شناسه دیجیتال (DOI): 10.22106/JLJ.2018.32734

حاکمیت قانون اساسی در رویارویی با بزه رایانه‌ای

حسن عالی‌پور*
محمد یکرنگی**

چکیده

رویارویی با بزه رایانه‌ای با به‌کارگیری همه راهکارهای پیگیرانه و پیشگیرانه پیوستگی دارد. راهکارهای پیگیرانه به تدبیرهای کیفری ماهوی از بزه‌انگاری و مسئول‌شناسی گرفته تا کیفرگذاری و کیفرگزینی را در بر می‌گیرد و راهکارهای پیشگیرانه نیز تدبیرهای اجتماعی، فنی، موقعیت‌محور و شخص‌محور را پیش از رخ دادن بزه رایانه‌ای بازگو می‌کند. تمامی این راهکارها باید از دو اصل بنیادین پیروی کنند: نخست، از ارزش‌ها و هنجارهای جامعه پشتیبانی کرده و برای دولت امنیت پدید آورد. دوم، آزادی‌های فردی و حقوق شهروندی را در تنگنا نگذارد. اگر رویارویی با بزه رایانه‌ای تنها با محور قرار دادن جامعه و دولت باشد؛ در این حال تهدید، بزه رایانه‌ای است که محور سیاست‌گذاری‌ها و کنش‌ها خواهد بود و رویارویی با آن، به امنیتی کردن جامعه می‌انجامد و اگر رویارویی با بزه رایانه‌ای تنها با محور قرار دادن آزادی‌های فردی باشد، در این حال تهدید، بزهکار رایانه‌ای است که کوشش می‌شود تا حقوق وی پاس داشته شود و از سوی دیگر حقوق و آزادی‌های شهروندان در فضای سایبر نیز همیشه در نگاه باشد.

نگاه امنیت‌محور به مبارزه با بزه رایانه‌ای و رویکرد آزادی‌مدار به پیکار با آن، هیچ یک با قانون اساسی سازگاری ندارند. هر اقدام پیگیرانه و یا پیشگیرانه باید در راستای قانون اساسی کشور که برای هر برنامه یا کنش و واکنشی، تراز امنیت ملی و آزادی‌های فردی را می‌شناساند، اصلاح شود. نوشتار کنونی نیز کوششی برای سازگار کردن پیکار با بزه رایانه‌ای با قانون اساسی و دوری از رویکرد یک‌طرفه امنیت‌محوری یا حق‌مداری در رویارویی با بزه رایانه‌ای است.

* عضو هیأت علمی پردیس فارابی دانشگاه تهران (نویسنده مسئول) Hassan.alipour@ut.ac.ir
** عضو هیأت علمی دانشکده حقوق و علوم سیاسی دانشگاه تهران Yekrangi@ut.ac.ir
تاریخ دریافت: ۹۵/۰۲/۲۳ تاریخ پذیرش: ۹۵/۰۶/۱۵

کلیدواژه‌ها: تروریسم سایبری، حمله سایبری، امنیت ملی، آزادی‌های فردی، قانون اساسی.

مقدمه

هر پدیده نویی در سه فرآیند به درون نظام حقوقی یک کشور راه می‌یابد که در طول هم جای دارند: در گام نخست باید ضابطه‌مند شود و همه کارها و کنش‌ها بر پایه قانون یا مقرره‌های فروقانونی انجام شود. دلیل بدیهی این ضابطه‌گرایی همان مسئولیت در برابر رفتارهای زیان‌بار یا سرزنش‌پذیر است. در گام دوم، جداسازی رفتارهای زیان‌بار یا سرزنش‌پذیر در مقام بزه که نظام کیفری بر پایه آن بنیاد می‌گیرد. در این گام، برخی از رفتارها بر مبانی اخلاقی، مذهبی، سیاسی یا مصلحت با کیفر روبه‌رو می‌شوند و پیرو آن بیشتر کنش‌های ظاهری، قهری و محدودکننده به ویژه اقدام‌های پلیسی توجیه می‌شود. در گام سوم، نوبت به اقدام‌های تأمینی و پیشگیرانه می‌رسد. سنخ این اقدام‌ها بر پایه شتاب‌آمیزی، گستردگی و در بیشتر موردها بدون نیاز به توجیه مسئولیت از سوی انجام‌دهنده آن است. اقدام‌های تأمینی و پیشگیرانه هنگامی انجام می‌شود که پیش از آن یک رفتار، قابل کیفر باشد.

فضای سایبر هم اکنون برجسته‌ترین مصداق پدیده نو در جهان امروز است؛ ولی این پدیده نو به طور بنیادی با پدیده‌های دیگر که در زمان پدید آمدنشان نو به شمار می‌رفتند، فرق دارد. فضای سایبر یا بستر تبادل اطلاعات چنانکه با عنوان «فضا» یا «بستر» یاد می‌شود، فراتر از پدیده و به عنوان یک جهان یا سپهری نو دانسته می‌شود که خود دارای پدیده‌های گوناگون و نو است و در این بستر یا فضا، هر روز پدیده نوی رخ می‌نماید. همین اندازه بس است که بدانیم فضای سایبر وارونه پدیده‌های دیگر که در حوزه خاص یا دوره معین نمود دارند، عام و فراگیر است و شاید نتوان فضای سایبر را پدیده نام نهاد؛ چرا که یک جهان یا بستر زندگی هم‌تراز با زندگی طبیعی بشر است و هر روز نیز گسترده‌تر و فراگیرتر می‌شود؛ برای نمونه، ایران در سال ۲۰۰۰، تنها دویست و پنجاه هزار تن کاربر اینترنتی داشت ولی در سال ۲۰۱۶، شمار کاربران ایرانی به پنجاه و شش میلیون و هفتصد هزار تن رسیده است. ۴۹.۲ از جمعیت جهان از اینترنت بهره‌مند هستند و این شمار با شتاب در حال افزایش است. ایران با وجود تنگناهای اینترنتی مانند پالایش یا شتاب کم، بیست درصد از تراز جهانی بالاتر است و ۷۰ درصد ایرانیان از اینترنت برخوردارند که به اندازه چهل درصد کاربران اینترنتی کشورهای خاورمیانه است.[1]

جدایی فضای سایبر از دیگر پدیده‌ها، در آغاز، این چالش بنیادین را پیش می‌کشد که اگر یک سپهر نو دانسته می‌شود، پس چگونه اصول قانون اساسی بر آن فرمان می‌راند؟ از یک سو می‌توان گفت که قانون اساسی ایران به مانند دیگر قانون‌های اساسی

1. http://www.internetworldstats.com/stats5.htm.

یک پیمان ملی برای انسان‌ها به همراه ساختارها و نهادهای ظاهری و برگرفته از همین انسان‌ها است، تاب آن را دارد که بر زیست سایبری امروزین که دولت الکترونیک بخشی از آن است، فرمان براند و ضابطه‌مندش کند و از سوی دیگر می‌توان گفت سپهر نو خود نیاز به قانون اساسی جداگانه یا سندی هم‌تراز با آن دارد و با پیمانی که در فضایی جداگانه پدید آمده، ضابطه‌مند نمی‌شود.

چالش پسین آنکه اگر زمینه‌های سند اساسی برای فضای سایبر فراهم نیست یا اینکه این فضا از ریشه نیاز به قانون اساسی جداگانه ندارد؛ ولی همین اندازه که در زمان نگارش حقوق و وظیفه‌های پیش‌بینی شده در قانون اساسی، فضای سایبر در نگاه نبوده است، بنابراین چگونه قانون اساسی را باید به گونه‌ای فراگیر و درست به کار برد یا تفسیر کرد که فضای سایبر را نیز در بر بگیرد؟ در این میان جایگاه قانون اساسی در چینش سیاست‌ها و راهکارهای رویارویی با تهدیدهای سایبری چیست؟

در این نوشتار، انگاره بر این است که فضای سایبر، فراتر از پدیده‌های نو است ولی سپهری نو برای زندگی نو نیست. این فضا با دگرگونی در همه کارها، برنامه‌ها و شیوه‌های پیشین، زندگی فردی و جمعی شهروندان را در مسیر دیگری قرار داده است ولی چنان نیست که انسان‌های نو آفریده باشد بلکه خود به خدمت همین انسان‌ها و دولت‌هایی است که پیش از آن بوده‌اند. از این رو، قانون اساسی که برای تنظیم پیوند شهروندان و دولت و شهروندان با هم و دولت با دولت‌های دیگر است، همچنان بر این فضا فرمان می‌راند ولی چالش سازگار کردن اصول قانون اساسی بر فضای سایبر همچنان هست. قانون اساسی که چهره سنتی، ملی و غیر الکترونیک دارد چگونه می‌تواند در فرمان‌روایی بر فضایی نو، جهانی و الکترونیکی کامیاب باشد و فراتر از این، چگونه می‌تواند سیاست‌های کلان رویارویی با تهدیدهای سایبری که بزه سایبری، تروریسم سایبری و جنگ سایبری را در بر می‌گیرد را ترسیم کند؟ برای پرداختن به این چالش‌ها، در بخش نخست به پدیدارشناسی تهدیدهای سایبری پرداخته می‌شود و در بخش دوم نیز، راهکارهایی رویارویی با تهدیدهای سایبری در نگاه خواهد بود. در این دو بخش تلاش بر این است که گفته شود، قانون اساسی چگونه باید بر فضای سایبر فرمان براند و به طور ویژه، برجسته‌ترین رسالت خود را یعنی تراز امنیت ملی و آزادی‌های فردی را که در اصل نهم قانون اساسی پیش‌بینی شده است، با چه رویکردها و تدبیرهایی نمود دهد:

۱. تراز در پدیدارشناسی تهدیدهای سایبری

از دید نظم حقوقی کنونی که بر پایه اسناد الزام‌آور مانند قانون بنیاد گرفته است، همه تهدیدهای سایبری پیش‌بینی شده در قانون، تنها بزه سایبری خواهند بود؛ چرا که

تروریسم سایبری خود چهره‌ای از بزه سایبری است و همه آن رفتارهایی کـه گـاهی بـا عنوان جنگ سایبری یا یورش سایبری گفته می‌شوند، باز هم بزه سایبری‌اند. دلیل ایـن امر این است که هر چند، برخی یورش‌های سایبری با پشتوانه دولت‌ها و یا حتی برنامـه آنها در آسیب رساندن به دیگر کشورها است ولی با نبود نظم حقوقی بین‌المللی که آنهـا را جنگ بداند، همچنان با قانون‌های درون سرزمینی، بزه سایبری بـه شـمار مـی‌شـوند. ولی اگر این تهدیدها تنها از دید رفتار مغایر با قـانون کیفـری بررسـی نشـوند و در ایـن میان محور جستار بر این باشد که این تهدیدها چه نسبتی با امنیت ملـی و آزادی‌هـای فردی برقرار می‌کنند؛ در این حـال دسـته‌بنـدی تهدیـدها بـه بـزه سـایبری، تروریسـم سایبری و جنگ سایبری از دید قانون اساسی توجیه‌پذیر است.

شناخت تهدیدهای سایبری بر پایه سه ویژگی رفتار مغـایر قـانون کیفـری، وجـود انگیزه ضدیت با نظام سیاسی و انجام آن از سوی دولت بیگانه بـه نوبـت، بـزه سـایبری، تروریسم سایبری و جنگ سایبری را شکل می‌دهد. ولـی چیسـتی تهدیـدهای سـایبری گاهی چنین سنجه‌هایی را به هم می‌زند. بـه سـخن دیگـر، اگـر خاسـتگاه یـک تهدیـد سایبری روشن نباشد، بسیار دشوار است که مرز میان سه پدیده گفته‌شده روشن شود.

تهدیدهای سایبری از دید رفتار و پیآمدهای آن و بـزه‌دیـدگان بـه هـر انـدازه کـه گسترده باشند، این تاب را دارند که با هر سه پدیده بـزه، تروریسـم و جنـگ همخـوانی داشته باشند ولی به طور عادی می‌توان میان این سه پدیده در فضای سایبر مرز کشـید و از دید قانون اساسی بررسی کرد که در دنباله به آنها پرداخته می‌شود:

۱ـ۱. تهدید بر پایه رفتار

تهدیدهای سایبری، بسیار گسترده‌تر از رفتارهـای بزهکارانـه سـپهر بیرونـی‌انـد و از خردترین بزه‌ها می‌آغازد تا به کلان‌ترین آنها می‌رسد. بزه سایبری در بستری رخ مـی‌دهـد که سه ویژگی بنیادین دارد: نخست اینکـه فضـای سـایبر برسـاخته از نیروهـا و نهادهـای غیردولتی است و کنترل رسمی و دولتـی بـر آن بـا فضـای بیـرون سـنجش‌پـذیر نیسـت. خدماتی که در این فضا داده می‌شود بیشتر از سوی اشخاص حقوقی غیر دولتی است. دوم اینکه فضای سایبر پیوندیافته از رایانه‌ها و سامانه‌هـای بیشـماری در جهـان اسـت کـه بـه شیوه‌های گوناگون با هم دیگر در پیوندند. چهـره پیونـدی و جهـانی فضـای سـایبر نشـان می‌دهد که باز نیروی دولت نمی‌تواند بر آن فرمان براند. سوم اینکـه فضـای سـایبر، سـپهر خلوت‌ها است. بخشی از این ویژگی انتخابی و بخشی قهری است. از جهت انتخابی، فضـای سایبر به ویژه اگر تنگناهای بیرونـی نمـود بسـیار داشـته و از کنتـرل نیرومنـد دولتـی یـا اجتماعی نشان دهند، به عنوان فضای خلوت شهروندان در می‌آید و در این فضا هـر آنچـه

که در نبود کنترل‌های دولتی و اجتماعی می‌خواهند انجام دهد، انجام می‌دهند. از جهت قهری، پایه و مایه فضای سایبر بر اطلاعات است و چنانکه از عنوان اطلاعات بر می‌آید، حریم خصوصی یا محرمانگی، بنیادی‌ترین اصل امنیت در فضای سایبری و برجسته‌ترین ویژگی زندگی سایبری است. همه آنچه که در زندگی بیرونی با اطلاعات پیوندی ندارد، در فضای سایبر در جامه اطلاعات در می‌آیند و اطلاعاتی شدن همه چیز به طور قهری، چهره خلوت‌گونه و محرمانه محور بودن فضای سایبر را برجسته‌تر می‌کند.

این سه ویژگی بنیادین به همراه این انگاره که بخش بزرگی از بزه‌های سایبری که از رهگذر تارنماها و شبکه‌های اجتماعی مجازی رخ می‌دهند، بزه‌های خرد و سبک‌تر از بزه‌های برابر در سپهر بیرونی هستند، نشان می‌دهد که از دید قانون اساسی که بر آن اصل تراز امنیت و آزادی فرمان می‌راند، نمی‌توان نسبت به بزه‌های سایبری رویکردی سختگیرانه و سرکوب‌گرانه داشت. حتی اگر برخی بزه‌های سایبری در سطح جهانی و بسیار گسترده رخ دهند، ولی باز نمی‌توان با چند مورد بزه سایبری کلان در سنجش با انبوهی از بزه‌های سایبری خرد، این پندار را پیش کشید که بزه سایبری از جهت چیستی و پیآمد خطرناک است و باید به شیوه‌ای امنیت‌گرا با آن برخورد کرد.

بزه سایبری با یک تعارض دیگر نیز روبه‌رو است و آن اینکه اگر بزه سایبری برای جهان خود یعنی فضای سایبر خطرناک است، بنابراین باید پذیرفت که فضای سایبر، جهانی در عرض جهان فیزیکی و طبیعی ماست. در این حال، این فضا خود نیاز به قانون‌گذاری اساسی و عادی جداگانه دارد. ولی اگر قرار است با قانون اساسی کنونی و قانون‌های عادی به همراه برخی قانون‌های ویژه بزه‌های سایبری، هنجارپذیری و ضابطه‌گرایی در فضای سایبری دنبال شود، در این حال، بزه سایبری تهدیدی است که با قانون اساسی باید سنجیده شود. از دید قانون اساسی که پشتیبان اصل‌های چندی مانند اصل تراز امنیت و آزادی، اصل قانونی بودن، اصل آزادی بیان و مانند اینها است، بزه سایبری به مانند پدیده‌های تهدیدآور بیرونی نه توان تهدید جامعه ایرانی را دارد و نه به اندازه‌ای نگران‌کننده، شهروندان را با چالش روبه‌رو می‌کند. از این دید، انگاره بر این است که از یک سو رویارویی با بزه سایبری باید با بهره‌گیری از قانون‌های سنتی کنونی باشد و از سوی دیگر قانون‌گذاری کیفری ویژه این تهدیدها در جایی که قانون‌های سنتی، کارآمد نباشند یا با کاستی‌هایی همراه باشند، باید در سطح کمینه انجام شود.

هر چند قانون اساسی ایران با چهارچوب‌های کنونی خود راه را بر قانون‌گذاری گسترده و تدبیرهای افسارگسیخته در رویارویی با بزه‌های سایبری می‌بندد ولی این رویکرد تا جایی است که انگیزه مرتکب خطرناک نبوده و به رویارویی با نظام سیاسی یا جامعه برنخاسته باشد.

۱ـ۲. تهدید بر پایه انگیزه

پس از جنگ سرد و تک‌قطبی شدن پیشوایی در جهان و کم‌رنگ شدن جنگ‌های گسترده و جهانی، تروریسم به جانشینی از جنگ عاملی شد تا هم به عنوان تهدیدی بر ضد امنیت ملی درآید و هم اینکه ابزاری بر دولت‌ها در تهدیدتراشی برای یکپارچگی اجتماعی و پیشبرد هدف‌های خود باشد. پدیده تروریسم به چهره‌ها و گونه‌های گوناگون رخ نموده است؛ چرا که عامل‌های بسیاری در این چندگانگی دست دارند. از دولت‌های پشتیبان تروریسم گرفته تا سازمان‌های تروریستی و نیز از شخصیت تروریست گرفته تا توانایی‌های تروریست‌ها، همگی سبب شده گونه‌های تروریسم از زیر گرفتن انسان‌ها با خودرو تا بهره‌گیری از فضای سایبری و از لشگرکشی رزمی تا کنش‌های انتحاری و از آلوده‌کردن محیط زیست تا بهره‌گیری از جنگ افزارهای هسته‌ای و شکافت‌پذیر، همه را در بر بگیرد. از این رو شاید نتوان گفت که آغازه سده بیست و یکم روی‌آوری تروریست‌ها به فضای سایبر و ابزارهای اطلاعاتی باشد؛ چرا که برای تروریست‌ها به اندازه‌ای که ظاهرگرایی و نمود بیرونی و چشمی یورش‌ها و خشونت‌ها اهمیت دارد، یورش‌های سایبری برجستگی ندارد. تروریسم خشن و بیرونی مانند آنچه که در دو رخداد تروریستی در تهران در هفدهم خرداد ۱۳۹۶ دیده شد، هم تروریست‌ها توانستند هراس در دل شهروندان بیاندازند و در این زمینه پیام‌هایی به جهانیان برسانند و هم اینکه کشورهای گوناگون با ایران همدردی کردند. به سخن دیگر، تروریسم خشن حتی برای بزه‌دیدگان هم همراه با همراهی و همدردی است ولی تروریسم سایبری این ویژگی‌ها را ندارد.

تروریسم سایبری در سال‌های کنونی به سمت دولتی‌شدن پیش‌رفته و گفته می‌شود که با پشتیبانی دولت‌ها انجام می‌شود. همین امر، تروریسم سایبری را میان بزه سایبری و جنگ سایبری رها کرده و ماهیتی سرگردان به آن داده است. اقدام تروریستی سایبری در تعبیر ساده «همان بزه سایبری با قصد تروریستی است.»[1] برخی دیگر آن را «حمله غیر قانونی و یا تهدید به حمله توسط تروریست‌ها ضد رایانه‌ها، شبکه‌ها و برنامه‌های ذخیره‌شده در آنها، برای تهدید و یا اجبار دولت یا مردم جهت پیشبرد اهداف سیاسی و اجتماعی مرتکب»[2] تعریف کرده‌اند. بری کالین[3] که گفته می‌شود واژه سایبر تروریسم را برای نخستین بار پیشنهاد داده، آن را این گونه تعریف

1. Sieber, Ulrich; Brunst, Phillip, Cyberterrorism and other Use of the Internet for terrorist purposes; threat analysis and evaluation of international conventions, Counter-Terrorism Task Force, Council of Europe, Council of Europe Publishing, 2007, p. 16.
2. Brenner, Susan, "Cybercrime, Cyberterrorism and Cyberwarfare", International review of penal law: cybercrime, AIDP, vol. 77, 2006, p. 457.
3. Barry Collin

کرده است: «سوءاستفاده عمدی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه‌ای برای تحقق هدفی که موید یا تسهیل‌کننده مبارزه یا اقدام تروریستی است.»[1] برخی از نویسندگان نشانه‌ها و نتیجه‌های بیرونی کنش‌های تروریستی در فضای سایبر را نیز در تعریف خود گنجانده‌اند؛ به گفته کانوی[2] از نظریه‌پردازان آمریکایی در زمینه تهدیدهای سایبری، «تروریسم سایبری عبارت است از یورش عمدی و آگاهانه با انگیزه‌های سیاسی به وسیله گروه‌های فروملی یا عامل‌های پنهانی برضد اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده، که منتهی به خشونت بر ضد کسان غیر نظامی و دیگر هدف‌ها شود.»[3]

انجام اقدام تروریستی بر ضد شبکه‌ها، سیستم‌ها و اطلاعات یا بهره‌گیری از فضای سایبر برای تروریسم در جهان فیزیکی، به چهار دلیل برای تروریست‌ها مهم است: «پایین بودن هزینه‌های ارتکاب از فراهم ساختن رایانه گرفته تا طراحی برنامه‌های آماده‌سازی خدمات دروغین، دشواری در ردیابی یا دستگیری مرتکب، نبود رویارویی حضوری به دلیل نبود محدوده‌ای مشخص برای انجام اقدام تروریستی و دست‌آخر بود هدف‌ها و قربانیان گوناگون در یک زمان.»[4] از همین رو محدوده اقدام‌های تروریستی سایبری به اندازه‌ای گسترده است که رایانه در جهت ارتکاب آنها، هم نقش‌افزار را دارد و هم نقش هدف یا موضوع. رایانه زمانی افزار بزه است که تروریست‌ها از رهگذر آن، مرام و هدف‌های خود را تبلیغ می‌کنند یا با کمک آن شیوه انجام اقدام‌های تروریستی را می‌آموزانند.

رخنه‌گری غیر مجاز به سیستم رایانه‌ای[5] و انجام رفتارهای بزهکارانه در آن[6] از دیگر روش‌های شناخته شده برای ارتکاب اقدامات تروریستی است. در این روش مرتکب با نفوذ فنی (هک) یا با نفوذ شفاهی (مهندسی اجتماعی)[7] بخش‌های آسیب‌پذیر سیستم یا شبکه را شناسایی کرده تا در زمان مناسب آن را از کار بیندازد یا اطلاعات را دگرگون سازد یا از بین ببرد و یا اینکه مانع دسترسی به داده یا سیستم و در نتیجه کارآیی آنها

۱. فلمینگ، پیتر؛ استول، مایکل، «سایبر تروریسم: پندارها و واقعیت‌ها»، ترجمه اسماعیل بقایی هامانه و عباس باقرپور اردکانی، در: تروریسم، گردآوری و ویرایش علیرضا طیب، نشر نی، چاپ دوم، ۱۳۸۴، ص. ۱۵۳.

2. Conway

3. Ozeren, Suleyman, Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment, UMI Dissertation Services, University of North Texas, August 2005, p. 28.

4. Phair, Nigel, Cybercrime: The reality of the threat, E-security Publishing, Canberra, 2007. p. 146.

5. Hacking

6. Cracking

7. Social engineering

حملات مهندسی اجتماعی عبارت است از روند نفوذ به سیستم‌های رایانه‌ای از طریق کاربرد حیله‌های گوناگون در خصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط به موارد آسیب‌پذیر شبکه. ر.ک: هیأت مؤلفان و ویراستاران انتشارات مایکروسافت، فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، برگردان فرهاد قلی‌زاده نوری، کانون نشر علوم، چاپ اول، ۱۳۸۱، ص. ۶۸۸.

شود. جدا از مهندسی اجتماعی، هک صرف رخنه غیر مجاز به سیستم است که در گام نخست چهره کیفری ندارد اما خرابکاری رایانه‌ای[1] چهره کیفری هک است که مرتکب با قصد ربایش داده یا دگرگون ساختن آن یا جابجایی اطلاعات، به اقدام‌های بزهکارانه دست می‌زند و از این رو تروریست سایبری شخصی است که «با انگیزه‌های سیاسی و اجتماعی، مهارت‌های هک را به خدمت می‌گیرد.»[2]

اقدام‌های تروریستی سایبری روی‌هم‌رفته به چهار شیوه انجام می‌شوند: «الف ـ یورش به اطلاعات که همان دگرگونی یا از میان بردن محتوای فایل‌های الکترونیکی، سیستم‌های رایانه‌ای یا محتویات گوناگون موجود در آنها است. ب ـ یورش به زیرساخت که بر پایه آن، مرتکب، سخت‌افزارها، پایگاه‌های عملیاتی یا برنامه‌های محیط رایانه را مختل می‌کند یا از بین می‌برد. ج ـ معاونت فنی در ارتکاب که عبارت است از به کارگیری ارتباطات الکترونیکی برای فرستادن نقشه‌ها و طرح‌ها به منظور انجام یورش‌های تروریستی یا تحریک به انجام آنها یا توسل به سایر تسهیلات. د ـ افزایش یا ارتقای منابع مالی که به موجب آن تروریست‌ها با بهره‌گیری از اینترنت برای خشونت سیاسی یا دیگر رفتارها، به گرفتن کمک‌های مالی افراد یا سازمان‌ها می‌کوشند.»[3]

رکن روانی اقدام‌های تروریستی نیز همچون روش ارتکاب آنها گوناگون بوده و تروریست‌ها با انگیزه‌های چندی در فضای سایبر حضور می‌یابند که از جمله آنها می‌توان به «طرح‌ریزی (مانند گردآوری اطلاعات، تجزیه و تحلیل آنها و تجهیز به نرم‌افزار پیشرفته و کمک‌رسان)، تأمین یا تراکنش‌های مالی (همچون به دست آوردن کمک‌ها و بخشایش‌های هواخواهان، انتقال پول، پولشویی)، هماهنگی برای اجرای عملیات (مانند فرستادن نشانه‌ها یا رمزهای عملیات و بسیج نیروها)، اقدام‌های سیاسی (مانند بازگویی قصدها و هدف‌های سیاسی) و تبلیغ و آموزش انگشت نهاد.»[4] گابریل وایمن[5] پژوهشگر اسرائیلی، برای نشان دادن اندازه و شیوه‌های بهره‌گیری از فضای سایبر می‌گوید: «گروه‌های مسلمان در ابتدای فعالیت روی اینترنت دوازده سایت داشتند اما این تعداد در انتهای سال ۲۰۰۳ به ۴۰۰ سایت افزایش یافت. وی نشان داده که چگونه طراحان یازهم سپتامبر از اینترنت برای یافتن اطلاعات ارزشمندی به منظور هواپیماربایی از قبیل چگونگی سوخت‌گیری، تعداد مسافران ثبت شده و مانند آن بهره برداری کرده اند.»[6]

1. Cracking
2. Embar-Seddon, Ayn; op.cit. p. 16.
3. Ballard, James David; Hornik, Joseph; Mckenzie, Douglas, "Technological facilitation of terrorism", in: Cyberterrorism, Alan O'Day (ed), Ashgate publishing company, 2004, p. 59.
4. Cohen, Fred, "Terrorism and cyberspace", in: Cyberterrorism, Alan Oday (Ed), Ashgate publishing company, 2004, pp.150-151.
5. Gabrielle Weiman

۶. کلهر، رضا، «جهاد مجازی: ماهیت و چالش‌ها»، فصلنامه مطالعات منطقه‌ای جهان اسلام، شماره ۳۲، ۱۳۸۶، ص. ۳۱.

در نگاه نخست پدیده تروریسم سایبری آنچنان رویارویی با امنیت ملی دارد که می‌توان رویکرد قانون اساسی در گزینش سیاست‌های قانون‌گذاری، قضایی، پلیسی و حتی دفاعی در برابر آن را دانست. این رویکرد قانون اساسی را می‌توان از دو نگاه بررسی کرد. در نگاه نخست، تروریسم سایبری با انگیزه‌های سیاسی و برای رویارویی با دولت انجام می‌شود. چنین انگیزه‌ای به خودی خود تهدیدکننده بر ضد یک جامعه به شمار می‌رود. بنابراین تروریسم سایبری تنها امنیت ملی را نشانه نمی‌رود بلکه آزادی‌های فردی را نیز نادیده می‌گیرد. در برابر این پدیده، هم امنیت ملی و هم آزادی‌های فردی هر دو موضوع تهدید هستند و نمی‌توان گفت که قانون اساسی رویکردی همانند بزه سایبری داشته و به تراز امنیت و آزادی و پاسداشت فضای باز و آزاد در سپهری سایبری را دارد؛ به ویژه آنکه در تروریسم سایبری، دولت یا امنیت ملی موضوع غایی است و زیان راستین نمی‌بیند و این شهروندان و اطلاعات آنها است که موضوع مستقیم‌اند و از رخداد تروریستی زیان می‌بینند و در بدترین رخدادها اگر سامانه‌های خدمات‌رسان حیاتی و ضروری از کار بیفتند این شهروندان هستند که زیان برخاسته از تروریسم سایبری را حتی از جهت جان و مال به دوش می‌کشند.

در نگاه دوم، آزادی فضای سایبر در برابر تروریسم سایبری مفهومی پذیرفتنی برای کاربران نخواهد بود. آنچنان که در بزه سایبری، ممکن است گستره جرم‌انگاری و برنامه‌های پس از آن، بتواند فضای آزاد سایبر را بر کاربران تنگ کند، ولی تروریسم سایبری یک پدیده مشخص و در همان حال، نیروی تهدیدکنندگی‌اش روشن است. پس نمی‌توان جرم انگاری بزه سایبری و برنامه‌های قضایی و پلیسی پیونددار با آن را یک تهدیدکننده برای آزادی و ماهیت فضای سایبر دانست.

با این حال، رویکرد ترازمندی آزادی و امنیت در قانون اساسی و دیگر اصل‌های پشتیبان از امنیت ملی و آزادی‌های فردی، نگاهی بیشینه و فراگیر به بزه‌انگاری پدیده تروریسم سایبری ندارد. در برابر این پدیده باید نگران دو مسیر بود: نخست فربگی تروریسم سایبری و دوم اغراق‌آمیز بودن آن. فربگی تروریسم سایبری در پرتو فربگی خود تروریسم جای دارد. پس از جنگ سرد و به طور ویژه رخداد یازدهم سپتامبر ۲۰۰۱، تروریسم به عنوان برجسته‌ترین تهدید بر ضد دولت‌ها رخ نمود. بخشی از این تهدید راستین و بخشی نیز به جانشینی از جنگ به عنوان یک تهدید نمادین شناسانده شد. همین روی‌آوری جهانی به پدیده تروریسم سبب شد تا به مفهومی برابر با بزه و در عرض آن در حقوق کیفری بسیاری از کشورها روی نماید. در چنین بستری، قانون‌گذاری‌های کیفری گونه‌ها و شیوه‌های چندی را در زیر تروریسم جای دادند که بسیار فراتر از مفهوم نخستین خود درباره هراس‌افکنی از رهگذر خشونت بر ضد جان و

مال رفت. همین چگونگی در سال‌های کنونی درباره تروریسم سایبری تکرار شده است. تروریسم سایبری به جنگی از رفتارهای گوناگون گفته می‌شود که به طور مستقیم یا غیر مستقیم با رفتار تروریستی یا گروه تروریستی پیوند دارد و همه رفتارهایی که برضد رایانه یا از رهگذر رایانه است را در بر می‌گیرد. بنابراین می‌توان دید که دولت‌ها بسیار فراتر از ممنوع انگاری هسته مرکزی تروریسم سایبری یعنی همان چه که بر ضد امنیت ملی است، فراتر رفته‌اند و از همین در می‌توان دید که هر قانون‌گذاری یا سیاست قضایی و پلیسی بر ضد تروریسم سایبری نیز نمی‌تواند با قانون اساسی سازگار باشد.

نگاه اغراض‌آمیز به تروریسم سایبری نیز بیان دیگری از این خوانش است که ممنوع انگاری این پدیده نمی‌تواند بدون مرز باشد. همانند بزه سایبری، این پدیده نیز در پایان بر ضد اطلاعات و سامانه‌ها رخ می‌دهد و چنان نیست که ارزش‌های بیرونی و هنجارهای سنتی را به طور مستقیم تهدید کند. در رخداد یورش سایبری از رهگذر باج‌افزار در آوریل ۲۰۱۷، به بیمارستان‌های انگلستان که در زمره نهادهای خدمات‌رسان ضروری به شمار می‌روند، رایانه‌ها کنار گذاشته شده و پزشکان و کارمندان بیمارستان‌ها به طور دستی به کار خود پرداختند. هر چند این گفته برای جایی است که تهدید سایبری شناسایی شده یا خود را شناسانده باشد یا هنوز خطری جانی پدید نیاورده باشد ولی به طور کلی تهدیدهای تروریستی سایبری همانند بزه سایبری به گونه‌ای نیست که بتواند همانند یک رفتار خشن، ارزش‌ها و هنجارهای بیرونی را به چالش بکشد.

۱ـ۳. تهدید بر پایه قدرت

امروزه قدرتمندی یک نهاد بر پایه اطلاعاتی است که دارا می‌باشد. بر این اساس، هر چه توانایی اخذ اطلاعات بالاتر رود، قدرت نیز افزون می‌گردد. این قدرت می‌تواند در عرصه سایبر پدیدار گردد. لذا، برخی قدرت سایبری را «توانایی استفاده از فضای سایبر برای خلق مزیت‌ها و تأثیر بر حوادث محیط‌های عملیاتی دیگر و بیان و کاربرد ابزارهای قدرت»[1] تعریف نموده‌اند. با توجه به اهمیت این قدرت، تحصیل آن، باعث ایجاد جنگ سایبری می‌گردد. جنگ سایبری برجسته‌ترین تهدید سایبری در زمان ما به شمار می‌رود. این تهدید به پشتوانه دولت یا دولت‌های بیگانه بر ضد سامانه‌های رایانه‌ای داخلی انجام می‌شود و سنجه بنیادین برای جداسازی این پدیده از تروریسم سایبری و بزه سایبری، پیونددار بودن با دولت یا دولت‌های بیگانه است.[2] هم گفته‌های مقام‌های

۱. عباسی، مجید؛ مرادی، حسین، «جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه»، فصلنامه مجلس و راهبرد، سال بیست و دوم، شماره ۸۱، بهار ۱۳۹۴، ص. ۴۵.

۲. هر چند نظر مخالف نیز وجود دارد و جنگ سایبری را وابسته به دولت تلقی نمی‌نمایند. برای مثال برنیک در کتاب بزه سایبری و جنگ سایبری، جنگ سایبری را این گونه تعریف می‌نماید: «اقدامات تدافعی و تهاجمی

برخی کشورها و همه رویه دولت‌ها نشان می‌دهد که جنگ سایبری نه تنها جایگزین جنگ‌های سنتی و خشن شده است بلکه مفهومی بسیار عام‌تر یافته به گونه‌ای که این جنگ ممکن است از سوی دولتی باشد که در پیوندهای سیاسی در زمره دولت‌های دشمن به شمار نرود. به گفته وزیر دفاع فرانسه در سال ۲۰۱۶، ۲۴ هزار یورش سایبری علیه اهداف دفاعی این کشور خنثی شده است. به گفته وی شمار چنین یورش‌هایی هر سال دو برابر شده است و زیرساخت‌های داخلی فرانسه نظیر آب، برق، ارتباطات و حمل و نقل در معرض خطر واقعی حملات سایبری قرار دارند.[1]

پیوند جنگ سایبری با ایران بسیار برجسته‌تر است. در سال‌های کنونی گفته شده که ایران همواره در جنگ سایبری بوده است. گاهی بر ضد این کشور یورش شده و ایران نیز در مقام دفاع سایبری برآمده است. در آذر ۱۳۹۵، چند شرکت غربی امنیت اطلاعات و همین‌طور مقام‌های سعودی گفتند که رایانه‌های چند نهاد دولتی در عربستان سعودی هدف حمله سایبری قرار گرفته است. در این یورش، سازمان هواپیمایی کشوری در عربستان نیز یکی از اهداف این حمله بوده و با پاک شدن اطلاعات حساس، فعالیت‌های این سازمان برای چند روز مختل شده است. گفته شده که این یورش سایبری، با ویروس شامون انجام گرفته است که در سال ۲۰۱۲ عامل وایپر آن رایانه‌های شرکت نفتی سعودی آرامکو را هدف گرفت و اطلاعات حدود ۳۰ هزار کامپیوتر را پاک کرد.

نمی‌توان چنین جنگی در فضای تبادل و نگه داشت اطلاعات را نادیده گرفت؛ چرا که پیش از آن دو یورش مهم سایبری (استاکس نت و فلیم) بر ضد سامانه‌های حیاتی در ایران به ویژه بر ضد سامانه‌های رایانه‌ای بنیادهای هسته‌ای، زیان‌های گسترده‌ای را به بار آورده بود. جنگ سایبری بر ضد ایران به ویژه نسبت به برنامه هسته‌ای، گرایش آشکار دمکرات‌ها از جنگ سنتی به جنگ سایبری را نشان می‌دهد. اینان، جنگ سایبری را شیوه مناسب‌تر و کارآمدتر برای شکست برنامه‌های نظامی و هسته‌ای ایران می‌دانستند؛ چندان که روزنامه نیویورک تایمز به نقل از یک فیلم مستند که با مقام‌های نظامی و اطلاعاتی آمریکا است، گزارش داده که دولت آمریکا در صورت شکست تلاش‌های دیپلماتیک برای مهار برنامه هسته‌ای ایران، طرحی گسترده برای حمله سایبری به تاسیسات اتمی این کشور را داشت. بنابه این گزارش برنامه «نیترو زئوس» با هدف فلج‌کردن سیستم‌های دفاع ضدهوایی، سیستم‌های ارتباطی و بخش‌های مهم شبکه برق این کشور طراحی شده بود که با امضای توافق اتمی کنار گذاشته شد. براساس

نهادها (عمومی و خصوصی) یا گروه‌ها برای تحصیل یا/ و بهره از اطلاعات با یاری ICT به منظور تفوق بر رقیب در جنگ»:

Bernik, Igor, Cybercrime and cyber warfare, John Wiley & Sons, 2014, p. 69.

1. http://www.bbc.com/persian/world-38547328.

این گزارش طرح را پنتاگون آماده کرده بود تا باراک اوباما رئیس جمهور آمریکا گزینه‌های دیگری غیر از جنگ علیه ایران داشته باشد. به گفته نیویورک تایمز: «مقام‌ها می‌گویند در اوج آن برنامه، طراحی نیترو زئوس با شرکت هزاران خدمه نظامی و اطلاعاتی آمریکا، صرف ده‌ها میلیون دلار هزینه و تعبیه تجهیزات الکترونیکی در شبکه‌های کامپیوتری ایران همراه بود». در همین حال سازمان‌های اطلاعاتی آمریکا طرحی جداگانه برای انجام حمله‌ای سایبری برای از کار انداختن تاسیسات غنی‌سازی فردو ایران در دل کوهی در نزدیکی قم آماده کرده بودند. با این حال طراحان هشدار داده بودند که چنین طرحی در صورت اجرا به طور بالقوه می‌تواند تأثیری قابل توجه بر غیر نظامیان داشته باشد، به خصوص اگر برق و ارتباطات بخش‌های وسیعی از ایران قطع شود.[1]

تا پیش از بنیاد گرفتن مقرره‌های بین‌المللی درباره جنگ، دو گزاره بنیادین در اندیشه‌های فلسفی بر شیوه جنگ‌آوری سایه انداخته بود: یکی دادگرانه بودن توسل به جنگ و دومی دادگرانه بودن رفتارهای جنگی. گزاره نخست درباره شیوه آغاز جنگ بود که باید دارای ویژگی‌های زیر باشد: «یک ـ جنگ باید از سوی یک قدرت قانونی آگاهی داده شده و آغاز گردیده باشد. دو ـ سبب پیش‌دستی در جنگ باید دادگرانه باشد. سه ـ جنگ واپسین دستاویز باشد. چهار ـ برای آغازگر، به طور بخردانه، دورنمای پیروزی وجود داشته باشد. پنج ـ خشونت به کار رفته باید سازگار (متناسب) با اندازه پایداری طرف درگیر باشد.»[2] گزاره دوم نیز درباره چگونگی رفتار در جنگ است که دارای دو اصل است: «اصل فرق‌گذاری که بر پایه آن جنگ تنها نسبت به هدف‌های قانونی روا داشته شود. اصل تناسب که با دستاویز آن، شیوه‌های خشونت‌آمیز، آسیب بیشتری در سنجش با گناه اصلی طرف درگیر، به بار نیاورد.»[3] به ویژه اصل نخست که دربردارنده یورش نبردن به غیر نظامیان است، برجسته‌ترین سنجه جداسازی جنگ و تروریسم است. از این ویژگی‌ها این پیامد به خوبی دانسته می‌شود که جنگ یک پدیده فیزیکی است و بر روی زمین، دریا و هوا که روی هم‌رفته سرزمین یک کشور یا فراتر از آن قابلیت‌های دیداری کره زمین است، نمود دارد. یکی دیگر از دلیل‌هایی که نشان می‌دهد «حقوق جنگ بر تهدیدهای سایبری فرمان نمی‌راند، این است که فضای سایبر بخشی از قلمرو سرزمینی یک کشور دانسته نمی‌شود. یورش به رایانه‌های یک کشور، ویژگی‌های بنیادین یورش به سرزمین کشور دیگر را دارا نیست تا بتواند در سایه حقوق جنگ جای بگیرد.»[4]

1. http://www.bbc.com/persian/iran/2016/02/160216_u04_nyt_cyberattack_iran_nuclear.
2. Coady, Tony, "Terrorism, Just war and supreme emergency", in Terrorism and Justice: Moral argument a threatened world, Tony Coady and Michael O Keefe (Eds), Melbourne University Press, 2002, p.11.
3. Ibid.
4. Beard, Jack, "Legal phantoms in cyberspace: The problematic status of information as a weapon and a target under international humanitarian law", Vanderbilt Journal of Transnational Law, vol. 47, 2014, p.96.

روشن است که قانون اساسی ایران تعابیری مانند جنگ سایبری یا نبرد سایبری را تهدیدی بر ضد ارزش‌های بنیادین کشور مانند تمامیت سرزمینی و استقلال نمی‌داند. می‌توان از تعبیر اعلان جنگ که از اختیارهای مقام رهبری است (بند ۵ اصل ۱۱۰)، پیآمد جنگ و اشغال نظامی بر انتخابات مجلس شورای اسلامی (اصل ۶۸)، برقراری محدودیت‌های ضروری در حالت جنگ و شرایط اضطراری (اصل ۷۹) و نیز به کارگیری دفاع در همین معنای بیرونی و فیزیکی به ویژه در اصل یکصد و پنجاه و یکم درباره توانایی دفاع مسلحانه از کشور و نظام جمهوری اسلامی ایران از سوی افراد، فهمید که نگرش قانون اساسی به پدیده بزرگی چون جنگ یا پدافند در برابر آن نمی‌توان به تهدیدهای سایبری دولت یا دولت‌های بیگانه کاهش یابد.

در برابر، جنگ سایبری که در زبان کشورها بیشتر به دفاع سایبری برجسته شده است، بخشی از رزم نهادهای نظامی یک کشور شده است. بیشتر کشورها در رویه خود پذیرفته‌اند که در جنگ، عامل دست‌اندازی دولت بیگانه برجستگی دارد و نه خشونت مادی یا دست به جنگ افزار بردن. بیشتر کشورهای جهان مانند ایالات متحده، روسیه، چین و انگلستان، در درون نهادهای رزمی خود، بخشی را به دفاع سایبری واگذار کرده‌اند. ایران نیز از سال ۱۳۹۰، قرارگاه دفاع سایبری را بنیاد نهاده که واکنشی به یورش‌های سایبری بزرگ مانند استاکس نت بوده است. از این فراتر وزارت دفاع ایالات متحده در گزارشی در سال ۲۰۱۱، یک قاعده‌گذاری نو در زمینه یورش‌های سایبری داشته است و آن اینکه یورش سایبری به سامانه‌های رایانه‌ای حیاتی این کشور، اعلان جنگ به شمار می‌رود. به گزارش وال استریت‌جورنال، پنتاگون «خرابکاری رایانه‌ای برخاسته از خواست کشور دیگر را به عنوان رفتار جنگی به شمار می‌آورد که می‌تواند پاسخ نظامی فیزیکی را به همراه داشته باشد.»[1]

هر چند خوانش قانون اساسی در زمانی که هنوز فضای سایبر بنیاد نگرفته بود؛ بر این پایه که جنگ سایبری یا پدافند سایبری را در بر بگیرد کوشش گمان‌آور است ولی نمی‌توان سیاست‌گذاری در زمینه دفاع سایبری را از قانون اساسی دور دانست. به طور روشن اصل یکصد و هفتاد و ششم، وظیفه‌هایی را به شورای عالی امنیت ملی می‌دهد که می‌تواند به گونه‌ای گواهی بر همسان‌سازی دفاع سایبری با دفاع سرزمینی باشد. «تعیین سیاست‌های دفاعی ـ امنیتی کشور در محدوده سیاست‌های کلی تعیین شده از طرف مقام رهبری.» و «هماهنگ نمودن فعالیت‌های سیاسی، اطلاعاتی، اجتماعی، فرهنگی و اقتصادی در ارتباط با تدابیر کلی دفاعی ـ امنیتی» به عنوان دو وظیفه بنیادین شورا از

1. https://www.wsj.com/article/sb10001424052702304563104576355623135782718.

جهت مفهوم بخشی به «تدابیر دفاعی ـ امنیتی» می‌تواند با دگرگونی‌های نو در حوزه نبرد سایبری نیز همخوانی داشته باشد.

۲. تراز در رویارویی با تهدیدهای سایبری

تراز میان امنیت و آزادی در گام رویارویی با تهدیدهای سایبری که به کیفرگذاری، کیفرگزینی، تعیین یا اعمال ضمانت اجراهای غیر کیفری و واکنش‌های پلیسی می‌پردازد، برجستگی بسیار بیشتری در سنجش با تهدیدانگاری دارد؛ ولی تهدیدانگاری به طور روشن به ضمانت اجراها و اقدام‌های قضایی و پلیسی جهت می‌دهد. به سخن دیگر، تعیین یا اعمال ضمانت اجراها در طول شناسایی تهدید جای دارد و به همان اندازه که تهدید، بزرگ و نگران‌کننده شناسانده شود، ضمانت اجراها نیز سخت‌تر خواهند بود. به هر اندازه که در سیاست و فرهنگ یک ملت، رویکرد منفی با فضای سایبر بنیاد بگیرد و از در دشمنی به آن نگریسته شود؛ همین فضا در تعیین و اعمال ضمانت اجرا و حتی در باور و گرایش ضابطان دادگستری، دادرسان و مجریان قانون نیز پدید می‌آید.

درباره رویارویی با تهدیدهای سایبری در ایران نمی‌توان به طور قطعی پذیرفت که آنچه در سیاست‌های کلان و تبلیغی درباره این تهدیدها هست و یا حتی در قانون‌گذاری‌ها یا مقرره‌گذاری‌ها بازتاب داشته است، در سیاست‌های قضایی، پلیسی و اجرایی نیز نمود داشته است. فضای سایبر و به طور ویژگی شبکه‌های اجتماعی مجازی، سپهری است که همین مجریان نیز از آن برخوردارند و حتی اگر نهادهای حکومتی، کارمندان خود را از فضای سایبر در محیط کاری بی‌بهره کنند یا تنگناهایی پدید آورند ولی برای اینان، بهره‌گیری از فضای سایبر فرق با دیگر شهروندان ندارد. بنابراین نخستین چالش در رویارویی با تهدیدهای سایبری، همین دوگانگی برنامه و عمل است. برنامه بر پایه دیده‌بانی فضای سایبر و تنگ نظری درباره آن است ولی عمل نشانگر نگرش باز درباره تهدیدهای سایبری است. این دوگانگی خود سبب می‌شود تا رویارویی با تهدیدهای سایبری از دریچه قانون اساسی ایران بررسی گردد که به راستی چه برخوردی در این راستا توجیه‌پذیر و بخردانه است؟

قانون اساسی ایران به طور روشن نشان نداده است که یک قانون‌گذار یا مقرره‌گذار تا چه مرزی می‌تواند آزادی‌ها را در تنگنا بگذارد و به چه اندازه می‌تواند در برابر پدیده‌ها یا بسترهای نو، هنجارهای نو پدید آورد و ارزش‌هایی بدون پیشینه بشناساند. با این حال نمی‌توان از ویژگی قانون اساسی در این زمینه چشم پوشید: نخست، اصل قانونی‌بودن و اصل قانون‌گذاری از سوی مجلس شورای اسلامی. این دو اصل در کنار هم

معنا می‌یابند. هر ضابطه‌گرایی و هنجارگذاری با قانون به دست می‌آید و هر قانونی نیز تنها از سوی مجلس شورای اسلامی گذارده می‌شود. هیچ مصوبه یا دستور جدا از قانون برای شهروندان، الزام پدید نمی‌آورد مگر در موردهای استثنایی که قانون اساسی گفته است مانند موردهای استثنایی مصوبه‌های مجمع تشخیص مصلحت نظام در همان زمینه که شایستگی دارد یا مصوبه‌های شورای عالی امنیت ملی در راستای چرایی خود و در همان گستره صلاحیت‌اش. با این حال اگر قانون عادی سنجه‌ای برای پیش‌بینی هنجارها در فضای سایبر است و این کار نیز تنها در شایستگی مجلس شورای اسلامی است، چه پایندانی است که قانون و قانون‌گذار به گستردگی و زیاده‌خواهی در راستای محدود کردن آزادی‌ها در فضای سایبر نکوشند؟ چه پایندانی است که همین قانون‌گذار نهادها یا شیوه‌هایی نو برای دیده‌بانی سختگیرانه در فضای سایبر پدید نیاورد، مانند آنچه که درباره کمیته پالایش در قانون جرایم رایانه‌ای ۱۳۸۸ آزموده شده است. این چالش، اصل دوم را پیش می‌کشد که همانا اصل اساسی بودن واکنش در برابر تهدیدهای سایبری است؛ یعنی سازگاری برنامه‌ها و اقدام‌ها با اصل‌های قانون اساسی.

قانون اساسی ایران، نگرشی دوگانه به مفهوم آزادی دارد. در نگاه کلان با به‌کارگیری تعابیری مانند «امت» یا «حقوق ملت» و با نگرشی ویژه به تفکیک‌ناپذیری آزادی‌های مشروع و امنیت ملی و استقلال سرزمینی، اساساً قائل به جمعی‌بودن حقوق و آزادی‌های فردی است. در یک نگرش بومی و دینی، فرد به تنهایی در نظام اسلامی جایگاه برجسته ندارد و همه در پیکره یکتا و در چهره ملت یا امت نمود دارند. از این دید، شاید رویکرد فردگرایانه نااستوار و کم‌رنگ می‌شود ولی در برابر، چهره یکسان و برابر برای همه شهروندان از مقام‌های سیاسی و حاکمیتی گرفته تا افراد عادی، نشان می‌دهد که در قانون اساسی ساختار هرمی یا پیوند طولی در برخورداری از حقوق و آزادی‌ها نیست. این چگونگی را می‌توان همچنین در برخی اصل‌ها مانند بند دوم اصل چهارم، که به بالا بردن سطح آگاهی‌های عمومی در همه زمینه‌ها با استفاده صحیح از مطبوعات و رسانه‌های گروهی و وسائل دیگر می‌پردازد، پرداخت. در این اصل، افزایش آگاهی‌های همگانی خود سنجه‌ای برای پیشبرد رسانه‌های مجازی و تراکنش‌های اطلاعاتی است. در اینجا «عموم» بیانی از همان جمع‌محوری «حقوق ملت» یا «ملت واحده» یا تفکیک‌ناپذیری آزادی‌های مشروع و امنیت ملی است. همچنین حق مردم در اعمال امر به معروف و نهی از منکر نسبت به دولت در اصل هشتم قانون اساسی بازتاب دیگری از جداناپذیری ملت از دولت است. در این اصل، تنها این دولت نیست که شهروندان را از منکر باز می‌دارد و یا به معروف وادار می‌کند و نیز تنها این شهروندان نیستند که برای همدیگر به امر به معروف و نهی از منکر دست می‌یازند؛ بلکه همین

حق را شهروندان به دولت که همه حاکمیت را در بر می‌گیرد، دارند. شهروندان به عنوان یک کل، این حق را دارند که دولت را در راهی بخواهند که قانون اساسی نشان می‌دهد. جدا از اینکه شهروندان می‌توانند قانون‌گذار یا نهادهای دیگر را که در رویارویی با تهدیدهای سایبری به ضابطه رفتار می‌کنند، را نهی از چنین منکری کنند، ولی فراتر از آن رویکرد جمع‌محورانه گزاره امر به معروف و نهی از منکر است که نشان می‌دهد در رفتار برخی نهادهای ویژه یا قشرهای خاص از شهروندان آن بر این قاعده یا حق چیره شده‌اند و اعمال آن را تنها حق خود می‌پندارند در حالی که چنین نیست و از دید قانون اساسی، حقی جمع‌محور است. چنین حقی نشان می‌دهد که در دید قانون اساسی، در امر به معروف یا نهی از منکر، کسی یا نهادی یا حتی دولت و حاکمیت دست بالاتر در اعمال آن ندارد و برای همگان این حق پیش‌بینی شده است. این خود نشانگر جداناپذیری مفهوم دولت و ملت در قانون اساسی و جایگاه برابر آنها است که می‌تواند از قیم سالاری و پدرمداری در برخورد با شهروندان جلوگیری کند.

در نگاه خرد، قانون اساسی به رویکرد فردمحورانه حقوق و آزادی‌های فردی نیز روی کرده است. پیش‌بینی حقوقی در زیر عنوان «حقوق ملت» همسان با آنچه در اسناد حقوق بشر آمده است، نشان می‌دهد که قانون اساسی به آزادی‌های تک‌تک شهروندان نیز روی کرده است. تعبیر «آزادی‌های مشروع» در اصل نهم قانون اساسی که دولت حتی با وضع قانون نیز نمی‌تواند به بهانه امنیت ملی آنها را در تنگنا بگذارد، خود بیانی از همین آزادی‌ها است که در بخش «حقوق ملت» پیش‌بینی شده است. جدا از این با نشانه «رعایت حقوق انسانی غیر مسلمانان» که در اصل چهاردهم و درباره شیوه برخورد دولت مسلمان ایران با نامسلمانان آمده این گزاره را پیش می‌کشد که حقوق انسانی مسلمانان اگر نه به اولویت ولی به نشانه همین اصل، در نگاه قانون اساسی بوده است و باز هم آنچه برجسته‌تر از همه پیش کشیده می‌شود؛ تراز میان آزادی‌های فردی مسلمانان و غیر مسلمانان و امنیت ملی است. این تراز همچنانکه در بیان تهدیدهای سایبری به عنوان یک الگو و راهنما نمود دارد در چینش تدبیرهای رویارویی با این تهدیدها نیز همین ویژگی را دارد. با این رویکرد در دنباله به جهت‌های رویارویی با تهدیدهای سایبری از دید قانون اساسی پرداخته می‌شود:

۲ـ۱. رویارویی مرتکب محور

رویارویی با مرتکب یا پدید آورنده تهدید سایبری، برجسته‌ترین چالش نظام پیگرد و قضاوت است. در اینجا به طور روشن، امنیت‌گرایی و آزادی‌گرایی با هم سر ناسازگاری دارند. مرتکب تهدید سایبری و به طور ویژه بزه سایبری گستره‌ای وسیع از اشخاص

حقیقی و حقوقی را در بر می‌گیرد که با روی آوردن به این نکته کـه بـه هـر انـدازه کـه بهره‌گیری از فضای تبادل اطلاعات افزایش می‌یابد، شمار مرتکبان هم بیشـتر مـی‌شـود؛ پس نباید چالش تهدید در فضای سایبر را با مرتکب گره زد.

مرتکب تهدید سایبری در سنجش با تهدید سنتی، سه ویژگی مهـم دارد: نخسـت اینکه نوجوان یا جوان است. بهره‌گیری از ابزارهای الکترونیکی پیوند تنگـاتنگی بـا سـن افراد دارد و به هر اندازه که یـک فـرد بـر ابزارهـای الکترونیکـی چیـره شـود، گـزینش رفتارهای تهدیدآمیز نیز برای وی شدنی خواهد بود. در برابر، نـرخ تهدیـدها و بـزه‌هـای سنتی در فضای بیرون به سمت میانسالی می‌رود؛ چرا که تهدیدهای سایبری بیشـتر بـر پایه توان ذهنی‌اند و تهدیدهای بیرونی بیشتر پایه توان اندامی. به همین دلیل، هر چنـد که برخی از بزه‌های عادی سایبری به راستی نیاز به استعداد و پیچیـدگی رفتـار ندارنـد ولی به طور کلی، تهدید سایبری از کسانی سر می‌زند که سر وکارشان بیشتر با ابزارهای الکترونیکی است.

دوم اینکه اشخاص حقوقی است. هدف اشخاص حقوقی از بنیادگیری و فعالیت بـه ویژه شرکت‌های تجاری، سود و شهرت همگانی است و همین نیز انگیزه‌ای نیرومند برای انجام بزه‌های سایبری است. جدا از این اشخاص حقوقی، بازیگران اصلی فضای سـایبری از خدمات‌دهی تا میزبانی و از اطلاع‌رسانی یا بازاریـابی و تبلیـغ‌انـد؛ از ایـن رو، مرتکـب بخش بزرگی از بزه‌های سایبری به ویژه بزه‌های کلان و پیچیده، اشخاص حقوقی‌اند.

سوم اینکه، ناکردگان بزه در فضای سنتی‌اند. هر چند آماری در زمینه هم‌پوشـانی ارتکاب بزه سایبری و بزه سـنتی در دسـت نیسـت ولـی بـا بررسـی پرونـده و رخـدادها می‌توان این فرضیه را داشت که مرتکبان تهدیدهای سایبری، توان یا اراده یـا گسـتاخی بایسته برای انجام بزه‌های بیرونی را ندارند. اینان کسانی‌اند کـه هنجارهـای اجتمـاعی و کنترل‌های قهری بیرونی را پاس می‌نهند ولی در فضای سایبر یا باور به ایـن کنتـرل‌هـا ندارند یا اینکه فضا را برای انجام تهدید به دور از کنترل‌کننده‌ها، مناسب می‌بینند.

سه ویژگی نوجوانی و جوانی مرتکب، اعتباری بودن آن به همراه نقش کـم رنگـش در هنجارشکنی‌های بیرونی و فیزیکی، نشان از این دارد که رویارویی با مرتکـب تهدیـد سایبری نباید بر پایه رویکرد سخت‌گیرانه پلیسی و سرکوب‌گرانه قضایی باشد. در اینجـا همان رویکرد جداناپذیری امنیت و آزادی قانون اساسـی مطـرح مـی‌شـود کـه مرتکـب تهدید سایبری را نمی‌توان به تنهایی از دریچه تهدید و با رویکرد امنیت گرایی سنجید.

پس از تصویب و لازم‌الاجرا شدن قانون جرایم رایانه‌ای ۱۳۸۸، یکی از مهـم‌تـرین خرده‌هایی که بر آن گرفته می‌شود، مدارا با مرتکب اسـت. گفتـه مـی‌شـود کـه چنـین قانونی از جهت کیفر بازدارندگی نداشته و ضـمانت اجراهـای سـبک، انگیـزه انجـام بـزه

سایبری را بالا می‌برد. چنانکه از میان ۱۹ ماده نخست این قانون تنها پنج جرم دارای حبس بالاتر از درجه شش می‌باشند. (مواد ۷۴۱، ۷۳۹، ۷۳۴، ۷۳۵، ۷۳۱) ولی در برابر، قانون‌گذار عادی به چه اندازه می‌تواند در این زمینه سخت‌گیر باشد و شهروندان درگیر با فضای مجازی و شبکه‌های اجتماعی مجازی که انجام بزه‌های پیش‌بینی شده در قانون‌های کنونی، از بیشتر این شهروندان انتظار می‌رود، سرکوب کند؟ در اینجا باید خوانشی دیگر از تراز امنیت‌گرایی و آزادی‌گرایی در فضای سایبر با رویکرد اصل نهم قانون اساسی گفته شود. نگاره بر این است که فضای سایبر، سپهر آزادی‌ها است و امنیت‌گرایی در آن نه از جهت مبنا و نه از لحاظ بود شرایط استثنایی، توجیه‌پذیر نیست:

هم امنیت و هم آزادی، پاره‌های بنیادین و حذف ناشدنی زندگی فردی و اجتماعی انسان‌هاست و به اندازه‌ای در هم تنیده‌اند که نمی‌توان مرز روشنی میان آنها کشید. در زندگی فردی، آزادی هر کس به معنای داشتن امنیت است و امنیت داشتن نیز همان آزادی است. آزادی و امنیت، هر دو برای فرد ارزش و هدف‌اند و پاره‌ای از چیزی نیستند تا به دستاویز آن از هم جدا گردند، بلکه جداناپذیری این دو به دلیل پیوستگی‌اشان با خواست‌ها و آرمان‌های انسان‌هاست. از این روست که گفته‌اند: «آزادی، فی‌نفسه یکی از ارزش‌هاست و قابل فروکاستن به ارزش‌های مادی نیست. اگر آزادی را برگزینیم، باید آماده باشیم با آن بمیریم؛ زیرا هیچ ضمانتی نیست که آزادی پیروز خواهد شد.»[1]

در برابر، در زندگی باهمادی (اجتماعی) که پای دولت به میان کشیده می‌شود؛ جداناپذیری امنیت و آزادی به عنوان پاره‌های فرمانروایی ملت ـ دولت معنا می‌گردد. در اینجا با باور به اینکه «آزادی ماهیتی میان‌فردی و میان‌سازمانی دارد نه درون فردی و درون‌سازمانی»،[2] آزادی تنها در زندگی اجتماعی و در کنار امنیت اجتماعی و امنیت ملی معنا می‌یابد و چون همه اینها پایه‌های فرمانروایی مردم‌سالار است، از همدیگر جداناپذیرند.

نسبت جداناپذیری در پی روشن ساختن پیوند آزادی و امنیت در سطح اجتماعی و ملی است نه فردی؛ چه از دید فردی، گمانی در اینکه امنیت و آزادی در هم تنیده‌اند، نیست ولی در دید اجتماعی، امنیت و آزادی در حالی از هم جداناپذیر می‌گردند که به عنوان ارزش و هدف مستقل شناسانده نشوند، بلکه تنها به جهت اینکه مایه‌های استواری حاکمیت ملت‌ها و دولت‌ها هستند، خویشاوند همدیگر گشته‌اند. با این حال نسبت جداناپذیری امنیت و آزادی، پیوند ناگسستنی با حاکمیت داشته که می‌توان گفت در سه جا نمود پیدا می‌کند: نخست، در تهدیداتی که بر ضد آنهاست همسان‌اند.

۱. شی یرمر، جرمی، اندیشه سیاسی کارل پوپر، ترجمه عزت‌الله فولادوند، چاپ دوم، نشر ماهی، ۱۳۸۶، ص. ۴۸.

2. Day, Patrick, "Is the concept of freedom essentially contestable?", Philosophy, Vol. 61, no. 235, 1976, p. 117.

دوم، پایه‌های مشترکی برای پیشبرد حقوق بشر به شمار می‌روند و سوم اینکه به عنوان ابزارهای همسان یک فرمانروایی قانون‌مند و مردم‌سالار قرار می‌گیرند.

عامل نخست پیوند جداناپذیری امنیت و آزادی در این است که این دو، تهدیدها و آفت‌های همسانی دارند و فرقی نمی‌کند که این تهدیدها از سوی طبیعت باشند مانند زمین‌لرزه و خشک‌سالی یا از سوی انسان همچون جنگ و آشوب؛ در هر حال امنیت رخت بر می‌بندد و آزادی به تنگنا می‌افتد. کن بوث[1] تهدید را عامل برجسته نزدیکی امنیت و آزادی می‌داند. به باور وی، «امنیت به معنای نبودن تهدید است. آزادی یعنی رها کردن مردم از محدودیت‌ها و زنجیرهای مادی انسانی که او را از انجام دادن آنچه آزادانه برگزیده است باز می‌دارد. جنگ و تهدید ناشی از آن، یکی از این زنجیرهاست. همچنین فقر، آموزش و پرورش ضعیف، فشار سیاسی و مانند آن از دیگر تهدیدها به شمار می‌روند. امنیت و آزادی روی یک سکه هستند. آزادی (نه قدرت یا نظم) امنیت واقعی را به وجود می‌آورد. بنابراین آزادی، امنیت است.»[2]

دیگر عامل همسانی امنیت و آزادی، رکن بودنشان برای پشتیبانی از حقوق بشر است. در اینجا آزادی‌ها و حقوق بشر خود در دل سیاست‌های بیرونی که بخشی از امنیت ملی است جا می‌گیرند و در آن می‌آمیزند. این است که امنیت ملی بر پایه پیشبرد آزادی‌ها قرار می‌گیرد و برای فرمانروایی دولت ـ ملت، امنیت و آزادی با هم کنار می‌آیند؛ به همین دلیل برخی حقوق‌دانان با پیش کشیدن دیدگاه «حقوق بشر بین‌المللی»، بر این باورند که «حقوق بشر خود از جمله سیاست‌های خارجی کشورهاست. این سیاست در زمان کارتر نمونه‌ای از برجسته‌ترین سیاست‌های دولت ایالات متحده بوده و هر چند در سال‌های آغازین ریگان فراموش شده ولی پس از وی همواره در نگاه خارجی دولتمردان آمریکایی بوده، به طوری که هم اکنون حقوق بشر در سیاست بیرونی آمریکا نهادینه شده است.»[3]

عامل سوم جداناپذیری امنیت و آزادی، زمانی است که این دو، افزاری برای فرمان‌روایی به شمار روند. این حالت را به روشنی، صدر اصل نهم قانون اساسی جمهوری اسلامی ایران پذیرفته است که بر پایه آن «در جمهوری اسلامی ایران آزادی و استقلال و وحدت و تمامیت ارضی کشور از یکدیگر تفکیک‌ناپذیرند و حفظ آنها وظیفه دولت و آحاد

1. Ken Booth

۲. موتیمر، دیوید، «فراتر از راهبرد: تفکر انتقادی و مطالعات نوین امنیتی»، در: امنیت و راهبرد در جهان معاصر، با ویرایش کریگ.آ.اشنایدر، برگردان اکبر عسگری صدر و فرشاد امیری، انتشارات پژوهشکده مطالعات راهبردی، ۱۳۸۵، ص. ۱۲۹.

3. Shestack, Jerome, "Human rights, the national interests and U.S foreign policy", The annals of the American academy of political and social science, vol. 506, 1989, p.18.

ملت است...». این اصل پیشینه و الگویی ندارد و آشکار نیست گردآورندگان اصل، خواسته به نگارش چنین اصل پوشیده و در همان حال طلایی دست زده‌اند یا ناخواسته.

بخش نخست اصل نهم دربردارنده دو نکته برجسته است: یکی اینکه آزادی در عرض استقلال و وحدت و تمامیت ارضی کشور جا می‌گیرد که همه اینها ستون‌های حاکمیت ملی به شمار می‌روند و دیگر اینکه نگهداری از آنها همچون یک وظیفه هم بر گردن دولت است و هم بر عهده تک‌تک شهروندان. به سخن دیگر، با آنکه امنیت یک حق فردی و اجتماعی و نیز آزادی یک حق فردی هستند ولی در همان حال برای شهروندان این تکلیف را پدید می‌آورند تا در راه نگهداری آنها بکوشند. پس هم‌چنانکه استقلال و وحدت و تمامیت ارضی محورهای بنیادین نظام نوپا هستند، اصل نهم «آزادی را نیز یکی از محورهای اصلی نظام سیاسی کشور قرار داده که به صورت حقوق ملت از یک سو و دمکراسی و حاکمیت ملی در بنیان‌گذاری نظام و اداره امور کشور به اتکای آرای عمومی از سوی دیگر متظاهر می‌شود.»[1]

چالشی که در حاکمیت اصل نهم نسبت به فضای سایبر هست، این است که اگر فضای سایبر فضای آزادی‌ها و به دور از دیده‌بانی جامعه و دولت است، چه نیاز به این اصل است، در حالی که سنگینی ترازو به سمت آزادی‌ها است تا امنیت ملی. این سخن هنگامی است که فضای سایبر، فضای هم عرض با فضای بیرونی و جدا از آن دانسته شود ولی نمی‌توان نادیده گرفت که فضای سایبر با پشتیبانی دولت‌ها یا اجازه آنها بنیاد گرفته و پیشرفت داشته است. به همین دلیل همین دولت‌ها هستند که برای چنین فضایی تصمیم می‌گیرند. با رویه کنونی که کشورها، فضای سایبر را به دلیل اطلاعات (که از دوران باستان، عنصر بنیادین امنیت یک جامعه است) و زیر ساخت‌های حیاتی، بخشی از سرزمین خود می‌پندارند، حاکمیت اصل نهم نمود بیشتری دارد. بدین حال از دید مرتکب که حقوق وی و پاسداشت جایگاه و شخصیتش در نگاه است، اصل نهم کمک می‌کند که برخورد پلیسی و قضایی به جای آنکه مرتکب محور باشد، رفتارمحور است؛ چرا که فضای سایبر این توانایی را ندارد که مرتکبان خطرناک بیافریند ولی این توانایی را به خوبی دارد که رفتارهای خطرناک با پیامدهای بسیار گسترده را زمینه‌ساز باشد.

۲ـ۲. رویارویی رفتار محور

رفتار بزه‌های سایبری به جهت ویژگی‌های فضای سایبر از سه جهت، توان خطرناکی بالا دارد: نخست، انجام رفتار در رایانه‌های بیشمار پیونددار با هم و حتی در

۱. هاشمی، سیدمحمد، حقوق اساسی جمهوری اسلامی ایران: اصول و مبانی کلی نظام، جلد اول، چاپ اول، انتشارات دانشگاه شهید بهشتی با همکاری موسسه نشر یلدا، ۱۳۷۴، ص. ۱۷۲.

رایانه‌های محدود ولی لبریز از اطلاعات، به گستردگی رخ می‌دهد. به سخن دیگر، رفتار بزه سایبری، به خودی خود این توانایی را دارد که در سطح گسترده رخ بدهد و تنها این گزینش مرتکب است که بخواهد آن رفتار را محدود کند وگرنه طبیعت رفتار، ره به سوی گستردگی و فراگیری دارد. طبیعت رفتار با ویژگی‌های ذاتی اطلاعات و تبادل اطلاعات پیوند دارد.

دوم، گستردگی رفتار بر موضوع‌های گوناگون است. گستردگی رفتار تنها به جهت ویژگی‌های فنی و اطلاعاتی نیست، بلکه موضوع‌ها یا همان ارزش‌هایی که از سوی رفتار تهدید می‌شوند، در این فضا بسیار پرشمارند. این موضوع‌ها هم اطلاعات و سامانه‌ها را در بر می‌گیرد و هم کاربران و مشترکان و همه نهادهایی که با رایانه کار می‌کنند. گوناگونی موضوع‌ها به پخش بدافزارها و نیز به اندازه آسیب‌پذیری موضوع‌ها بستگی دارد تا به گزینش و برنامه‌ریزی مرتکب. در خرداد ۱۳۹۶، گفته شده که نزدیک به ده هزار تن در ایران، بزه‌دیده باج‌افزار وانا کرای بوده‌اند. این بدافزار هر چند در پی رایانه‌های سطح بالای اشخاص حقیقی و حقوقی ثروتمند است ولی در اصل بیشتر قربانیان، کسانی بودند که سامانه‌های رایانه‌ای آنها آسیب‌پذیرتر بوده و با نسخه ویندوز قدیمی‌تر کار می‌کرده‌اند. این گستردگی موضوع تنها به جهت پخش بدافزارها نیست بلکه تجمیع موضوع‌ها نیز خود عامل دیگری برای خطرناکی رفتار خواهد بود. این ویژگی در کلاهبرداری رایانه‌ای بسیار برجسته است. دو شیوه مشهور، دسترسی غیر مجاز به سامانه نهادهای بانکی و مالی و نیز طراحی تارنمایی همسان با تارنمای موسسات مالی و فراخوان صاحبان حساب به آنجا، هر دو شیوه‌ای بر پایه پرشماری بزه‌دیدگان است.

سوم، گستردگی پیآمد و زیان‌های رفتار است. با اطلاعاتی شدن بیشتر امور به ویژه امور مالی و اسرار تجاری و اقتصادی و حساب‌های بانکی، انجام رفتار بر ضد رایانه‌های پرشمار، زیان‌های گسترده مالی و حتی پیآمدهای گوناگون بهداشتی، اقتصادی، زیست محیطی و مانند آنها را سبب می‌شود. گستردگی موضوع و گستردگی پیامد در سنجش با سپهر بیرونی، با رفتار همخوانی ندارد. به سخن دیگر، مرتکب برای چنین گستره‌ای از زیان، تلاش نکرده و همه اینها به جهت یک رفتار ساده مانند پخش بدافزار یا رخنه به سامانه حفاظت شده به دست می‌آید. پس در این فضا، سنجش تناسب رفتار و نتیجه تا اندازه‌ای گمراه‌کننده است؛ چرا که نتیجه به اندازه‌ای بسیار محتمل و بر پایه اندازه آسیب‌پذیری موضوع، شیوه‌های رویارویی با رفتار مجرمانه، انجام در فضای اینترنت یا شبکه‌های داخلی یا حتی سامانه‌های غیر مرتبط با هم و مانند آن، نقش پررنگی در پیامدسازی رفتار سایبری دارد. ولی نمی‌توان از نگاه دور داشت که

چنین ویژگی‌ای را به حساب رفتار سایبری مـی‌گذارنـد و از همـین در خطرنـاکی آن را نشان می‌دهند.

سنجش تهدید سایبری از دید رفتار، بـه خـوبی نشـان مـی‌دهـد کـه ایـن پدیـده خطرناک از تهدیدهای بیرونی است ولی چالشی که از دید قانون اساسی مطرح می‌شود، این است که آیا تنها از دید رفتار و پیامدهای آن می‌توان، رویکردی سخت‌گیرانـه بـرای تهدیدهای سایبری روا داشت؛ به ویژه آنکه دلیل‌های اصلی خطرناکی تهدید سایبری بـا مرتکب آن پیوند ندارد، بلکه به جهت ویژگی‌های فضای سایبر و نیـز نقـش بـزه‌دیـدگان است. سخت‌گیری کیفری بر پایه رفتار، سختگیری بر مرتکب آن است. از همین دریچـه باید گفت که سیاست کیفری در برابر رفتارهای تهدیدآمیز، دستاوردی مگر سخت‌گیری بر مرتکب آن ندارد ولی اگر به جای ایـن سیاسـت بـه سیاسـت‌هـای پیشـگیرانه و نیـز اقدام‌های تأمینی در فضای سایبر روی بیاوریم، گونه‌ای واکنش شایسته در برابـر تهدیـد است؛ چرا که واکنش باید با طبیعت کنش تهدیدآمیز همخوانی داشته باشـد. از ایـن رو، از دید قانون اساسی، رفتار تهدیدآمیز بهانه‌ای برای سخت‌گیری بر ضد حقوق مرتکبان و نیز شهروندان نخواهد بود و در این میان، در برابر رفتارهای تهدیـدآمیز بایـد رویکـردی فنی و پیشگیرانه و نیز جبران زیان را در نگاه داشت تا رویکردهای کیفری.

۲ـ۳. رویارویی غریزی

حقوق کیفری از زمان آفرینش انسان تا کنون در برابر رفتارهـای ضـد ارزش‌هـای بنیادین و طبیعی یعنی جان و دارایی، غریزی عمل کرده است. در زمان ما نیز دولـت‌هـا از انسان‌ها یاد گرفته‌اند که به طور ویژه در برابـر جنـگ و تروریسـم کـه هـر دو پدیـده بیشتر بر ضد جان‌ها و اموال، غریزی عمل کنند. گزاره نیز این بوده است: بـه هـر انـدازه تهدید بیشتر، حقوق کیفری خشن‌تر. در همه دوران‌ها هم از سوی انسان و هم از سـوی دولت‌ها، حقوق کیفری در مقام واکنش بوده است. واکنش در چهره نخستین و طبیعـی خود بر پایه غریزه و همان دفاع در برابر تهدید بزه است. این تهدید به هر اندازه بیشـتر، واکنش حقوق کیفری نیز خشن‌تر می‌گردد. واکنش اگر همراه با قدرت باشـد، بـه نمـاد کیفر در می‌آید و نمی‌توان میان دفاع کردن در برابر تهدید بزه یا کیفر دادن آن جـدایی گذاشت که هر دو واکنش طبیعی و غریزی به بزه به شمار می‌روند.

تهدید تروریسم سایبری و جنگ سایبری نیز به هـر انـدازه افـزایش یابـد، حقـوق کیفری نیز امنیتی، خشن و سرکوب‌گر خواهد بود و این ویژگی را نمی‌توان خرده‌ای بـر حقوق کیفری دانست؛ چرا که شیوه رفتار آن بر پایه غریزه است. هر تهدید هر اندازه که خشونت‌بارتر و بزرگ‌تر باشد، پاسخ سخت‌تر به همراه خواهد داد. کم رنگ‌کـردن چنـین

پاسخی که بر پایه غریزه است، دست‌کم تا زمان کنونی شدنی نبوده است. بسیار روشن است که هر جامعه یا دولتی در برابر یک یورش جنگ افزارانه یا اقدام تروریستی به شتاب، چهره امنیتی و واکنشی به خود می‌گیرد و همین چهره در دادرسی و صدور حکم نشان می‌دهد. در برخی نظام‌های حقوقی مانند ایران، حتی این چهره را در حالت عادی و در زمان قانون‌گذاری نیز نمود داده‌اند مانند استثناهایی که در قانون مجازات اسلامی ۱۳۹۲ درباره بزه‌های ضد امنیت ملی روا داشته شده است. بدین حال سخت‌گیری حقوق کیفری در برابر تهدیدهای سایبری به ویژه تهدیدهای بزرگ نه بر پایه گزینش بخردانه که بر پایه غریزه است و امر غریزی در هر حال می‌تواند در زمان بروزش توجیه‌پذیر باشد. با این حال آیا یک تهدید سایبری را می‌توان چنان بزرگ، پررنگ و همسان با تهدیدهای بیرونی مانند تروریسم خشن یا جنگ دانست که واکنش غریزی در برابر آن دفاع‌پذیر باشد؟ از پایه می‌توان غریزه و واکنش غریزی را در فضای سایبر که مرز روشنی با فضای طبیعی بشر دارد، نیز سازگار دانست؟ این پرسش‌ها، همان پاسخ‌هایی را به همراه دارد که پیش از این درباره بزه سایبری و تروریسم سایبری گفته شده است.

نتیجه‌گیری

حاکمیت قانون اساسی در رویارویی با پدیده جرم، مبتنی بر ایجاد توازن میان حقوق متهم یا محکوم، حقوق بزه‌دیده و حقوق جامعه و دولت است. برقراری این تراز هر چند به روشنی در قانون اساسی نیامده است ولی اصل‌های این قانون به خوبی گویا است که در رویارو شدن با پدیده‌های نو و رفتارهای ناهنجاری که با این پدیده‌ها پیوند دارند، تراز میان سه حقوق پیش گفته باید پاس داشته شود. ولی بسیار رخ داده است که قانون‌گذاری‌های کیفری پیرو رخدادهای سرزنش‌پذیر و تأثیرگذار در جامعه بوده است که نشان می‌دهد رویکردهای کیفری چه از سنخ قانون‌گذاری و چه از رسته قضایی و پلیسی، توانایی آن را دارند تا پیرو واکنش‌ها و احساس‌های اجتماعی باشند. با این حال بزه‌های سایبری در این زمینه ویژگی‌های دیگری دارند.

بزه‌های سایبری از جهت‌های گوناگون از بستر انجام آن گرفته تا مرتکب آن و نیز از اندازه سرزنش‌پذیری در نزد شهروندان جامعه گرفته تا بایسته‌های بین‌المللی پیرامون آن، پویایی و نسبیت در سیاست کیفری را سبب شده است. با آنکه بیشتر بزه‌ها، سرزنش‌پذیری اجتماعی و زیان‌های همگانی در بالای هرم چرایی بزه‌انگاری قرار دارد ولی نسبت به بزه‌های سایبری، به جای جامعه این دولت است که در مقام ساختن سرزنش‌پذیری و خطرناکی برای این رفتارها برآمده است. بر همین پایه، نهادهای گوناگون دولتی و حاکمیتی برای رویارویی با آنها پافشاری می‌کنند و همین نگاه سبب شده است تا به طور کلی سیاست کیفری ایران در رویارویی با بزه‌های سایبری با اصول قانون اساسی هماهنگ نباشد.

رویارویی چه بر پایه گزینش رفتار باشد یا انجام‌دهنده آن و چه بر پایه سنخ‌بندی تهدید سایبری به بزه سایبری، تروریسم سایبری و جنگ سایبری؛ به طور کلی بایسته‌های قانون اساسی در گزینش یک سیاست سخت‌گیرانه و سرکوب‌گر را سبب نمی‌شود. قانون اساسی به گونه‌ای پیوند امنیت ملی و آزادی‌های فردی را ترسیم کرده است و به شیوه‌ای چهارچوب‌های زندگی فردی و جمعی را تنیده که تهدید سایبری یک تهدید راستین و نگران‌کننده نیست به گونه‌ای که سیاست کیفری تقنینی، قضایی و پلیسی سخت‌گیرانه بطلبد.

به طور کلی تهدیدهای سایبری در ایران برآمده از پیوند عکس حساسیت دولتی نسبت به تهدید سایبری و بی‌تفاوتی بیشتر شهروندان به واقعی‌بودن این تهدیدها، ناسازگاری تهدیدهای سایبری با تهدیدهای خشن سپهر بیرونی، جبران‌پذیر بودن پیآمدهای تهدید سایبری با راهکارهای بیرونی و از همه برجسته‌تر رویکرد شهروند ایرانی به فضای سایبر در مقام بستری برای اعمال حقوق و آزادی‌های فردی چه

توجیه‌پذیر باشد و چه نباشد، همگی نشان می‌دهد که سیاست کیفـری در رویـارویی بـا تهدید سایبری در ایران اگر قرار است با قانون اساسی سازگار باشد، نیاز به دگرگونی‌های بنیادین دارد.

منابع

- جلالی، امیرحسین، «تروریسم سایبری»، فصلنامه تخصصی فقه و حقوق، شماره ۱۰، پاییز ۱۳۸۵.
- شی یرمر، جرمی، اندیشه سیاسی کارل پوپر، ترجمه عزت‌الله فولادوند، چاپ دوم، نشر ماهی، ۱۳۸۶.
- عباسی، مجید؛ مرادی، حسین، «جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه»، فصلنامه مجلس و راهبرد، سال بیست و دوم، شماره ۸۱، بهار ۱۳۹۴.
- فلمینگ، پیتر؛ استول، مایکل، «سایبر تروریسم: پندارها و واقعیت‌ها»، ترجمه اسماعیل بقایی هامانه و عباس باقرپور اردکانی، در: تروریسم، گردآوری و ویرایش علیرضا طیب، نشر نی، چاپ دوم، ۱۳۸۴.
- قاسمی، علی؛ چهاربخش، ویکتور بارین، «حملات سایبری و حقوق بین‌الملل»، مجله حقوقی دادگستری، شماره ۷۸، ۱۳۹۱.
- کلهر، رضا، «جهاد مجازی: ماهیت و چالش‌ها»، فصلنامه مطالعات منطقه‌ای جهان اسلام، شماره ۳۲، ۱۳۸۶.
- موتیمر، دیوید، «فراتر از راهبرد: تفکر انتقادی و مطالعات نوین امنیتی»، در: امنیت و راهبرد در جهان معاصر، با ویرایش کریگ.آ.اشنایدر، برگردان اکبر عسگری صدر و فرشاد امیری، انتشارات پژوهشکده مطالعات راهبردی، ۱۳۸۵.
- هاشمی، سیدمحمد، حقوق اساسی جمهوری اسلامی ایران: اصول و مبانی کلی نظام، جلد اول، چاپ اول، انتشارات دانشگاه شهید بهشتی با همکاری موسسه نشر یلدا، ۱۳۷۴.
- هیأت مؤلفان و ویراستاران انتشارات مایکروسافت، فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، برگردان فرهاد قلی‌زاده نوری، کانون نشر علوم، چاپ اول، ۱۳۸۱.

- Ballard, James David; Hornik, Joseph; Mckenzie, Douglas, "Technological facilitation of terrorism", in: Cyberterrorism, Alan O'Day (ed), Ashgate publishing company, 2004.
- Beard, Jack, "Legal phantoms in cyberspace: The problematic status of information as a weapon and a target under international humanitarian law", Vanderbilt Journal of Transnational Law, vol. 47, 2014.
- Bernik, Igor, Cybercrime and cyber warfare, John Wiley & Sons, 2014.

- Brenner, Susan, "Cybercrime, Cyberterrorism and Cyberwarfare", International review of penal law: cybercrime, AIDP, vol. 77, 2006.
- Coady, Tony, "Terrorism, Just war and supreme emergency", in Terrorism and Justice: Moral argument a threatened world, Tony Coady and Michael O Keefe (Eds), Melbourne University Press, 2002.
- Cohen, Fred, "Terrorism and cyberspace", in: Cyberterrorism, Alan Oday (Ed), Ashgate publishing company, 2004.
- Day, Patrick, "Is the concept of freedom essentially contestable?", Philosophy, Vol. 61, no. 235, 1976.
- Embar-Seddon, Ayn, Cyberterrorism, in: Cyberterrorism, Alan O'Day (ed), Ashgate Publishing Company, Farnham, 2004.
- Ozeren, Suleyman, Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment, UMI Dissertation Services, University of North Texas, August 2005.
- Phair, Nigel, Cybercrime: The reality of the threat, E-security Publishing, Canberra, 2007.
- Podesta, John; Goyle, Raj, "Lost in cyberspace? Finding American liberties in a dangerous digital world", Yale law and Policy Review, Vol. 23, 2005.
- Shestack, Jerome, "Human rights, the national interests and U.S foreign policy", The annals of the American academy of political and social science, vol. 506, 1989.
- Sieber, Ulrich; Brunst, Phillip, Cyberterrorism and other Use of the Internet for terrorist purposes; threat analysis and evaluation of international conventions, Counter-Terrorism Task Force, Council of Europe, Council of Europe Publishing, 2007.
- Tully, Stephen, "Protecting Australian Cyberspace: Are our international lawyers ready?", Australian international Law Journal, vol. 19, 2012.