نظارت بر فضای مجازی و حریم خصوصی کاربران

مصطفی علیمرادی*
malimoradi@noornet.net

چکیده
نظارت بر فضای مجازی با هدف صیانت از حقوق کاربران، از الزامات این فضاست که در کشورهای گوناگون، قوانین و مقرراتی برای آن تدوین شده و بر پایه آن، حقوق و تکالیفی برای کاربران فضای مجازی تعیین گردیده است. از چالش‌های مطرح در نظارت بر فضای مجازی، تعارض احتمالی آن با حریم خصوصی کاربران است. در این مقاله، به بررسی جنبه‌های نقض حریم خصوصی کاربران با وضع قوانین نظارتی و راه‌های جلوگیری از نقض حریم خصوصی پرداخته خواهد شد.

کلیدواژگان: نظارت بر فضای مجازی، حریم خصوصی، صیانت از کاربران فضای مجازی، قوانین و مقررات فضای مجازی، جرایم فضای مجازی، امنیت فضای مجازی.

---

* کارشناس برنامه‌ریزی راهبردی اداره کل طرح و برنامه مرکز نور.

مقدمه

فضای مجازی که در بستر فناوری اطلاعات شکل گرفته، به تناسب این فناوری دارای شتاب در پیشرفت و پیچیدگی است. این پیچیدگی‌ها در ابزار و شیوه‌های استفاده به گونه‌ای است که حتی بسیاری از کسانی که در استفاده از آن مهارت دارند، به همه جنبه‌ها و شئون آن واقف نیستند. این فضای مبهم و بسیار نامتعین که هم از دید ابزار، فنون و کاربرد، و هم از دید ماهیت فضای مجازی که در آن هویت‌های فعالان تشخّص و تعیّن دقیق ندارد، زمینه را برای ارتکاب جرایم فراهم کرده است. از دید روان‌شناختی، نامشخص بودن هویت واقعی افراد در این فضا، وضعیتی را برای کاربران به وجود می‌آورد که بسیاری از رفتارهایی که در فضای واقعی شرم انجام آن را دارند، به‌راحتی انجام دهند.

آسیب‌هایی که ممکن است بر کاربران فضای مجازی برسد، بسیارند و گاه برخی از آنها هنوز از منظر کارشناسان و متخصصان ناشناخته مانده است. روزانه، شکایات بسیاری از آسیب‌های فضای مجازی به مراجع قانونی برده می‌شود.

در یک دسته‌بندی، جرایم فضای مجازی را به پنج دسته تقسیم کرده‌اند:

۱. جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، شامل: دو عنوان جعل رایانه‌ای، تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی؛

۲. جرایم مالی و اقتصادی، مانند: اقسام سرقت و کلاه‌برداری رایانه‌ای فروش محصولات غیر قانونی، قمار و نظایر آن؛

۳. جرایم علیه عفت و اخلاق عمومی؛

۴. هتک حیثیت و آبروی اشخاص حقیقی و حقوقی، سازمان‌ها و نهادها و نشر اکاذیب؛

۵. جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، شامل: دسترسی غیر مجاز، شنود غیرمجاز و جاسوسی رایانه‌ای (امامی، ۱۳۸۹، ص۴۶).

از مهم‌ترین راهکارهای جلوگیری از ارتکاب جرم در فضای مجازی، نظارت بر فعالیت کاربران در فضای مجازی و بستن مسیرهای وقوع جرم است؛ اما از چالش‌های بسیار مهم در نظارت کردن بر فضای مجازی، تعارض‌های احتمالی‌اش با حریم خصوصی کاربران است.

تعارض‌های نظارت بر فضای مجازی و حفظ حریم خصوصی کاربران

در نمونه‌های بسیار، مانند حملات تروریستی و تهدید امنیت ملی، دولت‌ها ترجیح می‌دهند که در تقابل دوگانه حریم خصوصی و امنیت، جانب امنیت را بگیرند که در این صورت، حریم خصوصی افراد محدود می‌شود و تعریف حریم خصوصی در این وضعیت، بسیار تنگ خواهد شد. شاید بهترین مثال در این زمینه، اقدام دولت آمریکا در نظارت بر عملکرد کاربران اینترنتی و کنترل تماس‌های تلفنی شهروندان بدون اطلاعات آنها پس از حوادث یازدهم سپتامبر سال ۲۰۰۱م باشد.

گفتنی است که همه شئون نظارت بر فضای مجازی، با حریم خصوصی در تناقض نیست. بسیاری از روش‌های نظارتی فضای مجازی، به نقض یا تهدید حریم خصوصی کاربران منجر نمی‌شود. از میان این شیوه‌ها، می‌توان به نمونه‌های ذیل اشاره کرد:

* تدوین مقررات و اخذ تدابیر خاص برای صدور مجوز فعالیت در فضای مجازی؛

* مدیریت یکپارچه فضای مجازی و پرهیز از تشتت قوا در نظارت و قانون‌گذاری؛

* آگاهی‌بخشی به کاربران و فعالات فضای مجازی در زمینه تهدیدها و چالش‌های این فضا؛

* مشارکت‌آفرینی و استفاده از ظرفیت جمع‌سپاری در حوزه نظارت و امنیت.

اما برخی از شئون نظارت، ممکن است سبب نقض حریم خصوصی شود. از نمونه‌های تعارض این دو عرصه را می‌توان چنین برشمرد:

* رصد پیام‌های خصوصی کاربران در سکوهای گوناگون؛

* وارسی دستگاه رایانه شخصی، گوشی هوشمند یا ابزارهای دیگر کاربران؛

* رصد محتواهای متنی و شنود اسناد صوتی، تصویری و ویدئویی کاربران در فضای مجازی؛

* گردآوری، پردازش و تحلیل محتوای تولیدشده یا رفتارهای کاربران؛

* گردآوری و دسته‌بندی اطلاعات هویتی و تماس کاربران.

مسئله تعارض میان نظارت بر فضای مجازی با هدف حفظ امنیت ملی و صیانت از حقوق کاربران و حریم خصوصی آنان، از مسائل چالشی است و در بین صاحب‌نظران در این زمینه، اختلاف نظرهای بسیار وجود دارد. برخی از ایشان، مهم‌ترین مسئله را حریم خصوصی کاربران می‌دانند و نقض آن را به هیچ وجه مجاز نمی‌شمرند. برخی دیگر، امنیت را مسئله محوری قلمداد می‌کنند که برای رسیدن به آن، می‌توان از امور دیگر صرف نظر کرد. برخی دیگر از صاحب‌نظران، در پی دستیابی به راه حلی هستند که میانِ این دو جمع کرد؛ به نحوی که هم امنیت پایدار بماند و هم حریم خصوصی کاربران محترم باشد.

عباسیان و همکاران (۱۳۹۸) در مقاله خود آورده‌اند که توجه بـه مسائل امنیتی مربوط به شهروندان، تا جایی باید مورد نظارت و کنترل حکومتی باشد که خود به‌نوعی در حریم خصـوصـی و امنیت فردی مردم در جامعه دخیل نگردد؛ زیرا نظارت و کـنـتـرل بی‌اندازه حکومتیان در روند کاربری،

مسئله تعارض میان نظارت بر فضای مجازی با هدف حفظ امنیت ملی و صیانت از حقوق کاربران و حریم خصوصی آنان، از مسائل چالشی است و در بین صاحب‌نظران در این زمینه، اختلاف نظرهای بسیار وجود دارد. برخی از ایشان، مهم‌ترین مسئله را حریم حصوصی کاربران می‌دانند و نقض آن را به هیچ وجه مجاز نمی‌شمرند. برخی دیگر، امنیت را مسئله محوری قلمداد می‌کنند که برای رسیدن به آن، می‌توان از امور دیگر صرف نظر کرد. برخی دیگر از صاحب‌نظران، در پی دستیابی به راه حلی هستند که میانِ این دو جمع کرد؛ به نحوی که هم امنیت پایدار بماند و هم حریم خصوصی کاربران محترم باشد

خود به‌نوعی اختلال در حریم شخصی و امنیت اطلاعات آنها وارد خواهد کرد (عباسیان، افشانی و اسلامی، ۱۳۹۸).

فتحی و شاه‌مرادی (۱۳۹۶) برآن‌اند که در تعریف و ترسیم امنیت در فضای مجازی، باید به گونه‌ای عمل کرد که دو مؤلفه «نظم عمومی» و «امنیت و حریم خصوصی» اصل قرار گیرد و دولت‌ها باید در ارائه راهکارها هم به نظم و امنیت عمومی و هم حریم خصوصی توجه کنند و این، هنر دولت است که در انجام وظایفش در فضای مجازی، میان امنیت و حریم خصوصی تعادل برقرار کند (فتحی و شاه‌مرادی، ۱۳۹۶، ص۲۵۱).

نگاه هزینه ـ فایده‌ای به تعارض نظارت و امنیت فضای مجازی با حریم خصوصی

فضای مجازی به سبب آسان‌سازی امور گوناگون در زندگی مردم، بسیار مورد استقبال قرار گرفته است و از طیف‌های گوناگون و از هر سن و جنس، طبقه اجتماعی، قومیت و سطح تحصیلاتی، در این فضا فعالیت می‌کنند و در عین حال، هیچ‌یک از این ویژگی‌های افراد، برای فعالان فضای مجازی شناخته‌شده نیست و راهی برای حصول اطمینان از اینکه فردی که در فضای مجازی در حال تعامل با آن هستیم، چند سال دارد، جنسیتش چیست، از چه قومیتی و در چه سطح تحصیلات یا طبقه اجتماعی است، وجود ندارد؛ حتی فراتر از آن، نمی‌توان فهمید که شخص مورد تعامل، اصلاً انسان است یا ماشین.

در چنین فضای مبهمی که هر روز به ابعاد ابهامات آن افزوده می‌شود، نبودِ نظارت، سبب وقوع بحران‌های بسیار برای جامعه خواهد شد. از همین روی، کشورهای گوناگون، با به کاربردن راهکارهای گوناگون، قواعد و مقرراتی برای کاربران فضای مجازی ایجاد و در بسیاری از کشورها، محدودیت‌هایی برای استفاده از آن اِعمال می‌کنند. چنان‌که گذشت، مناقشه‌انگیزترین مسئله در نظارت بر فضای مجازی، امکان تعرض به حریم خصوصی کاربران است.

مفهوم حریم خصوصی در کشورهای گوناگون، دارای معانی مختلف است و بر پایه قوانین حاکم بر آنها، معنای حریم خصوصی از کشوری به کشور دیگر تغییر می‌کند.

در ایران، حقوق و آزادی‌هایی که تحت عنوان حریم خصوصی قابل حمایت‌اند، غالباً به طور ضمنی و در بطن قواعد مختلف و گاه ناقص مورد حمایت قرار گرفته است؛ برای نمونه، می‌توان

به الفاظی دال به این معنا استناد کرد؛ مانند دسترسی به داده‌ها، شنود غیرمجاز و هتک حیثیت به وسیله سامانه‌های رایانه‌ای یا مخابراتی که در قانون جرایم رایانه‌ای مصوب ۱۳۸۸ آمده (آقابابایی و عباسی، ۱۳۸۹، ص۲۱) و یا اسنادی دیگر مانند: مبانی اسلامی نظام حقوقی ایران، قانون اساسی، قانون آیین دادرسی کیفری، قانون آیین دادرسی مدنی، قوانین و مقررات مربوط به ارتباطات پستی، تلفنی و اینترنتی. این نمونه‌ها، در زمره قوانینی هستند که گاه به طور ضمنی و گاهی صریح، از برخی از مصادیق حریم خصوصی حمایت می‌کند. (احمدی جشفقانی و شوق‌نیان، ۱۳۹۷، ص۱۳۸).

گفتنی است، لایحه‌ای در حمایت از حریم خصوصی در دولت هشتم تنظیم شده است که هنوز به قانون تبدیل نشده و در آن، حریم خصوصی تعریف شده و ابعاد حقوقی آن، تعیین گردیده است.

در برخی مقالات، حریم خصوصی کاربران فضای مجازی را در دو حوزه بررسی کرده‌اند:

الف. ارتباطات خصوصی یا غیرعمومی کاربران که در قالب متن، صوت و تصویر انجام می‌شود؛

ب. پایگاه‌های داده که حاوی اطلاعات شخصی کاربران است و افراد گوناگون ممکن است به‌راحتی به آن دسترسی یابند.

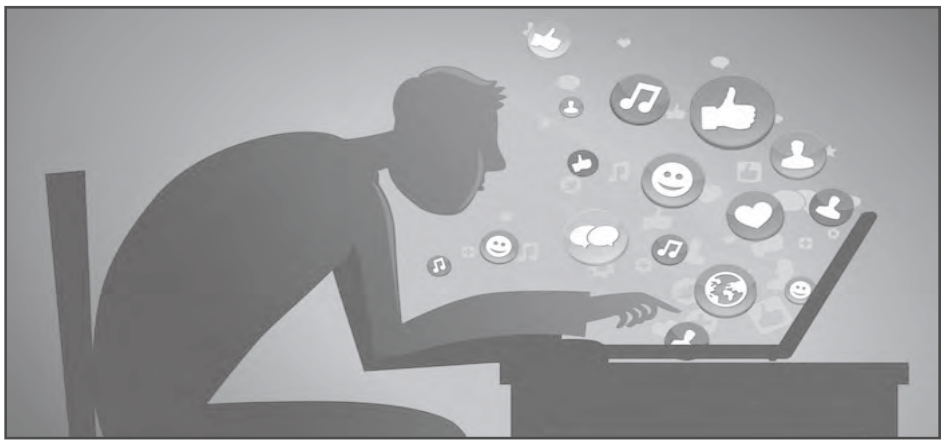
همچنین، حریم خصوصی افراد ممکن است در مراحل گوناگونِ فعالیت در فضای مجازی تهدید شود:

* عملیات تولید اطلاعات؛
* عملیات گردآوری اطلاعات؛
* پردازش اطلاعات؛
* انتقال داده و اطلاعات.

مهم‌ترین مصادیق نقض حریم خصوصی در مرحله تولید و گردآوری اطلاعات، شامل این نمونه‌هاست:

ـ گردآوری داده‌های شخصی برای هدف غیرقانونی و نامشروع؛

قوانین حریم خصوصی باید به گونه روشن برای همه افراد جامعه، به‌ویژه کاربران فضای مجازی، تعریف شود و افراد پیش از هر گونه فعالیت در این فضا، با مقررات، قوانین، چالش‌ها و تهدیدهای آن به‌خوبی آگاه شوند. مفاهیمی مانند: سواد رسانه، سواد فضای مجازی و سواد دیجیتال، اشاره به مهارت‌هایی دارد که با دارا شدن آنها، افراد توانایی انجام بهتر، ساده‌تر و کم‌مشکل‌ترِ کارها را در فضای مجازی خواهند داشت. ازاین‌روی، کسب این مهارت‌ها نیز از مقدمات فعالیت در فضای مجازی است



ـ گردآوری داده‌های شخصی بدون جلب رضایت یا بدون اجازه صریح قانون‌گذار؛

ـ گردآوری داده‌های شخصی از طریق روش‌های غیرقانونی یا به صورت سِرّی و ارسال نرم‌افزارهای جاسوسی یا نصب دوربین و میکروفن‌های مخفی؛

ـ گردآوری داده‌های شخصی مازاد و غیرمرتبط با هدفی که موضوع داده‌ها موافقت شده؛

ـ نقض اصل شفافیت در گردآوری داده؛

ـ گردآوری داده‌های نادرست، ناقص یا قدیمی؛

ـ نقض اصل ناشناس در گردآوری داده‌ها در موارد غیرضروری یا بدون اجازه قانون.

در حوزه پردازش اطلاعات نیز مصادیق نقض حریم خصوصی را می‌توان این‌چنین برشمرد:

ـ پردازش اطلاعات برای اهداف نامشروع؛

ـ پردازش داده‌های شخصی بدون جلب رضایت صاحبان داده؛

ـ پردازش با روش‌های غیرصادقانه و فریب‌آمیز برای کسب نتیجه‌های خاص یا تولید و استفاده از داده‌های کاذب؛

ـ تخریب یا تغییر داده‌های شخصی از طریق پردازش؛

ـ نقض اصل شفافیت در پردازش داده‌ها؛

ـ پردازش داده‌های ناشناس، با روشی که سبب آشکارسازی هویت شخصی گردد؛

ـ پردازش بیش از حدّ توافق‌شده یا غیرمرتبط با هدف اعلام‌شده.

نمونه‌های نقض حریم خصوصی در انتقال داده هم عبارت‌اند از:

ـ افشا و انتقال داده‌های شخصی برای اهداف نامشروع؛

ـ افشا و انتقال داده‌های شخصی بدون رضایت صاحب یا مجوز قانونی؛

ـ نقض اصل کیفیت داده‌ها در مرحله انتقال که موجب پایداری جرم افترا شود (آقابابایی و عباسی، ۱۳۸۹).

نظارت فضای مجازی نیز از مفاهیم بسیار مشکک است که شامل مصادیق گوناگونی می‌شود. نظارت

در فضای مجازی نیز انعطاف در تعیین مرزها و حدود حریم خصوصی افراد، معنادار است. بنا بر حکم عقلی، نظارت بر فعالیت‌های افراد در فضای مجازی، گاهی به بررسی و رصد محتواهای کاربران منجر می‌شود و این امر اگر بر پایه قانون مدون و اعلام قبلی انجام شود، نه تنها منافی حریم خصوصی یا نقض آن نخواهد بود که به امنیت بیشتر حریم خصوصی کاربران نیز کمک خواهد کرد. ناامن‌شدن فضای مجازی، زمینه را برای تهدیدهای امنیتی مانند: خرابکاری، اخلال امور، ترور، جاسوسی و نظایر آن فراهم می‌سازد

ممکن است از وضع قوانین بازدارنده تا بررسی همه محتواها، رفتارها و تعاملات افراد در فضای مجازی را دربرداشته باشد.

در یک تحقیق، راهکارهای دولت‌ها برای نظارت بر فضای مجازی، این‌گونه دسته‌بندی شده است:

*** راهبردهای ایجاد و تنوع‌سازی:**

ـ ایجاد شبکه اجتماعی مجازی ملی؛

ـ ایجاد شبکه‌های اجتماعی تخصصی؛

ـ ایجاد شبکه‌های اجتماعی مجازی برای گروه‌های مختلف سنّی و سلیقه‌ای.

*** راهبردهای همکاری و تشریک مساعی:**

ـ انعقاد توافق‌نامه با تأمین‌کنندگان شبکه‌های اجتماعی مجازی یا تأمین‌کنندگان خدمات اینترنتی؛

ـ استفاده از ظرفیت‌های مردمی برای تأمین سلامت و امنتی در جامعه؛

ـ استفاده از مشارکت‌های مردمی برای مدیریت بحران و بالابردن اتحاد ملی؛

ـ همکارهای میان‌کشوری و تشکیل انجمن‌ها و اتحادیه‌های منطقه‌ای و بین‌المللی.

*** راهبردهای استفاده هدفمند:**

ـ ارائه خدمات دولت الکترونیک از طریق شبکه‌های اجتماعی مجازی؛

ـ ارتباط دولت با مردم و دریافت نظرات آنان با گشودن صفحات کاربردی در شبکه‌های اجتماعی؛

ـ توسعه تعاملات بین‌المللی؛

ـ افزایش نظارت‌های دولتی بر افکار مردم از طریق پایش شبکه‌های اجتماعی.

*** راهبردهای ترویجی و آموزش و آگاه‌سازی:**

ـ بالا بردن سهم کشور در عرضه تولید محتوا و حضور رسانه‌ای در سطح بین‌المللی؛

ـ فراهم‌سازی بسترهای زیرساختی برای تقویت حضور مردم و سازمان‌ها در شبکه‌های اجتماعی مجازی؛

ـ پیگیری شکایت‌های افراد در صورت هتک حریم خصوصی آنها؛

ـ تهیه برنامه‌های کنترل والدین؛

ـ تدوین برنامه‌های آموزشی و آگاه‌سازی والدین؛

ـ تدوین برنامه‌های آموزشی و آگاه‌سازی کاربران از خط قرمزها.

*** راهبردهای تدافعی:**

ـ پایش بر اساس برخی کلمات؛

ـ پایش نمایه کاربری شخصی کاربران؛

ـ فیلترینگ موضوعی یا موقت شبکه‌های اجتماعی؛

ـ فیلترینگ مطلق شبکه‌های اجتماعی؛

ـ فیلترینگ داوطلبانه؛

ـ قانونگذاری و تعیین خط قرمزها در شبکه‌های مجازی و تعیین جرایم؛

ـ سیاست نام واقعی. (طالب‌پور، شیدایی و خلیل‌زاده سلماسی، ۱۳۹۳، ص۴۷ ـ ۴۹)

از میان این دسته‌بندی، تنها راهبرد تدافعی، با مسئله حریم خصوصی ممکن است تعارض داشته باشد.

شایان توجه است که مسئله نظارت بر فضای مجازی، از دغدغه‌های اصلی همه حکومت‌ها در سراسر جهان است و کشورهای گوناگون، بدون بحثی، مهار کردن فضای مجازی را حق خود می‌دانند و از راه‌های مختلف بر نظارت بر آن تأکید دارند. (ذوالفقاری، ۱۴۰۰)

حق، آن است که قوانین حریم خصوصی باید به گونه روشن برای همه افراد جامعه، به‌ویژه کاربران فضای مجازی، تعریف شود و افراد پیش از هرگونه فعالیت در این فضا، با مقررات، قوانین، چالش‌ها و تهدیدهای آن به‌خوبی آگاه شوند. مفاهیمی مانند: سواد رسانه، سواد فضای مجازی و سواد دیجیتال، اشاره به مهارت‌هایی دارد که با دارا شدن آنها، افراد توانایی انجام بهتر، ساده‌تر و کم‌مشکل‌ترِ کارها را در فضای مجازی خواهند داشت. ازاین‌روی، کسب این مهارت‌ها نیز از مقدمات فعالیت در فضای مجازی است.

با تعیین حدود و ثغور حریم خصوصی، قوانین نظارتی را می‌توان تدوین کرد. در وضعیت عادی که همه امور به گونه به‌هنجار در حال انجام است، قوانین کمترین احتمال تعارض با حریم خصوصی را خواهند داشت؛ اما در وضعیت‌های بحرانی، نظارت‌ها نیز تشدید می‌شوند و در این حالت، تعارض‌ها میان این دو، بسیار بیشتر به چشم خواهد آمد.

مسئله در این اوضاع، انتخاب یکی از این دو حالت است: امنیت و حریم خصوصی. آیا در هر وضعیتی، محترم داشتن حریم خصوصی و تعریفی سخت و غیرمنعطف از آن، ضرورت دارد، یا امنیت مقدم بر آن خواهد بود.

امنیت، اساس هر کاری است و بدون داشته جامعه ایمن، هیچ کاری پایه نمی‌گیرد و در جامعه ناایمن، حرمت هیچ چیز را نمی‌توان پاس داشت. پس، با نگاه هزینه و فایده، نظارت بر فضای مجازی با هدف صیانت از حقوق کاربران و امنیت اجتماعی، بر حفظ حریم خصوصی ترجیح خواهد داشت. احتمال نقض حریم خصوصی، در فرایند به‌کارگیری راهکارهای امنیتی و تدابیر پیشگیرانه و نظارت بر فضای مجازی، اجتناب‌ناپذیر است؛ اما بدون نظارت و اتخاذ تدابیر امنیتی در فضای مجازی، امکان وقوع جرم و تهدید حریم خصوصی کاربران، زمینه‌های بسیار بیشتری خواهد یافت.

حق، آن است که بر پایه عقل سلیم، حریم خصوصی، امری منعطف است و بسته به حالات و اوضاع گوناگون، حدود آن تغییر می‌کند؛ برای نمونه، در زندگی واقعی، در حالت عادی ممکن است شخصی اجاز نزدیک شدن شخص دیگر را به محدوده‌ای از حریم خود ندهد؛ اما برای همین شخص، به هنگام حاضر شدن افراد در مکان‌های شلوغ، این حریم به حداقل ممکن کاهش می‌یابد.

نمونه دیگر که مؤید منعطف بودن حدود حریم شخصی است، تفتیش بدنی به هنگام مراجعه به مکان‌های خاص، مانند: فرودگاه، اماکن مذهبی و یا مکان‌های امنیتی را می‌توان یاد کرد؛ درحالی‌که در حالت عادی، کسی حقّ تفتیش بدنی و وسایل شخص دیگر را ندارد.

در فضای مجازی نیز انعطاف در تعیین مرزها و حدود حریم خصوصی افراد، معنادار است. بنا بر حکم عقلی، نظارت بر فعالیت‌های افراد در فضای مجازی، گاهی به بررسی و رصد محتواهای کاربران منجر می‌شود و این امر اگر بر پایه قانون مدون و اعلام قبلی انجام شود، نه تنها منافی حریم خصوصی یا نقض آن نخواهد بود که به امنیت بیشتر حریم خصوصی کاربران نیز کمک خواهد کرد. ناامن‌شدن فضای مجازی، زمینه را برای تهدیدهای امنیتی مانند: خرابکاری، اخلال امور، ترور، جاسوسی و نظایر آن فراهم می‌سازد.

سخن پایانی

جهان فضای مجازی، همانند جهان واقعی، محلّ تعاملات افراد با یکدیگر است و همان‌گونه‌که جهان واقعی بدون وضع قوانین و مقررات، آشفته و پُرهرج‌ومرج می‌شود که در آن، هیچ امنیتی قابل پیش‌بینی نیست. فضای مجازی نیز نیازمند وضع قوانین و نظارت بر اجرای آن است. همه نخبگان جامعه، اساتید حوزه و دانشگاه، پژوهشگران و متخصصان فضای مجازی، بر این نکته اذعان دارند که فضای مجازی، نیازمند نظارت است؛ همچنان‌که همه جوامع نیز بر فعالیت کاربرانشان در فضای مجازی نظارت دارند.

نگرانی بزرگ کاربران برای نظارت بر فعالیتشان در فضای مجازی، تهدید شدن حریم خصوصیشان است. اینکه کاربری در انجام تعاملاتش در فضای مجازی احساس کند که کسی همواری کارهای او را می‌پاید، سبب احساس ناامنی در او خواهد شد.

یکی از اصلی‌ترین دغدغه‌ها برای حاکمیت‌ها و فعالان فضای مجازی، همین تعارض میان نظارت و فضای مجازی است؛ چالشی که به نظر رفع‌ناشدنی است. هیچ تضمینی وجود ندارد که حریم خصوصی افراد در این فضا نقض نمی‌شود. اطلاعات افشاشده از ارائه‌دهندگان خدمات اینترنتی و صاحبان نرم‌افزارها و شرکت‌های بزرگ در این زمینه، نشان آن دارد که این شرکت‌ها همواره و بدون اطلاع کاربران، دادگان آنها را برداشت می‌کردند و به سازمان‌های دولتی و بین‌المللی می‌فروختند.

مسئله امنیت حریم خصوصی، از مهم‌ترین خواسته‌های کاربران در فضای مجازی است و این امر، به شعار بسیاری از شرکت‌های ارائه‌دهنده خدمات اینترنتی تبدیل شده که با این شعار، به جذب کاربران می‌پردازند.

نظارت بر فضای مجازی در ایران، امری بسیار دشوارتر از دیگر کشورهاست و مسائل بسیاری پیش روی حاکمیت برای نظارت بر فضای مجازی وجود دارد. نخست اینکه قوانینی مدون و مصوب برای بسیاری از مفاهیم حقوقی فضای مجازی، مانند حریم خصوصی و حدود و ثغور آن، تعریف

جرایم فضای مجازی و تعیین مصادیق آن، و تعیین مجازات‌های متناسب با جرم برای آن وجود ندارد. دوم آنکه نهادهای نظارتی گوناگونی در حوزه فضای مجازی وجود دارد؛ اما مشخص نیست که کدام‌یک از آنها متولی قانون‌گذاری و نظارت بر فضای مجازی‌اند.

همین امر، چالش تعارض میان حریم خصوصی و نظارت را بیشتر می‌کند؛ زیرا کاربران نمی‌دانند کدام نهاد نظارتی فعالیت‌هایشان را زیر نظر دارند و یا چندین نهاد و با کارکردهای گوناگون، احتمال دارد نظارت بر محتواهای آنها دسترسی داشته باشند.

بنابراین، گام نخست در حل تعارض میان حریم خصوصی و نظارت فضای مجازی، تعریف و تبیین مفاهیم، قلمروها و چارچوب حریم خصوصی است؛ زیرا به دلیل روشن نبودن قانون و تعریف حریم خصوصی، افراد در برخورد با آن به گونه سلیقه‌ای رفتار خواهد کرد.

در گام بعد، تعیین نهاد ناظر بر فضای مجازی است که برای این کار، باید میان نهادهای نظارتی و اجرایی تفکیک وظایف صورت گیرد. در حال حاضر، نظارت بر انتشار صوت و تصویر فراگیر، بر عهده سازمان صدا و سیما و تعیین مصادیق آن، بر عهده شورای عالی فضای مجازی است. نظارت بر انتشار غیرفراگیر نیز بر عهده اتحادیه کسب‌وکارهای مجازی قرار دارد و این اتحادیه، موظف به صدور مجوز برای فعالیت‌های کاربران در فضای مجازی است. (سرحدی و طاهری، ۱۳۹۹، ص۱۳۹)

در گام‌های بعدی، الزام شرکت‌های خدمات‌دهی به کاربران به اجرای قوانین تأمین‌کننده حریم خصوصی، مانند توافق‌نامه محرمانگی اطلاعات یا قوانین منع نشر محتوا نیز ضروری است.

پس از طی همه این مراحل، تعارض‌های میان حریم خصوصی و نظارت، به میزان بسیاری کاهش خواهد یافت و کاربران فضای مجازی، از نظارت و ایمن‌سازی فضای مجازی استقبال خواهند کرد.■

منابع

۱. احمدی جشفقانی، حسین علی و آرش شوق‌نیان. ۱۳۹۷. «رعایت حریم خصوصی در فضای مجازی؛ مورد مطالعه: حقوق ایران». مدیریت فردا: ۱۳۵ ـ ۱۴۴.

۲. آقابابایی، حسین و مراد عباسی. ۱۳۸۹. «حریم خصوصی، فضای مجازی و چالش‌های پیشگیرانه فراروی ناجا». مطالعات پیشگیری از جرم: ۲۹ ـ ۵۸.

۳. امامی، حسن. ۱۳۸۹. «بررسی ابعاد جرایم اینترنتی». مطالعات بین‌المللی پلیس: ۳۶ ـ ۵۳.

۴. ذولفقاری، یگانه. ۱۴۰۰. «کنترل‌های دولتی بر کاربران اینترنت در جهان؛ حکمرانی فضای مجازی و جهان امروز». پاسدار اسلام: ۴۴ ـ ۴۶.

۵. سرحدی، کاظم و محسن طاهری. ۱۳۹۹. «جستاری در اعمال نظارت مطلوب بر انتشار صوت و تصویر در فضای مجازی از منظر حقوقی». حقوق اداری: ۱۳۹ ـ ۱۶۰.

۶. طالب‌پور، علیرضا، منصور شیدایی و مریم خلیل‌زاده سلماسی. ۱۳۹۳. «مرور و دسته‌بندی راهبرد کشورهای جهان در مواجهه با شبکه‌های اجتماعی مجازی». راهبرد: ۴۳ ـ ۷۲.

۷. عباسیان، کورش، سید علی‌رضا افشانی و حسین اسلامی. ۱۳۹۸. «چالش‌های مرتبط با نقش دولت در فضای مجازی؛ ارائه یک نظریه زمینه‌ای». فصلنامه پرستار و پزشک در رزم: ۸۱ ـ ۹۲.

۸. فتحی، یونس و خیرالله شاه‌مرادی. ۱۳۹۶. «گستره و قلمرو حریم خصوصی در فضای مجازی». مجله حقوقی دادگستری: ۲۲۹ ـ ۲۵۳.