تحلیل حقوقی گونه‌شناسی نقض حریم‌خصوصی در فضای‌سایبر

علی صابرنژاد[1]،پری حسین‌پور[2]

چکیده

در جهان امروزی با پیشرفت فناوری وتکنولوژی، فضای جدیدی پا به عرصه روزگار نهاده است که ازآن به فضای سایبر تعبیر می‌گردد. عناصری که دراین فضا مطرح می‌گردند، جنبه‌ی مادی وعینی ندارند و به‌صورت مجازی نمود می‌یابند. مسئله‌ی امنیت نیز در این فضای مذکور بسیار حائز اهمیت می‌باشد، چرا که زمینه ساز فعالیت دراین فضا وجود اطمینان و امنیت می‌باشد، تا از ورود افسار گسیخته متخلفان به این عرصه اجتناب شود؛ و بالتبع مسئله‌ی حریم خصوصی دراین فضا اهمیت شایانی دارد، دراین محیط احتیاج به این است که از داده‌های اشخاص که نمود حریم خصوصی دراین فضا هستند محافظت‌ها و مراقبت‌های لازم به عمل آید.مقاله حاضرمی‌کوشد تا در باب حمایت از حریم خصوصی اشخاص در فضای سایبر گونه‌شناسی نقض این حریم در فضای سایبر راتحلیل نماید،در واقع این مقاله می‌کوشد تا با چنین تحلیلی وارد بررسی این موضوع شود که دیدگاه حقوق داخلی و برخی اسناد بین‌المللی دراین باب چیست و چه مقرره‌هایی را برای تحلیل حمایت از آن عرضه نموده است؟

کلمات کلیدی:فضای سایبر، حریم خصوصی، امنیت سایبری

[1] دکتری حقوق بین‌الملل عمومی، عضو هیات علمی مدعو گروه حقوق بین‌الملل، واحد بستان آباد، دانشگاه آزاد اسلامی، ایران، بستان آباد.(نویسنده مسئول)Ali.sabernejad@gmail.com

[2] کارشناس ارشد حقوق بین‌الملل

مقدمه

جامعه‌ای که فضای آن با انواع واقسام تخلفات مخدوش شود و در هر گوشه و کنار آن بتوان بزهکاران ومتخلفان را یافت که پیوسته در حال ایذاء دیگران می‌باشند، موردتوجه ورغبت هیچ کس نخواهد بود. چرا که پیداست در چنین محیط آنارشیسمی[1] نمی توان به راحتی به فعالیت پرداخت و ایمنی لازم برای زندگی در آن محیط، متصور نخواهد بود. از سویی دیگر وجود مسئله‌ای همچون امنیت از دیر باز موردتوجه بشری بوده و در ادیان آسمانی نیز موردتوجه جدی قرار گرفته است؛ تا آنجا که پیامبر اسلام نعمت امنیت را در کنار سلامتی از نعمتهای مجهول و مغفول آدمی می‌دانند، که بسیار حائز اهمیت است.

امنیت همواره به‌عنوان یکی از خواسته‌های اساسی بشر موردتوجه بوده است،به گونه‌ای که آدمی برای رسیدن به یک محیط مطلوب برای زیستن به تنهایی در آن، بسیار مشتاق بوده است و این تمایلی است به مصون ماندن ازدسترسی واطلاع سایرین که مطلوب نوع بشری است؛ چنین حیطه‌ای از زندگی انسان را حریم خصوصی[2] نامیده‌اند.

حریم خصوصی و محرمانگی اطلاعات شخصی، مهمترین و جنجالی‌ترین بحثی است که در حوزه‌ی فناوری اطلاعات وجود دارد. این موضوع قدمتی به بلندای زمانی دارد که اینترنت و شبکه‌های اجتماعی فراگیر شده است، در واقع همچنان که هیچ کس در فضای واقعی نمی-پذیرد که اطلاعات شخصی و خانوادگی خود را در اختیار دیگران قرار دهد؛ در این فضای نو نیز کسی به این فکر نمی‌افتد که خود داده‌های شخصی خویشتن را افشا کند. بنابراین در کشورهای غربی که خاستگاه فضای وب و حتی می‌توان با صداقت گفت که به وجود آورنده و اولین تقنین کنندگان قوانین در عرصه‌ی سایبر بوده‌اند و قوانین بین‌المللی را نیز اکثریت این کشورها و در اتحادیه‌ی اروپا تقنین کرده‌اند،سیاست محرمانگی[3] را یکی از ارکان کاربری اینترنت قرار داده‌اند.

---

[1] Anarchism
[2] Privacy
[3] Privacy policy

معمولاً در شبکه‌های اجتماعی، جزئی‌ترین اطلاعات کاربران نیز قابل دریافت و انتشار است. علاقمندی‌ها، میزان تحصیلات، ارتباط خانوادگی، ارتباطات دوستانه، شغل، محل زندگی، محل تحصیل، محل تولد و بسیاری از جزئیات دیگر مورد سؤال قرار می‌گیرد. برخی از وب سایت‌های شبکه‌های اجتماعی، حتی رنگ مو و رنگ چشم، اندازه قد کاربر را نیز می‌پرسند. از سوی دیگر بدیهی است که هزینه‌های سرسام آور وب سایت‌ها که خدمات خود را به‌صورت رایگان عرضه می‌کنند نمی‌تواند تنها از طریق تبلیغات تأمین شود؛ و منطقی است که وب سایت‌های شبکه‌های اجتماعی مخارج خود را از طریق فروش اطلاعات تجاری و غیر تجاری که با داده کاوی از انبوهی در اطلاعات کاربران و محتواهای چندرسانه‌ای آنان به دست آمده است تأمین کنند. از این رو محرمانگی اطلاعات کاربران از سوی این‌گونه سایت‌ها ادعایی بیش نیست.

با همه‌ی این موضوعات و خطراتی که پیوسته در کمین است؛ شناختن این موضوع حیاتی است که تعرض به حریم‌خصوصی در فضای‌سایبر به چه در صورت‌هایی انجام می‌گیرد. در این مقاله ما نیز آن را بررسی می‌کنیم و صور مختلف آن را برشمرده و توضیح می‌دهیم.

۱.فضای سایبر

اصطلاح فضای سایبر [۱] یا فضای هدایت شده، نخستین بار در سال ۱۹۲۸ میلادی در یک داستان علمی [۰] تخیّلی به کار برده شد. از آن زمان تاکنون فضای سایبر را به معنای مکانی غیر فیزیکی و مجازی می‌شناسیم که واقعیت‌ها را با عنوان واقعیت مجازی در فضای الکترونیکی بازتاب می‌دهد.[۲] (سایبراسپیس) توهم و تصور باطل توافقی است که انسانها خلق کرده اند، یک ناحیه واقعی است که فعالیت‌هایی در این فضا اتفاق می‌افتد از جمله تبادل و تجمیع اطلاعات. در واقع فضای سایبر محیطی است مجازی و غیرملموس که در فضای شبکه‌های

---

[۱] Cyber space

[۲] مسعودی،امیر،امنیت اطلاعات در فضای سایبر،تهران،نشریه کتاب ماه،۱۳۸۳،ص۱۶

بین المللی (که از طریق اینترنت به هم وصل می‌شوند) وجود دارد.در این محیط،تمام اطلاعات مربوط به روابط افراد،ملت ها،فرهنگ‌ها ،کشورها،به‌صورت ملموس و فیزیکی(به‌صورت نوشته ،تصویر ،صوت و اسناد)در یک فضای مجازی و به شکل دیجیتالی وجود داشته و قابل استفاده ودر دسترس استفاده کنندگان و کاربران می‌باشد ،کاربرانی که از طریق کامپیوتر،اجزای آن و شبکه‌های بین المللی به هم مرتبط هستند.[1]

عطف توجه به تعاریفی که ارائه گردیده است می‌توان مساله‌ای همچون غیر فیزیکی بودن این محیط راکه همانا ازآن به‌عنوان مجازی بودن یاد می‌شود، خصیصه‌ی بارز این محیط نامید. بااین‌حال می‌توان ویژگی‌های دیگری نیز برای محیط سایبر برشمرد که عبارتند از :

"۱.دست یابی کاربران به هرگونه خدمات اطلاعات الکترونیکی بدون در نظر گرفتن این که اطلاعات و خدمات در کدام نقطه دنیا واقع شده است.

۲-ارتباط کاربر با کاربران دیگر و استفاده از خدمات آن ها.

۳-انجام دادن معاملات تجاری در سطح بین المللی بدون دخالت فرد."[2]

از بیان تعاریف و چنین ویژگی‌هایی به‌وضوح فهمیده می‌شود، که این فضا در واقع محیطی بسیار حساس است و می‌توان از آن دونوع تعریف را ارائه نمود؛ بعضی از تعاریف بیشتر بر پایه‌ی مجازی بودن تأکید کرده و تفسیر موسعی از این فضا ارائه نموده‌اند. و بعضی دیگر با رویکردی تنگ نظرانه و تفسیری مضیق، آن را فقط حیطه‌ی کامپیوتر و اینترنت میدانند و چنین بیان می‌دارند که «حقوق سایبر شاخه‌ای از حقوق مرتبط با کامپیوتر و اینترنت است؛ که راجع به موضوعاتی مانند حقوق مالکیت فکری، آزادی عقیده و دسترسی آزاد به اطلاعات بحث می‌کند»[3]. این رویکرد در جامعه‌ی اروپایی امروزی در بین نظریه پردازان رسوخ بیشتری یافته تا آنجا که بعضی حقوق کامپیوتر و حقوق سایبر را یکی دانسته و می‌گویند: «حقوق کامپیوتر

---

[1] بای،حسین علی و پورقهرمانی،بابک،بررسی فقهی و حقوقی جرایم رایانه ای،قم،پژوهش گاه علوم و فرهنگ اسلامی،۱۳۸۸،ص۲۱

[2] همان،ص۲۲

[3] black-law-dictionary,approaches to cyber space,london,ashgate publishing,2004,p.744

شاخه‌ای از علم حقوق است که فناوری اطلاعات را قانونمند می‌کند، فناوری اطلاعات در ابتدا شامل کامپیوتر هاست، امّا به‌طور بالقوه شامل وسایلی که اطلاعات را متقل می‌کند مانند ارتباطات راه دور و پخش گسترده نیز می‌شود».[۱] با توجّه به قسمت آخر این تعریف می‌توان آن را شامل رسانه‌های گوناگون نیز دانست، البته باید افزود که تعریف ارائه شده به دلیل توصیفی که در قسمت آخر دارد قابل قبول تر است.چرا که بیان کننده‌ی این تعریف، خود ذهنیتی باز نسبت به فضای سایبر دارد و می‌توان گفت بعضی مواقع آن را به‌صورت مصداقی تحلیل می‌نماید؛[۲] تا آن جا که در بیان دیگر می‌افزاید فناوری اطلاعات این امکان را به وجود آورده اطلاعاتی که قبلا پدیده زودگذری بود،در واسطی فیزیک مانند استقرار یافته و همچون متاع فیزیکی قابل تجارت باشد.[۳]که این چنین نگاهی به فناوری اطلاعات علاوه بر بیان مصداقی، بیانگر درک عمیق نویسنده‌ی آن است چرا که در دهه‌ی ۱۹۹۰ واژه سایبرجایگزین عناوین دیگری مانند فناوری اطلاعات و ارتباطات و حقوق انفورماتیک شد و مشتقات زیادی از آن مانند"سایبرکافی"[۴] و"سایبر لا"[۵]ساخته شد.[۶]

آن‌چه که مهم است، این‌که امروزه این فضا از اهمیت شایانی برخوردار می‌باشد، کلیه بخش‌های اقتصادی تمامی کشورها، از جمله امکانات دولتی و خصوصی، بانکداری و امورمالی، حمل و نقل، تولید، پزشکی، آموزش و پروش و دولت، همگی برای انجام عملیات روزانه وابسته به رایانه هستند. فضای سایبر ابزاری برای قدرت و ثروت است.[۷]

---

[۱] Reed,chirs,computer law,blackstone press,1993,p.2

[۲] پورقهرمانی، بابک، صابرنژاد، علی، حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل،انتشارات مجد،۱۳۹۳،ص۴۱

[۳] Ibid:341

[۴] Cyber Coffe

[۵] Cyber Law

[۶] حسین‌پور،پری، صابرنژاد، علی، آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل،انتشارات مجد،۱۳۹۴،ص۳۲

[۷] پورقهرمانی، بابک و صابرنژاد، علی، ضرورت تدوین قواعد بین‌الملل برای مبارزه با جنگ سایبری، چهارمین همایش مجازی بین‌الملل ایران و جهان،۱۳۹۲،ص۲۹

۲.حریم خصوصی در فضای سایبر

بحث حریم‌خصوصی در فضای سایبر همان بحث حمایت از داده هاست، و داده به معنای مشخصات و ویژگی‌ها بیشتر مدنظر است. و البته که منظور از داده‌ها در بحث حریم خصوصی نیز داده‌های شخصی[۱] است که همانا مشخصات، ممیّزات و اطلاعات مربوط به یک شخص (سوژه) معین یا قابل تمایز که موجب تمایز او از سایر افراد گروه می‌باشد. البته در برخی از کشورهای جهان سوم از جمله کشورهای آمریکایی لاتین و آفریقا تعریفی موسع از داده‌های شخصی به دست داده و بیان داشته‌اند که «اطلاعات و دانشی که بر حاکمیّت، امنیّت، ثبات اقتصادی و فرهنگ اجتماعی اثر می‌گذارد باید تحت مفهوم حمایت از داده قرار گیرند»[۲].که صد البته چنین تفسیر موسعی قابل قبول نمی باشد. به هرحال گونه‌های نقض حریم خصوصی در فضای سایبر به شرح زیر می‌باشد:

۱-۲.نفوذ[۳]، زیر نظر گرفتن[۴]

این واژه که در ترجمه‌ی انگلیسی آن واژه‌ی هک آورده شده است، رایج‌ترین نوع نقض حریم خصوصی است و می‌توان گفت که در اندیشه‌ی مردم ما بیشتر موردتوجه قرار گرفته است. این واژه نزد اهل فن کامپیوتری و سایبر در یک مفهوم عام شامل هرگونه ورود غیر مجاز، از کار انداختن سیستم و همچنین تخریب و تغییر داده‌ها می‌شود.[۵]ولی آنچه که در اینجا از واژه فوق مدنظر است، صرف نفوذ به یک سیستم اطلاعاتی می‌باشد هرچند منجر به پردازش،

---

[۱] Personal Data

[۲] قاجار قیونلو،سیامک،مقدمه حقوق سایبر، تهران،میزان،۱۳۹۱،ص۳۴۹

[۳] Hacking

[۴] Monitoring

[۵] Tulloch mitch,microsoft encyclopedia of networking,second edition, microsoft press,washington,2002,p.126

اصلاح، انتقال و یا تخریب داده‌ها نشود. مراد از واژه‌ی نفوذگر [1] نیز شخصی است که سعی در ورود غیرمجاز به یک سیستم کامپیوتری را دارد. [2]

البته باید ذکر گردد که، این مسئله مطابق اصل امنیت [3]، یک عمل تخلف آمیز به شمار خواهد آمد چرا که مطابق اصل امنیت باید کسی که داده‌ها را به دست آورده و یا دارنده داده باید تدابیر ضروری برای جلوگیری از نفوذ به این داده‌ها را به کار برد. البته دارند داده‌ها(سوژه) در صورتی که بتواند ثابت کند که نقض امنیت سیستم به لحاظ ضعف تدابیر امنیتی ناشی از ضعف سطح دانش موجود بوده و قابل انتساب به او نمی‌باشد؛ می‌تواند از مسئولیت [4] ناشی از عدم رعایت تدابیر مناسب امنیتی رهایی یابد. البته باید بیفزاییم که عمل تخلف آمیز نفوذ خود منشأ سایر جرایم و اعمال تخلف آمیز دیگری نیز خواهد بود و یکی از این اعمال تخلف آمیز که البته یکی از اموری است که همزمان با نفوذ انجام می‌گیرد، مسئله‌ی زیر نظر گرفتن می‌باشد. مبرهن است، اطلاعات زیادی در محیط سایبری وجود دارد که انگیزه‌ی کافی را برای زیر نظر گرفتن دیگری به وجود می‌آورد. وسیله‌ای که زیر نظر گرفتن فعالیت‌ها را ممکن می‌سازد، کوکی [5] نام دارد. خدمات دهندگان اینترنتی، بازاریاب‌ها و دیگر شرکت‌ها، با قرار دادن فایل کوچکی به نام کوکی در حافظه رایانه‌ی شما، یک فناوری برای زیر نظر گرفتن فعالیت‌هایتان در اختیار دارند. کوکی‌ها ماهیتاً بد یا متجاوز به حریم خصوصی افراد نیستند ولی مسیر سوءاستفاده گسترده را باز می‌کنند. در افراطی‌ترین و جامع‌ترین موارد یک شرکت اینترنتی

---

[1] Hacker

[2] اصلانی،حمیدرضا،حقوق فناوری اطلاعات،تهران،میزان،۱۳۸۴،ص۱۸۶

[3] Security Principle.

[4] بحث مسئولیت از این باب در حقوق بین‌الملل باید بیان گردد که دستورالعمل‌های اتحادیه‌ی اروپا چون در مقام تقنین نیستند و وارد جزئیات نگردیده لذا در این باب بحث خاصی مطرح نکرده‌اند ولی از محتوای کلام آنها پیداست که چنین عملی ممنوع می‌باشد.

[5] کوکی که نام کامل آن کوکی اچ تی تی پی (HTTP cookie) می‌باشد. بسته‌ای از اطلاعات است که توسط سرور به مرورگر اینترنتی فرستاده می‌شود و در صورت لزوم نیز از مرورگرهای کاربرها به سرور باز می‌گردد. ایجاد کنندگان وبگاه‌ها کوکی‌ها را می‌سازند تا امکان دسترسی بهتر به سایتشان را فراهم نمایند. لومونتولی (Lou montulli) یکی از کارمندان شرکت نت اسکیپ کامیونیکشینز (Net Scape Communications) اولین کسی بود که تکنیک کوکی را به اجرا در آورد .

می‌تواند پرونده‌ای شامل اطلاعات خرید، سلیقه موسیقیایی، اطلاعات سرمایه‌گذاری مورد علاقه، مهمترین موضوع‌های بهداشتی و سلامتی برای کاربر و مخاطب خبری مورد علاقه‌ی وی شکل دهد.[1] که صد البته چنین امری نیز مصداق بارزی از نقض حریم خصوصی می‌باشد. در حقوق ایران نیز در ماده‌ی ۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ مقرر گردیده است که: هر کس به‌طور غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال با هر دو مجازات محکوم خواهد شد، نکته جالب در این ماده بیان کرده حفاظت شدن از حریم داده‌هاست، که مسئولیت را زمانی محقق می‌داند که حفاظت و تدابیر امنیتی لازم به عمل آمده باشد.

۲-۲.جمع آوری غیر مجاز[2]

به دست آوردن و تحصیل داده‌ها باید با روش قانونی و مشروع صورت گیرد. عطف توجه به تخلف آمیز بودن جمع آوری غیر مجاز داده‌های شخصی با تأسی از بیانات نویسنده‌ی ایرانی هم عصرمان می‌توان افعال زیر را مصداق بارز عمل تخلف آمیز در این ورطه به شمار آورد.[3]

۱- جمع آوری داده‌های شخصی از طریق روش‌های غیرقانونی یا به‌صورت سری (نصب دوربین یا میکروفن‌های مخفی).

۲- جمع آوری داده‌ها بدون جلب رضایت سوژه یا اجازه صریح قانونگذار، ولو آنکه ابزار یا روش جمع آوری غیرقانونی نباشد.

۳- جمع آوری داده‌های اضافی و غیر مرتبط با هدفی که برای آن شخص سوژه موافقت خود را اعلام نموده یا قانونگذار اجازه داده است.

---

[1] جیمز پاتر،دبلیو،باز شناسی رسانه های جمعی با رویکرد سواد رسانه ای،ترجمه یزدیان،امیر،آزادی، پیام و ناد علی،منا،تهران،مرکز پژوهش‌های صدا و سیما،۱۳۹۱،ص ۴۸۱

[2] Unlawful collection of data

[3] اصلانی،پیشین،ص۱۹۲

۴- جمع آوری داده‌ها برای هدف غیرقانونی یا نامشروع ولو آنکه روش گردآوری داده‌ها قانونی باشد.

۵- خودداری از مهیا نمودن امکان انتخاب برای سوژه دایر بر اعلام موافقت یا مخالفت با جمع آوری داده‌ها آن هم به نحو مطلوب و مفید.

۶- خودداری از اعلام عواقب اعلام موافقت یا مخالفت سوژه به وی.

۷- قصور در اعلام اطلاعات کافی در باب گردآوری داده‌های شخصی، هدف چنین کاری و همچنین رویه مورد عمل در صیانت از داده‌ها.

۸- اعلام حقوق سوژه در بهره‌مندی از روش‌های تعقیب و جبران به او.

درباره‌ی حمایت‌های به وجود آمده در زمینه‌ی این نوع نقض حریم خصوصی می‌توان از دستورالعمل 95/46/EC اتحادیه‌ی اروپا نام برد، که از منظر این دستورالعمل گردآوری داده‌ها به جز در موارد مصرح مجاز در سایر موارد آن تخلف[1] محسوب می‌گردد و ضمانت اجراهای قانونی نیز بر آن مترتب است. در حقوق داخلی نیز در این باره می‌توان به ماده ۵۸ قانون تجارت الکترونیکی نظری انداخت که بیان می‌دارد: ذخیره، پردازش و یا توزیع داده و پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام-های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنان به هر عنوان غیرقانونی است ولی در این ماده کلمه ذخیره به هیچ عنوان به معنی گردآوری نیست زیرا ذخیره در مرحله نگهداری داده است نه تحصیل. ولی در ماده۱ قانون جرایم رایانه‌ای قانونگذار بیان داشته است که هر کس به‌طور غیر مجاز داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی پیدا کند ... محکوم خواهد شد. از این ماده که راجع به نفوذ و دسترسی غیر مجاز است به طریق اولی می‌توان پی برد که گردآوری غیرمجاز نیز جرم است.

---

[1] این حکم از مطالعه ماده ۱۴ این دستورالعمل که پردازش داده‌ها به جز موارد مصرحه‌ی قانونی را ممنوع می‌داند و بند ب ماده ۲ که پردازش داده‌ها را شامل گردآوری آنها نیز می‌داند، به دست می‌آید.

۳-۲.تغییر غیر مجاز[۱]

زمانی که نفوذگر غیر مجاز وارد حریم خصوصی شخصی دیگر در سیستم‌های کامپیوتری و محیط دیتا می‌شود؛ بسته به هدف او می‌توان آثاری را مشاهده کرد، که یک نمونه از آن تغییر غیر مجاز داده‌ها می‌باشد. البته به جاست که در همین جای بحث بیفزاییم، چنین اقدامی ممکن است به‌صورت‌های مختلف رخ دهد. یکی از روش‌ها وقتی است که فردی رایانه‌ی شخصی را به کنترل خود درآورد[۲] و در فعالیتی شبکه‌ای با دیگران مرتبط سازد. از این رو، بازاریاب‌ها از این شبکه به‌عنوان منبعی برای ارسال میلیون‌ها پیام به نام نشانی آی.پی[۳] شما استفاده می‌کنند. در بیشتر اوقات، صاحبان رایانه‌های شخصی که به کنترل دیگران در آمده‌اند، از این اتفاق آگاه نیستند. یکی دیگر از روش‌ها را آگهی دهندگان اعمال می‌کنند. آگهی دهندگان با استفاده از یک مرورگر کنترل صفحه‌ی شخصی شما را در اختیار می‌گیرند، یا موتور جستجوگری را در رایانه‌ی شخصی شما جای دهند. ممکن است چنین کاری بی ضرر به نظر برسد ولی این مرورگر یا موتور جستجوگر به گونه‌ای طراحی شده است که شما را فقط به سایت‌های خاصی رهنمون می‌سازد.[۴]

به هر حال می‌توان تغییر داده‌ها را در ۴ فاز مجزا (با توجه به نیت نفوذگر) مورد بررسی قرار داد:

۱-شخصی قصد خاصی ندارد.

۲-شخصی قصد تخریب رایانه‌ای[۵] دارد.

۳-شخصی قصد جعل سایبری[۶] دارد.

---

[۱] Unlawful change in the data

[۲] Hijacking

[۳] IP(Internet Protocol)

[۴] جیمز،پیشین،ص۴۹۲

[۵] Sabotage

[۶] Forgery

۴-شخص قصد نشان دادن اطلاعات کذبی را دارد.

که اگر بتوانیم به موضوع کمی جزایی‌تر نگاه کنیم مورد اول و دوم را می‌توان تخریب رایانه‌ای نامید؛ و مورد سوم نیز همان جعل خواهد بود منتهی در فضای سایبری، و مورد آخر نیز افترای عملی می‌باشد.

در حقوق بین‌الملل در کنوانسیون بوداپست سال ۲۰۰۱ میلادی مصوبات کنوانسیون توصیه-هایی به اعضا می‌کند که نشانگر توجه خاص به تخلف‌آمیز بودن این افعال می‌باشد. در بند ۱ ماده ۴ در باب ایجاد اختلال در داده‌ها مقرر می‌دارد که: «بند۱: هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع صدمه زدن، پاک کردن، خراب کردن، دستکاری یا قطع داده‌های رایانه‌ای را که به‌طور عمدی و غیرقانونی صورت گیرد جرم انگاری نماید».

و همچنین در مورد جعل نیز مقرر می‌دارد: «ماده ۷- جعل مرتبط با رایانه: هر یک از اعضا باید به گونه‌ای اقدام به وضع قانون و مقررات نماید که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع وارد کردن، تغییر، حذف یا قطع عمدی و غیرقانونی داده‌های رایانه‌ای را که منجر به ایجاد داده‌های غیر معتبر می‌شود؛ با همان قصدی که از آن انتظار می‌رفت یا در راستای اهداف غیرقانونی به‌عنوان داده‌هایی که از اعتبار کافی برخوردارند، به کار گرفته می‌شوند، چه این داده‌ها به‌طور مستقیم قابل خواندن باشد چه نباشد جرم انگاری نماید. عضو مورد نظر مقرر می‌دارد که وجود قصد فریب یا دیگر مقاصد ناروا، پیش از اتصاف مسئولیت کیفری لازم و ضروری است».

در قوانین داخلی ایران درباره تخریب داده‌ها در ماده ۸ قانون جرایم رایانه‌ای آمده است که: «هر کس به‌طور غیرمجاز داده‌های دیگری را از سیستم‌های رایانه‌ای یا مخابراتی یا حاصل-های داده حذف یا تخریب یا مختل یا غیر قایل پردازش کند. به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات مجکوم خواهد شد» و در بحث جعل رایانه‌ای نیز ماده ۶ همان قانون مقرر می‌دار که: «هر کس به‌طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد

میلیون ریال یا هر دو مجازات محکوم خواهد شد: الف) تغییر داده‌ای قابل استناد و یا ایجاد یا وارد کردن متقلبانه داده‌ها. ب) تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علایم آن ها.

و درباره نشر اکاذیب که می‌تواند در موقعیت خاصی افترای عملی نیز باشد مقرر می‌دارد: «ماده ۱۶: هر کس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر و تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۵ میلیون تا ۴۰ میلیون ریال محکوم خواهد شد. تبصره: چنانچه تغییر یا تحریف به‌صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات محکوم خواهد شد».

علی رغم تفاوت‌های زیادی که این اقدامات با همدیگر دارند ولی در همه‌ی آن‌ها فصل مشترکی وجود داد که آن‌ها را زیرمجموعه‌ی عنوانی به نام تغییر غیر مجاز داده‌ها قرار می‌دهد؛ و آن عبارتست از اینکه همه‌ی این تخلفات در یک نکته خلاصه می‌شود که شخص نفوذگر، اقدام به تغییر دادن و دستکاری داده‌ها نموده و از این طریق به هدف خود نایل می‌شود.[1] یکی دیگر از راه‌های تغییر غیرمجاز داده‌ها نیز حملات ویروسی می‌باشد. وقتی داده‌ای مورد حمله ویروسی قرار بگیرد رایج‌ترین ضرباتی که به رایانه وارد می‌شود این است که فایل‌های اطلاعاتی خراب شده یا از بین بروند.

۴-۲.سرقت هویت[2]

[1] اصلانی،پیشین،ص۱۹۸

[2] Identity theft

با ظهور اینترنت خطر سرقت هویت نیز دو چندان شد. این جرم از ناتوانی مصرف کنندگان [و کاربران] در نظارت بر گستره‌ی دسترسی به اطلاعات حساس [چه کسانی می‌توانند به این اطلاعات دسترسی داشته باشند] و شیوه‌ی حفاظت از آن‌ها ناشی می‌شود.

در فضای مجازی به‌عنوان قلمرویی که در آن ارتباطات و تعامل بین دو فرد رایانه از طریق تبادل اطلاعات دیجیتال برقرار می‌شود. عنصر هویتی که در گونه ارتباط و تعامل ضروری است اهمیت بسیار زیادی دارد. هویت دیجیتال در اصل تلاش برای ایجاد سازماندهی خودکار و یکپارچه ساختن همه‌ی جوانب جهان واقعی در جهان الکترونیکی آنلاین و ارتباط آن‌ها با هویت‌های آفلاین است.[۱]

باید بیان کرد که دستیابی به این اطلاعات به شیوه‌های متعددی امکان پذیر است، مانند سرقت کد کاربرها و شماره دسترسی، استراق سمع الکترونیکی، شانه سواری[۲] (دید زدن از روی شانه‌ی کاربر) و اتفاقی.[۳] امروزه نوعی نحوه‌ی به دست آوردن اطلاعات شخصی پدید آمده که اصطلاحاً به آن فیشینگ[۴] می‌گویند؛ که به معنای کپی همانند سازی شده از یک اینترنتی آشناست که کاربر را گمراه کرده و در واقع وسیله‌ای برای به دست آوردن اطلاعات شخصی وی به شمار می‌آید. این حملات شکل‌هایی نظیر درخواست اطلاعات از سوی بانک قلابی، اعلام برنده شدن شما در قرعه کشی و یا پیغامی از طرف شبکه‌های اجتماعی به خود بگیرد.[۵]

در حقوق بین‌الملل در کنوانسیون جرایم سایبری به اعمال موخر سرقت هویت در ماده ۶ اشاره گردیده است، ولی نه در این کنوانسیون و نه در اسناد شورا و اتحادیه اروپا هیچ اشاره‌ی صریحی به سرقت هویت نشده است. ولی در این میان، انجمن بین‌المللی حقوق جزا با پذیرش

---

[۱] شکر خواه،یونس، فضای مجازی،تهران،دانشگاه تهران،۱۳۹۰،ص۶۵

[۲] Sboulder surfing

[۳] www.ou.eduloupd/idtheft.htm

[۴] Fishing

[۵] پور قهرمانی، بابک،سرقت هویت(جعل هویت)به عنوان جرم ناشناخته رایانه ای،مراغه،همایش منطقه‌ای چالش جرایم رایانه‌ای در عصر امروز،۱۳۹۰،ص۳

خطوط راهنمایی پیشنهادی به قانونگذاران ملی در توصیه نامه شورای اروپا علاوه بر فهرست جرایم شورای اروپا، قاچاق کلمات رمز را بدون اینکه تعریف کرده باشد، در لیست جرایم آتی و به‌عنوان جرم مستقل به رسمیت شناخته است؛ و به نظر می‌رسد منظور انجمن بین‌المللی حقوق جزا همان سرقت هویت بوده است.[1]

درباره سرقت هویت در حقوق ایران متاسفانه نص قانونی خاصی که صریحاً به آن اشاره نماید نه در قانون تجارت الکترونیک و نه در قانون جرایم رایانه‌ای به چشم نمی‌خورد ولی در قانون سنتی می‌توان به ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس وکلاهبرداری (مصوب ۱۳۶۷ مجمع تشخیص مصلحت نظام) و ماده ۵۵۶ قانون مجازات اسلامی اشاره نمود.

۵-۲.انتقال غیر مجاز

انتقال غیرمجاز داده‌ها ناقص حریم خصوصی در محیط سایبری است. زیرا این اصل از این جهت قابل توجیه می‌باشد که آن‌چه دارنده یا پردازش‌گر داده را مجاز به در اختیار داشتن داده‌ها می‌کند (حکم قانون یا رضایت شخص سوژه)، لزوماً نسبت به شخص ثالث قابل تسری نمی‌باشد.[2]

از طرفی برخی از شرکت‌ها با استفاده از کوکی‌ها جای داده شده در رایانه‌های مشتریان خود، اطلاعات را جمع‌آوری می‌کنند و با تشکیل داده بنیادها آن‌ها را به یکدیگر می‌فروشند[3]. که صد البته در این مورد خاص حتی تحصیل اطلاعات هم غیرمجاز می‌باشد، ولی این موضوع حتی در جایی که تحصیل اطلاعات مجاز نیز بوده باشد به چشم می‌خورد زیرا برخی از شرکت‌هایی که اطلاعات مشتریان خود را جمع‌آوری می‌کنند؛ متعهد شده‌اند تا این اطلاعات را به فروش نرسانند. ولی سرانجام مجبور به چنین کاری می‌شوند.

---

[1] همان،ص۴

[2] اصلانی،پیشین،ص۲۰۲

[3].Selling information

در حقوق بین‌المللی درباره‌ی حمایت از این‌که انتقال غیرمجاز داده‌ها ممنوع بوده باشد، می‌توان به مواد ۲۵ و ۲۶ دستورالعمل شماره 95/46/EC اتحادیه اروپا اشاره کرد که علاوه بر بیان ممنوعیت استثناهای آن را نیز بر می‌شمارد که بر پایه‌ی چهار محور رضایت شخص و تأمین منافع حیاتی او، منافع ملی و امنیت عمومی، انتقال قراردادی و امر آمر قانونی می‌باشد.[۱]

قانونگذار در حقوق داخلی به‌نوعی به انتقال غیرمجاز داده‌ها اشاره کرد و آن ماده ۹ قانون جرایم رایانه‌ای می‌باشد: هر کس به‌طور غیرمجاز با انجام اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سیستم‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آن‌ها را مختل کند به حبس از ۶ ماه تا ۲ سال یا جزای نقدی از ۱۰ تا ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد.

۶-۲.افشای غیرمجاز

در مرحله‌ی به دست آوردن اطلاعات زمانی که اطلاعات یک شخص در اختیار دیگری قرار می‌گیرد، فقط آن شخص مجاز به استفاده بوده و در انتقال و افشای آن داده‌ها مجوزی ندارد. مگر آن‌که خلاف آن ثابت گردد و همانطور که در بند ب ماده ۲ دستورالعمل شماره 95/46/EC اتحادیه اروپا آمده، افشای داده‌ها از مصادیق پردازش می‌باشد و به موجب ماده ۷ همان سند نیز پردازش به جز موارد مصرح در قانون غیر مجاز می‌باشد یعنی اصل بر عدم پردازش است.[۲]

در حقوق داخلی در ماده ۱۷ قانون جرایم رایانه‌ای در این باره مقرر شده است که: هر کس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت و یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند، یا در دسترس دیگران قرار دهد، به نحوی که

---

[۱] http://europe.eu.int/smartapi/cqi/sga-doc

[۲]. http://www.coles.kennesaw.edu/acc/courses/sctiulzKE/mis/456EC.htm

منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

نتیجه‌گیری

با تدقیق در آن‌چه که تفصیل آن گذشت، می‌توان بیان کرد که حریم خصوصی در فضای سایبر به گونه‌های مختلفی مورد تعرض قرار می‌گیرد که مهمترین آن‌ها عبارتند از:نفوذ و زیر نظر گرفتن، جمع آوری غیر مجاز، تغییر غیر مجاز،سرقت هویت،انتقال غیر مجاز و افشای غیرمجاز.البته باید بیان کرد که این‌گونه‌های نقض به‌صورت حصری نیستند و با پیشرفت‌ها و تحولات شگفت‌آور فضای سایبر، بر این انواع افزوده خواهد گردید.

در باب حمایت از حریم خصوصی در فضای سایبر در مقابل این‌چنین گونه‌های خاص نقض آن، در سطح بین المللی در کنوانسیون جرایم سایبری۲۰۰۱بوداپست و همچنین در دستورالعمل‌های اتحادیه اروپا، مخصوصا در دستورالعمل95/46/EC، مقرره‌هایی بیان شده است،از سویی دیگر در حقوق داخلی ایران نیز در قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون تجارت الکترونیک مصوب۱۳۸۵ قواعدی در این باب به‌چشم می‌خورد ولی باید افزود که درباره‌ی گونه‌های خاص نقض حریم خصوصی در این فضا، همچون سرقت‌هویت نه در حقوق داخلی و نه در مقررات بین‌المللی مطلب خاصی به چشم نمی‌خورد و مجری‌قانون ناگزیر از اعمال قواعد قوانین سنتی بر این موضوع می‌باشد.

پیشنهادات

با توجه به نتیجه گیری‌های به عمل آمده عمده ترین مشکلی که به چشم می‌آید عبارتست از این‌که قواعد خاصی چه در عرصه‌ی بین‌المللی و داخلی، در مورد بعضی از این انواع نقض‌های حریم خصوصی-به‌طور مثال سرقت‌هویت- در فضای سایبروجود ندارد؛لذا می-توانیم قوانین فضای طبیعی را به این فضا تعمیم دهیم، ولی باید این نکته مد نظر باشد که به

خاطر تفاوت‌های فاحشی که بین فضای حقیقی و فضای سایبر وجود دارد، به جای استناد به آن ها، باید درهریک از موارد قانونگذاری‌های دقیقی صورت پذیرد.

البته فارغ از این موضوع پیشنهاد دیگری که می‌توان ارائه داد ضرورت این موضوع است که باید قواعد و قوانین تخصصی که در این موضوع تقنین می‌گردند، به‌طور مستمر مورد بازنگری قرارگیرند چرا که چنین مسئله‌ای ذات فضای سایبر است که پیوسته و مستمر در حال تغییر، تحول و تکامل است،بدیهی است که باید این نکته در نظر گرفته شود که به خاطر ذات خاص فضای سایبر، در این فضای نوین، بی‌قانونی بسیار بهتر از قانون‌هایی که به دلیل عدم شناخت دقیق این محیط،جایگاه مجرم و مبری را درهم می‌آمیزد.

منابع و مآخذ

اصلانی،حمیدرضا،حقوق فناوری اطلاعات،تهران،میزان،۱۳۸۴

بای،حسین علی و پورقهرمانی،بابک،بررسی فقهی و حقوقی جرایم رایانه ای،قم،پژوهش گاه علوم و فرهنگ اسلامی،۱۳۸۸

پور قهرمانی، بابک،سرقت هویت(جعل هویت)به‌عنوان جرم ناشناخته رایانه ای،مراغه،همایش منطقه‌ای چالش جرایم رایانه‌ای در عصر امروز،۱۳۹۰

پورقهرمانی، بابک و صابرنژاد، علی، ضرورت تدوین قواعد بین‌الملل برای مبارزه با جنگ سایبری، چهارمین همایش مجازی بین‌الملل ایران و جهان،۱۳۹۲

پورقهرمانی، بابک، صابرنژاد، علی، حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل،انتشارات مجد،۱۳۹۳

حسین‌پور،پری، صابرنژاد، علی، آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل،انتشارات مجد،۱۳۹۴

جیمز پاتر،دبلیو،باز شناسی رسانه‌های جمعی با رویکرد سواد رسانه ای،ترجمه یزدیان،امیر،آزادی، پیام و ناد علی،منا،تهران،مرکز پژوهش‌های صدا و سیما،۱۳۹۱

شکر خواه،یونس، فضای مجازی،تهران،دانشگاه تهران،۱۳۹۰

قاجار قیونلو،سیامک،مقدمه حقوق سایبر، تهران،میزان،۱۳۹۱

مسعودی،امیر،امنیت اطلاعات در فضای سایبر،تهران،نشریه کتاب ماه،۱۳۸۳

black-law-dictionary,approaches to cyber space,london,ashgate publishing,2004

Reed,chirs,computer law,blackstone press,1993,p.2

Tulloch mitch,microsoft encyclopedia of networking,second edition, microsoft press,washington,2002
http://europe.eu.int/smartapi/cqi/sga-doc
http://www.coles.kennesaw.edu/acc/courses/sctiulzKE/mis/456EC.htm
http://www.ou.eduloupd/idtheft.htm.