شماره مجوز انتشار: ۸۷۰۱۹ ISSN: 2783-1329

بررسی تشابهات و تفاوت های قوانین جرایم سایبری در قانون جرایم رایانه ای ایران و مقررات بین المللی

مصطفی عباسی[۱] / محدثه قوامی پور سرشکه[۲] / حامد نبی زاده[۳]

* نوع مقاله: پژوهشی / تاریخ دریافت: ۱۴۰۲/۱۲/۲۱ / تاریخ پذیرش: ۱۴۰۳/۰۱/۲۰

چکیده

در سالهای اخیر با گسترش فعالیتها و ارتباطات جهانی در فضای مجازی و توسعه شبکه‌ها و پلتفرم‌های مبتنی بر فضای سایبری و ابری، شاهد افزایش تعداد و تنوع جرایم اینترنتی و سایبری نیز هستیم. بدیهی است که برای کنترل جرایم در بستر جدیدی مثل اینترنت و فضای سایبر نیزمند تدوین قوانین و هنجارهای دارای ضمانت اجرایی بالا برای پیشگیری، کنترل و برخورد با جرایم سایبری هستیم. در این مقاله به صورت مروری نگاهی داریم به فعالیتهای انجام شده در زمینه تصویب قوانین جرایم سایبری در سطح داخلی و بین المللی . لازم به ذکر است که سابقه تصویب قوانین سایبری در جهان به ۱۹۷۸ در آمریکا و آخرین قانون تصویب شده در این زمینه نیز به توافقنامه تصویب شده در کنواسیون جرایم سایبری در سال۲۰۰۹ برمی‌گردد. ایران نیز بعد از بررسی‌هایی در دوره‌های زمانی معتلف سرانجام در سال ۱۳۸۸ قانون جرایم رایانه‌ای را تصویب کرد. با همه این تلاش‌ها به نظر می‌رسد با پیشرفت روزافزون تکنولوژی و افزایش تنوع و گستردگی کاربرد از فضای سایبری قوانین مربوط به این حوزه بر عکس جرایم سنتی نیازمند بازبینی همیشگی و مداوم است.

واژگان کلیدی: فضای سایبری، جرایم رایانه‌ای، جرایم سایبری، قوانین بین المللی.

[۱] دانشجوی دکتری حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی، لاهیجان، ایران. (نویسنده مسئول)
abbasi.mostafa.96@gmail.com
[۲] دانشجوی دکتری حقوق کیفری و جرم شناسی، دانشگاه آزاد اسلامی، لاهیجان، ایران.
mohadesehghavamipour@gmail.com
[۳] دانشجوی دکتری حقوق خصوصی،دانشگاه ازاد بین المللی، ارس، ایران.
lawyer.nabizadeh@gmail.com

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: 2783-1329

مقدمه

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. لذا با توجه به ویژگی های فضای جدید، محدودیت های همچون مرز، ملیت، مسافت، زمان و مکان و... معنا ندارد. وقتی در خصوص فناوری بحث می شود نمی توان رایانه را نادیده گرفت. رایانه، خود بزرگترین فناوری عصر حاضر است و سایر فناوری های نوین یا به وسیله آن و یا بر بستر آن شکل می گیرند. البته فناوری ها در کنار مزایای خود می توانند بسترساز سوءاستفاده هایی نیز باشند. و دامنه خطرهای آن افزایش می یابد (صادقی، ۱۳۹۴: ۱). اصطلاح جرم یا جرایم سایبری امروزه اصطلاح پرکاربردی است و در رسانه های ارتباط جمعی و شبکه های مجازی و خبرهای مربوط به جرایم و مجازاتها بسیار شنیده می¬شود. اما تعاریف متعددی از این پدیده وجود دارد به عنوان مثال «براساس تعریف کمیته اروپایی مسائل جنایی در شورای اروپا در سال ۱۹۸۹ چنین تعریفی از جرایم سایبری ارائه شده است: هر فعل مثبت غیرقانونی که کامپیوتر، ابزر یا موضوع جرم باشد یعنی به عبارت دیگر هرجرمی که ابزار یا هدف آن تاثیرگذاری بر عملکرد کامپیوتر باشد»(صادقی و پورخاقان شاه رضایی، ۱۳۹۶: ۲). یا «در کنوانسیون جرایم سایبری ۲۰۰۱ بوداپست که جدیدترین و جامع ترین سند بین المللی در این خصوص است. بر اساس کنوانسیون بوداپست، جرایم سایبری شامل آن دسته از جرایمی است که درباره رایانه و زیرساخت‌های شبکه باشد. این جرایم و جنایات عبارت از انتشار و استفاده از هرگونه نرم‌افزار مخرب، هک شدن، سرقت مشخصات کاربران، نفوذ، دستکاری، سرقت هویت، تقلب و استثمار جنسی کودکان است. به نظر می رسد کامل ترین تعریف این باشد : هرجرمی که قانون گذار به صراحت رایانه را به منزله موضوع یا یا وسیله جرم جزء رکن مادی آن اعلام کرده باشد، یا عملا رایانه به منزله موضوع یا وسیله ارتکاب یا وسیله ذخیره یا پردازش یا انتقال دلایل جرم در آن نقش داشته باشد»(آناهید و یوسف زاده، ۱۳۹۵: ۶۲۷) به طور کلی جرایم سایبری (رایانه ای) در برگیرنده همه اوضاع و احوال و کیفیاتی است که در آن شکل های پردازش الکترونیک داده ها، وسیله ارتکاب و یا هدف یک جرم قرار گرفته است و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است(فتاحی، ۱۳۹۷: ۱۰۰). در سطح جهانی جهت پیگیری حقوقی و فضایی جرایم سایبری قوانینی تصویب شده است؛ کنوانسیون جرایم سایبری معروف به «کنوانسیون جرایم سایبری بوداپست» که به اختصار «کنوانسیون بوداپست» گفته می‌شود، نخستین معاهده بین‌المللی است که به جرایم رایانه ای و اینترنتی می‌پردازد و می‌کوشد قوانین ملی را سازگار کرده، روش‌های

تحقیقات را ارتقا دهد و همکاری بین کشورها را بهبود بخشد. بحث جرایم رایانه ای در ایران ابتدا در اوایل دهه ۱۳۸۰ مطرح شد. آن زمان بیشتر حوزه هایی را در بر می گرفت که به جعل اسناد دولتی و شخصی مربوط میشد. چنانکه اولین جرم رایانه ای در خرداد ۱۳۷۸ به ثبت رسید که در آن یک دانشجوی کامپیوتر و یک کارگر چاپخانه در کرمان، چکهای تضمینی را جعل می کردند(فتاحی، ۱۳۹۷: ۱۰۰). و بدین ترتیب در بحث قوانین مربوط به جرایم رایانه ای مورد توجه قرار گرفت و یکی از مهمترین قوانین مربوط به فضای مجازی و رایانه، قانون تجارت الکترونیک مصوب سال ۱۳۸۲ است که باب چهارم آن از ماده ۶۷ تا ۷۷ به جرایم و مجازات‌های موضوع این قانون اختصاص دارد و دیگری قانون جرایم رایانه ای مصوب سال ۱۳۸۸ است که در سه بخش (جرایم و مجازات‌ها، آیین دادرسی و سایر مقررات) در ۵۶ ماده به تصویب رسیده است. مقنن ایران در قانون جرایم رایانه ای در بخش جرایم و مجازات‌ها این موارد را جرم‌انگاری کرده است که شامل جرایم علیه محرمانه بودن داده‌ها و سامانه‌های رایانه ای و مخابراتی مثل دسترسی و شنود غیرمجاز یا جاسوسی رایانه ای، جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه ای و مخابراتی مثل جعل رایانه ای یا تخریب و اخلال در داده‌ها، سرقت و کلاهبرداری مرتبط با رایانه، جرایم علیه عفت و اخلاق عمومی و هتک حیثیت و نشر اکاذیب است. براین اساس در این مقاله در نظر داریم به بررسی قوانین مربوط به جرایم سایبری بپردازیم و سوال اصلی این است که در خصوص جرایم سایبری (رایانه ای۹ چه قوانینی در کشور وجود دارد؟

۱- تعریف، انواع و تاریخچه جرایم سایبری

۱-۱- تعریف جرایم سایبری

بدیهی است که پیش بررسی قوانین مربوط به جرایم سایبری ابتدا باید تعریف دقیقی از جرایم سایبری داشته باشیم. در ادامه تعریف مفهومی و قانونی جرایم سایبری ارائه می گردد: برای تعریف جرایم سایبری ابتدا باید به تعریف مفهوم «فضای سایبری» بپردازیم. فضای سایبری که معادل آن در فارسی، «فضای مجازی» نامیده می شود، واژه سایبر از نظر لغوی به معنای مجازی و غیرملموس و مترداف (وطنی و اسدی،۱۳۹۵: ۱۰۱) لغت یونانی کایبرنتس (Kybernetes) به معنای سکاندار یا راهنما، است. اولین بار اصطلاح سایبرنتیک توسط ریاضیدانی به نام نوربرث وینر در کتابی با عنوان سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین، در سال ۱۹۴۸ بکاربرده شده است. اما واژه «فضای سایبری» نخستین بار توسط "ویلیام گیبسون" نویسنده داستانهای علمی تخیلی در کتاب «نورومستر» در سال ۱۹۸۴ به کار برده شد. با همه این توضیحات فضای سایبری در تعریف

مفهومی اش، به مجموعه هایی از ارتباطات درونی انسانها از طریق کامپیوتر و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی اشاره دارد(حقیقی،۱۳۹۵: ۲). سایبر در فارسی به مجاز و مجازی ترجمه شده است؛ اما این ترجمه گویای دقیق این واژه نیست زیرا محیط سایبر محیطی است حقیقی و واقعی نه دروغین و مجازی و فقط به شکل مادی و ملموس احساس شدنی نیست و این نکته کافی نیست که به آن مجاز و مجازی اطلاق شود. اما سایبر در اصطلاح به همه محیط هایی گفته می شود که اساس فعالیت آن ها بر مبنای پردازش و طبق سامانه صفر و یک کار می کنند. سایبر در زبان عموم مردم به غلط اینترنت نامیده می شود درحالی که اینترنت یک شبکه رایانه ای بین المللی بزرگ است که نظیر آن چندین شبکه بزرگ مثل یوزنت، تله نت و ... وجود دارد. تعداد این شبکه های بزرگ بالغ بر ۱۹ شبکه است(پرویزی، ۱۳۸۴: ۳۸ و ۴۰). لازم به ذکر است که برای تعریف «جرم سایبری» باید به این نکته اشاره کرد که نهادها و سازمان ها و اندیشمندان و حقوقدانان از زمان پیدایش این پدیده برای بیان تعریف دقیقی از آن درحال تلاش هستند اما تاکنون به اجماع نظر در تعریف این مفهوم نرسیده اند و جرم سایبری در قوانین هر کشور دارای تعریفی متفاوت است اگرچه در برخی کشورها مانند ایران، در قانون جرایم رایانه ایشان تعریفی دقیق از این مفهوم ندارند. به عنوان مثال گروهی از کارشناسان سازمان همکاری و توسعه اقتصادی[1] در سال ۱۹۸۳جرایم رایانه ای را عبارت از هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار یا انتقال داده ها، می دانند (زیبر[2] ، ۱۳۹۰:۱۸). در تعریفی دیگر «جرائم سایبری در اصطلاح به جرائمی گفته می شود که در محیطی غیرفیزیکی علیه فناوری اطلاعات با حالات شبیه سازی و مجاز یسازی ارتکاب می یابد(جاویدنیا، ۱۳۸۸: ۲۲۵). اما مشهورترین تعریف از جرایم سایبری بر اساس نقش رایانه و تجهیزات مشابه آن صورت گرفته است. در این تعریف جرم رایانه ای یا سایبری عبارت است از هرگونه عمل مجرمانه ای که در آن رایانه، وسیله یا هدف جرم باشد(شیرزاد، ۱۳۸۸: ۳۵). باتوجه به تعریف فوق جرایم سایبری به سه دسته تقسیم می شود: دسته اول جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع شده اند. مانند: سرقت و...؛ دسته دوم جرایمی که در آن رایانه به عنوان ابزار توسط مجرم برای ارتکاب جرم به به کار گرفته شود مانند جعل و...؛ و دسته سوم جرایمی که می توان آنها را جرایم سایبری محض نامید. این نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می پیوندند اما آثار آنها در دنیای واقعی ظاهر میشود. مانند: دسترسی غیرمجاز به سیستم های رایانه¬ای، قاچاق صوت، سرقت مجازی رایانه ها و ...(جهانشیری و همکاران،۱۳۹۴: ۱۵). جرایم

[1] Organization for Economic Cooperation and Development (OECD)
[2] Sieber Ulrech.

سایبری دارای ویژگی هایی چون سرعت، ناشناختگی، بزرگ مقیاس بودن، ارزان و کم هزینه بودن بزه، عدم حضور مجرم در صحنه جرم، فراملی بودن، بالا بودن رقم سیاه بزه، اتوماتیک بودن جرم، درونی بودن جرم، ضعف یا فقدان کنترل اجتماعی(جوان جعفری،۱۳۸۹ : ۱۸۲-۱۷۵).

۱-۲- تفاوت جرم سایبری و رایانه ای

همانطور که قبلا گفته شد جرائم سایبری در اصطلاح به جرائمی گفته می شود که در محیطی غیرفیزیکی علیه فناوری اطلاعات با حالات شبیه سازی و مجازی سازی ارتکاب می یابد(جاویدنیا، ۱۳۸۸: ۲۲۵). باید یادآور شد که جرائم سایبری به جهت گسترش خود، رفته رفته جانشین عباراتی چون جرم های رایانه ای و جرم های اینترنتی شدند. به جرائم سایبر، جرائم علیه فناوری اطلاعات نیز گفته می شود(پرویزی، ۱۳۸۴: ۴۰). واژه رایانه به گونه ای دقیق و جامع نمی تواند گستردگی این محیط را نشان دهد، زیرا بسیاری از ابزار و وسایل امروزی با داده هایی کار می کنند که اساساً به آن ها رایانه اطلاق نمی شود. ازاین رو عبارت هایی مانند جرم های رایانه ای یا جرم های اینترنتی نیز نمی توانند به گونه ای دقیق جرم های ارتکابی مربوط به این حوزه را پوشش دهند. برای نمونه یک سامانه ضبط و پخش الکترونیکی، رایانه نیست؛ اما به طور کلی در زیرمجموعه جهان سایبر قرار می گیرد(وطنی و اسدی،۱۳۹۵: ۱۰۲). پس در این مقاله همان واژه جرم سایبری ملاک قرار می گیرد. جالب است که در قانون مجازات اسلامی واژه جرم و جرایم رایانه ای، معادل جرم و جرایم سایبری در نظر گرفته شده است.

۱-۳- تعریف جرم سایبری در قوانین بین الملل

در اواسط دهه ۱۹۹۰ میلادی، نسل جدیدی از فناوری رایانه (که در واقع باید آن را ماحصل فناوری ارتباطی و اطلاعاتی نامید) تجلی پیدا کرد. رایانه ها در یک روند تکاملی بسیار سریع، به سیستم های رایانه ای متشکل از چندین وسیلهٔ رایانه ای که قابلیت ارتباط بین سیستم ها و شبکه های بین المللی را داشتند، تبدیل شدند. رایانه ها به وسیلهٔ شبکه ها، روز به روز ارتباط گسترده تری پیدا کرده و از طریق مخابرات و ماهواره، هرگونه دریافت، انتقال، صدور علایم، تصاویر، صداها، نوشته ها و نشانه ها را مقدور ساخته اند. لذا با توجه به این قابلیت شگرف فناوری ارتباطی، تحول عظیم در دنیای ارتباطات و عصر فناوری اطلاعات به وجود آمد که از مشخصه های این فناوری جدید، شکل گیری ارتباط بین افراد ملل دنیا در یک فضای مجازی و در محیط شبکه های بین المللی است که به نوبهٔ خود، سهم بسزایی در تغییر شکل و کارکرد روابط اجتماعی دارد و به همان نسبت در تغییر الگوی ماهیت جرایم از خصوصیات متمایز کنندهٔ : کلاسیک نیز تحول ایجاد کرده

است(زرگر، ۱۳۸۵: ۲۰۶).این نوع جرایم با جرایم پیشین، عدم وابستگی ارتکاب جرم به حضور فیزیکی مجرم در محل بروز نتایج جرم، زمان ارتکاب، مکان ارتکاب، بزه دیده و شکل ارتکاب است. به این نوع جرایم که در این نوع فضا (مجازی) وقوع پیدا می کند؛ جرایم سایبری گفته می شود(صبح خیز، ۱۳۹۴: ۱۲۱). یک تعریف عمومی، جرم سایبری را به عنوان هرگونه فعالیتی که در آن رایانه ها یا شبکه ها، ابزار، هدف یا مکانی برای فعالیت تبهکاری هستند، توصیف می کند. پیش نویس کنوانسیون بین المللی به تقویت حفاظت در برابر جرایم سایبری و تروریسم اشاره دارد. جرایم سایبری اعمالی در رابطه با سیستم های سایبری است. برخی تعریف ها، در تلاش برای در نظر گرفتن اهداف و نیت ها هستند و جرایم سایبری را دقی قتر تعریف می کنند. اما باید توجه داشت که در ابعاد بین الملل، تعریف دقیق و شفافی از جرم سایبری صورت نگرفته است(همان:۹).

۱-۴- تعریف جرم سایبری در قوانین ایران

همانطور که می دانیم هر عمل مجرمانه ای برای اینکه از نظر قانونی جرم تلقی شود نیازمند سه عنصر و رکن اساسس است که عبارتند از عنصر قانونی (شکستن قانون)، عنصر مادی (فعل یا ترک فعل خارجی) و عنصر روانی (جرم باید نتیجه خواست و اراده فرد بود) براین اساس جرایم سایبری دارای ویژگی هایی است که برای مجازات مجرمین آن نمی توان مانند جرایم سنتی عمل نمود. «امروزه رشد و توسعه تکنولوژی امکان استفاده از نیروهای انسانی سازمان یافته و منابع و امکانات متمرکز برای مقابله با بزهکاران فضای دیجیتال را سلب کرده است. دنیای جدید با ساختاری متفاوت و محیط اجتماعی نو آفریده شده است که در آن استفاده از مدل نظامی سلسله مراتبی با بزه ها و بزهکاران را مشکل و یا غیرممکن ساخته است»(جوان جعفری، ۱۳۸۹: ۱۷۴). با همه این توضیحات در مورد جرم سایبری در قانون اساسی ایران تعریف مشخصی از جرم سایبر/ جرم رایانه ای ارائه نشده است و قانوگذار ایران تنها دامنه مصداقی جرایم رایانه ای را مشخص کرده است(رضوی فرد و موسوی، ۱۳۹۵: ۳۴)؛ با مطالعه متن قانون جرایم سایبری مصوب ۱۳۸۸ و همچنین آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی مصوبه ۱۲ مرداد ۱۳۹۳ می بینیم که در هیچ کدام تعریفی از جرم رایانه ای یا جرم سایبری ارائه نشده است. در متن کامل قانون جرایم رایانه ای ذیل مواردی مانند جرایم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی؛ جرایم علیه صحت و تمامیت داده ها و سیستم های رایانه ای و مخابراتی؛ سرقت و کلاهبرداری مرتبط با رایانه؛ جرایم علیه عفت و اخلاق عمومی آورده شده است(قانون جرایم رایانه ای،۱۳۸۸). در یک جمع بندی کلی و بر اساس مطالعات موجود و تعریف جرم در نگاه حقوقی جمهوری اسلامی ایران که اذعان می دارد: جرم، هرفعل یا ترک فعلی است که درقانون برای آن

مجازات تعیین شده باشد، بنابراین جرم سایبری را می توان تلویحا چنین تعریف کرد که: هر فعل یا ترک فعلی است که در فضای سایبر به وقوع می پیوندد و برابر قانون برای آن مجازات تعیین شده باشد(صبح خیز، ۱۳۹۱: ۲۷).

۱-۵- انواع جرایم سایبری

مفهوم جرایم سایبری شامل گستره متنوعی از جرایم است. برای جرایم سایبری دسته بندیهای مختلفی پیشنهاد شده است که مشهورترین آنها بر اساس نقش رایانه صورت گرفته و با توجه به اینکه در اینجا رایانه است که مفهوم و مصادیق جرم را در فضای سایبر دگرگون ساخته، دسه بندی نیز با محوریت نقش آنها ارائه شده است(بهره مند و داودی، ۱۳۹۷: ۲۱).کنوانسیون جرایم سایبری بین چهار نوع مختلف از تخلفات سایبری تمایز قائل می شود:

جرایم علیه محرمانه بودن، تمامیت و دسترسی به سامانه ها و اطلاعات رایانه ای؛

جرایم مربوط به رایانه؛

جرایم مربوط به محتوای رایانه ای؛

جرایم مربوط به کپی رایت.

سه مقوله روی هدف حفاظت قانونی تمرکز می کنند:«جرایم علیه محرمانه بودن، تمامیت و در دسترس بودن سیستم ها وا طلاعات رایانه ای»؛ تخلفات وابسته به محتوا و و جرایم مربوط به کپی رایت. مقوله چهارم "جرایم مربوط به رایانه روی هدف حفاظت قانونی متمرکز نمی شود، بلکه روی روش تمرکز دارد. این ناهماهنگی منجر به همپوشانی بین مقوله ها می شود. به علاوه برخی عبارت ها که برای توصیف اعمال خلافکارانه استفاده می شود.(مثل تروریسم سایبری یا فیشنگ: توصیف کننده عملی است که که برای آشکارسازی اطلاعات قربانی بکار می رود و در اصل توصیف کننده استفاده از ایمیل برای فیش (ماهی) گرفتن برای گذرواژه یا اطلاعات مالی از دریای کاربران اینترنت است) اعمالی که در میان چندین مقوله قرار می گیرند را پوشش می دهد. با این وجود این مقوله ها توسط کنوانسیون جرایم سایبری به عنوان پایه ای مفید برای بحث در مورد جرایم سایبری ارایه شده اند(گرکی،۱۳۸۹: ۳۶).

۲- تاریخچه تدوین قوانین سایبری

در این بخش در نظر داریم به بررسی روند تدوین و تصویب قوانین مربوط به جرایم سایبری و مصادیق آن در جهان و ایران بپردازیم:

۲-۱- تاریخچه تدوین قوانین سایبری در جهان

از زمانی که اینترنت در سال ۱۹۶۴ توسط پائول باران[1] در شرکت «راند» پا به عرصه وجود گذاشت و عموم مردم توانستند از آن استفاده کنند، جرم های اینترنتی یا کامپیوتری نیز به وجود آمد. با گسترده شدن کاربرد اینترنت و ایجاد شبکه ها و پلتفرم های مختلف در فضای مجازی انقلابی ایجاد که منجر به پیدایش فضای سایبری گردید. به تبع این تحولات، جرایم اینترنتی نیز گسترش و توسعه یافته و بزه های سایبری مختلفی در این فضا پدید آمدند. امروزه در جهان جرایمی مانند: انتشار اخبار کذب، ارسال مطالب، تصاویر و فیلم های مستهجن، آموزش و تبلیغ تروریسم، هتک حرمت افراد استفاده از فضای متعلق به دیگران، ارسال پیام های مخرب، اخلال در دسترسی به دیگران، نقض حق مالکیت، هک و ویروسی کردن سایت ها، اجازه به حریم خصوصی افراد از طریق ایمیل ها بخشی از جرم های اینترنت محسوب می شوند.این نوع جرایم به طور وسیع تری در سطح امنیت ملی کشورها نیز اتفاق افتادند تا حد نشت اطلاعات سیاسی ـ امنیتی، سرقت اطلاعات مهم و حک سیستم های اینترنتی بانکها، سایتهای نظامی و... پیش رفت. تا جایی که هر کشور برای حفظ امنیت اطلاعات خود و شهروندانش اقدام به تاسیس پلیس امنیت فضای سایبری و به دنبال آن وضع قوانین مربوط به جرایم سایبری کرده است. از دیدگاه بین المللی امضای کنوانسیون جرایم رایانه ای که به وسیله شورای اروپا در ۸ نوامبر ۲۰۰۱ ضورت گرفت نخستین قدم در را مبارزه بین المللی قانونی با پدیده جرم رایانه ای بود. البته سابقه تلاش ها برای قانونگذاری در عرصه داخلی هر کشور در خصوص جرایم رایانه ای به زمانی قبل تر از ۲۰۰۱ بر می گردد. در آمریکا که یکی از پیشگامان در این عرصه محسوب می شود میان سال های ۱۹۷۸ تا ۱۹۸۶ تعداد ۴۵ ایالت از ایالات این کشور قانون جرایم رایانه ای را مورد پذیرش قرار دادند(رضوی فرد و موسوی، ۱۳۹۵: ۳۴).

به طور کلی جرائم رایانه از حیث ارتکاب در سه نسل مورد بررسی قرار می گیرند که عبارتند از:

نسل اول: جرائم رایانه ای: که تا اواخر دهۀ ۸۰ مصداق داشت و بیشتر شامل سرقت، کپی برداری از برنامه ها، سرقت تحقیقات و جرائم علیه حریم خصوصی در رایانه بود.

[1] PAUL BARAN

نسل دوم: جرائم علیه داده ها: که با گسترش فناوری تبادل اطلاعات و ارتباطات بین المللی در دهه ۹۰ ظهور کرد و تمام جرائم علیه فناوری اطلاعات و ارتباطات و رایانه را شامل می شود.

نسل سوم: جرائم سایبری: جرائم رایانه ای که از اواسط دهه ۱۹۹۰ آغاز می شود به جرائم سایبری یا جرائم در محیط سایبر معروف است.

به طور خلاصه می توان گفت که در ابتدا مسئله آنلاین بودن چندان چشمگیر نبوده و چگونگی انتقال داده ها به شکل امروزی وجود نداشته و لزوماً با مخابرات نیز پیوستگی وجود نداشته است، اما ابتدا مسئله «واسط» در آن قابل توجه بوده (نسل اول) و بعدها تمرکز در نسل دوم بر محتوا بیشتر شد و در نهایت تجمع رایانه ها، مخابرات الکترونیکی خاص و محضی را تحت عنوان فضای رایانه ای (فضای مجازی) به وجود آورده که مسائل کیفری ناشی از آن به گونه ای متفاوت و متمایز نسبت به جرائم رایانه ای در دهه ۶۰ و ۸۰ می باشد(تقی زاده و همکاران،۱۳۹۶: ۱۱۵).

۲-۲- تاریخچه تدوین قوانین سایبری در ایران

همسو با کشورهای جهان ایران نیز برای کنترل فضای اینترنت و پیشگیری و برخورد با جرایم سایبری اقدامات قانونی در این زمینه انجام داده است. لازم به ذکر است که اولین بار 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 تمایزی چندان بین جرم رایانه ای و جرم اینترنتی وجود ندارد، عمل آن‌ها به عنوان جرم اینترنتی محسوب می‌شود. پس از این بود که گروه‌های هکر، جرم‌های دیگری را مرتکب می‌شدند، مواردی چون جعل اسکناس، اسناد و بلیط‌های شرکت‌های اتوبوسرانی، جعل اسناد دولتی از قبیل گواهینامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک‌های مسافرتی و عادی بخشی از این جرائم اینترنتی هستند(حقیقی، ۱۳۹۵: ۵). در همین راستا در سال ۱۳۸۰ مسؤلان وقت پلیس آگاهی کشور، اداره کل مبارزه با جرایم رایانه ای را پایه گذاری کردند. با بروز جرایم رایانه ای و نبودن ابزارها و تجهیزات و از همه مهم تر، قانون مشخص، مشکلات عدیده ای در مسیر پیشگیری و کشف جرایم سایبری پدیدار شد تمام جرایم رایانه ای صرفاً در فضای مأموریتی پلیس خلاصه نمی شود. در یک جمع بندی باید گفت که تقریبا از اواخر دهه ۷۰ و ابتدای ۱۳۸۰ تدابیر گوناگونی در رده های حاکمیتی کشور در خصوص ضرورت مقابله با سواستفاده های مجرمانه سایبری اتخاذ شده که مهمترین آن ابلاغیه ۳ ماده ای مقام معظم رهبری درباره شبکه های اطلاع رسانی رایانه ای در سال ۱۳۸۰ است که می توان از آن به عنوان منشور سیاست جنایی ملی جرایم رایانه ای یاد کرد که دارای تدابیر پیشگیرانه

نیز بوده است. از سال ۱۳۸۱ فعالیت مجدد حوزه جرایم رایانه ای آغاز گردید که به تنظیم پیش نویس جرایم رایانه ای در شورای عالی توسعه قضایی قوه قضاییه منجر شد و نهایت لایحه جرایم رایانه ای بعد از گذشت ۱۵ سال از زمان تصویب توسط شورای عالی توسعه قضایی تهیه و پیشنهاد گردید که در خرداد ماه ۱۳۸۸ به تصویب شورای اسلامی رسید و مورد تایید شورای نگهبان قرار گرفت(دشتی و افشاری،۱۳۹۸: ۱۰۲)

در یک مرور خلاصه می توان عمده اقدامات قانونی و عملیاتی در حوزه مبارزه با جرایم سایبری در جمهوری اسلامی ایران به این شرح ارائه نمود:

سال ۱۳۸۱ : تشکیل معاونت مبارزه با جرایم خاص و رایانه ای در پلیس آگاهی ناجا.

اسفند ۸۷ : تهیه و ابلاغ سند امنیت فضای تولید و تبادل اطلاعات کشور توسط هیئت دولت.

تیر ۸۸ : تصویب قانون جرایم رایانه ای در مجلس شورای اسلامی و تأیید آن در شورای نگهبان.

اردیبهشت ۸۹ : تشکیل پلیس فضای تولید و تبادل اطلاعات(فتا) در ناجا.

اردیبهشت ۹۰ : تشکیل دادسراهای ویژه مبارزه با جرایم سایبری؛ تشکیل کمیته تعیین مصادیق مجرمانه به ریاست دادستانی کل کشور؛ تصویب آیین نامه های مربوط به جمع آوری و استنادپذیری ادله الکترونیکی و ...(جهانشیری و همکاران،۱۳۹۴: ۲۱).

لازم به ذکر است که در سال ۱۳۹۳ نیز آیین نامه جهت جمع آوری و استنادپذیری الدله الکترونیکی نیز در خصوص جمع آوری و محافظ از ادله و داده های الکترونیک به تصویب رسید.

۳- بررسی تطبیقی قوانین مربوط به جرایم سایبری در جهان و ایران

از ویژگی های مهم جرایم رایانه ای و اینترنتی، ماهیت فراملی بودن اینگونه جرایم است که به دلیل قابلیت های فنی رایانه ها و اجزای مرتبط با آن، امکان ذخیره سازی، حرکت، استفاده از داده ها از طریق شبکه ها و ایجاد ارتباط و انتقال سریع درسطح وسیع بین سیستم های رایانه ای افزایش یافته است، به طوری که دامنهٔ گسترش سیستم های رایانه ای از محیط رایانه و شبکهٔ داخلی به سطح بین المللی، گسترش پیدا کرده و موجب خلق نسل جدید جرایم رایانه ای یعنی جرایم در محیط سایبری شده است که ماهیت و خاصیت کاملا فراملی و بین المللی دارند. به هر حال، امروزه جرایم رایانه ای تبدیل به یک پدیدهٔ مجرمانهٔ کاملاً بین المللی شده است. در مسائل بین المللی،

اولین اثر جرایم رایانه ای، بحث صلاحیت است. علی الخصوص در قواعد حاکم بر صلاحیت سرزمینی و مکان ارتکاب، مقام صالح دچار مشکل می شود. زیرا جرایم رایانه ای، فراملی بوده که موجب تعدد محل ارتکاب و تعدد صلاحیت ها می شوند. در بحث صلاحیت ها، علاوه بر موضوعاتی از قبیل تابعیت مجرم، تابعیت بزه دیده، نو ع جرم ارتکابی بحث صلاحیت شخصی و واقعی نیز مطرح می شود(صبح خیز،۱۳۹۴: ۱۲۷). در طول قرون متمادی، سیستم های قضایی بر موضوعات ملموس و عینی متمرکز شده اند و مقررات جزایی به حمایت از این دسته موضوعات پرداخته است. این در حالی است که امروزه اموال غیر مادی اهمیت بسیار یافته اند. داده ها و اطلاعات تبدیل به نوعی دارایی شده اند که می توان موضوع ارتکاب جرم واقع شود و رژیم حقوقی مربوط به موضوعات این چنینی، تنها نمی توانند بر مبنای قیاس با قواعد موجود و مختص به موضوعات مادی بنا شود؛ زیرا نحوۀ ارزیابی و حمایت داده ها و اطلاعات با آنچه در خصوص اشیای مادی مقرر است تفاوت قابل ملاحظه ای دارد. بدین سان که اشیای مادی را می توان به افراد خاصی دسترسی نسبت داد، ولی اطلاعات کالایی عمومی است که علی الاصول بنابر قاعدۀ بایستی به صورت آزادانه در جامعه جریان داشه باشد. بنابراین، آزاد به اطلاعات همچون اموال مادی مشمول حمایت انحصاری واقع نمی شود. علاوه بر این، در راستای حمایت از اطلاعات، نه تنها باید منافع مالک یا دارندۀ آن مدنظر قرار گیرد، بلکه منافع کسانی که به نحوی با محتوای اطلاعات سرو کار دارند نیز باید محفوظ بماند. پس ملاحظه می شود که نمی توانیم به قواعد موجود در زمینۀ اموال مادی بسنده کنیم و به تغییر در طرح و چهارچوب قضایی جاری نیازمندیم. حقوق جزایی ماهوی در ارتباط با جرایم رایانه ای، از دو لحاظ با مشکل مواجه است: از یک سو، اوصاف و عناصر متشکله جرایم کلاسیک دستخوش تحولاتی گشته اند؛ تا جایی که نمی توان تعاریف مجرمانۀ موجود در متن قانونی را به جرایم رایانه ای مشابه تسری دارد و از سوی دیگر، عناوین مجرمانۀ نوینی نیاز است تا برخی دیگر از راه های سوء استفاده رایانه ای را که به طور جدی جوامع بشری را تهدید می کند، به عنوان جرم شناسایی کنیم(صبح خیز، ۱۳۹۴: ۱۳۴). در ادامه به بررسی جرایم سایبری در قوانین ایران و کشورهای جهان می پردازیم:

۳-۱- آمریکا

همانطور که در بخش تاریخچه گفته شد؛ امریکا جزو اولین کشورهایی است که تلاش نموده در سطح داخلی خود اقدام به وضع قوانینی برای کنترل و جلوگیری از جرایم رایانه ای وضع نماید. این کشور درحالی که کشورهای جهان را به ایجاد قانون سایبری هماهنگی ترغیب می کند، عمدتاً بر قانون بومی خویش تمرکز کرده است. در ایالات متحده آمریکا برای مقابله با جرایم سایبری در

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: 2783-1329

عرصه ی فناوری اطلاعات و تکنولوژی ارتباطات از سال های قبل اقدامات مهمی در تدوین قوانین واعمال مجازات برمتجاوزان صورت گرفته است(صادقی و پورخاقان شاه رضایی،۱۳۹۶: ۷). در تعریفی که پلیس فدرال آمریکا از جرایم رایانه ای ارائه نموده، جرم رایانه ای هر جرمی است که در انجام آن از رایانه کمک گرفته شده باشد (رضوی فرد و موسوی،۱۳۹۵: ۳۴). در کنگره قوانین فدرال آمریکا قوانین جرایم رایانه ای در سال ۱۹۸۴ تصویب شد که شامل قوانینی جهت کلاهبرداری و سوء استفاده رایانه ای بود که به واسطه این قوانین، رابرت موریس، دانشجوی کارشناسی ارشد در دانشگاه کرنل، برای انتشار اولین "کرم" بر روی اینترنت تحت پیگرد قانونی قرار گرفت. البته پیش از این، در سال ۱۹۶۱ قوانینی در رابطه با رایانه بررسی شده بود که از سال ۱۹۸۷ به اجرا در آمد. مثلا در رابطه با کلاهبرداری با کمک رایانه در این قانون آمده است: شخصی مرتکب جرم کلاهبرداری رایانه ای است که آگاهانه دسترسی یا امکان دسترسی به رایانه یا هر قسمت آن شود؛ یا یک برنامه یا داده-هایی را به منظور گول زدن یا به عنوان بخشی از فریب افراد ایجاد کند؛ باعث خسارت رایانه یا هر قسمت آن یا مخدوش کردن و حذف هر ببرنامه یا اطلاعات مندرج در آن رایانه شود؛ یا باعث دسترسی فردی به رایانه و یا هر قسمت آن شود تا بتوان کنترل بر پول، دارایی یا به خدمات دیگر داشت. با این حکم کسی که مرتکب جرم کلاهبرداری رایانه ای می شود با توجه به سطح مالی کلاهبرداری انجام شده، مجازات می شود(اینفو تک[1]، ۲۰۱۰؛ فریبرزی، ۱۳۹۰: ۱۷۴-۱۷۳). در سال ۱۹۸۶ قانون حریم خصوصی ارتباطات الکترونیکی در آمریکا تصویب شد. به علاوه، قانون کمیسیون تجارت فدرال[2] ، مجموعه ای از قوانین برای تبلیغات آنلاین در اختیار این کمیسیون به عنوان آزانس حمایت کننده از مصرف کنندگان ایجاد شده است. در ادامه مرکز شکایت جرایم اینترنتی[3] برای مشارکت دفتر تحقیقات فدرال[4] و مرکز ملی جرایم یقه سفیدها[5] تاسیس شد. هدف این مرکز دریافت شکایتهای مرتبط با جرایم اینترنتی، تحقیقات بیشتر و توسعه آن و سپس ارجاع آن به دفترهای فدرال، ایالتی، محلی و یا دفترهای اجرای قوانین بین المللی برای رسیدگی های لازم. پلیس آمریکا در سال ۲۰۰۳ به خاطر رشد زیاد جرایم رایانه ای تاکید داشت که یک سیستم کلی و کارآمد ضروری و مورد نیاز است تا به کنترل جرایم اینترنتی

[1] InfoTech
[2] FTCA= The Federal Trade Commission ACt
[3] IC3=The Internet Crime Complaint Center
[4] FBI= Federal Bureau of Investigation
[5] NW3C =National White Collar Crime Center

بپردازد. پس از آن دولت فدرال آمریکا کتاب راهنمایی[1] در رابطه با جعل، نقض حقوق مولف و سرقت اسرار تجاری از اکتبر ۲۰۰۴ منتشر کرده است(همان: ۱۷۹-۱۷۴).

۳-۲- گروه ۸

در سال ۱۹۹۹ گروه ۸[2] (G۸) کمیته ای فرعی را برای جرایم فناوری پیشرفته که با جنگ علیه جرایم سایبری سروکار دارند ایجاد کرد و برای مبارزه با جرایم سایبری توافقنامه ای را امضا کردند که به موجب آن: نباید مکان امنی برای آنهایی که از فناوری های اطلاعات سوء استفاده می کنند، باشد. تحقیق و پیگرد قانونی جرایم فناوری پیشرفته بین المللی باید در بین همه کشورهای درگیر مورد همکاری قرار بگیرد، بدون توجه به اینکه آسیب در کدام کشوراتفاق افتاده. کارکنان پلیس برای بررسی جرایم فناوری های پیشرفته باید آموزش داده شوند و مجهز شوند. همین گروه در کنفرانس سال ۲۰۰۰ موضوع جرایم سایبری را با محیط های دیجیتال بی قانون مورد بررسی قرار داد. در حین نشست گروه ۸ در سال ۲۰۰۷ در مونیخ، موضوع استفاده تروریست ها از اینترنت بیشتر مورد بحث قرار گرفت و شرکت کنندگان با جرم دانستن سوءاستفاده تروریست ها از اینترنت موافقت کردند. این توافق شامل اعمال ویژ های که کشورها باید جرم بدانند، نمی شود(گرکی،۱۳۸۹: ۲۰۱-۱۹۹).

۳-۳- سازمان ملل

در هشتمین نگره پیشگیری از جرایم ورفتار مجرمان در سال ۱۹۹۰، دبیر کل سازمان ملل با قانونگذاری در مورد جرایم رایانه ای موافقت کرد. بر این اساس، سازمان ملل کتابچه راهنمایی را در سال ۱۹۹۴ در پیشگیری و کنترل جرایم رایانه ای منتشر کرد. در سال ۲۰۰۰ دبیرکل با بیانیه ای در مبارزه با سوء استفاده از فناوری های اطلاعات موافقت کرد که مشابهاتی با طرح گروه ۸ در سال ۱۹۹۷ نشان می دهد. در این بیانیه، دبیرکل اعمالی را برای پیشگیری از سوء استفاده از فناوری اطلاعات مشخص کرد، شامل: کشورها باید تضمین کنند که قانونهایشان محیط های امن را برای آنهایی که از فناوری اطلاعات سوء استفاده می کنند حذف می کنند؛ پلیس در تحقیق و پیگرد موارد بین المللی سوء استفاده از فناوری اطلاعات باید در میان همه کشورهای مربوطه مورد

[1] With pdf format electronic

[2] شامل ۸ کشور است که عبارتند از: کانادا، فرانسه، آلمان، ایتالیا، ژاپن، انگلیس، ایالات متحده و روسیه. ریاست گروه ۸ که ۶۰ درصد اقتصاد دنیا را در اختیار دارد هر سال گردشی می باشد.

همکاری قرار بگیرد؛ پرسنل پلیس برای بررسی سوء استفاده از فناوری اطلاعات باید آموزش دیده و مجهز شوند(گرکی،۱۳۸۹: ۲۰۱). در یازدهمین کنگره پیشگیری از جرم و عدالت کیفری در بانکوک در سال ۲۰۰۵، اعلامیه ای مورد پذیرش قرار گرفت که بر نیاز به یکسا نسازی در جنگ با جرایم سایبری تأکید داشت. در سال ۲۰۰۷ شورای اقتصادی و اجتماعی سازمان ملل با بیانیه ای در همکاری بین المللی در مورد پیشگیری، پیگیری، پیگرد و مجازات کلاهبرداری اقتصادی و هویتی و جرایم وابسته موافقت کرد. هر دو این بیانیه ها به طور شفاف چالش های جرایم اینترنتی ۳ را مورد بررسی قرار نمی دهند اما با توجه به جرایم قابل اعمال می باشند(همان:۲۰۴).

۳-۴- شورای اروپا و کنواسیون جرایم سایبری

در سال ۱۹۷۶ شورای اروپا[1] بر ماهیت بین المللی جرایم رایانه ای تأکید داشت و در کنفرانسی بر روی جنبه های جرایم اقتصادی این موضوع بحث کردند. این موضوع در دستور جلسه باقی مانده بود. در سال ۱۹۸۵، شورای اروپا کمیته کارشناسی را برای بحث در مورد جنبه های قانونی جرایم رایانه ای تعیین کرد. شورای اروپا، با در نظر گرفتن اینکه جرایم سرانجام با بررسی های متوالی در ۱۹۸۹ ، با در نظر گرفتن اینکه جرایم رایانه ای اغلب خصوصیت فرامرزی دارند؛ با آگاه بودن از نتایج موردنیاز برای یکسان سازی بیشتر قانون و اجرا، و برای بهبود همکاری قانونی بین المللی، به دولت کشور عضو توصیه کرد که: زمان بازبینی قانونگذاری هایشان با وضع قانونهای جدید، گزارش جرایم رایانه ای ارزیابی شده توسط کمیته اروپا در بررسی مشکلات جرایم، بویژه خطوط راهنما برای قانونگذاری های ملی در نظر گرفته شود. کمیته مشکلات جرایم اروپا[2] در سال ۱۹۹۶ تصمیم به ایجاد کمیته ای از کارشناسان برای بررسی جرایم سایبری گرفت. این کنوانسیون برای امضا در مراسمی در بوداپست در ۲۳ نوامبر ۲۰۰۳ ارایه شد، در این بین ۳۰ کشور کنوانسیون را امضا کردند(شامل ۴ کشور غیر عضو شورای اروپا، کانادا، ایالات متحده، ژاپن و آفریقای جنوبی که در مذاکرات شرکت کرده بودند). تا آوریل ۲۰۰۹، ۴۶ کشور امضا و ۲۵ کشور کنوانسیون جرایم سایبری[3] را مورد تایید قرار دادند. کشورهایی مثل آرژانتین، پاکستان، فیلیپین، مصر، بوتسوانا، و

[1] COE
[2] CDPC
[3] کنوانسیون جرایم سایبری معروف به «کنوانسیون جرایم سایبری بوداپست» یا به اختصار «کنوانسیون بوداپست» نخستین معاهده بین‌المللی است که به جرایم رایانه ای و اینترنتی می‌پردازد و می‌کوشد قوانین ملی را سازگار کرده، روش‌های تحقیقات را ارتقا دهد و همکاری بین کشورها را بهبود بخشد. این کنوانسیون توسط شورای اروپا در سال ۲۰۰۱ ارائه شد و از ۲۳ نوامبر ۲۰۰۱ کشورها می‌توانستند آن را امضا کنند. از ابتدای ژوئیه ۲۰۰۴ کنوانسیون به اجرا درآمد. تا سال ۲۰۱۳، ۳۹ کشور از جمله کشورهای عضو اتحادیه اروپا این کنوانسیون را مصوب نموده و ۱۲ کشور نیز آن را امضا کرده‌اند.

نیجریه بخشهایی از قانونگذاریشان را مطابق با این کنوانسیون به نگارش درآورده اند. اگر چه این کشورها هنوز کنوانسیون را امضا نکرده اند، اما آنها از فرآیند استانداردسازی یکسان سازی مورد نظر تدوین گران کنوانسیون پیروی می کنند. امروزه این کنوانسیون به عنوان ابزار بین المللی مهمی در مبارزه با جرایم سایبری شناخته می شود و توسط سازمان های بین المللی متفاوتی حمایت می شود(گرکی،۱۳۸۹: ۲۱۱).

۳-۵- قطعنامه اتحادیه بین المللی ارتباطات

اتحادیه بین المللی ارتباطات چندین قطعنامه مرتبط با موضوع جرایم سایبری را درحالی صادر نموده است که مستقیما و با مقررات و قوانین کیفری مشخص به مسئله نمی پردازند. از جمله مهم ترین این قطعنامه عبارتند از:

قطعنامه شماره ۱۳۰ صادره در کنفرانس مستقل اتحادیه در گوادالجارای مکزیک در سال ۲۰۱۰ با موضوع تقویت نقش اتحادیه بین المللی ارتباطات در ایجاد اطمینان و امنیت دراستفاده از فناوریهای ارتباطاتی و اطلاعاتی.

قطعنامه شماره ۱۴۹، صادره در کنفرانس مستقل اتحادیه در آنتالیای ترکیه در سال ۲۰۰۶، با موضوع بررسی و مطالعه ی تعاریف و ترمینولوژی در حوزه ایجاد اطمینان و امنیت در استفاده از فناوریهای ارتباطاتی و اطلاعات.

قطعنامه شماره ۵۰ صادره در مجمع جهانی استانداردسازی ارتباطات در سال ۲۰۰۸ در ژوهانسبورگ آفریقای جنوبی[1] درباره امنیت سایبری.

قطعنامه شماره ۵۲ صادره در مجمع جهانی استانداردسازی ارتباطات در سال ۲۰۰۸ در ژوهانسبورگ آفریقای جنوبی؛ با موضوع مواجهه و مبارزه با هرزنامه ها.

قطعنامه شماره ۵۸ صادره در مجمع جهانی استانداردسازی ارتباطات در سال ۲۰۰۸ در ژوهانسبورگ آفریقای جنوبی؛ در مورد تشویق کشورها به ویژه کشورهای در حال توسعه به تشکیل گروه های عکس العمل سریع رایانه ای.

[1] ITU Resoulution 50 (Johannesburg, 2008)

قطعنامه ی شماره ی۴۵ صادره در کنفرانس توسعه ی جهانی ارتباطات در سال ۲۰۰۶ در دوحه قطر؛ راجع به سازوکارهای افزایش همکاری در امنیت سایبری شامل مبارزه با هرزنامه ها (دشتی و افشاری، ۱۳۹۸: ۹۳-۹۲).

۳-۶- کنوانسیون بوداپست

کنوانسیون بوداپست به نام «پیمان جرایم اینترنتی بین المللی» نیز معروف است و اولین پیمان بین المللی ایجاد شده برای مقابله با جرایم اینترنتی است که حدود ۴۰ کشور مختلف در کنفرانس بین المللی بوداپست با موضوعات جرایم اینترنتی در ۲۳ نوامبر ۲۰۰۱ در مجارستان آن را امضا کردند. که از آن پس این پیمان به نام پیمان بوداپست معروف شد. این پیمان شامل تعاریف دقیق برای همه نوع از جرایم اینترنتی است و کیفر مربوط به هر کدام نیز مشخص شده است. در این پیمان سیستم کامپیوتری دسترسی غیرقانونی به اطلاعات، نقض قانون مالکیت معنوی تولید و پخش ویروسکامپیوتری و ترویج پورنوگرافی کودکان به عنوان یک عمل مجرمانه تعریف شده است و کشورها را موظف به الحاق به این قانون و ممنوعیت اینگونه جرمها در قوانین داخلی خود می سازد. همه کشورهایی که این پیمان را امضاء کرده اند قانون و مقررات یکسانی برای کنترل جرایم اینترنتی داشته و جهت همکاری بینالمللی یک خط تلفن استاندارد برای این بخش فراهم کرده اند. دستاورد این پیمان این است که تغییراتی عملی یا بهتر بگوییم انقلابی در قانونگذاری جرایم اینترنتی ایجاد کرده است(دشتی و افشاری،۱۳۹۸: ۹۹).

بعدها شورای اروپا در حدود ۲۰۰۶ پروژه ای جهانی در مورد جرایم اینترنتی راه اندازی کرد که به منظور تقویت ثبات داخلی بر اساس پیمان بوداپست طراحی شده بود. انقلاب قانونی و نهادی در مورد جرائم اینترنتی به حدود ۱۲۰ کشور مختلف توصیه شد؛ تحت تأثیر این فرایند مجمع عمومی سازمان ملل متحد، پیمان بوداپست را به عنوان پایه ای برای توسعه قانون و نهادی برای تحقیق و تعقیب جرایم اینترنتی ذکر کرده است و الحاق به آن را به تمام کشورهای جهان پیشنهاد کرد. سازمان ملل متحد نقش پیشگام در استانداردسازی پیمان بوداپست و مدیریت بهبود آن را بر عهده داشته است(همان).

۳-۷- ایران

قانون جرایم رایانه ای ایران مشتمل بر سه بخش و پنجاه و چهار ماده است و در بخش یکم این قانون به جرایم و مجازات مقرر در قانون می پردازد و در هفت فصل جرایم، به تقسیم بندی و در

فصل هشتم موارد تشدید مجازات را مطرح می کند. فصل یکم با عنوان جرایم، علیه محرمانگی دادهها و سامانههای رایانه ای و مخابراتی دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه ای را از مصادیق این نوع جرم شناخته و حداکثر مجازات این گونه جرایم توسط افراد عادی را بیست میلیون ریال تا شصت میلیون ریال جزای نقدی و از یک تا سه سال حبس در نظر گرفته است. عنصر مادی اینگونه جرایم، شبیه جرایم علیه امنیت در فضای واقعی است و فقط ابزار جرم تغییر یافته است. قانونگذار در فصل دوم و سوم جرایم، علیه صحت و تمامیت داده ها و سامانه های مخابراتی را عنوان نموده که عنصر مادی این نوع جرایم را میتوان مانند جرایم علیه اموال و مالکیت دانست. قانونگذار در این فصول، جرایم همچون جعل رایانه ای، تخریب و اخلال در سامانه های رایانه ای و سرقت و کلاهبرداری مرتبط با رایانه را مطرح نموده و حداکثر مجازات را برای جعل رایانه ای، حبس از یک تا پنج سال و جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال در نظر گرفته است. به نظر می رسد با توجه به اینکه جرایم رایانه ای مانند سرقت و کلاهبرداری رایانه ای ابتدا با جعل یک سایت مشهور شروع میشود قانونگذار چنین مجازات سنگینی را نسبت به دیگر جرایم در این بخش در نظر گرفته است. فصل چهارم قانون، به جرایم علیه عفت و اخلاق عمومی پرداخته و مصادیق محتویات مستهجن را بیان نموده است. عنصر مادی این جرایم مانند جرایم علیه عفت عمومی و ماده ۱۰۱ قانون مجازات اسلامی می باشد. حداکثر مجازات در نظر گرفته شده برای اینگونه جرایم، حبس از نود و یک روز تا یکسال و جزای نقدی از پنج میلیون تا بیست میلیون ریال است. فصل پنجم به مصادیق جرم هتک حیثیت و نشر اکاذیب به وسیله سامانه های رایانه ای پرداخته که عنصر مادی اینگونه جرایم مانند مواد ۱۱۳ تا ۳۱۱ قانون مجازات اسلامی می باشد. در فصل ششم مواد ۳۱۳ تا ۳۰۲ قانون مجازات اسلامی، قانونگذار مسئولیت کیفری اشخاص حقیقی و حقوقی مانند شرکتهای ارائه دهنده ی خدمات دسترسی را مشخص نموده و عدم تأمین نظر قانونگذار را جرم تلقی و حتی مجازات جزای نقدی تا یک میلیارد ریال و تعطیلی موقت در نظر گرفته است. از آنجایی که نوع خدمات این گونه شرکتها نقش به سزایی در کنترل جرایم سایبری دارند و در صورتی که موازین قانونی و اخلاقی را مانند پالیش سایتهای غیراخلاقی، رعایت ننمایند خسارات مادی و معنوی زیادی به جامعه وارد خواهد شد؛ قانونگذار چنین ضمانت اجرایی سنگینی را به نسبت سایر جرایم تعیین نموده است. ضمناً در این فصل، قانون کارگروهی را برای بررسی محتوای مجرمانه فضای سایبری تعیین نموده که این کارگروه به ریاست دادستان کل کشور دوبار در ماه تشکیل جلسه میدهد و مصادیق پالیش را رسیدگی مینمایند. این کمیته وظیفه دارد هر شش ماه در خصوص پرونده ی پالیش محتوای مجرمانه گزارشی را به روسای قوای سهگانه و شورای عالی امنیت ملی تقدیم کند. در فصل هفتم مواردی مانند توزیع و انتشار ویروس، معامله

نرمافزار، آموزش تخریب در سامانه های رایانه ای و مجازات حبس از نود و یک روز تا یکسال و جزای نقدی پنج میلیون ریال تا بیست میلیون ریال پیش بینی شده است. در فصل هشتم و قسمت آخر بخش یکم، مواردی همچون کارمند دولت یا عضویت نیروهای مسلح یا مقامات قضایی و به طور کلی عضویت رسمی و غیررسمی قوای سهگانه را که به مناسبت انجام وظیفه مرتکب جرم رایانه ای شدهاند و نیز تکرار جرم برای بیش از دو بار را جزء تشدید مجازات قلمداد نموده که مرتکب را به بیش از دو سوم حداکثر یک یا دو مجازات مقرر در قانون محکوم می نماید. در بخش دوم، قانونگذار، آیین دادرسی برخورد با جرایم رایانه ای را مشخص کرده و در ابتدا، اصل سرزمینی بودن و جرایم علیه حاکمیت جمهوری اسلامی را مطرح می کند و در ادامه نحوه ی حفظ ادله ی جرم، تفتیش و توقیف سامانه های رایانه ای را توسط ضابطان و نیزوظایف شرکتهای ارائه دهنده خدمات اینترنتی را در حفظ داده ها و اطلاعات رایانه ای مشخص می نماید. ضمنا اینکه ضابطین موظف به رعایت حریم خصوصی افراد بوده و در صورتی که ضابط برابر دستور مقام قضایی عمل نکرده باشد، مجازاتهای لازم پیش بینی شده است(دشتی و افشاری، ۱۳۹۸: ۱۰۴-۱۰۱).

به طور کلی در سطح قوانین بین المللی مصادیق جرایم سایبری عباتند از:

الف) جرائم کلاسیک با توصیف

جرائم علیه محرمانه بودن داده ها و سایبری؛ جرائمی که در این دسته قرار می گیرند جرائم سنتی محسوب می گردند. هرچند در حال حاضر به علت پیشرفت فناوری، با تجهیزات نوین انجام می شود که به عنوان مثال می توان به جعل و کلاهبرداری سایبری اشاره نمود.

ب) سامانه های رایانه ای و مخابراتی؛ از جمله جرائم این دسته می توان به شنود غیرمجاز داده های مخابراتی در یک ارتباط خصوصی یا داده های سری که واجد ارزش برای امنیت داخلی و خارجی کشور می باشند، اشاره نمود؛

ج) جرائم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی؛ تغییر، ایجاد، محو یا متوقف کردن داده های رایانه ای و مخابراتی به قصد تقلب، غیرقابل استفاده نمودن، تخریب یا اختلال در داده ها یا امواج الکترومغناطیسی، ممانعت از دستیابی اشخاص مجاز به داده ها با تغییر رمز ورود یا رمزنگاری از جمله جرائم این دسته اند؛

د- جرائم مرتبط با محتوا؛ این دسته جرائمی را در برمی گیرد که در آنها رایانه به عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم بکار گرفته می شود و فناوری اطلاعات فقط زمینه ارتکاب

آنها را فراهم می نماید. طبقه بندی ارائه شده در دهمین کنگره سازمان ملل متحد تبیین خواهد شد که بموجب آن، پنج دسته از جرائم رایانه ای به شرح ذیل معرفی شدند: دسترسی غیرمجاز؛ آسیب رساندن به برنامه ها و یا اطلاعات رایانه ای؛ خرابکاری به منظور جلوگیری از عملکرد صحیح سامانه های رایانه ای یا شبکه؛ استراق سمع و رهگیری غیرمجاز داده ها از یک سیستم یا شبکه های ارتباطی؛ و جاسوسی رایانه ای(تقی زاده و همکاران، ۱۳۹۶: ۱۴۳-۱۰۴).

جدول(۱): مقایسه مصادیق جرایم سایبری در قانون جرایم سایبری ایران و قوانین بین الملل

کشورها	مهمترین موارد و مصادیق جرایم سایبری در قوانین کشورهای جهان و ایران
ایران	محتوا علیه عفت و اخلاق؛ محتوا علیه مقدمات اسلام؛ محتوا علیه امنیت و آسایش عمومی؛ محتوا برای ارتکاب جرایم رایانه ای؛ محتوا علیه مقامات و نهادهای دولتی؛ امور سمعی و بصری و مالکیت معنوی
آمریکا	پست الکترونیکی مجرمانه؛ نامه های الکترونیکی ناخواسته؛ نامه های متقلبانه؛
کنگره سازمان ملل متحد	دسترسی غیرمجاز؛ آسیب رساندن به برنامهها و یا اطلاعات رایانه ای؛ خرابکاری به منظور جلوگیری از عملکرد صحیح سامانه های رایانهای یا شبکه؛ استراق سمع و رهگیری غیرمجاز داده ها از یک سیستم یا شبکه های ارتباطی؛ و جاسوسی رایانهای
کنوانسیون جرائم رایانهای شورای اروپا	دسترسی غیرقانونی یا غیرمجاز؛ شنود غیرقانونی یا غیرمجاز؛ مختل کردن داده ها؛ مختل کردن سامانه ها؛ سوء استفاده از دستگاه ها؛ جعل مرتبط با رایانه و کلاهبرداری رایانه ای؛ جرایم مرتبط با هرزه نگاری کودکان؛ جرائم مرتبط با نقض حق نشر و حقوق مرتبط؛
مصادیق جرم سایبری در قوانین بین المللی	جعل و کلاهبرداری سایبری؛ سامانه های رایانه ای و مخابراتی؛ شنود غیرمجاز داده های مخابراتی در یک ارتباط خصوصی یا داده های سری که واجد ارزش برای امنیت داخلی و خارجی کشور؛ جرائم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی؛ جرائم مرتبط با محتوا؛
کنوانسیون جرایم سایبری	جرایم علیه محرمانه بودن، تمامیت و دسترسی به سامانه ها و اطلاعات رایانهای؛ جرایم مربوط به رایانه؛ جرایم مربوط به محتوای رایانه ای؛ جرایم مربوط به کپی رایت.
کنوانسیون بوداپست	دسترسی غیرقانونی به اطلاعات، نقض قانون مالکیت معنوی؛ تولید و پخش ویروس کامپیوتری و ترویج پورنوگرافی کودکان.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: 2783-1329

در بررسی خط مشی ها، موافقت نامه ها و اقدامات راهبردی، آنچه قابل مشاهده بود این بود که هر کشور با یک همبستگی شدید اقدام به تدوین قوانینی با ضمانت اجرایی بالا برای کنترل و جلوگیری از جرائم سایبری نموده است. این تمرکز راهبردی شامل تغییر در رویکرد امنیت سایبری از کشف ساده جرم و مبارزه با جرائم جنایی در فضای سایبری به صورت موضعی تا چالش های پیچیده تر ازجمله حفاظت از زیرساخت های ملی در برابر حملات سایبری، چه حملات خارجی و یا چه داخلی کشور می باشد.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: 2783-1329

نتیجه گیری

با توجه به مطالعات انجام شده می توان گفت که موضوعات مرتبط با فضای سایبری از جمله جرایم سایبری، امروزه یک مقوله مهم در قوانین مجازات و جرم شناسی کشورهای جهان می باشد. بدیهی است که هنوز نیز با توجه به گذشت سالها از ابداع اینترنت مطالعات نشان می دهد که هنوز قوانین مربوط به فضای سایبری علی الخصوص در زمینه جرم شناسی سایبری دارای خلاء های قانونی بسیاری است. البته کنشگران عرصه بین المللی چون سازمان ملل و اتحادیه اروپا تلاش های زیادی برای قانومند نمودن این فضا انججام داده اند که به انها در این مقاله اشاره گردید. قوانین بین المللی در راستای قاعده مندسازی فضای سایبری علاوه بر تعریف جرایم سایبری مصادیق جرایم و مجازتهای مربوط به آن را تقنین نموده اند. درایران نیز از ال ۱۳۸۸ قوانین مربوط به جرایم رایانه ای در توافقنامه ای با همین عنوان تصویب شد و تلاش شد تا از نظر شارع قانون مصادیق جرم سایبری در فضای سایبری کشور، ارائه شود. اما به نظر می رسد که از نظر مصادیق و تعاریف جرم سایبری قانون جرایم رایانه ای کشور تار رسیدن به سرایط ایده آل راه درازی در پیش دارد.

منابع

۱- آناهید، فاطمه و حسن یوسف زاده، (۱۳۹۵)، بررسی جرایم رایانه ای ایران در مقایسه باسایرکشورها، کنفرانس ملی پدافند غیرعامل در قلمرو فضای سایبر، مراغه، دانشگاه آزاد اسلامی واحدمراغه.

۲- بهره مند، حمید و داودی، ذوالفقار، (۱۳۹۷)، پیشگیری اجتماعی از جرایم امنیتی ـ سایبری، مطالعات حقوق کیفری و جرم شناسی، دوره ۴۸، شماره ۱: ۴۶-۲۷.

۳- پرویزی، رضا، (۱۳۸۴)، پی جویی جرائم رایانه ای، تهران: جهان جا جم.

۴- تقی زاده، مهرداد؛ زمردی، کیوان و حاجیان، مهدی، (۱۳۹۶)، نقش اتحادیه اروپا در قاعده مند سازی جرائم سایبری، فصلنامه علمی ـ ترویجی مطالعات بین المللی پلیس، سال ۷، شماره ۲۹: ۱۰۴-۱۴۳.

۵- جاویدنیا، جواد، (۱۳۸۸)، جرایم تجارت الکترونیکی، تهران: انتشارات خرسندی.

۶- جوان جعفری، عبدالرضا، (۱۳۸۹)، جرایم سایبری و رویکردافتراقی حقوق کیفری (بانگاهی به قانون مجازات اسلامی بخش جرایم رایانه ای)، مجله دانش و توسعه، سال ۱۷، شماره ۳۴: ۱۹۱-۱۶۹.

۷- جهانشیری، جواد؛ حسینی، سیدمحمدرضا و ابراهیمی، احمد، (۱۳۹۴)، تبیین فرآیند تحقیقات مقدماتی در جرایم سایبری، فصلنامه پژوهش¬های اطلاعاتی و جنایی، سال ۱۰، شماره ۳: ۳۳-۹.

۸- حقیقی، لیلا، (۱۳۹۵)، مروری بر جرایم سایبری (با تاکید بر قوانین مجازات رایانه ای)، دومین کنفرانس ملی راهکارهای توسعه و ترویج آموزش علوم در ایران، ۱۸ تیرماه.

۹- دشتی، بیتا و افشاری، مریم، (۱۳۹۸)، مطالعه تطبیقی جرایم سایبری در ایران و حقوق بین الملل، پژوهشنامه حقوق تطبیقی، سال ۳، شماره ۴: ۱۱۰-۸۳.

۱۰- رضوی فرد، بهزاد و موسوی، نعمت اله، (۱۳۹۵)، مسئولیت کیفری در فضای سایبر در حقوق ایران، ژوهش حقوق کیفری، سال ۵، شماره ۴۵:۱۶-۲۹.

۱۱- زرگر، علیرضا، (۱۳۸۵)، امنیت و تهدید در جامعه اطلاعاتی، تهران: انتشارات قدیم.

۱۲- زیبر، اولریش، (۱۳۹۰)، جرایم رایانه ای، ترجمه محمدعلی نوری، رضا نخجوانی و مصطفی بختیاروند و احمد رحیمی، تهران: انتشارات گنج دانش.

۱۳- شیرزاد، کامران، (۱۳۸۸)، جرایم رایانه ای از منظر حقوق جزای ایران و حقوق بین¬¬الملل، تهران: انتشارات شرکت بهینه فراگیر.

۱۴- صادقی، فائزه و پورخان شاه رضایی، زینب، (۱۳۹۶)، بررسی تطبیقی قوانین جزایی ایران و امریکا در جرایم سایبری، پنجمین کنفرانس بین المللی رویکردهای پژوهشی در علوم انسانی و مدیریت، ۲۴ آذرماه.: ۸-۱.

۱۵- صادقی، مهدی، (۱۳۹۴)، بررسی حقوقی جرایم رایانه ای در ایران و سایر کشورها، اولین کنفرانس بین المللی علوم انسانی با رویکرد بومی اسلامی و با تاکید بر پژوهش های نوین، ساری، بسیج اساتید دانشگاه پیام نور استان مازندران، شرکت علمی پژوهشی و مشاوره ای آینده ساز.

۱۶- صبح خیز، رضا، (۱۳۹۱)، بررسی تطبیقی جرایم سایبری در نظام حقوق بین الملل و حقوق ایران، (پایان نامه کارشناسی ارشد)، دانشگاه آزاد اسلامی واحد مراغه.

۱۷- صبح خیز، رضا، (۱۳۹۴)، چالش های حقوقی جرایم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران، فصلنامه پژوهش های اطلاعاتی و جنایی، سال ۱۰، شماره ۳: ۱۳۷-۱۱۷.

۱۸- فتاحی، مختار، (۱۳۹۷)، بررسی عناصر تشکیل دهنده مادی ومعنوی مصادیق جرایم رایانه ای، نشریه قانن یار، شماره ۶: ۱۲۰-۹۹.

۱۹- فریبرزی، الهام، (۱۳۹۰)، سیر تحول قوانین مرتبط با جرایم رایانه ای در ایران و جهان، فصلنامه علمی و تخصصی فقه و تاریخ تمدن، سال۷، شماره ۲۷: ۱۸۵-۱۵۷.

۲۰- گرکی، مارکو، (۱۳۸۹)، جرایم سایبری: راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، تهران: نیروی انتظامی جمهوری اسلامی ایران.

۲۱- وطنی، امیر و اسدی، حمید، (۱۳۹۵)، سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگ یهای خاص این جرائم، پژوهشنامه حقوق اسلامی، سال ۱۷، شماره ۱: ۱۲۶-۹۹.

ISSN: 2783-1329
شماره مجوز انتشار: ۸۷۰۱۹

Examining the similarities and differences of cybercrime laws in Iran's computer crime law and international laws

Mostafa Abasi[1] / Mohadeseh Ghavamipour Sereshkeh[2] / Hamed Nabizadeh[3]

Abstract

In recent years, with the expansion of global activities and communications in cyberspace and the development of networks and platforms based on cyber and cloud space, we have seen an increase in the number and variety of internet and cyber crimes. It is obvious that in order to control crimes in a new platform such as the Internet and cyber space, we also need to formulate laws and norms with high enforcement guarantees to prevent, control and deal with cyber crimes. In this article, we have an overview of the activities carried out in the field of the adoption of cybercrime laws at the domestic and international level. It should be noted that the history of the adoption of cyber laws in the world goes back to 1978 in America and the last law passed in this field also goes back to the agreement approved in the Convention on Cybercrimes in 2009. Iran also passed the law of computer crimes in 2018 after investigations in different periods of time. With all these efforts, it seems that with the ever-increasing progress of technology and the increase in the variety and extent of use of cyber space, the laws related to this field, unlike traditional crimes, need constant and continuous review.

keywords: cyber space, computer crimes, cyber crimes, international laws.

[1] PhD student in criminal law and criminology, Islamic Azad University, Lahijan, Iran. (Corresponding Author)
abbasi.mostafa.96@gmail.com
[2] PhD student in criminal law and criminology, Islamic Azad University, Lahijan, Iran.
mohadesehghavamipour@gmail.com
[3] Doctoral student of private law, Azad International University, Ares, Iran.
lawyer.nabizadeh@gmail.com