اندیشه‌های حقوق عمومی ——— سال دوازدهم، شماره اول، پیاپی ۲۲، پاییز و زمستان ۱۴۰۱، ص ۶۹ـ۸۰

مسئولیت مدنی دولت در قبال پالایش (فیلترینگ) با نگاهی به حقوق خارجی و اسناد بین‌المللی حقوق بشری

حسین صادقی/ استادیار حقوق خصوصی دانشگاه تهران، تهران، ایران hosadeghi@ut.ac.ir
علیرضا قاسمی/ دانشجوی دکتری تخصصی فقه و حقوق خصوصی، دانشگاه خوارزمی
ar.ghasemi56@jmail.com orcid.org/0009-0005-3589-2592
دریافت: ۱۴۰۰/۰۵/۰۸ ـ پذیرش ۱۴۰۰/۰۸/۰۴

چکیده

دولت با پالایش فضای مجازی باعث به‌وجود آمدن چالش‌هایی در تعاملات اجتماعی کاربران شده است؛ زیرا زندگی اجتماعی و نظام‌های اجتماعی فیزیکی به‌سمت نظام‌های اجتماعی در بستر فضای مجازی منتقل شده است و پالایش نامناسب باعث اختلال در این نظامات می‌شود. حال مسئلهٔ اصلی این مقاله این است که اگر پالایش به ضرر کاربران فضای مجازی منجر شود، آیا دولت‌ها در قبال خسارات وارده مسئولیت مدنی خواهند داشت؟ در راستای پاسخ به سؤال، نگارندگان به این نتیجه رسیده‌اند که اگر سایت یا کانالی که فعالیت‌های قانونی انجام می‌دهد، پالایش شود، جبران خسارت امری مسلم است؛ ولی درصورتی‌که امکان اِعمال پالایش هوشمند وجود نداشته باشد و دولت به‌طور قانونی برای احتراز از یک تهدید امنیتی یا اقتصادی به پالایش غیرهوشمند مبادرت ورزد، دراین‌صورت، اگر زیان‌دیدگان اکثریت جامعه را تشکیل دهند، دولت الزامی به جبران خسارت ندارد؛ اما اگر زیان‌دیدگان تعداد محدود و معینی باشند، دولت ملزم به جبران خسارت است.

کلیدواژه‌ها: دولت، مسئولیت مدنی، ارتباطات الکترونیکی، پالایش، جبران خسارت، اسناد بین‌المللی.

مقدمه

با گسترش اثرگذاری فضای سایبری در امور اجتماعی، دولت‌ها ارادهٔ جدی‌تری برای تمشیت و مهندسی روابط اجتماعی شهروندان در فضای مجازی پیدا کرده‌اند که یکی از مظاهر آن، ایجاد محدودیت در دسترسی کاربران فضای مجازی به‌دلایل فرهنگی، امنیتی، اقتصادی و... است. در جریان این ارتباطات سایبری، ممکن است افعال زیان‌بار، همچون نقض حقوق مالکیت فکری و هتک حرمت اشخاص توسط کاربران خدمات یادشده و به‌واسطهٔ فعالیت و خدمات این‌گونه واسطه‌ها صورت گیرد که موجب طرح ادعاهایی از طرف زیاندیدگان علیه واسطه‌های مزبور شود (صادقی، ۱۳۸۹). فضای سایبر، یک گسترهٔ بدون مرز است که نمی‌توان در برابر آن خطوط مقسّم کشید یا با مرزهای طبیعی و مصنوعی آن را تکه‌تکه و جدا کرد. تفاوتی که بین مرز سایبری با مرز حقیقی وجود دارد، در عدم محدودیت در ترسیم مرز و مداربسته بودن آن است (لملای، ۲۰۰۳، ص ۵۲۷).

نکتهٔ مهم‌تر این است که در حال حاضر، محیط‌های مجازی تعاملی در حال برقراری ارتباط میان شهروندان و دولت‌هاست و به‌ویژه دولت‌های دموکراتیک درصددند با کمک این رسانه‌ها بتوانند طرح «دولتِ باز» را عملیاتی کنند؛ طرحی که از طریق شبکه‌های اجتماعی موجبات دسترسی بیشتر افراد به اطلاعات دولت‌ها و مشارکت در امور کشور را فراهم می‌کند (کلین توا، ۲۰۱۵، ص ۶). به‌عبارت‌دیگر، در راستای ارائهٔ خدمات الکترونیکی دولت در فضای سایبر، ممکن است در نتیجهٔ تقصیر یا خطای دولت و مستخدمین دولتی، زیانی به اشخاص وارد آید که در صورت ایراد خسارت، موضوع مسئولیت مدنی دولت در فضای سایبر مطرح می‌شود. مسئولیت مدنی دولت در فضای سایبر از این جهت اهمیت دارد که ماهیت فضای سایبر با دنیای واقعی متفاوت است و مختصات و اقتضائات خاص خود را دارد (ر.ک: ملکوتی و ساورایی، ۱۳۹۵).

این محدودیت‌ها، خود را در قالب‌های گوناگونی مانند پالایش و مسدودسازی نشان می‌دهد؛ اما گسترهٔ اِعمال محدودیت‌ها تا کجا باید باشد تا زندگی هوشمندِ مبتنی بر فضای مجازی دچار اختلال نشود؛ زیرا زمانی که مردم بسیاری از فعالیت‌های خود را در بستر چنین فضایی انجام می‌دهند، اِعمال پالایش و مسدودسازی، زندگی مردم و تعاملات آنها را دچار اختلال می‌کند و دولت باید با برنامه‌ریزی مناسب، این محدودیت‌ها را به‌صورت گسترده اِعمال نکند تا زندگی مردم که در بستر فضای مجازی است، دچار اختلال نشود (ماده ۳۳ منشور حقوق شهروندی جمهوری اسلامی ایران مصوب ۱۳۹۵). حقوق‌دانان بحث‌های مفصلی در زمینهٔ مسئولیت مدنی دولت در فضای واقعی مطرح کرده‌اند؛ اما این بحث در فضای مجازی بررسی نشده است؛ بنابراین با گسترش روزافزون گسترهٔ فضای مجازی، لازم است قواعد و حدود مسئولیت مدنی دولت در قبال پالایش فضای مجازی مشخص شود.

بنابراین ضروری است با تحلیل قواعد مسئولیت مدنی دولت، محدودهٔ صلاحیت دولت در اِعمال پالایش فضای سایبری مشخص شود تا به‌واسطهٔ پالایش نادرست، ضرر ناروایی به شهروندان وارد نشود و اگر ضرری به شهروندان وارد شد، ضمانت اجرایی برای جبران خسارت‌های واردشده وجود داشته باشد.

۱. مفهوم پالایش (فیلترینگ)

پالایش یا فیلترینگ را در دو معنای عام و خاص به‌کار برده‌اند. در معنای عام، پالایش عبارت است از فناوری‌هایی که از دستیابی به انواع خاص محتوا یا بستهٔ ویژه‌ای از محتوای اینترنتیِ در دسترس جلوگیری به‌عمل می‌آورد؛ اما در تعریف خاص، پالایش عبارت است از جلوگیری از دسترسی به اطلاعات بر مبنای محتوای اطلاعات و نه آدرس سایت. درحقیقت، معنای خاص پالایش، در مقابل مسدود کردن به‌کار می‌رود. طبق این تفکیک، هنگامی که دسترسی به کل یک سایت براساس آدرس آن سایت ممنوع می‌شود، آن سایت مسدود (یا بلاک) شده است و درصورتی‌که بخشی از محتوای آن ممنوع شده باشد، آن سایت پالایش شده است (کرامتی معز و میرخلیلی، ۱۳۹۹).

«پالایش» معادل فارسی فیلترینگ است که در قانون جرائم رایانه‌ای معادل‌سازی شده و عبارت است از محدود ساختن دسترسی کاربران اینترنت به پایگاه ها و خدمات اینترنتی، که براساس ملاحظات فرهنگی و سیاسی یک کشور، دسترسی به آنها برای عموم مردم مناسب نیست (جاویدنیا و همکاران، ۱۳۹۴). فیلتر یا پروکسی، معمولاً به‌عنوان بخشی از «دیوار آتش» سرویس‌دهندگان اینترنت مورد استفاده قرار می‌گیرد و نحوهٔ کار آن بدین صورت است که وقتی کاربر می‌خواهد در یک شبکهٔ محلی به یک سرویس‌دهندهٔ اینترنت دسترسی داشته باشد، یک درخواست از رایانه به سرویس‌دهندهٔ پروکسی می‌فرستد؛ سپس سرویس‌دهندهٔ پروکسی، اطلاعات را از سرویس‌دهندهٔ اینترنت به رایانهٔ درون شبکهٔ داخلی می‌فرستد و به‌صورت دقیق‌تر، پروکسی بسته‌های اطلاعات، یعنی اطلاعاتِ در حال عبور از شبکه را مورد کنترل و بررسی قرار می‌دهد و می‌تواند انتقال بسته‌های مشخص از اینترنت به شبکهٔ داخلی و برعکس را مسدود کند (حسینی‌نژاد و همکاران، ۱۳۹۶).

در قانون جرائم رایانه‌ای مصوب ۱۳۸۸، بدون اینکه تعریفی از فیلترینگ به‌عمل آمده باشد، این واژه با واژهٔ پالایش معادل‌سازی شده است. در مادهٔ ۲۱ قانون جرائم رایانه‌ای (ماده ۷۴۹ کتاب تعزیرات قانون مجازات اسلامی) آمده است: «کمیتهٔ تعیین مصادیق موضوع مادهٔ ذیل محتوای مجرمانه که در چارچوب قانون تنظیم شده است، اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به‌کار می‌رود را پالایش (فیلتر) کنند». بر این مبنا و با توجه به مفهوم اصطلاحی ذکرشده، می توان گفت که مفهوم قانونی «فیلتر» محتوای مجرمانه یا «پالایش»، همان مفهوم اصطلاحی است که به‌طور خلاصه، عبارت است از ایجاد محدودیت در دسترسی کاربران اینترنت به محتوای آن (جاویدنیا، ۱۳۹۸، ص ۲۵ـ۲۶).

پالایش در بسیاری از کشورها انجام می‌شود و محدود به کشوری خاص نیست؛ لیکن کیفیت و کمّیت آن متفاوت است و پدیده‌ای نوظهور در کشورما نیست و ایران را نمی‌توان تنها کشوری دانست که فیلترینگ را اِعمال می‌کند. این پالایش، در اَشکال مختلف انجام می‌شود؛ ازجمله: دستور دولت مبنی بر حذف محتوای غیرقانونی در وب‌سایت‌هایی که در داخل کشور میزبانی می‌شود؛ مسدود کردن محتوای غیرقانونی که در خارج از کشور میزبانی می‌شود؛ و پالایش کردن نتایج توسط موتور جست‌وجو مربوط به محتوای غیرقانونی (بابازاده مقدم و اسلام‌خواه، ۱۳۹۵). به‌طورکلی، علل اصلی اِعمال پالایش عبارت‌اند از: سیاسی، فرهنگی، اخلاقی، اجتماعی، امنیتی و... . شاید هم بتوان همهٔ مصادیق را در

معیار فرهنگی و اخلاقی جای داد؛ زیرا گسترهٔ فرهنگ آن‌قدر وسیع است که می‌تواند مصادیق متنوعی را دربرگیرد و پالایش غالباً به‌دلایل فرهنگی و ملاحظات مذهبی انجام می‌شود (پورنقی و همکاران، ۱۳۹۸).

۲. مفهوم حکمرانی فضای مجازی توسط دولت‌ها

ماهیت فضای مجازی با معماری و ساختار غیرمتمرکز آن، نحوهٔ اِعمال حکمرانی بر این فضا را به موضوعی پیچیده بدل کرده است. این پیچیدگی را می توان از این جهت بررسی کرد که اولاً ماهیت فضای مجازی ماهیتی جهانی است و کلیت آن نمی‌تواند توسط دولت‌های ملی حکمرانی شود؛ زیرا دولت‌های ملی در گسترهٔ سرزمینی و محدودهٔ مرزهای ملی خود دارای صلاحیت اِعمال حکمرانی‌اند؛ ثانیاً تحقق موفقیت در فضای مجازی نیازمند همکاری و مشارکت فعالانه و حداکثری ذی نفعان بخش دولتی، بخش خصوصی و نهادهای مدنی در سراسر دنیاست. این ذی‌نفعان شامل مالکان، متصدیان شبکه‌ها و خدمات سراسر دنیا، ثبت‌کنندگان نام‌های دامنه، سازمان‌های منطقه‌ای تخصیص آدرس‌های آی‌پی سازمان‌های استاندارد، مجریان و متصدیان خدمات اینترنتی، و کاربران اینترنت است.

حکمرانی فضای مجازی را می توان نحوهٔ ایجاد ارزش ها، هنجارها و استانداردهای رسمی و غیررسمی برای رفتار دولت و بازیگران غیردولتی (بخش خصوصی و نهادهای مدنی) در نسبت با فضای مجازی دانست. ایجاد سازوکارهای قانونی بهتر برای رسیدگی و مقابله با جرائم سایبری بین المللی، قواعد شفاف ملی برای اجرای قانون، و طراحی نظام حفاظتی یکپارچهٔ داده‌ها، ازجمله نتایج حکمرانی فضای سایبر است (فیروزآبادی، ۱۳۹۹، ص ۴۴).

فضای مجازی در زمان حاضر در تمامی ابعاد زندگی فردی و اجتماعی مردم جهان نفوذ کرده و در حال ایجاد یک تمدن جدید بشری است که از تمدن های قبل به مراتب فراگیرتر است. بدون شک، حکمرانی چنین فضایی که ازیک‌سو با تسهیل ارتباط و ارائهٔ فناوری ها و خدمات جدید و شگفت‌آور ضریب نفوذ بسیار بالایی دارد و بسیار سریع‌تر از فرهنگ غرب در حال هضم کردن کاربران، یعنی مردم خود است و ازسوی‌دیگر با قابلیت‌های خود در حال تبدیل کردن حاکمیت ملی، به یک حاکمیت شبکه‌ای، شرکتی فرامرزی است، که امری بسیار پیچیده و خطیر است. این مسئله، بیش از دیگر کشورها، برای جمهوری اسلامی ایران یک تهدید شمرده می‌شود؛ زیرا این کشور همواره در معرض تهدیدات دشمن خود، به‌ویژه جریان صهیونیسم قرار دارد و بیشتر شرکت‌های بزرگ و صاحب‌نفوذ در فضای مجازی تحت سلطهٔ این جریان قرار دارند.

شیوهٔ حکمرانی در کشور ما در حوزهٔ فضای مجازی، از رویکردی غیرمشارکتی، سلسله‌مراتبی و بالا به پایین پیروی می کند و فاصلهٔ زیادی با حکمرانی مطلوب دارد. در شیوهٔ کنونی، ذی‌ربطان غیردولتی و غیرحاکمیتی نقشی رسمی در تدوین، ابلاغ و ارزیابی سیاست‌ها، مقررات و قوانین ندارند؛ اما از آنها انتظار می‌رود که از تصمیمات اتخاذشده پیروی کنند؛ به‌عبارت‌دیگر، آنها تنها نقشی منفعلانه به هنگام اجرای سیاست‌ها و قوانین دارند. درعین‌حال ذی‌ربطان قدرتمند به‌صورت غیررسمی و غیرشفاف بر تصمیم‌گیری‌ها تأثیر می‌گذارند (فیروزآبادی، ۱۳۹۹، ص ۸۸).

۳. سیاست‌های دولت‌ها در قبال پالایش در حقوق خارجی و اسناد حقوق بشری

برخی دولت‌ها سانسور اینترنت را در مورد موضوعاتی که تصور می‌کنند نامناسب است، خود بر عهده می‌گیرند. برای مثال، در چین، عربستان سعودی، سنگاپور، امارات متحدهٔ عربی، ایران و ویتنام، دولت به صورت متمرکز و کلان، محتواهایی را که مخلّ قوانین کشورند سانسور می کند. برخی از این کشورها ارائه دهندگان خدمات اینترنتی را به مسدود کردن موارد موردنظر ملزم می‌کنند و برخی دیگر نیز دسترسی محدودی را تحت نظارت دولت در اختیار کاربران قرار می‌دهند (عاملی، ۱۳۹۰، ص ۳۶۴).

سامان‌دهی اینترنت در آمریکا بیشتر به شکل خودتنظیم و بدون دخالت دولت صورت می‌گیرد؛ اما برخی سازوکارهای سامان دهی مشترک با دولت نیز برای تضمین امنیت (برای مثال، در مبارزه با تروریسم)، حقوق ویژه (برای مثال، در مبارزه با سوءاستفاده های جنسی از کودکان) و حمایت از منافع اقتصادی ویژه (برای مثال، حمایت از حقوق پدیدآورندگان آثار) استفاده می‌شود. با وجود این، در الگوی آمریکایی، سامان‌دهی مشترک جنبهٔ استثنایی دارد و برای نیل به اهداف بسیار خاص مربوط به موضوع‌های معین استفاده می‌شود. درحالی‌که به‌نظر می‌رسد در اروپا، سامان‌دهی مشترک الگوی کلی و پیشرو در سامان‌دهی محتوای اینترنت است (فریدمن و جلو کویچ، ۱۳۸۷).

سانسور اینترنت در انگلستان، الگوهای متفاوتی را دربرمی‌گیرد. این الگوها شامل مسدود کردن دسترسی به سایت‌ها، و مقررات کیفی مربوط به انتشار یا مالکیت موارد خاص است؛ همچون مسئولیت نقض حق مؤلف، تحریک به عملیات تروریستی، و هرزه‌نگاری کودکان است (احمدوند، ۱۳۹۵، ص ۱۷۳).

در ژوئن سال ۲۰۰۹م، دولت آلمان قانونی را برای پالایش کردن وب‌سایت‌های پورنوگرافی تصویب کرد و بجز آلمان و ایتالیا که از پالایش اجباری برای وب‌سایت‌هایی با امثال این نوع محتوا استفاده می کنند، کشورهای اروپایی دیگر نظیر سوئد، نروژ، دانمارک، فنلاند و ایرلند، راهبرد پالایش داوطلبانه را در پیش گرفته‌اند. راهبرد آگاه‌سازی و آموزش نیز راهبردی پرطرفدار و تأکیدشده و فعال در اتحادیهٔ اروپاست که برای بالا بردن سطح آگاهی‌ها، توانمندسازی کاربران از طریق ابزارها و فناوری‌ها و پاسخ‌دهی به رفتار یا محتوای غیرقانونی، از آن استفاده می‌شود (روگو، ۲۰۰۹، ص ۷۲).

کارگروه رسانه و ارتباطات استرالیا، مسئول هدایت و ایجاد فناوری های پالایش اینترنتی و دیگر ابتکارات به‌منظور حفاظت از مشتریان است. این کارگروه که هرساله گزارشی در این زمینه منتشر می کند، در حال تحقیق برای دستیابی به فناوری شبکهٔ اجتماعی است تا پاسخ گویی و مشارکت ذی نفعان را در دولت افزایش دهد. این کارگروه، سازوکاری به‌نام هاتلاین طراحی کرده است که طی آن می‌توان محتوای ممنوع را به نمایندگی‌های قانونی گزارش کرد (اکبرزاده، ۱۳۹۷، ص ۹۱).

پالایش محتوای آنلاین به شکل‌های مختلفی در میان کشورهای اروپایی انجام می‌شود. برخی موارد عبارت‌اند از: دستور صادرشده توسط دولت‌ها به ارائه‌دهندگان خدمات اینترنت برای حذف وب‌سایت‌هایی که شامل مطالب غیرقانونی‌اند (زمانی که در داخل کشور میزبانی شده باشند)؛ دستورهای مسدودسازی توسط مقامات اجرایی برای

محتوای غیرقانونی میزبانی‌شده در خارج از کشور؛ و پالایش نتایج مربوط به محتوای غیرقانونی توسط موتورهای جست‌وجو که به‌عنوان یک شکل از خودکنترلی در نظر گرفته می‌شود. هرچند برخی از موارد و شکل‌های پالایش توسط موتورهای جست‌وجو و ارائه‌دهندگان خدمات اینترنت در تعدادی از کشورها اغلب به‌عنوان «خودکنترلی داوطلبانه» نام برده می‌شود، به‌نظر می‌رسد که این اقدام داوطلبانه مبتنی بر این درک ضمنی است که همکاری با دستورهای دولتی، از عواقب قانونی بعدی ممانعت خواهد کرد (بابازاده مقدم و اسلام‌خواه، ۱۳۹۵).

ارزش خدمت عمومی اینترنت و وظایفی که برای دولت‌ها در پی می‌آورد، به طور مشترک با چند سال فاصله، به‌ترتیب در محافلی نظیر یونسکو، اجلاس جهانی سران و شورای اروپا مطرح و شناخته شد. وظایف خدمت عمومی، ازجمله در متن اعلامیهٔ اصول ژنو ـ تصویب‌شده در اولین مرحلهٔ اجلاس یادشده در سال ۲۰۰۳م ـ پیش‌بینی شده است.

مفهوم آزادی اینترنتی، چند سال بعد در سال ۲۰۱۶م توسط شورای اروپا طی توصیه‌نامه‌ای به دولت‌های عضو پیشنهاد شد و وظایف و مسئولیت دولت‌ها باز هم به‌صورت منسجم‌تر پیش‌بینی شدند. با گذر زمان مشخص شد که بعضی دولت‌ها تمایل روزافزون به محدود کردن اینترنت دارند و نه‌تنها در پی تقویت حقوق کاربران نیستند، بلکه با ترفندهای گوناگون به سانسور و نظارت و... مبادرت می‌کنند.

مفهوم «آزادی اینترنت»، به‌مثابه برخورداری از حقوق بشر و آزادی‌های بنیادی و حمایت از آنها در فضای اینترنتی است و حقوق و مسئولیت دولت‌ها در این زمینه خاطرنشان شده است. به‌موجب مصوبهٔ فوق، دولت‌ها نه‌تنها نباید به حقوق بشر و آزادی‌های بنیادی افراد در اینترنت خدشه وارد کنند، بلکه ملزم شده‌اند شرایط را برای شکل دادن به یک فضای مطلوب برای آزادی اینترنت، فراهم سازند (معتمدنژاد، ۱۳۹۷).

از طرفی، میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی نیز ـ که یکی دیگر از اسناد مهم حقوق بشری است ـ در مادهٔ ۶ بر ضرورت شناسایی حقِ داشتن کسب‌وکار و انتخاب آزاد کسب‌وکار تأکید می‌کند: «کشورهای طرف این میثاق، حق کار کردن را که شامل حق هرکس است به اینکه فرصت یابد به‌وسیلهٔ کاری که آزادانه انتخاب یا قبول می‌کند، معاش خود را تأمین کند، به‌رسمیت می‌شناسند و اقدامات مقتضی را برای حفظ این حق معمول خواهند داشت...».

بنابراین انجام پالایش در مواردی که موجب سلب فعالیت کسب‌وکار اشخاص باشد، مغایر با این اصل مهم حقوق بشری و سند بین‌المللی است.

٤. فروض متصور مسئولیت مدنی دولت در قبال پالایش

دسترسی و ارائهٔ اینترنت در کشور ما، طبق مقررات، بر عهده و در انحصار دولت است؛ بااین‌حال دولت به اشخاص حقیقی و حقوقیِ خصوصی، نمایندگی ارائهٔ خدمات دسترسی اینترنت برای شهروندان و مصرف‌کنندگان عادی (کاربران) را می‌دهد و سایر نهادهایی که تحت عناوین مختلف مشغول به ارائهٔ خدمات

اینترنتی هستند، همگی در طول دولت‌اند و بدون اجازهٔ دولت، هیچ نهاد خصوصی یا عمومی قادر به ایجاد و ارائهٔ خدمات دسترسی به اینترنت نیست.

با توجه به پیوستگی فضای مجازی در جهان، از هر دولتی انتظار می‌رود که با ایمن‌سازی و نظارت قانونی و مستمر بر شبکهٔ اینترنت و دنیای مجازی، امکان تحقق افعال زیان‌بار را به حداقل برسانند؛ که البته قسمتی از این هدف، از طریق وضع قوانین ملی مناسب، و بخشی دیگر به‌وسیلهٔ آموزش مناسب شهروندان در جهت استفادهٔ بهتر و مناسب‌تر از فضای مجازی امکان‌پذیر خواهد بود. در کشور ما، تصویب قانون جرایم رایانه‌ای یا تأسیس شورای عالی فضای مجازی، که در سال ۱۳۹۰ به فرمان رهبری تشکیل شد، ازجمله اقدامات در راستای اعمال این وظیفه است.

بر این اساس اگر دولت به‌عنوان ایجادکنندهٔ نقطهٔ تماس بین‌المللی که در انحصار خودش است، در اجرای وظایف حاکمیتی خود در این فضای مجازی موجب ورود زیان به شهروندان شود، چنانچه اقدام دولت برای منافع عموم باشد، شامل معافیت مادهٔ ۱۱ قانون مسئولیت مدنی می‌شود؛ ولی اگر این اقدام دولت درنتیجهٔ اجرای غلط وظایف حاکمیتی خود باشد، مثلاً اگر شرکت مخابرات به‌عنوان ارائه‌دهندهٔ کلی خدمات دسترسی به اینترنت، به حریم خصوصی کاربران در فضای مجازی دست‌اندازی کرده، اطلاعات و اقدامات ایشان را در این فضا رصد کند، ازآنجاکه این اقدامات مغایر با وظایف دولت است، ارتکاب این اقدام زیان‌بار از سوی هریک از نهادهای دولتی موجب مسئولیت آنها خواهد بود و نباید آنها را مشمول معافیت بند پایانی مادهٔ ۱۱ قانون مسئولیت مدنی دانست که مقرر کرده است: «... ولی در مورد اِعمال حاکمیت دولت، هرگاه اقداماتی که برحسب ضرورت برای تأمین منافع اجتماعی طبق قانون به‌عمل آید و موجب ضرر دیگری شود، دولت مجبور به پرداخت خسارات نخواهد بود».

به‌نظر می‌رسد که این معافیت از مسئولیت مدنی دولت، ناشی از اِعمال حاکمیتی است که موافق اهداف دولت و برای منافع ملت باشد؛ برای مثال، دولت به‌منظور دفع حملات سایبری به تأسیسات کشور، مجبور به قطع ناگهانی اینترنت شود و در نتیجهٔ این امر، به شهروندان خسارت وارد کند؛ اما اگر در اجرای غلط یا به‌بهانهٔ اجرای وظایف حاکمیتی خسارتی به‌بار آید، در این حالت، شکی در تحقق مسئولیت مدنی دولت نخواهد بود و دولت به‌عنوان زیان‌زننده، مسئول خسارت تلقی می‌شود. بنابراین در این مورد، مسئولیت مدنی دولت محرز است و صرف اثبات انتساب زیان به فعل دولت، برای تحقق مسئولیت او کافی خواهد بود (ملکوتی، ۱۳۹۵، ص ۱۷۷).

قواعد مسئولیت مدنی نیز برای انتظام و تعادل بخشیدن به منافع متعارض اشخاص، مورد قبول شارعان و واضعان قرار گرفته است. بنابراین، اگر هدف اساسی قواعدِ مبتنی بر مسئولیت را جبران خسارات نامتعارف زیان‌دیده و جلوگیری از ورود این‌گونه خسارات قلمداد کنیم، این قواعد در ابتدا باید در خصوص کارگزاران کشور و شخصیت حقوقی دولت، که در مواردی ممکن است به‌ناحق و نابجا موجبات ورود ضرر در فضای سایبری به اشخاص شوند،

اِعمال گردد تا ازیک‌سو با مشاهدهٔ اِعمال قواعد مسئولیت مدنی در فضای سایبر دربارهٔ شخصیت‌های درجهٔ اول کشور و همچنین مسئولیت دولت، فرهنگ احترام به حقوق مادی و معنوی در فضای مجازی در میان عموم مردم نهادینه شود؛ و ازسوی‌دیگر، امنیت اشخاص موجب استمرار و سرمایه‌گذاری بیشتر و مطمئن‌تر در فضای سایبری می‌شود که عواید آن، اشتغال، امنیت اقتصادی، رونق داخلی و آرامش بیشتر مردم را در پی خواهد داشت. به این جهت امروزه نظریهٔ تقصیر در نظام‌های حقوقی جهان، اعم از کامن‌لا، رومی ژرمنی و حقوق اسلام، به‌عنوان یک اصل در برقراری مسئولیت مدنی پذیرفته شده است؛ لذا اصولاً در مواردی شخص مسئول قلمداد می‌شود که مرتکب یک تقصیر شده باشد (برای اطلاعات بیشتر در زمینه مسئولیت مبتنی بر تقصیر در ارتباطات الکترونیکی، ر.ک: صادقی، ۱۳۹۶، ص ۲۸۹ـ۲۹۲؛ همچنین، ر.ک: میری، ۱۳۹۴، ص ۵۶ـ۶۱). باید دید که آیا این اصل در مسئولیت مدنی دولت در فضای سایبری نیز پذیرفته شده است؟

حوزهٔ اقتصادی زندگی مردم که در بستر فضای سایبر گسترش یافته است نیز اگر با پالایش نامناسب دچار اختلال شود (مانند پالایش شبکهٔ اجتماعی تلگرام در دی ماه سال ۱۳۹۶ و پالایش سرورهای خارجی فضای مجازی در آبان ماه سال ۱۳۹۸، که بخشی از آن ماهیت اقتصادی و تجارتی پیدا کرده بود)، باعث به‌وجود آمدن چالش‌هایی در زندگی مردم گردید. ازاین‌رو در خصوص مسئولیت مدنی دولت در قبال پالایش فضای مجازی، چند حالت متصور است که مسئولیت یا عدم مسئولیت دولت در هریک از این حالات بررسی می‌شود:

۱ـ۴. امکان اِعمال پالایش هوشمند وجود داشته باشد

متخصصان معتقدند که پالایش هوشمند شبکه‌های اجتماعی، با توجه به رمزنگاری شدن آنها امری غیرممکن است. شاخهٔ مهندسی برق، کامپیوتر و فناوری اطلاعات بسیج دانشجویی دانشگاه‌های تهران، در گزارشی تخصصی، پالایش شبکه‌های اجتماعی را غیرممکن می‌داند. همچنین طبق گزارش بنیاد حریم الکترونیکی (FFE)، بیشتر شبکه‌های اجتماعی همچون تلگرام، اینستاگرام، فیس‌بوک، گوگل و...، ارتباطات خود را رمزنگاری می‌کنند؛ بنابراین امکان پالایش هوشمند آنها ممکن نیست (پورنقی و همکاران، ۱۳۹۸).

در حال حاضر، پالایش هوشمند شبکه‌های اجتماعی، به‌رغم تلاش‌های صورت‌گرفته، نتیجه‌ای در پی نداشته است و همچنان در هاله‌ای از ابهام قرار دارد؛ اما در مواردی که امکان اِعمال پالایش هوشمند وجود داشته باشد، دولت نباید بدون دلیل موجه به پالایش غیرهوشمند اقدام کند. در صورت اعمال پالایش غیرهوشمند یا اعمال پالایش هوشمند بدون دلیل موجه، دولت به طور قطع ملزم به جبران خسارت زیان دیدگان می‌باشد زیرا این حالت، داخل در عموم قاعدهٔ لاضرر است و مشمول مخصص این قاعده در مسئولیت مدنی دولت نیست.

اما اگر دولت با وجود امکان اِعمال پالایش هوشمند، به پالایش غیرهوشمند مبادرت ورزد و برای این کار دلیل موجه داشته باشد، مثلاً چنانچه با اِعمال پالایش هوشمند خطری که امنیت، اقتصاد، فرهنگ و اجتماع را تهدید

می‌کند، از بین نرود، عمل دولت در پالایش غیرهوشمند جواز قانونی دارد و تقصیر و قصوری رخ نداده است؛ و باید بین فرضی که زیان‌دیدگان اکثریت جامعه را تشکیل می‌دهند و فرضی که زیان‌دیدگان خاص و محدودند، تفاوت قائل شد. در فرضی که زیان‌دیدگان اکثریت جامعه را تشکیل می‌دهند، دولت مجبور به جبران خسارت نیست؛ زیرا این حالت بر مبنای جواز دولت در دفع خطر مهم تر قابل توجیه است؛ و در فرضی که زیان‌دیدگان محدودند، جبران خسارت امری الزامی است و داخل در عموم قاعدهٔ لاضرر است.

چنانچه امکان اعمال پالایش هوشمند وجود داشته باشد و دولت، تنها سایت، کانال یا گروهی را که آسیب اجتماعی، امنیتی یا اقتصادی به کشور وارد می‌کند، پالایش کند، به‌دلیل نامشروع بودن موضوع فعالیت، جبران خسارت منتفی است؛ ولی اگر سایت، کانال یا گروهی که فعالیت‌های قانونی و مشروع انجام می‌دهد، پالایش شود، جبران خسارت بر اساس قاعده «لاضرر» و نظریه «تقصیر» می‌باشد.

۲ـ۴. امکان اِعمال پالایش هوشمند وجود نداشته باشد

در حال حاضر در کشور ایران، امکان اعمال پالایش هوشمند در بیشتر موارد وجود ندارد؛ همانند شبکه‌های اجتماعی که رمزنگاری شده‌اند و پالایش هوشمند آنها ممکن نیست. در مواردی که امکان اعمال پالایش هوشمند وجود ندارد، چنانچه عمل دولت در اعمال پالایش غیرهوشمند برای احتراز از یک آسیب امنیتی، اجتماعی یا اقتصادی باشد و زیان‌دیدگان محدود باشند، جبران خسارت امری مسلم است؛ زیرا این فرض داخل در عموم قاعدهٔ لاضرر است؛ و چنانچه زیان‌دیدگان اکثریت جامعه را تشکیل دهند، دولت ملزم به جبران خسارت نیست؛ زیرا این حالت، بر پایه نظریه اعمال حاکمیت و احتراز از خسارت مهم تر موجب عدم مسئولیت دولت است؛ اما اگر دولت بدون دلیل موجه اقدام به پالایش غیرهوشمند کند، به‌دلیل آنکه در زمینهٔ اعمال پالایش رخ داده است، ملزم به جبران خساراتی است که به‌سبب پالایش غیرهوشمند به شهروندان وارد شده است؛ چه زیان‌دیدگان خاص باشند و چه اکثریت جامعه متضرر شوند (پورنقی و همکاران، ۱۳۹۸)؛ زیرا این حالت، داخل در عموم قاعدهٔ لاضرر است، هرچند که در فرض محدود نبودن زیان دیدگان دولت با محدودیت بودجه مواجه خواهد شد. با این اوصاف، امکان یا عدم امکان پالایش هوشمند، در مسئولیت مدنی دولت تأثیرگذار است.

نتیجه‌گیری

پیدایش فضای سایبری و داشتن ویژگی‌های منحصربه‌فردی همچون ناملموس بودن این فضا، باعث شده است که این محیط، خطرسازتر از محیط حقیقی باشد؛ همچنین، ویژگی هویت پنهان و دروغین فعالان این حوزه، که عامل رجوع کاربران اینترنت به واسطه‌های اینترنتی شده است، درواقع واسطه‌های اینترنتی امکان دسترسی کاربران را به این شبکه فراهم می‌کنند یا بعد از اتصال، امکاناتی را به کاربران خود ارائه می‌دهند؛ بنابراین اشخاص برای اتصال

به اینترنت از واسطه‌های اینترنتی، استفاده می‌کنند. لذا اهمیت جایگاه این واسطه‌های اینترنتی بسیار زیاد است؛ زیرا بدون آنها اصولاً برقراری ارتباط در فضای سایبری ممکن نخواهد بود.

امروزه، چه دولت را در کنار ملت بدانیم، چه در مقابل آنان، با توسعهٔ حوزهٔ عمل دولت‌ها، شاهد گستردگی تصمیمات و اقدامات آنها هستیم. این تصمیمات و اقدامات می‌تواند در عین راه‌گشایی در انجام مأموریت‌های دولت‌ها و فراهم کردن زمینه‌های پیشرفت و تعالی کشور و آحاد ملت، موجب ورود زیان و خسارت برای برخی از مردم شود و به مسئلهٔ مسئولیت مدنی دولت منتهی گردد.

کاربرد فناوری اطلاعات و ارتباطات جهت ارائهٔ خدمات دولتی به جامعه، که از آن تحت عنوان «دولت الکترونیک» نام می‌برند، ابتکار عمل جدیدی است که قصد دارد زمینهٔ دسترسی آسان‌تر و مطلوب‌تر شهروندان به خدمات عمومی را از طریق رسانه‌های الکترونیک فراهم کند و روابط مدیریت دولتی و شهروندان را به‌گونه‌ای جدید پی‌ریزی نماید. ازجمله راهکارهای ارتقای کارایی دولت، پیاده‌سازی و استقرار سیستم‌هایی است که به‌طور خلاصه با عنوان دولت الکترونیک شناخته می‌شوند. درواقع، دولت الکترونیک یکی از پدیده‌های مهم حاصل از به‌کارگیری فناوری اطلاعات و ارتباطات است که تحولات عمیقی را در شیوهٔ زندگی بشر امروزی ایجاد کرده است.

تردیدی نیست که پیدایش و گسترش روزافزون ابزارهای جدید ارتباطات و اطلاعات، ازجمله رایانه‌ها، تلفن های همراه و درنهایت، تولد فضای سایبر و به طور خاص اینترنت، که امکان مبادلات از راه دور و در محیط‌های الکترونیکی را بیش‌ازپیش در اَشکال گوناگون فراهم ساخته، به‌تبع اثرگذاری در مناسبات اقتصادی و اجتماعی، برخی از قواعد حقوق سنتی را نیز با چالش روبه‌رو کرده است؛ چراکه «حقوق» در مفهوم کلی، قواعد تنظیم مناسبات اجتماعی است. اگرچه ماهیت ارتباطات در فضای سایبری نسبت‌به جهان واقعی، به‌علت اقتضائات متفاوت هر دو فضا تغییر یافته است، اما این فناوری توان تغییر کلی ماهیت روابط و وضعیت‌های حقوقی حاکم بر این ارتباطات را نداشته و ندارد و قدر مسلم، انطباق آنها با محیط‌های الکترونیک و مجازی را ضروری می‌کند؛ چون فضای سایبر با توجه به مقتضای خود، رفتارها و اشخاص جدید را وارد قلمرو حقوق می کند و در کنار سایر مناسبات حقوقی، مسائل گوناگون حقوقی فعالان پرشمار این عرصه را مطرح می‌سازد. ازجمله شایع‌ترین و مهم‌ترین مسائل حقوقی فضای سایبر، مسئولیت مدنی دولت در فضای سایبر است که مسئلهٔ پالایش آن، در این مقاله مورد واکاوی و ارزیابی قرار گرفته است.

در جریان این ارتباطات سایبری، ممکن است افعال زیان‌باری نظیر نقض قانون و نقض اصول اخلاق سایبری صورت گیرد که موجب طرح ادعاهایی از طرف زیان‌دیدگان علیه دولت شود. به‌عبارت‌دیگر در راستای ارائهٔ خدمات الکترونیکی دولت در فضای سایبر، ممکن است در نتیجهٔ تقصیر یا خطای دولت و مستخدمین دولتی، زیانی به اشخاص وارد شود که درصورت ایراد خسارت، موضوع مسئولیت مدنی دولت در فضای سایبر مطرح می‌شود.

مسئولیت مدنی دولت در فضای سایبر، از این جهت اهمیت دارد که ماهیت فضای سایبر با دنیای واقعی متفاوت است و مختصات و اقتضائات خاص خود را دارد.

درصورتی‌که امکان اعمال پالایش هوشمند وجود داشته باشد و دولت تنها سایت، کانال یا گروهی را که آسیب اجتماعی، امنیتی یا اقتصادی به کشور وارد می‌کند، پالایش کند، به‌دلیل نامشروع بودن موضوع فعالیت، جبران خسارت منتفی است؛ ولی اگر سایت، کانال یا گروهی که فعالیت‌های قانونی و مشروع انجام می‌دهد، فیلتر شود، جبران خسارت امری مسلم است؛ اما چنانچه امکان اعمال فیلترینگ هوشمند وجود نداشته باشد و دولت به‌طور مشروع و قانونی برای احتراز از یک تهدید امنیتی، فرهنگی، اقتصادی یا اجتماعی به پالایش غیرهوشمند مبادرت ورزد، اگر زیان‌دیدگان اکثریت جامعه را تشکیل دهند، دولت به جهت محدودیت بودجه و اعمال حاکمیت الزامی به جبران خسارت ندارد؛ اما اگر زیان‌دیدگان تعداد محدود و معینی باشند، دولت ملزم به جبران خسارت است.

پیشنهادها

۱. فناوری ارتباطی و اطلاعات، بسان فناوری‌های دیگر که با انگیزهٔ خدمت و رفاه بشری پدید آمده است و گسترش می‌یابد، اثر دوگانه دارد: هم می‌تواند مطلوب جامعهٔ بشری واقع شود و هم می‌تواند دارای جنبه‌های منفی و تهدیدکنندهٔ حقوق بشری باشد که حقوق افراد جامعه را تحت تأثیر قرار می‌دهد. ازآنجاکه دامنهٔ استفاده از فضای سایبر محدود به جغرافیای خاصی نیست، درصورت عدم سامان‌دهی و استفادهٔ ناصحیح از آن، ممکن است بر حقوق شهروندان جامعهٔ جهانی از جنبه‌های مختلف اثر گذارد و موجب نقض حقوق شهروندی آنان، به‌ویژه حق بر حریم خصوصی شود که شدیداً متأثر از فناوری است. بنابراین، سامان‌دهی این فضا نیازمند سازوکارهای تقنینی و مقرراتی صحیح متناسب با مقتضیات آن فضا خواهد بود. حتی آن دسته از قوانینی که برای صیانت از حقوق بنیادی بشری وضع شده و لازم‌الاجرایند نیز شاید نیازمند بازنگری و بازآفرینی بر پایهٔ اندیشه‌های نوآورانه و سازگار با دنیای نوین باشند و دولت باید با پیش‌بینی سازوکارهای کارآمدهمچون بیمه مسئولیت در فضای سایبر، از حقوق اساسی شهروندان خود در برابر تهدیدها و آسیب‌های ناشی از بسط و توسعهٔ فناوری صیانت به‌عمل آورد.

۲. تشکیل کمیتهٔ صیانت از حریم خصوصی شهروندان در فضای سایبر، متشکل از حقوق‌دانان زبده (نمایندگان قوهٔ قضاییه)، کارشناسان فنی و حقوقی (نمایندگان سازمان تنظیم مقررات و ارتباطات رادیویی)، نمایندهٔ شورای عالی امنیت ملی، نمایندهٔ شورای عالی فضای مجازی و نمایندهٔ اپراتورها.

۳. افزایش مسئولیت‌های دولت در تمامی سطوح (فراهم کردن، ایجاد کردن، حمایت کردن و ارتقای نهادهای دولتی و همهٔ بخش‌های جامعهٔ مدنی به‌صورت یک شخصیت واحد) به‌منظور ایفای نقش در حفظ حقوق شهروندان در فضای سایبر.

منابع

احمدوند، بهناز، ۱۳۹۵، ***جایگاه دولت در نظام جامع رسانه‌های همگانی***، تهران، خرسندی.

اکبرزاده، علیرضا، ۱۳۹۷، ***مخاطب محوری در مواجهه با شبکه‌های اجتماعی***، چ چهارم، اصفهان، سیمای فلق.

بابازاده مقدم، حامد و عمار اسلام‌خواه، ۱۳۹۵، «پالایش (فیلترینگ) اینترنت در اروپا»، ***علوم خبری***، ش ۱۷،ص ۱۳۷-۱۵۶.

پورنقی، سالار و همکاران، ۱۳۹۸، «مسئولیت مدنی دولت در قبال فیلترینگ (پالایش) فضای مجازی»، ***حقوق و فناوری اطلاعات***، سال اول، ش ۱، ص ۱۰۴-۱۴۴.

جاویدنیا، جواد و همکاران، ۱۳۹۴، «واکاوی سیاست‌های پالایش محتوای مجرمانه (فیلترینگ) از منظر فقهی»، ***دین و ارتباطات***، سال بیست و دوم، ش ۲، ص ۳۵-۶۱

جاویدنیا، جواد، ۱۳۹۸، ***واکاوی پالایش محتوا (فیلترینگ) از منظر فقهی و حقوقی***، تهران، خرسندی.

حسینی‌نژاد، سیدمجتبی و همکاران، ۱۳۹۶، «تحلیل و بررسی فقهی اجرای فیلترینگ در فضای مجازی»، ***حکومت اسلامی***، ش ۸۴ ص ۲۷-۵۶.

صادقی، حسین، ۱۳۸۹، «مسئولیت مدنی واسطه‌ها و تأمین‌کنندگان خدمات ارتباطات الکترونیک»، ***مطالعات حقوق خصوصی***، دوره چهلم، ش ۲، ص ۱۹۹-۲۱۸.

ـــــ ، ۱۳۹۶، ***مسئولیت مدنی در ارتباطات الکترونیکی***، چ دوم، تهران، میزان.

فریدمن، ال، هن بل و جلو کویچ، ۱۳۸۷، «راهبردهای دولتی برای ساماندهی مشترک اینترنت در امریکا، اروپا و چین»، ترجمهٔ محمدعلی نوری و فائزه عامری، ***اطلاع‌رسانی حقوقی***، سال ششم، ش ۱۴، ص ۱۷۳-۱۸۹.

فیروزآبادی، ابوالحسن، ۱۳۹۹، ***درآمدی بر حکمرانی فضای مجازی***، تهران، دانشگاه امام صادق﵇ و مرکز ملی فضای مجازی.

کرامتی معز، هادی و سیدمحمود میرخلیلی، ۱۳۹۹، «نقد سیاست‌های پالایش (فیلترینگ) در پیشگیری از بزه‌دیدگی نوجوانان در شبکه‌های اجتماعی مجازی به‌عنوان محیطی نوین از جغرافیای انسانی»، ***نگرش‌های نوین در جغرافیای انسانی***، سال دوازدهم، ش ۲، ص ۷۵-۹۶.

عاملی، سیدسعیدرضا، ۱۳۹۶، ***نظریه‌ها و مفاهیم اساسی دولت الکترونیک***، تهران، امیرکبیر.

معتمدنژاد، رؤیا، ۱۳۹۷، «وظایف دولت‌ها در عرصه تکنولوژی‌های دیجیتال از دولت انحصارطلب تا دولت رگولاتور»، ***علوم خبری***، ش ۲۸، ص ۹-۳۶.

ملکوتی، رسول، ۱۳۹۵، ***مسئولیت مدنی در فضای سایبر***، تهران، مجمع علمی و فرهنگی مجد.

میری، حمید، ۱۳۹۴، ***مسئولیت مدنی ارائه‌کنندگان خدمات اینترنتی***، تهران، مؤسسهٔ مطالعات و پژوهش‌های حقوقی.

Clintova, Maria, 2015, "Open Government Policy In Canada: Will Social Media Change Interaction Between Government And Citizens?", ***presented at the International Conference on Public Policy***, Milan, Italy, Catholic University of Sacro Cuore.

Lemley, mark, 2003, "place and cyberspace", ***California Law Review***, V. 91, Issue 2, Article 5, p 521-542.

Rogow, Faith, 2009, "Teaching Media Literacy in Less Than an Hour", ***Journal of Media Literacy Education***, N.1, p.72-78.