حمایت قانونی از آسیب‌دیدگان سایبری

امیرحسین جلالی فراهانی،* محبوبه منفرد**

تاریخ دریافت ۹۱/۱۰/۲	تاریخ پذیرش ۹۲/۳/۱

یکی از راهکارها و همچنین دستاوردهای برپایی و برقراری نظم در جامعه، جبران زیان‌های ناشی از بی‌نظمی‌هاست. با این کار جامعه نشان می‌دهد که آسیب‌دیدگان را در برابر ناهنجاری‌ها و هنجارشکنی‌ها تنها نگذاشته و از آنها، چه در هنگام پیشگیری از آسیب‌ها و چه برخورد با بزهکاران پشتیبانی می‌کند. این نیاز، به‌ویژه هنگامی احساس می‌شود که جامعه در برابر تهدیدها و آسیب‌های نوین و ناشناخته‌ای قرار می‌گیرد که نه می‌تواند از آنها مصون باشد و نه درصورت واکنش در برابر آنها امید دارد که از پشتیبانی شایسته‌ای برخوردار شود. دنیای نوپدید سایبر چنین وضعیتی دارد و شاید بیش از هر فناوری نوین دیگری دستاوردها و البته پیامدهایش را به کام کاربرانش چشانیده است. مصون‌ماندن از آسیب‌ها و تهدیدهای روزافزون سایبری به پشتیبانی همه‌جانبه و فراگیری نیاز دارد که سرآغاز آن در اختیار قانونگذار است. قانونگذار با وضع قواعد، سازوکارها و تمهیدات گوناگون و تقسیم حق‌ها و مسئولیت‌های مترتب بر این حوزه، به کاربران اطمینان می‌دهد که جامعه در برابر آسیب‌ها پاسخ‌گوست. برای ایفای این وظیفه ملی، قانونگذار باید حیطه کار خویش، تهدیدها و آسیب‌های پیش رو و تدبیرهای پیشگیرانه و واکنشی آنها را بشناسد، مجموعه احکام الزام‌آور قانونی را، پیش‌بینی و به مجریان ابلاغ کند و همواره روزآمد و آگاه باشد. در این صورت می‌توان امیدوار بود نه تنها از آسیب‌دیدگان سایبری حمایت شایسته‌ای به عمل می‌آید، بلکه اقدام‌های قانونی در برابر تهدیدهای سایبری، خود برهم‌زننده نظم و امنیت عمومی نخواهند بود.

کلیدواژه‌ها: آسیب سایبری؛ پشتیبانی قانونی؛ تدابیر جبرانی؛ تدابیر پیشگیرانه؛ تدابیر واکنشی

---

* کارشناسی ارشد حقوق کیفری و جرم‌شناسی، دانشکده حقوق و معارف اسلامی، دانشگاه امام صادق (ع)، پژوهشگر حقوق فناوری اطلاعات و ارتباطات (نویسنده مسئول)؛ Email: jalalyfarahany1979@gmail.com

** کارشناسی ارشد حقوق کیفری و جرم‌شناسی، مؤسسه آموزش عالی شهید اشرفی اصفهانی، واحد اصفهان، پژوهشگر حقوق و فناوری اطلاعات و ارتباطات؛ Email: mahboubeh.monfared@gmail.com

مقدمه

۱. فضای سایبر: از یکجانشینی فرصت‌ها تا یکجاگزینی تهدیدها

شاید متمایزترین و مهم‌ترین ویژگی دنیای سایبر از دنیای خاکی[1] یا فیزیکی، برچیده شدن مفهوم ماده و مختصات مکانی آن است. همین توانمندی باعث شده همه‌چیز یکجا باهم باشد و هم‌زمان به کاربری‌های متفاوتی پرداخته شود. برای مثال در کنار آموزش الکترونیکی، نیازمندی‌هایمان را خریداری کنیم، امور بانکی‌مان را پیش ببریم، گپ و گفت روزانه‌مان را در محیط‌های ارتباطی خصوصی، غیرعمومی و عمومی داشته باشیم و با همه اینها، پایگاه‌های خبری و سرگرمی‌های مورد علاقه‌مان را هم مرور و بررسی کنیم (کیسی، ۱۳۸۶: ۷).

این ویژگی متمایز و منحصربه‌فرد در خدمت تهدیدآفرینان سایبری هم قرار دارد و می‌توانند هم‌زمان چندین هدف را با یک تیر نشانه روند؛ بی‌آنکه نیازی به حضور در محیط‌های گوناگون داشته باشند و بر هزینه جنایت[2] خود بیفزایند. آنها با آسودگی کامل و از همان حریم خصوصی[3] یا خلوت خویش انواع تهدیدها را می‌آفرینند و عواید جنایی[4] سرشاری را به‌دست می‌آورند. برای مثال، هم‌زمان می‌توانند با سوءاستفاده از داده‌های مالی اشخاص، در پایگاه‌های خبری حیثیت دیگران را هتک کنند، داده‌های برخی دیگر را حذف و سامانه‌هایشان را مختل کنند یا از کار بیندازند. بی‌شک چنین وضعیتی زاییده این فناوری نیست و هر ابزاری می‌تواند کاربری سودمند و زیان‌باری داشته باشد که از انگیزه و قصد بهره‌بردار آن ناشی می‌شود[5] و عاقلانه نیست که به بهانه پاکسازی جامعه و سالم نگاه داشتن آن از تبهکاری‌های فناورانه، دیگر اعضای جامعه از آنها محروم شوند. حال آنکه باید کاربرد از این فناوری‌ها به‌نحوی برنامه‌ریزی و اجرا شود که هزینه جنایت برای بزهکاران بالقوه افزایش یابد تا از تحقق نیات شومشان جلوگیری شود.

---

1. Terrestrial World

۲. منظور از هزینه جنایت یا جرم (Cost of Crime) میزان خطری است که بزهکار بالقوه احتمال می‌دهد درصورت ارتکاب جرم متحمل خواهد شد که شامل احتمال درگیری با بزه‌دیده بالقوه، دستگیری و امکانات و نیروی مورد نیاز برای ارتکاب جرم می‌شود.

3. Privacy

4. Proceeds of Crime

۵. برای مطالعه بیشتر درباره انواع انگیزه‌های جنایی سایبری، رک.: محبوبه منفرد، «بررسی جرم‌شناختی بزهکاری رایانه‌ای»، فصلنامه *مطالعات پیشگیری از جرم*، نشریه پلیس پیشگیری نیروی انتظامی، در دست چاپ.

۲. آماج‌های سایبری: از دارایی‌های فردی تا سرمایه‌های ملی

در دنیای سایبر، دارایی‌های سایبری[1] آماج[2] تهدیدهای گوناگونی قرار می‌گیرند. این دارایی‌ها می‌تواند مادی و معنوی باشد. منظور از دارایی مادی سایبری، همه امکانات و ملزومات مورد نیاز برای برپایی و پشتیبانی از دنیای سایبری است. دنیای سایبر از شهرهای سایبری و خطوط مواصلاتی بین آنها تشکیل شده که همان مراکز یا پایگاه‌های داده‌اند[3] و فعالان سایبری می‌توانند محتوای الکترونیکی‌شان را ذخیره و امکان دسترسی برای دیگران را فراهم کنند. البته این مراکز یا پایگاه‌ها همیشه در معنای عرفی خود از ابررایانه‌ها[4] تشکیل نمی‌شوند و یک سامانه رایانه‌ای مستقل نیز می‌تواند چنین نقشی را حتی به شکل محدود ایفا کند. سامانه‌های ارتباطی که به مبادله داده‌ها با این مراکز می‌پردازند، سازه‌ای از این شهرها به‌شمار می‌آیند و ماندگاری و پویایی این فضا را تضمین می‌کنند. خطوط مواصلاتی یا ارتباطی نیز قاعدتاً همان شبکه‌های ارتباطی بی‌سیم یا باسیم‌اند که امکان مبادله داده‌ها را فراهم می‌آورند. این خطوط سازه‌ها یا سامانه‌هایی را شامل می‌شوند که جابه‌جایی درست و سریع داده‌ها را امکان‌پذیر می‌کنند که می‌توان به مسیریاب‌ها،[5] سرورهای نام دامنه[6] و هاب‌ها[7] اشاره کرد (جلالی فراهانی، ۱۳۹۱: ۱۰۷).

اما شالوده و جان‌مایه فضای سایبر را داده‌های آن تشکیل می‌دهد که به شکل‌های گوناگون نمایان می‌شوند. هر محتوای رایانه‌ای با هدف پیشبرد یک یا چند مورد از امور خرد و کلان فردی یا اجتماعی تولید می‌شود و در دنیای سایبر جریان و متناسب با نقش و جایگاه پدیدآورنده خود ارزش و اعتبار می‌یابد. اگر محتوا، داده‌های تجاری کسب‌وکار را دربرداشته باشد، ارزش مالی آن را برمی‌گیرد و اگر زندگی شخصی فردی یا اطلاعات طبقه‌بندی شده کشوری را نمایان سازد، بر ارزش‌های دیگری استوار می‌شود.

دارایی‌های معنوی نیز به دو گروه فردی و جمعی یا ملی قابل تقسیم است. نمونه

---

1. Cyber Assets
2. Target
3. Database
4. Supercomputer
5. Router
6. Domain Name Server (DNS)
7. Hub

آشکار دارایی‌های معنوی فردی، آثار فکری است که به شکل‌های ادبی ـ هنری یا صنعتی ـ بازرگانی بروز می‌کند. برای مثال، شعر یا موسیقی و همچنین اسرار تجاری یا طرح صنعتی، در زمره آثار فکری یا دارایی معنوی فردی قرار می‌گیرد. این فرد می‌تواند شخص حقیقی یا حقوقی باشد. البته معمولاً دارایی معنوی فردی به اشخاص حقیقی تعلق می‌گیرد. هویت و فرهنگ ملی نیز در زمره دارایی معنوی جمعی یا ملی است که می‌تواند ارزش‌های گوناگونی را برای مردم خود به ارمغان آورد. این طیف گسترده از دارایی‌های معنوی جمعی می‌توانند در دنیای سایبر و در شکل داده‌ها، اطلاعات و محتوای گوناگون صورت گیرد. برای مثال، نام دامنه کشوری یا ملی، مانند ir. یا .ایران، صرف‌نظر از ارزش‌های مالی که از واگذاری آن به اشخاص داده می‌شود، اعتبار ویژه‌ای نیز دارد، تاحدی‌که در مواردی شاخص ترسیم قلمرو حاکمیتی کشورها در این دنیای بی‌کران تعریف شده است.[1] همچنین برخی نمادها که نمایانگر ارزش‌های فرهنگی یک کشور هستند و به شکل داده‌های رایانه‌ای به نمایش درمی‌آیند، از همین ویژگی برخوردارند.[2]

۳. صیانت از آماج‌های سایبری: از سیاستگذاری قانونی تا برنامه‌ریزی اجرایی

سالم‌سازی و سالم نگاه داشتن فضای سایبر از ناهنجاری‌ها و هنجارشکنی‌های سایبری، درجایی‌که جلوه واکنشی و کیفری می‌یابد، همانند دنیای فیزیکی وظیفه‌ای ملی است که مسئولیت آن برعهده مجریان قانون است. یکی از عوامل اصلی برهم‌زننده نظم اجتماعی عدالت خصوصی است، به این معنا که زیان‌دیدگان یا داوطلبان، خودسرانه با بزهکاران برخورد و آنها را کیفر دهند. ازاین‌رو نظام‌های حاکمیت ملی حق و وظیفه خود می‌دانند که به نمایندگی از

---

۱. قانون مجازات اسلامی در ماده (۷۵۶) خود نام دامنه ملی را گزینه‌ای برای ترسیم قلمرو حاکمیتی سایبری ایران در نظر گرفته است. برای آگاهی بیشتر از نقش‌آفرینی نام‌های دامنه در سامان‌دهی نظام دادرسی کیفری سایبری کشورها، رک.: امیرحسین جلالی فراهانی (۱۳۸۹ الف). *درآمدی بر آیین دادرسی کیفری جرائم سایبری*، چاپ اول، تهران، نشر خرسندی.

۲. طراحی نام‌های دامنه که به‌صورت اختصاصی و برپایه محل، موضوع یا نماد خاصی تعریف و به ذی‌نفع آن واگذار می‌شود، مانند islam.، tehran.، مراحل ثبت درخواست‌ها را در شرکت آیکان (ICANN) سپری می‌کند. برای آگاهی از مباحث این حوزه درباره راهبری شبکه جهانی اینترنت، رک.: علیرضا کاشیان و دیگران (۱۳۸٤). *راهبری اینترنت* (مشارکت فراگیر)، انتشارات دبیرخانه شورای عالی اطلاع‌رسانی.

شهروندانشان از آنها در برابر تهدیدها و آسیب‌های هنجارشکنانه صیانت کنند.

ازآنجاکه اعمال این وظایف برعهده مجریان قانون است؛ برای جلوگیری از سوءاستفاده و قوه قاهره‌ای[1] که در اختیار دارند؛ اقداماتی باید انجام داد تا حقوق و آزادی‌های مشروع شهروندان نقض نشود. ازاین‌رو جامعه بر پایه تشریفات رسمی (مانند نمایندگان قوه قانونگذاری) مجموعه قوانین و مقرراتی را وضع و لازم‌الاجرا کرده است. قوانین و مقررات حاکم بر یک حوزه، جلوه سلسله‌مراتبی[2] دارد؛ به این معنا که هرچه از سطح سیاستگذاری راهبردی دور و به اجرا نزدیک می‌شود، مصوبات و تصمیمات حاکمیتی نیز کلیت و عمومیت خود را از دست می‌دهد و جلوه‌ای کاربردی‌تر و برنامه‌ای ـ اجرایی می‌گیرد. همه عرصه‌ها و حوزه‌های اجتماعی بر این اساس نظم‌انگاری شده‌اند و نکته حائز اهمیت این است که مقررات پیرو باید همسو با قوانین پایه باشد نه در تعارض با آن. برای مثال، حمایت از آسیب‌دیدگان سایبری از همان قواعد عمومی حمایت از آسیب‌های اجتماعی پیروی می‌کند که در پرتو آن می‌توان برنامه‌ریزی‌های تخصصی انجام داد. گرچه این سخن به معنای نفی نگاه اختصاصی به این حوزه و ضرورت توجه به شرایط ویژه حاکم بر آن نیست.

طبق قانون اساسی جمهوری اسلامی ایران تدوین سیاستگذاری راهبردی را مقام معظم رهبری و شوراهای عالی زیرمجموعه ایشان یعنی شورای عالی امنیت ملی، شورای عالی انقلاب فرهنگی، مجمع تشخیص مصلحت نظام و همچنین شورای عالی فضای مجازی انجام می‌دهند.[3] سیاستگذاری تقنینی نیز برعهده مجلس شورای اسلامی است و سرانجام سیاستگذاری یا برنامه‌ریزی اجرایی را دستگاه‌های اجرایی مانند کمیسیون فناوری اطلاعات و ارتباطات دولت (فاوا)، کمیسیون تنظیم مقررات ارتباطات (موضوع قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، مصوب ۱۳۸۲) و نهادهای مرتبطی مانند

---

1. Coercive Power
2. Hierarchy

۳. از جمله سیاست‌های راهبردی که تاکنون این مراجع درباره فضای تولید و تبادل اطلاعات کشور تصویب و ابلاغ کرده‌اند، عبارت‌اند از: ۱. سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای ابلاغی مقام معظم رهبری (خرداد ۱۳۸۰)؛ ۲. سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)» (۱۳۸۹)؛ ۳. مصوبه شورای عالی انقلاب فرهنگی درباره مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای (آبان ۱۳۸۰)؛ ٤. ابلاغیه مقام معظم رهبری درباره تأسیس شورای عالی فضای مجازی (اسفند ۱۳۹۰).

سازمان حمایت از مصرف‌کنندگان (موضوع قانون حمایت از مصرف‌کنندگان، مصوب ۱۳۸۸) انجام می‌دهند. شناسایی مصوبات و تصمیمات هریک از این مراجع و جانمایی آنها در این نظام سلسله‌مراتبی، نقش بسزایی در تضمین حقوق و انتظارات مشروع شهروندان دارد.[۱]

۴. نگاه این نوشتار: از امکان‌سنجی راهکارها تا نیازسنجی تدبیرهای حمایتی از آسیب‌های سایبری

صیانت از شهروندان یا کاربران فناوری‌های رایانه‌ای و مخابراتی در برابر تهدیدهای سایبری، مجموعه‌ای از حق‌ها و تکلیف‌ها را پدید می‌آورد که استیفا و ایفای شایسته آنها نیازمند قوانین و مقررات یکپارچه، هماهنگ و هم‌سویی است که مراجع صلاحیت‌دار وضع و به مخاطبان و مجریان آنها ابلاغ می‌کنند. اما برای آنکه مجموعه مصوبات و تصمیمات حاکمیتی ناظر بر این حوزه با کاستی و تعارض با احکام روبه‌رو نباشد، ضروری است پیشاپیش امکان‌سنجی مطلوبی از تدابیر صیانتی و حمایتی سایبری به‌عمل آید.

۱ انواع تدبیرهای حمایتی از آسیب‌دیدگان سایبری

به‌طورکلی از آسیب‌دیدگان بالقوه و بالفعل ناهنجاری‌های اجتماعی به دو شکل می‌توان حمایت کرد: ۱. صیانت از آنها در برابر تهدیدها با اتخاذ تدبیرهای پیشگیرانه؛ ۲. ترمیم و جبران زیان‌های وارده به آسیب‌دیدگان و همچنین پیگرد و کیفر تهدیدآفرینان.

فضای سایبر از این قاعده مستثنا نیست و باید در همین چارچوب تدابیر متناسب و اثربخش آن را شناسایی، تعریف و اجرا کرد. در این قسمت به‌ترتیب تدبیرهای پیشگیرانه و واکنشی (جبرانی و ضمانت اجرایی) ناظر بر این حوزه بررسی و تحلیل شده است.

۱-۱ تدبیرهای پیشگیرانه حمایتی

پیشگیری از رخداد یک رویداد، نیازمند دو کار اساسی است: ۱. آگاهی از چگونگی

---

۱. انتظار مشروع (Reasonable Expectation) گفتمان نوینی در ادبیات حقوق اداری است که از مسئولیت مقامات صلاحیت‌دار درباره مصوبات و به‌ویژه تصمیمات آنها سخن می‌گوید. رک.: مسیح بهنیا (۱۳۹۰). «اصل انتظارات مشروع و حمایت از آن در حقوق اداری با تأکید بر مطالعه آرای قضایی»، رساله دکتری حقوق عمومی، دانشگاه تهران، پردیس قم.

رخداد آن؛ و ۲. خنثی‌سازی عناصر اساسی تشکیل‌دهنده آن (مهدوی، ۱۳۹۰: ۲۵؛ ابراهیمی، ۱۳۹۰: ۸۸). به‌این‌ترتیب پیشگیری از رخداد یک آسیب به آگاهی از تهدید و همچنین عناصر تشکیل‌دهنده آن نیازمند است. مثلاً برای پیشگیری از تعرض به افراد، متناسب با ویژگی‌های فردی و وضعیت محیطی آن می‌توان تهدیدهای گوناگونی را شناسایی کرد. تعرض به کودکان با تعرض به زنان تفاوت‌های بارزی دارد و تعرض به سالمندان و ناتوانان نیز مشابه یکدیگر نیست. بنابراین برشمردن عناصر تشکیل‌دهنده هریک از آنها نیازمند بررسی و تحلیل متمایز و مختص به خودند.[1]

در بسیاری موارد، ناآشنایی آسیب‌دیدگان بالقوه یا والدین یا حامیان آنها از تهدیدهای پیش رو، بر آسیب‌پذیری آنها می‌افزاید و آنها را در کانون خطر قرار می‌دهد. گاهی نیز آنها به‌رغم آگاهی از تهدیدها، به‌دلیل نداشتن ابزار و امکانات پیشگیرانه یا تدافعی لازم، بزه‌دیده می‌شوند. این وضعیت در عرصه‌های نوپدیدی چون فضای سایبر می‌تواند بسیار خطرناک‌تر باشد؛ زیرا هنوز سطح آگاهی عمومی و اختصاصی شهروندان نسبت به تهدیدهای بالقوه به حدی نرسیده که آگاهانه از حضور در محیط‌های پرخطر سایبری پرهیز کنند و همچنین امکانات و ابزارهای امنیتی سایبری نیز به‌اندازه کافی در دسترس همگان قرار ندارد تا بتوان سطح ایمنی مطمئنی را برای کاربران در معرض خطر فراهم کرد (کیسی، ۱۳۸۶: ۲۸۲). ازاین‌رو با توجه به اهمیت موضوع، در این گفتار دو تدبیر رشد آگاهی و تأمین نیازمندی‌های فناورانه امنیتی به‌عنوان تدبیرهای پیشگیرانه حمایتی از آسیب‌دیدگان بررسی می‌شود.

۱-۱-۱ رشد آگاهی درباره تهدیدهای سایبری

به‌رغم گسترش خیره‌کننده ابزارهای فناورانه مخابراتی و رایانه‌ای و کاربری فراگیر آنها در امور گوناگون زندگی، افراد بسیاری هستند که از تهدیدهای ناشی از کاربری‌های ناامن

---

۱. برای آگاهی از اقسام بزه‌دیدگان و اشخاص در معرض خطر بزه‌دیدگی و راهکارهای مصون‌سازی آنها چه در عرصه پیشگیری و چه واکنش در برابر متجاوزان، رک.: ابوالقاسم خدادی (۱۳۹۱). «راهکارهای افزایش حمایت از گروه‌های در معرض خطر بزه‌دیدگی»، رساله دکتری جزا و جرم‌شناسی، دانشگاه تهران و مهرداد رایجیان اصلی (۱۳۹۰). *بزه‌دیده‌شناسی حمایتی*، چاپ دوم، تهران، نشر دادگستر.

خود ناآگاه‌اند و گمان می‌برند همانند نامی که بر این دنیای پررمزوراز نهاده شده؛ یعنی فضای مجازی،[1] همه چیز جلوه‌ای غیرواقعی[2] دارد، بنابراین درصورت رویارویی با تهدیدها، چیزی را از دست نمی‌دهند (ویلیامز، ۱۳۹۱: ۹۲). در نتیجه به‌سادگی داشته‌ها و دارایی‌های ارزشمند الکترونیکی‌شان را به اشتراک یا بدتر از آن به حراج می‌گذارند و زمینه آسیب‌رسانی به خود را فراهم می‌آورند.

از جمله تهدیدهایی که بدون دستیابی به اطلاعات ابتدایی یک کاربر، امکان آسیب‌رسانی جدی به وی وجود ندارد، نقض حریم داده‌های الکترونیکی، سرقت و سوءاستفاده‌های گوناگون از آنهاست. این داده‌ها می‌تواند به امور شخصی یا خانوادگی، امور مالی و بانکداری یا کسب‌وکار و اداری مربوط شود. دسترسی غیرمجاز به آنها ممکن است پیامدهای ناگواری بیافریند و کاربر را با چالش‌های جدی روبه‌رو کند. سرآغاز این تهدیدها با دستیابی به اطلاعاتی رقم می‌خورد که کاربر، خواسته (داوطلبانه یا ارادی) یا ناخواسته در اختیار نفوذگران می‌گذارد (کیسی، ۱۳۸۶: ۲۹۳). برای مثال به‌کار بردن شماره‌های پرکاربرد (مانند ۱۲۳٤)، شماره شناسنامه یا کارت ملی که به‌آسانی از راه‌های دیگر به‌دست می‌آید، می‌تواند قلمروهای خصوصی الکترونیکی را با تهدیدهای گوناگونی روبه‌رو کند (بهره‌مند بگ‌نظر و جلالی فراهانی، ۱۳۹۱: ۱۴۴).

برای از بین بردن ناآگاهی و بالا بردن اطلاعات کاربران درباره تهدیدهای گوناگون سایبری، ضروری است تدابیر آموزشی عمومی و اختصاصی پیوسته و هماهنگی تعریف و اجرا شود. بنابراین در مجموعه تدابیر آگاهی‌بخش عمومی، مانند آشنایی با مفهوم و اقسام داده‌های شخصی، ارزش ذاتی و موارد کاربرد آنها، تهدیدهای پیش رو و راهکارهای صیانت از آنها، باید سطح یادگیری پایه کاربران نسبت به تهدیدهای رایج و مبتلابه هدف‌گذاری شود. این موضوع‌ها فقط به‌طورکلی و عمومی مطرح می‌شوند و توضیحات تفصیلی و تخصصی به آموزش‌های اختصاصی واگذار می‌شود.

در سطح تخصصی‌تر نیز همانند آنچه در دیگر برنامه‌های آموزشی آسیب‌های اجتماعی اجرا می‌شود باید آسیب‌دیدگان بالقوه را بر پایه تهدیدهای ویژه رده‌بندی و از

---

1. Virtual World
2. Unreal

یکدیگر متمایز کرد. برای مثال، کودکان به‌دلیل داشتن ویژگی‌هایی با تهدیدهایی روبه‌رو هستند که بزرگسالان از آنها در امانند و یا زنان نسبت به مردان در برابر برخی تهدیدها آسیب‌پذیرترند. شاغلان در بنگاه‌های اقتصادی و محیط‌های اداری نیز با تهدیدهایی روبه‌رویند که دیگر مشاغل و شهروندان شاید از آنها آگاهی و تجربه نداشته باشند، معلولان، سالمندان و مقامات و کارکنان مشاغل حساس و حیاتی نیز باید در رده‌های متمایزی گنجانده شوند (منفرد، ۱۳۹۱: ۱۰۷).

تدبیر صیانتی که عموماً کاربران در فضای سایبر به‌کار می‌گیرند، گمنام‌سازی[1] هویت واقعی‌شان است. برای مثال زنان و دختران در محیط‌های اجتماعی الکترونیکی برای صیانت از تهدیدهای احتمالی، با جنسیت مذکر یا ناآشنا حضور می‌یابند. این راهکار گرچه می‌تواند سودمند باشد، اما درصورت ناآگاهی از چگونگی به‌کارگیری آن، حتی می‌تواند بر تهدیدهای پیش رو بیفزاید. حضور در فضای سایبر با هویت گمنام به کاربر جرئت و پروای کاذبی می‌بخشد که به پشتوانه آن به آزمون عرصه‌های پرخطرتری رومی‌آورد، اما اوضاع هنگامی نگران‌کننده می‌شود که در کانون تهدیدها و خطرهای گوناگون هویت خویش را برملا کند (جلالی فراهانی، ۱۳۸۴: ۲۵).

حضور در فضای مجازی با هویت واقعی، آگاهانه و محتاطانه است و از انواع تهدیدها پیشگیری می‌کند و دیگران نیز از تجربه رفتارهای پرخطر با کاربر می‌پرهیزند. بنابراین نکته بسیار مهمی که باید در همه برنامه‌های آموزشی بر آن تأکید شود، این است که رویارویی کارآمد و اثربخش در برابر تهدیدهای سایبری در گرو نگاه واقع‌گرایانه از وضعیت، ظرفیت‌ها، توانمندی‌ها، کاستی‌ها و نارسایی‌های این حوزه است و شایسته نیست این تدبیرها به‌کار گرفته شود یا متولیان آموزشی آن را به‌عنوان یک گزینه معرفی کنند.

یکی از راه‌های مناسب برای آگاهی‌بخشی به آسیب‌دیدگان بالقوه سایبری، تدوین کدهای رفتاری[2] است. این مجموعه‌ها که با عناوینی چون منشورهای اخلاقی و حرفه‌ای[3] شناخته می‌شوند، عموماً برای بزهکاران بالقوه با هدف بازداری آنها از روآوری به بزهکاری

---

1. Anonymise
2. Codes of Conduct
3. Professional and Ethics Charters

با یادآوری پیامدهایی که در انتظار آنها خواهد بود (اعم از ضمانت اجراهای قراردادی، مقرراتی، مدنی و کیفری) تدوین می‌شوند. اما به‌نظر می‌رسد از این ظرفیت می‌توان برای بزه‌دیدگان بالقوه نیز بهره‌برداری و تهدیدهای پیش روی آنها را گوشزد کرد. ضمن اینکه ممکن است این آسیب‌ها برای‌شان مسئولیت‌هایی به دنبال داشته باشد که در این صورت با جدیت بیشتری به توصیه‌های ایمنی و امنیتی پایبند خواهند بود (منفرد، ۱۳۹۱: ۱۴۳).

۲-۱-۱ تأمین نیازمندی‌های فناورانه امنیتی

فقط آگاهی داشتن از تهدیدها برای پیشگیری از همه رخدادها کافی نیست و ضروری است به ابزارهای فناورانه امنیتی متناسب با آنها نیز تجهیز شد. بنابراین شناسایی، تفکیک و رده‌بندی گروه‌های در معرض خطر سایبری این مزیت را دارد که می‌توان ابزارهای فناورانه متناسب با تهدیدهای پیش روی هریک از آنها را تعریف و تهیه کرد. این موضوع ازآن‌رو اهمیت دارد که تهیه این ابزارها اساساً هزینه‌بر است و چنانچه کاربرد آنها به‌طور مطلوب ارزیابی و برآورد نشود، نه تنها تهدیدهای پیش رو را خنثی نمی‌کند بلکه ممکن است زمینه شکل‌گیری تهدیدهای جدید را فراهم آورد.

ابزارهای سخت‌افزاری یا نرم‌افزاری امنیتی ـ پیشگیرانه سایبری را یا کاربران و یا دیگر دست‌اندرکاران امور سایبری، به‌ویژه ارائه‌دهندگان خدمات به‌کار می‌برند. برای مثال، پالایش (فیلترینگ) محتوای مجرمانه الکترونیکی را هم ارائه‌دهندگان خدمات اینترنتی[1] و هم خود کاربران می‌توانند تنظیم و اجرا کنند. همچنین سامانه‌های پالایش محتوا را می‌توان سازگار با نوع کاربری و میزان آسیب‌پذیری کاربران تنظیم و اجرا کرد. برای مثال، پالایش محتوای در دسترس کودکان در مدارس و دیگر محیط‌های آموزشی و فرهنگی بر پایه فهرست‌های سپید صورت می‌گیرد، حال آنکه برای دیگران که پالایش حداقلی یا متعارف مدنظر است، به‌اصطلاح فهرست‌های سیاه به‌کار گرفته می‌شود (جلالی فراهانی، ۱۳۸۴: ۱۲۳).[2]

---

1. Internet Service Providers (ISPs)

۲. برای آگاهی از روند پالایش محتوای مجرمانه اینترنتی در ایران، رک.: مرکز پژوهش‌های مجلس شورای اسلامی، «تأملی بر فیلترینگ: ۱. اقدام پیشگیرانه از جرائم رایانه‌ای»، شماره ۸۳۷۱، خردادماه ۱۳۸٦؛ «تأملی بر فیلترینگ: ۲. مطالعه تطبیقی سایر کشورها»، شماره ۸٤٤۲، تیر ۱۳۸٦؛ «تأملی بر فیلترینگ: ۳. سالم‌سازی فضای سایبر و تعارضات ←

ابزارهـای فناورانـه دیگـر ماننـد انـواع ضـدویروس‌هـا، پویشـگرها[1] و شناسـاگرهای تهدیـد و تعرض‌های سایبری[2] از دیگر تمهیدات امنیتی پرکاربرد به‌شمار می‌آیند کـه بـا کاربردهـای عمـومی و ویژه طراحی و تولید می‌شوند. این ابزارها بیشتر برای تأمین امنیـت نسـبی رایانـه‌هـای رومیـزی[3] یـا روزانویی[4] مفیدند، اما برای مراکز مهـم، حسـاس و حیـاتی بایـد از سـامانه‌هـای پیشـرفته‌تـری ماننـد دیوارهای آتشین[5] بهره برد. مهم این است که با برآورد منطقـی تهدیـدهای احتمـالی، مناسـب‌تـرین ابزارها طراحی و تهیه شود. در غیر این صورت، باید در انتظار همان پیامدها بود.

نکته‌ای که درباره این‌گونه ابزارهای فناورانه ضروری اسـت، کوتـاهی عمـر آنهاسـت. پویایی همیشگی فناوری‌های اطلاعاتی و ارتباطی و پیدایش هرروزه فنون و ابزارهای نـوین، ناپایداری کارکرد و کارایی‌شان را در پی دارد و همین امر باعـث مـی‌شـود کـه همـواره بـه شیوه‌ها و روش‌های امنیتی نوین نیاز باشد و کوتاهی در این کار به بهـای تحمـل زیـان‌هـای ناروایی تمام شود (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۴۷). بـرای مثـال چنانچـه نسـخه روزآمـد یک نرم‌افزار ضدویروس خریداری، نصب و اجرا نشود، نمی‌توان به کارایی نسـخه کنـونی در برابر تهدید ویروسی جدید امیدوار بود و چـاره‌ای جـز تـأمین هزینـه آن نیسـت؛ گرچـه مدت کوتاهی از زمان خریداری این نسخه نگذشته باشد.

وجود این‌گونه مسائل، حمایت جـدی، پیوسـته و فراگیـر از آسـیب‌دیـدگان بـالقوه را ثابت می‌کند. در چنین وضعیتی، افراد بسیاری هسـتند کـه از تـأمین امنیـت خـویش سـر بـاز می‌زنند و از روزآمدسازی ابزارهای فناورانه‌شان به ستوه می‌آیند و بدتر آنکـه بـه ابزارهـای فناورانه نامعتبر رومی‌آورند که آسـیب‌هـای بـه‌مراتـب زیـان‌بـارتری را بـه‌بـار مـی‌آورنـد و دارایی‌های ارزشمند الکترونیکی‌شان را در برابر انواع تهدیدها، بی‌دفاع رها می‌کنند.

ازاین‌رو تهدیدهای جدی‌تری را می‌تواند برانگیـزد؛ زیـرا بـا توجـه بـه ماهیـت شـبکه‌ای

←موجود»، شماره ۸۵۷٤، مهر ۱۳۸٦؛ «تأملی بـر فیلترینـگ: ٤. مشـترک گرامـی دسترسـی بـه ایـن سـایت امکـان‌پـذیر نمی‌باشد»، شماره ۸۵۸۱، مهر ۱۳۸٦؛ «تأملی بر فیلترینگ: ۵. برنامه اقدام برای تحقق برنامـه سـالم‌سـازی فضـای سـایبر»، شماره ۸۹٤۷، اردیبهشت ۱۳۸۷؛ در تارنمای www.tarh.majlis.ir.

1. Scanner
2. Intrusion Detection System (IDS)
3. Desktop Computer
4. Laptop
5. Firewalls

فضای سایبر و ارتباط پیوسته کاربران با یکدیگر، آسیب هریک از آنها به زیان دیگران نیز می‌انجامد و ناخواسته سبب گسترش آن در محیط شبکه‌ای می‌شود. بسیارند هکرهایی که با پایگاه قرار دادن سامانه‌های کاربران بی‌گناه، حملات گسترده‌تر خود به سامانه‌های دیگران را برنامه‌ریزی و اجرا می‌کنند. بنابراین صیانت از هر کاربر به معنای صیانت از همه کاربران است و این نکته کلیدی باید در تعریف و اجرای تدبیرهای امنیتی سایبری لحاظ شود.[۱]

علاوه‌بر این هم‌گرایی شتابنده فناوری‌های ارتباطی، سامانه‌های رایانه‌ای و فرایندهای اطلاعاتی در عصر کنونی، بسیاری از ابعاد زندگی انسان‌ها را بیش‌ازپیش به فناوری‌های اطلاعاتی وابسته کرده است. امروزه، سامانه‌های رایانه‌ای شمار زیادی از محیط‌های کاری تفکیک‌ناپذیر مانند فرایندهای کسب‌وکار، محصولات صنعتی، اداره عمومی، بازارهای مالی و دیگر زیرساخت‌های مهم، مانند ایستگاه‌های [تأمین] نیروی متعارف، تأسیسات انرژی هسته‌ای، سامانه‌های ترافیک هوایی و دفاعی و سامانه‌های فرمان نظامی را تحت کنترل خود دارند (زیبر، ۱۳۸۸: ۲۶). درعین‌حال کشورهایی که بستر اصلی فعالیت‌هایشان فناوری اطلاعات است، آسیب‌پذیری بیشتری دارند. سامانه‌های حیاتی و حساس به‌طور خاص در معرض تهاجم‌ها و سوءاستفاده‌های مجرمانه هستند که از دلایل آن می‌توان پیچیدگی برنامه‌های رایانه‌ای، دسترسی شبکه‌های رایانه‌ای بین‌المللی، بی‌احتیاطی و بی‌مبالاتی کاربران در تأمین امنیت داده‌ها و سامانه‌ها، سوءمدیریت شبکه‌های داخلی شرکتی، سوءاستفاده افراد درون‌سازمانی و تهاجم هکرها از بیرون شرکت یا کشور اشاره کرد. این وضعیت، کشورها را در معرض خطرها و آسیب‌های بالقوه‌ای قرار می‌دهد که مهم‌ترین و نگران‌کننده‌ترین آنها خطر «تروریسم سایبری» و «جنگ سایبری» است که اساساً بر نقاط آسیب‌پذیر زیرساخت‌های حیاتی[۲] تمرکز دارند و سبب پیامدهایی در زیرساخت‌های اطلاعات می‌شوند.[۳]

---

۱. رک.: شرکت فناوری اطلاعات ایران مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر) (۱۳۸۸). *مجموعه مقالات و گزارشاتی درباره امنیت فضای تولید و تبادل اطلاعات* (ترجمه و گردآوری)، جلد اول و دوم، چاپ اول، نشر نهضت پویا.

2. Critical Information Infrastructure (CII)

۳. رک.: امیرحسین جلالی فراهانی (۱۳۸۵). «تروریسم سایبری»، فصلنامه *تخصصی فقه و حقوق*، تهران، پژوهشگاه فرهنگ و اندیشه اسلامی، سال سوم، ش ۱۰.

ازاین‌رو امروزه رویکرد عمومی دولت‌هایی که خدمات عمومی‌شان را الکترونیکی کرده‌اند، ارتقا و تضمین امنیت سامانه‌های اطلاعاتی دولت الکترونیکی، شامل داده‌ها، رایانه‌ها و شبکه‌هاست تا عملکرد بهینه امورشان را فراهم کنند. بنابراین ضروری است دولت‌ها پیش از آنکه با شتابزدگی و بی‌پروایی به دنبال گسترش شبکه‌های ارتباطی و «رایانه‌ای کردن»[1] زیرساخت‌های بنیادی و حیاتی مانند ایستگاه‌های انتقال نیرو، شبکه‌های پولی و بانکی، سیستم‌های حمل‌ونقل مجهز به سامانه‌های رایانه‌ای و تجهیزات پزشکی باشند، تدابیر امنیتی و حفاظتی متناسب با هر حوزه را پیش‌بینی و تقویت کنند. سازوکارهای امنیتی مؤثر به فرایندی نیازمند است که به دولت‌های دیجیتالی امکان می‌دهد به‌طور آگاهانه سطح قابل قبولی از امنیت را که در آن خطرهایی که تا حد کمینه کاهش یافته‌اند، مشخص سازند.

۲-۱ تدبیرهای واکنشی حمایتی

به‌رغم همه تدبیرهای کنشی و پیشگیرانه که برای صیانت از آسیب‌دیدگان بالقوه اتخاذ می‌شود، عده‌ای گرفتار تهدیدها شده و زیان‌های گوناگونی را متحمل می‌شوند. رهاسازی آنها در این مرحله نیز دو چالش اساسی در پی دارد: ۱. ممکن است آنها به آماج‌های همیشگی بزهکاران تبدیل شوند؛ و ۲. بر جرئت بزهکاران (تجری) افزوده شده و آنها بر تجربه‌های جنایی تازه‌ای روآورند. ضمن اینکه ممکن است بزه‌دیدگان خود سزای بزهکاران را بدهند که در این صورت بر بی‌نظمی‌ها افزوده خواهد شد. بنابراین ضرورت ایجاب می‌کند این فرایند حمایتی تا پایان ادامه یابد. حمایت واکنشی از آسیب‌دیدگان سایبری همانند بزه‌دیدگان و زیان‌دیدگان سایر آسیب‌های اجتماعی، می‌تواند به دو شکل صورت گیرد: نخست جبران زیان‌های وارده به آنها؛ دوم پیگرد و کیفر مرتکبان که در ادامه جلوه‌های سایبری این دو حوزه نیز بررسی و تحلیل می‌شود.

۱-۲-۱ جبران زیان‌های سایبری

در مقدمه نوشتار به انواع آماج‌های مادی و معنوی سایبری فردی و جمعی یا ملی اشاره شد.

---

1. Computerization

قاعدتاً هریک از این زیان‌ها سازوکار جبرانی[1] ویژه‌ای دارد که باید بر پایه قواعد عمومی حاکم بر نظام مسئولیت مدنی مورد توجه قرار گیرد.[2] ازاین‌رو در همین چارچوب تدابیر قابل اتخاذی برای جبران زیان‌های سایبری امکان‌سنجی و ارزیابی می‌شود.

در دنیای سایبر بنا به اینکه زیان‌دیده در آماج چه نوع تهدیدی قرار گیرد، ممکن است زیان‌های مادی و یا معنوی گوناگونی را متحمل شود: سامانه رایانه‌ای یا مخابراتی وی از کار بیفتد یا داده‌های رایانه‌ای وی تغییر کند، دست‌کاری شود، به‌کلی از بین برود یا حتی سرقت شود؛ اطلاعات شخصی، خانوادگی یا اسرارش در دسترس دیگران قرار گیرد و یا بدتر از همه فیلم، صوت یا تصویر وی با به‌کارگیری فناوری‌های رایانه‌ای به شکل مستهجن تحریف و منتشر شود. این رفتارهای ناپسند می‌تواند آسیب‌های حیثیتی جدی به سوژه اطلاعات[3] وارد آورد، به‌طوری‌که او را برای همیشه از حضور در عرصه‌های مختلف سایبری دور سازد.

برای جبران زیان‌های مادی رایانه‌ای، نخستین مسئله‌ای که باید درباره آن تصمیم‌گیری اساسی کرد، ارزش مالی داده‌های رایانه‌ای است، به این معنا که همانند دیگر اشیای دنیای خاکی، بتوان آنها را موضوع خرید و فروش قرار داد. در غیر این صورت نمی‌توان برای آنها دعوای جبران زیان مادی مطرح کرد. بسیاری از محاکم دادگستری و حتی مراجع تصمیم‌گیر قانونی، حتی کشورهای پیشرو در این عرصه نظیر ایالات متحده آمریکا، نخست برای داده‌های رایانه‌ای به‌دلیل ماهیت ناملموسشان[4] ارزش مالی قائل نبودند و درصورتی‌که به آنها آسیبی وارد می‌شد، فقط ارزش ابزار ذخیره‌ساز آن، مانند دیسک یا لوح فشرده را محاسبه می‌کردند، درحالی‌که ممکن بود ارزش داده‌های ذخیره شده در آن بالغ بر میلیون‌ها دلار باشد.[5]

موضوع بسیار مهم دیگر رسمیت بخشیدن، اعتباربخشی یا استنادپذیری داده‌های

---

1. Remedial Measure

۲. رک.: حسن ره‌پیک (۱۳۸۸). *حقوق مسئولیت مدنی و جبران‌ها*، چاپ پنجم، تهران، نشر خرسندی.

3. Data Subject

شخصی که اطلاعات به او مربوط می‌شود و لزوماً دارنده آن نیست.

4. Intangible Objects V. Tangible Objects

۵. رک.: حسین صادقی (۱۳۸۶). «مسئولیت مدنی در ارتباطات الکترونیکی»، رساله دکتری حقوق خصوصی، دانشگاه تهران.

رایانه‌ای به‌عنوان ادله قابل استناد در دعاوی است.[۱] بی‌گمان هنگامی که به داده واجد ارزش مالی زیانی وارد می‌شود، بهترین دلیل برای اثبات این مدعا، داده‌های رایانه‌ای است. اما چنانچه نتوان به این ادله استناد کرد، با وجود احکام قانونی پذیرنده زیان رایانه‌ای، امکان مطالبه و استیفای آن وجود نخواهد داشت. پس این موضوع که تغییر شکل اسناد کاغذی به الکترونیکی تغییری در ماهیت آنها پدید نمی‌آورد و با رعایت برخی معیارها و قواعد عمومی می‌تواند مورد استناد قرار گیرد باید برای مراجع صلاحیت‌دار رسیدگی به دعاوی زیان‌های رایانه‌ای حل شود.

بااین‌حال صِرف فراهم آمدن این نیازمندی‌ها که البته از ارکان اساسی جبران زیان‌های الکترونیکی به‌شمار می‌آیند، نمی‌تواند به تحقق اهداف این حوزه کمک کند ازاین‌رو باید سازوکارهای اجرایی آنها نیز فراهم شود. برای مثال چنانچه یک نرم‌افزار واجد حق نشر، مورد سوءاستفاده قرار گیرد و زیان‌هایی را به دارنده این حق وارد کند، باید بتوان زیان وارده را محاسبه و تعیین کرد. همچنین در جایی که نام کاربری و گذرواژه مربوط به امور مالی الکترونیکی فردی ربوده می‌شود، باید امکان محاسبه و برآورد زیان‌های مالی وجود داشته باشد؛ اما این کار زمانی دشوار می‌شود که از اسرار تجاری الکترونیکی شخص هم سوءاستفاده شده باشد که در این صورت، باید عواید به‌دست آمده از کاربری‌های ناروای این اطلاعات شناسایی و میزان زیان‌های وارده به دارنده اسرار محاسبه شود.

در زیان‌های معنوی که حیثیت افراد آسیب می‌بیند به‌طورقطع اعاده حیثیت در دستور کار قرار می‌گیرد. بنابراین باید به همان شکل و در همان وضعیت و موقعیتی که حیثیت هتک شده، اعاده آن به‌عمل آید. برای مثال چنانچه در تارنمایی به شخص توهین شده، اعتذار مرتکب در همانجا درج شود یا چنانچه خبر کذبی به وی نسبت داده شود، به همان ترتیب تکذیبیه آن در برابر دیدگان مخاطبان قرار گیرد.[۲] هرچند اذعان می‌شود اجرای چنین احکامی به تجربه و آزمون‌های بسیاری بستگی دارد و صرف وجود قوانین و مقرراتی نمی‌توان

---

۱. ر.ک.: عبدالله شمس (۱۳۸۹). *ادله اثبات دعوی حقوق ماهوی و شکلی*، چاپ هشتم، نشر دراک.

۲. ر.ک.: قاسم محمدی (۱۳۹۰). *جرم مطبوعاتی*، چاپ اول، تهران، سازمان مطالعه و تدوین کتب دانشگاهی علوم انسانی (سمت).

به‌طور شایسته زمینه جبران زیان‌های معنوی سایبری را فراهم آورد (انصاری، ۱۳۹۰: ۳۰۲).

برای اثبات زیان‌های مادی و معنوی الکترونیکی، باید ادله پشتیبان آنها را به‌درستی گردآوری کرد. برخی از این داده‌ها در اختیار بزهکار است، برخی دیگر در اختیار زیان‌دیده و یا ارائه‌دهنده خدمات. برای مثال بزهکار ممکن است محتوای توهین‌آمیز در تارنما را فوراً با محتوای دیگری جایگزین کند. در اینجا چنانچه زیان‌دیده این داده‌ها را در اختیار نداشته باشد، نمی‌تواند ادعای خود را در دادگاه ثابت کند. همچنین چنانچه مؤسسه مالی و اعتباری یا هر بانکی، اطلاعات تراکنش‌های مالی را نگهداری نکند، نمی‌تواند سوءاستفاده‌های به‌عمل آمده را از حساب الکترونیکی به اثبات رساند. بنابراین وجود یک نظام ذخیره و نگهداری اطلاعات کاربری‌های گوناگون الکترونیکی، از جمله نیازهای حیاتی استیفای حقوق ازدست‌رفته زیان‌دیدگان به‌شمار می‌آید.

سرانجام هدف‌گذاری برای جبران حداکثری زیان‌های مادی وارده به آسیب‌دیدگان سایبری می‌تواند به تعریف تدبیرهای نوآورانه بینجامد. بیمه سایبری راهکار رو به‌گسترشی است که با الهام از دنیای خاکی مورد توجه قرار گرفته است. ممکن است مسببان زیان‌های رایانه‌ای شناسایی و مسئول شناخته نشوند یا نتوان همه زیان‌های وارده را از آنها بازستاند و آسیب‌های وارده را به شکل متعارفی جبران کرد و یا از سامانه کاربر بدون آگاهی وی برای آسیب رساندن به دیگران بهره‌برداری شده باشد که در این صورت، ازلحاظ قانونی وی مسئول جبران زیان‌های وارده است. در پرتو چنین رویکردی، بیمه سایبری می‌تواند پاسخ‌گوی مسئولیت‌های احتمالی کاربران باشد و آن را تضمین کند. این تدبیر با ایجاد اطمینان به جبران زیان‌های وارده در فضای سایبر اعتماد ذی‌نفعان این حوزه را تأمین می‌کند و با رویکرد کنشگرانه و به عبارتی پیشگیرانه، جبران‌ناپذیری زیان‌های سایبری را به حداقل می‌رساند (کلانتری و سجادی، ۱۳۹۰: ۱۸۸).

۲-۲-۱ پیگرد بزهکاران سایبری

بخشی از زیان‌های رایانه‌ای در پی نیات سوء و پلید ایجاد نمی‌شوند، بلکه ممکن است یک رخداد یا حداکثر بی‌احتیاطی یا بی‌مبالاتی زمینه آن را فراهم آورد. بنابراین حکم به جبران زیان وارده می‌تواند کافی باشد، گرچه در مواردی به‌دلیل اهمیت و حساسیت موضوع،

ممکن است همان بی‌احتیاطی و بی‌مبالاتی نیز موضوع ضمانت اجراهای قراردادی، مقرراتی و حتی فراتر از آن؛ کیفر قرار گیرد.[۱]

هدف از وضع ضمانت اجراها،[۲] تضمین درستکاری است و حسب اینکه کار مورد نظر ازسوی و برای کدام مرجع تعریف و اجرا می‌شود، ضمانت اجرای آن متفاوت است. گاهی کار به‌موجب قرارداد تعریف می‌شود؛ پس ضمانت اجرای آن قراردادی است. گاهی کار را دستگاه اجرایی تفویض می‌کند که در این صورت برای آن ضمانت اجرای مقرراتی پیش‌بینی می‌شود. گاهی کار جلوه‌ای عمومی و ملی پیدا می‌کند که ضمانت اجرای آن را قانونگذار معین می‌کند. چنانچه قانونگذار سوءنیتی را در ایفای کار نبیند، به جبران زیان‌های مادی و معنوی بسنده می‌کند، اما اگر آن را محرز بداند، ممکن است به کمتر از کیفر بسنده نکند.

کیفر سنگین‌ترین ضمانت اجرای اجتماعی است که برای بداندیشان و هنجارشکنان در نظر گرفته می‌شود. با کیفر دادن به جان، آبرو، مال و آزادی مرتکب لطمه وارد می‌شود تا ازیک‌سو دوباره در پی ارتکاب جرم نباشد و ازدیگرسو، اعضای جامعه با دیدن هزینه‌ای که وی پرداخته از تحقق نیات شومشان خودداری کنند.[۳] بااین‌حال، ازآنجاکه کیفر خود هزینه‌ها و پیامدهای گوناگونی را بر جامعه تحمیل می‌کند، همواره آخرین حربه[۴] در برقراری نظم اجتماعی به‌کار می‌رود و در همین مرحله نیز برای تضمین حقوق و آزادی‌های مشروع شهروندان، اصول و قواعد سخت و الزام‌آوری برای مجریان قانون در اعمال قوانین و مقررات کیفری پیش‌بینی شده که عدم رعایت آنها می‌تواند به بی‌اعتباری فرایند کیفری بینجامد و مرتکب را به‌رغم ارتکاب رفتار ناپسند مجرمانه و وارد آوردن زیان‌های گوناگون به شهروندان و جامعه، از کیفر در امان دارد.

نخستین اصل حاکم بر کیفر رفتارهای ناپسند اجتماعی، قانونی بودن جرائم و مجازات‌هاست. بر پایه این اصل هیچ فردی را نمی‌توان به‌دلیل رفتار ناپسندش کیفر کرد

---

۱. برای مثال ماده (۹۴۸) قانون مجازات اسلامی، بی‌احتیاطی و بی‌مبالاتی زمینه‌ساز جاسوسی رایانه‌ای را جرم‌انگاری کرده است.

2. Sanctions

۳. رک.: برنار بولک (۱۳۸۷). *کیفرشناسی* (ویراست پنجم)، ترجمه علی‌حسین نجفی ابرندآبادی، چاپ هشتم، تهران، نشر مجد.

4. Ultima Ratio

مگر اینکه در قانون آن رفتار به‌دقت تعریف و کیفر آن مشخص شده باشد. این اصل از اعمال سلیقه‌های شخصی نظام عدالت کیفری در برخورد با رفتارهای ناپسند اجتماعی جلوگیری می‌کند. ازاین‌رو اصل منشعب برائت یا تفسیر مضیق یا محدود به‌نفع متهمان برگرفته شده است. در اینجا از تسری مواردی جلوگیری می‌شود که با تعریف به‌عمل آمده از جرم در قانون سازگاری ندارند. برای مثال چنانچه جرم به نحوی تعریف شده باشد که ارتکاب آن فقط به ابزار یا شگرد خاصی محدود شده باشد و مرتکب از ابزار یا شگرد دیگر استفاده کرده باشد، از کیفر معاف خواهد بود. همچنین اگر برای آماج یا موضوع یا بزه‌دیده جرم ویژگی‌هایی ذکر شده باشد، درصورت ناسازگاری آنها با ویژگی‌های مطرح شده در پرونده، ادامه رسیدگی منتفی و قرار منع تعقیب کیفری صادر می‌شود.

این وضعیت در رویارویی با پدیده‌های نو و فناوری‌های نوآورانه آشکارا دیده می‌شود که از آنها سوءاستفاده‌های گوناگون به‌عمل می‌آید، و اتفاقاً با همین توجیه می‌توان بزهکاران را یکی از پیشتازان عرصه‌های دانش و نوآوری دانست! زیرا آنها می‌کوشند برای ارتکاب جرائمشان از ابزارها و شیوه‌هایی استفاده کنند که قانونگذار آنها را پیش‌بینی نکرده است تا بتوانند از گزند آن در امان بمانند. هرچند گاهی همان شیوه‌ها و ابزارها با گرایش و کاربری گسترده به‌تدریج جایگزین شیوه‌ها و ابزارهای پیشین می‌شوند و جلوه‌ای بهنجار می‌گیرند. از جمله احکام کیفری که در برخورد با سوءاستفاده‌های نوین با نارسایی روبه‌رو شده، نشر اکاذیب است. ازآنجاکه قانون مجازات اسلامی، مصوب ۱۳۷۰، این جرم را فقط با پخش کردن یا توزیع اوراق و اسناد کاغذی قابل تحقق می‌دانست (ماده ٦٩٨)، پراکندن محتوای کذب رایانه‌ای در تارنماهای شبکه‌ای را دربرنمی‌گرفت و مرتکب چنین رفتاری از کیفر در امان می‌ماند. درحالی‌که گستره اطلاع‌رسانی یک تارنمای شبکه‌ای بسیار بسیار بیشتر از کاغذهایی است که در یک منطقه پخش می‌شوند و هتک حیثیت به‌مراتب جدی‌تری را برای بزه‌دیده همراه دارد.

همچنین هنگامی که قانونگذار جعل را فقط روی اسناد کاغذی قابل تحقق می‌داند، ارتکاب آن بر داده‌های الکترونیکی مشمول عنوان مجرمانه جعل نمی‌شود. یا در جایی که از تخریب اموال صحبت می‌شود، مصادیق آن چیزهای ملموس است و موارد ناملموس را دربرنمی‌گیرد. ازاین‌رو برای اینکه تخریب یا از کار انداختن یا مختل کردن پدیده‌های

ناملموس از حمایت کیفری بهره‌مند شوند، باید این‌گونه مصادیق نیز به تعریف موضوعات جنایی آنها افزوده شود. حتی در هتک حریم منازل و املاک غیر نیز این نکته مشهود است. ممکن است چنین پنداشته شود که حریم خصوصی به هر موقعیتی گفته می‌شود که عرفاً صاحب آن انتظار دارد دیگران از آگاهی درباره آن با هریک از حواس پنج‌گانه بدون رضایت وی خودداری کنند و قاعدتاً شامل هر موقعیت مکانی و غیرمکانی می‌شود.[۱] ولی هنگامی که قرار است تعرض به این موقعیت از حمایت کیفری برخوردار شود، ضروری است مصادیق مشمول آن به‌روشنی معلوم شود و به همین دلیل از نخستین رفتارهای ناپسندی که کشورها در جرم‌انگاری آن تردید نکرده‌اند، دسترسی یا نفوذ غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای[۲] یا همان هکینگ[۳] در کنار هتک حریم املاک و منازل است.

به‌این‌ترتیب با پیدایش و گسترش هر فناوری، کار حوزه قانونگذاری دوچندان می‌شود زیرا با وضع قوانین کیفری برای حفظ نظم و حمایت از آسیب‌دیدگان بالقوه احتمال دور زدن بزهکاران را می‌گیرد. در غیر این صورت، بزه‌دیدگان در برابر سوداگری‌های تبهکاران بی‌دفاع می‌مانند. یکی از شیوه‌هایی که قانونگذاران کشورها به‌طور جدی‌تر در تدوین قوانین کیفری به‌کار گرفته‌اند، قانونگذاری مستقل از فناوری یا فناوری خنثی[۴] است. در اینجا قانونگذار بی‌آنکه از ابزار، شیوه یا روش خاصی در ارتکاب جرم نام ببرد، به تعریف رفتار ناپسند می‌پردازد. برای مثال توهین می‌تواند به شکل گفتاری یا کرداری باشد و در محیطی اعم از فیزیکی یا الکترونیکی ارتکاب یابد. حال این هنر قانونگذار است که به نحوی این رفتار ناپسند را جرم‌انگاری کند که همه جنبه‌ها و جلوه‌های آن را دربرگیرد.[۵]

پس از جرم‌انگاری و کیفرگذاری برای نمونه‌های نوپدید سوءاستفاده‌آمیز سایبری با

---

۱. ماده (۱) لایحه حمایت از حریم خصوصی که دولت هشتم تقدیم مجلس شورای اسلامی کرده بود، حریم خصوصی را چنین تعریف کرده است: «قلمروی از زندگی هر شخص است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند. جسم، البسه و اشیای همراه افراد، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می‌شوند» (انصاری، ۱۳۸٦: ۳۱٦).

2. Illegal Access to Computer Data and System

3. Hacking

4. Technology Neutral

۵. مانند ماده (٦۰۸) قانون مجازات اسلامی که به‌موجب استفساریه ۱۳۷۹ اصلاح شد تا توهین کرداری را نیز دربرگیرد.

هدف حمایت از کاربران زیان‌دیده، باید آیین رسیدگی به این جرائم سامان‌دهی شود. همانند نظام آیین دادرسی مدنی، در اینجا نیز برای استنادپذیر بودن داده‌های رایانه‌ای به‌عنوان ادله قابل اثبات کیفری، باید سازوکارهای ویژه آن تعریف و اجرا شود؛ به‌ویژه آنکه در دنیای دیجیتال فرایندهای تفتیش و توقیف ادله، شنود، مستندسازی و بازسازی فرایند جنایی نیز مطرح است که ضرورت تعریف سازوکارهای کشف علمی جرائم رایانه‌ای را گریزناپذیر می‌سازد.

هنگامی زیان‌دیدگان سایبری به‌رغم رویارویی با تهدیدهای سایبری احساس امنیت می‌کنند که دریابند مجریان قانون دست‌کم از دانش و توانمندی هم‌سطح مجرمان رایانه‌ای برخوردارند و می‌توانند جرم ارتکابی آنها را شناسایی و با گردآوری ادله اثبات کافی، موجبات محکومیت و کیفر آنها را فراهم آورند. اما اگر آنها نتوانند از عهده رسیدگی به ساده‌ترین جرائم رایانه‌ای برآیند، زیان‌دیدگان دچار سرخوردگی شده و ممکن است خود به استیفای حق خویش روآورند که این امر برای نظام حاکمیت ملی پیامد مطلوبی ندارد.

نخستین حقوق و انتظاری که بزه‌دیدگان سایبری از مجریان قانون دارند، بهره‌مندی از خطوط ارتباطی دائمی (۲٤×۷) برای اعلام شکایات جنایی است. مجریان قانون باید بتوانند تمهیدات لازم برای ایمن‌سازی آنها، حفظ ادله جرم و شناسایی متهمان را سریع به اجرا درآورند.[1] حتی فراتر از آن، باید همانند دنیای فیزیکی پلیس گشت سایبر[2] وجود داشته باشد تا کاربران از حضور آنها در دنیای سایبر احساس امنیت مطلوبی داشته باشند و پلیس جلوه‌ای از آماده‌باش سایبری[3] خود را به نمایش گذارد. همچنین با اجرای تدابیر امنیتی ویژه مانند دام‌گستری،[4] به بزهکاران بالقوه نشان دهد که در موقعیت‌های جنایی گوناگون حضور دارد و بر هزینه جنایی آنها به نحو جبران‌ناپذیری بیفزاید.

---

۱. طبق ماده (۳۵) کنوانسیون جرائم سایبر شورای اروپا، «اعضا موظف‌اند یک مرکز تماس ۲٤ ساعته در دسترس در هفت روز هفته را تأسیس کنند تا معاضدت فوری جهت تحقیقات یا رسیدگی‌های کیفری مرتبط با داده‌ها و سیستم‌های رایانه‌ای یا جمع‌آوری ادله الکترونیکی جرائم را تضمین کنند. چنانچه رویه قضایی یا قوانین داخلی اجازه دهد، معاضدت مزبور باید به‌طور مستقیم شامل فراهم آوردن تسهیلات ذیل باشد: الف) مشاوره فنی؛ ب) حفظ داده‌ها مطابق مواد (۲۹) و (۳۰)؛ و پ) جمع‌آوری ادله، ارائه اطلاعات قانونی و مکان‌یابی متهمان» (جلالی فراهانی، ۱۳۸۹: ۱۱۲).

2. Cyber Patrol Police
3. Cyber Alert
4. Entrapment

۲ نقش قانونگذار در حمایت از آسیب‌دیدگان سایبری

در آغاز مقاله اشاره شد که حفظ نظم در جامعه وظیفه‌ای ملی است و برای اینکه همگان در ایفای چنین وظیفه‌ای مرتکب بی‌نظمی نشوند، مجموعه‌ای از بایدها و نبایدها بر پایه تشریفات از پیش تعریف شده رسمی انشا و به مخاطبان ابلاغ می‌شود. یکتایی مرجع انشای این احکام خود از ابزارهای برپایی نظم است و از دوگانگی، چندگانگی و در پی آن تغایر و تعارض احکام با یکدیگر جلوگیری می‌کند. این مرجع یگانه که براساس رهنمودهای مرجع بالادستی خود و هم‌سو با سیاست‌های راهبردی آن به تدوین و تنظیم این احکام می‌پردازد، قانونگذار نام دارد.

در همه کشورهای دارای نظام حاکمیتی یکپارچه، مسئولیت تعریف حق‌ها و تکالیف همه اعضای جامعه حتی مقامات و کارگزاران دستگاه‌های اجرایی برعهده قوه قانونگذاری است و هیچ مرجع حاکمیتی دیگری حق چنین اقدامی ندارد. فقط قانونگذار است که می‌تواند به اعضای جامعه بگوید چه کاری انجام دهند و از کدام کار بپرهیزند. سپس بر پایه احکام قانونی موضوعه، دستگاه‌های اجرایی ذی‌ربط مقررات یا آیین‌نامه‌های اجرایی متناسب را تدوین و اجرا می‌کنند. فلسفه تدوین آیین‌نامه‌های اجرایی این است که مجریان قانون از حدود وظایف و اختیارات تعریف شده در نص قانون فراتر نروند و امکان کنترل و نظارت بر آنها وجود داشته باشد. همچنین در نظام‌های حاکمیتی، مرجعی برای نقض آیین‌نامه‌های مغایر احکام قانونی پیش‌بینی شده که در کشور ما این وظیفه به عهده دیوان عدالت اداری است.

نکته بسیار مهمی که در باب قانونگذاری باید توجه شود این است که چنانچه حقی برای شخصی پیش‌بینی می‌شود، باید تکلیف متناظر آن برای شخصی که مسئولیت متوجه اوست نیز پیش‌بینی شود، در غیر این صورت قانون جنبه فرمایشی پیدا می‌کند و اجرا نمی‌شود. اگر قانونگذار درصدد حمایتِ گروهی از افراد جامعه برمی‌آید، باید مراجع مسئول و همچنین اقداماتی که باید صورت گیرد را معرفی و تعریف کند و قواعد و ضوابط حاکم بر چگونگی استیفای حق‌ها را ازسوی ذی‌نفعان شرح دهد. در این صورت می‌توان به کارایی و اثربخشی حکم قانونی امیدوار بود.

حمایت قانونی از آسیب‌دیدگان سایبری نیز به‌درستی از همین رویه پیروی می‌کند. با توجه به اینکه در اینجا هر حکم قانونی می‌تواند جلوه احقاقی و استحقاقی بیابد، به این معنا

که گروهی از افراد جامعه آن را مطالبه کنند، باید در برابر آن مسئولانی شناسایی و معرفی شوند و چنانچه قواعد و ضوابط حاکم بر این حوزه نیازمند بازنگری است، قانونگذار باید به آن اهتمام ورزد.

۱-۲ نهادسازی حمایتی از آسیب‌های سایبری

برخلاف عنوانی که برای نهادسازی[1] برگزیده شد لزوماً ایجاد ساختار و تشکیلات حاکمیتی جدید در بدنه دولت نیست که اگر فقط چنین مفهومی از آن استنباط شود، با رویکرد کلان کوچک‌سازی اندازه دولت[2] در تعارض است. مهم ایفای تکلیفی است که قانونگذار مقرر کرده و بر همین اساس باید دید چگونه می‌توان ساختار و تشکیلات متناظر آن را تعریف و عملیاتی کرد. ممکن است نهاد(های) کنونی توانایی پیشبرد وظایف جدید را داشته باشند و فقط به فرمان قانونگذار نیاز باشد؛ یا اینکه نهاد(های) کنونی با کاستی‌هایی روبه‌رو باشند که درصورت رفع آنها بتوان از توانمندی‌شان بهره برد و سرانجام ممکن است به‌دلیل نوآورانه بودن موضوعی، اساساً هیچ نهادی تاکنون تولی و تصدی آن را به عهده نگرفته باشد و در صلاحیت و ظرفیت هیچ‌یک از نهادهای کنونی هم نباشد و چاره‌ای جز تأسیس یک نهاد حاکمیتی جدید نباشد. در این صورت تشکیل این نهاد و تعیین وظایف و اختیارات آن به عهده قانونگذار خواهد بود.[3] با این درآمد به امکان‌سنجی نهادسازی حمایتی از آسیب‌دیدگان سایبری می‌پردازیم.

۱-۱-۲ نهادسازی پیشگیرانه

درخصوص تدابیر آگاهی‌بخش عمومی و اختصاصی سایبری، با توجه به گستردگی و گوناگونی مخاطبان، تهدیدها و آسیب‌ها به‌نظر می‌رسد تأسیس نهادی متولی برای مدیریت

---

1. Institution Building

۲. در بند «الف» سیاست‌های کلی اصل (۴۴) «سیاست‌های کلی توسعه بخش‌های غیردولتی و جلوگیری از بزرگ شدن بخش دولتی» آمده است.

۳. برای آگاهی از رویکردها و الگوهای نهادسازی مبارزه با فساد، مزیت‌ها و محدودیت‌های پیش روی هریک از آنها رک.: پیتر لانگست و دیگران (۱۳۸۷). *برنامه‌های جهانی مبارزه با فساد*، ترجمه امیرحسین جلالی فراهانی و حمید بهره‌مند بگ‌نظر، چاپ اول، تهران، مرکز پژوهش‌های مجلس شورای اسلامی.

یکپارچه امکان‌پذیر نباشد و کارایی و اثربخشی لازم را نداشته باشد. ازاین‌رو برای تدبیرگزینی نهادی می‌توان میان نهادهای متولی فرهنگ، آموزش و پرورش عمومی و اختصاصی تفکیک قائل شد. درخصوص امور عمومی سایبری، گزینه مناسب این است که هریک از نهادهای متولی در چارچوب وظایف و اختیارات خود به این امر مبادرت ورزند. برای مثال متولیان امور رسانه‌ای اعم از دیداری و شنیداری، رسانه‌های مکتوب و الکترونیکی در کنار برشمردن آسیب‌های اجتماعی عمومی، بخشی از برنامه‌های خود را به آسیب‌های سایبری اختصاص دهند.

بدیهی است برای این کار به نیرو و امکانات ویژه‌ای نیاز خواهد بود، اما در حدی نیست که ساختار و تشکیلات جداگانه‌ای پیش‌بینی شود. بنابراین کافی است، قانونگذار دستگاه‌های اجرایی ذی‌ربط را احصا کند و مشخصاً درباره تولید برنامه‌ها و محتواهای آموزشی سایبری وظایف آنها را برشمرد. ضمن اینکه قانونگذار می‌تواند دستگاه‌های ذی‌ربط را مکلف کند برای برنامه‌ها و محتواهای مربوط به این حوزه امتیازات و تسهیلات ویژه‌ای قائل شود. برای مثال پخش چنین محتواهایی از معافیت‌های هزینه‌ای برخوردار باشند و چنانچه قانونگذار چنین مجوزی را به دستگاه‌های ذی‌ربط اعطا کند، آسان‌تر می‌توانند در این حوزه‌ها سرمایه‌گذاری کنند و دستاوردهای آن زودتر دیده می‌شود.

برای تدابیر آموزشی اختصاصی، قانونگذار می‌تواند رویکرد سخت‌گیرانه‌تری را پیش گیرد و حتی یک یا چند نهاد متولی حوزه‌های مختلف سایبری را مکلف به ارائه آموزش‌های اختصاصی یا تدوین محتواهای آموزشی هدفمند و پاسخ‌گومحور کند و حتی در فواصل زمانی معین گزارش پیشرفت خود را به کمیسیون‌های تخصصی و ذی‌ربط خود (مانند کمیسیون فرهنگی) ارائه کند. هرچند حکم قانونی در مبارزه با جرائم فساد پیش‌بینی و دولت مکلف شده منشورهای اخلاق حرفه‌ای را با چنین رویکردی تدوین و لازم‌الاجرا کند.[1]

درخصوص کدهای رفتاری و منشورهای اخلاقی سایبری می‌توان دستگاه‌های اجرایی مختلفی را متولی تدوین و ابلاغ آنها کرد. برای مثال وزارت ارتباطات و فناوری اطلاعات با تکیه بر آسیب‌های فناورانه، وزارت فرهنگ و ارشاد اسلامی با تکیه بر آسیب‌های

---

۱. ماده (۷) قانون ارتقای سلامت نظام اداری و مقابله با فساد.

فرهنگی و وزارت اقتصاد و دارایی با تکیه بر آسیب‌های مالی سایبری به این امر مبادرت ورزند. مزیت کدها این است که دستگاه‌ها مجبورند وظایف ارکان و عوامل زیرمجموعه خود را به‌ویژه در تعامل‌های بین‌نهادی‌شان با دیگر دستگاه‌ها به‌طور شفاف تبیین و تعریف کنند که این اقدام خودبه‌خود به قوه قانونگذاری در ایفای وظیفه نظارتی‌اش یاری می‌رساند. پس دیگر نیازی به تأسیس نهاد متولی اختصاصی نیست و کافی است نهادهای متولی کنونی نسبت به مدون‌سازی و پاسخ‌گوسازی عوامل زیرمجموعه‌شان با کدهای رفتاری یا نظایر آن مکلف شوند.

در مرحله ایمن‌سازی آسیب‌دیدگان بالقوه سایبری، با توجه به طیف آماج‌هایی که برشمرده شد و پیامدهای ناگواری که ممکن است بر کشور تحمیل شود، چنانچه قانونگذار تصمیم بگیرد دست‌کم برای امور حیاتی، حساس و مهم سایبری نهاد متولی ویژه‌ای را در قالب یک سازمان دولتی پیش‌بینی کند، این اقدام می‌تواند بر میزان مسئولیت‌پذیری و پاسخ‌گویی نهاد مذکور بیفزاید؛ زیرا در ازای بهره‌مندی از ردیف بودجه مستقل، وظایف و اختیارات ویژه‌ای برای آن تعریف می‌شود. ضمن اینکه بالاترین مقام اجرایی آن مانند وزارت ارتباطات و فناوری اطلاعات، مسئولیت پاسخ‌گویی به امور آن را به عهده دارد.

این مراجع که از آنها به نیروهای واکنش سریع سایبری[1] یاد می‌شود، وظیفه شناسایی و خنثی‌سازی تهدیدها و همچنین بازیابی سامانه‌ها یا داده‌های آسیب‌دیده را به عهده دارند. آنها باید توان دریافت گزارش‌های رویدادها از مراجع مختلف و حتی کاربران و همچنین پاسخ‌گویی به آنها را به‌طور پیوسته و هماهنگ داشته باشند و بتوانند نقاط اصلی تهدیدآفرین را شناسایی و با همکاری مجریان قانون اقدامات قانونی را در دستور کار قرار دهند. گفتنی است قانونگذار برنامه چهارم توسعه پیرو بند «ج» ماده (۴۴) دولت را مکلف کرده بود «سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور» را تهیه و به تصویب برساند که قاعدتاً یکی از سرفصل‌های اصلی آن مرجع متولی امنیت این حوزه بود. در قانون برنامه پنج‌ساله پنجم توسعه، ماده (٤٦) وزارت ارتباطات و فناوری اطلاعات را متولی این امر کرده که این وزارتخانه نیز سازمان فناوری اطلاعات را با شرح وظایفی از جمله تأمین امنیت فناورانه این

1. Computer Emergency Response Team (CERT)

حوزه تأسیس و اساسنامه آن را به تصویب هیئت وزیران رسانیده و پیرو آن مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای) را تأسیس کرده است.[۱]

علاوه‌براین برخی تمهیدات ایمنی سایبری به‌دلیل ماهیت محدودکننده و حتی در مواردی سلب‌کننده آسایش و آسانی کاربری، باید مراجعی انجام دهند که از صلاحیت‌های ویژه‌ای برخوردارند و تشریفات ویژه‌ای را برای اجرای تدابیر خویش به‌کار می‌گیرند. درصورتی‌که چنین مراجعی وجود نداشته باشد، ضروری است نسبت به وضع احکام قانونی برای تعریف وظایف و اختیارات آنها اقدام شود.

از جمله تمهیدات پیشگیرانه فنی که تأثیر چشمگیری بر یکی از موازین حقوق بشری سایبری، یعنی آزادی اطلاعات یا جریان آزاد اطلاعات دارد، پالایش محتوای مجرمانه اینترنتی است. برای کمینه‌سازی آثار سوء این اقدام پیشگیرانه در استیفای این حق و بیشینه‌سازی دستاوردهای آن باید مرجع صلاحیت‌داری متشکل از همه عوامل تصمیم‌ساز و تصمیم‌گیر فنی، اجتماعی و اجرایی زیرنظر مقام صلاحیت‌دار قضایی به تدوین فهرست‌های فنی پالایش اقدام کنند. یادآور می‌شود قانونگذار جرائم رایانه‌ای، در ماده (۷۵۰) قانون مجازات اسلامی کمیته تعیین مصادیق محتوای مجرمانه رایانه‌ای را با همین هدف تأسیس کرده است.

فراتر از آن، تمهیدات پیشگیرانه تعرض‌آمیزتری مانند نظارت الکترونیکی[۲] یا حتی شنود[۳] ارتباطات غیرعمومی الکترونیکی را باید مرجع صلاحیت‌دار ویژه‌ای مدیریت و اجرا کند (موضوع ماده (۷۷۶) قانون مجازات اسلامی). حتی حق اجرای فنون تحقیقاتی ویژه پیشگیرانه‌ای مانند دام‌گستری نباید به هر مرجع صلاحیت‌دار عمومی واگذار شود. چنانچه قانونگذار به تأسیس نهاد ویژه‌ای اقدام نکند، دست‌کم مأموران دستگاه‌های متولی کنونی باید شرایط احراز تصدی این امور را داشته باشند و به‌طور مشخص آنها را در برابر مسئولیت‌هایشان پاسخ‌گو نگاه دارد و حتی برای نقض وظایف قانونی‌شان ضمانت اجراهایی را پیش‌بینی کند.

---

۱. در این قانون مواد دیگری نیز به امنیت ارتباطات و اطلاعات مخابراتی و رایانه‌ای پرداخته‌اند که می‌توان به مواد (٤٩)، (۲۰۵)، (۲۰۸)، (۲۱۱ بند «ح») و (۲۳۱) اشاره کرد.

2. Electronic Monitoring\ Electronic Surveillance

3. Interception

سرانجام با تأسیس شورای عالی فضای مجازی ازسوی مقام معظم رهبری دگرگونی‌های به‌نسبت بنیادینی در عرصه نهادی این حوزه رخ داده است. در ابلاغیه ایشان علاوه‌بر شورا، حکم به تأسیس مرکز ملی فضای مجازی نیز داده شده است که این مرکز در اساسنامه خود سه کمیسیون عالی پیش‌بینی کرده که یکی از آنها کمیسیون امنیت فضای مجازی است. حال باید دید این کمیسیون تا چه اندازه در ضابطه‌مندسازی تأمین امنیت همه‌جانبه و فراگیر این فضا، ارکان و اجزای آن نقش‌آفرین خواهد بود.

۲-۱-۲ نهادسازی واکنشی

با توجه به دشواری‌ها و حساسیت‌هایی که درباره تدابیر واکنشی، به‌ویژه کیفری در برابر تهدیدهای سایبری بیان شد، قاعدتاً مباحث نهادسازی این حوزه بر همان رویه پیش می‌رود. برای واکنش باید از اختیارات صلاحدیدی[1] به‌منظور ورود به حریم و محدود کردن آزادی‌های مشروع شهروندان برخوردار بود که از آن به قوه قاهره تعبیر می‌شود و بدون آن نمی‌توان به برخوردی اثربخش و بازدارنده در برابر هنجارشکنان امیدوار بود، ولی چون این اقدام خود به آسیبی جدی برای بهره‌برداری‌های مشروع و سازنده از دنیای سایبر تبدیل نشود، باید سازوکارها و فرایندهای اجرایی دقیقی را برای عملیات‌های گوناگون واکنشی تعریف و به آنها رسمیت بخشید تا دست‌کم مجریان این عملیات‌ها از رویارویی با مسئولیت‌های حقوقی گوناگون در امان مانند.

همان‌طور که درباره تدابیر واکنشی در برابر تهدیدهای سایبری در بالا گفته شد، بخش عمده‌ای از سازوکارها و فرایندهای اجرایی از همان رویه تدابیر کنشی امنیتی پیروی می‌کنند و هم‌سو با آنها پیش می‌روند. به بیان دیگر، با تعریف و تأمین نیازمندی‌های اجرایی ـ عملیاتی امنیت سایبری، بخش عمده و مهمی از نیازمندی‌های واکنشی آن نیز تأمین می‌شود و می‌توان از دستاوردهای تدابیر امنیتی برای پیشبرد اهداف تدابیر واکنشی نیز بهره برد. بنابراین برای هماهنگی هرچه بیشتر مجریان و متولیان این دو حوزه، می‌توان سازوکار یکپارچه‌ای را تعریف و تدارک دید که هم‌زمان هر دو وظیفه را البته بر پایه وظایف و اختیارات متمایز ایفا کنند.

بااین‌حال، همانند نظام پیشگیری از تهدیدها و تهاجم‌های سایبری، قاعده قانونی

---

1. Discretionary Power

متمایزی برای نهادسازی واکنشی سایبری دیده نمی‌شود و از همان رویه‌های کنونی پیروی شده است؛ حال آنکه مجریان قانون یا ضابطانی که قرار است در این عرصه و مرحله از مبارزه با تهدیدها و آسیب‌های سایبری وارد شوند نیازمند اختیارات و ابتکارعمل‌های متمایز و متفاوتی هستند تا بتوانند با کارایی بیشتری به ایفای وظایف خود بپردازند.

در قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری مصوب ۱۳۷۸، ضابطان دادگستری به دو گروه عام و خاص تقسیم می‌شوند. ضابطان عام، مجموعه نیروی انتظامی را تشکیل می‌دهند که بر پایه قانون تشکیل این نیرو در سال ۱۳۶۹، کشف جرائم و تعقیب مجرمان را یکی از وظایف اصلی خود می‌دانند. هرچند طبق قانون، یکی از مسئولیت‌های اصلی این نیرو، پیشگیری از وقوع جرائم نیز عنوان شده که با توجه به کلیت آن شامل همه اقسام پیشگیری از جرائم می‌شود، گرچه می‌توان استنباط کرد که منظور قانونگذار آن دسته از تدبیرهایی بوده که با دیگر وظایف نیرو در امر مبارزه با جرائم سازگاری دارد و به‌اصطلاح تدابیر پیشگیرانه انتظامی نامیده می‌شود.

گفتنی است ازنظر رده‌بندی درون‌سازمانی، نیروی انتظامی یکی از نهادهای پیشرو مبارزه با جرائم رایانه‌ای در کشور به‌شمار می‌آید. در سال ۱۳۷۸ با برگزاری نخستین همایش جرائم رایانه‌ای در کشور این موضوع را به اثبات رساند و یکی از ادارات کل خود را البته همراه با جرائم خاص (نظیر کلاهبرداری و جعل) به رسیدگی جرائم رایانه‌ای اختصاص داد (جلالی فراهانی، ۱۳۸۴: ۲۴۹). اما ارتقای وضعیت نهادی و اعطای استقلال به متولیان و ضابطان جرائم سایبری به‌مدت بیش از یک دهه انجامید و سرانجام در سال ۱۳۸۹ پلیس فناوری اطلاعات و ارتباطات کشور (پلیس فتا) در سطح معاونت نیروی انتظامی مشغول به‌کار شد. گرچه باید دید پس از مدت‌ها، این نیرو تا چه اندازه می‌تواند انتظارات جامعه سایبری را در مبارزه با جرائم و تهدیدهای فزاینده این عرصه برآورد.

نهاد بزرگ دیگری که در چند سال گذشته حضور مقتدرانه‌ای در دنیای سایبر به نمایش گذاشته، مرکز بررسی جرائم سایبری سپاه پاسداران انقلاب اسلامی است. این مرکز به‌ویژه با تهدیدآفرینان فرهنگی کشور در عرصه سایبر برخوردهای قاطعی داشته و چندین تارنمای بزرگ مروج اعمال منافی عفت را از بین برده است. نکته حائز اهمیت درباره این نیرو جایگاه قانونی آن است که طبق اصل یکصدوپنجاهم قانون اساسی این نیرو حق

و وظیفه خود می‌داند که با هرگونه تهدیدهای داخلی، اعم از نرم و سخت، برخورد کند و بنابراین ورود خود به تهدیدهای نوپدید را قانونی و هم‌سو با وظایف کلان خویش می‌داند. همچنین طبق قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری، نیروی مقاومت بسیج که از ارکان سپاه پاسداران است، ضابط دادگستری به‌شمار می‌آید (بند «۳» ماده (۱۵)) و می‌تواند طبق مقررات قانونی به این وظیفه عمل کند.

در کنار این نهادها، وزارت اطلاعات نیز صلاحیت ورود به جرائم مخل امنیت عمومی را به عهده دارد. ضمن اینکه در برخی قوانین، مانند قانون برنامه پنج‌ساله پنجم توسعه، تنفیذی از برنامه چهارم (ماده ۱۲٤)، ضابطیت جرائم کلان و عمده اقتصادی به این نهاد واگذار شده که قاعدتاً برخی جرائم و آسیب‌های سایبری در زمره این عناوین می‌گنجد.

به‌این‌ترتیب با توجه به گستردگی و گوناگونی آسیب‌ها و تهدیدهای سایبری، ضابطان عام و خاص گوناگونی می‌توانند ایفای وظیفه کنند. اما نکته اساسی، هماهنگی و توانمندسازی متوازن آنها با ایجاد یک نقطه کانونی برای تأمین نیازمندی‌های مشترک و مشابه است که به‌نظر می‌رسد چنین الزامی را باید قانونگذار عمل کند، در غیر این صورت هریک از دستگاه‌ها فقط برای رفع نیازهای خویش اقدام خواهند کرد. ضمن اینکه در این راه، عمده نیازهای فنی و فناورانه این دستگاه‌ها در اختیار مراجعی است که وظیفه تأمین امنیت پیشگیرانه فضای سایبری کشور را به عهده دارند که در گفتار پیشین به مرکز ماهر اشاره شد که زیرمجموعه وزارت ارتباطات و فناوری اطلاعات انجام وظیفه می‌کند. بنابراین هماهنگی میان همه این مجموعه‌ها از کارهای اولیه‌ای است که می‌تواند گام مؤثری در حمایت از آسیب‌دیدگان سایبری به‌شمار آید.

یکی از نوآوری‌های قانون جرائم رایانه‌ای نسبت به دیگر مصوبات قانونی این است که حوزه کشف جرائم و شناسایی مجرمان رایانه‌ای را قاعده‌مند کرده است، اما یکی از نارسایی‌های اساسی برای ضابطان جرائم رایانه‌ای تعیین تکلیف نکردن است. در این قانون فقط عنوان کلی ضابطان قضایی آمده است (ماده ۷۶۲)، حال آنکه این عنوان مراجع صلاحیت‌دار گوناگونی را شامل می‌شود و شایسته بود قانونگذار در این خصوص تعیین تکلیف و دست‌کم مراجع اصلی و معین این حوزه را مشخص می‌کرد؛ قاعده‌ای که می‌توانست به تخصیص منابع و نیروهای صلاحیت‌دار برای پاسخ‌گویی شایسته به تهدیدها و تعرض‌های این حوزه کمک

بسیاری کند و به‌ویژه بزه‌دیدگان سایبری را از بلاتکلیفی درآورد. این موضوع می‌تواند یکی از اصلاحیه‌های قانونی باشد و مورد توجه دست‌اندرکاران امر قرار گیرد.

پس از مرحله شناسایی، گزارش یا شکایت درباره تهدیدها و تعرض‌های جنایی سایبری به/ازسوی ضابطان دادگستری، نوبت به مراجع صلاحیت‌دار دادگستری می‌رسد. در اینجا قانونگذار برخلاف ضابطان دادگستری، از همان آغاز بر تخصص‌گرایی قضایی تأکید و قوه قضائیه را به تأمین سازوکار و تربیت نیروی قضایی مورد نیاز این حوزه مکلف کرده بود. نخستین بار در قانون برنامه چهارم توسعه، این حکم درباره دادگاه‌های تجارت الکترونیکی صادر شد (تبصره ماده ۳۳). پس از آن نیز قانون مجازات اسلامی در ماده (۷۵۸) خود صراحتاً قوه قضائیه را به تشکیل دادگاه‌های اختصاصی رسیدگی به جرائم رایانه‌ای مکلف کرد.

بااین‌حال گرچه وضعیت محاکم دادگستری ازنظر سامان‌دهی نهادی قانونی بهتر و روشن‌تر از ضابطان دادگستری است، اما آنها با مشکل دیگری که از برخی جهات جدی‌تر هم است، روبه‌رویند که عبارت است از صلاحیت قضایی؛[1] به این معنا که کدام دادگاه صلاحیت رسیدگی به جرائم سایبری دارد. این مسئله که حتی در کشورهای پیشرو این عرصه نیز همچنان از چالش‌های اصلی نظام عدالت کیفری سایبری به‌شمار می‌آید، به ماهیت جرائم سایبری برمی‌گردد و به‌آسانی نمی‌توان درباره آن تعیین تکلیف کرد. یک جرم سایبری، برخلاف بسیاری از جرائم فیزیکی می‌تواند محل‌های وقوع، مرتکبان و بزه‌دیدگان بسیاری داشته باشد و همین مسائل تعیین دادگاه صلاحیت‌دار کیفری را با مشکلات دوچندان روبه‌رو می‌کند. بنابراین ضروری است قانونگذار با رویکرد و در اولویت قرار دادن حمایت از آسیب‌دیدگان سایبری، درباره این موضوع نیز تعیین تکلیف کند و آنها را از سردرگمی در شناسایی مرجع صلاحیت‌دار قضایی و مراجعه به آن برهاند.

۲-۲ قاعده‌گذاری حمایتی از آسیب‌های سایبری

سیاستگذاری تقنینی به معنای تبیین حق‌ها و تکالیفی است که برای هر حوزه یا موضوع مشخص وضع و امکان استیفا و ایفای آن برای ذی‌نفعان و مسئولان فراهم می‌آید. ازاین‌رو

---

1. Judicial Jurisdiction

لازم نیست از شیوه‌ها و روش‌های اجرایی سخن گفته شود و این امر را به آیین‌نامه‌های اجرایی واگذار می‌کند، مگر اینکه شیوه یا روش مورد نظر موضوعیت یابد که در این صورت قانونگذار به آن تصریح می‌کند. در نص قانون فقط به ذکر قواعد هنجارین لازم‌الرعایه بسنده شده و امکان ابتکار عمل مجریان قانون محفوظ می‌ماند، چرا که ممکن است در وضعیت مختلف اجرای قواعد ملاحظات مختلفی را برانگیزد، بی‌آنکه اصول آنها دچار خدشه شود که در این صورت تغییر شیوه یا روش ازنظر قانونگذار بلامانع خواهد بود.

با توجه به توضیحاتی که درباره پویایی همیشگی فناوری‌ها و ابزارهای این حوزه داده شد، حمایت قانونی شایسته از آسیب‌دیدگان سایبری، در گرو پایبندی به روش‌ها و شیوه‌های روزآمد است و هنر قانونگذار این است که به نحوی قواعد خویش را وضع کند که امکان ابتکار عمل‌های کارآمد و اثربخش متناسب با مقتضیات گوناگون برای مجریان قانون فراهم باشد. در اینجا معمولاً توصیه می‌شود که قانونگذار رویکرد فناوری خنثی یا فناوری بی‌طرف داشته باشد، به این معنا که هنگام قاعده‌گزینی بر ابزار یا فناوری ویژه‌ای تکیه نکند تا درصورت تغییر آنها کاستی یا نارسایی قانونی رخ ندهد. در ادامه چگونگی قاعده‌گذاری در دو حوزه تدبیرگزینی پیشگیرانه و واکنشی حمایتی از آسیب‌دیدگان سایبری بررسی می‌شود.

۱-۲-۲ قاعده‌گذاری پیشگیرانه

یکی از موضوعاتی که قانونگذار باید قواعد حاکم بر آن را وضع و بر روند اجرایی شدن آن نظارت جدی داشته باشد، رشد آگاهی عمومی و اختصاصی شهروندان، به‌ویژه متناسب با دگرگونی‌های خرد و کلان اجتماعی است. این موضوع به حدی حائز اهمیت است که در اصول نخستین قانون اساسی کشورمان به‌طور صریح به آن اشاره شده و پرداختن به آن را از ضرورت رسیدن به کمال و تعالی بشر برشمرده است (اصل سوم).

اکنون عصر اطلاعات است و بی‌گمان در این دوران یادگیری کاربری با فناوری‌های اطلاعاتی و ارتباطی راه اصلی رشد آگاهی و دانش عمومی و اختصاصی است. آنچه در این دوران سواد رایانه‌ای[1] یاد می‌شود، چیزی جز دانش پایه برای یادگیری دیگر دانش‌های

1. Computer Literacy

متوسط و پیشرفته نیست (معنوی، ۱۳۸۳: ۶۱) و به‌راستی شخصی که در این دوران سواد رایانه‌ای را فرانگرفته باشد، هرچند از تحصیلات مطلوب غیررایانه‌ای برخوردار باشد، بی‌سوادی بیش نخواهد بود. این مسئله واقعیتی انکارناپذیر و گریزناپذیر است که روزبه‌روز چالش‌های ناآشنایی و بیگانگی شهروندان با آن آشکارتر می‌شود و هم‌اینک یکی از شاخص‌های اصلی ارزیابی توسعه‌یافتگی کشورها به‌شمار می‌آید.

با توجه به اهمیت موضوع، ضروری است قانونگذار تحول نظام آموزش ابتدایی تا عالی کشور را در پرتو سوادآموزی رایانه‌ای در دستور کار خود قرار دهد و دستگاه‌های ذی‌ربط را مسئول تأمین نیازمندی‌های ماهوی و شکلی این حوزه کند. تحول نظام آموزشی در این سطح نیازمند وضع قواعد نوینی است که بتوان بر پایه آنها آزمون‌های لازم را به انجام رساند. ضمن اینکه می‌توان در این مجموعه قواعد، بخشی را به گروه‌های نیازمند آموزش بیشتر و جدی‌تر اختصاص داد و برای آنها تسهیلات و امتیازات ویژه‌ای پیش‌بینی کرد. برای مثال، ناتوانان در کشورهای توسعه‌یافته از چنین امتیازاتی بهره‌مندند. همچنین، سالمندان و آنهایی که از معضل شکاف دیجیتالی[1] رنج می‌برند، باید از فرایندها و برنامه‌های آموزشی متمایز با دیگر گروه‌ها بهره‌مند شوند.

علاوه‌بر این ضروری است توجه ویژه‌ای به متولیان و مسئولان آموزش سایبری شود. دیگر موعد آن رسیده است که به سوادآموزی رایانه‌ای فراتر از یک دوره مافوق برنامه نگاه شود و همانند سوادآموزی مرسوم، دوره‌های ویژه‌ای برای تربیت متولیان و مربیان آموزش سایبری تدارک دیده شود و حتی در دانشگاه‌ها و دانشکده‌ها دوره‌ها و گرایش‌های ویژه‌ای به این امر اختصاص یابد. چنانچه دستاوردهای سودمندی نصیب جامعه شود و مربیان آموزشی در شاخه‌های گوناگونی تربیت شوند، می‌توانند نقش تعیین‌کننده‌ای در رشد آگاهی و سواد گروه‌های هدف خویش داشته باشند.

موضوع بسیار مهم دیگری که نیازمند قاعده‌مندسازی قانونی است، موضوعات سایبری است که باید از صیانت و حمایت قانونی بهره‌مند شوند. هم‌اینک قوانین پراکنده‌ای درباره انواع اطلاعات مشمول حمایت قانونگذار وجود دارد. اما نمی‌توان نگاه فراگیر قانونگذار را در حمایت از همه اطلاعات نیازمند حمایت استنباط کرد. در حوزه اطلاعات شخصی، برخی

---

1. Digital Gap

حوزه‌ها بدون ضابطه رها شده‌اند که از جمله می‌توان به اطلاعات مالی اشخاص (اعم از حقیقی و حقوقی) اشاره کرد. اساساً کدام اطلاعات اشخاص از ویژگی مالی برخوردار است و ضوابط حاکم بر آنها چیست؟ به‌این‌ترتیب قانونگذار باید درباره انواع، چگونگی و مدت زمان نگهداری، پردازش و نحوه بهره‌برداری و یا ارائه اطلاعات اشخاص قاعده‌گذاری متوازن و متعارفی به‌عمل آورد. حتی نگهداری بیش از حد این اطلاعات می‌تواند تهدیدآفرین باشد و هنگامی که کاربری مفید آنها به پایان رسید، دیگر دلیلی بر نگهداری بیشتر آنها نیست و باید از بین بروند. اما امر به نابودی اطلاعات نباید دستاویزی برای مراجع نگهدارنده شود که از مسئولیت نگهداری درست و دقیق آنها تا مواعد قانونی مقرر سر باز زنند.

همین شرایط با قدری تعدیل باید درباره اطلاعات عمومی نیز به اجرا درآید. هنوز برای نهادهای مسئول تفاوت اطلاعات مهم، حساس و حیاتی روشن نیست و ازاین‌رو نمی‌توان انتظار داشت طبقه‌بندی و ضابطه‌مندی دسترسی به آنها به‌طور همگن و هماهنگ انجام شود که این وضعیت خود بر آسیب‌پذیری زیرساخت‌های وابسته به این اطلاعات می‌افزاید. برای قاعده‌مندسازی قانونی امنیت داده‌ها و سامانه‌های آسیب‌دیدگان سایبری، می‌توان از قواعد عمومی حاکم بر امنیت اطلاعات در فضای سایبر بهره برد که پیش‌تر به آنها با عناوین دسترس‌پذیری، صحت و تمامیت و محرمانگی اشاره شد. در حوزه دسترس‌پذیری، قانونگذار از اطلاعات عمومی سخن می‌گوید که باید در دسترس همگان قرار گیرد و مهم‌تر از آن موارد استثنایی را ذکر کرد. برای مثال فصل چهارم قانون انتشار و دسترسی آزاد به اطلاعات، مصوب ۱۳۸۸، موارد استثنایی را چنین برشمرده است: ۱. اسرار دولتی، ۲. حمایت از حریم خصوصی، ۳. حمایت از سلامتی و اطلاعات تجاری و ۴. موارد دیگری مانند امنیت و آسایش عمومی که مؤسسات مشمول این قانون مکلف شده‌اند از ارائه این‌گونه اطلاعات درخواست شده خودداری کنند.

صحت و تمامیت، حق و اختیار اصلاح، تغییر، برچیدن، جایگزینی و به‌طورکلی هرگونه پردازش داده‌ها و اطلاعات را دربرمی‌گیرد که قانونگذار اشخاص و موارد مجاز چنین اقدامی را برشمرده و با رفتارهای غیرمجاز برخورد می‌کند. تاکنون در کشور ما فقط بر قاعده‌مندسازی کیفری این حوزه تمرکز شده (فصل دوم از بخش یکم قانون جرائم رایانه‌ای با عنوان جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای) و درباره سامان‌دهی آن مصوبه‌ای به چشم نمی‌خورد. به‌تازگی کوشش‌هایی انجام شده که از آن جمله می‌توان به

پیش‌نویس قانون ثبت‌احوال اشاره کرد که درباره میزان و چگونگی دخل‌وتصرف مأموران ثبت‌احوال در اطلاعات شخصی شهروندان ایرانی مقرراتی پیشنهاد شده است.

سرانجام محرمانگی، از حریم داده‌های شخصی و اطلاعات طبقه‌بندی شده حمایت می‌کند. بسیاری از کشورها برای صیانت از این حوزه‌ها قوانین حمایت از داده‌ها و حریم خصوصی[1] را به تصویب رسانیده‌اند، ولی کشور ما هنوز چنین قانونی را به تصویب نرسانده است و حتی پس از آنکه لایحه حمایت از حریم خصوصی به‌صورت طرح در دستور کار دوباره مجلس شورای اسلامی قرار گرفت، تا به امروز مسکوت مانده است. به‌علاوه از اطلاعات طبقه‌بندی شده به‌عنوان یک تکمله در قوانینی چون قانون آزادی اطلاعات[2] صیانت شده[3] یا حتی به‌صورت مستقل به تصویب رسیده است که کشور ما فقط قانون «مجازات انتشار و افشای اسناد محرمانه و سری دولتی» مصوب ۱۳۵۳ را دارد.[4]

۲-۲-۲ قاعده‌گذاری واکنشی

براساس مباحثی که در بخش گذشته بیان شد، قاعده‌گذاری قانونی برای واکنش حمایتی در برابر تهدیدهای زیان‌بار سایبری، هم در حوزه جبران زیان‌های رایانه‌ای و هم ضمانت اجراهای کیفری و غیرکیفری رایانه‌ای به پشتکار جدی قانونگذار نیازمند است و گرچه در دهه گذشته مصوباتی در این حوزه به تصویب رسیده، اما به‌دلیل ناهماهنگ بودن آنها با یکدیگر در برخی موارد ازیک‌سو و نارسایی‌ها و کاستی‌های ماهوی ازسوی‌دیگر، این احکام بدون اجرا باقی مانده‌اند. بنابراین در این بند علاوه‌بر اقداماتی که قانونگذار باید انجام دهد تا در برابر تهدیدهای سایبری، واکنش حمایتی با کاستی یا نارسایی روبه‌رو نباشد، به مجموعه مصوبات مرتبط و نکاتی نیز اشاره می‌شود: نخستین اقدامی که قانونگذار باید به‌عنوان قاعده بنیادی انجام دهد، دارایی‌های سایبری اشخاص، هم مادی و هم معنوی را به

---

1. Data Protection Act/Privacy Protection Act
2. Freedom of Information Act
۳. رک.: گزارش کارشناسی مرکز پژوهش‌های مجلس شورای اسلامی (۱۳۸۸). «آشنایی با قانون شفاف‌سازی اطلاعات عمومی جمهوری اندونزی»، شماره ۹۶۰۶، www.tarh.majlis.ir.
٤. رک.: همان، «اظهارنظر کارشناسی مرکز پژوهش‌های مجلس درباره لایحه آزادی اطلاعات» (۱۳۸۷). شماره ۲۸۰۹۳۵٦، www.tarh.majlis.ir.

رسمیت شناسد. برای رسیدن به این هدف شاید به تصریح واجد ارزش بودن داده‌ها به‌موجب قانون نیاز نباشد؛ زیرا اگر آن‌گونه که صاحب‌نظران حقوقی می‌گویند، مال چیزی است که مفید باشد و نیاز مادی و معنوی را برآورد و همچنین قابلیت تخصیص به شخص یا گروهی داشته باشد (کاتوزیان، ۱۳۸۷: ۹)؛ بنابراین تفاوتی نمی‌کند که منقول باشد یا غیرمنقول، مادی باشد یا معنوی (مانند سرقفلی)، ملموس باشد یا ناملموس. گرچه در مقطعی این پیشنهاد به قانونگذار داده شده بود،[1] اما به‌جای آن قانونگذار به داده‌ها به‌عنوان اسناد قابل استناد رسمیت بخشید و اشخاص توانستند با اطمینان آنها را در مناسبات اجتماعی خود به‌کار گیرند و در برابر سوءاستفاده‌های احتمالی از حق شکایت برخوردار شوند (مواد (۱۲ و ۱۴) قانون تجارت الکترونیکی و ماده (۴۸) قانون برنامه پنجم توسعه).

محاسبه زیان‌های رایانه‌ای از جمله حوزه‌هایی است که قانونگذار باید به آن ورود یابد و قواعدی را برای سامان‌دهی آن به رسمیت شناسد. واقعیت این است که نظام مسئولیت مدنی در کشور ما به‌اندازه دیگر کشورهای پیشرو در عرصه‌های کلان حقوقی، پیشرفت چندانی نکرده و با کاستی‌هایی روبه‌روست و برای آگاهی از این موضوع، کافی است میزان و کیفیت استناد به قانون مسئولیت مدنی، مصوب ۱۳۳۹، در پنجاه سال گذشته مورد توجه قرار گیرد. اما هنگامی که زیان‌های ناشی از این عرصه‌های نوپدید به شهروندان وارد می‌شود، این کاستی‌ها بیشتر نمایان می‌شوند. برای مثال در دنیای خاکی ممکن است آسان‌تر از دنیای سایبری بتوان زیان مادی ناشی از عدم رعایت حق نشر پدیدآورنده اثر ادبی یا هنری را محاسبه کرد. همچنین هتک حیثیت و حرمت اشخاص در دنیای سایبری بسیار زیان‌بارتر از دنیای خاکی است و شاید هرگز نتوان همه آثار چنین زیان‌هایی را جبران کرد. همان‌طور که در جای‌جای فضای سایبر نشانه‌های چنین بی‌حرمتی‌هایی را می‌توان دید و تا مدت‌ها متحمل آسیب‌های ناشی از آن شد.

یکی از قواعدی که قانونگذار می‌تواند با پذیرش آن به جبران زیان‌های وارده به آسیب‌دیدگان کمک کند، خسارت تنبیهی[2] است. خسارت تنبیهی آن‌گونه که از نامش پیداست، ماهیت غیرترمیمی دارد و برای تنبیه خوانده خطاکار و بازداشتن او و دیگران از

---

۱. در بند «ج» ماده نخست پیش‌نویس لایحه جرائم رایانه‌ای تصریح شده بود که داده‌های رایانه‌ای ارزش مالی دارد.

2. Punitive Damages

ارتکاب سوءرفتارهای مشابه در آینده به‌نفع خواهان حکم می‌دهد. این قاعده که در نظام حقوق عرفی ریشه دارد، علاوه‌بر زیان‌های واقعی وارده به آسیب‌دیدگان و به‌ویژه برای جبران آسیب‌های روانی و عاطفی آنها تعیین و پرداخت می‌شود.[۱] بی‌گمان گاهی این آسیب‌ها بسیار زیان‌بارتر از آسیب‌های مادی وارده‌اند، درحالی‌که در برخی نظام‌های حقوقی، از جمله در کشور ما بدون جبران باقی می‌مانند و فقط راهکار پیش‌بینی شده کنونی، اعاده حیثیت است که آن نیز با محدودیت‌ها و حتی پیامدهایی روبه‌روست. به‌نظر می‌رسد عدم امکان محاسبه یک زیان، نبود آن را به اثبات نمی‌رساند و سزاوار است با بهره‌گیری از تجربه دیگر کشورها معیارهایی برای محاسبه این شکل زیان‌ها تعریف و وضع شود و چنین اقدامی قطعاً با موازین اسلامی، از جمله قاعده لاضرر سازگارتر است.

پس از گذر از قواعد به‌اصطلاح ثبوتی؛ یعنی قواعدی که زیان رایانه‌ای را به رسمیت می‌شناسد و قابل مطالبه می‌شود نوبت به اثبات قواعد می‌رسد. منظور از این قواعد، مجموعه احکامی است که به‌موجب آنها می‌توان زیان‌های وارده به زیان‌دیده را ارزیابی و به شکل مطلوبی وضعیت آسیبی وی را بازیابی کرد. در قسمت گذشته اشاره شد که برای سنجش و برآورد زیان‌ها به داده‌ها و اطلاعاتی نیاز است که لزوماً نزد کاربر زیان‌دیده نیستند و در سامانه‌های ارائه‌دهندگان خدمات جامعه اطلاعاتی، مانند ارائه‌دهندگان خدمات دسترسی یا میزبانی نگهداری می‌شوند و بدون آنها نمی‌توان گامی پیش نهاد. این داده‌ها علاوه‌بر کمک به شناسایی مرتکبان و مسببان زیان سایبری، می‌توانند ماهیت محتوای از بین رفته یا آسیب‌دیده رایانه‌ای را نیز نشان دهند.[۲] این موضوع به‌ویژه در جایی اهمیت و حساسیت نشان می‌دهد که به‌تدریج کاربران، خواسته یا ناخواسته به محیط‌های پردازشی و ارتباطی الکترونیکی عمومی می‌گرایند. آنچه اکنون رایانش ابری[۳] نامیده می‌شود، به

---

۱. رک.: علی خسروی فارسانی و شاهپور بیرانوند (۱۳۸۹). «مقایسه تطبیقی وجه التزام و خسارت تنبیهی»، مجله *حقوقی دادگستری*، ش ۷۰.

۲. باید توجه داشت که بررسی تخصصی چنین داده‌هایی آسان نیست و به خبرگان و کارشناسان خاصی نیازمند است. ازاین‌رو ضروری است در این حوزه سرمایه‌گذاری لازم انجام گیرد. برای مثال قوه قضائیه مکلف شود نظام کارشناس رسمی رایانه‌ای که البته هم‌اینک وجود دارد را ازلحاظ کمی‌وکیفی توانمند کند تا پاسخ‌گوی نیازهای جامعه باشند.

3. Cloud Computing

رک.: مرکز پژوهش‌های مجلس شورای اسلامی (۱۳۹۰). «رایانش ابری»، شماره ۱۲۰۳۸، www.tarh.majlis.ir.

گستره‌ای جهانی اشاره دارد که کاربران با در اختیار داشتن یک سامانه مجازی و نرم‌افزارهایی که به ذخیره‌سازی آنها بر سامانه‌های شخصی‌شان نیاز ندارند، به تولید، پردازش و ذخیره‌سازی داده‌هایشان می‌پردازند. درواقع هیچ داده‌ای روی سامانه شخصی کاربر ذخیره نمی‌شود و همه‌چیز در محیط رایانشی فراگیر به انجام می‌رسد. بنابراین باید این موضوع پیش‌بینی شود که چنانچه داده‌های کاربران آسیب دید یا از بین رفت، بتوان نسخه پشتیبان آنها را در اختیارشان گذاشت و ازآنجاکه این کار با هزینه‌هایی همراه است، چنانچه الزام قانونی نداشته باشد، بعید است ارائه‌دهندگان خدمات آن را بپذیرند و درصورت پذیرش نیز هزینه آن را به کاربران تحمیل می‌کنند.[1]

با توجه به اهمیت موضوع، قانونگذار تجارت الکترونیکی از کنشگران فضای سایبر خواسته به این امر اهتمام ورزند. در ماده (۸۱) این قانون آمده است: «اصل‌سازان، مخاطبین، بایگانان، مصرف‌کنندگان و کلیه کسانی که «داده‌پیام» در اختیار دارند موظف‌اند «داده‌پیام»هایی را که تحت مسئولیت خود دارند به‌طریقی نگهداری نموده و پشتوانه (Back up) تهیه نمایند که درصورت بروز هرگونه خطری برای یک نسخه، نسخه دیگر مصون بماند». همان‌طور که ملاحظه می‌شود، این حکم هیچ ضمانت اجرایی ندارد و بنابراین نمی‌توان به پاسخ‌گو بودن مراجع گفته شده امیدوار بود. ضمن اینکه در جای دیگری حکم یا قاعده تکمیلی وجود ندارد تا بتوان با پشتوانه قرار دادن آنها برای یکدیگر به دستاوردهای مطلوبی رسید. ازاین‌رو ضروری است قانونگذار ورود جدی‌تری به بازآفرینی قواعد ثبوتی و اثباتی مسئولیت مدنی، با رویکرد حمایت از آسیب‌دیدگان سایبری داشته باشد.

در بالا نکات لازم درباره ضمانت اجراها بیان شد، اما در مقام ارائه رهنمود تقنینی به قاعده‌گذاری سایبری بر این نکته تأکید می‌شود که قانونگذار از ظرفیت ضمانت اجراهای مقرراتی بیش از حد کنونی بهره‌برداری کند و از مراجع مقررات‌گذار بخواهد کنشگرانه‌تر و جدی‌تر به این عرصه وارد شوند. این موضوع به‌ویژه از آن جهت حائز اهمیت است که مراجع حسب وظیفه حاکمیتی خویش، ابتکار عمل به‌مراتب بیشتر و اثربخش‌تری نسبت به

---

۱. گفتنی است اکنون فقط مواد (۷۶۱ و ۷۶۰) قانون مجازات اسلامی بر لزوم نگهداری داده‌ها و اطلاعات درباره کاربران ازسوی ارائه‌دهندگان خدمات دلالت دارد.

حوزه در اختیار خویش دارند و می‌توانند کنشگران این عرصه را به نحوی سامان‌دهی کنند که خودبه‌خود از رخداد بسیاری از آسیب‌ها و زیان‌ها پیشگیری یا زمینه جبران و بازیابی آنها را به شکل کم‌هزینه‌تر و آسان‌تر فراهم کنند. این مراجع می‌توانند و باید ارائه‌دهندگان خدمات را مکلف کنند شبکه یا محیط رایانه‌ای را به‌طور پیوسته و با روزآمدترین ابزارها رصد کرده و تهدیدهای پیش روی کاربران خود را شناسایی و خنثی کنند و چنانچه از عهده آن برنیامدند به آنها اطلاع‌رسانی کرده یا دست‌کم شیوه‌های بازیابی داده‌ها و سامانه‌هایشان را آموزش دهند و خدماتی که می‌توانند از آن بهره‌مند شوند را به آنها گوشزد کنند. ضمن اینکه بخشی از این زیان‌ها را خود ارائه‌دهندگان خدمات به کاربران وارد می‌کنند که در اینجا دسترسی به داده‌ها و اطلاعات آنها می‌تواند در پیشبرد دعاوی زیان‌های رایانه‌ای حیاتی باشد.[۱]

بااین‌حال، ورود به این حوزه باید با پذیرش اختیارات صلاحدیدی برای مراجع مقررات‌گذار همراه باشد و نباید آنها را با محدودیت‌های قانونی روبه‌رو کرد. برای مثال، بند «ط» ماده (٤٦) قانون برنامه پنج‌ساله پنجم توسعه، مصوب ۱۳۹۰، به کمیسیون تنظیم مقررات ارتباطات اختیار داده با جلب رضایت از دارندگان پروانه‌های خدمات ارتباطی برای تخلفات آنها ضمانت اجرا مقرر و وصول کند که بدیهی است هیچ دارنده پروانه خردمندی به این مصوبه رضایت نمی‌دهد. وضع چنین حکمی از این نگاه نادرست ناشی می‌شود که پروانه‌ها ماهیت قراردادی دارند و مبتنی‌بر اراده طرفین‌اند و نه مجوزی و مبتنی‌بر اراده حاکمیت در برابر فعالان اقتصادی و قاعدتاً نمی‌توان از این نگاه نادرست، دستاوردی بهتر از آنچه در بند «ط» ماده (٤٦) نمایان شده انتظار داشت (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۹۱: ۲۵).

سرانجام در عرصه ضمانت اجراهای کیفری، علاوه‌بر ضرورت اصلاح و بازنگری نظام‌مند و پیوسته قوانین کیفری و روزآمدسازی آنها بر پایه نوآوری‌ها و پویایی‌های سایبری و حفظ پاسخ‌گویی نظام عدالت کیفری در برابر تهدیدهای جنایی، ضروری است سیاست

---

۱. با توجه به اهمیت موضوع یکی از وظایف مراجع مقررات‌گذار این است که بر قراردادهای منعقده ارائه‌دهندگان خدمات با مشترکانشان نظارت داشته باشند و به‌ویژه این موضوع را در پرتو مباحث موافقت‌نامه‌های کیفیت خدمات (SLA) ارزیابی می‌کنند. هرچند این نظارت فقط بر نمونه قراردادهای این خدمات اعمال می‌شود و آزادی اراده طرفین را در تغییر و تعدیل جزئیات و در پرتو مقررات مصوب از بین نمی‌برد.

کیفری این عرصه متناسب با وضعیت، اقتضائات و ملاحظات حاکم بر آن به‌ویژه با رویکرد حمایت از آسیب‌دیدگان سایبری بازتعریف شود. صرف‌نظر از اینکه کیفرهای رایجی چون حبس و جزای نقدی نسبت به دیگر جرائم تا چه اندازه از بازدارندگی، تناسب و اثربخشی برخوردارند، با توجه به ویژگی‌های متمایز جرائم و کنشگران جنایی سایبری، می‌توان به دستاوردهای آنها در این حوزه خاص نیز امیدوار بود؟[۱] بر این اساس، برای رشد کارایی و اثربخشی ضمانت اجراهای کیفری، می‌توان اجرایی بودن برخی نظریه‌های نوین حقوق کیفری را آزمود و کاستی‌ها و نارسایی‌ها را به آزمون گذارد. از جمله این آموزه‌ها، عدالت ترمیمی[۲] است که در آن رویکرد اصلی، حمایت همه‌جانبه از بزه‌دیده یا همان آسیب‌دیده از جرم است و ضمانت اجرای اصلی که برای مرتکب در نظر گرفته می‌شود، کوشش برای تحقق این هدف است. بنابراین وی مکلف می‌شود اقدامات مادی و معنوی مورد نظر را انجام دهد.[۳]

علاوه‌بر این، گزینه‌هایی مانند شرمسارسازی،[۴] به‌ویژه با این استدلال که به‌دلیل برخورداری از پیامدهای اجتماعی بسیار جدی‌تر برای مرتکب دستاوردهای بازدارنده‌تر و سودمندتری به همراه دارد، هم‌اینک ازسوی برخی نظریه‌پردازان جامعه اطلاعاتی برای اجرا در فضای سایبر بررسی و تحلیل شده است (ویلیامز، ۱۳۹۱: ۲۳۲). این قاعده شباهت زیادی به تشهیر به‌عنوان یک کیفر تعزیری دارد که قانونگذار نیز در مواردی از آن بهره‌برداری کرده است که از جمله آنها می‌توان به افشای هویت محکومان جرائم اقتصادی اشاره کرد.[۵] اما در اینجا مرتکب به کار نادرست خود اقرار می‌کند و در برابر جامعه متعهد می‌شود برای جبران زیان‌های ناشی از رفتار یا ترک رفتار زیان‌بارش اقدامات مادی و معنوی ضروری را انجام دهد.

---

۱. یادآور می‌شود قانونگذار در ایران برای مجرمان رایانه‌ای فقط از حربه حبس و جزای نقدی بهره برده و در اندک مواردی ظرفیت دیگر ضمانت اجراها مانند محرومیت‌های اجتماعی سایبری را شناسایی و به‌کار برده که از جمله آنها حکم مقرر در ماده (۷۵۵) قانون مجازات اسلامی است.

2. Restorative Justice

۳. رک.: هوارد زهر (۱۳۸۸). *کتاب کوچک عدالت ترمیمی*، ترجمه حسین غلامی، چاپ دوم، تهران، انتشارات مجد.

4. Shaming

۵. تبصره‌های «۱» و «۳» ماده (۱۸۸) قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری مصوب ۱۳۷۸ (اصلاحی ۱۳۸۵).

چنین آموزه‌هایی به این دلیل سودمند است که قانونگذار و مجریان قانون از ظرفیت‌ها و توانمندی‌های همین عرصه برای جبران آسیب‌ها و زیان‌های وارده به شهروندان بهره می‌برند و نظام حاکمیت ملی هزینه اندکی برای برقراری و بازیابی نظم ازدست‌رفته می‌پردازد. در اینجا شهروندان سایبری خود کیفر عادلانه و منصفانه تبهکاران را دنبال می‌کنند و زمینه‌های اجرای شایسته چنین احکامی را فراهم می‌آورند و دیده‌بان‌های سایبری به نمایندگی از حاکمیت بر حسن اجرای آن احکام نظارت می‌کنند (همان: ۲۲۱). باید پذیرفت که جامعه وارد عرصه و دنیای نوپدیدی شده است که لزوماً نمی‌توان برای برقراری نظم در آن از همین سازوکارهای کنونی بهره برد. باید نگاه خود را روزآمد کرد و بر پایه توانمندی‌های سازگار با شرایط نوین به برنامه‌ریزی و عملیاتی کردن برنامه‌ها پرداخت.

۳ جمع‌بندی، نتیجه‌گیری و راهکارها

دنیای متمدن امروز به خود می‌بالد که به ابزاری مجهز شده که او را در اداره جامعه و برقراری نظم و عدالت توانمندتر از گذشتگانش کرده است.[۱] به‌راستی «قانون» سندی است که ازیک‌سو جامعه را از هرج‌ومرج می‌رهاند و به زورگویان اجازه زورگویی و به ستمدیدگان اجازه مقابله‌به‌مثل یا به بیان بهتر اجرای خصوصی عدالت را نمی‌دهد و ازسوی‌دیگر متولی نظم و عدالت در جامعه است، یعنی حاکمیت را از خودکامگی و تبعیض و تمایز ناروا بازمی‌دارد. به‌این‌ترتیب چنانچه این تعریف و کارکرد را برای قانون پذیرفت و به آن باور داشت، باید کوشید با شناسایی بهنگام کاستی‌ها و نارسایی‌های آن، از شکل‌گیری بی‌نظمی و بی‌عدالتی در جامعه جلوگیری شود. منشأ همه اختلاف‌ها، تخلف‌ها، سوءاستفاده‌ها و تعرض‌ها، نادیده انگاشتن یا برداشت نادرست از حق یا مسئولیتی است که به عضوی از جامعه اعطا یا واگذار شده و این مهم به عهده قانونگذار است که با رسمیت

---

۱. این سخن به معنای نبود پیشینه قانونگذاری در گذشته‌های دور نیست و آثار بجامانده، به‌ویژه از تمدن‌های بین‌النهرین شکل‌های نخستینی از قانونگذاری را نشان می‌دهند، اما سازمان‌دهی و سامان‌بخشی آن به‌عنوان رکنی از نظام حاکمیت ملی و تعریف سازوکارها و تشریفات رسمی قانونگذاری، از دستاوردهای نوین بشری به‌شمار می‌آید. برای آگاهی از پیشینه کهن قانونگذاری رک.: هری هافنر (۱۳۸۴). *قوانین هیتی‌ها* (قانون‌نامه‌ای از آسیای صغیر)، ترجمه فرناز اکبری رومنی، انتشارات حقوقی.

بخشیدن به حق‌ها و مسئولیت‌های مشروع، جامعه را به‌سوی نظم و عدالت رهنمون کند.

یکی از ویژگی‌های اصلی قانون که اتفاقاً با هدف متعالی آن هم‌سویی دارد و نبود یا کمبود آن می‌تواند یکی از عوامل برهم‌زننده نظم اجتماعی به‌شمار آید، پایداری احکام آن است. نظم در گذر زمان برقرار می‌شود و نباید و نمی‌توان انتظار داشت که جامعه یک‌شبه منظم شود. مردم به‌تدریج خود و زندگی‌شان را با هنجارهای قانونی سازگار و هماهنگ می‌کنند و پس از آن انتظار دارند در یک بازه زمانی متعارف بر پایه همان هنجارها برای آینده برنامه‌ریزی کنند. در این صورت قانون، به جامعه پایداری می‌دهد و خودبه‌خود امور آن را تنظیم می‌کند. چنین جامعه‌ای از تصمیم‌ها و سلیقه‌های فردی به دور است و در اصطلاح نظام اجتماعی، خود به تمشیت امور می‌پردازد.

اما چنانچه قانونگذار پی‌درپی رویکرد و رویه‌اش را دگرگون کند، جامعه دچار سردرگمی می‌شود و اگر نتواند با تولی‌گری حاکمیت حق یا مسئولیتش را استیفا یا ایفا کند، قانون خودخوانده خویش را جایگزین مصوبات قانونگذار خواهد کرد. در چنین جامعه‌ای که بیشتر به یک جنگل شبیه است، زور حکم‌فرماست[1] و زورگویان حق و تکلیف یکایک اعضای جامعه را تعیین می‌کنند.

دلیل تعریف و تنظیم تشریفات به‌نسبت طولانی، رسمی و لازم‌الاجرا برای تصویب احکام قانونی جز این نیست که آنچه قرار است سند قانونی به جامعه ابلاغ شود، باید بتواند اداره جامعه را به‌مدت طولانی تضمین کند. ازاین‌رو مراحل و مراجع مختلفی پیش‌بینی شده‌اند تا با مداخله بهنگام و کارشناسانه خود بتوانند این هدف را دست‌یافتنی کنند.

بااین‌حال همین ویژگی می‌تواند چالش‌هایی را برانگیزد و به شکل دیگری زمینه هنجارشکنی‌ها را فراهم آورد. هرچند شاید ایراد از آن نباشد و تدوین نامناسب و نادرست احکام قانونی چنین پیامدهایی را پدید آورد. جامعه در فرایند تکاملی خود، هرروزه با یاری جستن از دانش‌های گوناگون می‌کوشد به فناوری‌هایی دست یابد که پیمودن این راه را آسان‌تر و پرشتاب‌تر کند برای مثال، با پیدایش وسایل نقلیه موتوری زمینی، دریایی و هوایی، بشر برای همیشه با سختی‌های جان‌فرسای جابه‌جایی خداحافظی کرد. ولی ورود

---

1. Might is Right

این ابزارها به زندگی نظم‌هایی را تحمیل کرد که برای تنظیم روابط و مناسبات تازه بر پایه حق‌ها و مسئولیت‌های مترتب بر هریک از آنها، ورود قانونگذار را ناگزیر کرد. به‌طوری‌که در این دهه‌ها احکام گوناگونی را از تصویب گذراند؛ از «قانون اصلاح قانون بیمه اجباری مسئولیت مدنی دارندگان وسایل نقلیه موتوری زمینی در مقابل شخص ثالث، مصوب ۱۳۸۷» گرفته تا «قانون رسیدگی به تخلفات رانندگی، مصوب ۱۳۸۹» یا حتی «قانون مجازات خودداری از کمک به مصدومین و رفع مخاطرات جانی قانون مجازات خودداری از کمک به مصدومین و رفع مخاطرات جانی، مصوب ۱۳۵۴».

در دیگر حوزه‌ها نیز تأثیرپذیری قانونگذار از فناوری‌های معاصر کم‌وبیش دیده می‌شود. برای مثال در عرصه ارتباطات و رسانه، تا هنگامی که کاغذ رواج داشت، فقط همان موضوع قانونگذاری بود. پس از ورود تلگراف، تلفن، مخابرات، رادیو و تلویزیون و سرانجام رایانه‌ها و اینترنت به‌تدریج آنها نیز بر صحیفه قانونی افزوده شدند. عناوین و مفاهیمی که قانونگذار برای تنظیم امور فناورانه برگزیده، گویای این واقعیت است که فقط در همان کانون زمانی، دردسرها و دشواری‌های آن ذهنش را درگیر می‌کرده و به فراسوی آن نگاهی نداشته است. بنابراین در پی دگرگونی و جایگزینی یک فناوری با فناوری‌های دیگر و شکل‌گیری نظم نوینی بر کارکردها و کاربردهای زندگی، حکم قانونگذار بی‌اثر می‌شد.

برای رهایی از این ناپایداری و نابسامانی قانونی در پی نوآوری‌های فناوری باید به پختگی قانونگذاری فناورانه رسید؛ به این معنا که قانونگذار خود را اسیر رنگ‌به‌رنگ شدن فناوری‌ها نکند و احکامش را به شکلی پیش‌بینی کند که دست‌کم دگرگونی‌های جزئی و موردی نظم قانونی را به تشویش و تلاطم نیندازد. برای مثال هنگامی که «قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، مصوب ۱۳۸۶» فقط لوح فشرده را موضوع حکم خود قرار داد، حتی در آن زمان حامل‌های داده نوآورانه‌تری به بازار راه یافته بودند (ولو به شکل محدود) که سزاوار بود قانونگذار ذهنش را تنها به یک شیء گرد مسطح با منفذی در کانون آن محدود و معطوف نمی‌کرد.

برای دستیابی به این سطح از پختگی، برخی ندای بی‌طرفی فناورانه را سرمی‌دهند که البته در این مقاله به آن اشاره شد. اما در عمل تا چه حد می‌توان به این شعار پایبند بود. آیا می‌توان قواعد و الزامات قانونی همه فناوری‌ها را درهم‌آمیخت؟ آیا رویکرد بی‌طرفانه به

عرصه‌های مختلف فناورانه می‌تواند نگاه تخصصی به آنها و عرصه‌های اجتماعی تأثیرگذار و تأثیرپذیر بر/از آنها را فراهم آورد؟ آیا این رویکرد به ابهام و ابهام قانونی و فرار از مسئولیت‌ها و ناکام ماندن ذی‌حق‌ها نخواهد انجامید؟ به‌این‌ترتیب، پیش‌فرض‌ها و مفروضات، معیارها و شاخص‌ها و قواعد حاکم بر یک نظام قانونگذاری کارا و کارآمد بی‌طرفانه فناوری چه خواهد بود؟

در این نوشتار یکی از مهم‌ترین موضوعاتی که قانونگذار باید درباره آن تدبیر فناورانه مناسبی برای صیانت از جامعه اتخاذ کند، طرح و بررسی شد. امروزه کسی از گسترش خیره‌کننده فناوری‌های اطلاعاتی و ارتباطی ناآگاه و بیگانه نیست و کاربری‌های آن از دولت‌مداری و اداره خدمات عمومی گرفته تا پول و بانکداری، آموزش و کسب‌وکار، همه و همه دیدنی و دوست‌داشتنی است و کمتر کشوری از پیاده‌سازی آن سر باز زده است. اما آیا همه فرصت‌های خیره‌کننده، عاری از تهدید است و آیا می‌توان کاربران و دست‌اندرکاران این فناوری‌ها را که خیل آنها از دولت با همه زیرمجموعه‌ها و ارکان آن و انواع مؤسسات خصوصی و بنگاه‌های اقتصادی گرفته تا آحاد شهروندان گسترده است، در این دنیای بی‌دروپیکر، بی‌دفاع رها کرد؟ همچنین وظیفه رویارویی و برچیدن تهدیدها با کیست و به چه شکل باید عمل کند و آیا حق دارد به بهانه مبارزه با تهدیدها، بهره‌برداری از فرصت‌های فناورانه را محدود یا ممنوع کند؟

سرانجام همه این پرسش‌ها به همان بحث نخستین برمی‌گردد که برپایی و ماندگاری نظم نوین سایبری نیازمند تعریف، تشخیص و متمایزسازی حق‌ها و مسئولیت‌های هریک از کنشگران سایبری است و این کار جز قانونگذار از عهده هیچ مرجع دیگری ساخته نیست. ممکن است صیانت از کاربران یا دست‌اندرکاران سایبری جز با ایفای برخی وظایف ازسوی خودشان امکان‌پذیر نباشد و عملاً نتوان مرجع دیگری را مسئول شناخت یا اینکه برقراری امنیت نیازمند تعریف و اجرای پلکانی و سلسله‌مراتبی مسئولیت‌هاباشد و چنانچه مرجعی به وظیفه خویش عمل نکند، دیگری نتواند از عهده وظایف واگذار شده‌اش برآید و همین امر خود چالش‌هایی را پدید می‌آورد؟

این مقاله کوشیده با همین نگاه بررسی همه‌جانبه و فراگیری درباره کارهای تقنینی مورد نیاز برای صیانت از آسیب‌دیدگان بالقوه و بالفعل سایبری داشته باشد. تاکنون

مصوبات عام و خاص گوناگونی در سطوح مختلف سیاستگذاری راهبردی (سیاست‌های ابلاغی مقام معظم رهبری) تا تقنینی و اجرایی ابلاغ شده است. اما اینکه این اقدامات تا چه حد صیانت از کاربران و دست‌اندرکاران سایبری را تأمین و از آنها در برابر انواع تهدیدها حفاظت می‌کند، پرسشی است که باید با تحلیل و ارزیابی‌های دقیق‌تر به آن پاسخ داد. چنانچه دیده شد در مواردی قانونگذار با رویکرد حمایتی، حتی تدابیر کیفری را وضع و ابلاغ کرده اما در اجرایی و اثربخش بودن آنها تردیدهای بسیار وجود دارد و در مواردی این احکام در برابر یکدیگر قرار گرفته و دستاوردهای مورد انتظار را بی‌اثر می‌سازد.

وجود نگاه صیانتی از آسیب‌دیدگان در سیاستگذاری تقنینی برای سامان‌دهی نظام نوین فناوری‌های اطلاعاتی و ارتباطی، الگوی راهبری ـ نظارتی ـ اجرایی یکپارچه، هماهنگ و سازگاری را ارائه می‌دهد که بر پایه آن می‌توان همه تدبیرهای خرد و کلان حاکم بر این حوزه را ارزیابی و تحلیل کرد. این موضوع به‌ویژه در جامعه‌ای مانند ما اهمیت مضاعف می‌یابد که مراجع حاکمیتی گوناگونی اختیار و حق قانونگذاری دارند و ناهماهنگی آنها با یکدیگر نابسامانی‌هایی را پدید آورده و می‌آورد که تاوان اصلی آن را کنشگران این عرصه خواهند پرداخت.

با توجه به گستردگی و گوناگونی تهدیدهای پیش روی کنشگران سایبری، ازیک‌سو چه برای کاربر و چه برای ارائه‌دهنده خدمات که به‌نوبه خود در گروه‌های مختلفی گنجانیده می‌شوند، و ازسوی‌دیگر گستردگی و گوناگونی تمهیدات و تدابیری که می‌توان در برابر این تهدیدها و آسیب‌ها اتخاذ کرد چه به‌منظور پیشگیری از رخداد آنها و چه برخورد با تهدیدآفرینان و هنجارشکنان سایبری، ضروری است برای تحقق اهداف سالم‌سازی فضای سایبر با به‌کارگیری کاراترین و اثربخش‌ترین تدبیرها، سند راهبردی امنیت کنشگران سایبری ایران با تمرکز بر محورهای زیر تدوین، و مراجع صلاحیت‌دار در دستور کار قرار دهند:

۱. مفهوم و اقسام امنیت در فضای سایبر تبیین شود. پیرو مباحث مطرح شده در این نوشتار، می‌توان امنیت را به دو حوزه عمومی و فردی سایبری تقسیم کرد و در هریک از آنها مباحث امنیتی مربوط به هویت، حیثیت و مالکیت عمومی و فردی تبیین شود.

۲. ویژگی‌های هریک از کنشگران بالقوه آسیب‌پذیر در برابر تهدیدهای سایبری، اعم از حقیقی و حقوقی تبیین شود که شامل معیارهای فردی مانند سن، جنسیت و اجتماعی مانند شغل می‌شود. ۳. انواع تمهیدات و تدابیری که می‌توان چه در مرحله پیشگیری، اعم از اجتماعی و وضعی و چه واکنشی، اعم از مقرراتی و قانونی در برابر ناهنجاری‌ها و هنجارشکنی‌های سایبری شناسایی شود. ۴. حریم و حرمت کنشگران سایبری به هنگام تعریف تمهیدات پیشگیرانه و واکنشی سایبری رعایت گردد. ۵. آزادی‌های مشروع کنشگران سایبری محترم شمرده شود و از اتخاذ تدابیری که استیفای حقوق مترتب بر آنها را محدود یا با دشواری روبه‌رو می‌کند، مانند دسترسی آزادانه به اطلاعات قانونی، پرهیز گردد. ۶. تأکید و اولویت بر تدابیر پیشگیرانه باشد، ضمن اینکه به تدابیر واکنشی توجه و نیازمندی‌های قانونی و اجرایی آنها به‌ویژه برای اقدام در عرصه فراملی تأمین گردد.

منابع و مآخذ

۱. ابراهیمی، شهرام (۱۳۹۰). *جرم‌شناسی پیشگیری*، ج ۱، چاپ اول، تهران، نشر میزان.

۲. انصاری، باقر (۱۳۸٦). *حقوق حریم خصوصی*، چاپ اول، تهران، نشر سمت.

۳. _____ (۱۳۹۰). *حقوق رسانه*، چاپ اول، تهران، نشر سمت.

۴. بولک، برنار (۱۳۸۷). *کیفرشناسی* (ویراست پنجم)، ترجمه علی‌حسین نجفی ابرندآبادی، چاپ هشتم، تهران، نشر مجد.

۵. بهره‌مند بگ‌نظر، حمید و امیرحسین جلالی فراهانی (۱۳۹۱). «اطلاعات شخصی و پیشگیری از جنایات سازمان‌یافته فراملی»، *همایش حقوق ثبت و احوال*، دانشگاه تهران.

۶. جلالی فراهانی، امیرحسین (۱۳۸٤). «پیشگیری از جرائم رایانه‌ای»، پایان‌نامه کارشناسی ارشد حقوق کیفری و جرم‌شناسی، دانشگاه امام صادق (ع).

۷. _____ (۱۳۸۹ الف). *درآمدی بر آیین دادرسی کیفری جرائم سایبری*، چاپ اول، تهران، نشر خرسندی.

۸. _____ (مترجم) (۱۳۸۹ ب). *کنوانسیون جرائم سایبر و گزارش توجیهی آن*، چاپ اول، تهران، نشر خرسندی.

۹. _____ (۱۳۹۰). «بایسته‌های حقوقی دفاع مشروع سایبری»، *مجموعه مقالات همایش ملی دفاع سایبری*، چاپ اول، تهران، نشر سازمان انتشارات جهاد دانشگاهی.

۱۰. _____ (۱۳۹۱). «بنیان‌های حقوقی زندگی دوم»، *مجموعه مقالات همایش تخصصی بررسی ابعاد زندگی دوم*، چاپ اول، تهران، نشر سازمان انتشارات جهاد دانشگاهی.

۱۱. خانعلی‌پور واجارگاه، سکینه (۱۳۹۰). *پیشگیری فنی از جرم*، چاپ اول، تهران، نشر میزان.

۱۲. ره‌پیک، حسن (۱۳۸۸). *حقوق مسئولیت مدنی و جبران‌ها*، چاپ پنجم، تهران، نشر خرسندی.

۱۳. زیبر، اولریش (۱۳۸۸). «مهار پیچیدگی فضای جهانی سایبر: هماهنگ‌سازی حقوق کیفری مرتبط با رایانه»، *مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات* (نکوداشت مرحوم استاد محمدحسن دزیانی)، ترجمه امیرحسین جلالی فراهانی، تهران، انتشارات روزنامه رسمی کشور.

۱٤. شمس، عبدالله (۱۳۸۹). *ادله اثبات دعوی حقوق ماهوی و شکلی*، چاپ هشتم، نشر دراک.

۱۵. صادقی، حسین (۱۳۸۶). «مسئولیت مدنی در ارتباطات الکترونیکی»، رساله دکتری حقوق خصوصی، دانشگاه تهران.

۱۶. کاشیان، علیرضا و دیگران (مترجمان) (۱۳۸٤). *راهبری اینترنت* (مشارکت فراگیر)، چاپ اول، تهران، انتشارات دبیرخانه شورای عالی اطلاع‌رسانی.

۱۷. کاتوزیان، ناصر (۱۳۸۷). *دوره مقدماتی حقوق مدنی* (اموال و مالکیت)، چاپ بیست‌وسوم، تهران، نشر میزان.

۱۸. کلانتری، رضا و سیدهادی سجادی (۱۳۹۰). «بیمه سایبر و نقش آن در توسعه اعتماد به خدمات تجارت الکترونیکی»، همایش ملی اقتصاد و تجارت الکترونیکی، وزارت ارتباطات و فناوری اطلاعات، اصفهان، نشر طوبی نصف جهان.

۱۹. کیسی، اوئن (۱۳۸۶). *دلایل دیجیتالی و جرم رایانه‌ای* (علم قانونی، رایانه‌ها و اینترنت)، ترجمه امیرحسین جلالی فراهانی و علی شایان، چاپ اول، تهران، معاونت حقوقی و توسعه قضایی قوه قضائیه، انتشارات سلسبیل.

۲۰. محمدی، قاسم (۱۳۹۰). *جرم مطبوعاتی*، چاپ اول، تهران، نشر سمت.

۲۱. مرکز پژوهش‌های مجلس شورای اسلامی (۱۳۹۱). «بررسی تکالیف اپراتورهای تلفن همراه»، شماره مسلسل ۱۲۷۷۳.

۲۲. معنوی، فیروزه (۱۳۸۳). «سواد رایانه‌ای: ضرورت یا هیاهو»، مجله *اطلاع‌شناسی*، ش ۳.

۲۳. منفرد، محبوبه. «بررسی جرم‌شناختی بزهکاری رایانه‌ای»، *فصلنامه مطالعات پیشگیری از جرم*، نشریه پلیس پیشگیری نیروی انتظامی، در دست چاپ.

۲٤. _____ (۱۳۹۱). «پیشگیری از جرائم رایانه‌ای از گذر کدهای رفتاری»، پایان‌نامه کارشناسی ارشد حقوق کیفری و جرم‌شناسی، دانشگاه غیرانتفاعی شهید اشرفی اصفهانی.

۲۵. مهدوی، محمود (۱۳۹۰). *پیشگیری از جرم* (پیشگیری رشدمدار)، چاپ اول، تهران، نشر سمت.

۲۶. نجفی ابرندآبادی، علی‌حسین و حمید هاشم‌بیکی (۱۳۹۰). *دانشنامه جرم‌شناسی*، چاپ دوم، تهران، انتشارات کتابخانه گنج دانش.

۲۷. ویلیامز، ماتیو (۱۳۹۱). *بزهکار مجازی: بزه، انحراف و مقررات‌گذاری برخط*، ترجمه امیرحسین جلالی فراهانی و محبوبه منفرد، چاپ اول، تهران، نشر میزان.