فصلنامه علمی وسایل ارتباط جمعی ـ رسانه Quarterly Journal of Media Scientife Promotional

نوع مقاله: پژوهشی DOI:10.22034/bmsp.2021.272929 http://qjmn.farhang.gov.ir

Vol. 33, No. 1, Spring 2022

راهکار حقوقی تأمین امنیت سایبری

نوشتهٔ

رسول ملکوتی*

مونا خلیل‌زاده**

تاریخ دریافت: ۹۹/۱۱/۲۲

تاریخ پذیرش: ۱٤۰۰/۰٤/۸

چکیده

با توجه به رشد روزافزون نرخ استفاده از فضای سایبر در دنیای کنونی، چه در سطح کلان (امور دولتی و حاکمیتی) و چه در سطح خرد (میان شهروندی)، از مهم‌ترین وظایف قانونگذار در این بستر، تأمین امنیت، اعم از مدنی و کیفری است. بدیهی است که ارتکاب جرم یا هرعملیات متقلبانه مادون آن، در این فضا با رشد فناوری، روزانه دستخوش تغییر می‌شود. گاهی، بین جرم ارتکابی و مجازات تعیین‌شده، تناسبی وجود ندارد، لذا فرد بزهکار، با برآورد دستاورد خود در این فضا و با علم به میزان مجازات تعیین‌شده، اقدام به ارتکاب جرم می‌کند. با توجه به اینکه رفتارهای بزهکارانه در این فضا، علاوه بر اینکه در هر دو سطح، اعم از زیرساخت‌های اساسی دولت و امنیت کاربران، می‌تواند موجب ناامنی شود، و از سوی دیگر، سازوکار متفاوتی از آنچه در قواعد مسئولیت مدنی در فضای واقعی موجود است، برای فضای سایبر از سوی قانونگذار تاکنون تعبیه نشده، به نظر می‌رسد ارئهٔ راهبردی، جهت به‌روزرسانی برخی از مواد قانون جرایم رایانه‌ای، با توجه به مقتضیات روز، بتواند تا حد قابل توجهی امنیت هر چه بیشتر را در فضای سایبر تأمین کند.

کلیدواژه: فضای سایبر، امنیت سایبری، راهبرد حقوقی، جرایم سایبری.

* استادیار گروه حقوق، دانشگاه آزاد اسلامی، واحد پردیس (نویسنده مسئول)، تهران، ایران rasoolmalakooti@yahoo.com

** دکتری حقوق بین الملل، دانشگاه تهران، تهران، ایران mona.kh65yahoo.com

مقدمه

اگر قرن ۲۱، به‌درستی قرن انفجار اطلاعات نامیده شده است، وجه تسمیهٔ این نامگذاری تا حدود زیادی مرهون تشکیل فضای سایبر و به طور اخص، ظهور اینترنت است که با بروز آن، مرزهای جغرافیایی نادیده انگاشته و حاکمیت ملی دولت‌ها، به معنای سنتی در این فضا، بی‌معنی یا حداقل کمرنگ شد. اگرچه جامعهٔ جهانی، تمایلی به اعمال حاکمیت ملی هر کشور بر فضای سایبری در دسترس شهروندان خود نداشت و تلاش‌های جامعهٔ جهانی معطوف به فراملی قلمداد کردن این فضا است (ملکوتی، ۱۳۹۷: ۲٤۰)؛ اما اهمیت تأمین امنیت شهروندان و حاضران این فضا، مورد اجماع همهٔ کشورهای عضو سازمان ملل متحد است؛ در این خصوص از دیرباز، کنوانسیون‌های مختلفی تصویب و به امضا رسیده است.[1] بنابراین، مسلم است که فراملی بودن فضای سایبر و فقدان حاکمیت مرکزی منسجم در آن، منافاتی با همکاری کشورها در سطح بین‌المللی یا اهتمام هر کشور در سطح ملی، برای تأمین امنیت مدنی یا کیفری نخواهد داشت، که شقوق تسهیل جبران زیان وارده یا مجازات مناسب مجرم را در این فضا تأمین کند (ضیایی، ۱۳۹٦: ۲۲۹).

در کشور ما، اگرچه از تصویب قانون جرایم سایبری بیش از یک دهه گذشته است، و تلاش شده حاکمیت در این فضا نیز تثبیت شود، اما حقیقت این است که نه‌تنها قانونگذار در مورد مسائل مدنی منجر به زیان و به بیان دیگر تأمین امنیت مدنی، گام مؤثری بر نداشته، بلکه مجازات‌های تعیین‌شده با هدف تأمین امنیت کیفری نیز، گاهی ناچیز است و هدف مزبور را تأمین نخواهد کرد. در این مقاله، کوشش شده، ضمن معرفی چالش‌های قانونی این موضوع، راهکارهای حقوقی مناسبی برای تأمین امنیت سایبری، با نگاهی به عملکرد برخی سیستم‌های عمدهٔ حقوقی جهان معرفی شود.

مفهوم و اقتضائات فضای سایبر

۱. کنوانسیون جرایم سایبری بوداپست مصوب سال ۲۰۰۱ میلادی.

برای نیل به مقصود فوق لازم است ابتدا مفهوم و اقتضائات فضای سایبر روشن شود:

مفهوم و ماهیت فضای سایبر

فضای سایبر از دو جهت وجود و ماهیت قابل بررسی است. از نظر وجودی (فنی) عبارت است از شبکه‌های عنکبوتی و غیرملموس الکترونیکی که با در هم تنیده شدن، این شبکهٔ سراسری و جهانی را شکل داده‌اند. از نظر فنی، این شبکهٔ جهانی سایبر از خود استقلال ندارد و حاصل در هم تنیده شدن و ادغام بخش‌های مختلف است که درنهایت یک قلمرو نامحدود سایبر را، در فضای خلأ شکل داده است. فضای سایبر را از نظر وجودی می‌توان ظرف نامحدودی دانست که هر کس با دسترسی به آن، امکان وارد کردن یا تخلیهٔ مظروف (محتوا) را درآن دارد؛ بدون اینکه قدر آن اشباع شده یا محدودیتی برای سایرین ایجاد شود (ملکوتی، ۱۳۹۵: ۲۲۷).

اما اینکه ماهیت حقوقی فضای سایبر، با تعریف ارائه‌شده چگونه است، نظریه‌های مختلفی بیان شده:

الف. ماهیت ملی

برخی معتقدند، فضای سایبر در هر کشوری، همانند قلمرو مادی و فیزیکی آن تلقی می‌شود و جزء خاک آن کشور به حساب می‌آید، بنابراین در حاکمیت و کنترل کامل آن کشور است و هرگونه که خواست، می‌تواند برای کنترل آن، اقدام به وضع مقررات کند. یعنی، اگرچه فضای سایبر، قلمروی سراسری در همهٔ نقاط جهان دارد، اما از نظر حاکمیت، در کنترل دولت کشوری است که در آن، مورد استفاده قرار می‌گیرد و از این نظر، تفاوتی با خاک آن کشور ندارد (ملکوتی، ۱۳۹۷: ۲٤۳). به عبارت دیگر، فضای سایبر از نظر وجود و لزوم وضع مقررات در حوزه صلاحیت هر کشور، تفاوتی با جهان واقعی و سایر رسانه‌ها ندارد، وضع مقررات در آن به معنی آزادی همراه با برخی محدودیت‌های ضروری خواهد بود (دریوکس[1]، ۲۰۰۵: ۸).

۱. Derieux

ب. ماهیت غیرملی[1]

به نظر این گروه، ذات فضای سایبر، به گونه‌ای است که ماهیت فراملی دارد و هیچ کشوری نمی‌تواند آن را کنترل و مدیریت کند، ادعای تشابه و محدودیت قلمرو سایبر به مرزهای واقعی یک کشور، قابلیت تحقق و امکان ندارد. بنابراین، دولت‌ها نمی‌توانند و نباید بر فضای سایبر کنترل و نظارتی داشته باشند، چون در اصل، فضای سایبر در قلمرو حاکمیت ایشان شکل نگرفته است (واین[2]، ۲۰۰۳: ۳۲) و جامعهٔ جهانی هم، نمی‌تواند کنترلی بر آن داشته باشد؛ چون نسبت به آن سمتی ندارد. به عبارت دیگر، فضای سایبر منطقه‌الفراغی[3] است که از دسترس حکومت‌های ملی دور است (ملکوتی، ۱۳۹۷: ۱۱۲).

در فضای سایبر، نمی‌توان حکومت را بر اساس قاعدهٔ حاکمیت، شبیه به آنچه در دولت، از جنبهٔ ملی وجود دارد، در نظر گرفت. بنابراین قواعد حاکم بر این فضا، مجموعه‌ای از حاکمیت‌های فراملی و تا حدی ملی است؛ همچنین، قواعد غیرحقوقی شامل کدهای شبه قانونی و هنجارهای اجتماعی شبکه است. با توجه به طراحی خاص و ویژگی‌های این فناوری ارتباطی، مفاهیم سنتی وضع قوانین و مقررات که ظهور در زمان و مکان دارد، نمی‌تواند در آن قابل اجرا باشد. دولت‌ها مجبور هستند، انحصارطلبی سنتی خود را کنار گذاشته و حکمرانی اینترنت را، با توجه به خصوصیات منحصربه‌فرد این فضا بپذیرند و تبعاً روش‌های خود نظام‌دهی، به‌ویژه در زمینهٔ دسترسی به محتوای اینترنت، بیشتر در این فضا حاکم خواهد بود. نتیجه اینکه اگرچه امکان مقررات‌گذاری و اعمال آن وجود دارد، اما هویت

۱. غیرملی به معنی جهانی نیست.

2. Wayne

۳. نظریه‌ای است در فقه شیعه، که از وجود قلمروی فاقد حکم شرعی در دین خبر می‌دهد. این نظریه را، سید محمدباقر صدر در کتاب *اقتصادنا* مطرح کرده است. بر طبق نظریه منطقةالفراغ، دین به حاکم اسلامی اجازه داده است تا در برخی مسائل اجتماعی، با در نظرگرفتن ضوابطی و با توجه به نیازهای هر زمان، حکم و قانون وضع کند (حسینی، ۱۳۸۱: ۹۰) . در اینجا، منظور این است که فضای سایبر از نظر شمول قواعد حاکمیت دولت‌ها، منطقه‌الفراغ است و موضوع احکام دولتی و حاکمیتی قرار نمی‌گیرد.

نهاد مقررات‌گذاری و ابزارهای استفاده در تدوین قوانین و مقررات، مطابق با الگوهای سنتی دولتی نیست (قاجار، ۱۳۸٦: ٦٦).

ج. ماهیت عام جهانی

این گروه معتقدند، اگرچه فضای سایبر در قلمرو حاکمیت دولت و کشور خاصی نیست و هیچ دولتی نمی‌تواند ادعای حاکمیت مطلق بر آن را داشته باشد، اما نهایتاً در حاکمیت جامعهٔ جهانی است و دولت‌ها، به‌اتفاق، صاحب صلاحیت‌اند که در مورد آن تصمیم‌گیری کنند. به عبارت دیگر، فضای سایبر، همچون قلمرو دریاهای آزاد است که اگرچه هیچ کشوری توان وضع قانون و اعمال حاکمیت در خصوص آن را ندارد، اما جامعهٔ جهانی برای انتظام‌بخشی به آن، چاره‌ای جز وضع مقررات از طریق کنوانسیون‌ها و پروتکل‌های مختلف ندارد (ملکوتی، ۱۳۹۷: ۲٤۷). نمایندهٔ یونسکو، در کنگرهٔ بین المللی " اخلاق و اطلاعات" تلویحاً به این نگاه اشاره کرده است، با شناخت نقش مرکزی و راهبردی اطلاعات در همهٔ فعالیت‌های زندگی کنونی ــ ازسیاست تا عملیات بانکی، از آموزش تا مصرف، از عملکرد دولت تا نظام اجتماعی ـ حقوقی تا سازماندهی فرهنگ و هویت ملی ــ به‌زودی ضرورت پدید خواهد آمد تا مذاکرات خاص آن برای یک توافق سیاسی، دربارهٔ اصول بنیادی حقوق اطلاعاتی، آغاز شود. در حالی‌که، مباحثه‌های مربوط به تضمین حقوق بشر و حفظ محیط زیست، برای حساس‌سازی گستردهٔ افکار عمومی نسبت به این مسائل از قرن گذشته تاکنون، همچنان ادامه دارد و پیوسته طرفداران بیشتری پیدا می‌کنند (معتمدنژاد،۱۳۹۰: ٤۸۸).

۲. خصوصیات و اقتضائات فضای سایبر

در این قسمت خصوصیات و اقتضائات فضای سایبر مورد بررسی قرار می‌گیرد.

الف. خصوصیات فضای سایبر

خصوصیت، ویژگی‌های وجودی یک پدیده است که به واسطهٔ این ویژگی‌ها، موجودیت آن پدیده وصف می‌شود. خصوصیات وجودی فضای سایبر عبارت‌اند از:

- **ناملموس بودن**

فضای سایبر، به دلیل اینکه الکترونیکی است، قابل لمس نیست و قلمرویی انتزاعی و شکل‌گرفته در خلأ است؛ به همین علت عنصر زمـــان و مکان، در فضای سایبر مفهوم نـــدارد (ملکوتی، ۱۳۹۷: ۲۷). اصطلاح " فضا" نیز دال بر همین موضوع است، چون " مکان" جایی است که از نظر منطقی طول، عرض و ارتفاع دارد، در حالی‌که فضا فاقد این اوصاف است.

- **دسترسی آسان**

عدم تمرکز[۱] و دسترسی آسان[۲] در هر زمان و مکانی، از جمله ویژگی‌های ذاتی فضای سایبر است (موک‌لر[۳]، ۲۰۰٤: ۱۰). این دسترسی آسان از این جهت قابل توجه است، که در هر شرایطی و در هر مکانی که امکان دسترسی به این فضا مهیا شد، کاربر واردشده، با همهٔ کاربران حاضر در آن، از نظر امکان و نقطه حضور، در شرایط یکسان خواهد بود.

- **قلمرو بی‌نهایت**

چون عنصر زمان و مکان، در فضای سایبر بی‌معنا است و این فضا در نوعی خلأ شکل گرفته، بنابراین در آن، حد و مرزی قابل ترسیم نیست و حضور در فضای سایبر، عرصه را بر دیگران تنگ نمی‌کند، رقابت در این فضا نیز، به معنای مرسوم در جهان واقعی، قابلیت تحقق ندارد.

- **تخصصی بودن فضا**

ورود به فضای سایبر، علاوه بر توانایی‌های عمومی، نوعی تخصص و آشنایی را، ولو اجمالی، با اصطلاح‌ها و ابزارهای نرم‌افزاری مخصوص آن لازم دارد. به عبارت دیگر، جهـان‌شـمولی زبان دیجیتال، منطـق کاملاً شبکه‌ای و همچنین معماری خاصی که موجب دشوار یا غیرممکن شدن سانسور و کنتـرل می‌شود، از ویژگی‌های قابل توجه فضای سایبر به شمار می‌آید (کاستلز، ۱۳۸۲: ٤۰۸).

۱. Decentralization

۲. scalable

3. Muclier

- **تعاملی بودن**

در فضای واقعی رفتارها اغلب جنبهٔ فردی دارد و یک‌طرفه است مانند راه رفتن، خوردن، نوشتن و ... در حالی‌که، در فضای سایبر، اساساً رفتار یک‌جانبه بی‌معنا است و هر کنش و تراکنشی در این فضا، به معنی دادن یا گرفتن اطلاعات " به" یا " از" افراد معلوم یا ناشناس است (عاملی و همکاران، ۱۳۹۱: ۳۸).

- **غیرقابل کنترل بودن**

غیرملموس و بی‌نهایت بودن فضای سایبر، که امکان حضور فیزیکی نیروهای بازدارنده را از بین برده است، موجب شده، این فضا، در مقایسه با فضای واقعی، قابلیت کنترل نداشته باشد و هر کاربر حاضر در این فضا، خود را سلطان بلامنازع آن می‌شمارد. عدم کنترل این فضا، به حدی است که برخی ادعا کرده‌اند، با ورود عصر فناوری اطلاعات و فضای سایبر، حق حریم را باید به فراموشی سپرد (فروم‌کین[1]، ۲۰۰۰: ۵۲) .

- **عدم امکان قلع قطعی اطلاعات**

در دنیای واقعی، عمل زیانبار ماهیت موقتی دارد و با گذشت زمان قابل ترمیم است؛ در حالی‌که در فضای سایبر، هر گونه اطلاعات و محتوای واردشده در آن، امکان قلع قطعی ندارد؛ چون به محض ورود، قابلیت دسترسی را در هر نقطه و برای هر کسی دارد. به طور مثال کلیهٔ اطلاعات در نشانی internetarchive.com آرشیو شده و برای همیشه در دسترس است.

- **وسعت ضرر و عدم امکان مهار واقعی خسارت**

چون زمان و مکان، در فضای سایبر بی‌معنا است و در خلأ شکل گرفته است، زیان حادث در این فضا، از لحاظ ماهیت دارای فزایندگی لحظه‌ای است و به صورت مستمر، با کپی در سایر تارنماها و تخلیه و بارگذاری مجدد در حال تکثیر و افزایش است (ملکوتی، ۱۳۹۷: ۳٤).

1. Froomkin

- **هویت پنهان یا دروغین حاضران فضای سایبر**

غیرملموس بودن فضای سایبر، موجب شده بسیاری از حاضران و کاربران این فضا، با هویت دروغین یا ناشناس در آن فعالیت کنند و همین ناشناسی مقتضی است که اشخاص، به‌راحتی مرتکب رفتارهایی می‌شوند که در فضای واقعی از ارتکاب آن ابا دارند. به این حالت، در اصطلاح روانشناسی، " بازداری زدایی" گفته می‌شود (شجاعی، ۱۳۸۷: ۸٤).

ب. اقتضائات فضای سایبر

منظور از اقتضائات[۱] نتایج و الزام‌هایی است که از ویژگی‌ها و خصوصیات پیش‌گفته ناشی می‌شود. اهم این اقتضائات عبارت‌اند از:

- **رسانه بودن فضای سایبر**

مهم‌ترین اقتضاء ماهیتی فضای سایبر، کارکرد آن به عنوان یک رسانه است. صاحب‌نظران علوم اجتماعی، رسانه را از نظر پایگاه شکل‌گیری و نوع ارائهٔ محتوا به دو دستهٔ رسانه جمعی[۲] و رسانهٔ اجتماعی[۳] تقسیم‌بندی کرده‌اند (افتاده، ۱۳۹۱: ٦۷). رسانهٔ جمعی مانند تلویزیون و مطبوعات، دارای جایگاه اجتماعی یک‌طرفه با مخاطبان خود هستند؛ اما رسانه‌های اجتماعی، در ارتباط با مخاطبان خود، جایگاه دوطرفه و غیرمنفعل دارند. فضای سایبر، نوعی رسانهٔ اجتماعی است که در کنترل مالک خاصی نیست و طیف وسیعی از تفکرات عمومی در آن یافت می‌شود. به گونه‌ای که امکانات رسانه‌های اجتماعی، برای تمام کاربران یکسان است و بحث و گفت‌وگوی دوطرفه میان مخاطبان و بررسی فوری بازخورد[٤] محتوای ارائه‌شده وجود دارد (کی مور، ۱۳۸۳: ۹۳).

از طرف دیگر، فضای سایبر به عنوان رسانهٔ اجتماعی، ماهیتی چندرسانه‌ای دارد. بدین معنا که در قالب معین و تعیین‌شدهٔ قبلی، کارکرد ندارد، بلکه هم‌زمان، قابلیت این را دارد که

۱. مقتضی به حالتی گفته می‌شود که وجود معلول را اقاضه می‌کند. به بیان دیگر، به چیزی گفته می‌شود که علی‌القاعده موجب ایجاد نتیجه در زمینهٔ مورد نظر می‌شود. مثلاً در عالم طبیعت، اگر بذری در خاک نهاده شود (زمینه)، علی‌القاعده مقتضی این است که بذر سبز شود (نتیجه)، مگر اینکه مانعی مانند خرابی حادث شود. در عالم حقوق هم مثلاً مقتضی وقوع بیع این است که مالکیت منتقل و مبیع و ثمن تسلیم و تَسلُّم شود، مگر اینکه مانعی مانند بطلان و ... ایجاد شود. (برای مطالعه بیشتر، ر.ک.به: ملکوتی، ۱۳۹۸: ۱۱۷ به بعد).

۲. mass media

۳. Social Media

۴. Feed back

کارکردهای مختلف و متفاوت یک رسانه را عهده‌دار شود؛ به گونه‌ای که، هم‌زمان می‌توان در فضای سایبر محتوای تصویری، صوتی یا مکتوب مشاهده کرد (جلالی فرهانی، ۱۳۸۸: ٦٨). در عین حال، گسترهٔ آن نیز جهانی است؛ محدود به قلمرو خاص و در مالکیت گروه یا شخص معینی هم نیست و محدودیت‌های مرسوم رسانه‌های سنتی را، مانند معدود بودن تعداد کانال‌ها ندارد (سیمپسون[1]، ۲۰۰۷: ٦١).

اگرچه فضای سایبر، به عنوان رسانه تلقی می‌شود، اما تابع محض اصول و ضوابط حاکم بر رسانه‌ها نخواهد بود. چون رسانه بودن، تنها کارکرد فضای سایبر نیست و این فضا، با همهٔ اشتراکاتی که با ویژگی‌های رسانه دارد، تفاوت‌های اساسی با آن دارد. از جمله اینکه، در اصل در فضای سایبر، بر خلاف سایر رسانه‌ها، اطلاعات به مخاطب ارائه نمی‌شود، بلکه توسط اشخاص و به درخواست خودشان از طریق جست‌وجو[2] یا کلیک[3]، در دسترس آنها قرار می‌گیرد. از این رو، اقدام تولید و عرضه‌کنندگان و اطلاعات، در فضای سایبر را، بر خلاف مطبوعات و سایر رسانه‌ها، نمی‌توان همیشه ارائهٔ[4] اطلاعات دانست؛ بلکه آن‌ها، تنها امکان ارتباط را، برای کاربران و استفاده‌کنندگان فضای سایبر فراهم می‌آورند (افضلی، ۱۳۸۸: ۲۵۳). ایشان خود، اطلاعات مورد نظرشان را تحصیل می‌کنند و در این مورد آزادی عمل دارند (ملکوتی، ۱۳۹۵ : ۱٤۳). از این جهت ممکن است اصطلاح "خود رسانه[5]" یا "شبه رسانه[6] "برای فضای سایبر رساتر باشد.

1. Simpson
2. Search
3. Click
4. Submission
5. Self Medium
۶. Similar Medium

- **گردش آزاد اطلاعات**

اطلاعات یا محتوا[1] در فضای سایبر، به‌مثابهٔ خون در رگ است و به عقیدهٔ برخی، شکل‌گیری فضای سایبر، نتیجهٔ فرایند دایم نوآوری و قابلیت دسترسی آزاد به اطلاعات بوده است (کاستلز، ۱۳۸۲: ٤١٣). فضای سایبر، با وجود اطلاعات یا امکان وجود اطلاعات در آن است که تبلور پیدا می‌کند و بدون آن، فضای سایبر، معنای خود را از دست می‌دهد. اصل گردش آزاد اطلاعات از جمله اصول مهم شهروندی است، که دولت‌ها موظف به رعایت آن هستند. در کشور ما نیز، با تصویب قانون انتشار و دسترسی آزاد به اطلاعات، مصوب ۱۳۸۸، بر این موضوع تأکید شده است و نه‌تنها مؤسسه‌های عمومی و دولتی مکلف به ارائه و انتشار اطلاعات مربوط به خود هستند؛ بلکه به موجب مادهٔ ۸ قانون مزبور، کلیهٔ مؤسسه‌های عمومی و خصوصی، در قبال درخواست اشخاص ثالث که اطلاعات مربوط به آنها است، ملزم به ارائهٔ اطلاعات به ایشان هستند.[2]

بنابراین، با اینکه اصل گردش آزاد اطلاعات در فضای واقعی، یکی از ملاک‌های ارزیابی کیفیت پیشرفت جوامع و رعایت حقوق شهروندی است و دولت‌ها، هر کدام، بسته به نگرش اجتماعی و سیاسی خود، آن را محدود یا مجاز می‌کنند؛ این اصل در فضای سایبر از جمله اصول ذاتی است که رعایت نکردن آن، به معنی نابودی فضای سایبر خواهد بود. ورود[3] و خروج[4] و گردش اطلاعات در فضای سایبر، از طریق جست‌وجو صورت می‌گیرد، از لوازم ذاتی این فضا است به هیچ عنوان، امکان محدود کردن آن از طریق نرم‌افزار یا سخت‌افزار وجود ندارد.

---

۱. بند الف از مادهٔ ۱ قانون انتشار و دسترسی آزاد به اطلاعات، در تعریف آن مقرر می‌دارد: " هر نوع داده که در اسناد مندرج باشد یا به صورت نرم‌افزاری ذخیره گردیده و یا با هر وسیله دیگری ضبط شده باشد" همین‌طور بند الف مادهٔ ۱ از آیین‌نامه ساماندهی و توسعهٔ رسانه‌ها و فعالیت‌های فرهنگی دیجیتال شماره۱۷۲٤۱۲/ت٤۱۲۵۵هـ در تعریف محتوا مقرر می‌دارد: " محتوا مواد دیداری، شنیداری، نوشتاری و یا ترکیبی از آن‌ها در هر شکل و قالب است."

۲. مادهٔ مزبور مقرر می‌دارد: «مؤسسه عمومی یا خصوصی باید به درخواست دسترسی به اطلاعات در سریع‌ترین زمان ممکن پاسخ دهد و در هر صورت مدت زمان پاسخ نمی‌تواند حداکثر بیش از ده روز از زمان دریافت درخواست باشد...»

3. Uploading
4. Downloading

- **آزادی بیان**

اصل آزادی بیان از جمله حقوق اساسی و بنیادین بشری است که در اصول ۱۸ و ۱۹[۱] اعلامیه جهانی حقوق بشر و نیز بند ۲ میثاق بین‌المللی حقوق مدنی و سیاسی[۲] مورد توجه قرار گرفته است. برخی معتقدند آزادی اطلاعات نشئت‌گرفته از اصل آزادی بیان است (معتمدنژاد، ۱۳۹۰: ٤). ولیکن به نظر می‌رسد، میان این دو اصل تفاوت وجود دارد. آزادی بیان، مفهومی اعم از آزادی اطلاعات دارد و آزادی اطلاعات، بیشتر در ارتباط با مراجع عمومی و دولتی مفهوم پیدا می‌کند. به عبارت دیگر، آزادی اطلاعات از حقوق شهروندی و آزادی بیان از حقوق انسانی و مقدم بر آن است. آزادی بیان از این جهت به عنوان اقتضاء ماهوی فضای سایبر اهمیت دارد که این فضا علاوه بر جنبهٔ عمومی، یک کارکرد تخصصی، به عنوان رسانه دارد و اصل مهم حاکم بر هر رسانه‌ای، اصل آزادی بیان است؛ به گونه‌ای که هر اقدام محدود یا کنترل‌کننده در این فضا ممکن است با شائبهٔ یا انتقاد مخالفت با آزادی بیان مواجه شود (شوابا[۳]، ۲۰۰٦ : ۱۹۱).

علاوه بر آن، در اسناد مهم بین‌المللی، به لزوم بسترسازی و حمایت دولت‌ها، برای تحقق اصل آزادی بیان و اطلاعات، در فضای سایبر تأکید شده است. از جمله مصوبهٔ یونسکو که در بخشی از آن مقرر شده برای دموکراتیک کردن روش:

> دسترسی به فناوری‌های اطلاعات و ارتباطات، احتمال موفقیت روشی کند، بی‌نظم و بدون برنامه درست قبلی، نسبت به روشی با حضور جامعهٔ مدنی، رسانه‌ها، دولت و بخش خصوصی که به صورت متحد کار می‌کنند، بسیار کمتر است. یک برنامهٔ منسجم ملی، در زمینهٔ فناوری اطلاعات و ارتباطات، مشارکت فعالان ارتباطات دوربرد و ارائه‌دهندگان خدمات اینترنتی را، برای اجرای آن و تدوین سیاستی در زمینهٔ قیمت‌گذاری،که نیازهای جوامع درحاشیه مانده را در نظر بگیرد، ایجاب می‌کند. چنین برنامه‌ای همچنین سازمان‌های جامعهٔ مدنی را موظف می‌سازد بر محور هدف‌های مشترک بسیج شوند و به توانمندسازی از

---

۱. مادهٔ ۱۹ مقرر می‌دارد: "هر کس حق آزادی عقیده و آزادی بیان دارد و حق مزبور شامل آن است که از داشتن عقیده خود، بیم و اضطرابی نداشته باشد و در کسب اطلاعات و افکار و در اخذ و انتشار آن به تمام وسایل ممکن و بدون ملاحظات مرزی آزاد باشد.))

۲. " هر کس حق آزادی بیان دارد .این حق شامل آزادی تفحص(جست‌وجو) و تحصیل و اشاعه اطلاعات و افکار از هر قبیل بدون توجه به سرحدات، خواه به‌صورت شفاهی یا به‌صورت نوشته یا چاپ یا به صورت هنری یا هر وسیله دیگر به انتخاب خود است."

۳. Schwaba

طریق آموزش حرفه‌ای و حساس کردن مردم کمک کنند. علاوه بر این، ممکن است انجام اصلاحات قضایی یا نهادی الزام باشد تا تنظیم مقررات منسجم برای فناوری اطلاعات و ارتباطات را تضمین کند. همهٔ دست‌اندرکاران باید در ایجاد زیرساختار مناسب شرایط محلی، با هدف تأمین شبکه‌های با هزینه کمتر و طول باند بیشتر برای همه جوامع و به ویژه در حاشیه‌مانده‌ترین جوامع مشارکت داشته باشند.[1]

مفهوم امنیت سایبری

امنیت در لغت، به معنای در امان بودن و مصون بودن از هرگونه ترس و تهدید است (رزونا و همکاران، ۱۳۹۰: ۸۸). پیشرفت در هر عرصه‌ای، حتی در عرصهٔ علمی، ورزشی و فرهنگی، مرهون امنیت است. علاوه بر این تجارت، امور اقتصادی، سرمایه‌گذاری در مناطق مختلف نیز با توجه ویژه به مؤلفهٔ امنیت انجام می‌شود. بدیهی است که در فضای سایبر نیز، اولین مؤلفه‌ای که مورد توجه قرار می‌گیرد، چه در سطح کلان و چه در سطح خرد، بحث امنیت است. در ساده‌ترین شرایط، اولین خواستهٔ افرادی که وارد فضای سایبر می‌شوند، تأمین امنیت داده‌ها و اطلاعات آنها است.

بدون شک، اسلام به عنوان یک نظام حقوقی جامع و مترقی که پاسخگوی نیازهای فردی و اجتماعی افراد در همهٔ زمان‌ها و مکان‌هاست از این قاعده مستثنی نیست. با دقت در متون دینی، احکام و مقررات اسلامی، ملاحظه می‌شود که اهمیت امنیت در همهٔ عرصه‌ها و راه‌حل‌های تحقق بخشیدن به امنیت اجتماعی، در دین اسلام، بیش از سایر نظام‌های حقوقی مورد توجه قرار گرفته است. پیامبر اعظم(ص) می‌فرمایند: «وطنی که امنیت و شادی در آن نیست، خیری در آن نیست» همچنین، امیرالمؤمنین علی(ع) نیز در همین رابطه فرموده‌اند: «لاخیر فی الوطن الامع الأمن و المسره» (ری شهری، ۱۳۸٤: ۸۳) از مفاد این دو حدیث، چنین بر می‌آید که سرور و مسرت، فرع بر امنیت بوده و شادی بدون امنیت بی‌معنی است. علاوه بر اینکه از دیدگاه معصومین، وطنی ارزش و خیر دارد که دارای امنیت باشد، در اصل کشور ناامن، مورد توجه هیچ‌کس قرار نمی‌گیرد و رو به نابودی است. در روایت‌های دیگر منسوب به پیامبر اعظم

۱. شاخص های توسعه رسانه، چارچوبی برای ارزیابی توسعه رسانه ها مورد تایید شورای بین دولتی برنامه بین المللی برای توسعه ارتباطات،۱۳۹۰: ۹۳.

(ص) آمده است: « نعمتان مکفورتان؛ الأمن و العافیه» (ابن‌باویه، ۱۳۷۷: ۷۰)یعنی «سپاس دو نعمت به‌جا آورده نشده و مورد ناسپاسی و ناشکری واقع شده‌اند، امنیت و عافیت.» و حضرت امام سجاد (ع) نیز در دعای مشهور خود فرموده‌اند: «خدایا مرا خوف و ناامنی، ضعیف و ناتوان نکرده تا قدر امنیت را بدانم» (صحیفه سجادیه: دعای بیستم) همچنین، حضرت علی(ع) فرمودند: «نعمت در دنیـــا، امنیت و سلامتـی جسم است و تمـام نعمت در دنیـــا و آخـرت وارد شدن بـــه بهشت است» (ابن‌باویه، ۱۳۷۷: ۳٤). که اهمیت امنیت را بیان می‌کند و اینکه در روایات معصومین (ع) امنیت در کنار سلامتی ذکر شده، بیانگر اهمیت و ضرورت وجود و تأمین آن و تأثیر آن در سایر شئون زندگی بشر است. همهٔ این آیه‌ها و روایت‌ها و موارد مشابه دیگر، بیانگر توجه اسلام به مسئله امنیت است.

فضای سایبر نیز، با توجه به ماهیت خود، فضای تهدیدآمیزی را ایجاد کرده که می‌تواند مخل امنیت افراد تلقی شود. فرصتی که، جهت استفادهٔ حداکثری از فضای سایبر، برای دولت و ملت ایجاد شده، نیاز به امنیت را در تمام سطوح، بیش از گذشته کرده است؛ و می‌بایست این فضا را از رخدادهایی چون بزهکاری و تروریسم سایبری و ... حفاظت کرد (کیان‌خواه، ۱۳۹۸: ۱۷٦). عواملی چون دسترسی آسان، ارزان بودن ورود، عدم امکان شناسایی در فضای عنکبوتی سایبری و ... (خلیل‌زاده، ۱۳۹۲: ٦۷) تأثیر شگرفی را بر گسترش جرایم ارتکابی و درنهایت، تهدید امنیت افراد در این فضا داشته است. بدیهی است که ارئهٔ معیارهای تکنیکی، به‌تنهایی نمی‌تواند برای حفظ امنیت افراد در حوزهٔ سایبر کافی باشد و این فضا، نیازمند یک سازوکار حقوقی و ارائهٔ راهبردهای حقوقی جهت ایجاد امنیت کاربران و صیانت از آنها است (فرهادی، ۱۳۹٦: ۷۲).

مقصود از امنیت سایبری، آن است که کاربران و به طور کلی حاضران در فضای سایبر (فهیمی، ۱۳۸۳: ۷۳) که بیشتر از شهروندان عادی قلمداد می‌شوند، از حضور در این فضا، نخست، احساس امنیت کنند که شقوق این امنیت، جلوه‌های مختلف حفظ داده و اطمینان حداکثری از لو نرفتن یا عدم سرقت را در بر می‌گیرد. دوم؛ مجرمان و مرتکبان افعال زیانبار،

قبل از انجام فعل، بازدهی فعل زیانبار را، در قبال مجازات یا الزام به جبران خسارت وارده، ناچیز بشمارند و جنبهٔ بازدارندگی مقصود قانونگذار از این جهت تأمین شود.

بحث امنیت سایبری، به قدری حائز اهمیت است که دولت بریتانیا، در سال ۲۰۱۶، یک سازمان دولتی تحت عنوان " مرکز ملی امنیت سایبری" تأسیس کرده است. این سازمان، سالانه در گزارشی، تعداد حمله‌های سایبری علیه دولت بریتانیا، تعداد حمله‌های دفع‌شده و چیستی و چگونگی آن و راهکارهای نوین مقابله با این گونه حمله‌ها و افزایش ایمنی در فضای سایبر را ارائه می‌دهد. ایالات متحدهٔ آمریکا نیز، بعد از واقعهٔ یازده سپتامبر که امنیت سایبری خود را مختل دید، بحث امنیت سایبری را برای اولین بار، مورد توجه قرار داد و آن را به بخش خصوصی واگذار کرد (بوش[1] ، ۲۰۰۳: ۱۱۲) که البته در دوران انتخابات جدید ایالات متحدهٔ آمریکا و حمله‌های سایبری رخ داده و تاثیر آن در نتیجه انتخابات ناکارآمدی این بخش ثابت شد (صانعیان، ۱۳۹۸: ۱۸۹).

راهبرد قانونی امنیت سایبری

مقصود از راهبرد قانونی آن است که قانونگذار، در وضعیت فعلی نظام حقوقی کشور، با وضع چه قواعدی در پی تأمین امنیت سایبری بوده است؟ با توجه به اینکه فضای سایبر، فضایی بدون حد و مرز است، بدیهی است که سیاستگذاری در حوزهٔ داخلی، به‌تنهایی در تأمین امنیت راهگشا نخواهد بود؛ بلکه این فضا نیازمند یک سازوکار جهانی و بین‌المللی است. در واقع با پیشرفت فناوری، دولت‌ها نیازمند ایجاد تشکیلاتی هستند، که به صورت منظم و مستمر، با همکاری سایر دولت‌ها، در زمینهٔ قواعد مربوط به فضای سایبر و تأمین امنیت، با توجه به نیاز جامعه، خود را به‌روز کنند (یاسمی‌نژاد، ۱۳۹۰: ۱۱). جرایم سایبری، به قدری پویا هستند که ارائهٔ یک قانون و راهکار ملی، نمی‌تواند برای مدت طولانی کارآمد باشد (خلیل‌زاده، ۱۳۹۳: ٤٣).

1. Bush

برای تأمین امنیت سایبری و ارائهٔ راهبردی مؤثر در این فضا، ابتدا نیازمند جرم‌انگاری هستیم. پراکندگی و تعدد نهادهای موازی پیشگیری از جرایم در فضای سایبر و ناهماهنگی بین نهادهای ذی‌ربط، باعث هدر رفتن امکانات و ظرفیت‌ها و خنثی شدن برخی فعالیت‌ها در این فضا شده است. برای مثال، در حال حاضر نیروی انتظامی، وزارت فناوری اطلاعات و ارتباطات، سپاه پاسداران انقلاب اسلامی، ارائه‌دهندگان خدمات میزبانی و اپراتورهای تلفن همراه، سازمان تنظیم مقررات و ارتباطات رادیویی در این راستا فعالیت دارند (علیوردی‌نیا، ۱۳۹۳: ۵۰).

در مصوبهٔ شورای عالی فضای مجازی، با موضوع توسعهٔ فضای مجازی سالم، مفید و امن که مورخ ۱۳۹٤/۰۱/۳۰ توسط دبیر شورای عالی فضای مجازی ابلاغ شده، فضای سایبر ایمن تعریف شده است. در این مصوبه آمده:

> فضای ایمن فضایی است که متشکل از شبکه‌های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش‌های اسلامی و مقررات کشور ارائه می‌شود و کاربران می‌توانند بر اساس ویژگی‌های جمعیتی از قبیل سن، جنس، شغل و تحصیلات از محتوا و خدمات مورد نیاز بهره‌مند شوند و حتی‌الامکان در برابر محتوا و رفتارهای آسیب‌زا محفوظ بمانند.

البته که این تعریف، به موضوع فضای سایبر سالم و امن پرداخته است، اما به نظر می‌رسد که از نظر محتوایی و با رویکردی اسلامی به آن نگریسته است و تنها به پالایش اطلاعات، با رویکرد اسلامی نظر داشته است.

از آنجا که امنیت، مفهومی چندوجهی دارد، با توجه به مصوبهٔ شورای عالی فضای مجازی با موضوع نظام ملی پیشگیری و مقابله با حوادث فضای مجازی مورخ ۹٦/۰۸/۱۵، نیروی انتظامی جمهوری اسلامی، مسئول رسیدگی به حوادث فضای سایبر است که در حوزهٔ عمومی اتفاق می‌افتد؛ البته این، به معنای نادیده گرفتن فعالیت سایر نهادها در این بستر نیست. بدیهی است، برای ایجاد محیطی امن در فضای سایبر، باید کلیهٔ فعالان این حوزه با یکدیگر مشارکت داشته باشند. باید در نظر داشت که ایجاد امنیت در این فضا، تنها با همکاری بخش خصوصی امکان

پذیر نیست و نیاز به حضور و مشارکت حکومت نیز دارد، در غیر این صورت امنیت، پایداری و تداوم نخواهد داشت (حاجی ده‌آبادی، ۱۳۹۸: ۵۱).

تهدیدهای سایبری، ناقض حریم خصوصی اشخاص حقیقی و حقوقی است و امنیت ملی کشور را تهدید می‌کند. حریم خصوصی فضای سایبر، از جنس اطلاعات است و از طرق مختلف از جمله نفوذ به سیستم رایانه‌ای اشخاص، استفاده از روش‌های فریب، تارنماها و شبکه‌های اجتماعی نقض می‌شود. نقض امنیت داده، موجب مسئولیت کیفری و مدنی است و واسطه‌های الکترونیک در تحقق این نقض، نقش مؤثری دارند. بر این اساس، پیشنهاد می‌شود قوانین و مقررات موضوعهٔ این حوزه از جمله قانون مسئولیت مدنی مصوب ۱۳۳۹، متناسب با تهدیدها و حمله‌های سایبری، بازنگری شود و لوایح مرتبط با حقوق سایبری از جمله لایحهٔ حمایت از اطلاعات و حریم خصوصی افراد در فضای مجازی و لایحهٔ مسئولیت ارائه‌دهندگان خدمات حوزهٔ فناوری اطلاعات در مراحل تصویب قرار گیرد (نعمتی، ۱۳۹۶: ۱۵۷). باید این مهم مورد توجه قرار بگیرد که هرچند مبانی و منابع تحقق مسئولیت مدنی، در دنیای واقعی و فضای سایبر مشترک هستند، نمی‌توان منکر تفاوت‌هایی بین آن‌ها بود؛ بنابراین علاوه بر ضرورت ارئهٔ یک راهبرد عملی، لازم است، مسئولیت مدنی بین واسطه‌ها و گروه‌های فعال در حوزه سایبری تبیین شود تا در هر مورد مشخص شود مسئولیت، چه زمان به صورت مجزا و چه زمانی اشتراکی است و اینکه آیا این مسئولیت، مبتنی بر نظریه تقصیر[1] است یا مسئولیت محض[2] (مبتنی بر نظریهٔ خطر).

در بحث مسئولیت کیفری، در فضای سایبر نیز باید توجه داشت که همزمان با خلق این فضا، جرایمی نیز در آن و یا با استفاده از آن رخ می‌دهد که مبارزهٔ کیفری با این جرایم نیازمند چند گام، جرم‌انگاری و ایجاد و توسعهٔ مسئولیت کیفری است. تعیین مسئولیت کیفری در این

۱. مسئولیت مبتنی بر تقصیر یا فرض تقصیر؛ در این نوع مسئولیت، بار اثبات تقصیر برعهدهٔ زیان‌دیده است. و زیان‌دیده از تمام دلایل می‌تواند برای اثبات تقصیر استفاده کند. در واقع مسئولیت ضمان زیان‌زننده، مشروط به اثبات تقصیر وی از ناحیه زیان‌دیده است.

۲. مسئولیت محض یا بدون تقصیر، مسئولیتی است که به موجب آن شخص موظف به جبران خسارتی است که به دیگری وارد آورده است، بدون آنکه احتیاجی به اثبات تقصیر فاعل زیان باشد.

فضا، به قدری حائز اهمیت بوده که برای نخستین بار در قانون ایران، حتی برای اشخاص حقوقی مرتکب جرم در فضای سایبر نیز، مسئولیت کیفری در نظر گرفته شده است.

برای ارائهٔ یک راهبرد کارآمد، به منظور تحقق مسئولیت کیفری در فضای سایبر، نیاز است که علاوه بر رعایت اصول عمومی جرم‌انگاری، ویژگی‌های منحصربه‌فرد فضای سایبر نیز، مورد توجه قرار گیرد. بنابراین می‌بایست در ارائهٔ این راهبرد، قوانین بین‌المللی و قوانین استاندارد موجود در فناوری اطلاعات، لحاظ شود، ضمن آنکه جرم‌انگاری در پرتو سیاست جنایی مشارکتی که اعمال آن در مورد جرایم سایبری هم ممکن و هم ضروری است، کاستن از بار سنگین عدالت کیفری، به دستیابی به یک قانون کارآمد و راهبردی کمک خواهد کرد (حاجی ده‌آبادی، ۱۳۹۸: ۷۹).

تداخل صلاحیت‌ها در فضای سایبر

یکی از مباحث حقوق کیفری، بحث صلاحیت مراجع رسیدگی به جرم است، که در اصل مبتنی بر محل ارتکاب جرم، محل کشف جرم، محل دستگیری متهم یا محل اقامت متهم است. ضابطهٔ تعیین هر یک از این موارد می‌تواند برای تعیین دادگاه صلاحیت‌دار حایز اهمیت باشد. در فضای سایبر نیز، با توجه به اینکه تعیین محل ارتکاب جرم و کشف متهم بسیار دشوار و در مواقعی غیر ممکن است، تعیین دادگاه صلاحیت‌دار نقش مهم و گاه پیچیده‌ای در این حوزه دارد؛ زیرا فضای سایبر، فاقد حد و مرز است و افراد با هویت‌های جعلی مرتکب جرم می‌شوند. بنابراین طرح راهکار و راهبردی در این خصوص و نیاز به ارائهٔ نظریه‌های جدید در این فضا اجتناب‌ناپذیر است.

در همین راستا، برخی سعی کرده‌اند همان قواعد سنتی ناظر بر صلاحیت کیفری مراجع قضایی را، با نگرشی جدید، در این فضا اجرا کنند و برخی دیگر با طرح تئوری‌های نو در خصوص صلاحیت، از قبیل " فضای سایبر به عنوان یک فضای آزاد بین‌المللی" و یا پیش‌بینی دادگاهی ویژه به نام " دادگاه دیجیتالی یا سایبری" و یا صلاحیت " دادگاه ذی ارتباط منطقی با

جرم" را مطرح کرده‌اند. کشور ایران، در قانون مجازات جرایم رایانه‌ای، در مادهٔ ۲۸ تئوری اول، یعنی اجرای قواعد سنتی با نگرشی جدید را اتخاذ کرده است (فروغی، ۱۳۹۱: ۳٤).

این ماده مقرر داشته که علاوه بر موارد پیش‌بینی‌شده در دیگر قوانین، دادگاه‌های ایران برای رسیدگی به این موارد صالح خواهند بود:

الف. داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته است و به هر نحو در سامانه‌های رایانه‌ای و مخابراتی، یا حامل‌های دادهٔ موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب. جرم از طریق تارنماهای (وب‌سایت‌های) دارای دامنهٔ مرتبه بالای کد کشوری[1] ایران ارتکاب یافته باشد.

ج. جرم، توسط هر ایرانی یا غیرایرانی، در خارج از ایران، علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای (وب‌سایت‌های) مورد استفاده، یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای (وب‌سایت‌های) دارای دامنهٔ مرتبه بالای کد کشوری ایران، در سطح گسترده ارتکاب یافته باشد.

در کشور ما از لحاظ رویهٔ عملی، تا قبل از تصویب قانون مجازات جرایم رایانه‌ای، قضات سعی داشتند قواعد سنتی صلاحیت را، با اتخاذ معیاری جدید و موافق با فضای جدید اجرا کنند؛ که در این خصوص، رویه واحدی هم اتخاذ نشده بود. با تصویب قانون جرایم رایانه‌ای، این قانون مطالبی را در مواد ۲۸، ۲۹، ۳۰ و ۳۱ به موضوع صلاحیت اختصاص داده است. در بندهای الف و ب مادهٔ ۲۸، با تسری قلمرو حاکمیت کشور به سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های دادهٔ موجود در قلمرو حاکمیت زمینی، دریایی و هوایی کشور و تارنماهای دارای

---

۱. دامنهٔ اینترنتی بالا معادل Top Level Domain (TLD) است و به بالاترین سطح دامنه‌های اینترنتی گفته می‌شود که در محدوده نام و در منطقهٔ ریشه (RooT Zone) قرار گرفته و نصب می‌شود، به عنوان پسوند نام دامنه در آخرین بخش دامنه‌های سطح پایین‌تر قرار می‌گیرد.

دامنهٔ مرتبهٔ بالای کد کشور ایران، قاعدهٔ صلاحیت سرزمینی را، به گونهٔ دیگری نسبت به جرایم ارتکابی در فضای سایبر اعمال کرده است.

در بند ج، صلاحیت شخصی سنتی و در بند د: «با قبول هرزه‌نگاری اطفال به عنوان جرم، موضوع صلاحیت جهانی، قاعدهٔ صلاحیت جهانی را برای رسیدگی به جرایم سایبری پیش‌بینی کرده است». قانون تجارت الکترونیکی، مصوب ۱۳۸۲، در مورد محل انجام یک معاملهٔ الکترونیکی، در مادهٔ ۲۹، قواعدی را بیان کرده و در فصل چهارم، به بحث صلاحیت جزایی اشاره کرده و مقررات حاکم بر صلاحیت جزایی در خصوص جرایم تجارت الکترونیکی را به بخش دوم همین قانون احاله کرده است، که در همین راستا، با تصویب و تأیید قانون جرایم رایانه‌ای فوق‌الذکر، قواعدی راجع به شیوهٔ اعمال صلاحیت در بخش دوم همین قانون پیش‌بینی شده است.

البته باید این نکته را در نظر داشت که در رسیدگی به جرایم رایانه‌ای، مانند جرایم سنتی، قواعد صلاحیت ذاتی و شخصی نیز رعایت می‌شود؛ برای مثال در فرضی که متهم مرتکب سرقت رایانه‌ای و جاسوسی رایانه‌ای می‌شود، اتهام وی از حیث جاسوسی رایانه‌ای، در دادگاه انقلاب رسیدگی می‌شود و از حیث صلاحیت شخصی نیز برخی جرایم هستند که محل وقوع آن‌ها، نقشی در تعیین صلاحیت محل دادگاه ندارد؛ مانند جرایمی که شخصیت مرتکب، تعیین‌کننده صلاحیت است، مانند جرایم استانداران، روحانیون، قضات و ... یا مواردی که سن مرتکب تعیین‌کننده صلاحیت باشد، مانند جرایم اطفال یا مواردی که به اعتبار شغل متهم باشد، مانند جرایم مربوط به افراد نظامی که به مناسبت شغل در حین انجام وظیفه مرتکب می‌شود که در این حالت با پیروی از قاعده صلاحیت شخصی در مراجع صالح یعنی دادگاه پایتخت یا مرکز استان یا اطفال یا دادگاه نظامی حسب مورد رسیدگی می‌شود.

در خصوص تعارض صلاحیت در حوزه‌های قضایی داخلی، اختلاف در صلاحیت و چگونگی آن، در فصل دوم از باب اول مواد ۲۶ الی ۳۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی سال ۷۹ آمده است. قانون آیین دادرسی جرایم رایانه‌ای نیروهای مسلح

و دادرسی الکترونیکی که در تاریخ ۱۳۹۳/۰۷/۰۸ به تصویب مجلس شورای اسلامی رسید، از مادهٔ ٦٦٤ تا مادهٔ ٦٨٧ (فصل دهم قانون آیین دادرسی جرایم رایانه‌ای نیروهای مسلح و دادرسی الکترونیکی) درست همان موارد ذکرشده در قانون جرایم رایانه‌ای آمده است، با این تفاوت که با توجه به تغییر تشکیلات قضایی، قوهٔ قضاییه در مادهٔ ٦٦٦ این قانون موظف شده، به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدید نظر را برای رسیدگی به جرایم رایانه‌ای اختصاص دهد. این دادگاه می‌تواند به صلاحدید خود و بر اساس قواعد پیش‌بینی‌شده در مادهٔ مزبور، از قانون جرایم رایانه‌ای یا دیگر قواعد، نظیر ارتباط منطقی با یک حوزه، پرونده‌ها را به آن‌ها ارجاع یا احاله کند (جلالی فراهانی، ۱۳۸۸: ۱۰۰).

بر اساس مادهٔ ٦٦٥ همین قانون:

> چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

لذا دیده می‌شود که قانون مجازات جرایم رایانه‌ای ایران، با در نظر گرفتن چالش‌های فضای سایبر و مشکل بودن تعیین محل ارتکاب جرم سایبری، مرجع محل گزارش جرم و یا محل کشف جرم را، در جایی که محل وقوع قابل تعیین نباشد، جایگزین ضابطهٔ محل وقوع جرم کرده و همان مراجع را برای رسیدگی صالح دانسته است. در هر حال، بر اساس قوانین کنونی ایران، اصل بر این است که مرجع صالح رسیدگی به جرایم سایبری، مرجع محل وقوع جرم است؛ ولی در صورت عدم امکان تعیین محل وقوع جرم، که بیشتر وقت‌ها چنین امکانی وجود ندارد، محل گزارش یا کشف ملاک خواهد بود (امینی‌نیا و همکاران، ۱۳۹۷: ۵۹). در میان محل گزارش و محل کشف، اگرچه بیشتر وقت‌ها این دو محل یکی هستند، ولی در صورت متفاوت بودن آن‌ها، حسب مادهٔ ٦٦٥ قانون مزبور، اولویت با محل کشف است و محل گزارش، ناظر به زمانی است که جرم کشف نشده باشد. و در مواردی که اجزاء مختلف عنصر مادی جرم، در چند حوزهٔ قضایی مختلف اتفاق می‌افتد یا مواردی که یک شخص، مرتکب چندین جرم

متفاوت سایبری در چند حوزهٔ قضایی مختلف می‌شود، ممکن است چندین حوزهٔ قضایی خود را برای رسیدگی صالح بدانند، در این حالت، تبصرهٔ مادهٔ ۵۲ قانون جرایم رایانه‌ای مقرر می‌دارد:

درمواردی که در بخش دوم این قانون برای رسیدگی به جرایم رایانه‌ای مقررات خاص از جهت آیین دادرسی پیش‌بینی نشده است، طبق مقررات قانون آیین دادرسی اقدام خواهد شد.

حال با در نظر گرفتن مقررات شکلی قانون جرایم رایانه‌ای و مقررات مربوط به صلاحیت مندرج در قانون آیین دادرسی کیفری، مصوب ۹۲، فرض‌های مختلفی جهت تعیین دادگاه صالح از حیث صلاحیت محلی متصور است که به شرح آن می‌پردازیم:

۱. مطابق اصول کلی آیین دادرسی کیفری و نیز قانون جرایم رایانه‌ای در جایی که محل وقوع جرم معلوم باشد، دادگاه محل وقوع جرم برای رسیدگی صالح است.

۲. اگر یک یا چند جرم سایبری، که از حیث مجازات مشابه است، در یک حوزهٔ قضایی کشف یا گزارش شود که محل وقوع آن معلوم نباشد، مطابق مادهٔ ۲۹ قانون جرایم رایانه‌ای، دادسرای محل کشف مکلف است، تحقیقات مقدماتی را انجام دهد؛ چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات، مبادرت به صدور قرار می‌کند و دادگاه مربوطه نیز رأی مقتضی صـــادر می‌کند.

۳. جرم سایبری واقع شده؛ ولی اجزاء مختلف عنصر مادی آن، در دو حوزه واقع شده‌اند و محل وقوع جرم معلوم نباشد، به دلیل بروز اختلاف میان مراجع قضایی، رأی وحدت رویه شماره ۷۲۹ مورخ ۹۱/۱۲/۱، در خصوص جرم کلاهبرداری مرتبط با رایانه مقرر می‌دارد: هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضایی مختلف صورت گرفته باشـد، دادگاهی که بانک افتتاح‌کننده حساب زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشت شده در حوزهٔ آن قرار دارد، صالح به رسیدگی است.

٤. در صورت وقوع چند جرم مختلف، که از حیث مجازات در حوزه‌های قضایی متفاوت (اعم از سایبری و غیر سایبری) است، در صورتی که محل وقوع جرایم معلوم باشد، دادگاه محل وقوع مهم‌ترین جرم، صالح به رسیدگی است.

۵. در صورت وقوع چند جرم مشابه از حیث مجازات (اعم از سایبری و غیر سایبری) که محل وقوع جرایم مشخص نباشد و متهم نیز دستگیر نشده باشد؛ دادگاهی که ابتدا شروع به رسیدگی کرده، صالح است.

٦. در صورت وقوع چند جرم مشابه از حیث مجازات، در حوزه‌های قضایی مختلف که محل وقوع جرایم نیز معلوم نباشد، دادگاه محل دستگیری متهم، صالح به رسیدگی است.

۷. در صورت وقوع چند جرم مشابه از حیث مجازات، در حوزه‌های قضایی مختلف که متهم نیز دستگیر شده، ولی محل دستگیر شدن محل وقوع جرم نباشد، دادگاه محل وقوع جرم که ابتدا شروع به رسیدگی کرده، صالح به رسیدگی است (جعفری، ۱۳۹۲: ۷۰).

راهکار حقوقی تأمین امنیت در فضای سایبر

تناسب، هماهنگی و همسویی، میان مجازات و جرم از لوازم یک نظام کیفری متعادل است. مبنای منطقی، برای مجازات از اصول اولیه و بنیادین نظام عدالت کیفری و عامل مشروعیت آن است. در نظام کیفری ایران، تاکنون، لااقل مبانی کلی و فراگیر برای تناسب مجازات با جرم ارتکابی مکتوب نشده است. نبود اصول بنیادی، در تعیین کیفر، در مرحله تقنین و اجرا از عمده ایرادها، یا شاید عمده‌ترین ایراد نظام کیفری ایران است. گاهی قانونگذار، در تعیین مجازات جرمی، فاصله بین حداقل و حداکثر آن را به ٤٠ برابر رسانده است و دادگاه، بدون الزام به توجیهی، در بین حداقل و حداکثر آن مختار است هر میزان مجازات تعیین کند، که نوعاً تناسبی بین مجازات و جرم دیده نمی‌شود؛ این امر، اصل تناسب مجازات با جرم را مخدوش خواهد کرد. بنابراین بیان معیار کلی و بنیادین، برای رعایت اصل تناسب جرم با مجازات از اصول راهبردی است که باید در نظام کیفری ایران به آن پرداخته شود (سبزه‌واری‌نژاد، ۱۳۹٦: ۱۳۳).

همواره در تعیین کیفر، ارزش مجازات باید سنجیده شود. بدین معنا که گاهی فرد بزهکار، دستاورد ارتکاب جرم و میزان مجازات تعیین‌شده برای آن را بررسی می‌کند که آیا این جرم، با توجه به میزان مجازات تعیین‌شده برای آن، ارزش ارتکاب دارد یا خیر؟ به‌فرض فرد بزهکار با دسترسی غیر مجاز به سامانه‌های رایانه‌ای بخش دولتی و سرقت داده‌های مربوط به

زیرساخت‌های اساسی دولت به اطلاعاتی دست پیدا می‌کند که می‌تواند سود مالی زیادی را، با فروش آن به دول متخاصم، به دست بیـاورد. این در حالی است که مجازات دسترسی غیر مجاز (موضوع مادۀ ۱ قانون جرایم رایانه‌ای[۱]) و سرقت داده (موضوع مادۀ ۱۲ قانون جرایم رایانه‌ای[۲]) جزای نقدی بسیار اندکی در پی خواهد داشت[۳]. بدیهی است که بزهکار، با بررسی میزان مجازات و دستاورد حاصل از ارتکاب جرم، به این نتیجه می‌رسد که می‌تواند با ارتکاب جرم چه میزان مال به دست آورد و چه میزان مجازات خواهد شد؛ همین موضوع، انگیزۀ او را برای ارتکاب به جرم قوی‌تر خواهد کرد. قطعاً اگر میزان مجازات، با توجه به اهمیت جرم تعیین شود، فرد بزهکار، هرگز خود را در جایگاهی قرار نمی‌دهد که بخواهد با علم به میزان مجازات، اقدام به ارتکاب جرم کند.

از ایرادهای دیگری که می‌توان در بحث جرایم رایانه‌ای بدان توجه داشت، بحث تحصیل و جمع‌آوری دلایل استنادپذیر است، با توجه به ویژگی‌های خاص این فضا، بر خلاف فضای سنتی، قاضی و ضابطان امکان مشاهده و جمع‌آوری ادله را ندارند، به معنای واقعی محل وقوع جرمی وجود ندارد که بتوان آثار وقوع جرم را بررسی کرد، نوع تحقیقات، توقیف اسباب وقوع جرم و ... نیاز به تخصص خاصی دارد. در واقع، جایگزین شدن موضوع‌های غیر ملموس و سایبر، به جای ادلۀ ملموس و واقعی، مسایل حقوقی نوینی را پدید می‌آورد که به یقین،

۱. هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیلۀ تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰)، ریال یا هر دو مجازات محکوم خواهد شد.

۲. هرکس به طور غیرمجاز، داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون (۱،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال، یا هر دو مجازات محکوم خواهد شد.

۳. لازم به توضیح است که با تصویب قانون کاهش مجازات‌های حبس تعزیری، مصوب سال ۱۳۹۹، با توجه به مادۀ ۳۷ آن، جهات تخفیف مجازات‌های تعزیری افزوده شده است، ضمن آنکه، بر اساس تبصرۀ مادۀ ۲ همین قانون، مجازات حبس می‌بایست به صورت میزان حداقلی تعیین‌شده در قانون، مجازات اسلامی ۹۲ اعمال شود و در صورتی‌که قاضی تصمیم داشته باشد به بیش از حداقل مجازات رأی دهد، می‌بایست دلایل خود را ارائه کند، بدیهی است که با وجود این تبصره رویکرد قضات در صدور رأی، حداقل مجازات تعیین‌شده خواهد بود که با توجه به میزان کم جزای نقدی و حبس‌های تعیین‌شده در قانون جرایم رایانه‌ای، مسئولیت کیفری برای مرتکب بسیار ناچیز بوده، کما اینکه این میزان کم نیز، با توجه به قانون کاهش حبس تعزیری در قانون مجازات اسلامی در موارد بسیار زیادی قابل تبدیل به مجازات های دیگر از جمله مجازات جایگزین حبس است.

بازخورد مستقیمی نیز در حقوق کیفری خواهد داشت. از این رو، لزوم آموزش مجریان قانون، امری است که باید مورد توجه قرار بگیرد.

همان طور که دادسرای جرایم رایانه‌ای، به عنوان دادسرای تخصصی، در حال حاضر صلاحیت رسیدگی به جرایم ارتکابی را در این بستر دارد، می‌بایست دادگاه‌های کیفری و تجدید نظر نیز، شعب ویژه، برای رسیدگی به آرا و قرارهای صادره از دادسرا داشته باشند، زیرا به نظر می‌رسد رسیدگی در دادگاه‌های بدوی و تجدید نظر، در خصوص منع تعقیب یا کیفرخواست صادره از دادسرای تخصصی جرایم رایانه‌ای، نیازمند یک رویکرد و بررسی از جانب متخصصان این امر است، که متأسفانه، در حال حاضر، این گونه دعاوی در شعب عمومی و بیشتر وقت‌ها، با قضات غیر متخصص در امر جرایم رایانه‌ای مورد رسیدگی قرار می‌گیرد.

از دیگر مشکلات فضای سایبر، عدم جرم‌انگاری استفاده از نرم‌افزارهای عبور از فیلتر (VPN) است. اصول ۳۶ و ۳۷ قانون اساسی، که شاخصه و سرلوحهٔ همه قوانین مطروحه در کشور است، حکم به مجازات و اجرای آن را تنها از طریق دادگاه صالح و به موجب قانون مورد شناسایی قرار داده است. حتی قانونگذار، اصل را بر برائت می‌داند و هیچ‌کس از نظر قانون مجرم شناخته نمی‌شود، مگر اینکه جرم او در دادگاه صالح ثابت شود. بر اساس مادهٔ ۲ قانون مجازات اسلامی، فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد، جرم محسوب می‌شود. با توجه به این موارد و از آنجا که درخصوص جرایمی که در فضای مجازی اتفاق می‌افتد، قانون خاص آن وجود دارد، به نظر می‌رسد هیچ ماده‌ای از مواد ۵۶گانه آن وجود ندارد که استفاده از فیلترشکن‌ها یا پروکسی‌ها را عمل مجرمانه معرفی کند؛ مضافاً آنکه در این خصوص نیز، نظریهٔ شماره ۷/۳۶۷ مورخ ۱۳۹۹/۲/۲۵ اداره حقوقی قوه قضاییه می‌گوید:

> نظر به اینکه در قانون جرایم رایانه‌ای مصوب ۸۸ برای صرف استفاده از فیلترشکن یا دانلود رایگان آن مجازاتی پیش‌بینی نشده، لذا با توجه به اصل ۳۶ قانون اساسی و مقررات مادهٔ ۲ قانون مجازات اسلامی، اعمال موضوع استعلام قانوناً جرم تلقی نمی‌شوند.

نگاهی به رویهٔ قضایی نیز اثبات می‌کند، تاکنون در دستگاه قضایی، پرونده‌ای با عنوان مجرمانهٔ استفاده از فیلترشکن، به صدور رأی منجر نشده است.

استفاده از فیلترشکن‌ها، باعث پنهان ماندن هویت افراد می‌شود، با نمایش یک آی‌پی غیر واقعی، افراد می‌توانند اقداماتی چون دسترسی غیر مجاز، سرقت داده، جعل رایانه‌ای و ... را به گونه‌ای انجام دهند که هرگز هویت واقعی آنها قابل کشف نباشد. و این پرونده‌ها، علاوه بر اینکه پیچیدگی رسیدگی را بیشتر می‌کنند، باعث بالاتر رفتن هزینهٔ کشف جرم برای دستگاه قضا و ضابطان می‌شوند. لذا، ضرورت سالم نگهداشتن فضای سایبر از طریق فراهم ساختن بستر مناسب، برای فعالیت‌های مشروع از یک‌سو و پاک‌سازی آن از وجود چنین تهدیدهایی، ایجاب می‌کند که ضوابط و مقررات اثربخش و بازدارنده‌ای در این حوزه به تصویب برسد. در این راستا، کمیسیون حقوقی و قضایی مجلس شورای اسلامی، با پیشنهاد طرح الحاق یک بند، به مادهٔ ۲۵ قانون جرایم رایانه‌ای، کوشیده تا نیازمندی‌های برخورد بازدارندهٔ قانونی را با تولید، تکثیر، انتشار، توزیع، معامله و یا در دسترس قرار دادن VPN تأمین کند؛ که علی‌رغم برگزاری جلسات متعدد، با حضور نمایندگان سازمان‌های ذی‌صلاح این مهم به نتیجه نرسیده است (طهماسبی و همکاران، ۱۳۹۷: ۱۲۳).

نتیجه‌گیری

اگرچه ویژگی‌ها و اقتضائات فضای سایبر، به کل متفاوت از فضای واقعی است، اما با توجه به نبود نص خاص، در خصوص جبران خسارات حاصله در فضای سایبر، باید گفت که نظام حقوقی مسئولیت مدنی در این فضا، همان قواعد سنتی موجود در قانون مدنی و سایر قوانین مربوط است که نتیجهٔ آن، عدم امکان تأمین امنیت مدنی و رصد اطمینان‌بخش کنش‌های حقوقی در این فضا خواهد بود. بنابراین، نه‌تنها از باب تقنین، بلکه از حیث صلاحیت قضایی نیز، تاسیس شعب یا مراکز حقوقی، با کارشناسان و قضات متخصص، برای تأمین هرچه بیشتر این امنیت ضروری است.

اما به لحاظ کیفری، اگرچه از جهت تقنینی و قضایی، اقدام‌های مهمی صورت پذیرفته، اما راه، نیمه پیموده شده است. خلأها و نارسایی‌های موجود، در قانون جرایم رایانه‌ای را، به طور عمده می‌توان ناشی از عدم لحاظ مفاهیم و ماهیت جرایم رایانه‌ای و عدم تناسب مجازات با جرم ارتکابی یا ویژگی‌ها و اقتضائات این فضا دانست؛ که خود نشانهٔ شتاب‌زدگی قانونگذار در تصویب قانون است. همین موضوع، باعث وقوع هرچه بیشتر جرم در این فضا شده و نیز، موجب شده با جرایمی روبه‌رو شویم که برای آن‌ها مجازاتی پیش‌بینی نشده، یا میزان مجازات به قدری حداقلی است که مرتکب با علم به آن و برآورد دستاورد ناشی از آن، جرم را با کمال میل و اطمینان انجام می‌دهد.

از دیگر موارد نقص موجود در قانون جرایم رایانه‌ای، مستقر ساختن بار مسئولیت، بر عهدهٔ ارائه‌دهندگان خدمات دسترسی و میزبانی است، که بیشتر نیز در بخش خصوصی فعال هستند و توان مالی و انسانی محدودی دارند. همچنین، عدم تعیین مجازات برای استفاده از فیلتر شکن‌ها، که باعث مجهول ماندن بیش‌ازپیش هویت مرتکب می‌شود و می‌تواند نقش حائز اهمیتی، در ابتر ماندن اجرای مجازات و جبران خسارت بزه‌دیده داشته باشد. از ایرادهای شکلی این قانون نیز، می‌توان به یکدست نبودن متن قانون اشاره کرد، قانونگذار در برخی موارد از واژه رایانه و در برخی موارد از واژهٔ کامپیوتر استفاده کرده است.

منابع

ابن‌بابویه، محمدابن‌علی. ۱۳۷۷. *خصائل شیخ صدوق*. ترجمهٔ محمدباقر کمره‌ای. قم: انتشارات کتابچی.

افتاده، جواد.۱۳۹۱. " تفاوت میان رسانه‌های اجتماعی و رسانه‌های جمعی". *کتاب ماه علوم اجتماعی*. شماره ٥٦: ٦٧_٧٢.

افضلی، مهدی. ۱۳۸۸. *مسئولیت کیفری انتسابی در فضای سایبر*. حقوق فناوری اطلاعات و ارتباطات. (مجموعه مقالات) تهران: معاونت حقوقی و توسعه قضایی قوه قضاییه، مرکز مطالعات توسعه قضایی.

امینی‌نیا، عاطفه و حمیدرضا علیزاده. ۱۳۹۷. " اعمال صلاحیت کیفری (تعارض قوانین) در مورد جرایم ارتکابی در فضای سایبر". ماهنامه *پژوهش ملل*. دورهٔ سوم. شماره ۳۰.

جعفری، مجتبی.۱۳۹۲. " تعدد جرم و آثار آن در قانون جدید مجازات اسلامی ۹۲". فصلنامه *پژوهش حقوق کیفری*. سال دوم. شماره ۵: ۱۱۵ـ ۱۹۶.

جلالی فراهانی، امیرحسین. ۱۳۸۸. *درآمدی بر آیین دادرسی کیفری جرایم سایبری*. تهران: انتشارات خرسندی.

حاجی ده‌آبادی، احمد و احسان سلیمی. ۱۳۹۸. " اصول جرم‌انگاری در فضای سایر با رویکرد انتقادی به قانون جرایم رایانه‌ای". فصلنامه *مجلس و راهبرد*. سال ۲۱. شماره ۸۰ : ۶۱ـ ۸۸ .

حاجی ده‌آبادی، محمدعلی و احسان سلیمی. ۱۳۹۸. " بزهکاری و بزه‌دیدگی بومی‌های اینترنت، از علت‌شناسی تا پاسخ‌دهی در پارادایم ترمیمی". دوفصلنامه *مطالعات حقوق کیفری و جرم شناسی*. دوره ۴۹. شماره ۱: ۴۱ـ۶۳.

حسینی، سیدعلی.۱۳۸۱. "بازشناسی، تحلیل و نقد نظریه منطقه الفراغ". فصلنامه *اندیشه صادق*. شماره ٦ و ۷.

ضیایی، سیدیاسر و مونا خلیل‌زاده. ۱۳۹۲. " مسئولیت بین‌المللی دولت‌ها ناشی از حملات سایبر". فصلنامه *پژوهش‌های حقوقی*. دورهٔ ۱۲. شمارهٔ ۲۳: ۸۷ ـ۱۲۲.

خلیل‌زاده، مونا.۱۳۹۳. *مسئولیت بین‌المللی دولت‌ها در برابر حمله‌های سایبری*. تهران: انتشارات مجد.

رزونا، جمیز و دیگران.۱۳۹۰. *انقلاب اطلاعات، امنیت و فناوری‌های جدید*. ترجمه علیرضا طیب. تهران: انتشارات پژوهشکده مطالعات راهبردی.

ریچارد کی، مور.۱۳۸۳. " دموکراسی و فضای سایبر". ترجمه عبدالرضا زکوت روشندل. فصلنامه *رسانه*. سال پانزدهم. شماره سوم: ۸٦ ـ ۱۱۰.

ری‌شهری، محمدمهدی.۱۳۸٤. *میزان الحکمه*. مؤسسه فرهنگی دارالحدیث.

سبزه‌واری‌نژاد، حجت.۱۳۹٦. " جایگاه اصل تناسب جرم و مجازات در حقوق کیفری ایران و انگلستان". فصلنامه *دیدگاه‌های حقوق قضایی*. دوره ۲۲. شمارهٔ ۷۷ و ۷۸: ۱۲۳ ـ ۱٦٤.

بیست و ششمین اجلاس یونسکو. ۱۳۹۰. " شاخص‌های توسعه رسانه، چارچوبی برای ارزیابی توسعه رسانه‌ها مورد تأیید شورای بین دولتی برنامه بین‌المللی برای توسعه ارتباطات. انتشارات دفتر منطقه‌ای یونسکو. تهران.

شجاعی، محمدصادق. ۱۳۸۸. " روانشناسی و آسیب‌شناسی اینترنت". فصلنامه *روانشناسی و دین*. سال دوم. شماره ۵: ۱۱۵ ـ ۱٤۲.

صانعیان، علی. ۱۳۹۸. " امنیت سایبری در آمریکا ساختارها و روندها". فصلنامه *سیاست خارجی*. سال سی و سوم. شماره ۱: ۱۹۱ ـ ۲۲۸.

صحیفه سجادیه ، دعای بیستم.
ضیایی، سیدیاسر و احسان شکیب‌نژاد. ۱۳۹٦. " قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران". دوفصلنامه *مجله حقوقی بین‌المللی*. دورهٔ سی و چهارم. شماره ۵۷: ۲۲۷ ـ ۲٤۷.
طهماسبی، جواد و خیرالله شاهمرادی. ۱۳۹۷. " چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری". *مجله حقوقی دادگستری*. دورهٔ ۸۲ . شماره ۱۰٤: ۹۵ ـ ۱۲۱.
عاملی، سعیدرضا و دیگران. ۱۳۹۱. *فضای سایبر (ملاحظات اخلاقی، حقوقی و اجتماعی)*. تهران: انتشارات دانشگاه تهران.
علیوردی‌نیا، اکبر.۱۳۹۳. " مدیریت پیشگیری از جرم در ایران". فصلنامه *سیاست‌های راهبردی کلان*. سال دوم. شمارهٔ ۸ : ۳۷ ـ ۵۸.
فروغی، فضل‌الله و امیر البوعلی. ۱۳۹۳. " صلاحیت کیفری مراجع قضایی در فضای سایبر". فصلنامه *تحقیقات حقوقی دانشگاه شهید بهشتی*. دوره ۱۵. شماره ۵۸: ۳۱۱ ـ ۳۵٦.
فرهادی‌آلاشتی؛ زهرا و عبدالرضا جوان‌جعفری بجنوردی. ۱۳۹٦. " نقض آزادی جریان اطلاعات در فرآیند پیشگیری موقعیت مدار از جرایم سایبری". فصلنامه *پژوهش حقوق کیفری*. دوره ۵ . شماره ۱۸: ٦۹ ـ ۱۰۰.
فهیمی، مهدی. ۱۳۸۳. *عصر اطلاعات و میزان تأثیر علم و فناوری در جنگ‌های اخیر*. تهران: دانشگاه مالک اشتر.
قاجار، سیامک. ۱۳۸٦. *حقوق سایبر*. تهران: نشر میزان.
کاستلز، مانوئل. ۱۳۸۲. *عصر اطلاعات*. جلد اول، چاپ سوم، تهران: طرح نو.
معتمدنژاد، کاظم.۱۳۹۰. " تحولات مبانی حقوقی آزادی رسانه‌ها در عرصه‌های ملی، منطقه‌ای و بین‌المللی". فصلنامه *پژوهش حقوق*. ویژه‌نامه حقوق ارتباطات. شماره ۱۵.
معتمدنژاد، کاظم.۱۳۹۰. *حقوق ارتباطات بین المللی*، جلد دوم. تهران: دفتر مطالعات و توسعه رسانه‌ها.
کیان‌خواه، احسان. ۱۳۹۸. " چالش‌های راهبردی حکمرانی با گسترش فضای سایبر". فصلنامه *علمی امنیت ملی*. دوره ۹. شماره ۳٤: ۱۵۳ ـ ۱۷٤.
ملکوتی، رسول. ۱۳۹۸. *اصول فقه*. تهران: انتشارات مجد.
ملکوتی، رسول. ۱۳۹۸. " بررسی وضعیت حقوقی حاکمیت دولت در فضای مجازی". *مجموعه مقالات همایش جنبه‌های حقوقی فناوری اطلاعات و ارتباطات ایران*. تهران: دانشگاه علم و فرهنگ، چاپ دوم.
ملکوتی، رسول. ۱۳۹۵. " درآمدی بر مسئولیت مدنی در فضای سایبر". فصلنامه *پژوهش حقوق خصوصی*. سال چهارم. شماره ۱۵: ۱۲۹ ـ ۱٤۹.

ملکوتی، رسول. ۱۳۹۵. *مسئولیت مدنی در فضای سایبر*. تهران: انتشارات مجد.

نعمتی، نبی‌اله، امیر صادقی‌نشاط. ۱۳۹۶. " بررسی مسئولیت مدنی ناشی از نقض امنیت داده در تهدیدات سایبری". فصلنامه *پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین (ع)*. سال ششم. شماره ۲۳.

یاسمی‌نژاد، عرفان؛ اکرم آزادی؛ محمدرضا امویی. ۱۳۹۰. " فضای مجازی، امنیت اجتماعی، راهبردها و استراتژی‌ها". همایش ملی صنایع فرهنگی نقش آن در توسعهٔ پایدار.

Bush, George walker ,2003, U.S. President, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”. http://www.whitehouse.gov (accessed August 11, 2016)

Emmanuel Derieux, 2005, *droit des medias* ,Paris: Dalloz Micheal, Froomkin. 2000, “The Death of Privacy”? *Stanford Law Reeview*, Vol ،52.

Milton Mucller ،Hans Klein & Marc Llolitscher and LccMcknight, 2004. “Internet Governance: the State of Play, the Internet Governance Project”, ،at: www.internetgovernance.org.

Schwabac ,Aarson. 2006. *Internet and the Law,Technology,Society and Compromises*, ABC-CLIO,California.

Wayne, C ،J, R, Clyde, 2003. *Who Rules The Net? Internet Governance and Jurisdiction*, Washington D, C: Cato Institute, ISBN: 1-930865-43-0 ،468.

Wes Simpson & Greenfield Howard. 2007. *IPTV and Internet Vdeo*,UK: Oxfor.