همایش ملی مطالعات و پژوهش های علمی علوم انسانی

نهاد برگزار کننده همایش: موسسه قانون یار با حمایت معنوی دانشگاه آزاد اسلامی واحد کرمانشاه
سردبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی شماره مجوز: ۷۸۸۶۴-۴۸۵۳
سال برگزاری همایش: ۱۳۹۷ شماره مقاله: ۸۳۵/۱۹۹ رده بندی کنگره: ط ۵۲۶/۲

مسئولیت کیفری عدم تامین امنیت محتویات متفرقه در فضای مجازی

حامد افشار

چکیده

تولید یا ارایه یا انتشار محتویات غیرقانونی در فضای مجازی رایانه و اینترنت جرم و قابل مجازات است و قاعدتاً مسوولیت کیفری بر کسی بار می شود که عناوین مجرمانه مربوط به محتویات رایانه ای را انجام دهد، اما چون دسترسی به اینترنت و خدمات آن از طریق ارایه دهندگان خدمات اینترنتی میسر می شود، این عوامل در بعضی مواقع باید مسوولیت کیفری ناشی از ارایه محتویات غیرقانونی را متحمل شوند. غیرقانونی بودن محتویات، گاه به این دلیل است که قانون از آن ها حمایت کرده و شخصی این حمایت قانونی را نقض کرده است، مثل محتویات متضمن نقض کپی رایت یا نقض حریم خصوصی. گاهی نیز غیرقانونی بودن محتویات به این دلیل است که این محتویات ذاتاً غیراخلاقی و نامشروع هستند، مثل انتشار تصاویر یا فیلم های مستهجن. ارایه دهندگان خدمات اینترنتی بر اساس مقررات و در حد متعارف مکلف هستند از طریق تدابیری همچون پالایش، نصب دیوار آتشین و مواردی از این دست، از ارایه محتویات غیرقانونی تعریف شده در قانون جلوگیری کنند. مسوولیت پالایش و ممانعت از ارایه محتویات غیرقانونی را می توان «مسوولیت پیشگیرانه» یا «مسوولیت پیش از ارتکاب جرم» نامید . در مورد مسوولیت پس از ارتکاب جرم، برای ارایه دهندگان خدمات اینترنتی بر فرض آگاهی و اطلاع از محتویات مستهجن یا غیرقانونی، سه نوع مسوولیت کیفری مطرح می شود: مسوولیت کیفری مستقیم، مسوولیت کیفری ناشی از فعل غیر و مسوولیت مشترک .

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

بخش اول: کلیات

مهم‌ترین و عمده‌ترین مبحث در خصوص مسئولیت در فضای سایبر، مسئولیت ارائه کنندگان خدمات اینترنتی است؛ قرار گرفتن ارائه کنندگان خدمات در مسیر گذار اطلاعات، خصوصاً واقع شدن آنان به عنوان واسطه‌هایی در سپهر بزرگ‌ترین شاهراه ارتباطی و اطلاعی جهان که از طریق رایانه‌های کارگذار خود، داده محتوا را در این کلان شبکه اطلاعاتی انتقال می‌دهند یا فضایی را برای ذخیره داده محتوا به سایر اشخاص ارائه می‌نمایند، بی شک نمی‌تواند فارغ از تکالیف و مسئولیت‌هایی برای آنان باشد و این امر تکلیف آنان را نسبت به سایر اشخاصی که در فضای سایبر نقش آفرین‌اند دشوارتر می-کند.[1]مسئولیت کیفری ارائه کنندگان خدمات به طور کلی مبتنی بر دو دسته خدمات و «ذخیره‌ی» اطلاعات است؛ و در این میان، یا ارائه کنندگان خدمات اینترنتی در شبکه اینترنت، اطلاعات «ایجاد شده توسط خود» را ارائه یا ذخیره می‌کنند و یا این که به ارائه یا ذخیره‌ی اطلاعات ایجاد شده «توسط دیگران» اقدام می‌کنند. مسئولیت تولید و ارائه اطلاعات غیرقانونی توسط خود ارائه کننده‌ی خدمات در صورتی که وی ارائه کننده‌ی محتوا باشد و به کلام حقوقی «مباشرت» وی در این کار، همان‌گونه که کلاً در بحث ارائه اطلاعات غیرقانونی در همگی رسانه‌ها وجود دارد، در هر حال بر دوش ارائه کننده اطلاعات باقی است و خود ارائه کننده‌ی داده محتوا باید پاسخ‌گو باشد.[2] لکن با توجه به

[1] شیایزری، کریانگ ساک کیتی، حقوق بین‌المللی کیفری، ترجمه بهنام یوسفیان، محمد اسماعیلی، انتشارات سمت، چاپ اول، ۱۳۸۳.ص۷۸

[2] . در همین راستا، در بند ۳ از ماده‌ی ۵ قسمت «ب» مصوبه‌ی شورای عالی انقلاب فرهنگی با عنوان «ضوابط و مقررات شبکه‌های اطلاع رسانی رایانه‌ای» (آئین نامه‌ی واحدهای ارائه کننده‌ی خدمات اطلاع رسانی و اینترنت رسا (ISP) آمده است: «شرکت رسا (ISP) دارای مسئولیت قانونی بوده و نسبت به کلیه ضوابط و تعهدات زیر پاسخ‌گو می‌باشد:

این که مبنای اینترنت بر محور آزادی در ایجاد و ارائه اطلاعات توسط عموم استوار است، فرض دوم که همانا ذخیره یا در دسترس گذاشتن اطلاعات ایجاد شده توسط دیگر کاربران در سطح جهانی است اهمیت بیشتری می‌یابد و از آن‌جا که اطلاعاتی که توسط دیگران ایجاد می‌شود نسبت به اطلاعات ایجاد و ارائه شده توسط خود ارائه کنندگان خدمات در سطح بسیار بیشتری قرار دارد باید دید که آیا ارائه کنندگان خدمات در کنار مباشر اصلی تولید و ذخیره‌ی اطلاعات چه تکالیف و مسئولیت‌هایی دارند؟ و اگر مسئولیتی متوجه آن‌هاست حدود آن تا چه اندازه است؟ به عبارت دیگر ارائه کنندگان خدمات به لحاظ عدم پیش‌گیری از ارائه و اشاعه‌ی داده محتوای غیرقانونی که توسط دیگری ایجاد شده و لکن از طریق رایانه‌های کارگذار آن‌ها در فضای سایبر منتشر شده یا در رایانه‌های کارگذار آن‌ها ذخیره شده و قابل دسترسی می‌گردد چه تکالیف و مسئولیت‌هایی دارند؟

پاسخ به این سؤال و به طور کلی بحث مسئولیت ارائه کنندگان خدمات اینترنتی یکی از چالش برانگیزترین مباحث مربوط به مسئولیت در طی دو هفته دهه‌ی گذشته بوده است؛ خدمات در فضای سایبر و خصوصاً خدمات اینترنت طی چندین دهه‌ی اخیر آن قدر رشد پرشتابی داشته که ناگهان جهان با یک فوران اطلاعاتی بی‌سابقه در حوزه‌ی نشر داده محتوا مواجه شده است. پیش از رشد شبکه‌های سایبر و خصوصاً اینترنت، حوزه‌ی نشر محدود

۵-۳-۱- مؤسسات و شرکت‌های رسا (ISP) و کاربران برای محتوایی که خود بر روی شبکه عرضه می‌نمایند طبق این آیین نامه مسئول و پاسخ‌گو می‌باشند.

تبصره: ارائه خدمات دسترسی به منابع اطلاعات، مشمول این بند نمی‌باشد.

۵-۳-۲- مسئولیت رعایت قوانین مالکیت معنوی و حق تألیف و تصنیف به عهده ارائه کننده‌ی اطلاعات در شبکه می‌باشد». هم‌چنین در ماده‌ی ۶ از قسمت «ج» مصوبه‌ی مذکور (آیین نامه‌ی دفاتر خدمات حضوری اینترنت (Coffee Net)) نیز آمده است: «دفاتر و کاربران برای محتوایی که خود تولید و عرضه می‌نمایند مطابق مقررات و ضوابط قانونی موجود کشور از جمله رعایت قوانین و مقررات و حق مالکیت معنوی، مسئول و پاسخ‌گو می‌باشند».

بود؛ تنها کسانی می‌توانستند اطلاعاتی را به سمع و نظر عموم برسانند که ابزار آن را در اختیار داشتند. هم این ابزار محدود بود و هم این که این ابزار محدود در اختیار عده‌ای محدود قرار داشت؛ صرفاً روزنامه نگاران و صاحبان نشریه دارندگان مراکز پخش برنامه-های رادیویی و تلویزیونی، دارندگان سیستم‌های تابلوی اعلانات[1] و نظایر آن‌ها امکان نشر داده محتوا را داشتند.[2] با گسترش شبکه‌های سایبر و اینترنت تقریباً اکنون این اماکن برای همه فراهم شده است که فضایی برای خود داشته باشند و بتوانند هر اطلاعاتی که دلخواهشان است در آن فضا ذخیره و برای دیگران قابل دسترس سازند. لذا قسمت عمده‌ی اطلاعات موجود در اینترنت توسط مشترکین خدمات میزبانی در شبکه قرار می‌گیرد که دارای سایت (وبگاه یا تارگاه) های اینترنتی هستند و با اجازه‌ی فضایی از ارائه کنندگان خدمات اینترنتی، اطلاعات خود را در یارانه‌های میزبان ارائه کنندگان خدمات اینترنتی وارد می‌کنند. چنین اطلاعاتی در شبکه برای همه قابل دسترس خواهد بود. افزایش وبگاه-هایی که امکان ارائه‌ی نظرات در خصوص موضوعات مختلف را به کاربران می‌دهند، نظیر وبگاه‌های گروه خبری، محیط‌های گپ اینترنتی یا محیط‌هایی که به رایگان به کاربران اجازه‌ی می دهند که صفحه اینترنتی خاص خود را داشته باشند نیز بر شتاب گسترش میزان داده محتوا و جریان آن افزوده است. بدین ترتیب، خود ارائه کنندگان خدمات اینترنتی معمولاً کم‌ترین نقش را در ارائه‌ی اطلاعات در اینترنت دارند و غالباً بستر لازم را برای گیرندگان خدمات فراهم می‌کنند تا آن‌ها اطلاعات خود را ذخیره یا در اینترنت ارائه کنند.[3]

بخش دوم: مسئولیت مجرمانه ارائه و ذخیره اطلاعات مجرمانه

[1]. Bulletion Board System.

[2] سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین¬الملل و حقوق کیفری ایران، انتشارات خیام، چاپ اول، ۱۳۹۲.ص۸۲

[3] محسنی، منوچهر، جامعه شناسی جامعه اطلاعاتی، نشر دیدار، چاپ اول، ۱۳۸۰.ص۷۴

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.[1]

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 است. در

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

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 مالك ملکی را به این دلیل که ملك خود را در اختیار دیگری قرار داده و او در آن ملك 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

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

ذخیره می‌گردد در بسیاری موارد غیر ممکن، و حتی در صورت آگاهی، اثبات و احراز آن مشکل است.[1]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 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 رایانه-های 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 آن-گاه 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

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

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]

بخش سوم: 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 آدرس ارجاع ارائه می‌دهد. مسئولیت ارائه‌کنندگان خدمات

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

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.[۲]

- 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

---

[۱]. مشابه رویه مذکور را با شرایطی ساده‌تر می‌توان در ماده ۱۴ قانون صدور چک کشور خودمان برای دستور عدم پرداخت وجه چک‌های 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]. Information Location Tools

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.[1]

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 یافته-های منطقی و تجارب حاصل در بعد مسئولیت کیفری در فضای سایبر 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 اول:تحلیل مسئولیت کیفری ارائه دهندگان خدمات در تجارت الکترونیک شورای اروپا

الف) آلمان: آلمان اولین کشوری است که در زمینه مسئولیت ارائه‌کنندگان خدمات اینترنتی اقدام به وضع مقرراتی خاص کرده است. سابقا ماده ۵ «قانون بهره‌برداری از خدمات راه دور» مصوب ۱۹۷۷ این کشور- که خدمات ارتباطی و اطلاعاتی را (به غیر از خدمات مطرح در «قانون ارتباطات راه دور» مصوب ۱۹۹۶) پوشش می‌داد، و به عنوان بخشی از «قانون چند رسانه‌ای» به تصویب رسیده بود- اختصاص به مسئولیت کیفری ارائه-کنندگان خدمات اینترنتی داشت. طبق بند ۱ این ماده، ارائه‌کنندگان خدمات اینترنتی که خدمات «میزبانی» را ارائه می‌نمودند صرفاً در صورتی که نسبت به غیرقانونی بودن

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

اطلاعات آگاه بوده و حذف یا غیرقابل دسترس کردن آن اطلاعات به لحاظ فنی ممکن و منطقاً مورد انتظار می‌بود مسئولیت داشتند.[1]

از سوی دیگر، بند ۳ ماده قانون مزبور اشعار می‌داشت که ارائه‌کنندگان خدماتی که صرفاً «دسترسی» به اطلاعات را برای کاربران فراهم می‌کنند (خدمات دسترسی و انواع آن)، از هر گونه مسئولیتی معافند و طبق بند ۴، ارائه‌کنندگان خدمات اینترنتی موظف بودند به محض اطلاع از این‌که اطلاعاتی که ارائه می‌شود غیرقانونی است- جز در ارتباطات خصوصی که باید رعایت محرمانگی و حریم خصوصی ارتباطات را بکنند- آن اطلاعات را غیرقابل دسترس سازند، البته مشروط به آن‌که غیر قابل دسترس ساختن اطلاعات مزبور به لحاظ فنی ممکن و منطقاً مورد انتظار باشد؛ در غیر این‌صورت ارائه‌کنندگان خدمات اینترنتی مسئول خواهند بود. غیرقابل دسترس کردن اطلاعات ممکن بود به دستور مقام قضایی یا دستور مراکز ذیصلاح اداری باشد. علت وضع دو بند فوق همان‌گونه که گفته شد، حجم بسیار بالای اطلاعاتی بود که در رایانه‌های کارگذار ارائه‌کنندگان خدمات اینترنتی ذخیره می‌گردد.[2]بدین ترتیب این کشور پیش از آن‌که دستورالعمل تجارت الکترونیک شورای اروپا و حتی قانون کپی‌رایت هزاره دیجیتال آمریکا مقرراتی را برای یکسان‌سازی مسئولیت ارائه‌کنندگان خدمات اینترنتی وضع کند با توجه به مشکلات حادث در صدور آرائی که به صورت غیرمنطقی ارائه‌کنندگان خدمات اینترنتی را مسئول می‌دانست و پیش از این مورد اشاره قرار گرفت، مقرراتی را در این خصوص وضع کرده بود که که به انصاف باید آن را نخستین مقررات پیشرو در این‌باره دانست. با تصویب

[1] سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین المللی و حقوق کیفری ایران، انتشارات خیام، چاپ اول، ۱۳۹۲.ص۱۰۵

[2] شیایزری، کریانگ ساک کیتی، حقوق بین¬المللی کیفری، ترجمه بهنام یوسفیان، محمد اسماعیلی، انتشارات سمت، چاپ اول، ۱۳۸۳.ص۴۷

دستورالعمل تجارت الکترونیک شورای اروپا در این کشور، با اصلاحاتی جزیی تقریبا همان مقررات اعمال می‌شود که ذیلا مورد بررسی قرار خواهد گرفت.[1]

ب) سوئد: سابقاً مقرراتی چند در قانون «تابلوهای اعلان الکترونیکی» کشور سوئد وجود داشت که نسبت به ارائه‌کنندگان خدمات اینترنتی نیز اعمال می‌شد. ماده ۵ قانون مزبور اشعار می‌داشت که ارائه‌کنندگان خدمات تابلوهای الکترونیکی (و از جمله ارائه‌کنندگان خدمات اینترنتی) باید به محض دریافت اخطار مبنی بر این‌که اطلاعاتی که ارائه می‌دهند غیرقانونی است، نسبت به حذف آن‌ها اقدام نمایند. به علاوه ماده ۴ قانون نظارت داشته باشند؛ البته این نظارت به این صورت نبود که ارائه‌کنندگان خدمات بر جزءجزء اطلاعاتی که ارائه می‌کنند نظارت داشته باشند، بلکه اگر به صورت کامل و یا برای مدتی طولانی نظارت نداشتند مسئول بودند. این نظارت نسبت به مورد متفاوت بود؛ ارائه‌کنندگان خدماتی که محتوای تجاری (برنامه‌های حاوی مطالب تبلیغاتی) ارائه می‌کردند تکلیف نظارتی بیشتری نسبت به سایر ارائه‌کنندگان خدمات داشتند؛ اما اگر محتوای اطلاعاتی که ارائه می‌کردند بسیار زیاد و حجیم بود، کاربران می‌توانستند از ارائه‌کنندگان خدمات مزبور شکایت کنند تا نسبت به غیرقابل دسترس کردن آن‌ها اقدام شود.

ج) اتریش: در این کشور بندهای ۱ و ۲ ماده ۷۵ و نیز فراز ۶ از بند ۱ ماده ۱۰۴ «قانون ارتباطات» که به ارائه‌کنندگان خدمات ارتباطی به طور کلی اشاره داشت و به لحاظ موسع بودن ارائه‌کنندگان خدمات اینترنتی را نیز در بر می‌گرفت، اشعار می‌داشت که اگر ارائه-کنندگان خدمات ارتباطی «به طور متعارف تدابیری را جهت پیشگیری از سوءاستفاده از سیستم‌های خود» به عمل نیاورند مسئول خواهند بود. از سوی دیگر، براساس بند ۲ ماده

[1] دلفانی، علی اشرف، مبانی مسئولیت کیفری در حقوق اسلام فرانسه، انتشارات مؤسسه بوستان کتاب قم، چاپ اول، ۱۳۸۲.ص ۵۰

۷۵، ارائه‌کنندگان خدمات ارتباطی که صرفا خدمات دسترسی را ارائه می‌کردند، از هر گونه مسئولیتی معاف بودند.

چنانچه مشاهده می‌شود قانون این کشور نیز نسبت به انواع خدماتی که ارائه‌کنندگان خدمات اینترنتی ارائه می‌کنند، از اجمال بسیاری برخوردار بود. در واقع، اتخاذ «تدابیری متعارف» برای پیشگیری از سوءاستفاده از سیستم‌های ارتباطی مواردی نظیر استفاده از نرم-افزارهای لازم جهت جلوگیری از برنامه‌های مخرب و موجد اختلال را شامل می‌شد که به ارائه داده محتوای مجرمانه ارتباطی نداشت. از سوی دیگر، ارائه‌کنندگان خدمات دسترسی از هر گونه مسئولیت معاف شناخته شده بودند که این امر صحیح نبود، چه آنان باید در صورت اطلاع از غیرقانونی بودن اطلاعاتی که ارائه می‌کردند نسبت به پیشگیری از ادامه انتشار آن‌ها اقدام می‌کردند و در غیر این صورت مسئول بودند. با تصویب دستورالعمل تجارت الکترونیک شورای اروپا این کشور نیز مقررات خود را در این زمینه با آن هماهنگ کرده است.

چ) انگلستان: کشور انگلستان پیش از دستورالعمل شورای اروپا قانون خاصی در خصوص مسئولیت کیفری ارائه‌کنندگان خدمات اینترنتی به تصویب نرسانده بود. با این حال موادی از «قانون افتراء»[1] مصوب ۱۹۹۶ این کشور به مسئولیت ارائه‌کنندگان خدمات ارتباطی اشاره داشت. طبق فراز «e» بند ۳ماده ۱ قانون مزبور، اگر شخصی عامل یا ارائه-کننده [خدمات] دسترسی به سیستم‌های ارتباطی باشد که از طریق آن‌ها اظهارات افتراءآمیز منتقل یا از طریق شخصی که وی بر او نظارت مؤثر ندارد ارائه می‌گردد، «در

[1] . Defamation Act

صورت توجه متعارف» نویسنده، سردبیر یا ناشر قلمداد نمی‌گردد و بنابراین مسئولیتی ندارد.[1]

بند دوم: مسئولیت ارائه‌کنندگان خدمات اینترنتی در خدمات دسترسی

دستورالعمل شماره EC/۳۱/۲۰۰۰ 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)»[2] 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.[3]

---

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

[2] . Directive on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in Internet Market (Directive on Electronic Commercr)

توضیح این نکته ضروری است که شورای اروپا در خصوص تنظیم مقررات ارتباطات ارائه خدمات الکترونیکی در جامعه اطلاعاتی، ابتدا دستورالعملی به نام «دستورالعمل چارچوب» ۱۹۹۹/۵/EC Directive (Framework Directive) را به عنوان مبنای کار در این خصوص تصویب کرده و سپس به مرور و با افزودن دستورالعمل‌های مختلف، با جزئیات بیشتری مقررات لازم برای قاعده‌مند کردن جامعه اطلاعاتی را وضع کرده است. «دستورالعمل تجارت الکترونیک» نیز قسمتی از این مقررات است. برای توضیح بیشتر در این باره ر.ک

http://www.culleninternational.com/documents/Cullen/telecom/eurodoc/regsystem/frworkdirective/frworkdirectivearticle01.com

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

این دستورالعمل در بند ۱۷ مقدمه و بند a ماده ۲ خود که به تعاریف می‌پردازد بیان داشته است، تعریف «خدمات جامعه اطلاعاتی»[1] همان است که سابقاً در دستورالعمل شماره EC/۳۴/۹۸ مصوب ۲۲ ژوئن ۱۹۹۸ در خصوص «وضع رویه‌ای برای ارائه اطلاعات در حوزه موازین و مقررات فنی و مقررات راجع به خدمات جامعه اطلاعاتی»[2] که توسط دستورالعمل شماره EC/۸۴/۹۸ مصوب ۲۰ نوامبر ۱۹۹۸ در خصوص «حمایت حقوقی از خدمات مبتنی یا مشتمل بر دسترسی مسروط»[3] 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»[4] 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.[5]

---

[1] . Information Society Services

[2] . Directive Laying Down A Procedure for the Provision of Information in the Field of Technical Standards and Regulations and of Rules on Hnformation Society Services

[3] . Legal Protection of Services Based on, or Consisting of, Conditional Access

[4] . Recipient of the Service

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

از این نظر، چنانچه مشاهده می‌شود، در دستورالعمل‌های اتحادیه اروپا عنوان ارائه-کنندگان خدمات اینترنتی به کار نرفته است. در واقع اصطلاح «ارائه‌کنندگان خدمات اطلاعاتی» و تعریف موسعی که از «خدمات اطلاعاتی» ارائه شده نشانگر آن است که دستورالعمل‌های مزبور ارائه خدمات اینترنتی را قسمتی از خدماتی می‌دانند که در بطن خدمات گسترده‌تری به نام خدمات جامعه اطلاعاتی قرار می‌گیرد به طوری که این خدمات دایره وسیعی از انواع خدمات را که از طریق ابزار الکترونیک ارائه می‌شود در بر می‌گیرد؛ این خدمات با توجه به بند ۱۸ مقدمه دستورالعمل تجارت الکترونیک که خدمات جامعه اطلاعاتی را تبیین کرده گستره وسیعی از خدمات اقتصادی آن لاین را شامل می‌شود که به درخواست شخص به وی ارائه می‌شود و می‌تواند شامل فروش آنلاین کالاها، فعالیت‌های اقتصادی آنلاین، ارائه اطلاعات، ارائه ابزاری برای جستجو، بازیابی و دسترسی به اطلاعات، انتقال اطلاعات، میزبانی اطلاعات، برنامه‌های ویدیوئی به محض مطالبه[1] و نیز پست الکترونیکی باشد. لکن خدمات پخش برنامه‌های رادیویی و تلویزیونی[2] جزو خدمات جامعه اطلاعاتی محسوب نمی‌شود. از این‌رو خدمات جامعه اطلاعاتی هم براساس بند مذکور و هم براساس تعریفی که از آن‌ها در دستورالعمل شماره EC/۳۴/۹۸ که توسط دستورالعمل شماره EC/۴۸/۹۸ اصلاح شده خدماتی است که عمدتاً جنبه اقتصادی دارد و از طریق ابزار الکترونیک به طور کلی و نه صرفاً اینترنت- ارائه می‌شود. بدین ترتیب این خدمات بیشتر در حوزه تجارت الکترونیک قرار می‌گیرد و از همین روست که مسئولیت ارائه‌کنندگان این خدمات نیز در چارچوب این دستورالعمل مورد بررسی قرار گرفته است.

[1] . Video on Demand

[2] . Radio and Television Broadcasting

بخش چهارم: مسئولیت ارائه‌کنندگان خدمات اینترنتی در خدمات انباشت موقت اطلاعات

در مباحث پیشین دیدیم که امکان کنترل و نظارت فیزیکی ارائه‌دهنده خدمات بر داده محتوای مجرمانه امکان‌پذیر نیست. لکن با پیشرفت فناوری و روش‌های کنترل خودکار نظیر استفاده از نرم‌افزارهای پالایشگر (فیلتر) این محدودیت تا حدود زیادی مرتفع می‌شود. اما آیا مسئولیت ارائه‌کنندگان خدمات در این‌باره چگونه و به چه میزان باید باشد؟ این امر را می‌توان در دو بعد خدمات دسترسی و خدمات میزبانی مورد مطالعه قرار داد:

بند اول : پالایش محتویات مجرمانه در خدمات دسترسی

در خصوص اطلاعاتی همچون هرزه‌نگاری کودکآنکه ضرر آن «جنبه عمومی» داشته و کاربران را به طور کلی تحت تأثیر منفی قرار می‌دهد، در برخی کشورها ارائه‌کنندگان خدمات اینترنتی را رأسا موظف به غیرقابل دسترس کردن اطلاعات نموده‌اند.[1] «پالایش اطلاعات»[2] غیرقانونی نظیر محتوای متضمن هرزه‌نگاری و خصوصا هرزه‌نگاری کودکان از جمله این اطلاعات است. در پالایش چنین اطلاعاتی، ارائه‌کنندگان خدمات اینترنتی با پیکره‌بندی رایانه‌های کارگذار خود اطلاعاتی که متضمن عباراتی نظیر[3] است را در حین عبور از رایانه‌های کارگذارشان متوقف و برای کاربران غیرقابل دسترس می‌کنند. این امر توسط ارائه‌کنندگان خدماتی که به عنوان[4] عمل می‌کنند و در کشور ما طبق «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» مصوب شورای عالی انقلاب فرهنگی با عنوان

[1] دلفانی، علی اشرف، مبانی مسئولیت کیفری در حقوق اسلام فرانسه، انتشارات مؤسسه بوستان کتاب قم، چاپ اول، ۱۳۸۲.ص۵۰

[2] (Filtering)

[3] Sex Child یا Child Porn

[4] Back Bone

ایجادکنندگان نقطه تماس بین‌المللی شناخته می‌شوند بسیار راحت‌تر و هماهنگ‌تر صورت خواهد گرفت. در ماده ۶ از قسمت «الف» مصوبه مذکور آمده است: «کلیه ایجادکنندگان نقطه تماس بین‌المللی (از جمله شرکت مخابرات ایران) موظف می‌باشند تا امکانات فنی لازم در حفاظت و کنترل متمرکز از شبکه‌های مزبور، به شرح ذیل را فراهم آورند:

الف) سیستم پالایش مناسب به منظور ممانعت از دسترسی به پایگاه‌های ممنوع اخلاقی و سیاسی و حذف ورودی‌های[1] غیرمطلوب. تعیین ضوابط پالایش توسط کمیسیون راهبردی شورای عالی اطلاع‌رسانی صورت خواهد گرفت...».

بند «د» از مصوبه نیز مذکور ظاهرا برای جلوگیری از اقداماتی است که برای گذر از فیلتر توسط کاربران جهت دسترسی به وبگاه‌های مسدود شده به عمل می‌آید. در ماده ۵ از قسمت «ب» مصوبه مذکور نیز همین تکلیف عینا برای رساها آمده است: «۵-۳- شرکت رسا[2] دارای مسئولیت قانونی بوده و نسبت به کلیه ضوابط و تعهدات زیر پاسخ‌گو می‌باشد:

امکان و اعمال برقراری پالایه[3] در شبکه رسا (ISP) باید فراهم باشد. ضوابط و مصادیق موارد پالایش توسط شورای عالی اطلاع‌رسانی تصویب و اعلام می‌شود.

مسئولیت رسا در مورد دسترسی به اطلاعات عرضه شده توسط دیگران محدود به ایجاد امکان و اعمال برقراری پالایه در شبکه خواهد بود...». البته به نظر می‌رسد با تصویب قانون جرایم رایانه‌ای کمیته تعیین مصادیق عملاً عهده‌دار وظیفه کمیسیون راهبردی شورای عالی اطلاع‌رسانی شده باشد.

علاوه بر روش پالایشی که به ترتیب فوق صورت می‌گیرد، در برخی کشورها ارائه-کنندگان خدمات موظف به سد کردن و غیرقابل دسترس کردن اطلاعاتی نیز شده‌اند که

[1] (Port)
[2] (ISP)
[3] (Filter)

براساس دستور مقامات قانونی و به طور خاص به آنان اعلام می‌شود. باید دانست در برخی کشورها هیأتی تشخیص محتویات و وبگاه‌های مجرمانه را بر عهده داشته و با اعلام چنین گروهی باید داده محتوای مزبور غیرقابل دسترس گردد. در این راستا در کشور استرالیا چنین بود و در کشور ما نیز قبلا براساس مصوبه‌ای از شورای عالی انقلاب فرهنگی که در راستای فراز ۳ از بند ۳ ماده ۵ قسمت «ب» مصوبه مقررات و ضوابط شبکه‌های اطلاع-رسانی رایانه‌ای تصویب شده بود، مصادیق و ضوابط پالایش اطلاعات توسط کمیته‌ای مرکب از نمایندگان صدا و سیما، و وزارت‌خانه‌های ارشاد و اطلاعات صورت می‌گرفت که اکنون کمیته تعیین مصادیق ماده ۲۱ قانون جرایم رایانه‌ای جایگزین آن شده است. براساس ماده ۲۱ مزبور در مورد اطلاعات مجرمانه‌ای که ضرر آن جنبه عمومی دارد هم کمیته تعیین مصادیق و هم مقام قضایی به شرحی که قبلاً آمد می‌توانند دستور پالایش بدهند. اما در مورد پالایش براساس روبوت‌های پالایشگر هم این قانون ضوابط فنی کمیته تعیین مصادیق را مجری دانسته است.

با این حال نمی‌توان رویه‌ای مانند پالایش خودکار اطلاعات را در خصوص غیرقابل دسترس کردن آن دسته از اطلاعات غیرقانونی که سبب ضرر شخصی می‌گردند به کار برد؛ برای مثال، ممکن است اطلاعاتی مربوط به زندگی خصوصی یک فرد، اطلاعاتی متضمن توهین یا افتراء به یک شخص یا نسخه‌هایی از یک نرم‌افزار یا اطلاعات یک کتاب به صورت غیرقانونی در سایتی که محل میزبانی اطلاعات آن در خارج از کشور قرار دارد، نهاده شود به‌طوری‌که برای همگان قابل دسترس باشد. مسلما این امر نقض مستقیم حقوق اشخاص نظیر حریم خصوصی یا مالکیت فکری صاحبان آن‌هاست.[1]

[1] بردبار، محمد حسن، درآمدی بر حقوق ارتباط جمعی، انتشارات ققنوس، چاپ اول، ۱۳۸۱.ص۱۰۳

در این موارد که میزبان آن اطلاعات ارائه‌کننده خدماتی است که در خارج از کشور قرار دارد و نمی‌توان درخواست حذف یا غیرقابل دسترس کردن آن اطلاعات را از وی نمود یا این‌که ارائه‌کننده خدمات میزبانی اطلاعات مزبور را به هر دلیلی غیرقابل دسترس نمی‌نماید، ممکن است شخص خواستار آن شود که اطلاعات مزبور حداقل برای کاربران در داخل کشور غیرقابل دسترس گردد. امکان غیرقابل دسترس کردن چنین اطلاعاتی بهتر است از طریق ارائه‌کنندگان خدمات اینترنتی که به عنوان Bone Bake عمل می‌کنند صورت گیرد؛ علت این امر نیز آن است که سایر ارائه‌کنندگان خدمات اینترنتی اطلاعات را از آن‌ها دریافت و به کاربران منتقل می‌سازند و لذا غیر قابل دسترس کردن آن اطلاعات از طریق آن‌ها که مبادی ورود اطلاعات به کشور هستند بسیار راحت‌تر و هماهنگ‌تر خواهد بود. تبصره ۲ ماده ۲۱ قانون جرایم رایانه‌ای غیرقابل دسترس کردن این اطلاعات را با دستور مقام قضائی ممکن دانسته است.[۱]

بند دوم: پالایش محتویات مجرمانه در خدمات میزبانی

در مورد داده محتوای مجرمانه دارای جنبه عمومی، چنانچه پیش از این مورد اشاره قرار گرفت، ارائه‌کنندگان خدمات میزبانی به لحاظ حجم بسیار زیاد اطلاعاتی که میزبانی آن‌ها را ارائه می‌کنند، تکلیفی در بررسی و بازبینی فیزیکی آن اطلاعات ندارند و علی‌الاصول این کار از توان آن‌ها خارج است. لذا صرفا باید به محض اطلاع از اینکه اطلاعاتی غیرقانونی در فضای واگذار شده توسط آن‌ها ذخیره شده است، نسبت به غیرقابل دسترس کردن آن اطلاعات اقدام نمایند. غیرقابل دسترس کردن این اطلاعات رأساً و با تشخیص خود ارائه‌کنندگان خدمات در مواردی که اطلاعات «آشکارا» غیرقانونی است، نظیر اطلاعات متضمن هرزه‌نگاری کودکان، ایرادی ندارد. با این حال در بسیاری موارد غیرقابل

[۱] 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.ص۵۰

دسترس کردن دائم اطلاعات نباید رأساً و به تشخیص خود ارائه‌کنندگان خدمات میزبانی صورت گیرد، چه، ارائه‌کنندگان خدمات اساساً صلاحیتی برای تشخیص اطلاعات و داده محتوای مجرمانه ندارند. جریان آزاد اطلاعات و حق افراد در نشر و دسترسی به اطلاعات که از جمله‌ی حقوق بشر است و عدم صلاحیت ارائه‌کنندگان خدمات میزبانی در تصمیم-گیری نسبت به قانونی یا غیرقانونی بودن اطلاعاتی که واقعاً مشخص نیست چنین است یا نه، ایجاب می‌کند که با در نظر گرفتن حق مسلم افراد در نشر اطلاعات، غیر قابل دسترس کردن اطلاعات در فضای واگذار شده توسط آنان صرفاً با دستور مقام قضایی صورت می-گیرد. ماده ۲۳ قانون جرایم یارانه‌ای در این مورد هم تشخیص کمیته تعیین مصادیق یا مقام قضایی را لازم‌الاتباع دانسته و تکلیفی برای ارائه‌کنندگان خدمات میزبانی در نظر نگرفته است، لکن در تبصره بیان داشته که اگر ارائه‌کننده خدمات به مطالب مجرمان‌های برخورد نماید باید آن را به کمیته تعیین مصادیق اطلاع دهد. بدیهی است که دستور دائم برای حذف اطلاعات، در صورتی‌که ضرر اطلاعات غیرقانونی مورد ادعا صرفاً جنبه شخصی دارد (نظیر اطلاعات متضمن توهین به افراد) باید با طرح دعوی و اثبات غیرقانونی بودن اطلاعات توسط مدعی صورت گیرد. ماده ۲۳ قانون جرایم یارانه‌ای برخلاف خدمات دسترسی در مورد این‌گونه اطلاعات در خدمات میزبانی ساکت است، لکن این سکوت دلیل آن نیست که کمیته تعیین مصادیق یا مقام قضایی رأساً بتوانند دستور غیرقابل دسترس نمودن چنین اطلاعاتی را بدهند.

بند سوم :حدود مسئولیت کیفری ارائه‌کنندگان خدمات در صورت عدم پالایش اطلاعات غیرقانونی

جریان آزاد اطلاعات که پیش از روند رو به رشد اطلاعاتی شدن جوامع از اهمیت چندانی برخوردار نبود، با گسترش و توسعه ابزارهای ارتباطی و اطلاعی و سیر جوامع برای تبدیل شدن به جوامع اطلاعاتی اهمیت فوق‌العاده‌ای یافته است و اینترنت به عنوان بزرگ-

ترین فضای مجازی و اطلاعاتی نقش عمده‌ای در این فرآیند دارد. از این رو آزادی در نشر و دسترسی به اطلاعات که به عنوان یکی از اساسی‌ترین حقوق انسانی در اسناد بین-المللی راجع به حقوق بشر مورد اشاره قرار گرفته، در این جوامع اهمیت بسیاری یافته که جز در موارد مصرح قانونی هیچ کس نمی‌تواند آن را محدود سازد. ارائه‌کنندگان خدمات اینترنتی در مسیر ارائه و نشر اطلاعات در اینترنت قرار گرفته‌اند و از این رو هر گونه تحدید در آزادی نشر و دسترسی به اطلاعات توسط آنان‌که برخلاف قانون صورت گیرد، حقوق اساسی کاربران را نقض کرده است به طوری که حتی می‌تواند موجبات مسئولیت آن‌ها را فراهم نماید.

با این حال چنانچه می‌دانید فضای سایبر و خصوصاً اینترنت در عین حال که سرشار از اطلاعاتی مفید است، دربردارنده اطلاعات غیرقانونی نیز هست که روزانه در سطح جهانی و با سرعت و گستردگی بسیار پخش می‌شوند و بعضاً تأثیرات بسیار مخربی بر روی کاربران و خصوصا کاربران کودک دارند. قسمتی دیگر از این اطلاعات نیز حقوق شخصی اشخاص را مورد تعرض قرار می‌دهد.[1]

ارائه‌کنندگان خدمات اینترنتی یا در مسیر گذار این اطلاعات واقع‌اند و خدمات دسترسی به اطلاعات را فراهم می‌آورند یا این‌که خود فضای ذخیره چنین اطلاعاتی را فراهم می-سازد و خدمات میزبانی اطلاعات را ارئه می‌کنند. از این‌رو هیچ کس نمی‌تواند بهتر از خود آنان در کنترل اطلاعات غیرقانونی تأثیرگذار باشد. پیش از این اشاره شد که ارائه‌کنندگان خدمات اینترنتی در خدمات دسترسی و در برابر اطلاعات غیرقانونی ارائه شده توسط غیر در سطح اینترنت مسئولیتی ندارند، مگردر موارد خاص که پیش‌تر بیان گردید؛ اما باید

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

توجه داشت که نمی توان به نقش کنترل‌کننده و پیش‌گیرنده آنان درپخش واطلاعات غیر قانونی بی‌توجه بود.ازاین رو اگرتکلیف ومسئولیتی برای ارائه کنندگان خدمات دسترسی متصور است، نه اساساً درارائه اطلاعات غیر قانونی توسط غیر،که درصورت بی توجهی وبی مبالاتی آنان در کنترل و غیر قابل دسترس کردن این اطلاعات است. کنترل اطلاعات غیرقانونی نظیر هرزه‌نگاری کودکآنکه تاثیرات منفی و مضر درسطح کلی کاربران و علی الخصوص کاربران کودک دارد، ازطریق راهکارهایی فنی نظیر پالایش اطلاعات مقدور است. [1]

دراین‌باره توجه به چند نکته ضروری است: اولاً اینکه تعیین نرم افزار پالایش‌گر باید به شکلی استاندارد توسط صنعت مربوطه (نظام صنفی) معین و مشخص گردد؛ به عبارت دیگر چنین نباشد که روش‌ها و ابزار پالایش به صورت سلیقه‌ای انتخاب گردد تا بتوان ازاختلاف عملکرد ارائه کنندگان خدمات مختلف جلوگیری شود. اکنون در ایران براساس قانون جرایم رایانه‌ای این تکلیف در مورد داده محتوای مجرمانه برعهده کمیته تعیین مصادیق است. ثانیاً به کاربران و مشترکین این حق داده شود که در صورتی‌که وبگاهی اشتباهاً پالایش گردد بتوانند به ارائه کننده خدمات اطلاع داده و رفع ممنوعیت دسترسی به آن را بخواهند. این امکان اطلاع رسانی باید از طریق ارائه‌کنندگان خدمات به کاربران و مشترکین و از طریق ابزاری چون شماره تماس یا آدرس پست الکترونیکی ارائه‌کننده خدمات میسر گردد. این امر به این خاطر است که در بسیاری از موارد حقوق کاربران و مشترکین در دسترسی به اطلاعات یا در دسترس گذاردن اطلاعات خود به علت پالایش اشتباه اطلاعات، خصوصاً آن‌گاه که پالایش توسط ربوت‌های جست‌وجوگر که فاقد

[1] انصاری، باقر و سایر نویسندگان، مسئولیت مدنی رسانه¬های همگانی، انتشارات معاونین پژوهش، تدوین و تنقیح قوانین و مقررات، چاپ اول، تابستان ۱۳۸۱.ص۸۹

قدرت تشخیص هستند صورت می‌گیرد، مورد تضییع قرار می‌گیرد. در کشور ما اکنون کمیته تعیین مصادیق مرجع اعتراض در مورد پالایش است، اما به نظر می‌رسد که این کمیته در مورد دستور مقام قضائی که ولو به اشتباه داده محتوایی را غیرقابل دسترس نموده بتواند دستور رفع عدم دسترسی را صادر نماید ثالثاً باید توجه داشت که هیچ یک از نرم-افزارهای پالایش اطلاعات نمی‌تواند به طور کامل چنین اطلاعاتی را پالایش کند؛ پالایش اطلاعات توسط رایانه‌ها صورت می‌گیرد و هیچ کس انتظار ندارد که کاری که یک ماشین انجام می‌دهد با دقت‌نظر کامل و عاری از خطا باشد. این انتظار هم از آنان نمی‌رود که به محض اینکه نرم افزار جدیدی برای پالایش اطلاعات به بازار آمد، فورا با پرداخت هزینه‌ای گزاف توسط آنان خریداری و مورد استفاده قرار گیرد تا اینکه کوچک‌ترین محتوای خلاف قانونی به کاربران منتقل نشود. از این‌رو اگر ارائه‌کنندگان خدمات اینترنتی به صورت متعارف و به طبق ضوابط فنی اعلام شده اقدام به پالایش چنین اطلاعاتی کنند، به‌طوری‌که درعرف خاص آن حرفه تقصیری از این جهت متوجه آن‌ها نباشد مسئولیتی نخواهند داشت. [1]

بخش پنجم:مسئولیت کیفری کاربران در قبال داده محتوای مجرمانه

کاربر عنوانی کلی برای هر کسی است که به نحوی از فضای سایبر استفاده می‌کند. این طبقه هیچ‌گونه محدودیتی همچون سن یا جنس نداشته و هر کسی که از سیستم رایانه‌ای و فضای سایبر استفاده کند کاربر محسوب خواهد شد. با این همه کاربر با مشترک یا گیرندگان خدمات متفاوت است؛ گیرندگان خدمات علاوه بر کاربرانی که از خدمات دسترسی یک ارائه‌کننده خدمات بهره می‌گیرند، می‌توانند گیرندگان خدمات میزبانی نیز

[1] تننباوم، آندرو اس، شبکه¬های کامپیوتری، ترجمه عین¬الله جعفرنژاد قمی، انتشارات علوم رایانه، چاپ سوم، پاییز ۱۳۸۳.ص۶۸

باشند. در چنین مواردی معمولاً قراردادی بین خدمات مشترکین میزبانی و دسترسی با رائه-کنندگان خدمات منعقد می‌گردد.بنابراین مشترکین خدمات اینترنتی حسب خدماتی که دریافت می‌کنند می‌توانند مشترکین خدمات دسترسی (دریافت داده محتوا، اطلاعات یا سایر خدمات نظیر خدمات پیوند، خدمات گپ اینترنتی یا IRC و نظایر آن) یا مشترکین خدمات میزبانی (ذخیره اطلاعات) باشند. مشترکین خدمات دسترسی در دیدگاهی کلی در قالب تعریف کاربران قرار می‌گیرند و در واقع رابطه بین این دو عموم و خصوص مطلق است. معذلک مشترکین خدمات میزبانی غالباً با کاربران شبکه معنای متفاوتی دارند که مسئولیت‌های آنان ذیلاً در مبحث مربوط به مشترکین خدمات میزبانی مورد بررسی قرار گرفته است. منظور ما در این قسمت از کاربران صرفاً مشترکین خدمات دسترسی نیست و مراد کلیه کاربران می‌باشد.[1]

مسئولیت کاربران آنگاه که خود داده محتوایی مجرمانه را به دیگران ارائه می‌کنند امری بدیهی و فارغ از هر گونه توضیح است. یک کاربر ممکن است مرتکب اعمال مجرمانه بسیاری گردد؛ تصاویر مستهجن در اختیار دیگران قرار دهد، به دیگران افتراء بزند، محتویات کذب منتشر کند، به دیگران توهین کند، وارد حریم خصوصی اطلاعاتی دیگران شود، داده‌ها و اطلاعات رایانه‌ای را جعل کند، مرتکب کلاهبرداری و تقلب مالی شود، پیام‌های ناخواسته ارسال کند، داده‌ها و سیستم‌های رایانه‌ای دیگران را با اختلال مواجه سازد و به‌طور کلی مرتکب بیشماری از این‌گونه اقدامات غیرقانونی گردد. بدیهی است که چنین شخصی یک بزهکار رایانه‌ای است و باید در قبال اقدامات خود پاسخ‌گو باشد.

[1]. در اکثر کشورها، ارائه‌کنندگان خدمات دسترسی طی انعقاد قراردادی به گیرندگان این‌گونه خدمات چنین خدماتی را ارئه می‌دهند. معذلک در کشور ما در زمینه خدمات دسترسی معمولا با کاربران قراردادی منعقد نمی-شود؛ ارائه خدمات دسترسی در کشور ما از طریق فروش کارت‌هایی که به کارت اینترنت معروف است و حاوی نام کاربر و یک گذر واژه است صورت می‌گیرد.

اما از بعد ارائه محتوای مجرمانه که هر گونه متن، پیام، تصویر، فیلم، انیمیشن (پویا نمایی)، صوت و موسیقی را در بر می‌گیرد یک نکته قابل تدقیق است؛ چنانچه پیشتر ذکر گردید فضای سایبر یک فضای منفعل است، یعنی برخلاف آنچه که در رسانه‌هایی نظیر تلویزیون می‌بینیم، غالباً اطلاعات و مطالب به محض روشن کردن دستگاه رایانه به دست کاربران نمی‌رسد، بلکه تا درخواست خود شخص وجود نداشته باشد این اطلاعات به وی منتقل نخواهد شد. از این نظر چنانچه پیش‌تر نیز بیان شد معمولاً داده‌ی محتوایی رایانه‌ای و همچنین خدماتی که در فضای سایبرارائه می‌شود بدون درخواست شخص قابل ارائه نیست و در واقع داده محتوا و خدمات در این فضا بر مبنای «مطالبه»[1] اشخاص ارائه می گردد. لذا شاید بهترین عنوان درخصوص ارائه داده محتوا در فضای سایبر«قابل دسترس ساختن»[2] داده محتوا باشد، بدین معنا که اطلاعات توسط اشخاص مختلف در این فضا قابل دسترس می‌گردد لکن دسترسی کاربر به آن اطلاعات تنها در صورتی است که خود کاربر تحصیل آن اطلاعات را بخواهد. کاربر نشانی وبگاهی که داده محتوای موجود در آن ذخیره شده است را از طریق وارد کردن آدرس URL در جستجوگر[3] مورد نظر همچون Internet Explorer یا Aol درخواست می‌کند، یا ممکن است از طریق موتورهای جستجوگر به جستجو پرداخته و با وارد شدن در پیوندهای ارائه شده توسط موتور جستجو که به صورت پیوند ارائه می‌گردد به این داده محتوا دسترسی یابد. در هر صورت منظور این است که غالباً داده محتوا یا خدماتی که کاربر دریافت می‌دارد جز با خواست خود او ارائه نمی‌شود. لذا ابتدایی‌ترین سؤالی که در این خصوص مطرح می‌شود آن است که با وجودی که اشخاص ارائه‌کننده داده محتوا صرفاً داده محتوا را قابل دسترس می‌سازند و غالباً نقشی در

[1] . Available on Demand

[2] . Making Available

[3] . Browser

ارائه و نشر آن اطلاعات ندارند و این اطلاعات با خواست خود کاربران در اختیارشان قرار می‌گیرد آیا مسئولیتی متوجه ارائه‌کنندگان محتوا خواهد بود؟

پاسخ به این سؤال روشن است؛ در واقع این درست است که داده محتوای غیرقانونی ارائه شده توسط یک کاربر نظیر محتوای مستهجن بدون درخواست کاربران دیگر به آن‌ها منتقل نمی‌شود و در این فرآیند خواست و فعل کاربران نهایی[1] نیز مشارکت دارد لکن این امر نمی‌تواند علت توجیه‌کننده‌ای برای کسانی باشد که صاحب این اطلاعات را قابل دسترس ساخته‌اند. برای مثال مشترک خدمات میزبانی که صاحب وبگاهی است و تصاویر مستهجن کودکان رابرای مشاهده و حتی ذخیره کاربران توزیع می‌کند نمی‌تواند با توسل به این توجیه که وی فقط اطلاعات را در دسترس کاربران گذاشته و در ارائه ونشرآن اطلاعات نقشی نداشته است از خود رفع مسئولیت نماید. اقدام چنین شخصی همانند کسی است که اسلحه‌ای را در دسترس دیگری قرار می‌دهد تا وی مرتکب قتل شود و با توسل به اینکه در تحقق قتل نقشی نداشته از خود رفع مسئولیت می‌نماید؛ یا این‌که همچون ناشر روزنامه‌ای است که اطلاعاتی مجرمانه را منتشر می‌کند و با این عذر که خوانندگان خود روزنامه را خریداری و مطالعه کرده‌اند از یر بار مسئولیت شانه خالی می‌کند.[2]

مسئولیت ارائه‌کننده محتوا در این خصوص به دو علت است: اول اینکه چنین شخصی ابتدائاً و بالذات قصد دسترسی سایر کاربران را به این اطلاعات داشته است. ثانیا درخواست مشاهده این‌گونه اطلاعات توسط سایر کاربران نهایی و در معنای دیگر «فعل» کاربران نهایی موجب انقطاع رابطه سببیت یا حداقل شرطیّت بین فعل صاحب وبگاه با نتیجه حاصله

[1] . End Users

[2] 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.ص۵۸

که همانا دسترسی دیگران به این اطلاعات است نمی‌گردد، چه براساس رابطه علی و معلولی تا این اطلاعات توسط او قابل دسترسی نمی‌گردید توسط کاربران دیگر مورد مشاهده قرار نمی‌گرفت. با این حال باید توجه داشت که بسیاری از قوانین کشورهای مختلف علاوه بر ارائه‌کنندگان محتوا، کاربران را در صورت ذخیره و در اختیار داشتن برخی اطلاعات چنین مسؤل می‌شناسند. برای مثال حتی در اختیار داشتن داده محتوای مستهجن کودکان در سیستم‌های یارانه‌ای کاربران موجبات مسئولیت آنان را فراهم خواهد آورد.

از این موضوع گذشته و به بحث اصلی خویش که بازمی‌گردیم سؤال اساسی دیگری که مطرح می‌شود این است که آیا کاربران و مشترکین تکلیفی در قبال پیشگیری از اشاعه داده شده محتوای غیرقانونی دارند؟ به عبارت دیگر آیا می‌توان آنان را برای جلوگیری از اشاعه این‌گونه اطلاعات مکلف و در صورت عدم پیش‌گیری مسئول دانست؟

غالب حقوق‌دانان در این مورد موافق مسئولیت کاربران نیستند و در این باره دلایلی را ارئه داده‌اند؛ اولاً این‌که تمامی داده محتوا و اطلاعات مجرمانه دارای جنبه عمومی نیستند. برای مثال داده محتوایی که متضمن توهین یا افتراء به دیگری است جنبه خصوصی دارد و نمی‌توان هیچ‌گونه مسرولیتی را برای نهایی که صرفاً چنین اطلاعاتی را مشاهده می‌کنند تصور کرد. ثانیاً در مورد داده محتوایی همچون تصاویر مستهجن کودکان که حیثیت عمومی جرم از اشاعه آن‌ها ناشی می‌گردد، نیز می‌توان چنین مسئولیتی را برای آنان قائل شد، چه، کاربران هیچ‌گونه کنترلی برای این‌گونه اطلاعات ندارند و در برابر این گونه داده محتوا صرفا یک ناظر محسوب می‌شوند. به عبارت دیگر این‌گونه اطلاعات بدون هر گونه دخالت آنان در شبکه ارائه می‌شوند و قدرت کنترلی بر پالایش این‌گونه اطلاعات ندارند؛

لذا مسئولیت آنآنکه هیچ‌گونه حق و توانایی نظارت و کنترلی بر این اطلاعات ندارند از دیدگاه مسئولیت عاریتی قابل تصور نیست.[1]

از منظر مسئولیت مشارکتی هم حتی مقرر نمودن تکلیفی چون اطلاع دادن به مقامات قانونی به هنگام مشاهده اطلاعات و اقدامات خلاف قانون در مورد کاربران نهایی به همین دلیل نه عملا امکان‌پذیر است و نه اینکه منصفانه است؛ امکان‌پذیر نیست چرا که معمولاً اثبات اینکه کاربری از اطلاعات یا اقدامات غیرقانونی آگاه بوده است غالباً دشوار است و حتی در صورت اثبات آگاهی از این امر غالباً با نقض حریم خصوصی اطلاعاتی اشخاص در تعارض قرار می‌گیرد، چرا که هیچ‌کس با چنین دلایلی نمی‌تواند اطلاعات مربوط به مشاهده اطلاعات توسط دیگران را پویش و تعقیب کند؛ و منصفانه نخواهد بود چرا که تبدیل تکلیفی اخلاقی به تکلیفی حقوقی نیازمند آن‌چنان درجه‌ای از قوت است که وضع چنین تکلیفی را بر دوش کاربران نهایی توجیه کند و اقناع حقوقی لازم را برانگیزد. صرف‌نظر از این‌که چنین اقناعی حاصل نمی‌گردد، اعمال تکلیفی چنین بر دوش کاربران ناقض آزادی و حقوق شهروندی آنان است.[2]

با این همه در مورد داده محتوای غیرقانونی، عده‌ای از حقوق‌دانان اشخاصی را که تکلیف محافظت از کاربران را برعهده دارند مسئول می‌دانند؛ برای مثال عده‌ای والدین یا مسئولان دانشگاه‌ها را در قبال داده محتوایی که کاربران کودک براثر بی‌مبالاتی آن‌ها، همچون قرار ندادن گذر واژه یا سیستم پالایش مناسب، به آن دسترسی می‌یابند مسئول

[1] تننباوم، آندرو اس، شبکه‌های کامپیوتری، ترجمه عین‌الله جعفرنژاد قمی، انتشارات علوم رایانه، چاپ سوم، پاییز ۱۳۸۳.ص۱۳۲

[2] 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.ص۶۰

می‌دانند. در این‌باره اگر مسئولیتی متوجه پدر و مادر یا مسئولان آموزشگاه‌ها نیز که باشد، باید توجه داشت که چنین مسئولیتی در چهارچوب مسئولیت کاربران قرار نمی‌گیرد چرا که در اینجا این کودک است که کاربر است و ممکن است والدین یا مسئولان خود کاربر نباشند. بنابراین بررسی مسئولیت والدین و مسئولان آموزشگاه‌ها در چهارچوب کلی مسئولیت اشخاص ثالث در قبال رفتار دیگری (عاریتی یا مشارکتی) مورد بررسی قرار می‌گیرد و از حوزه مسئولیت کاربران در قبال داده محتوای مجرمانه خارج است، مگر این‌که والدین یا مسئولان آموزشگاه‌ها را نیز کاربر در معنای کلی آن بدانیم. علاوه بر این، هر چند در برخی کشورها آموزشگاه‌ها مکلف به بکارگیری نرم‌افزارهای پالایش محتویات مستهجن شده‌اند، لکن در مورد تکلیف والدین به چنین اقدامی اتفاق نظر وجود ندارد. [1]

نتیجه‌گیری

در پایان این مقاله باید گفت در سیاست‌های جنایی جوامع کنونی، مسئولیت کیفری اعتباری باید به عنوان یک «بعد ضروری» و به عنوان آخرین راهکار مورد توجه و اعمال قرار گیرد. در مسئولیت ارائه‌کنندگان خدمات، حتی در موارد اندکی که مسئولیت آنان مورد پذیرش قرار گرفته است، یک مسئله را نباید فراموش کرد و آن این‌که این اطلاعات» توسط دیگران» منتشر یا ذخیره شده است و از این‌رو برای مسئول دانستن ارائه‌کنندگان خدمات در برابر فعل «دیگری» باید با کمال حزم و احتیاط حقوقی رفتار و منصفانه و با انعطاف فراوان تصمیم‌گیری نمود. معیارهایی که در قوانین برخی کشورها چون قانون کپی‌رایت هزاره دیجیتال ایالات متحده یا دستورالعمل تجارت الکترونیک شورای اروپا در

[1] شیخ الاسلامی، عباس، جرایم مطبوعاتی، بررسی تطبیقی سیاست جنایی جمهوری اسلامی ایران و انگلستان، انتشارات جهاد دانشگاهی مشهد، چاپ اول، تابستان ۱۳۸۰.ص۹۵

محدود نمودن مسئولیت ارائه‌کنندگان خدمات مورد پذیرش قرار گرفته حاصل فراز و نشیب رویه قضائی آن کشورها در حوزه مسئولیت در فضای سایبر است که به لحاظ برخورداری از یک پشتوانه تجربی باید در مقام عمل مورد توجه قرار گیرد. در کشور ما قانون جرایم رایانه‌ای در مورد ۲۱ تا ۲۳ عملاً عمده تکلیف در حوزه کنترل بر داده محتوا را بر عهده کمیته تعیین مصادیق و در برخی موارد برعهده مقام قضائی نهاده است. در هر صورت ارائه‌کنندگان خدمات بی‌چون و چرا باید از دستور دو مرجع فوق تبعیت کنند و این عدم اطاعت از دستور است که چه عامدانه باشد و چه مبتنی بر سهل‌انگاری، مواجه با کیفرهایی سخت خواهد شد. در این‌که چنین رویه‌ای تا چه حد صحیح است در گرو گذشت زمان و محک خوردن این قانون در مقام تجربه است، با این همه آزادی دسترسی به اطلاعات با چنین رویه‌هایی مورد مخاطره قرار خواهد گرفت. افزون بر این حق دارندگان اطلاعات که خود را محق در نشر اطلاعات می‌بینند از آن جهت که مرجعی قضائی در فضای آزاد و علنی نسبت به قانونی بودن یا نبودن اطلاعات آن‌ها تصمیم نمی-گیرد مورد لطمه قرار خواهد گرفت، چرا که بدون توجه به اصل ۳۷ قانون اساسی مجرمانه بودن رفتار و اطلاعات منتشره در یک دادگاه صالح مورد رسیدگی قرار نگرفته است. بازگشت به اصولی که فوقاً بیان شد و تصویب قانونی جامع در این زمینه با احترام کامل به اصل آزادی بیان و نشر اطلاعات که فضای سایبر دائر مدار آن‌هاست در کنار برقراری یک نظام منصفانه مسئولیت راه برون شد از معظلات پیش روی قانون فوق است. در حوزه امنیت اطلاعات نیز تهیه کدهایی رفتاری توسط صنعت مربوطه و ابلاغ آن‌ها به ارائه-کنندگان خدمات و سپس پیش‌بینی مسئولیت در قانون می‌تواند حمایت مؤثر از اطلاعات و سیستم‌های رایانه‌ای کاربران را تأمین نماید.

منابع و ماخذ

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

۲. افراسیابی، محمد اسماعیل، حقوق جزای عمومی، جلد دوم، انتشارات فردوسی، چاپ اول، ۱۳۷۷.

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

۴. تافلر، الوین، موج سوم، ترجمه شهین‌دخت خوارزمی، نشر سیمرغ با همکاری نشر فاخته، چاپ نهم، تهران، ۱۳۷۳.

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

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

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

۸. دادگران، سیدمحمد، مبانی ارتباطات جمعی، انتشارات فیروزه، چاپ چهارم، سال ۱۳۸۱.

۹. شامبیاتی، هوشنگ، حقوق جزای عمومی، جلد دوم، مؤسسه انتشاراتی ویستار، چاپ سوم، تهران، ۱۳۷۲.

۱۰. شیایزری، کریانگ ساک کیتی، حقوق بین‌المللی کیفری، ترجمه بهنام یوسفیان، محمد اسماعیلی، انتشارات سمت، چاپ اول، ۱۳۸۳.

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، ۱۳۷۴.

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

۱۴. علی‌آبادی، عبدالحسین، حقوق جنایی، جلد اول، چاپ دوم، تهران، انتشارات فردوسی، ۱۳۶۹.

۱۵. کراملیش، کریستین، کتاب آموزشی اینترنت، ترجمه مهرناز آرین، انتشارات تورنگ، چاپ پنجم، ۱۳۸۰.

۱۶. محسنی، مرتضی، دوره حقوق جزای عمومی، جلد ۳، مسئولیت کیفری، انتشارات کتابخانه گنج دانش، چاپ اول، ۱۳۷۶.

۱۷. محسنی، مرتضی، دوره حقوق جزای عمومی، جلد ۱، انتشارات گنج دانش، چاپ سوم، تهران، ۱۳۸۲.

۱۸. محسنی، منوچهر، جامعه شناسی جامعه اطلاعاتی، نشر دیدار، چاپ اول، ۱۳۸۰.

۱۹. میر سعیدی، سید منصور، مسئولیت کیفری، جلد اول، قلمرو و ارکان، انتشارات میزان، چاپ اول، بهار ۱۳۸۳.

۲۰. نوربها، رضا، زمینه حقوق جزای عمومی، نشر دادآفرین و گنج دانش، چاپ ششم، تهران، ۱۳۸۱.

۲۱. وبستر، فرانک، نظریه‌های جامعه اطلاعاتی، ترجمه اسماعیل قدیمی، انتشارات قصیده‌سرا، چاپ دوم، ۱۳۸۳.

۲۲. ولیدی، محمد صالح، مسئولیت کیفری، انتشارات امیرکبیر، تهران، ۱۳۸۹چاپ سوم

۲۳. اچ تی تی پی چگونه کار می‌کند، مجله اینترنت چگونه کار می‌کند، برگزیده مقاله‌های ماهنامه ریزپردازنده، گردآورنده علیرضا محمدی‌فر، چاپ دوم، ۱۳۸۲، انتشارات ریزپردازنده.

ب: مقالات و منابع اینترنتی

i. Brenner, Susan,Toward a Criminal Law for Cyberspace: Distributed Security, University of Dayton School of Law, http://law.bepress.com/expresso/eps 15/

ii. Brenner, Susan, Toward a Criminal Law for Cyberspace, Product Liability and other Issues, http://tlp.law.pitt.edu/articles/BrennerSpring2005a.pdfIssues

iii. Bryant, Rebecca, What kind of Space is Cyberspace?

iv. http://www.mic.ul.ie/stephen/cyberspace.pdf

v. Engle,Eric, Extraterriotorial Corporate Criminal Liability: A Remedy for Human Rights Violations? Pp 10-14