مزیت‌ها و محدودیت‌های فضای سایبر
در حوزه‌های آزادی بیان، آزادی اطلاعات و حریم خصوصی

امیرحسین جلالی فراهانی[1]

چکیده

بازشناسی بستر مشترکی به نام اطلاعات میان دو حوزهٔ موازین حقوق بشری (در نوشته حاضر آزادی بیان، آزادی اطلاعات و حریم خصوصی) و فناوری اطلاعات و ارتباطات الکترونیکی باعث شده که بحث‌های مربوط به چگونگی تحقق این موازین وارد عرصهٔ جدیدی شود. قابلیت‌های شگفت‌انگیز و بی‌همتای این فناوری در امر اطلاع‌رسانی و ارتباطات، افق‌های جدیدی را در مقابل دیدگان بشر امروز گشوده است. با وجود این، بهره‌برداری از این فرصت مغتنم نباید موجب غافل ماندن از تهدیدهای بالقوهٔ ناشی از کاربری نادرست آن شود. البته هرگونه افراط و تفریطی در نهایت به ضرر جامعه تمام خواهد شد و نکتهٔ ظریفِ حیاتی در برقراری توازنی متعارف میان آزادی‌های مشروع و پیش‌گیری از ناهنجاری‌ها نهفته است.

واژگان کلیدی

فضای سایبر، آزادی بیان، آزادی اطلاعات، حریم خصوصی

---

۱. کارشناس ارشد حقوق کیفری و جرم‌شناسی

مقدمه

از زمان رسمیت یافتن موازین حقوق بشر تاکنون، بحث‌های بسیاری در این حوزه مطرح و اسناد بین‌المللی و منطقه‌ای مهمی تصویب شده است و کم‌تر کشوری را می‌توان یافت که چند اصل از قانون اساسی خود را به تبیین آن اختصاص نداده باشد[۵:۵۱]. آزادی بیان[۲]، آزادی اطلاعات[۳] و حق بهره‌مندی از حریم خصوصی[۴]، از جمله مصداق‌های مهم حقوق بشر به حساب می‌آیند. آنچه موجب می‌شود این سه مصداق در اینجا و در کنار هم بررسی شوند، وجود رکن مشترک اطلاعات در میان آنها ست.

مفهوم اطلاعات هرچند بدیهی می‌نماید، تاکنون به تعریفی جامع و مورد اتفاق همگان از آن اشاره نشده است؛ ولی، می‌توان گفت که مجموعه‌ای از نمادها و نشانه‌ها ست که درک مفاهیم را در قالب‌هایی مانند متن، صدا، تصویر یا ترکیبی از آنها برای انسان امکان‌پذیر می‌کند. بی‌گمان، اگر این ابزار انتقال و درک مفاهیم وجود نمی‌داشت، میان انسان و پیرامون وی جدایی همیشگی حاکم می‌شد و این وابستگی مطلق به هیچ شیوهٔ دیگری رفع‌شدنی نیست [۱۸:۶۳].

هرگونه محدودسازی یا گسترش قلمرو اطلاعات می‌تواند بر زندگی فردی و اجتماعی افراد تأثیر مستقیم بگذارد. هریک از سه حوزهٔ آزادی بیان، آزادی اطلاعات و حق بهره‌مندی از حریم خصوصی کوشیده اند تا با وضع قواعدی، حق‌ها و تکلیف‌های افراد را در امور خصوصی و اجتماعی خود تعریف و مشخص کنند.

امروزه، اطلاعات به‌منزلهٔ گران‌بهاترین سرمایه همگان و به‌ویژه سیاست‌گذاران و تصمیم‌گیران جامعه‌ها را متوجه خود کرده است؛ تا آنجا که به باور برخی، ارزش آن از کالاهایی مانند گندم و فولاد بیش‌تر است. همین

2.freedom of expression
3. freedom of information
4. right to privacy

مسأله موجب شده که روزگار کنونی روزگار اطلاعات[5] نامیده شده و در عمل مبنای همهٔ برنامه‌ریزی‌ها قرارگیرد [۱۱:۱۷]. از سوی دیگر، به دلیل ارزش یافتن بی‌مانند اطلاعات در مناسبات جهانی، متخصصان حوزه‌های مختلف کوشیدند تا ابزار یا ابزارهایی را ابداع کنند که بهره‌برداری آسان و سریع از آن را امکان‌پذیر کرده و به حداکثر برسانند [۱۰:۲۹].

سرانجام، در سال ۱۹۴۶ این کوشش‌ها به بار نشست و رایانهٔ الکترونیکی[6] به‌منزلهٔ ابزار ذخیره‌ساز و پردازشگر بی‌رقیب اطلاعات به جامعهٔ بشری ارائه شد [۲۱:۳۲]. به‌تدریج، پدیدآورندگان این ابزار الکترونیکی دریافتند که قابلیت‌ها و ویژگی‌های آن بسیار فراتر از حوزه‌های مورد تصور آنان است؛ به‌ویژه آنکه در کنار این نرمش‌پذیری بی‌مانند، سادگی کاربری آن نیز درخور توجه است. به همین دلیل، امروزه کم‌تر خانه‌ای را می‌توان یافت که به تسخیر سیستم‌های رایانه‌ای درنیامده باشد و انواع کارکردهای رایانه‌ای بدون محدودیت سنی، دانش فنی و مالی در اختیار همگان قرار گرفته تا از آنها حتی برای امور جاری و روزمره نیز استفاده شود. با وجود این، این میزان انس‌پذیری و گرایش بسیار اعضاء جامعه به فناوری رایانهٔ الکترونیکی را نباید تنها در قابلیت‌های مستقل آن پی‌جویی کرد. مهم‌ترین عاملی که به شکوفایی هرچه بیش‌تر قابلیت‌های رایانهٔ الکترونیکی کمک کرد و آنها را با آسانی و سرعت بیش‌تری در اختیار جهانیان قرار داد، اتصال سیستم‌های رایانه‌ای به یکدیگر به‌وسیلهٔ ارتباطات الکترونیکی[7] است. بی‌گمان، اموری مانند تجارت[8] و دادوستد الکترونیکی[9]، پول[10] و بانک‌داری الکترونیکی[11]،

5. information age
6. electronic computer
7. electronic communications
8. e-commerce
9. e-business
10. e-cash
11. e-banking

یادگیری الکترونیکی[12]، دادگاه‌های الکترونیکی[13] و حتی در مفهومی کلان دولت الکترونیکی[14] که همگی در راستای تحقق جامعهٔ اطلاعاتی[15] پدیدار می‌شوند، در یک یا چند سیستم رایانه‌ای به‌هم متصل در یک نقطهٔ کوچک امکان‌پذیر نیست و به شبکه‌های بزرگ رایانه‌ای نیاز است تا بتوانند نیازهای ذخیره‌سازی و پردازش حجم انبوه اطلاعات را برآورده کنند. بنابراین، به‌تدریج شبکه‌های بزرگ رایانه‌ای در سراسر جهان به یکدیگر متصل شدند تا اینکه جهانی به‌واقع جدید و متمایز از دنیای فیزیکی به نام فضای سایبر[16] شکل گرفت و آن گونه که شاهدیم، کم‌تر حوزه‌ای را می‌توان یافت که امور مربوط به آن تحت تأثیر این فضا قرار نگرفته باشد [۸:۲۱].

از میان این قابلیت‌های شگرف، می‌توان به کارکردهای اطلاع‌رسانی و رسانه‌ای قوی و نیز حریم‌های امنِ با کارکردهای ارتباطی فردی یا گروهی گونه‌گون اشاره کرد که در قالب‌های متن، صدا، تصویر یا حتی چندرسانه‌ای به شکل زنده ارائه می‌شوند. در این میان آنچه مطلوبیت آنها را به اوج می‌رساند، نبود محدودیت‌های مکانی و زمانی است.

تبعیض‌ناپذیری کاربری، یکی از اصول حاکم بر بهره‌برداری از فناوری اطلاعات و ارتباطات الکترونیکی است که دلیل اصلی شکوفایی جهانی آن در این مدت اندک نیز به شمار می‌آید [۱۲:۱۱۰]. به بیان دیگر، برخلاف جهان فیزیکی که محدودیت‌ها و موانع بسیاری برای افراد وجود دارد، لوازم دست‌رسی به این فضا به بهترین و راحت‌ترین شکل آن فراهم است که نمونهٔ آشکار آن را در

12. e-learning
13. e-courts
14.e-government
15. information society
16.cyber space

راه‌اندازی و بلاگ‌های گونه‌گون ــ در مقایسه با رسانه‌های ارتباط جمعی و به‌ویژه مطبوعات ــ می‌بینیم. ولی، این وضعیت مزیت مطلق نیست؛ زیرا به‌راحتی می‌تواند ابزار تحقق مقاصد سوء نیز قرار گیرد و به همان اندازه یا حتی بیش‌تر از آن آسیب‌های جبران‌ناپذیری بر جامعه‌ها وارد کند. همین امر موجب شده حتی کشورهایی که خود را پیرو تحقق حداکثری این موازین می‌دانند، دغدغه‌هایی را بروز داده و تمهیدهایی را برای کاستن از زیان‌های ناشی از سوءاستفاده‌های احتمالی اتخاذ کنند [۵۱: ۲۸].

بر این پایه، مزیت‌ها و محدودیت‌های فضای سایبر برای سه حوزهٔ پیش‌گفته در سه بند جداگانه بررسی می‌شود. منظور از مزیت‌ها، ظرفیت‌های این فضا برای تحقق این اهداف حقوق بشری است، اما از محدودیت‌ها آسیب‌پذیری‌های این فضا در برابر انواع سوء استفاده‌ها دنبال می‌شود. هرچند مجال کافی برای تبیین مبانی و پیش‌نیازهای ضروری دست‌یابی به نظام متعارفی[17] که بتواند راه‌حل میانه‌ای را ارائه کند، فراهم نیست. در واقع، این نوشتار درآمدی است بر ورود به این‌گونه بحث‌های ضروری روزگار کنونی و بحث مربوط به بررسی امکان قانون‌گذاری و خلأهای آن به مجال دیگری موکول می‌شود.

الف- مزیت‌ها و محدودیت‌های فضای سایبر برای آزادی بیان

پیش از وارد شدن به بحث‌های خاصی که فضای سایبر در مورد اصل آزادی بیان به‌وجود آورده، لازم است مفهوم آن در حدی که مورد توجه اسناد بین‌المللی حقوق بشری بوده، تبیین شود. بر این پایه، اعلامیهٔ جهانی حقوق بشر (۱۹۴۸) در مادهٔ ۱۹ خود مقرر می‌دارد: «هرکس حق آزادی عقیده و بیان دارد و این حق مستلزم آن است که از داشتن عقیده بیم نداشته باشد و در دریافت و انتشار اطلاعات و

17. reasonable system

افکار، به تمام وسایل ممکن، بدون ملاحظات آزاد باشد». بی‌گمان، این ماده همانند دیگر مفاد این سند به شکل کلی تنظیم شده و استیفاء این حقوق ایجاب می‌کرد که این مفاهیم دقیق‌تر و شفاف‌تر تعریف شده و حدود و ثغور آنها مشخص شود. از این رو، در سال ۱۹۷۶ میثاق بین‌المللی حقوق مدنی و سیاسی به تصویب دولت‌های عضو سازمان ملل رسید. در این سند دو مادهٔ ۱۸ و ۱۹ به تبیین این موضوع پرداخته اند. مادهٔ ۱۸ حق آزادی تفکر[18]، آگاهی[19] و دین[20] را به رسمیت می‌شناسد که آزادی عقیده موضوع مادهٔ ۱۹ را نیز در برمی‌گیرد. تأکید اصلی این ماده، محترم شمردن آزادی تفکر دربارهٔ همهٔ موضوع‌های مربوط به ایمان شخصی و تعهد به دین یا اعتقاد خاص است و آن‌گونه که در بند ۲ مادهٔ ۴ میثاق آمده، حتی در شرایط خاص و اضطراری هم نباید آن را خوار شمرد و تحقیر کرد. البته، این ماده میان آزادی تفکر، آگاهی و دین یا عقیده و آزادی ابراز آنها تفکیک قائل شده است. گروه نخست تحت حمایت مطلق اند تا اندازه‌ای که، طبق مادهٔ ۱۷ و بند ۲ مادهٔ ۱۸، هیچ کس را نمی‌توان مجبور کرد تا افکار خود را آشکار کند یا به دین یا عقیدهٔ خاصی بگرود. ولی، بر گروه دوم محدودیت‌هایی اعمال شده که در جای خود به آنها اشاره خواهد شد [۱۵۵ :۳۰].

مادهٔ ۱۹ با عنوان آزادی عقیده[21] حق داشتن اعتقاد بدون مداخله را با هیچ استثنا یا محدودیتی به رسمیت می‌شناسد (بند ۱). در اینجا نیز میان اصل این حق و آزادی ابراز آن تفکیک صورت گرفته و در بند ۲ نه‌تنها «انتقال اطلاعات و عقاید به هر نحو»، بلکه آزادی «جست‌وجو» و «دریافت» آنها «صرف‌نظر از مرزها» و با هر رسانه‌ای را دربرمی‌گیرد؛ «چه شفاهی، چه مکتوب یا چاپی، در قالب هنر یا با هر رسانهٔ دیگری

18. thought
19. conscience
20. religion
21. opinion

به انتخاب خود». با وجود این، ابراز آزادانهٔ عقیده به شکل مطلق پذیرفته نشده و محدودیت‌هایی بر آن وارد شده که به شرایط اعمال آن اشاره خواهد شد [۳۰:۱۳۳].

۱. مزیت‌های فضای سایبر برای آزادی بیان

در روزگار کنونی، فضای سایبر با قابلیت‌های رسانه‌ای جدید خود تحولی بنیادین را در عرصهٔ اطلاع‌رسانی رقم زده است. امروزه، اقبال جهانی به سمت رسانه‌های الکترونیکی به‌ویژه شبکه‌های اطلاع‌رسانی رایانه‌ای که جلوهٔ بارز آن شبکهٔ جهانی اینترنت است، به‌اندازه‌ای رسیده که دیگر رسانه‌های ارتباط جمعی مانند رادیو، تلویزیون، انواع نشریه‌های چاپی و ... به حاشیه رانده شده‌اند. توجه به این قابلیت‌ها می‌تواند درستی این داوری را تأیید کند [۲۴:۹]:

۱. هرکس می‌تواند با کم‌ترین هزینه و محدودیت در تأمین مکان و کارکردهای رایانه‌ای مورد نیاز برای تولید محتوا، به طور مستقل به‌منزلهٔ یک رسانه فعالیت کند. نمونهٔ بارز آن میلیون‌ها وبلاگ است که افراد با اندکی دانش فنی می‌توانند رسانه‌ای اطلاع‌رسان را با جذابیت‌های مطلوب راه‌اندازی کنند. کافی است این وضعیت را با فرایند طولانی و پرهزینهٔ گرفتن مجوز و تشکیلات گستردهٔ لازم برای انتشار نشریه‌های چاپی مختلف یا راه‌اندازی یک شبکهٔ رادیویی یا تلویزیونی مقایسه کنید تا بهتر درک شود؛

۲. شبکه‌های اطلاع‌رسانی رایانه‌ای گستردگی جهانی دارند، در حالی که دیگر نشریه‌ها یا رسانه‌های رادیویی و تلویزیونی بیش‌تر بُرد ملی دارند. اگرچه شبکه‌های ماهواره‌ای رادیویی و تلویزیونی ماهیتی فرامرزی دارند، در صورتی که محدودیت‌ها و هزینه‌های راه‌اندازی و پشتیبانی پیوستهٔ آنها در کنار دیگر محدودیت‌های حاکم بر آنها مورد توجه قرار گیرد، بی‌همتایی شبکه‌های رایانه‌ای به‌خوبی روشن خواهد شد؛

۳. شبکه‌های اطلاع‌رسانی رایانه‌ای ماهیتی دوسویه دارند، در حالی که اصولاً

رسانه‌های ارتباط جمعی ماهیتی یک‌سویه دارند و امکان ارائهٔ نظر برای بیش‌تر مخاطبان آنها فراهم نیست. شبکه‌های رایانه‌ای با ارائهٔ انواع کارکردهای شگفت‌انگیز رایانه‌ای به بهترین شکل، امکان برقراری انواع ارتباطات را میان دارندگان رسانه‌ها و مخاطبان آنها فراهم کرده اند. از نمونه‌های بارز آن می‌توان به گپستان‌های رایانه‌ای[۲۲] و گردهمایی‌های آن‌لاین[۲۳] اشاره کرد که امکان برقراری ارتباط میان بسیاری از افراد را در دورترین نقاط جهان فراهم آورده اند؛

۴. شبکه‌های رایانه‌ای ماهیتی چندرسانه‌ای دارند. هر یک از رسانه‌های چاپی یا رادیویی و تلویزیونی بر یک عامل رسانه‌ای محوریت یافته اند. برای نمونه، نمی‌توان از روزنامه‌ها انتظار داشت که کار تلویزیون را انجام دهند و برعکس. ولی، در فضای سایبر وضعیت به گونه‌ای است که هم‌زمان می‌توان محتوای روزنامه‌ها و مجله‌های الکترونیکی را در کنار مشاهده یا شنیدن اخبار صوتی و تصویری آن مطالعه کرد.

این مزیت‌ها هنگامی برتری شبکه‌های اطلاع‌رسانی رایانه‌ای را بر رسانه‌های فیزیکی به اوج می‌رسانند که به **جرأت‌آفرینی فضای سایبر** در پشت سر گذاشتن خط قرمزهای قانونی و بی‌پروایی استیفاء کنندگان این حق در بیان اظهاراتی که ممکن است پیامدهای قانونی به همراه داشته باشد، نیز توجه کنیم. در جهان فیزیکی، به دلیل حساسیت این حوزه، پیوسته بر رسانه‌های ارتباط جمعی نظارت می‌شود و در صورت مشاهدهٔ تخلف، مراجع مربوط به‌سرعت اعمال ضمانت‌اجراءهای تأمینی و کیفری را در دستور کار قرار می‌دهند[۲۴]. همین امر

22. chat rooms

23. on-line conferences

۲۴. مادهٔ ۱۳ ق.ا.ت و تبصره ۲ ماده ۲ قانون اهداف و وظایف وزارت فرهنگ و ارشاد اسلامی، مصوب ۱۳۶۵ و ق.مط. شایان ذکر است که در سال ۱۳۷۹ تبصره ۳ به ماده یک ق.مط افزوده شد و نشریه‌های الکترونیکی مشمول این قانون شدند، بی‌آنکه ماهیت آنها روشن شود و اساساً مشخص نیست که با وجود این تمایزهای فاحش، این ضوابط قانونی تا چه‌اندازه نسبت به آنها اعمال شدنی است.

باعث می‌شود که دارندگان این رسانه‌ها بسیار محتاط باشند. ولی، ماهیتِ بدون مرز فضای سایبر امکان به‌کارگیری انواع هویت‌های ناشناس و مجعول و ابزارهایی را فراهم آورده که مسیر ارتباطات و تعاملات الکترونیکی را مخدوش کرده و بدین وسیله شناسایی پدیدآورندگان و دریافت‌کنندگان را با مشکلات جدی روبه‌رو می‌کنند[۹۷ :۲۸]، همگی موجب شده اند که افراد به‌راحتی حریم‌های قانونی ملی و حتی موازین به‌رسمیت شناخته‌شدهٔ منطقه‌ای[۲۵] و بین‌المللی را نقض کنند.

۲. محدودیت‌های فضای سایبر در تحقق آزادی بیان

ملاحظه شد که به لحاظ حساسیت و سوءاستفاده‌آمیز بودن این حق ضروری است، ابراز و اظهار آن با محدودیت‌هایی روبه‌رو شود. زیرا، بدون استثناء همهٔ کشورها پذیرفته اند که اگر هرکس هر آنچه را اعتقاد دارد بر زبان آورد و بکوشد تا آن را به دیگران نیز انتقال دهد، ثبات جامعه متزلزل خواهد شد و برقراری نظم و امنیت که از وظایف ذاتی حکومت‌هاست، با مشکلات بسیاری روبه‌رو خواهد شد. بنا بر این، در اسناد مربوط، این حق به کشورها داده شده که محدودیت‌هایی را اِعمال کنند. مادهٔ ۲۹ ا.ج.ح.ب. آزادی عقیده و بیان را در چهارچوب قانون و در پرتو رعایت حق‌ها و آزادی‌های دیگران و مقتضیات اخلاقی و نظم عمومی و رفاه همگان که شایستهٔ یک جامعهٔ مردم‌سالار است، به رسمیت شناخته است. ولی، برای اینکه کشورها با توسل به این عذرهای کلی اتباع خود را در استیفاء این حق محدود نکنند یا از آن محروم نسازند، میثاق بین‌المللی حقوق مدنی و سیاسی

۲۵. در هفتم نوامبر ۲۰۰۲ پروتکلی با عنوان **«پروتکل الحاقی کنوانسیون جرائم سایبر در خصوص جرم‌انگاری اعمال دارای ماهیت نژادپرستانه و بیگانه‌ستیزانه‌ای که از طریق سیستم‌های رایانه‌ای ارتکاب می‌یابند»** به تصویب اعضاء شورای اروپایی و غیراروپایی عضو کنوانسیون رسید که در آن از دولت‌های عضو خواسته شده نشر مطالب نژادپرستانه و بیگانه‌ستیزانه از طریق سیستم‌های رایانه‌ای (ماده ۳)، تهدید با نیت نژادپرستانه یا بیگانه‌ستیزانه (ماده ۴)، اهانت با نیت نژادپرستانه یا بیگانه‌ستیزانه (ماده ۵)، عدم پذیرش، به شدت خفیف جلوه دادن، تأیید یا توجیه کشتار جمعی یا جنایات علیه بشریت (ماده ۶) و شرکت و معاونت در این جرائم (ماده ۷) را جرم‌انگاری کنند.

کوشیده است تا شفافیت و صراحت بیش‌تری را در این زمینه ایجاد کند. بر پایهٔ بند ۳ مادهٔ ۱۸ این میثاق، آزادی ابراز مذهب یا معتقدات را نمی‌توان تابع محدودیت‌هایی نمود، مگر آنچه که منحصراً به موجب قانون برای حمایت از امنیت، نظم، سلامت یا اخلاق عمومی یا حقوق و آزادی‌های اساسی دیگران ضرورت داشته باشد» [۱۸۶ : ۱۴]. یا بند ۳ مادهٔ ۱۹ تأکید می‌کند که استیفاء حق آزادی ابراز عقیده، با وظایف و مسؤولیت‌هایی همراه است؛ ولی، تحمیل آنها با رعایت سه شرط امکان‌پذیر است:۱- در قانون تصریح شده باشد، ۲- تنها یکی از هدف‌های مقرر در قسمت‌های الف و ب بند ۳ را تأمین کند و ۳ـ دولت عضو باید ضرورتِ اعمال آن را توجیه کند[۱۳۳ : ۳۰]. همچنین، در سال ۱۹۹۵ میلادی، گروهی از متخصصان حقوق بشر با هدف کمک به کشورها در اجرائی کردن هدف‌های میثاق، بیانیهٔ ژوهانسبورگ را دربارهٔ امنیت ملی، آزادی بیان و دست‌رسی به اطلاعات منتشر و در آن با تفصیل بیش‌تری موازین حقوق بشر را تبیین کردند[۲۶]. اصل یک این بیانیه در مورد آزادی بیان بوده و تقریباً همان مفاد اعلامیهٔ جهانی و میثاق را بازتاب می‌دهد. ولی، زیر اصل‌های سه‌گانهٔ آن در تبیین دقیق‌تر این موضوع اشعار می‌دارند: «**اصل ۱.۱ـ اعمال قانونی: الف)** اعمال هر محدودیت بر بیان و اطلاعات باید توسط قانون مقرر شود. قانون باید قابل دست‌رسی، بدون ابهام، موشکافانه و به دقت تدوین شود، به‌گونه‌ای که افراد بتوانند پیش‌بینی کنند که آیا یک کنش خاص غیرقانونی است یا خیر. ب) قانون باید امکانات کافی را برای محافظت [از آزادی بیان و اطلاعات] در برابر سوءاستفاده فراهم کند؛ این محافظت از جمله شامل بررسی قضائی فوری، کامل و مؤثر درباره اعتبار و صحت محدودیت از سوی یک دادگاه یا هیأت داوری می‌شود. **اصل ۲.۱ـ مراقبت از مصلحت مشروع امنیت ملی:** هر محدودیتی بر بیان

۲۶. سند شمارهٔ CN.|4/1996/39 سازمان ملل متحد.

و اطلاعات که حکومت در پی توجیه آن بر پایه امنیت ملی است، باید هدفی حقیقی داشته و اثر آن بر حفظ مصلحت مشروع امنیت ملی قابل اثبات باشد.

اصل **۱.۳ - ضرورت در یک جامعه مردم‌سالار**: برای اثبات اینکه یک محدودیت بر آزادی بیان و اطلاعات برای حفاظت مصلحت مشروع امنیت ملی ضروری است، حکومت ثابت می‌کند: الف) بیان اطلاعات مورد نظر تهدیدی جدی علیه مصلحت امنیت عمومی مشروع است؛ ب) محدودیت تحمیل شده، کم‌ترین ابزار محدودکننده ممکن برای حفظ آن مصلحت است؛ و ج) محدودیت با اصول مردم‌سالارانه سازگار است» [۱۷:۳].

با توجه به ویژگی‌های بی‌همتای فضای سایبر در بیشینه‌سازی استیفاء این حق و حتی جرأت‌آفرینی آن در پشت سرگذاشتن خط‌قرمزها و حریم‌های قانونی، همهٔ کشورها به‌فراخور نگرانی‌هایی جدی را بروز داده و از آنجا که اِعمال سازوکارهای کیفری چندان نتیجه‌بخش نیست، به سمت تدابیر پیش‌گیرانه و به‌ویژه ابزارهای فنی روآورده اند تا نه‌تنها از آسیب‌ها و پیامدهای به‌مراتب زیان‌بارتر این اقدام‌ها در امان باشند، بلکه در زمینهٔ اِعمال ضمانت‌اجراءهای کیفریِ عمدتاً فرامرزی نیز سرمایه‌گذاری بیهوده نکنند.

۲ـ۱. مفهوم و کارکرد ابزارهای محدودکنندهٔ دست‌رسی به فضای سایبر

به طور کلی، سازوکارهایی که می‌توان از رهگذر آنها آزادی بیان در فضای سایبر را سامان‌دهی کرد عبارت اند از: فیلترها[۲۷] و تدابیر صدور مجوز[۲۸] که در زمرهٔ تدابیر محدودکنندهٔ دست‌رسی افراد به محتوا و برنامه‌های رایانه‌ای قرار می‌گیرند. هر دوی

27. filters

گفتنی است که مصوبهٔ شمارهٔ ۴۸۸ شورای عالی انقلاب فرهنگی به‌تاریخ ۱۳۸۰/۸/۱۵ آیین‌نامهٔ تأمین، توزیع و عرضهٔ خدمات اینترنت و اینترانت ملی کمیسیون تنظیم مقررات ارتباطات وزارت ارتباطات و فناوری اطلاعات، مصوب ۱۳۸۵/۵/۱، و آیین‌نامهٔ سامان‌دهی فعالیت پایگاه‌های اطلاع‌رسانی (سایت‌های) اینترنتی ایرانی هیأت دولت مورخ ۱۳۸۵/۵/۲۹ معادل **پالایه** را برای فیلتر به‌کار برده اند.

28. verification or authentication technologies

این ابزارها فنی بوده و بستر اجرائی مشترکی دارند، ولی با توجه به هدف طرح ریزی، تولید و اجراء تفاوت‌هایی با یکدیگر دارند که شناسایی آنها مفید است.

فیلترها از مهم‌ترین تدابیر پیش‌گیرانه از جرم‌های سایبری اند که تقریباً از همان ابتدا برای جلوگیری از وقوع تعرض‌های رایانه‌ای به‌کار می‌رفتند و به همین دلیل، همپای فناوری اطلاعات و ارتباطات الکترونیکی رشد کرده و تکامل یافته اند و اکنون نمونه‌های بسیاری از آنها در موقعیت‌های مختلف شبکه‌ای و سیستمی به کار می‌روند. در اینجا، با نصب سیستم‌ها یا برنامه‌های خاص روی گره‌های[۲۹] دست‌رسی به شبکه ــ یعنی رایانه‌های شخصی، مسیریاب‌ها[۳۰]، سیستم‌های ارائه‌دهندگان خدمات شبکه‌ای و از همه مهم‌تر ایجادکنندگان نقطهٔ تماس بین‌المللی ــ از ورود یا فرستادن داده‌های نامجاز یا غیرقانونی جلوگیری می‌شود. از نمونه‌های دیگر می‌توان به دیوارهای آتشین[۳۱] و پراکسی‌ها[۳۲] اشاره کرد که مبناء عمل آنها فهرستی از موضوع‌های مجاز[۳۳] یا نامجاز[۳۴] است که بر اساس فرایند انطباق عمل می‌کنند[۲۸:۵۱]. چنانچه مسؤولان ذی‌ربط تشخیص دهند که یک موضوع در چهارچوب استیفاء مشروع حق آزادی بیان نمی‌گنجد، ساده‌ترین اقدامی‌که می‌توانند انجام دهند این است که با وارد کردن مشخصات سایت موردنظر در فهرست سیاه یا عدم درج آن در فهرست سفید فیلترها، از دست‌رسی کاربران به آن جلوگیری کنند.

در تدابیر صدور مجوز[۳۵]، بر اساس معیارهای خاص، از ورود اشخاص ناشناس یا فاقد اعتبار جلوگیری می‌شود. نمونهٔ ساده آن به‌کارگیری گذرواژه[۳۶] است. به

29. nodes
30. routers
31. firewall
32. proxy
33. white list
34. black list
35. verification or authentication technologies
36. password

این ترتیب، فقط کسانی حق بهره‌برداری از یک سیستم یا سایت را خواهند داشت که پس از طی مرحله‌های شناسایی و کسب اعتبار لازم، گذرواژه دریافت کنند. ممکن است این مجوز بر اساس سن، جنسیت، ملیت، دین یا گرایش‌های خاص فکری داده شود. امروزه، در این حوزه پیشرفت‌های بسیاری صورت گرفته است. برای مثال، برای ارتقاء امنیت، از شیوه‌های بیومتریک نیز استفاده می‌شود و به جای گذرواژه یا افزون بر آن، از اسکن عنبیه یا شبکیهٔ چشم یا اثرانگشت برای شناسایی فرد استفاده می‌شود تا ضریب خطا به حداقل برسد [۵۳: ۲۸].

صدور مجوز یکی از مناسب‌ترین راه‌های سامان‌دهی بهره‌برداری از فضای سایبر به منظور ابراز آزادانهٔ عقاید است: نخست، امکان دست‌رسی همگان به داده‌های خاص وجود ندارد و بدین وسیله سوءاستفادهٔ افراد ناصالح به حداقل می‌رسد، در حالی که به افراد اجازه داده می‌شود که آزادانه و بدون واهمه دیدگاه‌های خود را دربارهٔ مسائل مختلف به آگاهی مراجع مسؤول و دیگران برسانند؛ دوم، از بروز نقاط ضعف فیلترها که در ادامه به آن خواهیم پرداخت، جلوگیری می‌شود (هرچند بهره‌برداری از این مزیت به بسترسازی لازم از سوی مراجع ذی‌ربط بستگی دارد).

۲ـ ۲. محدودیت‌های ابزارهای محدودکنندهٔ دست‌رسی به فضای سایبر

با ملاحظه نقاط ضعف ابزارهای محدودکننده دست‌رسی مشخص می‌شود که به‌کارگیری آنها در قالب تدابیر پیش‌گیرانهٔ وضعی سایبری به‌طور عمده حالت مسکن داشته و راه‌حلی بنیادین و اساسی انگاشته نمی‌شود و بهتر است به تدابیر پیش‌گیرانهٔ اجتماعی اولویت داده شود[۳۷] [۶: ۱۵۲].

۳۷. شایان ذکر است که اتحادیهٔ اروپایی در برنامهٔ اینترنت امن‌تر خود که به شکل چهارساله آن را از ۱۹۹۸ اجراء می‌کند، نیمی از بودجهٔ خود را به برنامه‌های رشد آگاهی کاربران و مسؤولان تربیتی آنان و به‌ویژه پدر-مادران اختصاص داده است. ر.ک:

Official Journal of European Union; p6-TA (2004) 0072; Safer Use of the Internet and New Technologies; p. 38.

مهم‌ترین ایراد وارد بر فیلترینگ این است که با ابزاری فاقد فکر با طیف گسترده‌ای از انسان‌های بافکر مبارزه می‌شود. درست است که فهرست عنوان‌های مختلف و گونه‌گون آن را یک یا چند نفر از همین انسان‌ها تهیه می‌کنند، باز همین برنامه‌ها هستند که بر اساس فرایند انطباق، از دست‌رسی به محتوای غیرقانونی جلوگیری می‌کنند.

فیلترینگ برای مبارزه با فضایی طرح‌ریزی می‌شود که همواره پویاست. لحظه‌به‌لحظه بر گستره آن افزوده می‌شود و موضوع‌های جدید با عنوان‌های جدید به آن می‌پیوندند و هرگونه مجال برای روزآمد کردن فهرست فیلترها از تولیدکنندگان آنها سلب شده است. بنا بر این، هیچ‌گاه نمی‌توان انتظار داشت که این برنامه‌ها بتوانند بر اساس شرایط و اوضاع و احوال جدید عمل کنند.

به طور کلی، ماهیت فنی فیلترینگ به گونه‌ای است که همواره در معرض دو خطا قرار دارد: مسدود سازی بیش از اندازه[38] و مسدود سازی کم‌تر از اندازه[39]. صورت نخست که بیش‌تر هم شایع است، در جایی بروز می‌یابد که تولیدکنندگان فیلترها برای به حداکثر رساندن کارآیی برنامهٔ خود چنان حساسیت آن را بالا می‌برند که هرگونه مورد مشکوک را دست‌رس‌ناپذیر می‌سازد. به طور کلی، می‌توان عوامل منع بیش از اندازه را در سه مورد خلاصه کرد [۴۱ : ۲۸]:

۱. از آنجاکه مبناء سنجش یک صفحهٔ وب‌سایت به یک سیستمِ فاقد فکر سپرده شده، ممکن است هرگونه مورد مبهم را هم سانسور کند. آنچه در حوزهٔ فیلترینگ دردسرساز است، موضوع‌های به اصطلاح خاکستری اند[40]. موضوع‌های مبهم یا به‌اصطلاح دو پهلویی که تصمیم‌گیری دربارهٔ درستی یا نادرستی آنها دشوار است؛

۲. اطلاعات موجود در اینترنت همواره در حال نو شدن است. بنابراین ممکن است،

38. over blocking
39. under blocking
40. grey subjects

محتوایی که به خاطر آن وب‌سایتی دسترس‌ناپذیر شده اصلاح یا حذف شده باشد. اما تا زمانی که فهرست فیلترها اصلاح نشود، آن وب‌سایت مجاز مسدود خواهد ماند.

۳. ممکن است یک سایت هم محتوای مناسب و هم محتوای نامناسب داشته باشد. ولی، از آنجا که معمولاً فیلترها توانایی تفکیک این دو را ندارند، کل سایت را دست‌رس‌ناپذیر می‌کنند.

همچنین، عوامل مسدودسازی کمتر از اندازه را می‌توان چنین خلاصه کرد:

۱. هر لحظه موضوع‌های جدیدی به اینترنت افزوده می‌شود و محتوای صفحه‌های وب نیز تغییر می‌کند. در صورت تغییر محتوا باید فهرست فیلترها نیز تغییر کند که کار دشواری است. با اینکه تولیدکنندگان فیلترها در مقاطع خاصی محصولات خود را روزآمد می‌کنند، باز هرگز نمی‌توانند فاصلهٔ خود را با پیشرفت خیره‌کنندهٔ فضای شبکه‌ای و محتوای آن متناسب کنند؛

۲. الگوریتم‌های مورد استفاده برای شناسایی محتوای نامجاز (یعنی فنون رایانه‌ای) ناقص اند. برای مثال، اگر در یک حوزه اصطلاح‌ها یا کلیدواژه‌های جدیدی رایج شوند، تا زمانی که شناسایی و به فهرست فیلترها افزوده شوند، به‌اندازهٔ کافی در دست‌رس همگان قرار داشته و تأثیر خود را خواهند گذاشت؛

۳. بسیاری از سایت‌های نامجاز، نام‌های دامنه‌ای دارند که بسیار شبیه سایت‌های معتبر اند. برخی از سایت‌های نامجاز فقط در پسوند نام یعنی .com، .gov، .net و امثال آن با یک سایت مجاز تفاوت دارند. اگر فیلتر مورد نظر نتواند این دو را از یکدیگر تفکیک کند، یا باید برای دست‌رسی به سایت مجاز از دسترس‌ناپذیر کردن سایت نامجاز صرف‌نظر کند، یا اینکه از دسترس‌پذیر بودن سایت مجاز خودداری نماید.

در کنار این گونه مشکلات فنی، باید هزینهٔ تهیه و از آن مهم‌تر روزآمد نگه‌داشتن این ابزارها را هم مورد توجه قرار داد. به‌کارگیری آنها از عهدهٔ اشخاص عادی خارج است و نیاز به متخصصان ویژه دارد که در اینجا نیز باید هزینه‌های

آموزش و روزآمد نگه‌داشتن حوزهٔ تخصص آنان را هم مورد نظر قرار داد. از این رو، هنگام تصمیم‌گیری دربارهٔ به‌کارگیری این فناوری‌ها که حتی یک لحظه هم به دوام آنها امیدی نیست، باید واقع‌گرایانه و سنجیده تصمیم‌گیری شود.

ب-مزیت‌ها و محدودیت‌های فضای سایبر برای آزادی اطلاعات

رکن دیگر استقرار و نهادینه‌سازی مردم‌سالاری واقعی عبارت است از دست‌رسی آزاد و بی‌محدودیت آحاد مردم به اطلاعات به‌ویژه اطلاعات دولتی تا با آگاهی از چگونگی سیاست‌گذاری و عمل‌کرد کارگزاران دولتی، از سوءاستفاده‌های گونه‌گون از سمت دولتی ــ به‌ویژه ریشه‌دارترین و زیان‌بارترین آنها یعنی فساد اداری[41] ــ جلوگیری کنند.

در این زمینه، اصل ۱۱ بیانیهٔ ژوهانسبورگ با تأکید بر وجود این حق و ضرورت آن اشعار می‌دارد: «هر کس حق کسب اطلاعات از مقامات دولتی را دارا ست، اگرچه در ارتباط با امنیت ملی باشد...». همان گونه که ملاحظه می‌شود، این مسأله به‌اندازه‌ای اهمیت دارد که دست‌رسی به اطلاعات مرتبط با امنیت ملی نیز استثناء نشده است؛ هرچند در اینجا نیز ملاحظاتی رعایت شده است[42] [۶: ۱۷].

41. corruption

۴۲. با وجود این، احراز این ضرورت حیاتی به زمان حال مربوط نمی‌شود و حکومت‌های پیشین نیز بر این مسأله واقف بودند و به آن اعتقاد داشتند. توجه به سخنان امیرمؤمنان علی(ع) به خوبی این میزان قدمت و اهمیت را نشان می‌دهد. در بحبوحهٔ جنگ صفین، دو تن از لشگریان دربارهٔ دو موضوع از ایشان پرسیدند که واکنش آن حضرت نسبت به هر یک از آنان آموزنده است. نخستین پرسش دربارهٔ توحید بود. ولی، در مرتبهٔ دوم فردی نزد آن حضرت آمد و پرسید: چرا مردم بیست سال پیش شما را به خلافت برنگزیدند؟» آن حضرت فرمود: چه بدموقع سؤال کردی، اما تو حق داری سؤال کنی (و لک حق المسئله) و من باید پاسخ تو را بدهم» (خطبه ۱۶۲ نهج‌البلاغه). همچنین، در نامهٔ ۵۰ ایشان چنین آمده است: شایسته است کسانی که جایگاه حکومتی پیدا می‌کنند، آن را سفره‌ای برای بهره‌مندی نبینند و در مقابل مردم متواضع‌تر شوند. ای مردم بدانید حق شما بر من این است که هیچ اطلاعاتی را از شما دریغ نکنم، مگر اطلاعاتی که مربوط به مسائل امنیتی باشد» [۱: ۱۵].

برای درک مفهوم و کارکرد این اصل حقوق بشری، ضروری است نقش آن در پیشگیری از فساد اداری، مورد توجه قرار گیرد. مطابق آنچه در **کنوانسیون سازمان ملل متحد برای مبارزه با فساد**[۴۳] (مریدا، ۲۰۰۳) تأکید شده، برای پیش‌گیری از این جرم الگوی پیش‌گیری وضعی[۴۴] و اجتماعی[۴۵] مورد توجه قرار گرفته است. در پیش‌گیری اجتماعی، کوشش می‌شود تا با اتخاذ تدابیر آموزشی، مجرمان بالقوه با پیامدهای اعمال ناشایست خود آشنا شوند و در عین حال، برخی سالب‌های انگیزه[۴۶] مانند افزایش حقوق و پاداش‌های سلامت اداری نیز در دستور کار قرار می‌گیرد. از سوی دیگر، به دیگر کنشگران این رفتار نیز انواع جرم‌های فساد و شیوه‌های پیش‌گیری و گزارش آن به مراجع صلاحیت‌دار آموزش داده و از ارتکاب چنین جرم‌هایی باز داشته می‌شوند. زیرا، اصولا فساد جزء جرم‌های بدون بزه‌دیده[۴۷] شناخته می‌شود. برای مثال، رشوه‌دهندگان ــ چه به اجبار این کار را انجام دهند، چه طیب خاطر ــ از رفتار خود رضایت دارند و به همین دلیل، کشف این‌گونه جرم‌ها دشوار است. بنا بر این، باید آنان را آگاه کرد که حق دارند بدون تحمل بار مالی یا غیرمالی ناشایست، از خدمات دولتی مناسب بهره‌مند شده و فساد مانعی جدی برای احقاق حق آنان است[۲۹۰: ۳۱].

در پیش‌گیری وضعی، تکیه بر شفاف‌سازی[۴۸] است و کوشش می‌شود تا از شکل‌گیری یا بروز فرصت‌های[۴۹] مستعد فساد جلوگیری شود. بهترین گزینه نیز

---

43. united Nations Convention Against Corruption
44. situational prevention
45. social prevention
46. disincentives
47. victimless offences
48. transparency
49. opportunity

در دست‌رس قرار دادن عمومی همهٔ اطلاعات مربوط به امور و فعالیت‌های آن حوزه است؛ مانند اطلاعات مربوط به مناقصه‌های دولتی[۵۰] و نیز اطلاعات مربوط به دارایی‌های کارگزاران دولتی[۵۱] که در مورد اخیر از بروز تعارض منافع[۵۲] جلوگیری می‌کند [۳۱:۲۴۰].

۱. مزیت‌های فضای سایبر برای آزادی اطلاعات

همان گونه که در مقدمه اشاره شد، فضای سایبر در بهینه‌سازی فرایندها تحول بنیادینی ایجاد کرده است؛ تا اندازه‌ای که، تقریباً در همهٔ حوزه‌های خرد و کلان به کار می‌رود. طی سال‌های اخیر، بحث‌های کلان دربارهٔ تحقق دولت الکترونیکی به طور جدی مطرح و در این راستا اجلاس‌های منطقه‌ای و جهانی برگزار شده که از آن جمله **اجلاس جهانی جامعهٔ اطلاعاتی**[۵۳] در سوئیس در دسامبر ۲۰۰۳ است که در آن، **اعلامیهٔ اصول**[۵۴] با حضور ۵۴ رئیس جمهور و نخست‌وزیر و ۸۹ وزیر و همچنین سفیران و نمایندگان سیاسی در جمعی دوازده هزار نفری از اقشار فعال این حوزه تصویب شد و طبق آن ملزم شدند که در راستای استقرار جامعهٔ اطلاعاتی و بایسته‌های آن بکوشند. در سال ۲۰۰۵ نیز که این اجلاس در تونس برگزار شد، اعلامیهٔ دیگری با عنوان تعهد تونس[۵۵] به تصویب رسید [۸:۱۷۵].

طرح جدی این گونه بحث‌ها بدین دلیل است که به‌کارگیری این فناوری از سودمندی و فایده‌رسانی فراتر رفته و به ضرورت تبدیل شده است؛ به‌گونه‌ای که، حضور در جامعهٔ جهانی کنونی متضمن بهره‌مندی از زیرساخت‌ها و سازوکارهای فناوری اطلاعات و ارتباطات الکترونیکی است.

50. public procurement
51. public officials
52. conflict of interest
53. World Summit on Information Society
54. Declaration of Principles
55. Tunis Commitment

دربارهٔ آزادی اطلاعات، ملموس‌ترین نتیجه‌ای که از الکترونیکی شدن امور دولتی عاید شهروندان می‌شود، این است که زمینه‌های بروز فساد اداری کاهش می‌یابد. زیرا، مهم‌ترین عامل ارتکاب فساد- یعنی اعمال نظر شخصی و سوءاستفاده از سِمَت اداری- حذف می‌شود و از این پس برنامه‌های رایانه‌ایِ از پیش‌تنظیم‌شده اند که به جای کارگزاران به نیازهای مراجعه‌کنندگان پاسخ می‌دهند. حتی اگر شهروندان هم تمایل داشته باشند که خارج از سازوکارهای مقرر اداری عمل کرده و در ازاء آن منافع نامشروع پرداخت کنند، این امکان نیز از آنان سلب خواهد شد و بدین ترتیب، مبارزهٔ دوسویهٔ مؤثری علیه فساد به عمل خواهد آمد [۲۴: ۲۹].

همچنین، فضای سایبر بهترین ابزار شفاف‌سازی امور دولتی است. زیرا، اطلاعات طبق روال از پیش تنظیم‌شده، تولید و بدون اعمال تبعیض در میزان یا چگونگی دست‌رسی به افراد ارائه می‌شوند. هم‌اکنون نمونهٔ بارز این اقدام را می‌توان برگزاری مناقصه‌ها به شیوهٔ الکترونیکی دانست که گامی مهم در تحقق این هدف متعالی است[۵۶] [۶۴: ۴].

همچنین نباید از قابلیت‌های فضای سایبر در پیش‌برد هدف‌های پیش‌گیری

۵۶. قانون برنامهٔ چهارم توسعهٔ اقتصادی، اجتماعی و فرهنگی کشور مصوب شهریورماه ۱۳۸۳ با تأیید کارآیی این فناوری در مبارزه با فساد، در مادهٔ ۱۴۲ چنین مقرر می‌دارد: سازمان مدیریت و برنامه‌ریزی کشور و دستگاه‌های موضوع مادهٔ ۱۶۰ این قانون موظف‌اند به منظور افزایش پاسخ‌گویی دستگاه‌های اجرایی در مقابل مردم، با استفاده از فناوری‌های نوین اداری و بازنگری مهندسی فرایندها و روشها و رشد شاخص‌های مربوط به مشتری‌مداری و آموزش اداری و توسعهٔ فرهنگ مدیریت و ارزیابی عملکرد و راهکارهای لازم برای جلوگیری از مفاسد اداری، سطح کیفی خدمات خود را افزایش داده و در تدوین ضوابط و مقررات و بخشنامه‌ها، دستورالعمل‌های ذی‌ربط رضایت و تکریم ارباب رجوع به عنوان یکی از اهداف اصلی و تأثیرگذار در سرنوشت اداری و استخدامی کارکنان ملحوظ نمایند». همچنین، هم‌اکنون لایحهٔ انتشار و دست‌رسی آزاد به اطلاعات در مجلس شورای اسلامی مطرح است که در صورت تصویب نهایی با توجه به پیشنهادهای اصلاحی و الحاقی، یکی از سازوکارهای ارجح در آن به کارگیری ابزارهای الکترونیکی معرفی و بر آن تأکید شده است[۳۱: ۱۵].

اجتماعی از فساد غافل شد. در بند پیشین، به کارکردهای بی‌مانند آن در امر اطلاع‌رسانی و ارتباطات اشاره شد. این رسانه با توجه به نفوذ پرشتابی که در میان قشرهای مختلف جامعه دارد، به‌خوبی می‌تواند در امر آموزش و اطلاع‌رسانی مورد استفاده قرار گیرد و به اعتلاء و نهادینه‌سازی این حق مسلم حقوق بشری کمک کند[۳۱:۱۹۱].

۲. محدودیت‌های فضای سایبر در تحقق آزادی اطلاعات

پیش از ورود به بحث، لازم به ذکر است که با اینکه دو اصل آزادی بیان و آزادی اطلاعات مشابهت‌های بسیاری با یکدیگر دارند و به همین دلیل از فضای سایبر برای تحقق آنها تا حدودی به یک شکل بهره‌برداری می‌شود ــ یعنی در هر دو به‌طور عمده از قابلیت‌های اطلاع‌رسانی و ارتباطی استفاده می‌شود ــ موانع سایبری آنها مشابه نیست. برای روشن شدن این موضوع دو مؤلفهٔ اساسیِ تشکیل‌دهندهٔ این دو حق با یکدیگر مقایسه می‌شوند.

اطلاعاتِ موضوع آزادی بیان، یافته‌ها و دیدگاه‌های شهروندان نسبت به امور کشورشان است که با هدف آگاهی بیش‌تر مردم و از آن مهم‌تر مسؤولان نسبت به آنچه در کشور می‌گذرد، بازتاب می‌یابد. ولی، در آزادی اطلاعات، دولت موظف است که اطلاعات مربوط به امور حاکمیتی و تصدی‌گری خود را جز در موارد کاملاً مشخص و محدود در اختیار شهروندان قرار دهد تا آنان مشارکت آگاهانه‌تری در ادارهٔ حکومت داشته باشند. از این رو، نه‌تنها نوع اطلاعات، بلکه عامل ارائه و انتشار آنها نیز متفاوت است و در عمل تفاوتی نمی‌کند که اجراء این قاعده در فضای سایبر دنبال شود یا در جهان فیزیکی. زیرا، این تمایزهای بنیادین در همه جا وجود دارند. برای مثال، نمی‌توان از فیلترینگ برای رعایت مصالح و مقتضیات آزادی اطلاعات در فضای سایبر استفاده کرد؛ هرچند امکان به‌کارگیری مشترک برخی از ابزارها مانند تدابیر صدور مجوز انکارشدنی نیست.

ولی، دربارهٔ محدودیت‌ها و موانع پیش روی تحقق هدف‌های آزادی اطلاعات در فضای سایبر، به طور کلی می‌توان آنها را در دو گروه قرار داد: گروه نخست به ماهیت خود این فضا مربوط می‌شود و گروه دوم محدودیت‌ها و ضوابط قانونی است که همانند آزادی بیان بر اساس مصالح و مقتضیاتی تصویب و لازم‌الاجراء شده اند که در اینجا فقط گروه نخست بررسی می‌شوند. محدودیت‌های ذاتی فضای سایبر را در دو قسمت می‌توان بررسی کرد: ضعف زیرساخت‌های فناوری اطلاعات و ارتباطات الکترونیکی و خطرپذیری داده‌های الکترونیکی.

۲ـ۱. ضعف زیرساخت‌های فناوری اطلاعات و ارتباطات الکترونیکی

کشوری می‌تواند در تحقق جامعهٔ اطلاعاتی و دولت الکترونیکی گام‌های اساسی بردارد و از فضای سایبر برای دست‌رس‌پذیر کردن هرچه بیش‌تر اطلاعات دولتی برای شهروندان استفاده کند که زیرساخت‌های اساسی فناوری اطلاعات و ارتباطات الکترونیکی را فراهم آورد. این مسأله تا اندازه‌ای ضروری است که اگر چنین نشود، خسارت‌ها و آسیب‌های احتمالی این فضا بیش از منافع آن خواهد بود. بر این پایه، منظور از زیرساخت[۵۷] فقط تجهیزات و امکانات فنی الکترونیکی نیست، بلکه دو عامل مهم دیگر یعنی سواد رایانه‌ای ـ که به کاربران و دست‌اندرکاران آن مربوط می‌شود ـ و محتوای دیجیتالی نیز به همان اندازه تأثیر گذار اند. به عبارت دیگر، زمانی یک کشور می‌تواند ادعا کند که در بهره‌برداری همه‌جانبه از این فناوری و تحقق هدف‌های توسعهٔ دانش‌بنیاد پایدار در هزارهٔ نوین پیشگام است که هر سه عامل فوق را تأمین و تقویت کند. زیرا، ضعف در هر یک به‌تنهایی موجبات بروز شکاف دیجیتالی[۵۸] را فراهم خواهد آورد [۱۳: ۱۹].

به این ترتیب، برای تحقق آزادی اطلاعات در فضای سایبر، ابتدا دولت به

57. infrastructure
58. digital divide

مفهوم عام خود موظف است که تجهیزات فنی موردنیاز ــ از شبکه‌های بزرگ ذخیره و پردازش داده گرفته تا سیستم‌های رایانه‌ای شخصی ــ را در همهٔ اداره‌ها و مراجع مسؤول و در سراسر جامعه تأمین کند تا از این لحاظ کارگزاران دولتی و مردم کمبود نداشته باشند [۸:۲۰۴]. سپس، باید زمینهٔ کسب مهارت بهره‌برداری از این ابزارها را برای هر دو گروه پیش‌گفته فراهم آورد [۱۵:۱۳]. در غیر این صورت، نمی‌توان از یک قشر بی‌سواد رایانه‌ای انتظار داشت که آگاهانه به وظایف و حقوق خویش عمل کنند. در پایان نیز، تا زمانی که اطلاعات موضوع این حق به زبان ملی در قالب الکترونیکی درنیامده و همچنین برنامه‌های نرم‌افزاری مورد نیاز آنها نگارش و منتشر و به طور مستمر روزآمد نشود، هر میزان پیشرفت در دو حوزهٔ دیگر با بن‌بست روبه‌رو خواهد شد. بنا بر این، همان‌گونه که ملاحظه می‌شود، این سه عامل پیوند محکمی با یکدیگر داشته و باید در کنار هم و با رعایت شرایط و ملاحظه‌های یکدیگر توسعه و ارتقا یابند [۱۱:۳].

۲ــ۲. خطرپذیری داده‌های الکترونیکی

همان گونه که قابلیت‌های فضای سایبر نسبت به جهان فیزیکی بسیار است، آسیب‌پذیری آن نیز نگران‌کننده است؛ به‌گونه‌ای که، با وجود انواع ابزارهای امنیتی اجرا شدنی در سطوح زیربنائی، گره‌ها و نقاط پایانی، باز هم تعرض‌های رایانه‌ای[۵۹] که به مختل شدن کارکرد سیستم‌ها و از میان رفتن داده‌های رایانه‌ای می‌انجامند، رو به فزونی اند. وجود این گونه مسائل باعث شده که بسیاری از مراکزی که به امور حساس اشتغال دارند، از اتصال سیستم‌های رایانه‌ای خود به شبکه‌های جهانی اطلاع‌رسانی خودداری کرده و به شکل درون‌سازمانی و آف‌لاین[۶۰] به اشتراک‌گذاری داده‌ها بپردازند.

59. computer intrusions
60. offline

در این میان، امور و به‌تبع آن اطلاعات دولتی در فضای سایبر نه‌تنها از چنین تعرض‌هایی مصون نیستند، بلکه متناسب با نوع ساختار حکومت و عملکرد دولتمردان نیز ممکن است دشمنان دولتی و مردمی بسیاری آنها را تهدید کنند. از جملهٔ بارزترین آنها گروه‌های تروریستی اند و از آنجاکه فضای سایبر از جنبه‌های مختلف تحقق هدف‌های تروریستی را برای آنها بسیار آسان‌تر کرده است، به‌تدریج در حال انتقال اقدام‌های خود به این فضا هستند و به همین دلیل، به‌تازگی، بحث **تروریسم سایبری**[61] به طور جدی از سوی صاحب‌نظران مطرح شده و در همین راستا، کشورها اقدام‌های سیاست‌گذاری، قانون‌گذاری و اجرائی گسترده‌ای را با توجه به میزان تهدیدپذیری خود در دستور کار قرار داده اند[۱۴۲:۷].

با توجه به این مسائل، دولتمردان حق دارند تا وقتی به گونه‌ای متعارف و پذیرفتنی از امن بودن فضای سایبر مطمئن نشوند، از انتقال کامل امور خود به این فضا و فاصله گرفتن همیشگی از جهان فیزیکی خودداری کنند. درست است که در جهان فیزیکی نیز اداره‌ها، امور و اطلاعات دولتی در معرض تهدیدهای گوناگونی قرار دارند، این تهدیدها هیچ‌گاه جلوهٔ جهانی ندارند و به شکل ساده‌تر و با در اختیار گرفتن نیروها و امکاناتی نه چندان پیشرفته نیز می‌توان امنیت لازم را برقرار کرد. ولی، در فضای سایبر، ممکن است هر لحظه هزاران نفر در سراسر جهان برای رخنه به یک وب‌سایت یا پایگاه داده دولتی و از میان بردن داده‌های آن، در حال برنامه‌ریزی و اجراء گزینه‌های مختلفی باشند بی آنکه بتوان اقدام نتیجه‌بخشی را به اجراء گذاشت.

به هر حال، با توجه به همهٔ این مسائل، باز هم فضای سایبر و به‌تبع آن دولت الکترونیکی مزیت‌هایی برای جامعه و عموم مردم دارند که تقریباً همهٔ کشورها در حال اجراء طرح‌های بسیار خرد و کلان برای رسیدن به هدف‌های الکترونیکی

61. cyber terrorism

خود اند. هدف اصلی این است که با به حداقل رساندن تهدیدها، امکان بهره‌برداری بیش‌تر شهروندان از فضای سایبر برای احقاق حقوق خود فراهم شود.

پ. مزیت‌ها و محدودیت‌های فضای سایبر برای حریم خصوصی

موازین حقوق بشری‌ای که تاکنون با محوریت اطلاعات بررسی شدند، دست‌رس‌پذیری حداکثری به آن با کم‌ترین محدودیت را دنبال می‌کردند. ولی، اصل مهم حقوق بشری حریم خصوصی در اینجا، خلاف آن را دنبال می‌کند؛ یعنی، محدود کردن حداکثری دست‌رسی به طیفی از اطلاعات و آگاهی از آن. بنا بر این، برای اینکه همهٔ هدف‌های این موازین تأمین شود، باید جنبه‌های مختلف آنها به‌دقت بررسی و تحلیل شود.

برخلاف ظاهر ساده و درک‌شدنی حریم خصوصی، این مفهوم یکی از پیچیده‌ترین و چالش برانگیزترین مصداق‌های حقوق بشر است و به همین دلیل، نسبت به بقیهٔ حق‌ها مطالعات و نظریه‌پردازی‌های بیش‌تری برای شناسایی دقیق ماهیت و حوزهٔ شمول آن صورت گرفته است. به طور خلاصه، زمان طرح جدی بحث‌های مربوط به حریم خصوصی به حدود صد سال پس از اعلامیهٔ حقوق بشر و شهروند فرانسه برمی‌گردد که دو دادرس دیوان عالی امریکا به نام‌های ساموئل وارن[۶۲] و لوئیس براندیس[۶۳] با ابراز نگرانی از تعرض مجریان قانون به مکان‌ها و امور خصوصی شهروندان، به دولت هشدار دادند که به حریم خصوصی افراد احترام بگذارند و معیاری با عنوان «حق تنها ماندن»[۶۴] را مطرح کردند. پس از آن، اصلاحیهٔ چهارم قانون اساسی[۶۵] در این کشور تصویب شد که از آن به‌منزلهٔ

62.Samuel Warren
63. Louis Brandeis
64. let to be alone
65. Fourth Amendment of the Constitution

منشور حریم خصوصی شهروندان امریکایی یاد می‌شود و به‌تدریج در این کشور و دیگر کشورها قوانینی دربارهٔ حمایت از حریم خصوصی تصویب شد [۲۴:۱۵۷].

در اعلامیهٔ جهانی حقوق بشر نیز به این اصل توجه شده است. طبق مادهٔ ۱۲، این اعلامیه« احدی در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود نباید مورد مداخله‌های خودسرانه واقع شود و به شرافت و حیثیتش نباید تعرض شود. هرکس حق دارد در مقابل این گونه مداخلات و تعرضات مورد حمایت قانون قرار گیرد». همچنین، مادهٔ ۱۷ م.ب.ح.م.س بر حق اشخاص در محفوظ ماندن از مداخله‌های خودسرانه یا غیرقانونیِ مأموران دولتی یا اشخاص خصوصی حقیقی یا حقوقی در حریم، خانواده، منزل یا مکاتبه‌های خود و نیز عدم تعرض به شرافت و حیثیت آنان تأکید می‌کند. در اینجا، منظور از مداخلهٔ غیرقانونی این است که تنها به موارد تصریح‌شدهٔ قانونی اکتفا شود. مداخلهٔ خودسرانه نیز اقدام‌های فراقانونی را دربرمی‌گیرد. دلیل ذکر آن در کنار واژهٔ غیرقانونی تأکید بر این نکته بوده که حتی مداخله‌هایی که به موجب قانون صورت می‌گیرد، باید در چهارچوب شرایط و هدف‌های میثاق، متعارف و متناسب باشند. در هر حال، هر اقدامی باید به‌صراحت در قانون پیش‌بینی شده باشد.

۱. مزیت‌های فضای سایبر برای حریم خصوصی

فضای سایبر نه تنها ارتباطات خصوصی را وارد حوزه‌های بدیع و شگفت‌انگیزی کرده است، بلکه ناگزیر بخش عمده‌ای از اطلاعات شخصی نیز به شکل دیجیتالی درآمده و در بانک‌های گستردهٔ داده ذخیره و به شیوه‌های گوناگون پردازش می‌شوند.

۱ـ۱. ارتباطات خصوصی الکترونیکی

امروزه، انواع ارتباطات خصوصی مکتوب، صوتی و حتی ویدیویی الکترونیکی با کیفیتی مطلوب به صورت زنده و با امکانات جانبی بسیار، به شکل بی‌سیم یا

باسیم به طور گسترده در فضای سایبر در اختیار همگان قرار گرفته و نسبت به امکاناتی که این فضا برای برقراری این‌گونه ارتباطات ارائه می‌کند، نه‌تنها هزینه‌های آن اندک است، بلکه کار با آنها نیز آسان بوده و نیازمند مهارت فنی خاصی نیست. پیجرها[۶۶]، پست الکترونیکی[۶۷] و گپستان‌های اینترنتیِ حتی سه‌بعدی که می‌توان به دلخواه طرح‌ریزی کرد و حتی امکان برگزاری نشست‌های گروهی خصوصی را به شکل چندرسانه‌ای ترتیب داد، گوشه‌ای از قابلیت‌های فضای سایبر است که پیوسته جلوه‌های نوینی از آن نیز پدید می‌آید.

این وضعیت به‌خودی‌خود تحولی شگفت‌انگیز و مثبت در حوزهٔ ارتباطات و به‌تبع آن حریم خصوصی افراد انگاشته می‌شود؛ زیرا، باعث شده که آنان به بهترین شکل امور خصوصی خود را توسعه دهند و در بسترهای دیگری جز جهان فیزیکی از مواهب یک محیط خصوصی با امکانات مطلوب بهره‌مند شوند.

ولی، در کنار پیشرفت‌هایی که تقریباً می‌توان آنها را در زمرهٔ توسعهٔ کمیِ امور خصوصی افراد قرار داد، نباید بهبود کیفی آنها را نادیده انگاشت. در جهان فیزیکی، ابزارهای محدودی برای مصون داشتن محرمانگی[۶۸] و تمامیت ارتباطات خصوصی از انواع تعرض‌ها وجود دارد. ولی، نمونه‌های بسیار پیشرفته‌تری از آنها در فضای سایبر در دسترس است که امکان حفظ حریم داده‌های الکترونیکی را به شکل بسیار مطلوب‌تری فراهم کرده است. دو شیوهٔ رایجِ کارآمد عبارت اند از: ۱ــ رمزنگاری[۶۹] و استگانوگرافی[۷۰] و ۲ــ ناشناس‌کننده‌ها[۷۱].

دلیل اشاره به دو کارکرد **رمزنگاری** و **استگانوگرافی** این است که هر دو برای

66. pagers
67. e-mail
68. confidentiality
69. cryptography
70. steganography
71. anonymizers

مصون داشتن محرمانگی و تمامیت محتوای[۷۲] ارتباطات از تعرض‌های گوناگون به کار می‌روند. در رمزنگاری، متن اصلی[۷۳] به رمزنوشته[۷۴] تبدیل می‌شود و تا کلید رمزگشای[۷۵] آن موجود نباشد، خواندنی نخواهد بود. ولی، استگانوگرافی که شیوهٔ نوینی است، به فرد امکان می‌دهد که محتوای پیام خود را در میان محتوای دیگری که ظن‌برانگیز نیست، جای داده و بدین ترتیب، ذهن هر متعرضی را منحرف سازد [۲۷: ۳۷۳].

ناشناس‌کننده‌ها ابزار بسیار کارآمد دیگری اند که فضای سایبر در اختیار کاربران خود قرار داده تا از امور خصوصی خود حداکثر محافظت را به عمل آورند. این ابزار در واقع تکمیل‌کنندهٔ رمزنگارها و استگانوگرافی است؛ زیرا، مسیر حرکت ارتباطات خصوصی را به گونه‌ای مخدوش می‌کند که ردیابی آن برای دیگران اگر ناممکن نشود، بسیار دشوار خواهد بود. این مسأله از آن جهت اهمیت دارد که برخلاف جهان فیزیکی، مسیر حرکت پیام‌های الکترونیکی از خود پیشینه‌ای با عنوان آمد-شد داده‌ها[۷۶] به جا می‌گذارد که نه‌تنها خودشان ارزشمند اند، که می‌توانند زمینهٔ شناسایی دیگر اطلاعات خصوصی را نیز فراهم کنند. بنابراین، این ابزار می‌تواند از بروز بسیاری از تعرض‌ها به حریم خصوصی افراد جلوگیری کند [۲۸: ۶۶].

۱ـ۲. داده‌های خصوصی الکترونیکی

در روزگار کنونی که اطلاعات به گران‌بهاترین سرمایه تبدیل شده است، بهره‌برداری از اطلاعات خصوصی برای گردش کار امور گونه‌گون ضروری انکارناپذیر است. برای مثال، در ازای ارائه اطلاعات خصوصی به یک بنگاه یا

72. content
73. plain text
74. cipher text
75. decipher or decryption key
76. data traffic

مؤسسه اعتباری می‌توان شماره اعتباری دریافت کرد و به داد و ستد و تجارت الکترونیکی پرداخت یا از خدمات آموزشی آن لاین بهره برد.

همچنین، مزیت دیگری که فضای سایبر برای داده‌های خصوصی اشخاص به ارمغان آورده، تطبیق[77] آنها بر یکدیگر است. پیش از پیدایش فناوری رایانه و حتی سه چهار دهه پس از آن، داده‌های حوزه‌های مختلف به گونه‌ای نامتمرکز نگهداری می‌شدند و در عمل امکان گردآوری همهٔ داده‌های مربوط به یک فرد وجود نداشت یا با دشواری امکان‌پذیر بود. ولی، فضای سایبر متناسب با میزان مشارکت جدی عرصه‌های مختلف جامعه در امور آن‌لاین به اشخاص اجازه می‌دهد که اطلاعات مربوط به خود را در کم‌ترین زمان جمع‌آوری کرده و از امور شخصی و خصوصی‌شان بهتر آگاه شوند. بسیار اتفاق می‌افتد که اشخاص از برخی امور خصوصی مستند و ثبت‌شدهٔ خود آگاهی ندارند و چه‌بسا در اثر این ناآگاهی هزینه‌های جبران‌ناپذیری را متحمل شده یا فرصت‌های ارزشمندی را از دست داده اند. امروزه، با اتصال روزافزون انواع پایگاه‌های داده‌ای[78] به شبکه‌های آن‌لاین، امکان دست‌رسی افراد به داده‌های مربوط به خودشان و کاوش در میان آنها فراهم شده است[۲۶:۳۰۰].

۲. محدودیت‌های فضای سایبر در حفظ حریم خصوصی

همان گونه که مزیت‌های فضای سایبر برای دو اصل آزادی بیان و آزادی اطلاعات با حریم خصوصی تفاوت داشت، محدودیت‌های آن نیز یکسان نیست.

راه‌های گونه‌گونی برای شناسایی آسیب‌پذیری حریم داده‌های الکترونیکی وجود دارد. از جمله اشخاصی که با هدف‌های گوناگون این حوزه را مورد تعرض قرار می‌دهند. در این صورت، می‌توان نوع داده‌های خصوصی مورد توجه آنها را

77. data matching
78. data base

شناسایی و با سیاست‌گذاری درست و به‌هنگام، نسبت به رفع تهدیدهای احتمالی اقدام کرد [۱۹:۱۶]. این عوامل عبارت اند از: مجریان قانون، ارائه‌دهندگان خدمات شبکه‌ای و دیگر فعالان سایبری.

۲ـ۱. مجریان قانون

حساسیت برانگیز بودن این مراجع از آن جهت است که بنابه‌قاعده باید از قانون پیروی و از هرگونه اقدام خودسرانه خودداری کنند. در همین زمینه، توصیه‌های فنی دربارهٔ مادهٔ ۱۷ م.ب.ح.م تصریح دارد که مجریان قانون باید تمامیت و محرمانگی مکتوبات را به هر دو شکل قانونی[۷۹] و عملی[۸۰] رعایت کنند. نامه باید بدون بازکردن یا مطالعه به دست گیرنده برسد. نظارت ـ چه الکترونیکی و چه غیر آن ـ شنود تلفنی، تلگراف و دیگر شکل‌های ارتباط، استراق سمع و ضبط مکالمه‌ها ممنوع است. بازرسی منزل اشخاص باید به دلایل ضروری محدود شود و نباید به حد آزاربرسد. در جایی که به بازرسی بدنی نیاز است، با اتخاذ تمهیدهای مؤثر باید حفظ شرافت و حیثیت فرد مورد بازرسی تضمین شود [۳۰:۱۵۵].

با وجود این، فضای سایبر ویژگی‌های خاص و بی‌همتایی را به جامعهٔ حقوق کیفری و به‌ویژه مجریان قانون تحمیل کرده است. بسیاری از معیارهای اجراءشدنی در جهان فیزیکی در اینجا کارآیی ندارند و برای آنها باید خط‌مشی‌های جداگانه‌ای تدوین کرد. عدم حضور فیزیکی مجرمان در صحنهٔ جرم، دشوار بودن شناسایی آنان به دلیل امکان اتخاذ هویت‌های جعلی و غیرواقعی، و حتی در صورت شناسایی آنان، دشوار بودن دستگیری‌شان به دلیل وجود فاصلهٔ فیزیکی که در بسیاری از موارد به فراسوی مرزها کشیده می‌شود، و مشکلات مربوط به رعایت مقررات کیفری سایر کشورها همگی باعث شده اند که برای آیین دادرسی کیفری سایبری، قوانین و مقررات به‌کلی متمایزی پیش‌بینی و در مواردی

79. de jure
80. de facto

امتیازهایی نسبت به معیارهای جهان فیزیکی اعطاء شود و حتی جلوهٔ منطقه‌ای و بین‌المللی نیز بیابند[۲۱:۲۲].

با این همه، هر اندازه وضعیت عملکرد مجریان قانون در فضای سایبر پیچیده و دشوار باشد، باز هم باید اقدام‌های آنان را به‌گونه‌ای ضابطه‌مند کرد تا از تعرض به حقوق مسلم کاربران ــ به‌ویژه حوزهٔ حساس حریم داده‌های الکترونیکی‌شان ــ جلوگیری شود یا پیامدهای آن به حداقل برسد. به همین منظور، هم‌زمان با طرح بحث‌های مربوط به توسعهٔ اختیارات مجریان قانون در فضای سایبر، مسائل مربوط به عدم تعرض به آنان نیز مطرح شده است[۳۵:۲۳]. به طور خلاصه، آسیب‌پذیری حریم داده‌های الکترونیکی از سوی مجریان قانون در دو حالت تصور شدنی است: پیش‌گیری از وقوع جرم، و تحقیق دربارهٔ مجرمان و پی‌گرد آنان.

ابتدا یادآوری دو نکته ضرورت دارد. نخست، تعرض‌آمیز بودن یک اقدام دلیلِ غیرقانونی بودن آن نیست. ممکن است قانون‌گذار به این نتیجه برسد که برای حفظ نظم و امنیت جامعه، لازم است اشخاص از برخی حق‌های خود ــ از جمله، حریم خصوصی ــ چشم‌پوشی کنند که البته نفع مستقیم آن ابتدا متوجه خود آنان خواهد بود. دوم، پیش‌گیری از وقوع جرم وظیفه‌ای نیست که تنها بر عهدهٔ مجریان قانون باشد، بلکه دیگر اشخاص و مراجع نیز متناسب با وظایف اجتماعی خود به موجب قانون مکلف به این کار خواهند بود.

دربارهٔ تدابیر پیش‌گیرانهٔ سایبری که برای جلوگیری از وقوع جرم‌های سایبری یا مرتبط با فضای سایبر اجراء می‌شوند، گزینه‌های گونه‌گونی وجود دارد. از جملهٔ آنها تدابیر نظارتی[۸۱] است که در جهان فیزیکی دوربین‌های مداربستهٔ الکترونیکی برای کنترل مکان‌های خاص مثال زدنی اند. ولی، در فضای سایبر، مجموعه‌ای از برنامه‌های رایانه‌ای به کار می‌روند که بر حسب نوع برنامه‌ریزی

81. monitoring measures

برای آنها، همهٔ داده‌های مربوط به مبادله‌های الکترونیکی کاربرانی را که به هر دلیل در مظان ارتکاب جرم اند، جمع‌آوری می‌کنند تا مسؤولان مربوط آنها را به طور زنده بررسی کنند یا اینکه برای رسیدگی بعدی ذخیره می‌شوند. این اقدام تا اندازه‌ای مورد توجه مجریان قانون کشورها قرار گرفته است. برخی از آنها نیز به دلیل کارآیی‌شان در پیش‌گیری از وقوع تخلف‌ها و جرم‌ها، به گشت‌های پلیس در جهان فیزیکی تشبیه شده و گشتِ پلیسیِ سایبر[۸۲] نام گرفته اند[۲۳ :۲۸].

از آنجا که مجریان قانون ــ به‌ویژه پلیس ــ عمده کوشش خود را صرف تحقیق دربارهٔ مجرمان و پی‌گرد آنان می‌کنند، اقدام‌های آنان در این حوزه بیش‌تر مورد توجه قرار می‌گیرد. البته، نباید حساسیت کار آنان را در این مقطع نادیده انگاشت. زیرا، در مرحلهٔ پیش‌گیری از وقوع جرم، هنوز قانونی نقض نشده و مجریان قانون باید به ضرورت‌ها اکتفاء کرده و از اقدام‌های نابه‌جا خودداری کنند. ولی، در اینجا جرمی اتفاق افتاده و اجراء عدالت و احقاق حق بزه‌دیدگان ایجاب می‌کند که مجرم یا مجرمان موردنظر شناسایی و به مراجع صلاحیت‌دار قضائی تحویل داده شوند. بنا بر این، بنا به قاعده، آنان باید ابتکار عمل بیش‌تری داشته باشند. به همین دلیل، اصل تناسب[۸۳] به‌منزلهٔ راهکار اصلی مورد توجه قرار گرفته است. با پذیرش حساسیت‌های ناشی از مصون ماندن حریم داده‌های الکترونیکی افراد از هرگونه تعرض ــ به‌ویژه اقدام‌های تعرض‌آمیز مجریان قانون ــ به این واقعیت نیز باید احترام گذاشت که اگر آنان برای انجام وظایف خود اختیار عمل نداشته باشند، در عمل مجرمانی که به‌گونه‌ای روزافزون ارتباط‌شان با فضای سایبر بیش‌تر می‌شود و به‌خوبی می‌توانند آنان را از رهگذر آثار الکترونیکی به‌جامانده و همچنین دیگر پیشینه‌های الکترونیکی دادگاه‌پسند شناسایی کرده و به مراجع قضائی تحویل دهند، از اجراء عدالت به دور

82. cyber patrol
83. proportionate principle

خواهند ماند و به‌تدریج فضای سایبر به بستر بسیار مناسبی برای اقدام‌های مجرمانه تبدیل خواهد شد [۷۵ :۲۳].

۲ـ ۲. ارائه‌دهندگان خدمات شبکه‌ای

یکی از وجوه تمایز اصلی فضای سایبر با جهان فیزیکی این است که تعامل با آن نیازمند عبور از پلی به نام ارائه‌دهندگان خدمات شبکه‌ای[۸۴] است. تفاوتی نمی‌کند که اتصال به این فضا به شکل بی‌سیم ـ برای نمونه، از رهگذر تلفن‌های همراه ـ یا باسیم ـ مانند اتصال از رهگذر رایانه‌های شخصیِ متصل به تلفن‌های ثابت ـ یا دیگر سیستم‌ها باشد. در هر حال، عبور از این پل الزامی است.

در اختیار داشتن این گلوگاه می‌تواند ابتکار عمل‌های بسیاری را به ارائه‌دهندگان خدمات دهد. آنها اطلاعات بسیاری دربارهٔ امور گوناگون کاربران خود به‌دست می‌آورند. هرگونه تعامل با فضای سایبر از خود پیشینه‌ای به جا می‌گذارد که می‌تواند گویای بسیاری از واقعیت‌ها ـ از جمله امور خصوصی کاربران ـ باشد. همچنین، اگر قصد هرگونه سوءاستفاده وجود داشته باشد، هم به لحاظ کیفی و هم کمّی بیش از دیگران برای ارائه‌دهندگان خدمات امکان‌پذیر است. آنها به‌راحتی می‌توانند انواع بسیاری از داده‌های الکترونیکی خصوصی دربارهٔ افراد را در مقیاس بسیار بالا گردآوری کنند و نسبت به دیگران با محدودیت فنی و نیروی انسانی متخصص هم روبه‌رو نیستند. به همین دلیل، ضروری است که اقدام‌های این گروه از فعالان زیربنائیِ فضای سایبر تحت شمول قواعد و ضوابط دقیق و لازم‌الاجرائی قرار گیرد تا امکان هرگونه سوءاستفادهٔ احتمالی از میان رود [۱۱۹ :۲۳].

در همین زمینه، در تفسیر مادهٔ ۱۷ م.ب.ح.م.س. آمده که گردآوری و نگهداری اطلاعات شخصی روی رایانه‌ها، بانک‌های داده‌ای و دیگر دستگاه‌ها ـ چه از سوی مراجع دولتی و چه از سوی اشخاص خصوصی حقیقی یا حقوقی ـ

84. network providers

باید به موجب قانون باشد. دولت‌ها باید تمهیدهای مؤثر را به گونه‌ای اتخاذ کنند که اطلاعات مربوط به زندگی خصوصی افراد در دسترس اشخاصی قرار نگیرد که برای دریافت، پردازش و استفادهٔ از آنها مجوز قانونی ندارند. در راستای اجراء مؤثرترین شکل حمایت از زندگی خصوصی، افراد باید بدانند که کدام داده‌های شخصی‌شان به شکل ناملموس در فایل‌های خودکارِ داده‌ای و به چه مقاصدی ذخیره شده اند. همچنین، باید مرجع عمومی یا اشخاصی را که بر فایل‌های آنان کنترل دارد یا می‌تواند داشته باشد، بشناسند. اگر این فایل‌ها در برگیرندهٔ داده‌های شخصی نادرست است یا برخلاف مقررات قانونی جمع‌آوری یا پردازش شده باشند، باید بتواند درخواست اصلاح یا حذف آن را بدهد [۳۰:۱۵۷].

۲ـ ۳. دیگر فعالان سایبری

به طور کلی، هرکسی که با هر عنوانی ـ مانند دادوستد و تجارت الکترونیکی ـ به ارائهٔ خدمات سایبری می‌پردازد، بخشی از داده‌های خصوصی مراجعه‌کنندگان خود را دریافت می‌کند. حال ممکن است این دست‌یابی به موجب قانون باشد یا خود کاربر با رضایت برای بهره‌مندی از خدمات بیش‌تر آنها را ارائه کند، یا اینکه فعال سایبری مورد نظر به شیوه‌های مجاز یا نامجاز به آنها دست یابد. مهم‌ترین مثالی که می‌توان در مورد الزام قانونیِ ارائهٔ داده‌های خصوصی بیان کرد، به فعالیت‌هایی مربوط می‌شود که برای گروهی از کاربران مجاز بوده و برای بقیه نامجاز اند. برای مثال، در بسیاری از کشورها، دست‌رسی به محتوای برخی سایت‌ها منحصر به بزرگسالان شده برای کاربران زیر هجده‌سال ممنوع است. بنابراین، برای تفکیک افراد مجاز از نامجاز، در ابتدای ورود به سایت‌ها از آنان خواسته می‌شود که اطلاعات معتبر شناسایی‌کنندهٔ خود را وارد کنند. یکی از مهم‌ترین آنها شمارهٔ کارت اعتباری[85] است، زیرا، این کارت تنها به اشخاص بالای

85. credit card

هجده سال داده می‌شود. ولی، این شماره بسیار ارزشمند است و می‌تواند موجبات انواع سوءاستفاده‌ها و به‌ویژه زیان‌های مالی را فراهم کند [۵۴: ۲۰].

همچنین، بهره‌برداری کاربران از فعالیت‌های رسمی مانند خدمات بانک‌داری الکترونیکی، آموزش الکترونیکی یا دیگر امور اداری در جامعهٔ کنونی مستلزم این است که یک سلسله داده‌های خصوصی در پایگاه‌های داده‌ای به شکل آن‌لاین نگهداری و پیوسته روزآمد شوند که همان دغدغه‌ها نسبت به آنها نیز وجود خواهد داشت.

با وجود این، به دلیل ضرورت استفاده از داده‌های خصوصی الکترونیکی در پیش‌برد امور آن‌لاین، مقررات برخی کشورها به صاحبان سایت‌ها اجازه می‌دهند که برای تسهیل پیش‌برد فعالیت‌های مشروع خود، داده‌های خصوصی کاربران را دریافت و به گونهٔ مقرر استفاده کنند. ولی، برای اینکه اختیار عمل از مراجعه‌کنندگان سلب نشود، در صفحه نخست گزینه‌ای با عنوان خط‌مشیِ حریم خصوصی[۸۶] گنجانیده و در آن جزئیات چگونگی استفاده از داده‌های خصوصی ذکر شده تا در صورت عدم رضایت کاربر، از وارد کردن آنها خودداری کند.

ولی، در جایی که فعالان سایبری رأساً به دریافت داده‌های خصوصی کاربران مبادرت می‌کنند، تهدیدهای جدی‌تری بروز می‌یابد؛ حتی اگر برخی از آن اقدام‌ها مشروع باشند. برای مثال، کوکی‌ها[۸۷] برنامه‌هایی اند که متناسب با نوع برنامه‌ریزی‌شان به محض اتصال کاربر به سایت مورد نظر، به سیستم رایانه‌ای وی انتقال می‌یابند و همهٔ اطلاعات مربوط به نوع سیستم‌عامل، برنامه‌های کاربردی موجود و نیز علاقه‌ها و مطلوبیت‌های فردی کاربر را به سایت مورد نظر منتقل می‌کنند [۳۸۳: ۲۶]. با اینکه درجاتی از کوکی‌ها مجاز شناخته شده اند و

86.privacy policy
87. cookies

برای سامان‌دهی حوزه‌های سایبری و به‌ویژه ارائهٔ خدمات شبکه‌ای و نیز دادوستد و تجارت الکترونیکی مفید ارزیابی می‌شوند، می‌توانند آسیب‌های زیان باری نیز به حریم داده‌های الکترونیکی افراد وارد آورند. چنانچه آنها به گونه‌ای برنامه‌ریزی شوند که همهٔ داده‌های خصوصی اشخاص را انتقال دهند یا اینکه سایت موردنظر داده‌های خصوصی دریافتی را به دیگر سایت‌ها واگذار کند، دیگر چیزی به نام داده‌های خصوصی، رضایت کاربر و اساسی‌تر از همه حریم داده‌های الکترونیکی معنا نخواهد داشت.

این وضعیت به‌تازگی به حد نگران‌کننده‌ای رسیده است. زیرا، عده‌ای جمع‌آوری، ذخیره‌سازی و بهینه‌سازی داده‌های خصوصی کاربران را حرفهٔ خود قرار داده و خود از آنها برای اقدام‌های تعرض‌آمیز بعدی استفاده یا به مرتکبان آنها واگذار می‌کنند. بارزترین آنها نشانی‌های پست الکترونیکی و همهٔ داده‌های خصوصی مربوط به آنها ست که برای فرستادن پیام‌های ناخواستهٔ الکترونیکی[88] (که به اختصار اسپم[89] نامیده می‌شود) مورد استفاده قرار می‌گیرند و به همین منظور، برنامه‌هایی طرح‌ریزی شده اند که به طور خودکار نشانی کاربران را از فضای سایبر جمع‌آوری کرده یا اینکه به شکل پیش‌فرض آنها را تولید می‌کنند و به مبالغی مانند هر یک میلیون نشانی پنجاه دلار فروخته می‌شود [۳۴ :۲۵].

در اینجا نیز، بحث بهره‌برداری از داده‌های خصوصی به‌وسیلهٔ انطباق آنها با یکدیگر مطرح است. این مزیت که از ویژگی متمرکزسازی و یکپارچه‌سازی داده‌ها در فضای سایبر ناشی می‌شود، به افراد امکان می‌دهد که با کنار هم قرار دادن همه یا بیش‌تر داده‌های خصوصی به نتایجی دست یابند که در حالت پراکندگی‌شان ناممکن یا بسیار دشوار است. بنابراین، سودجویان نیز به گونه‌ای نتیجه‌بخش‌تر

88. unsolicited electronic messages
89. spam

و مؤثرتر می‌توانند برای سوءاستفاده از داده‌های خصوصی افراد برنامه‌ریزی کنند.

با توجه به این توضیحات، به نظر می‌رسد که سامان‌دهی حریم داده‌های الکترونیکی در حوزهٔ این فعالان به‌مراتب نسبت به دو گروه مجریان قانون و ارائه‌دهندگان خدمات شبکه‌ای دشوارتر باشد. زیرا، در اینجا شخصیت‌های گونه‌گونی به فعالیت‌های بسیار مختلفی مشغول اند که سیاست‌گذاری و برنامه‌ریزی برای امور آنها کار بزرگی است. متأسفانه، آنچه در اینجا کار را دشوار می‌سازد، این است که به‌جز آنهایی که همانند مجریان قانون و ارائه‌دهندگان خدمات به شکل رسمی فعالیت می‌کنند ــ مانند بانک‌داران الکترونیکی ــ بقیه به ضابطه‌ای مقید نیستند و ابتکارعمل در دست آنان است که با مهارت فنی بالا و تجربهٔ ارزشمندی که از تعامل با این فضا به دست آورده اند، می‌توانند هرگونه فعالیت مجاز یا نامجازی را طرح‌ریزی و اجرا کنند.

نتیجه‌گیری

بحث‌هایی که در این نوشتار به اجمال مورد اشاره قرار گرفت، از جمله دغدغه‌های اصلی و اساسی صاحب‌نظران، سیاست‌گذاران و تصمیم‌گیران جهان امروز است. چه این رخداد را تصادفی بدانیم و چه برنامه‌ریزی‌شده، به هر حال این فناوری و این سه حوزهٔ حقوق بشری بستر واحدی دارند و امکان تفکیک آنها از یکدیگر وجود ندارد. همان گونه که ملاحظه شد، این رخداد بیش از آنکه زیان‌بار باشد، مواهبی به همراه داشته که در نوع خود بی‌مانند و بسیار سودمند اند.

ولی، از نکات اشاره‌شده دربارهٔ چگونگی عینیت یافتن حق آزادی بیان در فضای سایبر، ملاحظه شد که قابلیت‌های رسانه‌ای و اطلاع‌رسانی آن تحولی به‌واقع بنیادین را رقم زده است. با این همه، در دست‌رس بودن نامحدود آن برای مجرمان بالقوه دغدغه‌هایی جدی را نیز برانگیخته و به همین دلیل طرح‌ریزی و

به‌کارگیری ابزارهای سامان‌دهندهِ دست‌رسی[۹۰] به یک ضرورت تبدیل شده است. البته، باید توجه داشت که اصل بر آزادی شهروندان در بهره‌برداری از این فضا برای ابراز عقاید و دیدگاه‌های خود است و هرگونه اقدام محدودکننده باید موضع استثناء خود را حفظ کند؛ به‌ویژه آنکه به دلیل کارکرد ناهوشمندانهٔ این ابزارها، ضریب خطاء بالایی داشته و هم‌اکنون نیز مشکلات بسیاری را ایجاد کرده‌اند.

دربارهٔ آزادی اطلاعات نیز ملاحظه شد که این فناوری نه‌تنها می‌تواند به‌منزلهٔ ابزاری مؤثر به کار رود، بلکه نتایج سودمندی نیز در مبارزه با فساد اداری دارد که با توجه به کوشش جمعی بین‌المللی در مبارزه با این معضل مشترک بشری، نقش و جایگاه این فناوری روشن است؛ هرچند بهره‌مندی از این مواهب زمانی امکان‌پذیر خواهد بود که زیرساخت آن به مفهوم عام ــ یعنی تجهیزات فنی، سواد رایانه‌ای و محتوای دیجیتالی ــ تأمین و تقویت شود.

دربارهٔ حریم خصوصی نیز، به لحاظ تعارض ماهوی آن با دو حق بشری پیش‌گفته، لازم است که احتیاط‌هایی به عمل آید؛ کما اینکه یکی از استثناءهای مورد تأکیدِ قوانین آزادی اطلاعات، اطلاعات مربوط به حریم خصوصی افراد است. بنابراین، این حوزه هنر سیاست‌گذاران و تصمیم‌گیران جامعه را می‌طلبد که با اِعمال منطقی و واقع‌گرایانهٔ اصولی مانند متعارف بودن[۹۰] یا تناسب، استیفاء حقوق مشروع شهروندان را امکان‌پذیر سازند.

90. reasonableness standard

فهرست منابع

۱. اسماعیل‌نیا، محمود (مترجم)؛ **جامعهٔ اطلاعاتی در آئینهٔ پژوهش**؛ کمیسیون ملی یونسکو و دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸۴.

۲. انصاری، باقر؛ **مؤلفه‌های دولت شفاف: حق مردم بر دانستن**؛ نشریهٔ گفتمان حقوقی، دفتر همکاری‌های فناوری ریاست جمهوری، شماره اول، آبان ۸۱.

۳. ایپکچی، محمدحسن (مترجم)؛ **تنوع فرهنگی و زبانی در جامعهٔ اطلاعاتی**؛ کمیسیون ملی یونسکو و دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۴.

۴. باقری‌اصل، رضا و طلوع، علیرضا؛ **راهنمای جامع تهیه و تدارک الکترونیکی کالا و خدمات (مناقصه‌گذاری الکترونیکی)**؛ مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸۵.

۵. بسته‌نگار، محمد؛ **حقوق بشر از منظر اندیشمندان**؛ شرکت سهامی انتشار، ۱۳۸۰.

۶. جلالی فراهانی، امیرحسین و باقری اصل، رضا؛ **پیشگیری اجتماعی از جرایم سایبری راهکاری اصولی برای نهادینه‌سازی اخلاق سایبری**؛ مجموعه‌مقالات دومین همایش منطقه‌ای اخلاق و فناوری اطلاعات؛ مرکز تحقیقات مخابرات، آذرماه ۱۳۸۵.

۷. جلالی فراهانی، امیرحسین؛ **تروریسم سایبری**؛ فصلنامه تخصصی فقه و حقوق، شماره ۱۰، پاییز ۱۳۸۵.

۸. جهانگرد، نصرا... و دیگران؛ **گزارش روند برگزاری اجلاس جهانی سران دربارهٔ جامعهٔ اطلاعاتی و مشارکت ایران (ژنو-۲۰۰۳)**؛ دبیرخانهٔ شورای عالی اطلاع‌رسانی، اسفندماه ۱۳۸۳.

۹. جهانگرد، نصرا... و رشیدی کمیجان، علیرضا؛ **ایجاد توسعهٔ پویا (گزارش نهایی مؤسسهٔ فرصت‌های دیجیتال)**؛ دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸۴.

۱۰. خرم‌آبادی، عبدالصمد؛ **سابقه پیدایش، تعریف و طبقه‌بندی جرایم رایانه‌ای**؛ مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات؛ معاونت حقوقی و توسعه قضائی قوه قضائیه، نشر سلسبیل، ۱۳۸۴.

۱۱. دی آنجلیز، جینا؛ **جرایم سایبر**؛ مترجم: حافظی، سعید و خرم‌آبادی، عبدالصمد؛

دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۳.

۱۲. کاشیان، علیرضا و دیگران (مترجم)؛ **راهبری اینترنت**؛ دبیرخانه شورای عالی اطلاع‌رسانی، تابستان ۱۳۸۴.

۱۳. کاظمی‌پور، ابراهیم (مترجم)؛ **آموزش در جامعهٔ اطلاعاتی**؛ کمیسیون ملی یونسکو و دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۴.

۱۴. کولیور، ساندرا و دیگران؛ **آزادی، حق و امنیت**؛ مترجم: آقایی، علی اکبر؛ فصلنامه مطالعات راهبردی، شماره ۴۹، ۱۳۷۹.

۱۵. مرکز پژوهش‌های مجلس شورای اسلامی؛ **اظهارنظر کارشناسی دربارهٔ لایحهٔ آزادی اطلاعات؛ شمارهٔ ۷۵۹۶**، بهمن‌ماه ۱۳۸۵.

۱۶. مرکز پژوهش‌های مجلس شورای اسلامی؛ **حریم داده‌های الکترونیکی**؛ شماره ۸۰۶۹، آبان‌ماه ۱۳۸۵.

۱۷. نمک‌دوست تهرانی، حسن؛ **اصول ژوهانسبورگ: امنیت ملی، آزادی بیان و دسترسی به اطلاعات**؛ از سایت ایران و جامعه اطلاعاتی، مرکز پژوهش‌های ارتباطات، ۱۳۸۴.

۱۸. وبستر، فرانک؛ **نظریه‌های جامعهٔ اطلاعاتی**؛ مترجم: قدیمی، اسماعیل؛ نشر قصیده‌سرا، چاپ دوم، ۱۳۸۳.

۱۹. یزدان‌پور، اسماعیل (مترجم)؛ **علم در جامعهٔ اطلاعاتی**؛ کمیسیون ملی یونسکو و دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۴.

20. Board on Children, Youth and Families; **Technical, Business and Legal Dimensions of Protecting Children from Pornography on the Internet**; National Academy Press, 2004.
21. Casey, Eoghan; **Digital Evidence and Computer Crime;** Academic Press, 2001.
22. Council of Europe; **Explanatory Report of Convention on Cyber Crime;** at: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm; 2001.
23. Department of Justice of the United States; **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations**; 2002.

24. Graham J. H. Smith; **Internet Law and Regulation**; Sweet & Maxwell, 2002.
25. OECD Task Force on Spam; **Anti-Spam Regulation;** 15-Nov-2005.
26. Rowland, Diane & Macdonald, Elizabeth; **Information Technology Law**; Cavendish publishing, 2005.
27. Shinder, Debra Littlejohn; **Scene of the Cyber Crime, Computer Forensics Hand Book;** Syngress Publication, 2002.
28. Thornburgh, Dick & S. Lin Herbert, Editors; **Youth, Pornography and The Internet**; National Academy Press, 2004.
29. Transparency International; **Global Corruption Report; Special Focus: Access to Information**; 2003.
30. United Nations; **International Human Rights Instruments;** Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies; 2004.
31 .United Nations Office on Drugs and Crime; **The Global Program Against Corruption;** UN Anti-Corruption Toolkit Third Edition, Vienna, September 2004.