مسئولیت کیفری اطلاعات و داده های مجرمانه در فضای سایبر

(تاریخ دریافت ۱۳۹۶/۰۸/۰۸ ، تاریخ تصویب ۱۳۹۶/۰۹/۱۵)

الهام بیگلری فرد

دانش آموخته کارشناسی ارشد حقوق جزا و جرم شناسی

چکیده:

رشد فناوری ها و شبکه های دیجیتالی و رایانه ای تاثیر عمده ای در تحقق جامعه اطلاعاتی داشته است. به طور کلی رشد شگرف جامعه اطلاعاتی مرهون سیر تحول ابزار ارتباطی و اطلاعاتی است که روند تحول آنها از چند سده قبل آغاز گردیده است. در این پژوهش با بررسی دقیق مسئولیت کیفری ناشی از ارائه داده محتوای مجرمانه در فضای سایبر این مسئله را مورد تحقیق قرار خواهیم داد و سپس به بررسی دقیق مسئولیت کیفری انتسابی محتویات مجرمانه و عدم تامین امنیت در فضای سایبر می پردازیم و نهایتا مسئولیت ارائه کنندگان خدمات و داده های رایانه ای را در دستورالعمل تجارت الکترونیک شورای اروپا مورد بحث قرار خواهیم داد. این دستورالعمل مصوب۸ ژوئن ۲۰۰۰ در خصوص برخی از جنبه های حقوقی خدمات جامعه اطلاعاتی، خصوصاً تجارت الکترونیک در بازار داخلی و شورای اروپا ارائه داده است که در ضمن انجام این پژوهش به بررسی تمامی موارد ذکر شده می پردازیم. نهایتاً در ادامه پژوهش به شناخت و موشکافی مسئولیت کیفری ناشی از ارائه داده ها و اطلاعات مجرمانه در فضای سایبر پرداخته می شود و همچنین ضرورت تامین امنیت در فضای سایبر و مسئولیت ارائه دهندگان خدمات رایانه ای را با توجه به دستور العمل تجارت الکترونیک شورای اروپا مورد پژوهش و تحقیق و مطالعه قرار خواهیم داد.

واژگان کلیدی: فضای سایبر-جرایم اینترنتی-مسئولیت کیفری-خدمات اینترنتی-مجازات

بخش اول:مفهوم مسئولیت کیفری و ارکان و شرایط آن

به لحاظ واژه شناختی، فرهنگ دهخدا مسئول را کسی‌که از وی سؤال می‌کنند، سؤال شده، پرسیده و پرسش‌شده و مسئول بودن را مؤاخذ بودن، متعهد بودن و به سبب تعهد حفظ و حراست مورد باز خواست بودن معنا کرده است. در تعریف مسئولیت نیز آن را مصدر صناعی یا جعلی از مسئول و به معنای ضمانت، ضمان، تعهد، مؤاخذه و مسئول بودن آورده است.[1] در فرهنگ فارسی معین نیز «مسئولیت» به «معنای مسئول یا موظف به انجام کاری» و مسئول در دو معنا به معنای «چیز خواهش شده (مفعولی)، یا کسی‌که فریضه‌ای بر ذمه یه دارد که اگر بر آن عمل نکند بازخواست شود (فاعلی)» تعریف شده است.[2]

بند اول:تعریف مسئولیت کیفری

مسئولیت به معنای اصطلاحی در حقوق نیز از وجه تسمیه‌ی لغوی آن دور نیفتاده و به معنای لزوم پاسخ-گویی اشخاص در قبال اقدامات خود در برابر جامعه و دیگران است و در تعریف مسئولیت گفته‌اند : «مسئولیت عبارت است از وجود تعهد به انجام یا عدم انجام کاری و تحمل آثار و ضمانت اجرایی‌های مقرر در صورت نقض این تعهد».[3] یا این‌که «مسئولیت یعنی تعهد به پاسخ‌گویی به نتایج حاصل از عمل خود».[4] در کتب حقوقی تقسیم بندی‌های مختلفی از مسئولیت نظیر مسئولیت اخلاقی و قانونی(حقوقی) صورت گرفته است. رایج‌ترین این تقسیم بندی‌ها، تقسیم مسئولیت به مسئولیت مدنی، کیفری و انتظامی است؛ مسئولیت مدنی خود به مسئولیت قراردادی و مسئولیت غیر قراردادی تقسیم می‌شود و در هر حال هدف کلی آن جبران زیانی است که به واسطه نقض مفاد قرار داد یا ایراد ضرر به اموال کسی وارد آمده است.[5] مسئولیت انتظامی نیز به مسئولیت در برابر خطای انتظامی که ناشی از نقض وظایف اداری یا صنفی است میپردازد. به موضوع مسئولیت کیفری ذیلاً بیش‌تر پرداخته‌ایم، اما پیش از پرداختن به تعریف، شرایط ارکان و انواع مسئولیت کیفری شایسته است که ابتدا نگاهی به تاریخچه‌ی آن داشته باشیم.

---

[1]. دهخدا، علی اکبر، لغت نامه، تهران، اسفند۱۳۵۲، چاپخانه مؤسسه انتشارات و چاپ دانشگاه تهران، حرف میم، بخش دوم، ذیل واژه‌ی مسئولیت.ص۱۵۳

[2]. معین، محمد، فرهنگ فارسی معین، جلد پنجم، انتشارات امیر کبیر، ۱۳۸۱، حرف میم، ذیل واژه‌ی مسئولیت.

[3]. سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین‌المللی و حقوق کیفری ایران، انتشارات خیام، چاپ اول ، ۱۳۹۲، ص ۱۸.

[4]. افراسیابی، محمد اسماعیل، حقوق جزای عمومی، جلد دوم، انتشارات فردوسی، چاپ اول، ۱۳۷۷، ص ۱۰۰.

[5]. ر.ک کاتوزیان، ناصر، حقوق مدنی، (ضمان قهری- مسئولیت مدنی)، انتشارات دانشگاه تهران، چاپ سوم، ۱۳۷۰، ص ۱۰۳.

«در ایام باستانی، مسئولیت کیفری به آن معنی که امروز مورد نظر است، مطرح نبود؛ درآن ایام ارتکاب مادی عمل، صرف‌نظر از خصوصیات مرتکب، وی را در معرض مجازات قرار می‌داد؛ به این توضیح که هرگاه شخصی مرتکب جرمی می‌گردید، خواه از سلامت عقل بهره‌مند باشد یا خیر، مستحق مجازات بود. حتی در بسیاری موارد، مجازات جرایم غیر عمدی شبیه به جرایم عمدی بود».[1] حتی بعضاً برای مردگان، حیوانات و جمادات نیز قائل به مسئولیت و کیفر بودند.[2] در واقع، «در مراحل نخستین زندگی اجتماعی، مجازات واکنشی بود که صرفاً برای رفع ألم و ناراحتی ناشی از رفتاری خاص ابراز می‌شد و لاجرم تمایزی بین منشأ پیدایش درد و ألم در انواع گوناگون آن قائل نمی‌شدند؛ این منشأ در هر حال موضوع مجازات قرار می‌گرفت و در برابر رفتاری که به نحوی در ایجاد درد و ألم مؤثر بود «مسئولیت کیفری» داشت، فارغ از این‌که انسان یا حیوان یا حتی جماد باشد. در مراحل پیشرفته‌تر، مجازات به عکس‌العملی در برابر زیان ناشی از یک رفتار معین تبدیل شد؛ در این مرحله بشر یک گام فراتر گذاشت و مسئولیت کیفری یک موجود را بر مبنای نوع و میزان خسارت مالی یا جانی که از ناحیه‌ی او به هم می‌رسید معین می‌ساخت. مسئولیت یا همان تحمل مجازات در برابر رفتار معین، در این دو مرحله‌ی تاریخی صرفاً ماهیتی مادی و عینی داشت؛ یعنی یک موجود تنها به این سبب که منشأ ألم یا زیان و خسارت بوده مجبور به تحمل مجازات می‌باشد».[3]

حقوق‌دانان، به‌طور کلی دوره‌ی مسئولیت کیفری را به سه دوره « جنگ‌های خصوصی یا دوره انتقام فردی»، «دادگستری خصوصی» و «دادگستری عمومی» تقسیم می‌کنند.[4] به اعتقاد بسیاری از حقوقدانان در دوره جنگ‌های خصوصی اصل کل «انتقام» حاکم بر روابط افراد بوده و در واقع این حسّ انتقام‌جویی بوده است که اساس مسئولیت کیفری را شکل داده است. با این حال عده‌ای نیز بر این اعتقادند که صرفاً حس انتقام نبوده که مسئولیت کیفری را ایجاد کرده است، بلکه «مطالعات تاریخی نشان می‌دهد که در قدیمی‌ترین قوانین موجود از قبیل قوانین هند و مصر قدیم، موادی درباره امور کیفری و مجازات متخلفان و مجرمان وجود داشته است و حتی در پاره‌ای از امور، بدون داشتن مدّعی خصوصی و یا این‌که جرم متوجه یک شخص خاصی باشد مجازات‌هایی در نظر گرفته شده بود. به علاوه وقتی پدر یا رئیس خانواده به

---

[1]. محسنی، مرتضی، دوره‌ی حقوق جزای عمومی، جلد ۳، مسئولیت کیفری، انتشارات کتابخانه‌ی گنج دانش، چاپ اول، ۱۳۷۶، ص ۳۸.

[2]. همان منبع، صص ۱۰-۶.

[3]. میر سعیدی، منصور، مسئولیت کیفری، قلمرو و ارکان، جلد اول، انتشارات میزان، چاپ اول، بهار ۱۳۸۳، ص ۲۳.

[4]. ر.ک صانعی، پرویز، حقوق جزای عمومی، جلد ۱و ۲، انتشارات گنج دانش، چاپ ششم، تهران، ۱۳۷۴، ص ۴۵ و نیز محسنی، مرتضی، دوره‌ی حقوق جزای عمومی، ج۱، چاپ سوم، تهران، انتشارات گنج دانش، ۱۳۸۲، صص ۱۳۱ به بعد.

تنهایی یا به همراه ریش‌سفیدان قبیله در صدد تنبیه یا مجازات یکی از فرزندان و یا افراد خانواده خود بر می‌آمد، به هیچ‌وجه نمی‌توان ادعا کرد که منظور پدر یا رئیس خانواده از تنبیه و مجازات فرد خاصی، اجرای انتقام شخصی بوده است».[1]

بند دوم: ارکان و شرایط مسئولیت کیفری

نگرشی به کتب حقوق‌دانان در خصوص شرایط و مبانی تحقق و یا قابلیت انتساب مسئولیت کیفری نشان‌گر آن است که علی‌رغم تأثیرات مکتب تحققی در اندیشه‌های کیفری، هنوز هم اکثر آنان با تأثیر گرفتن از مکتب کلاسیک بر این اعتقادند که افراد در صورت داشتن رشد و بلوغ عقلی و اختیار در برابر کلیه اعمال خود مسئول خواهند بود. به اعتقاد اکثر این حقوق‌دانان «... برای این که بتوان مرتکب را جزائاً مسئول دانست، بایستی ساختمان بدنی و فکری او به حد کمال رسیده باشد و قوای روحی او سالم بوده و به واسطه‌ی بروز حادثه‌ی مربوط به وظایف الاعضا، قوای مزبور مختل یا زائل نشده باشد و به عبارت اُخری، مرتکب بایستی از نظر جزایی کبیر بوده و مجنون نباشد».[2] «دو عصاره تقصیر خواستن و دانستن است. پس عواملی که در تقصیر مؤثر می‌باشد، کیفیاتی است که خواستن و دانستن از آن‌ها متأثر می‌گردد».[3] شرایط مسئولیت کیفری در تعریف مسئولیت در معنای واقعی آن به موارد فوق بسنده نمی‌شود؛ در واقع «برای درک مفهوم واقعی مسئولیت از جهات گوناگون، باید علاوه بر وجود تعهد و تکلیفی که از طرف مقام صلاحیت دار وضع و برقرار می‌شود عوامل و شرایط دیگری را نیز در نظر گرفت:

اول- وجود وظیفه در انجام یا خودداری از انجام عملی که خود این وظیفه ممکن است در اثر مقررات قانونی و یا روابط اجتماعی به وجود آمده باشد.

دوم- اطلاع از وجود وظیفه، زیرا مطلقاً نمی‌توان شخصی را که نسبت به وظایف خود آگاهی ندارد مسئول شناخت. عدم اطلاع از وجود وظیفه ممکن است معلول نقص قوای عقلانی و عاطفی و یا نقص تربیت اجتماعی باشد و یا عملاً وجود وظیفه و محتوای آن به شخص موظف و مأمور ابلاغ نشده باشد.

[1]. محسنی، مرتضی، همان، ص ۱۳۴.

[2]. سمیعی، حسن، حقوق جزا، بی نا، بی تا، ص ۷۴.

[3]. باهری، محمد، تقریرات حقوق جزای عمومی، چاپ دوم، انتشارات دانشکده‌ی حقوق دانشگاه تهران، ۱۳۷۴

سوم- توانایی در انجام وظیفه، به فرض آن که دو عامل اول تحقق پیدا کند. منطقاً نمی‌توان کسی را که از انجام وظیفه عاجز است مسئول شناخت. عجز و ناتوانی مأمور در انجام وظیفه ممکن است معلول عوامل شخصی یا اجتماعی باشد».[1] به عبارت دیگر «انسان زمانی می‌تواند از نظر کیفری مسئول شناخته شود که:

اولاً- فاعل جرم از رشد جسمانی و عقلانی برخوردار بوده و با آزادی و از روی اختیار دست به ارتکاب جرم زده باشد؛

ثانیاً- مرتکب جرم قادر باشد که اراده خود را در جهت انجام یا خودداری از انجام عمل ممنوعی به کار گیرد.

ثالثاً- مرتکب جرم با عمل و آگاهی به حرمت عمل ، دست به انجام یا خودداری از انجام آن وظیفه یا تکلیف زده باشد.

رابعاً- مرتکب باید هم‌چنین قدرت و توانایی انجام آن وظیفه و یا تکلیف را نیز دارا باشد».[2] لذا باید توجه داشت که «هر کسی که با علم و اطلاع دست به ارتکاب جرم می‌زند لزوماً مسئول شناخته نمی‌شود، بلکه علاوه بر تحقق اراده ارتکاب و سوء نیت و یا تقصیر جزایی باید دارای اهلیّت و خصوصیات فردی متعارفی باشد تا بتوان وقوع جرم را به او نسبت داد. در نتیجه، وقتی انسان از نظر کیفری مسئول شناخته می‌شود که مسبّب حادثه‌ای باشد، یعنی بتوان آن حادثه را به او نسبت داد. پس مسئولیت کیفری محصول نسبت دادن و قابلیت انتساب است و مقصود از قابلیت انتساب آن است که بر مقامات قضایی معلوم گردد که فاعل جرم از نظر رشد جسمی و عقلی و نیروی اراده و اختیار دارای آنچنان اهلیت بوده است که می‌توان رابطه علیّت بین جرم انجام یافته و عامل آن برقرار کرد. در حقیقت مسئولیت کیفری از نتایج مستقیم انتساب جرم به فاعل آن احراز می‌شود».[3]

بخش دوم: مسئولیت کیفری انتسابی در نظام حقوقی

باید توجه داشت در برخی موارد قانون‌گذار شخص را صرفاً به خاطر کاری که نباید انجام می‌داده و داده یا باید انجام می‌داده و نداده، صرف‌نظر از این‌که بخواهد شرایط درونی مسئولیت را مد نظر قرار دهد یا صرفاً به لحاظ رابطه‌ی معنوی که مرتکب با ارتکاب جرم داشته است مسئول و مورد مؤاخذه می‌داند، برای مثال

---

[1]. ر.ک شامبیاتی، هوشنگ، حقوق جزای عمومی، جلد دوم، مؤسسه انتشاراتی ویستار، چاپ سوم، تهران، ص ۵۳.

[2]. همان، ص۲۴. به نظر می‌رسد که نویسنده محترم در بیان بند دوم و چهارم که ظاهراً تفاوتی با یک‌دیگر ندارند چنین خواسته بیان کند که در بند دوم اختیار و اراده مجرمانه از ارکان تحقق جرم است و برای مثال در شرایط اجبار یا اکراه که رفتار مجرمانه‌ای به وقوع می‌پیوندد شخص مسئولیتی ندارد، حال آنکه در بند چهارم قدرت و توانایی برای انجام تکلیفی که قانون‌گذار عدم انجام آن (ترک فعل) را جرم می‌داند جزو ارکان مسئولیت است.

[3]. ولیدی، محمد صالح، مسئولیت کیفری، انتشارات امیر کبیر، تهران، چاپ اول، ۱۳۶۶، ص ۱۵.

در برخی جرایم قانون‌گذار بنا به مصالحی اجتماعی لزومی نمی‌بیند که حداقل از بعد از اثباتی تقصیر مرتکب را ثابت کند و به صرف وقوع رفتار مجرمانه شخص را مسئول می‌داند. عده‌ای این دسته از جرایم را «مادی صرف» نامیده‌اند چرا که به صرف وقوع رفتار مجرمانه محقق می‌شوند و قانون‌گذار خود را بی نیاز از اثبات شرایط معنوی مسئولیت می‌بیند. در برخی موارد نیز قانون‌گذار صرف یک رابطه‌ی معنوی را، هرچند ضعیف، مبنای مسئولیت قرار می‌دهد. خصوصاً حالت اخیر آن‌گاه است که شخص ثالثی به واسطه‌ی رفتار دیگری مورد مؤاخذه قرار می‌گیرد. این‌گونه « قالب‌های مسئولیت» را مسئولیت اعتباری یا انتسابی نام نهاده‌اند که ذیلاً بیشتر به آن‌ها پرداخته‌ایم.[1]

مسئولیت اعتباری را می‌توان مسئولیتی دانست که بر شخص (اعم از حقیقی یا حقوقی) بدون داشتن تمامی شرایط مسئولیت کیفری حقیقی اعم از شرایط عینی یا معنوی مسئولیت منتسب می‌شود. چنان‌چه پیشتر بیان شد، برای این که شخصی حقیقتاً مسئول باشد باید جمیع شرایط حقوقی، عینی و معنوی در وی جمع باشد تا بتوان وی را مسئول تلقی کرد. حال اگر بدون وجود شرایط عینی یا معنوی مسئولیتی بر کسی یار شود این مسئولیت حقیقی نخواهد بود، بلکه مسئولیتی غیر واقعی و اصطلاحاً اعتباری است. برای مثال ممکن است شخص مرتکب هیچ‌گونه رفتار غیرقانونی نشده باشد لکن قانون‌گذار وی را مسئول بداند. یا این که شخصی مرتکب رفتار مادی شده باشد لکن قابل سرزنش نباشد و نتوان تقصیری را متوجه وی دانست.[2] رفتار مادی در مسئولیت اعتباری ممکن است ناشی از اقدام خود شخص یا اقدام شخص دیگر باشد؛ در حالت اخیر یعنی در صورتی که این انتساب مسئولیت به واسطه‌ی رفتار دیگری نسبت به شخص ثالثی باشد این مسئولیت، مسئولیت اعتباری ناشی از رفتار دیگری خواهد بود که از آن اجمالاً به مسئولیت ناشی از رفتار دیگری یا مسئولیت شخص ثالث نیز یاد می‌شود. منظور از مسئولیت ناشی از رفتار دیگری مسئول دانستن شخص ثالثی به واسطه‌ی رفتار یا نتیجه ی رفتار مجرمانه ای که دیگری انجام داده یا دیگری سبب آن شده است؛ این شخص ثالث در واقع هیچ‌گونه رابطه‌ی مادی با آن رفتار مجرمانه ندارد. حتی ممکن است رابطه‌ی معنوی مستقیم و آشکاری هم با آن‌چه که مرتکب به عنوان جرم انجام داده است نداشته باشد، لکن قانون گذار به دلایلی مصلحت را در آن می‌بیند که اشخاص دیگری را در کنار مرتکب اصلی مسئول بداند یا این‌که در برخی موارد تمامی مسئولیت را بر دوش ثالث بار کند و مرتکب اصلی را اصلاً مسئول نداند. چنین

[1] میر سعیدی، سید منصور، مسئولیت کیفری، جلد اول، قلمرو و ارکان، انتشارات میزان، چاپ اول، بهار ۱۳۸۳.ص۴۶

[2] کانتر، روزایت، تحول، ترجمه عبدالرضا رضایی نژاد، نشر فرا، چاپ اول، تهران، تابستان ۱۳۸۲.ص۷۶

مسئولیتی مبانی توجیهی خاص خود را دارد که در مباحث مربوطه به آن خواهیم پرداخت. اما ابتدا لازم است در مورد اَشکال مسئولیت غیرحقیقی و برخی مفاهیم مربوطه بررسی بیشتری داشته باشم.[1]

بند اول: مسئولیت کیفری اعتباری در فضای سایبر

از مباحث فوق به طور کلی چنین برداشت می‌شود که حقوق کیفری نمی‌تواند به واسطه‌ی مشکلات مورد اشاره در این فضای لایتناهی نظام سنتی مسئولیت یعنی تعقیب و مجازات مرتکب را در آن به معرض اجرا گذارده و از آن طریق نظم لازم را به نحوی شایسته مستقر سازد، چرا که در این فضا یا شناسایی مرتکب ممکن نیست یا این که مجازات وی با گستردگی خساراتی که فعل او به بار می‌آورد ثمری ندارد. لذا همان‌گونه که حقوق کیفری در عصر صنعتی در راستای دیدگاه‌های حمایتی به انواع دیگری از مسئولیت به غیر از مسئولیت حقیقی روی آورده تا بهتر بتواند به ضروریات حقوقی آن عصر پاسخ دهد، باید بر آن بود که با تحقق جامعه‌ی اطلاعاتی و گسترش فضای سایبر نیز باید از قالب‌های این‌گونه مسئولیت جهت «کنترل» هر چه بیشتر این فضا سود جست. برای نمونه در بحث مسئولیت نیابتی آن‌گاه که قانون اشخاصی دیگر را مکلف نموده که من باب پیش‌گیری در قبال افعال مجرمانه‌ی دیگران مسئول باشند، این امر در فضای سایبر نیز با همان توجیهات به دلیل لزوم رویکردهای پیش‌گیرانه قابل دفاع است. چنین چیزی که می‌توان از آن به «تمرکز زدایی» در حوزه‌ی مسئولیت یا به عبارتی بهتر «توزیع مسئولیت کیفری» یاد کرد، سیاست جنایی نوینی در این حوزه است که نیاز به کنترل و به کار گیری اقدامات پیش‌گیرانه توسط دیگران در فضای سایبر به وجود آورده است تا بتواند نقایصی ناشی از اعمال مسئولیت کیفری حقیقی نسبت به صِرف مرتکب را که در فضای سایبر کارآمد به نظر نمی‌رسد پوشش دهد. بر این اساس، مسئولیت در فضای سایبر بیشتر ناظر به تکلیف ناشی از پیش‌گیری است که متوجه اشخاص ثالثی است که خود دخالتی در اقدامات مجرمانه نداشته اند، لکن در جریان این اقدامات قرار گرفته‌اند.[2]

در واقع به واسطه‌ی ویژگی های فضای سایبر است که حقوق کیفری مجبور می‌شود به جای اعمال قواعد سنتی خود راهکارهای پیش‌گیرانه را که قطعاً کم هزینه‌تر، مطمئن‌تر و البته مؤثرتر از تعقیب و سرکوب بزه‌کار است اتخاذ نماید؛ و به همین دلیل است که روش‌های پیش‌گیری غیرکیفری در جایگاه اول توجه قرار می‌گیرند؛ در این میان خصوصاً توجه به راهکارهای فنی- که بر خلاف راهکارهای آموزشی که به سختی می‌توان به آن‌ها جنبه الزامی بخشید و اجبار در خصوص اجرای آن‌ها معمولاً به سختی مقدور و نیازمند طی

[1] ملیکان، احسان، اصول مهندسی اینترنت، نشر مؤسسه علمی-فرهنگی نص، چاپ چهارم، پاییز ۱۳۸۳.ص۴۳

[2] کانتر، روزایت، تحول، ترجمه عبدالرضا رضایی نژاد، نشر فرا، چاپ اول، تهران، تابستان ۱۳۸۲.ص۷۷

زمان طولانی برای نهادینه شدن است- اهمیت به‌سزایی می‌یابند و عمده رویکرد بر راهکارهای پیش‌گیری فنی و تکنولوژیک متمرکز می‌شود؛ و ناگفته پیداست که این امر خود سبب تحولات عمده‌ای در حوزه‌ی مسئولیت نیز می‌شود، چه، از آن‌جا که با توجه به مشکلات حادث در این حوزه قسمتی از بار تکلیف خصوصاً در حوزه‌ی پیش‌گیری بر اشخاص دیگر بار می‌شود، قطعاً این تکلیف حوزه‌ی مسئولیت را نیز دچار تحول می‌کند و با تمرکز زدایی از مسئولیت مرتکب اصلی تحمل قسمتی از تکلیف و مسئولیت بر دوش دیگر اشخاص استوار می‌شود.[1]

بخش سوم : داده ها و اطلاعات مجرمانه در فضای سایبر و مسئولیت کیفری ناشی از آن

بند اول:اطلاعات و محتویات غیرقانونی

در تعریف کلی، داده هرگونه علامت، نشان و نمادی است که اطلاعاتی را مخاطب آن انتقال می‌کند. این داده ممکن است متضمن مفهومی باشد یا این که فاقد هرگونه مفهوم باشد. برای مثال وقتی فردی تصویری را مشاهده می‌کند، آن تصویر علامات و نمادهایی را در ذهن مخاطب آن ایجاد می‌کند و صورتی را برای وی متشکل می‌سازد که ذهن با تحلیل و به اصطلاح آنالیز آن، مفهوم آن را درک می‌کند. به لحاظ فنی نیز داده‌ی رایانه‌ای از معنای کلی آن فاصله‌ی چندانی نگرفته است. داده در معنای فنی علایم، نمادها و سیگنال-هایی است که قابلیت ورود به یک سیستم رایانه‌ای، پردازش ، ذخیره ، انتقال و خروج را داشته باشد. داده می‌تواند به شکل آنالوگ، دیجیتال و یا موج (نوری یا الکترومغناطیسی) موجود باشد. برای مثال اطلاعات ثبت شده بر روی یک نوار کاست داده‌های آنالوگ است. هم‌چنین اطلاعات ارسالی از سوی یک ماهواره داده‌هایی است که به صورت موج ارسال می‌شود. اما اطلاعات موجود بر روی یک دیسکت فلاپی، داده-های رایانه‌ای است. به لحاظ فنی برای هر یک از داده‌های آنالوگ و دیجیتال شکل خاصی متصور است. در رایانه‌ها، داده دارای ساختار دیجیتالی است که به صورت توالی نمادهایی از الفبای دودوییِ صفر و یک ظهور می‌یابد.

داده‌های رایانه‌ای می‌توانند به اقسام مختلف وجود داشته باشند: داده‌ها ممکن است به صورت برنامه‌ی رایانه‌ای یا این که به صورت متن، صوت و تصویر که از آن به عنوان «داده محتوا» یا اختصاراً «محتوا» یاد می‌شود وجود داشته باشد.در بسیاری مواقع، با تمام تفاوت‌هایی که داده با اطلاعات دارد، این دو در معنای مشابهی مورد استفاده قرار می‌گیرند؛ در واقع، هر چند که ممکن است داده‌ای متضمن اطلاعاتی نبوده یا

[1] سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین‌المللی و حقوق کیفری ایران، انتشارات خیام، چاپ اول، ۱۳۹۲.ص۶۵

اطلاعات آن با بهره‌گیری از رمزنگاری بر مخاطب پوشیده باشد، با این حال اطلاعات رایانه‌ای مسامحتاً در مورد چنین داده‌هایی نیز به کار می‌رود. هم‌چنین باید توجه داشت که داده‌ها و اطلاعات رایانه‌ای به تنهایی و به خودی خود کارایی و مفهومی ندارند.[1] به عبارت دیگر داده‌ها و اطلاعات رایانه‌ای بدون وجود سخت-افزارهای رایانه‌ای نخواهند توانست عملکرد خود را به معرض اجرا بگذارند و مخاطب از آن‌ها چیزی نخواهد فهمید. منظور از سخت‌افزار رایانه‌ای نیز هرگونه سیستم رایانه‌ای است که به صورت دیجیتال و بر مبنای سیستم الفبایی دودوییِ صفر و یک عملکرد خود را به معرض اجرا بگذارد. از این دیدگاه این تعریف صرفاً شامل رایانه (کامپیوتر) به معنای مصطلح آن نیست و کلیه‌ی سیستم‌ها و دستگاه‌های رایانه‌ای را که مشمول تعریف و مشخصات فوق باشند در بر می‌گیرد.[2]

از دیدگاه حقوقی می‌توان اطلاعات را به اطلاعات قانونی و غیرقانونی تقسیم کرد؛ اطلاعات غیرقانونی لفظ عامی است که می‌تواند هرگونه اطلاعات مضر و ناسالمی را دربر گیرد که صراحتاً بر اساس قانون اطلاعات غیرقانونی محسوب می‌شوند. اطلاعات مجرمانه که تعریفی مضیق‌تر دارد نیز داخل در تعریف اطلاعات غیرقانونی قرار می‌گیرد، اما معنای آن دو یکی نیست؛ به معنای دیگر رابطه‌ی اطلاعات غیرقانونی و اطلاعات مجرمانه عموم و خصوص مطلق است، بدین معنی که هرگونه اطلاعات مجرمانه غیرقانونی است، لکن هرگونه اطلاعات غیرقانونی لزوماً مجرمانه نیست.[3]

بند دوم: نشریات الکترونیکی و دیجیتالی

رویه‌ی مذکور در ماده‌ی ۶ قانون مطبوعات به نشریات چاپی محدود نشده و به تصریح تبصره‌ی ۳ ماده‌ی ۱ آن قانون در اصلاحیه سال ۱۳۷۹ به نشریات الکترونیکی و محیط سایبر نیز تعمیم یافته است؛ این امر محدود به قانون مطبوعات و نشر کتاب نمی‌گردد. در ماده‌ی ۶ قسمت «ب» مصوبه‌ی شورای عالی اطلاع‌رسانی با عنوان «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» که اولین مقرره‌ی جدی در حوزه‌ی اینترنت در کشور ما به شمار می‌آید نیز چنین آمده است:

«تولید و عرضه موارد زیر توسط رساها و کاربران ممنوع می‌باشد:

- نشر مطالب احادی و مخالف موازین اسلامی.
- اهانت به دین اسلام و مقدسات آن.

[1] صبری، حمید، آشنایی با دانش ارتباطات، انتشارات مؤلف، چاپ اول.ص۴۴

[2] سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین‌المللی و حقوق کیفری ایران، انتشارات خیام، چاپ اول، ۱۳۹۲.ص۶۰

[3] جلالی، علی اکبر، شهر الکترونیک، انتشارات دانشگاه علم و صنعت ایران، چاپ اول، ۱۳۸۲.ص۷۹

- ضدیت با قانون اساسی و هرگونه مطلبی که استقلال و تمامیت ارضی کشور را خدشه دار کند.
- اهانت به رهبری و مراجع مسلم تقلید.
- تحریف یا تحقیر مقدسات دینی، احکام مسلم اسلام، ارزش‌های انقلاب اسلامی و مبانی تفکر سیاسی امام خمینی (ره).
- اخلال در وحدت و وفاق ملی.
- القاء بدبینی و ناامیدی در مردم نسبت به مشروعیت و کارآمدی نظام اسلامی.
- اشاعه و تبلیغ گروه‌ها و احزاب غیرقانونی.
- انتشار اسناد و اطلاعات طبق بندی شده دولتی و امور مربوط به مسائل امنیتی، نظامی و انتظامی.
- اشاعه فحشاء و منکرات و انتشار عکس‌ها و تصاویر و مطالب خلاف اخلاق و عفت عمومی.
- ترویج مصرف سیگار و مواد مخدر.
- ایراد افتراء به مقامات و هریک از افراد کشور و توهین به اشخاص حقیقی و حقوقی.
- افشاء روابط خصوصی افراد و تجاوز به حریم اطلاعات شخصی آنان.
- انتشار اطلاعات حاوی کلیدهای رمز بانک‌های اطلاعاتی، نرم افزارهای خاص، صندوق‌های پست الکترونیکی و یا روش شکستن آن‌ها.
- فعالیت‌های تجاری و مالی غیرقانونی و غیرمجاز از طریق شبکه‌های اطلاع‌رسانی و اینترنت از قبیل جعل، اختلاس، قمار و... .
- خرید، فروش و تبلیغات در شبکه اطلاع‌رسانی و اینترنت از کلیه کالاهایی که منع قانونی دارند ...».

البته قانون مجازات جرایم رایانه‌ای مصوب ۱۳۸۸ تا حدود زیادی این رویه را در خصوص فضای سایبر اصلاح و به نظر می‌رسد در حدود تعارض مقررات مزبور را ملغی کرده است. قانون مزبور در مواد ۲۱ تا ۲۳ خود که به مسئولیت ارائه کنندگان خدمات دسترسی و میزبانی می‌پردازد عبارت «محتوای مجرمانه» را به کار برده است که گستردگی عبارات مندرج در عبارات پیش گفته را ندارد و گستره‌ی اطلاعات غیرقانونی را در محدوده‌ی قوانین کیفری موجود محدود می‌نماید، اما متأسفانه تعریف ضمنی و البته نامحدود این قانون از محتوای مجرمانه در ماده‌ی ۲۱ آن که «اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای به کار می‌رود،» دانسته شده است هم‌چنان راه را برای تشخیص‌ها و تفسیرهای

نادرست و گسترده باز می‌گذارد. اثر چنین اقدامی می‌تواند در سانسور پالایش موسع اطلاعات که «کمیته‌ی تعیین مصادیق» در این قانون عهده‌دار آن شده است نمود یابد. در این‌باره بیشتر سخن گفته‌ایم.[1]

بند سوم:ارائه داده و خدمات اینترنتی در ایران

مصادیق اطلاعات غیرقانونی در قوانین کیفری فراوان است و محدود به اطلاعات مبتذل و مستهجن نمیگردد. موارد متعددی از این‌گونه اطلاعات را می‌توان در جرایم علیه امنیت کشور نظیر نشر اطلاعات طبقه بندی شده، تهدید به بمب گذاری، تحریک به عدم انجام وظایف، تشویق و ترغیب به ارتکاب جرایم علیه امنیت ملی نظایر آن‌ها مشاهده کرد. علاوه بر این در ستایر حوزه‌ها هم چون تبلیغ تبعیض نژادی، جرایم علیه شخصیت معنوی افراد نظیر توهین به رهبری، مراجع تقلید، مقدسات مذهبی، اشخاص، کارکنان دولت، رئیس دولت یا نماینده‌ی خارجی، نشر اکاذیب، ایراد افتراء، هجو، نشر مطالب خصوصی، تهدید، جرایم علیه حقوق مالکیت فکری و حقوق تجاری اشخاص و بسیاری از موارد دیگر که در قوانین مختلف از جمله قانون مطبوعات و قانون جرایم رایانه‌ای می‌توان اطلاعات غیرقانونی را مشاهده کرد.[2]

با این همه تعریف اطلاعات غیرقانونی بر اساس بافت و وضعیت سیاسی، فرهنگی و اجتماعی هر کشور، مشکلاتی را در اینترنت به وجود آورده است؛ اینترنت یک رسانه‌ی بین المللی و نمود کاملی از جریان در حال تکوین موسوم به «جهانی شدن» است که یک بُعد آن، هماهنگ و یک دست نمودن بافت فرهنگی و اجتماعی کشورها است. این فضای مجازی سرشار از اطلاعاتی است که ممکن است اشاعه‌ی آن در کشوری جرم و در کشوری دیگر جرم نباشد؛ وجهه‌ی بین المللی و جهانی اینترنت، ضرورت یکسان‌سازی تعریف جرایم اینترنتی و اطلاعات غیرقانونی را که بدون همکاری‌های بین المللی میسر نمی‌گردد، بیش از پیش مشهود می سازد. محدوده‌ی اطلاعات غیرقانونی در کشور ما بسیار بیشتر از سایر کشورهاست؛ برای نمونه، اطلاعات مبتذل طبق قوانین و عرف کشور ما تعریفی دارد که در بسیاری از مواقع، مصادیق آن در کشورهای دیگر اصلاً اطلاعات غیرقانونی شناخته نمی‌شود. از سوی دیگر آن چنان‌که عملاً در کشور خودمان شاهدیم، با ورود اینترنت به جامعه‌ی ما با نشر و دریافت اطلاعاتی که قبلاً مبتذل شناخته شده و انتشار و دریافت آن‌ها در رسانه‌های گروهی حتی جرم و قابل تعقیب کیفری می‌نمود، با تسامح بیشتری

[1] دادگران، سیدمحمد، مبانی ارتباطات جمعی، انتشارات فیروزه، چاپ چهارم، سال ۱۳۸۱.ص۶۷

[2] کانتر، روزایت، تحول، ترجمه عبدالرضا رضایی نژاد، نشر فرا، چاپ اول، تهران، تابستان ۱۳۸۲.ص۷۶

برخورد شده است. این امر نشان‌گر تغییر تدریجی برداشتی است که طی زمان و مکان از اطلاعات غیرقانونی صورت گرفته است.[1]

پیشتر بیان کردیم که قسمت عمده‌ای از مسئولیت اعتباری که در راستای تکلیف کنترل و نظارت در فضای سایبر بر اشخاص دیگر تحمیل می‌شود ناشی از تکلیف کنترل و پیش‌گیری از اشاعه‌ی داده محتوای مجرمانه است؛ در این میان نقش آفرینان اصلی محیط سایبر را می‌توان به سه دسته‌ی کلی تقسیم کرد: کاربران و مشترکین، ارائه کنندگان خدمات اینترنتی و اشخاص واسط بین ارائه کنندگان خدمات و کاربران که شامل مواردی نظیر ارائه کنندگان خدمات هادی، مدیران شبکه و صاحبان وبگاه‌ها می‌شوند. از آن‌جا که قسمت عمده‌ی مسئولیت در فضای سایبر حول محور ارائه کنندگان خدمات خواهد بود لذا ابتدا لازم است شناختی کلی نسبت به ارائه کنندگان خدمات و خدماتی که ارائه می‌دهند داشته باشیم.[2] ارائه کنندگان خدمات در فضای سایبر را می‌توان به دو دسته‌ی کلی ارائه کنندگان خدمات اینترنتی و ارائه کنندگان خدمات مخابراتی تقسیم کرد. در کشورهای انگلیسی زبان از ارائه کننده خدمات اینترنتی یاد شده و معمولاً به عنوان مرجعی که امکان دسترسی کاربران و مشترکین را به اینترنت فراهم می‌آورد، تعریف می شود. بعضاً نیز عبارت «ارائه دهنده‌ی خدمات بر خط» به جای عبارت مزبور به کار می‌رود. در ازاء خدمات مختلفی که ارائه کنندگان خدمات اینترنتی ارائه می‌دهند تقسیم بندی های مختلفی از آنان صورت گرفته است که بیشتر به لحاظ فنی اهمیّت دارد. برای مثال به ارائه کنندگان خدمات دسترسی ، و به ارائه کنندگان خدمات اینترنتی بی‌سیم گفته می‌شود.لکن باید توجه داشت که امروزه دیگر مرز دقیقی بین اینترنت ومخابرات نمی‌توان قائل شد. چه، علاوه بر این که اینترنت و مخابرات هر دو شبکه‌های اطلاع رسانی هستند، شبکه اینترنت در بیشتر دنیا بر روی شبکه‌های کابلی و غیرکابلی مخابراتی بنا شده و به موازات گسترش و توسعه‌ی فنی و ابزارهای مخابراتی و ارتباطی (هم‌چون ماهواره) از آن‌ها نیز جهت ارتباطات اینترنتی کمک می‌گیرد. از سوی دیگر به هر چه بیشتر دیجیتالی شدن مخابرات آنالوگ سنتی و سعی بر تلفیق اینترنت ومخابرات، این دو دیگر به راحتی از هم قابل تفکیک نیستند. تعریفی که نیز در تبصره ۱ ماده ۱ «قانون تأسیس شرکت مخابرات ایران» مصوب ۱۳۵۰ از واژه مخابراتی صورت گرفته آن‌چنان موسع است که اکنون می‌تواند ارتباطات اینترنتی را نیز پوشش می‌دهد. در تبصره ۱ ماده ۱ قانون مزبور آمده است که

[1] شایزری، کریانگ ساک کیتی، حقوق بین‌الملل کیفری، ترجمه بهنام یوسفیان، محمد اسماعیلی، انتشارات سمت، چاپ اول، ۱۳۸۳.ص ۴۰

[2] صبری، حمید، آشنایی با دانش ارتباطات، انتشارات مؤلف، چاپ اول.ص۱۳۲

«مقصود از مخابرات در این قانون عبارت است از انتقال و ارسال علائم و نوشته‌ها و تصاویر و صداها و هرگونه اطلاعات دیگر به وسیله سیم یا بی‌سیم و یا نور و یا هر رویه الکترومغناطیسی». همین تقارب تعریف قانونی بین خدمات اینترنتی و مخابراتی، سبب نزدیکی هر چه بیشتر مباحث حقوقی آن‌ها نیز گردیده است. اکنون ارائه کنندگان خدمات مخابراتی را در کنار ارائه کنندگان خدمات اینترنتی نام برده و به طور کلی با عنوان ارائه کنندگان خدمات در فضای سایبر یاد می‌کنند. در این‌جا مقصود ما از ارائه کنندگان خدمات ناشر بر هر دو این ارائه کنندگان بوده است، هر چند که تأکید بر خدمات اینترنتی بیشتراست.[1]

بخش چهارم: مسئولیت مجرمانه ارائه و ذخیره اطلاعات مجرمانه

ممکن است بیان شود که ارائه کنندگان خدمات اینترنتی که بستر لازم برای انتقال یا ذخیره‌ی اطلاعات را برای دیگری فراهم می‌آورند با فرض آگاهی از این که به هر حال اطلاعات مجرمانه‌ای در اینترنت وجود دارد اقدام به ارائه‌ی اطلاعات می‌نمایند و از این‌رو کسانی هستند که خود در انتشار اطلاعات مساعدت کرده و ابزار ارتکاب جرم را در اختیار دیگری گذاشته‌اند و لذا من‌باب تسهیل در رفتار مجرمانه‌ی دیگری مسئول‌اند. همین استدلال در ابتدای طرح بحث مسئولیت ارائه کنندگان خدمات، سبب شده بود که دادگاه-های برخی کشورها با توسل به این توجیه حقوقی که ارائه کنندگان خدمات بستر لازم برای دسترسی به اطلاعات یا ذخیره‌ی اطلاعات را برای دیگران فراهم می‌آورند و از این رو ارائه و ذخیره‌ی این‌گونه اطلاعات را تسهیل می‌کنند یا با این باور که ارائه کنندگان خدمات با آگاهی و علم- ولو اجمالی-از این‌که این اطلاعات که برای کاربران قابل دسترس می‌گردد مجرمانه است آن اطلاعات را قابل دسترس می‌سازند، لذا در واقع در انتشار اطلاعات مجرمانه مساعدت کرده‌اند من‌باب معاونت در رفتار مجرمانه‌ی دیگری مسئول بدانند.[2]

بند اول: بررسی مخالفان این قضیه

مخالفان این نظر از دو جهت بر آن ایراد گرفته و بیان داشته‌اند که اولاً باید توجه داشت که در خدمات دسترسی، نقل و انتقال داده‌ها به لحاظ فنی عملی خودکار است و ارائه کنندگان خدمات در جریان اطلاعات نقشی ندارند. در واقع، خدمات دسترسی اطلاعات به خواست خود کاربر به وی منتقل می‌شود و از این نظر فعل مثبتی نیست که گفته شود توسط ارائه کننده خدمات صورت می‌گیرد و لذا معاونت و مشارکت در جرم که با ارتکاب فعل مثبت (رفتار ایجابی) قابل تصور است در خدمات دسترسی منتفی

[1] کراملیش، کریستین، کتاب آموزشی اینترنت، ترجمه مهرناز آرین، انتشارات تورنگ، چاپ پنجم، ۱۳۸۰.ص۵۹

[2] دادگران، سیدمحمد، مبانی ارتباطات جمعی، انتشارات فیروزه، چاپ چهارم، سال ۱۳۸۱.ص۶۹

است. در خدمات میزبانی و ذخیره داده نیز این شخص دیگری است که اطلاعات را در فضای ارائه شده به او ذخیره می‌نماید و صرف ارائه‌ی فضا برای ذخیره‌ی اطلاعات مجرمانه بدون اطلاع از ماهیت غیر قانونی اطلاعاتی که ذخیره می‌شود ذاتاً رفتاری مجرمانه نیست که بگوییم عنصر مادی معاونت در ذخیره‌ی اطلاعات غیر قانونی را تشکیل می‌دهد. برای نمونه چگونه می‌توان ارائه دهنده‌ی خدماتی را که فضایی را برای ایجاد وبگاهی به شخصی ارائه داده است و آن شخص داده محتوای متضمن توهین و افتراء یا تصاویر مستهجن یا اثری که متضمن نقض مالکیت فکری دیگری باشد را درآن وبگاه قرار داده است با عنوان معاونت در ارتکاب جرم مسئول دانست و براساس مسئولیت مشارکتی مسئول دانست؟ این امر دقیقاً به آن می‌ماند که مالک ملکی را به این دلیل که ملک خود را در اختیار دیگری قرار داده و او در آن ملک مرتکب جرمی شده است مسئول بدانیم.

ثانیاً نباید فراموش کرد که در مسئولیت مشارکتی، آگاهی واقعی از مجرمانه بودن عمل و وحدت قصد با مباشر جرم لازم است و لذا در ارائه خدمات دسترسی و ذخیره‌ی اطلاعات، در صورت عدم وجود آگاهی واقعی از غیر قانونی بودن اطلاعاتی که ارائه یا ذخیره می‌گردد، شخص مسئولیتی ندارد.[1] منظور از آگاهی واقعی در این‌جا آن است که حتی با وجود اطلاعات اجمالی ارائه کننده‌ی خدمات مبنی بر این‌که به‌طور کلی می‌داند که در فضای اینترنت اطلاعات مجرمانه‌ای وجود دارد یا ممکن است اطلاعات مجرمانه‌ای در رایانه‌های کارگذار وی ذخیره گردد نمی‌توان مسئولیتی بر وی بار کرد. از سوی دیگر، بیان شد که کسب این آگاهی برای ارائه کنندگان خدمات اینترنتی به لحاظ حجم بسیار بالای اطلاعاتی که از مسیر رایانه‌های کارگذار آنان عبور کرده و یا در رایانه‌های کارگذار آنان ذخیره می‌گردد در بسیاری موارد غیر ممکن، و حتی در صورت آگاهی، اثبات و احراز آن مشکل است.[2]

بااین حال مؤافقان مسئولیت ارائه کنندگان خدمات بیان داشته‌اند که درست است که نمی‌توان گفت ارائه کنندگان خدمات در قبال ارائه داده محتوای غیر قانونی به کاربران به‌عنوان معاونت در جرم مسئول‌اند، لکن اولاً باید توجه داشت که ارائه کنندگان خدمات به‌طور کلی در ارائه اطلاعات نقش سبب را دارند و ارائه بستر لازم جهت ارائه یا ذخیره‌ی اطلاعات توسط آنان صورت می‌گیرد. ثانیاً هر چند که ارائه کنندگان خدمات از قانونی یا غیر قانونی بودن داده محتوایی که به کاربران ارائه می‌شود آگاهی واقعی ندارند و

[1] سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین‌المللی و حقوق کیفری ایران، انتشارات خیام، چاپ اول، ۱۳۹۲.ص۱۶۵

[2] دلفانی، علی اشرف، مبانی مسئولیت کیفری در حقوق اسلام فرانسه، انتشارات مؤسسه بوستان کتاب قم، چاپ اول، ۱۳۸۲.ص۵۴

کسب این آگاهی به لحاظ حجم بسیار بالای داده محتوای انتقالی به کاربران و مشترکین با نظارت فیزیکی ممکن نیست، لکن همان‌گونه که در مسئولیت مشارکتی بیان شد این‌گونه مسئولیت به شرطی که برای مساعدت در رفتار مجرمانه باشد حتی بعد از ارتکاب جرم و به واسطه‌ی ترک فعل در عدم جلوگیری از استمرار واقعه‌ی مجرمانه به شرطی که آگاهانه باشد قابل تحقق است؛ لذا آن‌گاه که ارائه کنندگان خدمات به‌نحوی از وجود چنین اطلاعاتی در فضایی که به دیگری ارائه کرده‌اند یا از گذر چنین اطلاعاتی از طریق رایانه‌های کارگذارشان به کاربران و مشترکین آگاه می‌شوند و اقدامی جهت جلوگیری از قابلیت دسترسی کاربران به آن اطلاعات به عمل نمی‌آورند مسئول هستند. برای نمونه آن‌گاه که ارائه کننده‌ی خدماتی مطلع می‌گردد که داده محتوای مستهجنی در وبگاهی قرار دارد که کاربران به آن دسترسی می‌یابند و دسترسی به آن‌را مسدود نمی‌سازد یا این‌که به درخواست شاکی، داده محتوای متضمن افترایی را که منسوب به اوست و در وبگاهی که میزبانی فضای آن توسط ارائه کننده‌ی خدمات ارائه شده قرار گرفته است، حذف یا غیر قابل دسترس نمی‌سازد مسئول خواهند بود. به‌عبارت دیگر بر مبنای این نظر، هرچند که ممکن است در ابتدای قرار دادن اطلاعات مجرمانه در چنین وبگاهی ارائه دهنده‌ی خدمات نسبت به وقوع جرم آگاه نبوده و از این رو تا این مرحله مسئولیتی متوجه وی نباشد، اما همین‌که به محض آگاهی از وقوع چنین اطلاعاتی نسبت به حذف یا غیر قابل دسترس نمودن آن اقدامی به عمل نمی‌آورد، در بقای آن اطلاعات با مرتکب اصلی مشارکتاً مسئول خواهد بود. در جرایمی چنین، صرف آگاهی، عنصر معنوی و عدم اقدام یا ترک فعل، عنصر مادی بزه محسوب می‌شود. در واقع ارائه دهنده‌ی خدمات در این موارد کافی است. به لحاظ عنصر مادی نیز نیازی به ارتکاب فعل مثبت ارائه دهنده‌ی خدمات نیست، بلکه در این موارد ترک فعل در حذف یا غیر قابل دسترس ساختن اطلاعات که توسط دیگری قابل دسترس شده است کفایت می‌کند. این توجیه دیدگاهی میانه در خصوص اعمال مسئولیت مشارکتی نسبت به ارائه دهندگان خدمات پیش روی می‌گذرد و حداقل عنصر آگاهی ثانوی ارائه کننده‌ی خدمات که پس از قرار دادن داده محتوای مجرمانه در فضای ذخیره شده حاصل می‌گردد و نیز ترک فعل اورا در عدم اقدام لازم جهت تحقق مسئولیت وی دخیل می‌داند.[1]

بند دوم:نگاهی به مسئولیت ارائه دهندگان خدمات اینترنت در اتحادیه اروپا

چنانچه قبلا بیان گردید، خدمات پیوند، خدماتی است که ارائه‌کننده خدمات جهت تسهیل و تسریع دسترسی به اطلاعات در شبکه‌های رایانه‌ای به صورت پیوندها، فهرست‌ها، نمایه‌ها فرامتن‌ها و هر گونه

[1] خلیق، غلامرضا، کارور شبکه اینترنت، انتشارات اشراقی و راهی، چاپ سوم، بهار ۱۳۸۲.ص۸۲

آدرس ارجاع ارائه می‌دهد. مسئولیت ارائه‌کنندگان خدمات پیوند در بند «d» ماده ۵۱۲ بخش ۱۷ مجموعه قوانین ایالات متحده و تحت عنوان «ابزار موقعیت داده»[۱] آمده است؛ براساس آن ماده اصل بر این است که ارائه‌کنندگان خدمات در قبال ارائه این خدمات با وجود شرایط ذیل مسئولیتی ندارند:

- از وجود اطلاعات غیرقانونی در محلی که به آن ارجاع می‌دهند آگاه نبوده و براساس قرائن و اوضاع و احوال مُثبته هم متوجه نشوند که اطلاعات ذخیره شده غیرقانونی است، در غیر این‌صورت اگر از وجود اطلاعات غیرقانونی آگاهی داشته یا به قرائن و اوضاع و احوال مؤید وجود اطلاعات غیرقانونی توجهی نکنند، مسئول خواهند بود. قاعده «پرچم سرخ» (بی‌مبالاتی فاحش) که در خدمات میزبانی بررسی شد در این خصوص نیز اعمال می‌گردد.
- به محض آگاه شدن از وجود اطلاعات غیرقانونی در محلی که به آن ارجاع می‌دهند خدمات پیوند را قطع نمایند.
- نسبت به ارائه «پیوند عمیق» اقدام ننماید. این امر در خدمات انباشت موقت مورد اشاره قرار گرفت.

نکته جالب توجه دیگری که در بند «m» ماده ۵۱۲ مجموعه قوانین ایالات متحده آمده آن است که صراحتاً اشعار می‌دارد که ارائه‌کنندگان خدمات اینترنتی تکلیفی در جستجو برای یافتن اطلاعات متضمن نقض کپی‌رایت و یا قرائن و اوضاع و احوال مثبته این امر ندارند. این امر در راستای مطالبی است که فوقاً در مورد عدم امکان کنترل فیزیکی در فضای سایبر به لحاظ حجم وسیع داده محتوای موجود در این فضا به آن اشاره رفت به طوری‌که مبین عدم پذیرش مسئولیت عاریتی ارائه‌کنندگان خدمات در این‌باره است.[۲]

چنانچه مشاهده می‌شود قانون مزبور تعادلی منطقی بین منافع ارائه‌کنندگان خدمات اینترنتی و صاحبان حق کپی‌رایت ایجاد کرده است و از سوی دیگر دربردارنده موادی است که عملاً نیازمند مشارکت صاحبان حق کپی‌رایت و ارائه‌کنندگان خدمات اینترنتی در مبارزه با اطلاعات متضمن نقض کپی‌رایت است. مقررات این قانون که براساس یافته‌های منطقی و تجارب حاصل در بعد مسئولیت کیفری در فضای سایبر

---

[۱]. مشابه رویه مذکور را با شرایطی ساده‌تر می‌توان در ماده ۱۴ قانون صدور چک کشور خودمان برای دستور عدم پرداخت وجه چک-های مفقود شده یا تحصیل شده از راه جرم به بانک مشاهده کرد که مدعی موظف است جهت اثبات حق خود ظرف یک هفته به دادگاه شکایت و رونوشت مصدق آن را به بانکد تحویل نماید. در غیر این صورت برای حفظ حق دارنده چک، بانک پس از گذشت یک هفته به درخواست وی توجهی نخواهد کرد و مبلغ چک را به دارنده آن پرداخت خواهد نمود.

[۲]دادگران، سیدمحمد، مبانی ارتباطات جمعی، انتشارات فیروزه، چاپ چهارم، سال ۱۳۸۱.ص۶۸

تصویب شده است بعدها به عنوان مدلی در خصوص مسئولیت مدنی و کیفری ارائه‌کنندگان خدمات مورد توجه شورای اروپا و کشورهای دیگر قرار گرفت.

بند سوم: مسئولیت ارائه‌کنندگان خدمات اینترنتی در خدمات دسترسی

دستورالعمل شماره **EC/**۲۰۰۰/۳۱ پارلمان و شورای اروپا مصوب ۸ ژوئن ۲۰۰۰ در خصوص «برخی از جنبه‌های حقوقی خدمات جامعه اطلاعاتی، خصوصا تجارت الکترونیک، در بازار داخلی (دستورالعمل راجع به تجارت الکترونیک)» مقرراتی را برای یکسان‌سازی تجارت الکترونیک در شورای اروپا ارائه داد؛ پاره‌ای از مقررات این دستورالعمل به موضوع مسئولیت ارائه‌کنندگان خدمات اینترنتی پرداخته است که لزوماً محدود به حوزه تجارت الکترونیک نیست و مسئولیت ارائه‌کنندگان خدمات جامعه اطلاعاتی را نیز- که ارائه‌کنندگان خدمات اینترنتی بخشی از آن هستند- در باب ارائه و ذخیره اطلاعات و در دو حوزه کیفری و مدنی پوشش می‌دهد.[۱]

این دستورالعمل در بند ۱۷ مقدمه و بند **a** ماده ۲ خود که به تعاریف می‌پردازد بیان داشته است، تعریف «خدمات جامعه اطلاعاتی» همان است که سابقاً در دستورالعمل شماره **EC/**۹۸/۳۴ مصوب ۲۲ ژوئن ۱۹۹۸ در خصوص «وضع رویه‌ای برای ارائه اطلاعات در حوزه موازین و مقررات فنی و مقررات راجع به خدمات جامعه اطلاعاتی» که توسط دستورالعمل شماره **EC/**۹۸/۸۴ مصوب ۲۰ نوامبر ۱۹۹۸ در خصوص «حمایت حقوقی از خدمات مبتنی یا مشتمل بر دسترسی مسروط» اصلاح شده است تعریف گردیده است. براساس بند ۲ ماده ۱ دستورالعمل مذکور خدمات جامعه اطلاعاتی هر گونه خدماتی است که معمولا در قبال عوضی، از راه دور و از طریق ابزار الکترونیک و با درخواست گیرنده خدمات به وی ارائه می‌شود. این تعریف موسع است و کلیه خدمات الکترونیکی از راه دور از جمله خدمات اینترنتی و خدمات ارتباطی راه دور (مخابرات) را نیز در بر می‌گیرد. اما براساس انتهای همین بند از ماده مذکور خدمات پخش رادیویی و تلویزیون جزو خدمات جامعه اطلاعاتی محسوب نمی‌شوند. بند**b** ماده ۲ «ارائه‌کننده خدمات» را هر شخص حقیقی یا حقوقی دانسته که خدمات جامعه اطلاعاتی را ارائه می‌کند. بند **b** این ماده نیز «گیرنده خدمات» را هر شخص حقیقی یا حقوقی می‌داند که به دلایل حرفه‌ای یا به هر دلیل دیگر از خدمات جامعه اطلاعاتی، علی‌الخصوص برای جستجو و یافتن اطلاعات یا برای قابل دسترس نمودن اطلاعات استفاده می‌کند.[۲]

---

[۱] خلیق، غلامرضا، کارور شبکه اینترنت، انتشارات اشراقی و راهی، چاپ سوم، بهار ۱۳۸۲.ص۲۵

[۲] دادگران، سیدمحمد، مبانی ارتباطات جمعی، انتشارات فیروزه، چاپ چهارم، سال ۱۳۸۱.ص۵۴

بند چهارم:مسئولیت کیفری مدیران سایت و وبلاگ

به طور کلی در چنین وبگاه‌هایی، هر چند که خدمات شبکه از طریق یک ارائه‌کننده خدمات دریافت می‌گردد، با این حال صاحب یا مدیر وبگاه حق نظارت بر اطلاعات دریافتی را داراست. «صاحبان وبگاه‌ها و مدیران شبکه» از آن جهت که می‌توانند بر اطلاعات دریافت شده نظارت داشته باشند می‌توانند واجد تکالیف و مسئولیت‌هایی باشند. چه، به هر صورت صاحبان و مدیران این‌گونه وبگاه‌ها را باید ارائه‌کنندگان خدمات کوچکی دانست که این فضا را برای استفاده در اختیار کاربران دیگر قرار داده‌اند. اما آیا می‌توان این افراد را با ارائه‌کنندگان خدمات مقایسه و مسئولیت‌های آنان را یکسان دانست و چنانچه در مباحث پیشین آمد را نیز توزیع‌کننده دانست و جز در صورت آگاهی از وجود اطلاعات غیرقانونی در وبگاهشان نظیر توهین، افتراء، تصاویر مستهجن و نظایرآن مسئول ندانست؟ یا این‌که می‌توان گفت که مدیران و صاحبان چنین وبگاه‌هایی باید به صورت فیزیکی بر محتویات اطلاعات خود نظارت کنند و اگر داده محتوایی را غیر قانونی یافتند نسبت به حذف آن اقدام کنند؟ از سوی دیگر، آیا مسئولیت حذف یا غیرقابل دسترس نمودن اطلاعات غیرقانونی صرفاً برعهده ارائه‌کننده خدمات است و صاحبان و مدیران وبگاه‌ها که چنین خدماتی را ارائه می‌کنند هیچ گونه مسئولیتی در قبال محتویات ارائه شده توسط دیگران در فضای آن‌ها ندارند؟[1]

پاسخ به این سؤالات اندکی دشوار است، چه، اگر بر این اعتقاد باشیم که حذف یا غیرقابل دسترس نمودن اطلاعات غیرقانونی باید به دستور مقام ذی صلاح که مرجع تشخیص غیرقانونی بودن اطلاعات است و آن هم صرفاً از طریق دستور به ارائه‌کنندگان خدمات فضای میزبانی چنین وبگاه‌هایی صورت گیرد باید مسئولیت مدیران و صاحبان چنین وبگاه‌هایی را منتفی دانست؛ به عبارت دیگر در چنین مواردی مسئولیت ارائه‌کنندگان خدمات نافی مسئولیت صاحبان و مدیران وبگاه‌ها خواهد بود.[2]

بخش پنجم:عدم تامین امنیت در فضای مجازی و بررسی مسئولیت کیفری ناشی از آن

بند اول:مفهوم امنیت در فضای سایبر و اهمیت آن

همین امنیت اطلاعات از دیرباز مورد توجه بوده و از منه‌ی قدیم همواره تلاش بر آن بوده که اطلاعات حساس و مهم را به دقت حفظ نمایند. این تلاش بیشتر در راستای عدم افشای اطلاعات بوده که می‌باید محرمانه می‌مانده و خصوصا در مواقعی مثل جنگ‌ها اهمیت حفظ آن‌ها چند برابر می‌شده است، لکن بقاء

[1] علی¬آبادی، عبدالحسین، حقوق جنایی، جلد اول، چاپ دوم، تهران، انتشارات فردوسی، ۱۳۶۹.ص۹۹

[2] صبری، حمید، آشنایی با دانش ارتباطات، انتشارات مؤلف، چاپ اول.ص۸۷

(تمامیت) اطلاعات شاید چندان مورد توجه نبوده است. اهمیت خود اطلاعات و مصون ماندن آن‌ها از تخریب و امحاء رفته رفته در جوامع و خصوصاً جوامع اطلاعاتی کنونی بیش از پیش شده است. قبلاً بیان شد که جوامع اطلاعاتی دائر مدار اطلاعات سودمند و بقاء اطلاعات نیز مبتنی بر سلامت و حفظ امنیت آن-هاست. از این‌رو تمامیت اطلاعات صرف‌نظر از محتوایی که انتقال می‌دهند دارای اهمیت فراوانی هستند و داده‌های دیجیتالی که به مدد فناوری رایانه‌ای ایجاد شده و تکثیر می‌یابند اهمیت بسزایی را در جوامع اطلاعاتی یافته‌اند. آنچه که به امنیت اطلاعات و سیستم‌های یارانه‌ای اهمیت فراوان بخشیده همانا گسترش فضای سایبر است. به اشتراک‌گذاری اطلاعات در اینترنت و اهمیت فوق‌العاده که استفاده از بانک‌های اطلاعاتی و پایگاه‌های داده اینترنت در حوزه‌های مختلف اطلاع رسانی، ارتباطات، تجارت الکترونیک، آموزش الکترونیک و مواردی از این قبیل دارند در نگاهی کلان، اهمیت اطلاعات شبکه‌ای را روشن می-سازد. «در چند دهه ظهور اول شبکه، پژوهشگران دانشگاه‌ها از آن برای ارسال پست الکترونیکی استفاده می‌کردند و کارمندان شرکت از آن برای (به اشتراک‌گذاری) چاپگر استفاده می‌نمودند. تحت این شرایط، امنیت چندان مورد توجه نبود. اما اکنون که میلیون‌ها نفر از شهروندان از شبکه برای بانکداری، فروش و پرداخت مالیات‌ها استفاده می‌کنند امنیت یک مسئله جدی است». [1]

اکنون نرم‌افزارهایی که حاصل تلاش فکری دانشمندان بسیار در حوزه رایانه است به زحمت و با صرف هزینه‌های مالی و زمانی تولید می‌شود و بعضا به بهانه زیادی توسط کاربران خریداری می‌شود. همین‌طور فایل‌های محتوایی همچون فایل‌های صوتی، تصویری و نوشتاری افراد ممکن است برآیند زحمت و رنج بردن آن‌ها طی سالیان متمادی باشد. اهمیت اطلاعات همچنین بستگی به میزان وابستگی جوامع به اطلاعات دارد؛ در واقع هر قدر جامعه‌ای اطلاعاتی‌تر باشد همان‌قدر اطلاعات در آن جامعه بیشتر اهمیت می‌یابد. این اهمیت اطلاعات را در هر کشور می‌توان از میزان تصویب قوانین آن کشور در این حوزه دریافت؛ قوانین مترقی کپی رایت در یک کشور نمونه‌ای از این قوانین می‌تواند باشد؛ برای مثال یک نسخه از نرم افزار سیستم‌عامل ویندوز در کشورهای پیشرفته که از مالکیت فکری اشخاص به شدت حمایت می‌شود- به بهای گزافی قابل خریداری است و قوانین نیز به شدت با نقض حقوق مؤلف از آن حمایت می‌کنند. اما همین نرم‌افزار در کشورهایی که حمایت از مالکیت معنوی در آن‌ها چندان دقیق نیست یا اصلا مالکیت

[1]. اس تننباوم، شبکه‌های کامپیوتری، ترجمه عین‌الله جعفرنژاد قمی، انتشارات علوم رایانه، چاپ سوم، پاییز ۱۳۸۳

معنوی مورد حمایت قرار نمی‌گیرد به ثمن بخس و حتی به صورت رایگان قابل خریداری یا تهیه است؛ نه قانونی در این باره هست و نه این‌که نیروهای انتظامی و قضایی به این مسئله چندان اهمیتی می‌دهند.[1]

علاوه بر داده‌ها، اطلاعات و برنامه‌های رایانه‌ای حاصل از تلاش فکری افراد، باید به اهمیت عمده داده‌های مالی افراد نیز در چرخه دریافت‌ها و پرداخت‌های الکترونیک و نقش این داده‌ها در تجارت الکترونیک توجه داشت. هر روزه میلیون‌ها پرداخت و دریافت داده‌های مالی در سطح جهان صورت می‌گیرد که حفظ آن‌ها از تعرض و حملات الکترونیکی دارای اهمیت ویژه‌ای است ودولتها توجه خاصی نسبت به این مسئله دارند. درکنار داده‌ها و اطلاعات البته سیستم‌های رایانه‌ای نیز اهمیت مشابهی دارند چرا که داده‌ها و سیستم-ها در یک درجه از اهمیت قرار می‌گیرند. آماری که هر ساله کشورهای مختلف از حملات به اطلاعات و سیستم‌های رایانه‌ای ارائه می‌کنند و میزان خسارات هنگفت ناشی از آن‌ها که بر دوش دولت، کاربران و ارائه‌کنندگان خدمات رایانه‌ای تحمیل می‌شود نشان‌گر ابعاد وخیم تعرض به امنیت به اطلاعات، سیستم‌ها و شبکه‌های رایانه‌ای است.

بند دوم:مسئولیت ارائه دهندگان در تامین امنیت اطلاعات

تدابیر امنیتی در مبارزه با حملات و تعرضات سایبر، به مراتبی که این حملات پیچیده‌تر می‌شوند، در حال تکامل‌اند. این حملات و خطرات آن چنان به سرعت روبه فزونی و پیچیدگی می‌گذارند که بعضاً راهکارهای مبارزه با آن‌ها مدت زمان زیادی از فرصت و انرژی متخصصین را جهت یافتن راهکار مبارزه با آن‌ها به خود مشغول می‌کند. از سوی دیگر این مشکل وجود دارد که راهکارهایی که مدتی جزء بهترین شگردهای مقابله با حملات سایبر محسوب می‌شد، اینک در مواجهه با حملات نوین بسیار کهنه و ناکارآمد جلوه نمایند. از این‌رو ارائه‌کنندگان خدمات اینترنتی نیز باید از ابزاری روزآمد جهت مبارزه با این حملات استفاده کنند. به پاره‌ای از این اقدامات ذیلاً اشاره شده است. قسمتی از این اقدامات در برابر ویروس‌ها، کرم‌ها و تروای رایانه‌ای، به کارگیری برنامه‌های ضد ویروس نظیر برنامه‌های پویشگر ویروس، برنامه‌های پویشگر اکتشافی و برنامه‌های پویشگرهای کاربردمرحله‌ایاست که از لحاظ فنی نرم‌افزارها و اقدامات شناخته شده‌ای به حساب می‌آید. لکن در برابر حملات جدید و ناشناخته که به لحاظ فنی -کاری از دست ارائه‌کنندگان خدمات اینترنتی برنمی‌اید، تنها اقدامی که حداقل می‌توانند انجام دهند اطلاع دادن به گیرندگان خدمات از پخش برنامخه‌های مخرب جدید و ارائه راهکارهای آموزشی به آن‌ها جهت مصون

[1] اصول مهندسی شبکه¬های رایانه¬ای، ترجمه و تألیف واحد تحقیقات و انتشارات مجتمع آموزشی و فنی تهران، انتشارات مؤسسه فرهنگی هنری دیباگران تهران، چاپ سوم، دی ماه ۱۳۸۲.ص۶۵

ماندن از این حملات است. برای مثال ارائه‌کنندگان خدمات اینترنتی در برابر پخش یک ویروس جدید که پویشگرهای آن‌ها نمی‌توانند آن را شناسایی نمایند، موظف‌اند پخش آن را به طریق مقتضی و یا حداقل با قرار دادن یک آگهی در سایت خود که ویروس جدیدی در شبکه اینترنت منتشر شده و ارائه توصیه‌هایی مبنی بر آلوده نشدن اطلاعات و سیستم‌هایشان، به اطلاع گیرندگان خدمات خود برسانند. البته آگاهی یافتن بر این امر نیز با توجه به این‌که روزانه تعداد فراوانی از این برنامه‌ها در اینترنت منتشر می‌شود امری غیرممکن می‌نماید.[1]

در خصوص حملات عمدی و مستقیم نظیر از بین بردن صفحات وب در ارائه خدمات میزبانی، باید راهکارهای فنی لازم جهت مبارزه با آن‌ها اتخاذ شود. برای این کار ابتداءاً باید از دسترسی غیرمجاز که مقدمه‌ای برای ارتکاب جرایم دیگر است جلوگیری به عمل آید. باورهای آتشین در برابر حملات مستقیم برای از بین بردن اطلاعات نظیر از بین بردن صفحات وب بسیار کارا هستند. در این خصوص ارائه‌کنندگان خدمات اینترنتی از باروری آتشین و سیستم تشخیص تجاوز (ورود غیرمجاز) جهت جلوگیری از دسترسی غیرمجاز استفاده می‌کنند.

همچنین به لحاظ فنی روش‌های متفاوتی برای مبارزه با حملات و شگردهای تحصیل اطلاعات خصوصی کاربران وجود دارد. این روش‌ها بسته به نوع حملات و شگردهایی که وجود دارد متفاوت است. البته باید توجه داشت که این روش‌ها اختصاص به مقابله با حملات علیه اطلاعات خصوصی و محرمانه نداشته و در بسیاری موارد برای امنیت اطلاعات و سیستم‌های رایانه‌ای و به طور کلی برای امنیت شبکه به معنای عام مورد استفاده قرار می‌گیرند. برای مثال سیستم باروری آتشین یا سیستم تشخیص ورود غیرمجاز هم برای امنیت موجودیت اطلاعات و سیستم‌های رایانه‌ای و هم برای حملات علیه اطلاعات خصوصی و محرمانه کاربران به کار می‌روند. در این‌باره ذیلاً بیشتر توضیح داده شده است.[2]

بند سوم: عدم تامین امنیت در فضای سایبر

«توانایی‌های مختلف، سرعت‌های بالای نقل و انتقال اطلاعات، پایین بودن هزینه بهره‌گیری از داده‌ها و مزایای فراوان فناوری الکترونیکی، امنیت و حفظ اسرار محرمانه ارتباطات و اطلاعات را که به ناچار از شبکه‌های ارتباطی جهان عبور می‌کنند، موضوع نگرانی متخصصان و کاربران رایانه و اینترنت قرار داده

[1] دادگران، سیدمحمد، مبانی ارتباطات جمعی، انتشارات فیروزه، چاپ چهارم، سال ۱۳۸۱.ص۱۱۱

[2] میر سعیدی، سید منصور، مسئولیت کیفری، جلد اول، قلمرو و ارکان، انتشارات میزان، چاپ اول، بهار ۱۳۸۳.ص۶۵

است. از این‌رو، شیوه‌های امنیتی پیشین وسایل ارتباط جمعی کتبی وکاغذی مانند پاکت‌های مهروموم شده و فایل‌ها و گاوصندوق‌های قفل‌دار جای خود را به فن امنیتی رمزنویسی رایانه‌ای داده‌اند».[1]

«مفهوم ساده رمزنگاری عبارت است از مبهم نمودن اطلاعات به طریقی که از دید فرد غیرمجاز پنهان شود و در عین حال فرد مجاز قادر به مشاهده و استفاده از اطلاعات باشد. فردی مجاز است که دارای کلید مناسب برای رمزگشایی باشد».[2] اعتبارسنجی نیز فرایندی است که اطمینان می‌دهد هر دو نقطه انتهایی ارتباط واقعا همان‌هایی هستند که اظهار می‌دارند. این امر نه تنها نشانه اصالت و هویت واقعی کاربر (نظیر شناسه کاربری و گذر واژه) است، بلکه شامل اصالت ارائه‌دهنده خدمات نیز هست. برای دسترسی به رایانه‌های کارگذا ابتدا باید هویت و اصالت کاربر احراز گردد تا اجازه دسترسی وی به رایانه‌های کارگذار ابتدا باید هویت و اصالت کاربر احراز گردد تا اجازه دسترسی وی به رایانه کارگذار ممکن شود. از این‌رو اعتبارسنجی برای مقابله با حملات دسترسی غیرمجاز و «صید اطلاعات شخصی» بسیار ضروری است.[3]

اعتبار طرفین ارتباط بیشتر در تجارت الکترونیک مصداق می‌یابد. از این نظر ارائه‌کننده خدمات باید با دادن تضمین‌های لازم جهت اعتبارسنجی ارتباطات، مانع از آن گردد که یکی از طرفین ارتباط، معامله‌ای کند یا سفارشی دهد یا سندی را به صورت الکترونیکی امضاء کند که بعدا آن را انکار کند، به لحاظ فنی به آن حمله «تکذیب» اطلاق می‌شود. اعتبارسنجی در معاملات باید امکان انکار را از طرفین معامله سلب نماید. همچنین اعتبار اطلاعات می‌تواند دربرگیرنده اصالت اطلاعات از تعرض و تغییر باشد، چرا که داده‌ها در صورت تغییر اعتبار خود را از دست می‌دهند؛[4]

فناوری رمزنگاری نیز روشی است که جهت ممانعت از دسترسی دیگران به اطلاعات خصوصی افراد مورد استفاده قرار می‌گیرد و در برابر حملات دسترسی به اطلاعات و خصوصاً شنود اطلاعات بسیار کارایی دارد. اما رمزنگاری فواید دیگری نیز دارد؛ به طور کلی با استفاده از رمزنگاری می‌توان سه سرویس امنیتی زیر را

---

[1]. بردبار، محمد حسن، منبع پیشین، ص ۱۵۴

[2]. کانتر، روزایت، تحول، ترجمه عبدالرضا رضایی نژاد، نشر فرا، چاپ اول، تهران، تابستان ۱۳۸۲.ص۷۶

[3]صبری، حمید، آشنایی با دانش ارتباطات، انتشارات مؤلف، چاپ اول.ص۱۷۴

[4]. قانون تجارت الکترونیکی در ماده خود اشعار دارد: «هرگونه تغییر در تولید، ارسال، دریافت، ذخیره و یا پردازش داده پیام با توافق و قرارداد خاص طرفین معتبر است». مواد ۱۰ تا ۱۶ این قانون نیز به داده پیام‌های مطمئن، امضای الکترونیکی مطمئن و شرایط اعتبار آن‌ها پرداخته است.

ارائه داد: محرمانه‌سازی، حفظ تمامیت (اعمال تغییر بر اطلاعات) و مجوزسنجی (اعتبارسنجی مبدأ اطلاعات و جلوگیری از تکذیب اطلاعاتی که از مبدأ آمده‌اند).[1]

رمزنگاری قدمتی بسیار طولانی دارد و کشورها در طول تاریخ و خصوصاً در زمان جنگ‌ها برای محرمانه ماندن اطلاعات مهم آن را مورد استفاده قرار می‌داده‌اند. ورود به دنیای ارتباطات رادیویی و ارسال امواج، مخابراتی و ماهواره‌ای و گسترده شدن و تحول آن‌ها- خصوصاً در قرن بیستم- و پس از آن اختراع رایانه‌ها و ایجاد شبکه‌های رایانه‌ای و استفاده‌های مختلف از آن‌ها نظیر تجارت الکترونیک، سرمنشأ پیدایش علم نوینی به نام فناوری رمزنگاری گشته است.[2] روش‌های رمزنگاری در طول زمان بسیار تغییر و تحول داشته‌اند. در واقع «این روش‌ها در حدود ۴۰۰۰ سال مورد استفاده قرار گرفته‌اند و شروع استفاده از آن‌ها با هیروگلیف‌های مکتوب مصرباستان بوده است. از زمان این اقدام یونانی‌ها و رومن‌ها به بعد، دولت‌ها برای حفاظت از ارتباطات مهم نظامی و دیپلماتیک خود از رمزنگاری استفاده کرده‌اند و امروزه الگوریتم‌های ریاضی‌ای که به واسطه کامپیوتر به وجود آمده‌اند، رمزنگاری را به طور مجانی و یا با هزینه بسیار کم برای اشخاص ممکن می‌سازند».[3]

بدیهی است که «رمزنگاری جلوی افراد را برای قطع (متوقف ساختن) پیغام‌ها نمی‌گیرد، اما مانع می‌شود که افراد بتوانند پیغام‌های قطع شده را بخوانند». از این‌رو در شنود اطلاعات، ممکن است که مهاجم بتواند داده‌ها را قطع نماید، اما نمی‌تواند از مضمون و محتوای آن‌ها چیزی بفهمد؛ مگر این‌که رمزشکنی کند. استفاده از یک سیستم رمزنگاری مناسب این احتمال را بسیار پایین می‌آورد.[4] پیام‌هایی که باید رمزنگاری شوند «متن ساده» نام دارند، اما متن خروجی فرآیند رمزنگاری را «متن رمزی» می‌نامند. رمزنگاری روش‌های متفاوتی دارد؛ از این روش‌ها می‌توان به روش جایگزینی، جابجاسازی (پس و پیش کردن)، پنهان‌ساری، سیستم ابزاری و الگوریتم‌های ریاضی یا کدهای منبع اشاره کرد.[5] روشی که در علوم رایانه‌ای مورد استفاده قرار می‌گیرد روش اخیر است. در این روش، «از کامپیوترها جهت مرتب کردن ردیف‌های صفر و یک که بیت

---

[1]. فناوری رمزنگاری، کمیته مبارزه با جرایم رایانه‌ای معاونت حقوقی و توسعه قضایی قوه قضائیه، ترجمه و ویرایش سپیده دولتشاهی، تیرماه ۱۳۸۲ ص ۳۳.

[2]صبری، حمید، آشنایی با دانش ارتباطات، انتشارات مؤلف، چاپ اول.ص۱۵۸

[3]. دادگران، سیدمحمد، مبانی ارتباطات جمعی، انتشارات فیروزه، چاپ چهارم، سال ۱۳۸۱.ص۱۲۵

[4]. متخصصین بین رمزها و کدها تفاوت قائل‌اند. رمز تبدیل کاراکتر برای کاراکتر یا بیت برای بیت است که بدون توجه به ساختار زبان شناسی پیام انجام می‌شود. [اما] کد یک کلمه را با کلمه یا نماد دیگر جایگزین می‌کند».

[5]وبستر، فرانک، نظریه‌های جامعه اطلاعاتی، ترجمه اسماعیل قدیمی، انتشارات قصیده‌سرا، چاپ دوم، ۱۳۸۳.ص۱۳۴

نیز نامیده می‌شوند به صورت گروه‌ها و بلوک‌هایی جهت ایجاد کلید استفاده می‌شود. هر کلید تعداد از پیش تعیین شده‌ای بیت دارد. منظم کردن بیت‌ها در هر کلید براساس الگوریتم‌های ریاضی که به وسیله الگوریتم رمزنگاری یا کد مبدأ ارائه شده‌اند صورت می‌گیرد. این الگوریتم‌ها سپس از کلمه‌های رمز برای رمزنگاری و رمزگشایی پیغام‌ها استفاده می‌کنند».

نتیجه‌گیری

در نهایت و جمع بندی کلی این پژوهش باید گفت جامعه کنونی جهانی در آستانه قرن بیست و یکم با شتاب به سوی جامعه اطلاعاتی در حرکت است. این جامعه بر مبنای در اختیار داشتن منابع دانش بنیان‌یافته و بسترهای آن به سرعت در حال شکل‌گیری است. دولت‌ها در آستانه قرن بیست‌ویکم درتلاش‌اند که هر چه سریع‌تر پیش‌زمینه‌های تحقق چنین جامعه‌ای را در کشورهای خویش تحقق بخشند تا هر چه بیشتر منابع دانش، فناوری و به تبع آن ثروت ناشی از آن را در اختیار گیرند.در حوزه خدمات دسترسی و میزبانی داده محتوا، انتشار یک‌باره محتویات غیرقانونی در اینترنت توسط دیگرآنکه ابزار نشر اطلاعات را در بعد جهانی برای همه فراهم کرده است، در ابتدا باعث گردید که در جامعه قضایی کشورها با استدلال‌ها و توجیهاتی غیرمستدل اقدام به صدور آرایی در راستای محکومیت ارائه‌کنندگان خدمات اینترنتی نمایند که در بسیاری موارد غیرمنصفانه و بدون توجه به اصول حقوق کیفری صادر شده بودند؛ به‌طوری‌که در بسیاری موارد، ارائه‌کنندگان خدماتی که از انتشار یا ذخیره مطالبی که خدمات دسترسی یا میزبانی آن را فراهم می‌کردند کاملاً ناآگاه بودند در کنار مرتکب اصلی و همچون او مسئول و محکوم شناخته شدند. این امر سبب گردید که حقوق‌دانان کشورها تلاش نمایند که چارچوب تکالیف و مسئولیت‌های ارائه‌کنندگان خدمات را در مبارزه با اطلاعات غیرقانونی روشن سازند؛ در این راستا، تحلیل مسئولیت کیفری ارائه‌کنندگان خدمات اینترنتی در حوزه ذخیره و ارائه اطلاعات چند مرحله را پشت سر گذارده است: در مرحله نخست حقوق‌دانان سعی کرده‌اند با توجه به برخی از مبانی مسئولیت کیفری مسئولیت ارائه‌کنندگان خدمات را در ارائه و ذخیره محتوای غیرقانونی توسط دیگران به حیطه نقد بگذارند. در این راستا، ارائه‌کنندگان خدمات و کاربران فاقد مختصاتی هستند که بتوان مسئولیت عاریتی را که به عنوان عمده قالب مسئولیت اعتباری مطرح می‌شود نسبت به آنان اعمال نمود؛ در مورد ارائه‌کنندگان خدمات قواعد مسئولیت اشتراکی تا حدود زیادی در این خصوص راه گشا بوده است و مسئولیت آن‌ها را تنها در صورت آگاهی نسبت به وجود اطلاعات غیرقانونی و عدم اقدام در غیرقابل دسترس نمودن آن اطلاعات پذیرفته شده است.

منابع و مآخذ

۱.اردبیلی، محمد علی، حقوق جزای عمومی طبق قانون مصوب۹۲، جلد نخست، انتشارات میزان، ۱۳۹۳

۲.اصول مهندسی شبکه‌های رایانه‌ای، ترجمه و تألیف واحد تحقیقات و انتشارات مجتمع ۳.آموزشی و فنی تهران، انتشارات مؤسسه فرهنگی هنری دیباگران تهران، چاپ سوم، دی ماه ۱۳۸۲

۴.انصاری، باقر و سایر نویسندگان، مسئولیت مدنی رسانه‌های همگانی، انتشارات معاونین پژوهش، تدوین و تنقیح قوانین و مقررات، چاپ اول، تابستان ۱۳۸۱

۵.بردبار، محمد حسن، درآمدی بر حقوق ارتباط جمعی، انتشارات ققنوس، چاپ اول، ۱۳۸۱

۶.تننباوم، آندرو اس، شبکه‌های کامپیوتری، ترجمه عین‌الله جعفرنژاد قمی، انتشارات علوم رایانه، چاپ سوم، پاییز ۱۳۸۳

۷.جلالی، علی اکبر، شهر الکترونیک، انتشارات دانشگاه علم و صنعت ایران، چاپ اول، ۱۳۸۲

۸.خلیق، غلامرضا، کار و شبکه اینترنت، انتشارات اشراقی و راهی، چاپ سوم، بهار ۱۳۸۲

۹.دلفانی، علی اشرف، مبانی مسئولیت کیفری در حقوق اسلام فرانسه، انتشارات مؤسسه بوستان کتاب قم، چاپ اول، ۱۳۸۲

۱۰.سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین‌المللی و حقوق کیفری ایران، انتشارات خیام، ۱۳۹۲

۱۱.شیخ‌الاسلامی، عباس، جرایم مطبوعاتی، بررسی تطبیقی سیاست جنایی جمهوری اسلامی ایران و انگلستان، انتشارات جهاد دانشگاهی مشهد، چاپ اول، تابستان ۱۳۸۰

۱۲.صانعی، پرویز، حقوق جزای عمومی، جلد ۱و۲، انتشارات گنج دانش، چاپ ششم، تهران، ۱۳۸۰

۱۳.صبری، حمید، آشنایی با دانش ارتباطات، انتشارات مؤلف، چاپ اول.

۱۴.کانتر، روزایت، تحول، ترجمه عبدالرضا رضایی نژاد، نشر فرا، چاپ اول، تهران، تابستان ۱۳۸۲