چند نوع ساختار قانونی برای عناوین مجرمانه جرایم سایبری مواجه هستیم. مفهوم کلی عناوین مجرمانه برگرفته از ماده دوم قانون مجازات اسلامی، مصوب سال ۱۳۹۲ است که بیان می دارد: رفتار اعم از فعل یا ترک فعل که در قانون برای آن مجازات تعیین شده است جرم است. در کنار این ماده قانونی که در قوانین قبلی کیفری ایران نیست، همین تعریف تقریبا به طور مشابه و با تفاوت‌های خاص حقوقی مشاهده می شود که امکان بیان آن از شاکله بحث ما خارج می باشد. قوانین دیگری نیز وجود دارد که به صراحت به جرم‌انگاری مصادیق مرتبط با جرایم سایبری پرداخته که اکثر دارای ایراد عمده عدم تعریف مشخص و معین این گونه جرایم است و تنها به بیان مصداق کفایت شده است. قوانین مرتبط که موضوع بحث ما است، شامل قانون تجارت الکترونیک مصوب ۱۳۸۲ که بر اساس ماده دوم این قانون، شبکه مرتبط با امور رایانه تعریف شده که دارای انواع مختلفی مانند شبکه حوزه شخصی، دانشگاهی و جهانی است که می تواند مصادیق متعددی داشته باشد. همچنین داده اطلاعات مرتبط در این زمینه و فضای سایبر نیز بیان شده است. قانون جرایم رایانه، مصوب سال ۱۳۸۸ که پس از آن به عنوان مواد هفتصد و بیست و نهم به بعد قانون مجازات اسلامی در بخش کتاب پنجم تعزیرات بیان گردیده است و دیگر به عنوان قانون خاص و جداگانه از قانون مجازات اسلامی شناخته نمی‌شود، و همچنین قانون مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می‌نمایند، مصوب سال ۱۳۸۵ که بر این اساس، برای تعیین مصداق جرایم مرتبط در این مهم، نیازمند کنشگران متعددی در این زمینه هستیم که شامل یک کامپیوتر که وسیله‌ای است که قابلیت پردازش اطلاعات را جهت تولید نتیجه خروجی مورد نظر

که قابل مشاهده است، می باشد. این کارکرد در سه مرحله انجام می‌شود که شامل الف) پذیرش ورودی ب) پردازش مطابق با قوانین از پیش تعریف‌شده، و همچنین تولید خروجی است. در کنار این مباحث، امنیت سایبری نیز از اهمیت بالایی برخوردار بوده است، که تا زمانی که امنیت اطلاعات مخدوش نشده است امنیت ملی نیز تهدید نمی شود که برای حفظ بیشتر امنیت در تمام حوزه‌های اجتماعی باید تدوین قوانین مناسب صورت پذیرد، به شرطی که این امر به امنیتی‌شدن محیط اجتماعی و زندگی اشخاص جامعه تبدیل نشود. بر همین اساس در ماده ۷۴۷ قانون مجازات اسلامی در بخش تعزیرات که در واقع همان ماده نوزدهم قانون جرایم رایانه‌ای مصوب ۱۳۸۸ است، در باب مسئولیت اشخاص حقوقی و میزان مسئولیت آن در کنار مسئولیت اشخاص حقیقی بیان شده است که صراحتا در صورت انتساب جرم به این اشخاص، مدیر شخص حقوقی و یا هر یک از کارمندان که جرم قابلیت انتساب به وی را دارد، دارای مسئولیت کیفری خواهد بود البته به شرطی که با اطلاع مدیر و یا در اثر عدم نظارت وی بر مرتکب، جرم رایانه‌ای اتفاق افتاده باشد که البته ایراد مندرج در این موضوع تا حدی در تبصره دوم این ماده که مسئولیت اشخاص حقوقی را به عنوان مانعی برای اشخاص حقیقی مرتکب در این زمینه نمی‌داند، بیان شده است که تا حدی محدودیت‌های مطرح شده را برای شخص مرتکب و یا مرتکبان از بین برده است. با توجه به آنچه که بیان گردید، جرایم رایانه‌ای در مواد ۷۲۹ الی ۷۵۵ به عنوان عنصر قانونی در این زمینه جرم‌انگاری شده است.

بعد از آن، در باب صلاحیت و آیین دادرسی مرتبط با آن می‌باشد که علاوه بر اینکه از جرم‌انگاری خارج شده است، مواد قانونی مرتبط جرایمی مانند دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، جعل رایانه‌ای، سرقت و کلاهبرداری مرتبط با رایانه، جرایم علیه عفت و اخلاق عمومی، هتک حیثیت و نشر اکاذیب مسئولیت کیفری اشخاص و همچنین دیگر جرایم مانند معامله، توزیع و در دسترس قرار دادن، و یا معامله داده‌ها و نرم‌افزارها محتوای آموزشی و موارد مشابه، شامل عناوین مجرمانه در بخش قانون مرتبط است.

چه مجازات‌هایی در قوانین ایران برای جرایم سایبری در نظر گرفته شده است؟

برای اعمال مجازات بر مرتکبین این گونه جرایم، باید به ماده چهاردهم قانون مجازات اسلامی مصوب سال ۱۳۹۲ توجه نمود که چهار نوع مجازات اصلی موجود در سیستم کیفری ایران را که شامل مجازات حدی، قصاص، دیات و تعزیرات می شود را بیان می‌دارد: سه نوع مجازات اولیه، عملا قابلیت اعمال به اشخاص حقوقی را در باب مجازات منتهی به پرداخت دیه را دارا می‌باشد که البته در برخی از موارد نیز مصادیق دیگری را نیز شامل می‌گردد. این در حالی است که مجازات‌های اعمالی که به عنوان مجازات تعزیری شناخته می‌شود، قابلیت اعمال به هر دو نوع شخص یعنی اشخاص حقیقی و حقوقی مرتکب در جرایم و همچنین جرایم رایانه‌ای را دارا می‌باشد که البته برخی از مجازات‌ها از جمله قصاص و یا اعدام برای اشخاص حقوقی به صورت تعطیلی دایمی شرکت و یا موسسه و یا تعطیلی موقت اعمال می‌شود. با توجه به آنچه که بیان گردید، ساختار تقسیم‌بندی جرایم به صورت بزه‌های ضد اشخاص که شامل قتل عمد، غیرعمد و تحریک به خودکشی بزه‌های جنسی، شامل تشویق جنسی کودکان، فحشاء، تطمیع، سوءاستفاده از اطلاعات شخصی کودکان، آزار جنسی و وادار نمودن به فحشاء است. به‌کارگیری نادرست از اینترنت برای فروش کالاهایی مانند نوشیدنی الکلی غیرمجاز،

دارو، و موارد مشابه است که متاسفانه در این زمینه خلاءهای فراوانی در قوانین مرتبط با آن قابل مشاهده است. زیان رساندن به زیرساخت‌ها، ورود غیرمجاز به رایانه، پخش نرم‌افزارهای زیانگر و از بین بردن داده مورد نظر است. کلاهبرداری، سرقت و سایر جرایم مشابه نیز باید مورد توجه قرار گیرد. مجازات‌های مرتبط با این موضوع در مواد ذکرشده، به نظر می رسد در برخی موارد، از اصل تناسب بین جرم و مجازات اعمالی که یکی از اصول کلی مباحث حقوقی است، عملا خارج شده است. به خصوص در اعمال جریمه نقدی در این گونه جرایم که منتهی به پرداخت جریمه نقدی می شود، این مجازات فاقد تاثیر پیشگیرانه، آن هم از نوع پیشگیری اولیه و یا ثانویه در باب عدم تکرار جرم است و حتی در برخی از مواقع، اعمال مجازات حبس مانند حبس شش ماه تا دو سال در کنار اعمال مجازات جریمه نقدی که اختیار اعمال آن در دست سیستم کیفری است، چندان کارآمد نمی‌باشد که می تواند هر کدام از مجازات‌ها را که صلاح دانست اعمال نماید و اجباری به اعمال هر دو مجازات در برخی از موارد وجود ندارد و خود از نقاط ضعف در این مهم می‌باشد. با این حال، مجازات‌های سنگین‌تری در برخی از جرایم مانند جاسوسی رایانه‌ای به خصوص در بند "ج" ماده ۷۳۱ که در اختیار قرار دادن و یا افشاء داده‌ها به دولت، سازمان، شرکت یا گروه‌های بیگانه را شامل می شود، حبس از پنج تا پانزده سال می‌باشد، را می‌توان مشاهده نمود که باز هم با توجه به اینکه هر شخصی در زمان ارتکاب جرم سود و یا ضرر جرم ارتکابی را می‌سنجد و بعد از آن مرتکب آن می شود، عمل مانعی برای ارتکاب جرم قلمداد نمی‌شود، چرا که حمایت و حفاظت از اطلاعات شخصی افراد و رعایت حریم خصوصی باید از خانواده و سیستم آموزشی به افراد آموزش داده شود که متاسفانه همچنان در این موضوع دارای فقر فرهنگی هستیم. اعمال مجازات انفصال موقت از خدمت که در ماده ۷۳۳ در مبحث جاسوسی رایانه‌ای نیز مطرح شده است، به عنوان مجازات اصلی و اولیه برای مرتکب اعمال می‌شود که فرد مرتکب از جمله مامور دولتی که مسئول حفاظت از اطلاعات بوده است، می‌باشد. با این حال به نظر می‌رسد که سنگین‌ترین مجازات اعمالی برای این گونه جرایم، مربوط به جرایم مرتبط با عفت و اخلاق عمومی است که مطابق تبصره سوم در ماده ۷۴۲ تعزیرات، حتی می‌تواند بر اساس برداشت و تفسیر برگرفته‌شده از این عنوان قانونی، مشمول اعمال مجازات مفسد فی‌الارض که تنها مجازات آن طبق ماده ۲۸۶ قانون مجازات اسلامی، اعدام است، می‌گردد. که شدیدترین مجازات اعمالی در این بخش با هدف حفاظت و حراست از حریم شخصی اشخاص می‌باشد که عملا با دید مبارزه و برخورد، تدوین قانون یا قوانین مرتبط با پیشگیری است. متاسفانه در سیستم کیفری ایران، به صرف مبارزه، برخورد و یا اعمال مجازات یعنی مرحله پس از ارتکاب جرم توجه می‌شود و به مرحله قبل از آن که متمرکز بر امور پیشگیری است، چندان توجه نشده است.

شورای عالی فضای مجازی متشکل از چه افراد حقیقی یا حقوقی است و چگونه بر فضای مجازی نظارت میکند؟

این شورا، یکی از شوراهای حاکمیتی در ایران است که در هفدهم اسفند ۱۳۹۰ با هدف ایجاد مرکز ملی فضای مجازی ایجاد شده است، چرا که فضای مجازی عملا نامحدود است و مرز ندارد و این امر با هدف پیشرفت در راستای هدف‌ها و پیشرفت‌های نظام جمهوری اسلامی ایران، تشکیل و ایجاد شده است. اعضای این شورا مشتمل بر دو بخش اشخاص حقیقی و حقوقی است: از جمله

رئیس‌جمهور (در حال حاضر وظیفه مرتبط بر عهده سرپرست قوه مجریه است که پس از تعیین تکلیف در این دوره، به رئیس‌جمهور بعدی واگذار می گردد)، رئیس مجلس شورای اسلامی به عنوان نماینده قوه مقننه، رئیس قوه قضاییه، رئیس سازمان صداوسیما، رئیس مرکز ملی فضای مجازی به عنوان دبیر شورا، وزیر ارتباطات و فناوری اطلاعات، وزیر فرهنگ و ارشاد اسلامی، وزیر علوم، تحقیقات و فناوری، وزیر آموزش و پرورش، وزیر اطلاعات، وزیر دفاع و پشتیبانی نیروهای مسلح، معاون علمی فناوری و اقتصاد دانش بنیان رئیس‌جمهور، رئیس کمیسیون فرهنگی مجلس شورای اسلامی، رئیس سازمان تبلیغات اسلامی، فرمانده کل سپاه پاسداران، فرمانده کل نیروی انتظامی، دادستان کل کشور و همچنین رئیس سازمان پدافند غیرعامل به عنوان اشخاص

حقوقی و سایر اشخاص حقیقی که هم اکنون شامل ۱۰ تن مانند عزت‌الله ضرغامی و سعید جلیلی است.

کار پلیس سایبری در ایران چیست و زیر نظر کدام سازمان یا ارگان فعالیت می‌کند؟

پلیس فضای تولید و تبادل اطلاعات، با نام اختصاری "پلیس فتا" و مشهور به پلیس سایبری ایران، یک واحد تخصصی فرماندهی انتظامی جمهوری اسلامی ایران است که وظیفه آن، جلوگیری و مبارزه با فیشینگ یا همان کلاهبرداری اینترنتی، جعل، سرقت اینترنتی، هک، نفوذ و جرایم سازمان‌یافته رایانه‌ای است. این سازمان جزو سازمان‌های نظارتی و امنیتی در ایران به شمار می رود که در اول بهمن سال ۱۳۸۹ با هدف نظارتی در کشور ایجاد شد. همچنین دسترسی غیرمجاز، برداشت اینترنتی غیرمجاز از حساب‌های بانکی اشخاص، شنود غیرمجاز، جعل رایانه‌ای، تخریب و اخلال در داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، استفاده غیرمجاز از پهنای باند بین‌المللی برای برقراری ارتباط مخابراتی، تولید و آموزش بدافزارها یا نرم‌افزارهای ارتکاب جرایم سایبری و گذرواژه، و اطلاعات کاربران از جمله موضوعاتی است که در حوزه پیگیری این سازمان می‌باشد.

جرایم سایبری در قوانین ایران در چه صورتی وجه جاسوسی به خود می‌گیرند؟

در قانون مجازات اسلامی در بخش مرتبط با امور رایانه، که همان طور که بیان گردید از ماده ۷۲۹ تعزیرات را شامل می شود، عملا جرایم به سه دسته اصلی جرایم ضد صحت و تمامیت داده و سیستم، جرایم ضد محرمانگی داده و سیستم، و بزه‌های قابل ارتکاب با رایانه تقسیم شده است. با توجه به اینکه به طور مشخص سوال مطرح شده، در باب جرام سایبری است، بررسی در مواد مرتبط، یعنی مواد ۷۳۱ و ۷۳۲ و ۷۳۳ قانون مجازات اسلامی در بخش تعزیرات در باب جاسوسی رایانه‌ای، مدنظر ما می‌باشد که صراحتا در یک مبحث جداگانه تحت همین عنوان بیان شده است که با جاسوسی از طریق غیر رایانه‌ای که در مواد ۴۹۸ به بعد تعزیرات که جرایم علیه امنیت، به ویژه جرایم جاسوسی غیر از امور رایانه‌ای را بیان نموده است، شامل می گردد که مرتبط با مواد ۵۰۱، ۵۰۳، و ۵۰۵، تعزیرات می‌باشد.

بر این اساس جاسوسی عبارت است از: گردآوری، گردآوری پنهانی و غیرقانونی اطلاعات مرتبط با امور سیاسی و نظامی یک کشور و یا اطلاعات متعلق به مردم می باشد که مراحل سه‌گانه جاسوسی که قابلیت بیان دارد شامل شناسایی تعیین اطلاعات مورد نیاز، جمع آوری اطلاعات و تجزیه و تحلیل اطلاعات جمع‌آوری شده می باشد که نهایتا منجر به هدف اصلی جاسوسی، یعنی ارائه اطلاعات به مسئولان یک دولت یا شرکت بیگانه جهت اتخاذ تصمیم است. همین موضوع منتهی به این امر نشده است که قانون‌گذار در جرم‌انگاری این جرم

منتظر حصول نتیجه شود، بلکه بدون توجه به مراحل مزبور، هر رفتار فیزیکی مرتبط با جاسوسی را به عنوان جرمی جداگانه تلقی نموده‌اند. جاسوسی رایانه‌ای در گام نخست، متضمن نفوذ و یا دسترسی یا دستیابی غیرمجاز به سیستم رایانه یا حامل داده است که اطلاعات طبقه‌بندی شده یا داده‌های حساس در آن ذخیره یا پردازش شده می‌باشد، را شامل می شود. بنابراین هک و یا نفوذ به سیستم رایانه‌ای معمول، مقدمه جاسوسی است.

این در حالی است که دستیابی به سیستم و جمع‌آوری اطلاعات می‌تواند به طرق مختلفی صورت گیرد که شامل مهندسی اجتماعی که در آن مرتکب با تماس تلفنی یا ارتباط از طریق ایمیل یا گپ زنی و با معرفی خود به عنوان یکی از کارمندان شرکت یا یک شخص معتبر، سعی در تخلیه اطلاعاتی مخاطب سیستم رایانه‌ای مربوطه می‌کند که در این روش، مرتکب قبل از اینکه دانش فنی مربوط به نفوذ به سیستم رایانه‌ای را دارا باشد و بر اساس آن و متکی بر آن مرتکب جرم شود، متکی به میزان نفوذ کلامی و یا رفتار خود شخص مرتکب است. ممکن است جاسوسی از طریق ارسال پیام‌های ناخواسته الکترونیکی یا اسپم واقع شود، پیام‌های ناخواسته هم می تواند شامل نرم‌افزارهای جاسوسی باشد و ممکن است شرایط تخلیه اطلاعاتی دریافت‌کننده پیام‌های ناخواسته را فراهم سازد و ساده‌تر از همه، جاسوسی رایانه‌ای ممکن است با فریب و یا تحریک متصدی حفظ اطلاعات رایانه‌ای طبقه‌بندی شده از طریق بهره‌گیری از مسائل شخصی یا عاطفی صورت گیرد. در جرم مذکور سه گام مطرح شده است که می‌توان آن را این گونه بیان داشت:

الف) دسترسی به سامانه‌های رایانه‌ای و مخابراتی که داده‌های سری در آن انباشت یا نگهداری می‌شوند که در ماد ۷۳۲ تعزیرات بیان شده است،

ب) دسترسی به داده‌های سری یا تحصیل یا شنود آن که در بند الف ماده ۷۳۱ بیان شده است و ج) در دسترس قراردادن برای کسانی که شایستگی و آگاهی از محتوای داده‌های سری را ندارند که در بند ب همین ماده بیان گردیده است و همچنین در دسترس قرار دادن یا افشاء داده‌های مذکور برای دولت، سازمان، شرکت یا گروه‌های بیگانه یا عاملان آن می باشد. با توجه به آنچه که بیان شد، پدیده جاسوسی رایانه‌ای بر پایه چهار رفتار جداگانه بنیاد شده است که هر یک بزه جداگانه‌ای به شمار می‌رود که شامل:

یک) نقض تدابیر امنیتی در ماده ۷۳۳ تعزیرات بیان شده است که عملا تکرار ماده ۷۲۹ می‌باشد،

دو) دسترسی به داده‌های سری یا تحصیل یا شنود و دسترسی تحصیل و شنود عمومی در یک معنا تحت عنوان دریافت اطلاعات به کار می‌روند،

سه) در دسترس قرار دادن داده‌های سری برای اشخاص فاقد صلاحیت،

چهار) افشاء و یا در دسترس قرار دادن داده های سری برای دولت، سازمان، شرکت و یا عاملان آن؛

البته باید بیان داشت که افشاء با در دسترس قرار دادن داده‌های سری متفاوت است که در دسترس قرار دادن چهره فردی، و افشاء، چهره همگانی دارد که بر همین اساس رفتار افشاء خطرناک‌تر خواهد بود.

با توجه به آنچه که بیان گردید جاسوسی رایانه‌ای، یک جرم عمدی است، مگر درباره در دسترس قرار گرفتن مندرج در ماده ۷۳۳ که به طور غیرعمد و از طریق بی‌احتیاطی، بی مبالاتی و یا عدم رعایت تدابیر امنیتی رخ دهد. با توجه به آنچه که بیان شد، برجسته‌ترین رکن روانی این عنوان مجرمانه، آگاهی مرتکب به اجزاء رکن مادی است که آگاهی به سری بودن داده و همچنین آگاهی به غیرصالح بودن فرد یا عامل بیگانه‌بودن شخص، باید مورد توجه قرار گیرد.

سایبر تروریسم و انجام اعمال خشونت‌آمیز و تروریستی در اینترنت

علی‌اصغر فریدی

در ماه مه سال ۱۰۲۱ میلادی، سازمان ملل متحد فرایند تاریخی تدوین یک معاهده بین‌المللی برای مبارزه با جرائم سایبری را آغاز کرد. این معاهده پیشگامانه، در صورت تصویب در مجمع‌عمومی سازمان ملل متحد، اولین سند الزام‌آور بین‌المللی در حوزه سایبر خواهد بود. اهمیت این معاهده را نمی‌توان نادیده گرفت، زیرا نوید ایجاد یک نظام قانونی جهانی برای مقابله با جرائم سایبری، تقویت همکاری‌های بین‌المللی و محاکمه مجرمان سایبری را می‌دهد. بااین‌حال، معاهده مورد نظر در جزئیات خود دارای مشکلاتی است که بدون یک محدوده مشخص و ضمانت‌های قانونی و اجرایی قوی، می‌تواند ناخواسته حقوق بشر را به خطر انداخته و به رژیم‌های سرکوبگر قدرت دهد تا آزادی بیان آنلاین را نابود کنند.

بااین‌وجود، پیش ازپرداختن پیچیدگی‌های این معاهده، درک وضعیت جرائم سایبری ضروری است. جرائم سایبری را می‌توان به دو گروه بزرگ طبقه‌بندی کرد: وابسته به فضای سایبری و فعال در فضای سایبری.

جرائم وابسته به فضای سایبری شامل جرائمی است که تنها از طریق استفاده از فناوری‌های اطلاعات و ارتباطات (ICT) امکان‌پذیر است. نمونه‌های بدنام جرائم وابسته به فضای سایبری شامل حملات باج‌افزاری است که در آن هکرها به سیستم‌ها نفوذ می‌کنند، داده‌ها را رمزگذاری می‌کنند و برای رمزگشایی باج می‌خواهند. از سوی دیگر، جرائم فعال در فضای سایبری شامل جرائم سنتی همچون کلاهبرداری آنلاین، سرقت هویت، یا استثمار آنلاین از کودکان است که به دلیل تسهیلات ناشی از فناوری اطلاعات و ارتباطات در مقیاس، سرعت و دامنه افزایش‌یافته است.

فوریت تدوین یک معاهده جرائم سایبری نو، ناشی از تکامل سریع فناوری و عوامل تهدید در دو دهه گذشته است. البته تلاش‌های ملی و بین‌المللی بسیاری برای مبارزه با استفاده مجرمانه از فناوری اطلاعات و ارتباطات انجام شده که ناشی از موج فزاینده جرائم سایبری است که افراد، جوامع، مشاغل و حتی دولت‌ها را تحت تأثیر قرار می‌دهد. برای نمونه، کلاهبرداری‌های عاشقانه به‌تنهایی بیش از ۱,۳ میلیارد دلار برای قربانیان در پنج سال گذشته هزینه داشته است. افزون بر این، یک حمله باج‌افزاری به دولت کاستاریکا در سال ۲۰۲۲ ،موجب ایجاد وضعیت اضطراری در این کشور شد و زیرساخت‌های دیجیتال این کشور را برای ماه‌ها فلج کرد.

امروزه مجرمان سایبری، از کلاهبرداران در مقیاس کوچک گرفته تا گروه‌های جرائم سایبری فراملی و سازمان‌یافته و عوامل تحت حمایت دولت‌ها، جرائم سایبری را به یک تهدید جهانی با عواقب و پیامدهای محلی تبدیل می‌کند.

در رابطه با همین موضوع سازمان حقوق‌بشر ایران با نیره انصاری، حقوقدان و فعال حقوق‌بشر گفتگویی انجام داده که مشروح آن در زیر آمده است.

جرایم سایبری در لغت و در قوانین حقوقی چگونه تعریف شده است؟

رشد سریع و در عین حال نامتوازن ساختار فضای سایبری، شبکه اینترنت و فضای مجازی را به یکی از فضاهای آسیب پذیر و خطرناک تبدیل کرده است که توجه جامعه جهانی و نهادهای امنیتی، انتظامی و قضائی را به طور نظام مند و هدفمند به منظور پیشگیری و مصون سازی این بستر از تهدیدهای موجود و پدیده نوظهور سایبر تروریسم را در فضای بین المللی می‌طلبد.

تروریسم سایبری یا سایبرتروریسم (به انگلیسی: Cyberterrorism) استفاده از اینترنت برای انجام اعمال خشونت‌آمیز، وحشت زا و خسارت ساز است که منجر به از بین رفتن یا تهدید به از دست دادن جان یا آسیب جسمی قابل توجهی، به منظور دستیابی به دستاوردهای سیاسی یا ایدئولوژیکی از طریق فضای مجازی می‌شود.

به حیث لغوی در فرهنگ‌های مختلف سایبر به‌معنی مجازی و غیرملموس است، محیطی است مجازی و غیرملموسِ موجود در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاه‌راه‌های اطلاعاتی مانند اینترنت به هم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هرآن‌چه در کره خاکی به‌صورت فیزیکی و به‌صورت ملموس وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) در یک فضای مجازی به‌شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران هستند، و از طریق رایانه و شبکه‌های بین‌المللی به هم مرتبط هستند.

افزون براین، برای تحقیق و پژوهش جرائم سایبری روش کارایِنگونه است که: با بررسی منابع، مقالات، کتابها، نتایج و مطالعات در حوزه جرایم سایبری، تروریسم بین المللی و سایبر تروریسم به روش غیر آزمایشی، مقایسه ای و کتابخانه ای، تهدیدها و مخاطرات سایبر تروریسم و ضرورت پیشگیری از جرایم سایبری در عرصه بین المللی مورد تحقیق و پژوهش قرار می گیرد.

آیا در قوانین حقوقی بین جرایم اینترنتی با جرایم سایبری تفاوتی وجود دارد؟

جرایم سایبری گونه‌ای از جرائم اینترنتی، و شامل جرم‌هایی است که در محیط سایبری رخ می‌دهند. محیط سایبری محیطی مجازی است که کاربران آن می‌توانند به هرگونه خدمات و اطلاعات الکترونیکی در سراسر دنیا دست‌رسی داشته باشند. مجرمان محیط سایبری شامل هکرها، کرکرها، فریک‌های تلفن بوده و انواع جرم‌های ممکن در این فضا را انجام داده، و سایبرکرایم و تروریسم سایبری خوانده می‌شوند. سایبرتروریسم مانند تروریست‌های معمولی ممکن است دارای انگیزه‌های سیاسی برای ارتکاب جرائم باشند. بحران‌سازهای سایبری شامل ویروس‌ها، خزنده وب و پالس‌های الکترومغناطیسی، کرم‌ها و بمب‌های منطقی است. پلیس سایبر براساس نوع جرم‌های سایبری، نیاز به آموزش‌های ویژه دارد.

جرائم سایبری و سایبرتروریسم دارای دو مفهوم متفاوت هستند، اما گاهی به دلیل تداخل در استفاده از این اصطلاح‌ها، به نحوی نادرست به جرائم سایبری به عنوان سایبرتروریسم اشاره می‌شود. جرائم سایبری، فعالیت‌های خشونت‌آمیز، وحشت‌زا و خسارت‌زا در فضای

سایبری است. مثال‌هایی از جرائم سایبری شامل حملات باج‌افزاری، کلاهبرداری آنلاین، سرقت هویت و استثمار آنلاین از کودکان می‌شود.

در رابطه با سایبر تروریسم باید بگوییم، در این حالت، از اینترنت برای انجام اعمال خشونت‌آمیز و تروریستی استفاده می‌شود. سایبرتروریسم منجر به از بین رفتن یا تهدید به از دست دادن جان یا آسیب جسمی قابل توجه می‌شود. این مفهوم به تروریسم سنتی اضافه می‌شود و معمولاً به منظور ترتیب دادن به حملات به زیرساخت‌های مهم، نظام‌های اطلاعاتی یا سایت‌های حکومتی استفاده می‌شود.

براین اساس جرائم سایبری به تخلفات مختلف در فضای سایبری اشاره دارد، و این در حالی است که سایبرتروریسم به اعمال خشونت‌آمیز و تروریستی با استفاده از فناوری اطلاعات و ارتباطات اشاره دارد. دراواسط دهه ۹۰ با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرائم رایانه‌ای، تحت عنوان جرایم سایبری (مجازی) یا «جرایم در محیط سایبری» شکل گرفته‌است. به این ترتیب جرایم اینترنتی را می‌توان مکمل جرایم رایانه‌ای دانست، به ویژه این‌که جرایم نسل سوم رایانه ای که به جرایم در فضای مجازی معروف است، بیش‌تر از طریق این شبکه جهانی به‌وقوع می‌پیوندد. یکی از زمینه‌های بحث تفاوت بین سایبرتروریسم و هکتیویسم است.

هکتیویسم «ازدواج هک با فعالیت سیاسی» است. هر دو عمل از منظر سیاسی هدایت می‌شوند و شامل استفاده از رایانه می‌شوند، با این وجود از سایبرتروریسم در درجه نخست برای ایجاد آسیب استفاده می‌شود.

چرا جرایم سایبری را سایبرتروریسم می‌خوانند؟

تعریف اصطلاح تروریسم دشوار است، تعیین یک تعریف و تبیین آن برای فضای مجازی می‌تواند کار سختی باشد. سازمان‌های مختلف تعاریف ویژه خود را ایجاد کرده‌اند، که اکثر آنها کاملاً گسترده هستند. همچنین در باره استفاده بیش از حد از این اصطلاح، افزایش سرعت در رسانه‌ها و فروشندگان امنیتی که کوشش در فروش «راه حل» دارند، اختلاف نظر وجود دارد.

یکی از راه‌های درک سایبرتروریسم شامل این باور است که تروریست‌ها می‌توانند با هک شدن به سیستمهای مهم زیربنایی، موجب از بین رفتن گسترده جان، هرج و مرج اقتصادی در سراسر جهان و خسارت‌های زیست‌محیطی شوند. ماهیت سایبرتروریسم مشتمل بررفتارهایی است که از رایانه یا فناوری اینترنت استفاده می‌کنند:

- با انگیزه سیاسی، مذهبی یا ایدئولوژیکی ایجاد می‌شود؛ که یک دولت یا بخشی از مردم را به مراتب مختلف ارعاب کند؛ - به‌طور جدی در زیرساخت‌ها دخالت می‌کند. اصطلاح «سایبرتروریسم» می‌تواند به طرق مختلف مورد استفاده قرار گیرد، اما محدودیت‌هایی در استفاده از آن وجود دارد. حمله به یک تجارت اینترنتی را می‌توان برچسب سایبر [تروریستی کیستی] عنوان کرد، اما زمانی که برای انگیزه‌های اقتصادی انجام شود و نه ایدئولوژیک، معمولاً

آن را جرم سایبری قلمداد می‌کند. کنوانسیون همچنین برچسب «سایبرتروریسم» را محدود به اقدامات افراد، گروه‌های مستقل یا سازمان‌ها می‌کند. هر نوع جنگ سایبری که توسط دولت‌ها در کشورها انجام شود به موجب قوانین بین‌المللی تنظیم و مجازات می‌شود. انستیتوی فناوری، «فناوریِ اطلاعات» را به عنوان سایبرتروریسم تعریف می‌کند.

FBI، یکی دیگر از آژانس‌های ایالات متحده، «تروریسم سایبر» را «حمله از پیش برنامه‌ریزی شده، با انگیزه سیاسی علیه اطلاعات، سیستم‌های رایانه ای، برنامه‌های رایانه ای و داده‌هایی تعریف می‌کند که منجر به خشونت علیه اهداف غیر جنگنده توسط گروه‌های فرعی یا عوامل مخفی» می‌شود.

این تعاریف تمایل دارند دیدگاه سایبرتروریسم را به عنوان گرایش سیاسی و / یا عقیدتی به اشتراک بگذارند.

چه مجازات‌هایی در قوانین ایران برای جرایم سایبری در نظر گرفته شده است؟

براساس اطلاعات موجود، نخستین جرم اینترنتی در ایران در سال ۱۳۷۸ به‌وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی رایانه در کرمان اقدام به جعل چک‌های تضمینی مسافرتی کردند و چون تفاوت و تمایز زیادی بین جرم رایانه‌ای و جرم اینترنتی وجود ندارد، عمل آن‌ها به‌عنوان جرم اینترنتی شمرده شد. پس از این بود که گروه‌های دیگری مرتکب خلاف اینترنتی می‌شدند؛ مواردی چون جعل اسکناس، اسناد و بلیط شرکت‌های اتوبوس‌رانی، جعل اسناد دولتی از قبیل گواهینامه رانندگی، کارت پایان خدمت، مدرک تحصیلی و جعل چک‌های مسافرتی و عادی بخشی از این جرائم اینترنتی هستند.

براساس آمارهای موجود در سال ۱۳۸٤، ۵۳، مورد پرونده مربوط به جرایم اینترنتی در ایران تشکیل شد که کشف جرایم آمار پنجاه درصدی را نشان می‌دهد. به‌طور کلی جرایم سایبری در ایران دامنه گسترده‌ای را در بر می‌گیرد. برخی از این جرایم به شرح زیر هستند: دسترسی و شنود غیرمجاز گذرواژه یا هر داده خصوصی دیگری که مربوط به شخص حقیقی یا حقوقی باشد)انتشار مطالب و محتوای مبتذل و مستهجن جاسوسی رایانه‌ای، جرایم علیه صحت داده‌ها و سیستم‌های رایانه‌ای از جمله تخریب، جعل و اخلال در سیستم‌های رایانه‌ای و مخابراتی و کلاهبرداری در فضای سایبری، جرم در عفت و اخلاق عمومی، نشر اکاذیب و داده‌های ناصحیح، انتشار و در دسترس قرار دادن معاملات فروش و انتشار آن‌ها، انتشار و پخش آموزه‌های نادرست در فضای سایبری، هک، فیشینگ و بدافزارها و گسترش ویروس‌های سایبری بوده است.، از مهم‌ترین موارد جرم اینترنتی و رایانه‌ای در سال ۱٤۰۲، ۳۲ مورد سوءاستفاده از کارت‌های اعتباری، ۱۱ مورد کلاهبرداری اینترنتی، ۷ مورد ایجاد مزاحمت از طریق اینترنت، ۳ مورد کپی‌رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوعات متفرقه بوده‌است.

باتوجه به آمارهای سال ۸٤ میزان موارد کشف‌شده مربوط به کلاهبرداری، جعل و دیگر جرایم رایانه‌ای و اینترنتی درصد رشد را نشان می‌دهد..

با توجه به توسعه زیرساخت‌های فناوری اطلاعات و ارتباطات در ایران و افزایش کاربران و استفاده‌کنندگان از اینترنت و دیگر فناوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلی، ارتباطات ماهواره‌ای، لزوم ایجاد و توسعه سازوکاری برای برقراری امنیت در فضای تولید و تبادل اطلاعات را توجیه می‌کند. همچنین توسعه خدمات الکترونیک نظیر دولت الکترونیک، بانک‌داری و تجاررت الکترونیک، آموزش الکترونیک و دیگر خدمات از این دست، لزوم ایجاد پلیس تخصصی را برای تأمین امنیت و مقابله با جرایمی که در این فضا به وقوع می‌پیوندند را آشکار می‌کند.

از دیگرفراز، رشد قارچ‌گونه جرایم در حوزه فضای تولید و تبادل اطلاعات، مانند کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جرایم اخلاقی و برخی جرایم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصّصی که توان پی‌جویی و رسیدگی به جرایم سطح بالای فناورانه داشته باشد، به وجود آید.

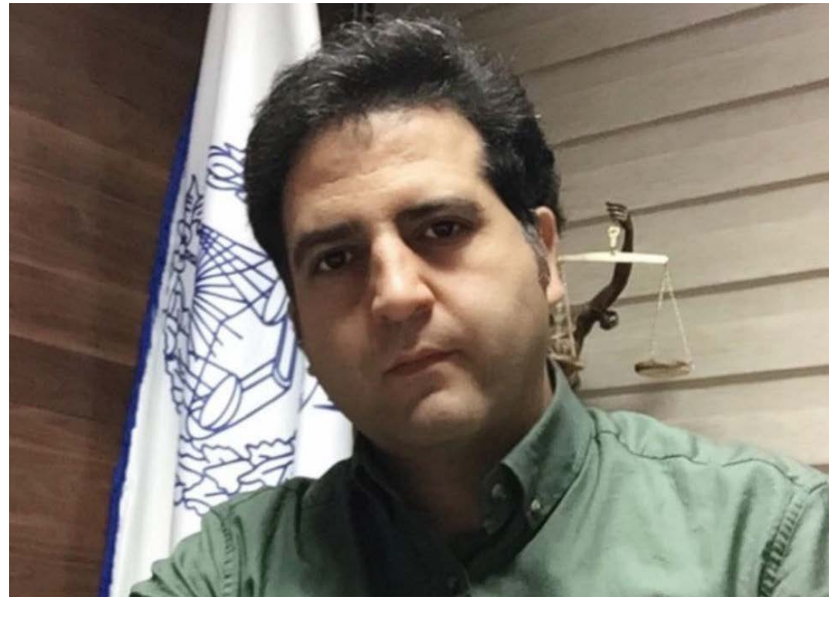
از سوی دیگر با توجه به تصویب قانون جرایم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوبات کمیسیون «افتای» دولت اسلامی درایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات،در بهمن‌ماه سال ۱۳۸۹ به دستور فرمانده نیروی انتظامی ایران، تشکیل شد.

در مبحث یکم از فصل دوم قانون جرایم رایانه ای مصوب خرداد ماه ۱۳۸۸ مجلس شوراي اسلامی؛ جعل رایانه‌ای به این شکل تعریف شده است: الف) تغییر یا ایجاد داده هاي قابل استناد یا ایجاد یا وارد کردن متقلبانه داده به آنها؛

ب) تغییر داده‌ها یا علایم موجود در کارت «ای» یا «های» رایانه‌هایِ حافظه یا قابل پردازش در سامانه مخابراتی یا تراشه ها یا ایجاد یا وارد کردن متقلبانه داده ها یا علائم به آنها (قانون جرایم رایانه ای، ۱۳۸۸).

طبیعت این جرایم و سوءاستفاده‌های رخ داده در این فضای جدید، هیچ‌گاه در دنیای حقیقی دیده نشده‌است. امنیت ناکافی فناوری، همراه با طبیعت مجازی آن، فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران‌کننده‌ترین جنبه فضای سایبری انتشار سریع اطلاعات در آن است؛ برای نمونه در لحظه کوتاهی بخشی از اطلاعاتی که می‌تواند مورد سوءاستفاده قرار گیرد، منتشر می‌شود. در فضای سایبری جستجو و پیدا کردن این جرایم نسبت به فضای فیزیکی پیچیده‌تر است. در دنیای واقعی سرقت از بانک کاملاً مشخص است، زیرا که پس از سرقت در خزانه بانک پولی موجود نیست؛ ولی در فناوری رایانه‌ای یک خزانه می‌تواند بدون هیچ علامتی خالی شود. برای نمونه سارق می‌تواند یک کپی دیجیتال از نرم‌افزار بگیرد و نرم‌افزار اصلی را همان‌طور که بوده باقی بگذارد. در فضای سایبری کپی عین اصل است، با کمی کار روی سامانه، سارق می‌تواند امکان هرگونه تعقیب و بررسی را از بین ببرد.

جرایم سایبری و خشونت آنلاین علیه زنان و کودکان



سیروان منصوری

توسعه و استقرار فناوری‌های نوین، جرایم سایبری را به عنوان یکی از موضوعات مهم و قابل بحث تبدیل کرده است. از یک طرف خلاءهای قانونی می‌تواند موجبات سوءاستفاده بزهکاران این حوزه را فراهم کند و از سوی دیگر دولت‌ها به بهانه پیشگیری در حوزه جرایم سایبری، ممکن است حقوق و آزادی‌های اساسی شهروندان را تحدید کنند. لیست جرایم سایبری در میان کشورها متفاوت است، اما جرایمی مانند استفاده از فناوری اطلاعات و ارتباطات برای مقاصد تروریستی، توزیع مواد مخدر، قاچاق اسلحه، همچنین جرایم مرتبط با محتوا مانند اطلاعات نادرست، اجبار به خودکشی، نفرت‌پراکنی، افراط‌گرایی و غیره را در بر می‌گیرد. در این میان، همه کشورها در صدد تصویب قوانین اختصاصی و ویژه در این زمینه هستند و حتی برای رسیدن به اهداف جرم‌شناسی پیشگیرانه لازم می‌بینند که در سطح بین‌المللی با سایر کشورها نیز همکاری متقابل داشته باشند.

مجله حقوق ما در این باره با سینا یوسفی، حقوق‌دان، گفت‌وگو کرده است:

خشونت علیه زنان و کودکان در فضای سایبری در ایران را چگونه برآورد می‌کنید؟

زنان و کودکان به عنوان یکی از اقشار آسیب‌پذیر، همواره به طرق مختلف و در فضاهای گوناگون مورد خشونت قرار می‌گیرند و به همین دلیل است که تمامی کشورها برای حمایت از زنان و کودکان، قوانین گوناگونی را تصویب می‌کنند. طبق گزارشات منتشره از سازمان ملل، خشونت علیه زنان بسیار بیشتر از مردان است و زنان ممکن است در محیط‌های گوناگون از قبیل محیط آموزشی، درمانی و حتی محیط خانوادگی مورد خشونت واقع شوند. با گسترش دسترسی جوامع به فضای مجازی و محیط سایبر، نوع و اشکال جرایم نیز تغییر نمودند و می‌توان گفت: با تغییر و گسترش ارتباطات و تعاملات افراد در فضای مجازی، خشونت علیه زنان و کودکان به حوزه سایبر نیز ورود پیدا کرد.

طبق تحقیقات صورت‌گرفته، می‌توان گفت که خشونت علیه زنان و کودکان در فضای مجازی به شیوه‌هایی اشاره دارد که شامل تهدیدها، آزارها، توهین‌ها، نشر اطلاعات شخصی خصوصی، گسترش اطلاعات غلط و ترویج ایدئولوژی‌های خشونت‌آمیز علیه زنان و کودکان می‌شود. این اقدامات ممکن است به طور مستقیم به زنان و کودکان آسیب برسانند و در برخی موارد، می‌تواند به خشونت فیزیکی یا روانی منجر شود. در فضای مجازی، خشونت علیه زنان و کودکان می‌تواند از طریق پیام‌های تهدیدآمیز در شبکه‌های اجتماعی، نشر تصاویر آزاردهنده، توهین‌های آنلاین، استفاده

از عبارات و محتوای غیراخلاقی و همچنین ترویج ایدئولوژی‌های نژادپرستی و جنسی، ظاهر شود.

در ایران نیز، جرایم این حوزه در حال حاضر، به عنوان یکی از معضلات جدی به شمار می‌آیند و نیازمند توجه و اقدامات موثر از سوی مراجع و نهادهای قانون‌گذاری و اجتماعی هستند تا از طریق پیشگیری و جبران آسیب‌های ناشی از آنها، خشونت علیه زنان و کودکان کاهش یافته و مهار گردد. ولی مع‌الاسف، در قوانین داخلی نه تنها بصورت عمومی چاره‌ای برای آن اندیشیده نشده است، بلکه در حوزه اختصاصی اقشار آسیب‌پذیر مثل کودکان و زنان نیز، قوانین حمایتی مناسبی در کشور وجود ندارد.

معاضدت قضایی متقابل در زمینه جرایم سایبری به چه شکل است؟

با تبدیل جرایم سایبری به عنوان یک معضل بین‌المللی، کشورها سعی کرده‌اند که بصورت متقابل در زمینه جرایم سایبری به همکاری بپردازند تا از این طریق، آسیب‌های آن را کاهش دهند. علاوه بر بحث تبادل نتایج تحقیقات علمی و بحث آموزش، با توجه به حوزه و بستر وقوع جرم، همکاری کشورها امری ناگزیر و اجتناب‌ناپذیر است.

به عبارت دیگر، ممکن است تعقیب و پیگیری یک جرم سایبری، مستلزم ورود به قلمرو حاکمیتی کشوری دیگر باشد که تحقیق، پیگرد و یا کشف و مهار جرم، جز از طریق معاضدت قضایی امکان پذیر نیست. کشورها عموما از طریق پیمان‌های دوجانبه و قراردادهای جمعی، چنین اقداماتی را پیش‌بینی و تسهیل می‌کنند که البته در سال‌های گذشته در سطح سازمان ملل متحد، اقدامات قابل توجهی در این زمینه صورت گرفته است.

جبران خسارت‌های ناشی از جرایم سایبری بزه‌دیدگان در قوانین ایران چگونه پیش‌بینی شده است؟

در قانون ایران و بخصوص قوانین مربوط به جرایم رایانه‌ای، قواعد خاصی برای این منظور پیش‌بینی نشده است و در واقع می‌توان گفت: در بحث جبران خسارت، اعم از مادی و معنوی، قوانین مربوطه ساکت است. فلذا در این مواقع می‌توان به قوانین عام از قبیل قانون مسئولیت مدنی و یا قانون آیین دادرسی کیفری و مطالبه ضرر و زیان ناشی از جرم، پس از اثبات وقوع جرم استناد کرد و صدور حکم مبنی بر جبران خسارت را از دادگاه درخواست نمود. البته باید گفت: به دلیل جدید بودن مباحث مربوطه در این حوزه، قضات معمولا در این خصوص از صدور حکم به نفع بزه‌دیده امتناع می‌کنند و مستند رای خود را هم، عدم وجود نص صریح قرار می‌دهند.

تناقض مساله پیشگیری از جرایم سایبری با اصل گردش آزاد اطلاعات در فضای مجازی، چگونه قابل توجیه است؟

سابقه کشورها در برخورد با جرایم حوزه سایبر، نشانگر آن است که مرز باریکی بین صرف پیشگیری

از وقوع جرایم این حوزه، و اصل آزادی بیان و گردش آزاد اطلاعات وجود دارد. در واقع هرگونه نگاه امنیتی صرف به این حوزه، می‌تواند موجب نقض حقوق بشر گردد. برخی دولت‌ها، از قوانین جرایم سایبری به عنوان وسیله‌ای برای جرم‌انگاری محتوای آنلاین و محدود کردن آزادی بیان، از جمله به منظور هدف قرار دادن روزنامه‌نگاران، فعالان حقوق بشر و مخالفان و یا کنترل و نظارت بر رفتار مردم، تحت عنوان معیارهای اخلاقی، سوءاستفاده می‌کنند. علاوه بر این، تحقیقات در مورد جرایم سایبری، می‌تواند تا حد قابل توجهی به حریم خصوصی افراد نفوذ کند. رهگیری و جمع‌آوری داده‌های مربوط به ترافیک آنلاین، می‌تواند به طور بالقوه حریم خصوصی افراد را به خطر اندازد. به علاوه خطر سوءاستفاده از اطلاعات شخصی حساس توسط سازمان‌های مجری قانون در طول این فرآیندها وجود دارد. به نظر، تنها راه مقابله با آن و حل این تناقض، تنظیم قوانینی شفاف و یکنواخت در سطح جهانی است که با مدنظر قرار دادن حقوق بشر و آزادی‌های اساسی، دولت‌ها را به رعایت آن ملزم نماید.

در سطح بین‌المللی پیشگیری از جرایم سایبری به چه شکل است و آیا اقداماتی در این زمینه صورت گرفته است؟

همان‌گونه که عرض کردم، بحث جرایم سایبری، نه تنها در حقوق داخلی، بلکه در حقوق بین‌الملل نیز موضوع جدیدی محسوب می‌شود و به دلیل گسترش چنین جرایمی، کشورهای عضو سازمان ملل نیز در پی چاره‌اندیشی جمعی در این حوزه هستند. از سال ۲۰۲۱ کشورهای عضو سازمان ملل متحد، درگیر فرآیند مذاکرات برای تدوین کنوانسیونی با هدف مقابله با استفاده مجرمانه از فناوری های ارتباطی و اطلاعاتی که معمولا با عنوان کنوانسیون جرایم سایبری سازمان ملل متحد شناخته می‌شود، شده‌اند. این کنوانسیون برای سیاست‌گذاری جهانی جرایم سایبری بسیار اهمیت دارد، چرا که ظرفیتی برای ارتقای همکاری‌های بین‌المللی فراهم آورده و در عین حال، مقامات اجرایی قوانین داخلی را برای تحقیق و مبارزه با جرایم سایبری توانمند می‌سازد و در واقع در این زمینه ظرفیت ایجاد می‌کند. این کنوانسیون، همچنین می‌تواند فرصتی را برای تقویت مولفه‌های عدالت کیفری و کاهش خطر استفاده از قوانین جرایم سایبری برای اعمال محدودیت‌های خودسرانه بر حقوق و آزادی‌ها فراهم آورد. موضوع مهمی که وجود دارد، این است که اگر این کنوانسیون بدون تدابیر کافی در حوزه حقوق بشری تدوین شود، می‌تواند با مشروعیت بخشیدن ناخواسته به گسترش کنترل دولت بر محتوای آنلاین، منجر به جرم‌انگاری آزادی بیان و تغییر شکل دسترسی مجریان قانون به داده‌ها شود و نهایتا، خطر قابل‌توجهی را برای حقوق بشر ایجاد کند و در واقع به طور بالقوه، حق حریم خصوصی و سایر حقوق و آزادی‌های اساسی را تضعیف کند.

جرایم سایبری، تاریخچه آن در ایران و جهان و مقوله سایبر-تروریسم

سیروان منصوری

به موازات تحولات اجتماعی، روابط شهروندان با یکدیگر و حکومت درگیر تنوع و تغییراتی می‌شود که عطف به ضرورت نظم‌بخشی به روابط اجتماعی-خصوصی و حاکمیتی در هر جامعه‌ای و نظر به انشاء کیفر در قالب یک واکنش اجتماعی-حکومتی نسبت به هنجارشکنی‌های اشخاص، اعم از حقیقی و حقوقی، لازم است دستگاه قضایی و ساختار تقنینی کشور بنا بر سیاست جنایی تعریف‌شده، به انشاء قوانین مرتبط با موضوع و تحولات اجتماعی اقدام کند. پیرو چنین ضرورتی است که به موازات گسترش فضای مجازی و تنوع روابط شهروندان در این فضا، واژه و اصطلاح سایبر و جرایم اینترنتی وارد ادبیات قضایی کشورها شده است و نظام‌های قضایی متعدد بنا به الزامات اخلاقی-حکومتی-اجتماعی، به تعریف جرایم سایبری و مجازات اقدام کرده‌اند.

مجله حقوق ما در این باره با محمدهادی جعفرپور، حقوق‌دان و وکیل دادگستری، گفت‌وگو کرده است.

جرایم سایبری در لغت و قوانین حقوقی چگونه تعریف می‌شود؟

پیش از تعریف جرایم سایبری، لازم است مفهوم فضای سایبر (سایبر سپیس)، شناسایی شود: فضای سایبر عبارت از محیطی است که در عصر ارتباطات، همزمان با تولید اصطلاح اینترنت در حوزه رسانه و ارتباطات مطرح شد، معادل فارسی آن فضای مجازی است. واژه سایبر از لغت یونانی (کیبرنتس) به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح (سایبرنتیک) توسط ریاضی‌دانی به نام «نوربرت وینر» در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است. سایبرنتیک، علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی و (کامپیوترها) است.

تعریف جرایم سایبری، پیش از آنکه به ارکان و عناصر تشکیل‌دهنده اینگونه جرایم وابسته باشد، به فضا و محیطی که امکان وقوع چنین رفتارهایی در آن مهیا است، وابستگی دارد. به عبارتی، شرط ضروری تحقق چنین جرایمی، مهیا بودن فضای ارتکاب جرم، یعنی فضای مجازی یا سایبر است. لذا به نظر می‌رسد بنا بر الزامات تعریف‌شده در علم منطق و کلام، در مقام تعریف واژگان، نمی‌توان به طور مطلق اصطلاح جرایم سایبری را تعریف کر،د بلکه مصادیق چنین جرایمی جایگزین مفهوم آن می‌شود. لذا بنا بر ماده ۷۲۹ تا ۷۷۶ قانون مجازات ذیل عنوان جرایم رایانه‌ای، میتوان به مصادیق اینگونه جرایم اشاره کرد. در تایید این ادعا، میتوان به مفهوم مخالف ماده ۷۸۰ که مقرر می کند: (چنانچه سامانه الکترونیکی یا رایانه‌ای و.. به عنوان وسیله ارتکاب جرم به کار

رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قانون جزای عمومی عمل خواهد شد) استناد کرد، که منظور و مقصور از جرم سایبری، ارتکاب هرگونه رفتار مجرمانه‌ای در محیط سایبر با استفاده از وسایل یا محیط الکترونیکی-مخابراتی و یا رایانه‌ای است.
نکته قابل توجه، مقررات تعریف‌شده در قانون تجارت الکترونیک است که دایره شمول و مصادیق وقوع این جرایم را گسترش داده است. با این وصف جرایم سایبری را میتوان به مواردی اطلاق کرد که فاعل رفتار مجرمانه، در صدد ارتکاب رفتاری در فضای غیرواقعی است که تحت عنوان سایبر یا فضای مجازی تعبیر می‌شود. در چنین رفتاری، از کامپیوترها به عنوان ابزاری جهت ارتکاب جرم استفاده می‌کنند. یک مجرم سایبری، ممکن است از دستگاهی برای دسترسی به اطلاعات شخصی کاربر، اطلاعات تجاری محرمانه یا اطلاعات دولتی استفاده کند. همچنین فروش یا استخراج اطلاعات فوق به صورت آنلاین، جرم سایبری محسوب می‌شود.

تاریخچه جرایم سایبری در جهان و ایران به چه زمانی برمی‌گردد؟

سرآغاز جرایم سایبری را به کنوانسیون جرایم سایبری بوداپست متصل می‌دانند و نخستین معاهده بین‌المللی که به جرایم رایانه‌ای و اینترنتی اشاره کرد و به تبع این کنوانسیون، در قوانین ملی کشورها چنین قانونی مصوب شد. این کنوانسیون، توسط شورای اروپا در سال ۲۰۰۱ ارائه شد و از ۲۳ نوامبر ۲۰۰۱، کشورها می‌توانستند آن را امضاء کنند. از ابتدای ژوئیه ۲۰۰۴، کنوانسیون به اجرا درآمد. تا سال ۲۰۱۳، تعداد ۳۹ کشور از جمله کشورهای عضو اتحادیه اروپا، این کنوانسیون را تصویب نموده و ۱۲ کشور نیز آن را امضاء کرده‌اند.
اما در نظام قضایی ایران، نخستین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی رایانه در کرمان، اقدام به جعل چک‌های تضمینی مسافرتی کردند و چون تفاوت و تمایز زیادی بین جرم رایانه‌ای و جرم اینترنتی وجود ندارد، عمل آن‌ها به‌عنوان جرم اینترنتی تعبیر شد. جعل اسکناس، بلیت شرکت‌های اتوبوس‌رانی، جعل اسناد دولتی از قبل گواهینامه رانندگی، کارت پایان‌خدمت، مدرک تحصیلی، اوراق خرید و فروش خودرو و چک‌های مسافرتی از دیگر موارد جرم رایانه‌ای در اوایل دهه ۸۰ به حساب می‌آمد.

آیا در قوانین حقوقی بین جرایم اینترنتی با جرایم سایبری اختلاف وجود دارد؟

همان‌طور که در تعریف این‌گونه جرایم اشاره شد،آنچه معیار تفکیک جرایم سایبری از سایر جرایم است، فضای ارتکاب این شق از جرایم است، لذا همان‌طور که مفهوم کلی فضای مجازی به فضای اینترنتی و سایبر تلقی می‌شود،

تفاوت چندانی بین جرایم اینترنتی و سایبری به نظر نمی‌رسد.

انوع جرایم سایبری شامل چه زیرشاخه‌هایی می‌شود؟

مصادیق جرایم سایبری به طور مشخص در قانون مجازات اسلامی تصریح شده است، اما خط ممیز اقسام این‌گونه جرایم، موضوع له جرم است، مواردی مانند زمانی که داده‌های اینترنتی موضوع جرم است، از قبیل سرقت یا جعل و تخریب داده‌ها، یا زمانی که جرایم سنتی مانند فحاشی یا افترا به واسطه فضای سایبر رخ می‌دهد مانند انتساب الفاظ رکیک از طریق ارسال داده پیام به مخاطب یا انتشار تصاویر مستهجن یا تصاویر خصوصی اشخاص در این فضا.

چرا گاهی جرایم سایبری را سایبر-تروریسم می‌خوانند؟

پاسخ این پرسش، به تعریف تروریسم وابسته بوده و ارتباطی مستقیم با مفهوم تروریسم دارد. آنچه معنای تروریسم را با یک قتل ساده متمایز می کند، هدف و نیت قاتل است و لذا با توجه به اهداف مرتکبین چنین جرایمی، چون هدف و نیت مرتکبین بر مصداق و مفهوم جرم غلبه دارد، این شکل از جرایم را به سایبر-تروریسم تعبیر می‌کند .گرچه نمیتوان یک قاعده کلی برای این امر لحاظ کرد و ممکن است که فاعل چنین رفتاری، به دور از اهداف تعریف شده در تروریسم، به ارتکاب جرم اقدام کند.
آنچه به عنوان تکمیل‌کننده بحث، قابل اشاره است:
با گسترش وسایل ارتباطی، کمیته‌ای با حضور وزارتخانه‌های اطلاعات، ارشاد، آموزش و پرورش، صداو سیما، ارتباطات و سازمان تبلیغات اسلامی تشکیل شد تا درباره فیلترینگ سایت‌ها تصمیم‌گیری کنند. در این زمان بحث اولیه درباره جرایم رایانه‌ای تا حد زیادی تغییر کرد. برخی از وبلاگ‌نویسان و روزنامه‌نگاران به اتهام نوشتن مطالب در وبلاگ‌ها و سایت‌ها، دستگیر شدند و به اتهاماتی مانند توهین به افراد و «مقدسات» یا افشای اسرار و اسناد دولتی محاکمه و مجازات شدند. دولت با فیلترینگ گسترده سایت‌ها و کنترل سرعت اینترنت، به دنبال تعاریف و مصداق‌های تازه‌ای از جرایم اینترنتی است. بر اساس ماده ۲۲ این قانون، کمیته تعیین مصادیق محتوای مجرمانه شامل وزیر یا نماینده وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر نماینده مجلس شورای اسلامی به انتخاب کمیسیون حقوقی و

قضایی و تأیید مجلس شورای اسلامی می‌شود و ریاست کمیته به عهده دادستان کل کشور خواهد بود.

این کمیته در دی‌ماه ۱۳۸۸، فهرستی از مصداق‌های محتوای مجرمانه را ارائه داد. این فهرست در پنج فصل در بخش‌های «محتوی خلاف عفت و اخلاق عمومی، محتوی علیه مقدسات، محتوی علیه امنیت و آرامش عمومی، محتوی علیه مقامات و نهادهای دولتی و عمومی و محتوایی که برای ارتکاب جرایم رایانه‌ای و سایر جرایم» تهیه شده بود. بخشی از این فهرست به مواردی اشاره دارد که در قانون مجازات اسلامی نیز آمده‌است ولی در برخی موارد مصادیق ارائه‌شده تازگی دارد.

از جمله موارد ممنوع‌شده در این قانون، انتشار فیلترشکن یا آموزش عبور از فیلترینگ می‌شود. این درحالی است که بسیاری از سایت‌ها در ایران فیلتر شده‌اند و کاربران با استفاده از فیلترشکن، از این سایت‌ها استفاده می‌کنند. مورد دیگر آن‌که اگر کسی لینک سایت‌هایی را که دارای «محتوی مجرمانه» هستند یا در آن‌ها نشانی‌های اینترنتی سایت‌های مسدودشده و نشریات توقیف‌شده را منتشر کند، مجرم است. به اشتراک گذاشتن لینک‌ها نیز از جمله کارهای مرسوم در اینترنت است که کاربران اینترنتی این گونه لینک‌ها را در سایت‌ها و وبلاگ‌ها قرار می‌دهند.

جرایم سایبری به سه دسته اصلی تقسیم می‌شوند: جرایم مرتبط با افراد، حق مالکیت و دولت‌ها. انواع روش‌های بکار گرفته شده و سطح دشواری، بسته به هر یک از این دسته‌ها متفاوت می‌باشد:

جرائم مرتبط با حق مالکیت: این دسته از جرایم، همانند نمونه واقعی، جرایمی هستند که به طور غیرقانونی اطلاعات بانکی یا کارت اعتباری یک فرد را در اختیار دارند. هکر، اطلاعات بانکی یک فرد را سرقت نموده تا به وجوه حساب او دسترسی پیدا کند، خریدهای آنلاین انجام دهد یا کلاهبرداری‌های فیشینگ را اجرا کند و افراد را وادار به ارائه اطلاعاتشان کند. آنها همچنین می‌توانند نرم‌افزاری مخرب را به منظور دسترسی به یک صفحه وب، حاوی اطلاعات محرمانه بکار بگیرند.

جرایم مرتبط با افراد: این دسته از جرایم سایبری، جرایمی هستند که اطلاعات مخرب یا غیرقانونی نظیر «سایبر استاکینگ» و قاچاق «ترافیکینگ» را به صورت آنلاین منتشر می‌کنند.

جرایم مرتبط با دولت‌ها: این دسته از جرایم سایبری، کمتر از دو دسته دیگر رخ می‌دهند، اما از آن دو دسته مهم‌تر می‌باشند. جرایم علیه دولت‌ها، تروریسم سایبری نیز نامیده می‌شوند. جرایم سایبری دولتی شامل هک‌کردن سایت‌های دولتی، سایت‌های نظامی یا انتشار تبلیغات سیاسی دروغین (پروپاگاندا) است. این دسته از تبهکاران، معمولا تروریست‌ها یا دولت‌های متخاصم سایر کشورها هستند.

حقوق ما

ما از عدالت سهمی داریم

دو هفته نامه الکترونیکی تخصصی حقوق بشر

صاحب امتیاز و مدیر مسئول:

سازمان حقوق بشر ایران/ محمود امیری مقدم

سردبیر این شماره: مریم نفوری

تماس با مجله: mail@iranhr.net