جرایم رایانه‌ای در پرتو حقوق بین الملل

احسان پهلوانی فرد[1]، علیرضا حسنی[2]

تاریخ دریافت: ۱۳۹۱/۰۵/۰۷

تاریخ پذیرش: ۱۳۹۱/۰٦/۲٤

چکیده

در عصر تکنولوژی به کمک فناوری و اطلاعات، ما دائما در حال ورود به عرصه جدیدی از علوم و فناوری هستیم که تاثیر گزافی بر تمام جنبه های زندگی ما گذاشته است. هیچ شکی وجود ندارد که سیستم های رایانه ای نقش اساسی در بازی دارند. با ظهور اینترنت در این عرصه، که نقش بسزایی را در فرصت ها و بازارهای جدید، برای بسیاری از افراد کسب و کار ایفا نموده است. در مقابل انقلابی در اطلاعات ایجاد شده که پرتو آن سراسر دنیا را احاطه کرده است. با افزایش استفاده از شبکه های کامپیوتری به عنوان ابزار به اشتراک گذاری داده ها، نیاز به حفاظت و حفظ یکپارچگی داده ها مطرح می شود. به دلیل افزایش دسترسی غیر مجاز از سیستم های کامپیوتری و سوء استفاده های افراد از این ابزارها در عرصه بین المللی نیازمند همکاری بین المللی هستیم. در این نوشتار تلاش گردید با مطالعه کتابخانه ای نقش سازمان های بین المللی و همچنین رویکرد جرم رایانه ای در عرصه ی بین الملل مورد توجه قرار گیرد .لازم به ذکر است که حجم مقاله محدود می باشد و سعی گردیده به بررسی اجمالی مورد بحث بپردازیم.

واژگان کلیدی: *جرایم رایانه‌ای، قانون جرایم رایانه‌ای، فضای سایبری.*

---

[1] دانشجوی کارشناسی ارشد حقوق بین الملل دانشگاه آزاد اسلامی واحد دامغان.

[2] دکترای حقوق خصوصی، عضو هیات علمی دانشگاه آزاد اسلامی واحد دامغان، وکیل پایه یک دادگستری.

مقدمه

در دنیای مجازی، افراد می‌توانند فارغ از محدودیت‌هایی چون مرزهای ملی، حاکمیت سیاسی، نظارت سازمان ها، مراجع مختلف، زبان، ملیت، نژاد، جنسیت و ... از هر کجای دنیا و در هر زمان با جوامع مختلف ارتباط برقرار نمایند، با آنها وارد گفتمان شوند و از نظرات آنها مطلع گردند. پس از گذشت انقلاب صنعتی که با بهره‌گیری از ابزارها و وسایل پیشرفته صنعتی، در امر تولید کالا تحولات شگرفی در سطح دنیا به وجود آورد و عصر صنعتی را رقم زد، اکنون پس از گذشت قرن ها دچار «انقلاب اطلاعات» شده ایم که تاثیرات آن نسبت به انقلاب صنعتی بیشتر است که در مقابل عواقب این دگرگونی اطلاعات شامل یک ایالت یا یک سرزمین مشخص نیست بلکه شامل تمام جوامع می گردد.

در دنیای مجازی همه کارکردهای دنیای واقعی انجام می شود با این تفاوت که فارغ از محدودیت‌های فیزیکی شکل می‌گیرد و بدون توجه به مکان و زمان و ... به وقوع می‌پیوندد و اثراتی که این جامعه مجازی می‌گذارد بسیار بیشتر از جامعه واقعی است. جامعه عاری از جرم تا به حال وجود نداشته و پس از این نیز وجود نخواهد داشت. با تحولات جامعه، جرایم نیز متحول شده است. با رشد جامعه، جرایم نیز رشد می کنند. فناوری های جدید، علاوه بر اینکه امکان ارتقاع جامعه را به وجود آورده، برای مجرمان فرصت خوبی را ایجاد نموده تا به راحتی بتوانند از افراد جامعه سوء استفاده کنند.

بیان مساله

توسعه روز افزون فضای مجازی، منجر به اثرات مثبت و منفی گردیده است. با ویژگی‌هایی که این جرم نسبت به بقیه جرایم دارد حایز اهمیت است که این جرم را موشکافانه نگاه کرد اما در این مقاله فقط به چند مورد از ویژگی‌های آن اشاره می‌شود. این فضا منجر شده که به حریم خصوصی افراد توجه نکرده و وارد مرزهای ملی و ایالتی شده و از اطلاعات اشخاص سوءاستفاده کرده و اثراتی جبران ناپذیر بر جای بگذارد. در دنیای واقعی برای ورود به حریم خصوصی به ناچار باید در آن مکان حضور یافته تا لفظ نقض حریم خصوصی را بیان کنیم، ولی در دنیای مجازی به این شکل نیست بلکه زیان‌زننده (مرتکب جرم رایانه ای) در فضای مجازی وارد شده و بدون متوجه شدن قربانی اطلاعاتی را تغییر یا برداشته و در نتیجه زیان آور بدون ورود به مکانی که قربانی در آنجا اطلاعات گذاشته، به هدف خود رسیده و شاید تا مدت های طولانی قربانی متوجه، نبود اطلاعات نشود. یکی از ویژگی‌های بارز این جرم فراملی بودن آن است. با توجه به این ویژگی اثر آن بر محدوده خاصی از یک سرزمین یا کشور معین یا ایالتی خاص نبوده بلکه یک مسئله بین‌المللی است. به خاطر همین ویژگی در رسیدگی به پرونده این نوع از جرایم، چندین کشور یا ایالت ممکن است درگیر باشند. مجرم در کشور دیگر فعالیت می‌کند ولی اثر آن در سرزمین بروز می‌کند. مجرم با توانایی‌هایی که دارد می تواند وارد تسلیحات هسته‌ای سازمان شود و اختلالاتی ایجاد نموده و یا وارد سیستم برق شده و در آنجا باعث قطعی برق یک منطقه شود و مجرم بدون حضور فیزیکی دست به این کارها می‌زند.

یافته های تحقیق

افزایش بزه دیده: ویژگی بعدی که نگرانی فراوانی را ایجاد نموده افزایش بزه دیده است. مجرم می‌تواند یک فرد یا یک سازمان خاص باشد اما تاثیرات آن را بر روی یک سرزمین یا چند کشور بگذارد. مثلاً وارد سیستم بانکداری شود و اطلاعات صاحبان حساب را تغییر داده یا وارد سیستم تسلیحات هسته‌ای شده، با ترفندهای خاص بمبی را فعال نموده و بمب فعال شده را به سمت یک ایالت یا چند کشور هدف گیری کند و با پرتاب بمب چندین هزار قربانی بر جای گذارد. نکته جالب توجه اینجاست که مجرم گاهی اوقات اطلاعات شخصی افراد را برداشته و آنها را تهدید می‌کند و چنانچه مراجع قضایی را مطلع کنند عکس‌ها و فیلم‌ها و کل اطلاعات شخصی آنها را در اینترنت در دسترس همه قرار می دهند در آخر قربانی از ترس آبروی خود به مراجع گزارش نمی‌دهد. یا مجرم زمانی که اختلال در یک شرکت معتبر وارد می‌کند آن شرکت از ترس اینکه اعتبارش زیر سوال برود از مطلع کردن مراجع قضایی استنکاف ورزیده و در مقابل، مجرم با آسودگی خاطر به کارهای خود ادامه می‌دهد. در واقع یکی از معضلاتی که این جرم دارد، نداشتن اطلاعات دقیق از مجرم می باشد که نیازمند همکاری بزه دیده است.

افزایش خسارت وارده: با افزایش چشمگیر سوء استفاده از رایانه که منجر به افزایش قربانیان گردیده در نتیجه تاثیر مستقیم بر افزایش خسارات داشته است. خسارات ناشی از این جرم بسیار زیادتر از دنیای واقعی است زمانی که یک شخص یا سازمانی وارد اطلاعات یک کشور شده و از اطلاعات محرمانه و سری آن مطلع شود، امنیت آن کشور زیر سوال رفته و در نتیجه خسارات وارده به این کشور بسیار زیاد است. مجرم به آسانی می تواند با ورود به سیستم بانکی، چندین هزار صاحب حساب در بانک را دچار سرگردانی کند و حساب آنها را مختل کند یا وارد

سیستم هوایی کشور شده و سیستم های هوایی را مخدوش نماید (باستانی، برومند: ص ۱۵ و ۲۴).

دیدگاه جرم شناسان نسبت به این جرم

جرم شناسان در طبقه بندی جرایم، این جرم را در حوزه «جرایم یقه سفید» مورد بررسی قرار می‌دهند. ادوین ساترلند آمریکایی که در سال ۱۹۰۴ میلادی بیان کرد مجرمان این جرم باهوش‌ترین مجرمین به حساب می‌آیند. با، هوش بالای خود و اطلاعات کافی از رایانه توانسته‌اند به آسانی به خواسته خود برسند. این مجرمین با ساختن ویروس‌های مختلف به شبکه‌های رایانه‌ای موجب اختلال در شبکه‌ها می‌شوند که ملازمه آن دانستن علوم رایانه همچون برنامه نویسی و ... است. مجرمین در این حوزه با دستکاری، اختلال، کاوش اطلاعات، موجب به هم ریختگی در سامانه‌های رایانه شده‌اند (جاوید نیا، جواد، ۱۳۸۸: ص ۳۲).

برخی از اصول حاکم بر فضای مجازی

واژه «فضای مجازی» اولین بار توسط ویلیام گیبسون در سال ۱۹۴۸ در رمان «غیبگو» مطرح شد. گیبسون معتقد بود فضای مجازی محیطی است که فعالیت‌های الکترونیکی در داخل آن شکل می‌گیرد. در این فضا آنچه تجربه می کنید همانند محیط واقعی است همانند صحبت کردن چهره به چهره با کسی یا خرید از فروشگاه و ... بنابراین فضای مجازی به مکانی تلقی می‌شود که گروهی از افراد با یکدیگر دیدار و مباحثه می‌کنند. این فضای جدید، فضای متمایزی

را شکل داده و نیاز دارد که حقوق جدید و نهادهای حقوقی مخصوص به خود را داشته باشد.[۱] عملکرد شبکه‌های جهانی، به مرزهای ملی توجه بسیار کمی داشته و یکی از بحث‌هایی که امروزه به طور وسیعی مطرح شده این است که رژیم حقوقی نوینی در محیط فضای مجازی مورد نیاز است. بنابراین در فضایی که مرزها هیچ معنایی ندارد صلاحیت را با کدام معیار مشخص کنیم؟ با چه قوانینی و اصولی مجرمین را تعقیب کنیم؟

اصل منع مداخله در امور کشورها

یکی از اصول مهم حقوق بین‌الملل اصل عدم مداخله در امور داخلی دولت‌ها است که حقوقدانان در روابط بین‌المللی اهمیت بسیاری بر آن قایل اند.مداخله به معنای دخالت مستبدانه کشور یا گروهی از کشورها در امور داخلی یا خارجی کشور یا کشورهاست، به منظور حفظ یا تغییر شرایط موجود، غالباً متضمن تهدید یا توسل به زور می‌باشد.[۲] مداخله ممکن است به دو صورت فردی یا مداخله دسته جمعی انجام گیرد و دارای اشکال گوناگونی است نظیر فشارهای دیپلماتیک، دعوت خود کشور از نیروی خارجی برای کمک به آن کشور و مداخله انسان دوستانه و ... را شامل می‌گردد. اصولاً دخالت در امور داخلی یک کشور تاثیرات منفی بر حاکمیت کشور گذاشته و همچنین موجب اختلال روابط بین‌المللی شده و صلح جهانی را به خطر خواهد انداخت. این اصل از اصول مهم حقوق اساسی دولت ها به شمار می‌رود که به استقلال دولت مرتبط می‌باشد.[۳]

---

[۱] خبر نامه تحولات حقوق فناوری (ظهور جامعه اطلاعاتی)، کمیته مطالعات حقوق تکنولوژی دفتر همکاری های فناوری ریاست جمهوری، شماره ۶، تهران ، اردیبهشت ۱۳۸۲، ص۲.

[۲] آرین، شهرام، شان نزول عدم توسل به زور و نزول شان آن، چاپ اول، چاپخانه گوهر، تهران، ۱۳۷۷؛ ص۸۵.

[۳] پژوهشکده حوزه و دانشگاه، اسلام و حقوق بین الملل عمومی، مولفان (محمد ابراهیمی ، سید علیرضا حسینی) زیر نظر آیت الله ناصر مکارم شیرازی،ج ۱، چاپ دوم، انتشارات سمت، تهران ۱۳۷۹ ، ص ۴۴۹.

بر طبق ماده ۱۹ میثاق بین‌الملل حقوق مدنی و سیاسی کلیه آحاد بشر، دارای حق آزادی بیان هستند که شامل آزادی در تفحص، تحصیل و اشاعه اطلاعات و افکار از هر قبیل خواه به طور شفاهی یا به صورت نوشته یا چاپ و یا به هر وسیله دیگر به انتخاب خود، می‌باشند. حال سوال اینجاست که حقوق نام برده که جزء حقوق اساسی بشر است در صورت نقض این حقوق اساسی می‌تواند توجیهی برای مداخله بشر دوستانه و در نتیجه مجوزی برای توسل به زور علیه دولت خاطی باشد؟

دولت‌های عضو سازمان ملل متحد، ضمن بند چهارم ماده دو منشور سازمان ملل متحد، متعهدند که از تهدید به زور یا توسل به آن علیه تمامیت ارضی یا استقلال سیاسی دیگر کشورها خودداری نمایند و بر اساس بند سه همان ماده، اختلافات خود را با روش های مسالمت آمیز که صلح و امنیت بین‌المللی و عدالت را به مخاطره نمی‌اندازد، فیصله دهند. همچنین بر اساس بند هفت ماده مزبور نمی‌توانند مقررات منشور سازمان ملل متحد را توجیهی برای دخالت در اموری قرار دهند که به طور ذاتی جزء صلاحیت ملی کشورها شمرده می‌شود. از طرف دیگر، دخالت بشر دوستانه در مواردی است که دولتی، حقوق اساسی مردمی را که در سرزمین او به سر می‌برند، به طور مداوم و گسترده، در معرض مخاطره قرار دهد. حال آیا در مواردی مانند نقض آزادی اطلاعات و بیان می‌توان آن را نقض حقوق اساسی شمرد و اگر چنین است آیا می‌توان متوسل به زور شد؟ با توجه به بند هفت ماده دو منشور، کشورها از دخالت در امور داخلی کشورهای دیگر ممنوع شده‌اند. لیکن این سوال مطرح است که آیا حق کسب اطلاعات و اخبار با تمام وسایل ممکن، در صلاحیت ذاتی کشورها بوده و جامعه بین‌المللی بر این اساس حق دخالت در این امر را ندارد؟ امروزه شبکه‌های ارتباطی از جمله اینترنت نقش عمده‌ای در رشد و خودآگاهی جامعه بشری و خدشه‌دار نمودن حاکمیت ملی به دلیل اینکه

فن‌آوری ارتباطات به مرزها بی‌اعتنا می‌باشد، داشته‌اند. و همین مساله پدیده جدیدی به عنوان «منافع متقابل بشری» به وجود آورده که جانشین «منافع متقابل ملی» شده است (تحریری، زهرا، ۱۳۸۳: ص ۱۰۵ – ۱۰۸).

اصل منع توسل به زور

ارتباطات جهانی از طریق شبکه‌های رایانه‌ای، امروزه دولت‌ها را با تهدید جدیدی رو به رو ساخته است. دولت‌های خارجی می‌توانند به کمک رایانه‌ها در سیستم‌های داخلی دولت‌های دیگر مانند منابع انرژی، ارتباطات دوربرد و تسهیلات مالی که می‌تواند موجب لطمه به دفاع ملی یا خدمات اساسی اجتماعی شود- وارد شده و اقدام به حملات رایانه‌ای و اطلاعاتی نمایند. شناسایی اشکال جدید سلاح‌های رایانه‌ای و تغییر مفاهیم حاکمیت و سرزمین که به وسیله بهم پیوستگی جهانی فراهم شده حقوق بین‌الملل را بر آن داشته که به تعریف مرزهای قانونی فضای مجازی بپردازد.[1] با توجه به این واقعیت که امروزه، زور غیر نظامی که با توسل به فضای مجازی صورت می‌گیرد، ممکن است به عنوان شکلی از دخالت، منجر به صدمه زدن یا آثار قاهرانه شود، یا امنیت ملی دولت‌ها را به خطر اندازد، حقوق بین‌الملل جدید نیاز به تعریف دقیق‌تر معیارها، جهت مشخص نمودن اقداماتی که به عنوان جریان اطلاعات فرامرزی رایانه‌ای مجاز هستند و اقدامات مجازی که ممکن است «حمله مسلحانه» علیه کشور دیگر محسوب شوند، دارد. همچنین به قواعد صریح تری در خصوص اقداماتی که به عنوان دفاع مشروع در پاسخ به یک جنگ اطلاعاتی مجاز است و این که چطور نهادهای بین‌المللی می‌توانند نیل به این موضوعات را

[1] . Joyner,Christopher , Information Warfare as International Coercion :Elements of Legal Framework, 2000,available at http://www.egil.org/journal/voll2/n05/120825.pdf.p.1.

تسهیل نمایند، نیاز می‌باشد. آلوین و هیدی تالفر[1] تاریخ جهان را در سه موج ترسیم نموده‌اند: موج کشاورزی، موج صنعتی و موج اطلاعات. امروزه تکثیر و رشد جهانی رایانه‌های به هم پیوسته، استفاده از اینترنت را به صورت فزاینده ای نمو داده است و انقلابی در جوامع، ارتباطات جهانی و حتی تجارب، به وجود آورده است.[2] در همین راستا، عصر اطلاعات، فرصت‌هایی را برای وقوع (جرم مجازی[3])، (جنگ مجازی) یا (جنگ اطلاعاتی) فراهم نموده است. عصر اطلاعات باعث شده که روش‌ها و ابزارهایی که دولت ها به وسیله آن، در صحنه بین‌المللی از خود عکس العمل نشان می‌دهند، در حال تغییر باشد. نحوه به کارگیری حقوق بین‌الملل نسبت به استفاده از بعضی ابزارهای جنگی معین شده است. به عنوان مثال، استفاده از سلاح‌های الکترو مغناطیس سلاح‌های مرتبط با انرژی مانند: لیزر، مایکروویو و تفنگ‌هایی با فرکانس بالای رادیویی، احتمالاً می‌تواند بر اساس اصول قانونی که در خصوص سلاح‌های سنتی وجود دارد، تنظیم شوند. لیکن به کارگیری حقوق بین‌الملل موجود نسبت به حمله اطلاعاتی خیلی آسان نیست.[4] واژه حمله اطلاعاتی در واقع بیانگر این می باشد که با استفاده از ابزارهای الکترونیک و تکنولوژی برتر در جهت دسترسی یا تغییر اطلاعات در سیستم اطلاعاتی کشور قرار گرفته، بدون اینکه الزاماً موجب صدمه مبارزان یا نظامیان فیزیکی شود. که اصطلاحا به حمله شبکه های کامپیوتری (هک) گفته می شود. ماهیت جنگ اطلاعاتی، این تصور را به ذهن متبادر می‌سازد که هر چند هنجارهای حقوق بین‌الملل که در منشور ملل متحد تجسم یافته مفید هستند، لیکن این قواعد ممکن است برای رسیدن به راه‌حل های قابل قبول در خصوص تکنولوژی جدید اطلاعات و پیامدهای آن، کافی نباشند. تکنولوژی‌های جنگ اطلاعات از طریق شبکه‌های رایانه‌ای، بعد از

---

[1] Alvin & Heidi Toffler
[2] Joyner,op.cit.,p.2
[3] Cyber crim
[4] Joyner,op.cit.,p.3

جنگ سرد، مسائلی را در خصوص تعریف قانونی «حمله مسلحانه» و «دفاع مشروع» که در منشور ملل متحد مقرر شده به وجود آورده است. امروزه این واقعیت که دولت‌ها می‌توانند به زیرساخت‌های اطلاعاتی کشورهای دیگر رخنه نموده و موجب صدمات فیزیکی فراوانی شوند، مسائل پیچیده‌ای را مطرح کرده که تا قبل از آن یعنی زمانی که دولت‌ها از طریق ارتش، هواپیماها، کشتی‌ها، تانک‌ها و سلاح‌های مرسوم، به یکدیگر حمله می‌نمودند، عنوان نشده بود.[1] بر اساس این اصل نمی‌توانیم چنانچه حمله سایبری اتفاق افتاد یا متوجه شدیم که حمله سایبری در حال به وقوع پیوستن است به آن کشور خاطی حمله کنیم.

اصل آزادی اطلاعات

آزادی اطلاعات در زمره آزادی‌های نسبتاً نو ظهور است که عنوانش با محتوایش تناسب زیادی ندارد. کسانی که از روی عنوان درباره محتوای این آزادی اظهارنظر کرده‌اند غالباً دچار خطا شده‌اند و افرادی که بر اساس مبنا و محتوای این آزادی درباره عنوانش اظهارنظر کرده‌اند عنوان مذکور را مورد انتقاد قرار داده و درست ندانسته‌اند. از این رو برای مطالعه آزادی اطلاعات، لازم است معنا و مبانی آن مشخص گردد و سپس محتوا و ساز و کارهای تحقق آن، در پرتو مبانی مذکور معین شود. در این گفتار، ابتدا تعریف آزادی اطلاعات و تفاوت‌های آن با آزادی‌های مشابه بیان می‌شود و مورد بررسی و تفحص قرار خواهد گرفت.

[1] Joyner , op.cit.,p5

تعریف آزادی اطلاعات

«آزادی اطلاعات»[1] اصطلاحی است که نخستین بار در ایالات متحده آمریکا به کار رفته و در مورد محتوای خود تا اندازه‌ای گمراه کننده است. شاید تصور شود که منظور از آن، آزادی همه انواع اطلاعات است اما این تصور درست نیست. منظور از آزادی اطلاعات، آزادی دسترسی افراد جامعه به اطلاعات موجود در موسسات عمومی و برخی موسسات غیر عمومی است. با توجه به گمراه‌کننده بودن این اصطلاح، برخی کشورها از عنوان دقیق‌تری در خصوص این آزادی استفاده کرده‌اندکه نشان‌دهنده محتوای آن می‌باشد. برای مثال، فرانسه از عنوان «آزادی دسترسی به اسناد اداری» استفاده کرده است. «حق دسترسی به اطلاعات» نتیجه و محصول آزادی اطلاعات و به تعبیری، آزادی اطلاعات چهار چوب‌بندی شده است. حق دسترسی به اطلاعات یعنی هر یک از اعضای جامعه بتواند تقاضای دسترسی به اطلاعاتی را داشته باشد که در یکی از موسسات عمومی نگهداری می‌شود و آن موسسه فقط در موارد استثنایی و احصاء شده و مشخص، اطلاعات درخواستی را در اختیار متقاضی قرار دهد.[2]

تفاوت آزادی اطلاعات با آزادی‌های مشابه

آزادی اطلاعات، جایگاه و هویت مستقلی در نظام آزادی‌ها دارد که باید از ارجاع یا تقلیل آن به آزادی‌های دیگر نظیر آزادی بیان یا مطبوعات یا کلام یا ارتباطات خودداری شود. برای آگاه شدن از هویت مستقل این آزادی توجه به تعاریفی که از آزادی‌های مذکور شده ضروری است:

---

[1] Freedom of information

[2] Peter Dyrberg; Current Issues in the Debate on Public Access to Documents , European law Review ,1999, p157. Available at http://europa.sim.ucm.es:8080/compludoc/AA?a=Dyrberg%2c+peter&donde=otras & zfr=0.

در تعریف آزادی بیان آن‌گونه که در ماده (۱۹) اعلامیه جهانی حقوق بشر بیان شده، عبارت است از اینکه: «انسان از داشتن عقاید خود، بیم و اضطرابی نداشته باشد و در کسب اطلاعات و افکار و در اخذ و انتشار آن، به تمام وسایل ممکن و بدون ملاحظات مرزی آزاد باشد». آزادی مطبوعات نیز متضمن آن است که محدودیت و نظارت قبلی بر انتشار وجود نداشته باشد و مدیران یا مالکان یک نشریه آخرین حرف را در مورد آنچه می‌خواهند بنویسند یا منتشر کنند داشته باشند. از این آزادی به آزادی انتشار نیز یاد می‌شود. آزادی کلام معنایی اعم از آزادی مطبوعات داشته و آزادی در صحبت کردن، چاپ کردن، پخش رادیویی یا تلویزیونی عقاید یا اطلاعات بدون مداخله و کنترل قبلی دولت را شامل می‌شود. آزادی ارتباطات نیز اصطلاح جدیدی است که بر حق برخورداری از امکان آگاه شدن و آگاه کردن، حق شرکت در اجتماعات و بحث ها و به‌طور کلی حقوق مراوداتی تأکید دارد. هدف این آزادی، آن است که نقص آزادی های بیان، مطبوعات و اطلاعات را جبران کند. حامیان این آزادی معتقدند که آزادی‌های مذکور صرفاً به جریان‌های یک سویه اطلاعات از سوی وسائل ارتباطی به سوی مردم منتهی می‌شود ولی آزادی ارتباط در صدد است زمینه جریان دوسویه و متقابل اطلاعات را فراهم آورد.[1] محدودیت‌ها و استثناهایی بر این اصل حاکم است. این آزادی اطلاعات را نباید تفسیر غیر واقع کرد و امنیت ملی، اسرار دولتی، حریم خصوصی و... افراد را در بر گیرد و با سوءاستفاده از این اصل منجر به فاش شدن اسرار ملی و شخصی گردد و جوامع به تاراج رود (انصاری، باقر، ۱۳۸۷: ص ۲۵ – ۲۷).

[1] C.Hamelink;NOTE on the draft Declaration on the Right To Communicate,ARTICLE 19,Global campaign for Free Expression,January 2003, at http://www.article19.org /pdfs/analysi s/Hamelink-declaration -the – right-to-communic ate.pdf.

نقش سازمان‌های بین‌المللی در ارتکاب این جرم:

تعدادی از سازمان‌های بین‌المللی از زمانی که متوجه این پدیده در حوزه بین‌الملل شدند دست به فعالیت‌هایی زدند. هر چند این فعالیت‌ها کافی نبوده و برای شناخت این جرم زمان زیادی می‌طلبد و کمک می کند قوانین داخلی کشورها در این زمینه تکامل یابد. تعدادی از سازمان‌های بین‌المللی برای تجزیه و تحلیل آخرین پیشرفت‌ها در جرایم سایبری به طور ثابتی کار می‌کنند و گروه‌های کاری را برای توسعه راهبردها برای جنگ با این جرایم ایجاد کرده‌اند.

گروه G8[1]

در سال ۱۹۹۹، گروه ۸ (G8) کمیته‌ای فرعی را برای جرایم فناوری پیشرفته که با جنگ علیه جرایم سایبری سر و کار دارند ایجاد کرد. در طول نشست آنها در واشنگتن رئیس بخش دادگستری و وزیران کشور با ۱۰ اصل و ۱۰ طرح برای مبارزه با جریان فناوری پیشرفته موافقت کردند.[2] روسای گروه ۸ بعداً به این اصول صحه گذاشتند که عبارت اند از:

- نباید مکان امنی برای آنهایی که از فناوری اطلاعات سوءاستفاده می‌کنند باشد.
- تحقیق و پیگرد قانونی جرایم فناوری پیشرفته بین المللی باید در بین همه کشورهای درگیر مورد همکاری قرار گیرد، بدون توجه به اینکه آسیب در کدام کشور اتفاق افتاده است.
- کارکنان پلیس برای بررسی جرایم فناوری‌های پیشرفته باید آموزش ببینند و مجهز شوند.

[1] گروه ۸ شامل ۸ کشور می باشد: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.

[2] http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf

در سال ۱۹۹۹، گروه ۸ طرح‌هایشان را با توجه به جنگ علیه جرایم فناوری‌های پیشرفته در کنفرانس وزیران در مبارزه با جرایم سازمان یافته در مسکو مشخص کرد.[۱] آنها نگرانی هایشان درباره جرایم (از قبیل موضوعات مستهجن کودکان)، همچنین قابلیت ردیابی معاملات و دسترسی فرامرزی به اطلاعات ذخیره شده را بیان کردند. ابلاغیه رسمی‌شان شامل چند اصل در مبارزه علیه جرایم سایبری است که امروزه در تعدادی از راهبردهای بین‌المللی یافت می‌شود.

سازمان ملل[۲]

در هشتمین کنگره پیشگیری از جرایم و رفتار مجرمان (در هاوانا،کوبا، ۲۷ آگوست، ۷ سپتامبر ۱۹۹۰)، دبیر کل سازمان ملل با قانونگذاری در مورد جرایم رایانه‌ای موافقت کرد.[۳] بر این اساس، سازمان ملل کتابچه راهنمایی را در سال ۱۹۹۴ در پیشگیری و کنترل جرایم رایانه ای منتشر کرد[۴]. در سال ۲۰۰۰، دبیر کل با بیانیه‌ای در مبارزه با سوءاستفاده از فناوری های اطلاعات موافقت کرد که مشابهاتی با طرح گروه ۸ در سال ۱۹۹۷ نشان می‌دهد.[۵] در این بیانیه، دبیر کل اعمالی را برای پیشگیری سوءاستفاده از فناوری اطلاعات مشخص کرد، شامل: کشورها باید تضمین کنند که قانون‌هایشان محیط‌های امن را برای آنهایی که از فناوری اطلاعات سوءاستفاده می‌کنند حذف می‌کنند: پلیس در تحقیق و پیگرد موارد بین‌المللی

[۱] ابلاغیه کنفرانس وزیران گروه ۸ در مبارزه با جرایم سازمان یافته فراملی، مسکو،۲۰-۱۹ اکتبر ۱۹۹۹.

[۲] سازمان ملل (UN) سازمان بین المللی است که در سال ۱۹۴۵ تاسیس شد و در سال ۲۰۰۷- ۱۹۱ کشور عضو داشته است.

[3] http://www.un.org/documents/ga/res/45/a45r121.htm

[4] http://www.uncjin.org .org/Documents/EighthCongress.html

[5] http://www.unodc.org.org/pdf/crime/a_res_55/res5563e.pdf

سوءاستفاده از فناوری اطلاعات باید در میان همه کشورهای مربوطه مورد همکاری قرار گیرد: پرسنل پلیس برای سوءاستفاده از فناوری اطلاعات باید آموزش دیده و مجهز شوند.[1]

شورای اروپا[2]

در سال ۱۹۷۶، شورای اروپا (COE) بر ماهیت بین‌المللی جرایم رایانه‌ای تاکید داشت و در کنفرانسی بر روی جنبه‌های 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 جنبه‌های قانونی جرایم رایانه‌ای تعیین کرد. در سال ۱۹۸۹، کمیته اروپایی در بررسی مشکلات جرایم با «گزارش کارشناسان در جرایم رایانه‌ای» با تجزیه و تحلیل عناصر قانونی کیفری لازم برای مبارزه با اشکال جدید جرایم الکترونیک، شامل کلاهبرداری رایانه‌ای جعل‌های رایانه‌ای موافقت کرد. کمیته وزیران در سال ۱۹۸۹ با پیشنهادی موافقت کرد که به طور ویژه بر ماهیت جرایم رایانه‌ای تاکید داشت (گرگی، مارکو، ص ۲۰۷).

چالش‌های موجود در جرم رایانه‌ای:

تعداد کاربران استفاده از اینترنت روز به روز در حال افزایش می‌باشد با پیشرفت علم در این حوزه، کاربران استفاده از اینترنت بیشتر و در مقابل، سوءاستفاده‌کنندگان در این حوزه با کمترین هزینه و وقت، بیشترین صدمه را به قربانیان وارد نموده است. قربانیان هم اغلب از ترس

---

[1] گرگی، مارکو؛ جرایم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، تاثیر: پلیس امنیت فضای تولید و تبادل اطلاعات ناجا، چاپ اول ۱۳۸۹ ص ۲۰۱.

[2] شورای اروپا که مقر آن در استراسبورگ می باشد در سال ۱۹۴۹ تاسیس شد .شورای اروپا را نباید با اتحادیه اروپا و شورای اروپایی ها اشتباه گرفته شود. شورای اروپا بخشی از اتحادیه اروپا نیست بلکه سازمانی جداست.

آبرو و اعتبار خودشان از بازگو کردن هک اتفاق افتاده در سیستم خود، خودداری نموده اند. مثلاً یک شرکت معتبر اگر اطلاعاتش هک شود چنانچه کاربران از این موضوع با خبر شوند از این شرکت سلب اعتماد می شود بنابراین از بازگو کردن ماجرا به ماموران خودداری نموده. در این مبحث به چند نمونه از چالش های موجود در این زمینه می پردازیم:

عدم کنترل اطلاعات: اینترنت میلیون ها صفحه وب را روزانه در اختیار کاربران گذاشته و افراد زیادی در حال ساخت صفحات وب می باشند. این امر باعث شده که کنترل در این زمینه بسیار سخت و مشکل شود و نبود سازمان متخصص در این زمینه مشکل را دو چندان کرده است.

عدم نیاز به مکان خاص: از آنجا که اینترنت یک فضای مجازی جدیدی را برای کاربران ایجاد نموده است کاربران متخلف از این امر سوءاستفاده کرده اند و هر گونه که مایل هستند از این محیط مجازی استفاده می کنند. شخص خاطی با یک دستگاه کامپیوتر و یک خط اینترنت می تواند وارد این فضای مجازی شده بدون آنکه حضور فیزیکی داشته باشد. این مشکل زمانی هویدا می شود که بخواهیم شخص خاطی را مورد پیگرد قانونی قرار داده و دستگیر کنیم. حال آنکه به راحتی شخص خاطی از هر مکانی دست به این کار می زند و ماموران در پیگیری دچار اشتباه و سرگردانی می شوند.

مشخص نبودن هویت: سرویس های اینترنتی امکانات خاصی را برای کاربران ایجاد می کنند که بدون آنکه کاربر هویتش را عنوان کند از این امکانات استفاده نموده و در این امر موسساتی هم این امکانات را در اختیار اشخاص گذاشته اند از جمله:

- پایانه های اینترنت عمومی (فرودگاه ها و کافی نت ها)
- شبکه های بی سیم

- خدمات موبایلی پیش پرداخت که به ثبت نام نیاز ندارند
- سرورهای ارتباطات بی نام
- سایت های بدون نام
- ایجاد وبلاگ بدون ثبت نام

مجرمان می توانند هویتشان را اعلام نکنند یا از طریق آدرس های جعلی پنهان کنند در این صورت تحت تعقیب قرار دادن این افراد مشکل می شود.

نبود قانون واحد و جامع

مهم ترین چالش، نداشتن قانون جامع و واحد می باشد. از طرفی روز به روز این فضای مجازی با سرعت در حال تغییر و دگرگونی است ولی قانونگذار نتوانسته هم پای این فضا پیش رود و قانون خود را به روز کند. از طرف دیگر با پی بردن مجرم به این خلاء های قانونی مشکلات فراونی را ایجاد نموده و هم چنین هر کشور براساس سیاق خود در این حوزه قوانین را وضع کرده است که مشکل را دو چندان می کند. ممکن است شخص براساس قانون یک کشور مجرم تلقی شده و در کشور دیگر مجرم نباشد در این صورت با پی بردن به این موضوع شخص خاطی مسلماً به کشوری می رود که وی را مجرم ندانند.

نتیجه گیری و پیشنهادها

در فضای مجازی از آنجا که بعد فرا مرزی آن بیشتر مشخص است، در نتیجه یک همکاری بین المللی در این عرصه می طلبد تا کشورها در درجه اول: یک قانون جامع نوشته تا همه ی عرصه های جرم را پوشش داده و دست اشخاص خاطی را قطع کنند و هر چه خلاء قانونی وجود دارد را محو نموده است. دوم: یک قانون واحد بین کشورها نوشته شود تا قانون یک شکل و هماهنگ داشته باشیم که در عرصه ی تعقیب دچار مشکل نشویم، سوم: یک مرجع بین المللی ایجاد کنیم تا به کنترل اطلاعات و پیگیری کاربران متخلف بپردازد تا مجرم را به راحتی تحت تعقیب قرار دهیم و چهارم: افراد آموزش دیده و متخصص را در سازمان های دولتی و غیر دولتی قرار دهیم تا اسرار دولتی سازمان پخش نشود. راهکار های مناسب برای پیشگیری از وقوع جرم:

- تقویت همکاری بین المللی و منطقه ای به منظور اجرای برنامه های پیشگیری از وقوع جرم.
- به کارگیری قانون واحد بین المللی در حوزه جرایم رایانه با توجه به اصول حقوق بین الملل.
- اعطای تکنولوژی از کشورهای توسعه یافته به کشورهای در حال توسعه.
- یک سازمان بین المللی در این عرصه به کنترل داده ها و اطلاعات بپردازد و در صورت مشاهده جرم به مراجع صالح اطلاع دهد و خاطیان را تحت تعقیب قرار دهد.
- ضمانت اجرای قوی وضع شود و قاطعانه برخورد گردد.

فهرست منابع

- باستانی، برومند (۱۳۸۳). جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، تهران: چاپ اول.

- جاوید نیا، جواد (۱۳۸۳). جرایم تجارت الکترونیک، نشر خرسندی، چاپ دوم.

- خبر نامه تحولات حقوق فناوری (ظهور جامعه اطلاعاتی)، کمیته مطالعات حقوق تکنولوژی دفتر همکاریهای فناوری ریاست جمهوری، شماره ۶، تهران: اردیبهشت ۱۳۸۲.

- آرین، شهرام (۱۳۷۷). شان نزول عدم توسل به زور و نزول شان آن، چاپ اول، تهران: چاپخانه گوهر.

- ابراهیمی، محمد و حسینی، سید علیرضا (۱۳۷۹). پژوهشکده حوزه و دانشگاه، اسلام و حقوق بین الملل عمومی، زیر نظر آیت آلله ناصر مکارم شیرازی، ج ۱، چاپ دوم، انتشارات سمت، تهران.

- تحریری، زهرا، پایان نامه: جایگاه حقوقی فضای مجازی رایانه ای در حقوق بین الملل، دانشگاه تهران: شهریور ۱۳۸۳.

- انصاری، باقر (۱۳۸۷). آزادی اطلاعات، نشر دادگستر، چاپ اول.

- گرگی، مارکو (۱۳۸۹). جرایم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، تاثیر: پلیس امنیت فضای تولید و تبادل اطلاعات ناجا، چاپ اول.

- Joyner, Christopher ,<<Information Warfare as International Coercion : Elements of Legal Framework>>,2000,available at http:/ www.egil.org/journal/voll2/n05/120825.pdf.p.1

- Peter Dyrberg; Current Issues in the Debate on Public Access to Documents , European law Review ,1999 , p157. Available at

http://europa.sim.ucm.es:8080/compludoc/AA?a=Dyrberg%2c+peter&donde=otras & zfr=0.

- C.Hamelink;NOTE on the draft Declaration on the Right To Communicate,ARTICLE 19,Global campaign for Free Expression,January 2003, at http://www.article19.org /pdfs/analysi s/Hamelink-declaration -the –right-to-communic ate.pdf.

- http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf

- http://www.un.org/documents/ga/res/45/a45r121.htm

- http://www.uncjin.org .org/Documents/EighthCongress.html

- http://www.unodc.org.org/pdf/crime/a_res_55/res5563e.pdf