فصلنامه علمی حقوق و مطالعات نوین، دوره ۴، شماره ۱، پیاپی ۱۰، بهار ۱۴۰۲ www.jhvmn.ir
شماره مجوز انتشار: ۸۷۰۱۹ ISSN: 2783-1329

حفظ داده‌های شخصی؛ حق شهروندان، تکلیف دولت‌ها

نرگس نخجوانی[۱]

* نوع مقاله: پژوهشی / تاریخ دریافت: ۱۴۰۱/۰۹/۲۷ / تاریخ پذیرش: ۱۴۰۱/۱۱/۲۰

چکیده

با فراگیری استفاده از امکانات مجازی و فراهم‌شدن امکان دسترسی به اطلاعات و داده‌های شخصی افراد، از یک سو این داده‌ها کالایی ارزشمند برای بنگاه‌های اقتصادی و دولت‌ها تبدیل شده‌اند که به انحای مختلف امکان بهره‌برداری اقتصادی یا امنیتی را برای ایشان فرهم می‌آورد و از سوی دیگر، زمینهٔ تعرض به حریم خصوصی افراد را فراهم آورده است، به این دلیل ساده که افراد ممکن است از جمع‌آوری این اطلاعات در مورد خودشان مطلع نباشند یا دلیل جمع‌آوری اطلاعات را ندانند. ماهیت نرم‌افزارهای کاربردی در جمع‌آوری مستمر داده‌های کاربران و استفاده‌های اعلام نشده از این داده‌ها، در کنار ضرورت حفظ حریم خصوصی، مداخله و تنظیمگری دولت‌ها در این حیطه در راستای حفظ حقوق شهروندان را ناگزیر ساخته است. مقالهٔ حاضر بر آن است تا با در نظر داشتن حفاظت از این داده‌ها به عنوان حق شهروندی و تکلیف دولت‌ها، وضعیت مقررات بین‌المللی در این حیطه و رویکرد نظام حقوقی داخلی را بررسی نماید.

واژگان کلیدی: حریم خصوصی، داده‌های شخصی، مقررات عمومی حفاظت از داده، حمایت از داده‌های شخصی.

[۱] دکتری تخصصی حقوق عمومی، دانشکده حقوق، دانشگاه علامه طباطبایی تهران. (نویسنده مسئول)
n.nkhjvn@gmail.com

مقدمه

نیاز به خلوت، و نیز حریمی که از دسترس «دیگری» در امان باشد، مفهومی نیست که انسان به‌تازگی دریافته باشد یا مورد توجه قرار داده باشد. با این حال شکل توجه حریم خصوصی و نوع حمایت از آن در طول زمان‌ها، و متأثر از شرایط فرهنگی و اجتماعی گوناگون، متفاوت بوده است. امروزه، وقتی از حریم خصوصی سخن می‌رود کمتر در مورد عوامل فیزیکی و حقیقی نگرانی وجود دارد. بلکه در عصر ما، با پیشرفت فناوری در حوزه‌های مختلف مواجهیم. در این میان، فناوری ارتباطی و فناوری اطلاعات، به‌سان فناوری‌های دیگر که با انگیزهٔ خدمت و رفاه به بشری پدید آمده است و گسترش می‌یابد، اثری دوگانه دارد: هم می‌تواند مطلوب جامعهٔ بشری واقع گردد و هم می‌تواند دارای جنبه‌های منفی و تهدیدکننده‌ای باشد که حقوق افراد جامعه را تحت تأثیر قرار می‌دهد (رییسی دزکی، ۱۳۹۹، ۱۴۳). در این راستا، چالش نسبتاً جدیدی که حریم خصوصی با آن روبه‌روست عرصه‌ای است که آن را فضای مجازی می‌خوانیم. فضایی که در آن کاربران، به‌ویژه با عضویت در شبکه‌های اجتماعی یا نرم‌افزارهای پیام‌رسان یا استفاده از سایر اپلیکیشن‌ها، اطلاعات شخصی خود را، به‌صورت عمومی یا خصوصی، با دیگران به اشتراک می‌گذارند. نرم‌افزارهای پیشرفته در کنار صرف ورود یا استفاده از برخی برنامه‌ها امکان دسترسی و پردازش اطلاعاتی را برای ارائه‌کنندگان خدمات اینترنتی فراهم می‌آورند که گاهی درخور توجه تلقی می‌شود و گاهی نیز اهمیت چنین اطلاعاتی نزد صاحب آن معلوم نیست. به نظر می‌رسد بارزترین نمود تعرض به حریم خصوصی در عرصهٔ فضای مجازی دسترسی غیرمجاز به داده‌های شخصی است. مقالهٔ حاضر، تلاش نموده به این سؤال پاسخ دهد که شهروندان در قبال داده‌های شخصی خود در فضایی مجازی از چه حقوقی برخوردارند؟ و چه تلاش‌هایی در سطح ملی و بین‌المللی برای حفاظت از آن صورت گرفته است؟ در این راستا، ضمن بررسی گذرای ارزش داده‌های شخصی ذیل حریم خصوصی و نیز اهمیت کلی این داده‌ها، حقوق شهروندی، تکلیف دولت‌ها را در خلال اسناد و مقررات بین‌المللی و قوانین داخلی بررسی شده است.

۱- حریم خصوصی

پیش از بررسی داده‌ها شخصی و ضرورت حمایت از آن به عنوان یکی از مصادیق حریم خصوصی، نگاهی اجمالی به مفهوم حریم خصوصی اجتناب‌ناپذیر است. تحقیقات و مطالعات مردم‌شناسی نشان می‌دهد در تمام جوامع و در تمام زمان‌ها و دوره‌ها، حتی در جوامع ابتدایی، قواعد اجتماعی وجود داشته است که ورود به اماکن خاصی را محدود می‌کرده و حضور در اماکن معینی را ممنوع

می‌دانسته است (فروغی، ۱۳۹۳، ۱۳۸). این معنی را می‌توان معنای مشترک و قدیمی حریم دانست. به همین ترتیب، می‌توان گفت حریم خصوصی از نظر لغوی به معنای جا، مکان و محدودهٔ شخصی‌ای است که ورود و مداخله در آن جایز نیست (آماده، ۱۳۸۹، ۱۸). اما از نظر کاربردی، برخی معتقدند که «حریم خصوصی فضایی است که نمی‌توان بدون اجازهٔ شخص به آن تجاوز یا تعرض کرد، درواقع، دسترسی به آن فضا برای دیگران امکان‌پذیر نیست» (انصاری، ۱۳۹۲، ۲۷۰). به عبارت دیگر، «حریم خصوصی عبارت است از حق اولیهٔ افراد در مصون‌ماندن حوزهٔ خصوصی ایشان از هرگونه مداخله یا تعرض فاقد مجوز قانونی و همچنین منع دیگران از وقوف بر اطلاعات این حوزه» (اصلانی، ۱۳۸۹، ۲۰).

۲- حریم خصوصی در فضای مجازی

برای تبیین نسبت حریم خصوصی با فضای مجازی و تعریف مرزهای آن و حقوق افراد در این فضا ناگزیر باید تعریفی از فضای مجازی یا سایبر در دست داشته باشیم. «فضای سایبر محیطی مجازی و غیرملموس است که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم وصل می‌شوند) وجود دارد. در این محیط، تمام اطلاعات مربوط به روابط افراد، ملت، فرهنگ‌ها، کشورها، به صورت ملموس و فیزیکی (به‌صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی و به شکل دیجیتالی وجود دارد و در دسترس کاربران است، کاربرانی که از طریق کامپیوتر و شبکه‌های بین‌المللی به هم مرتبط هستند» (باستانی، ۱۳۸۶، ۳۶). در فضای مجازی، به‌خصوص شبکه‌های اجتماعی، دیوارهای حریم خصوصی تخریب شده‌اند و درعوض تأکید بر امنیت قرار گرفته است. با روش‌های مختلف سعی شده است تا امنیت اطلاعات و داده‌های ردوبدل‌شده حفظ شود، اما حریم خصوصی به‌مرور در مرزهای حریم عمومی حل شده است (نیکویی‌مهر، ۱۳۹۷، ۲۳۱). در عصر حاضر، گویی انسان‌ها در خانه‌های شیشه‌ای زندگی می‌کنند و زندگی خصوصی آنها در بسیاری از موارد و موضوعات جنبه‌ای عمومی یافته است. سازمان‌های مختلف می‌توانند به کوکی‌ها، گزارش‌ها، آدرس‌های آی‌پی و حتی وب‌سایت‌هایی دسترسی پیدا کنند که در سابقهٔ جست‌وجو و وب‌گردی کاربران وجود دارد و ذخیره شده است (Belanger, 2006,54). آنها همچنین می‌توانند به حجم عظیم داده‌های شهروندان دسترسی پیدا کنند که روی منابع پراکنده اطلاعاتی قرار گرفته است و، به این ترتیب، از جنبه‌های پنهان و خصوصی زندگی افراد آگاه شوند (Margetts, 2013, 139). این مسئله اهمیت داده‌های شخصی در این روزگار را به خوبی روشن می‌سازد.

۳- اهمیت داده های شخصی

در ترمینولوژی حقوقی از حریم خصوصی به حق خلوت و رهابودن از نگاه دیگران و نظارت عموم تعبیر می‌شود. این مفهوم از حقوق بنیادینی است که مصادیق آن در چهار حوزه حریم خصوصی منازل و اماکن، حریم خصوصی جسمانی، حریم خصوصی اطلاعاتی و حریم خصوصی ارتباطی بررسی می‌شود (عبدی‌پور، ۱۳۹۴، ۱۱۰). درنتیجه، اطلاعات و ارتباطات آن چیزی است که در فضای مجازی در نسبت با حق بر حریم خصوصی مورد توجه قرار می‌گیرد. تعامل و ارتباط در فضای مجازی، و به‌طور کلی هر نوع استفاده از این فضا، مبتنی بر داده‌ها و اطلاعات است. در این فضا هر آنچه رخ می‌دهد به‌وسیلهٔ داده‌ها صورت می‌گیرد (احمدی ناطور، ۱۳۹۵، ۲). در سال‌های اخیر، تحولات مهمی در زمینهٔ شکل و سرعت ارتباطات شخصی رخ داده است و به وضعیتی منجر شده است که باید گفت استفاده از ارتباطات دیجیتال ذاتاً در معرض رهگیری است (انصاری، ۱۳۹۲، ۲۳۵). پیدایش فناوری‌های جدید، با تسهیل دسترسی، زمینهٔ سوءاستفاده از این اطلاعات را در گسترهٔ وسیعی فراهم آورده و بر نگرانی‌های مربوط به تهدید حریم خصوصی افراد در عصر ارتباطات دامن زده است. ازاین‌رو، بحث اطمینان از صیانت داده‌های شخصی در این فضا از اهمیت خاصی برخوردار می‌باشد (رییسی دزکی، ۱۳۹۹، ۱۲۴). به نظر می‌رسد با توجه به مطالب مذکور، می‌توان گفت درنهایت بحث حریم خصوصی در فضای مجازی همان بحث حمایت از داده‌هاست (همان، ۱۲۵و۱۲۶). برخی محققان معتقدند حریم خصوصی اطلاعاتی شامل داده‌هایی در مورد فعالیت‌های روزانهٔ یک فرد، زندگی شخصی وی، امور مالی او، تاریخچهٔ سلامت وی و حتی موفقیت‌های دانشگاهی‌اش می‌شود. به این ترتیب، داده‌های شخصی افراد هم می‌تواند شامل داده‌هایی شود که مربوط به یک فرد بوده و در جایی ذخیره شده باشد یا داده‌هایی باشد که مربوط به ارتباطات فرد است (تقوی فرد، ۱۳۹۶، ۳۰۹). علاوه بر این، تعرض به بعضی از امور، که در دایرهٔ حریم اشخاص قرار دارند، شاید مستقلاً تعدی به حرمت یا حریم شخص محسوب نشود، اما ممکن است زمینهٔ داوری‌هایی را فراهم آورد که به هتک حرمت او بینجامد. بنابراین، در عرصهٔ داده‌ها و فضای مجازی، حریم خصوصی مفهومی گسترده دارد و امروزه می‌تواند آزادی اندیشه، داشتن خلوت، کنترل بر اطلاعات شخصی، حمایت از حیثیت خود و حمایت در برابر تفتیش‌ها و رهگیری‌ها را شامل شود (رییسی دزکی، ۱۳۹۹، ۱۲۵). باید افزود که ارزش این داده‌ها تنها در بعد تجاری و مالی خلاصه نمی‌شود. ملاحظات امنیتی دولت‌ها نیز یکی از اموری است که حریم خصوصی افراد در فضای مجازی را به‌شدت در معرض خطر قرار داده است. با توجه به اینکه عمده‌ترین استفادهٔ افراد از فضای مجازی استفاده از موتورهای جست‌وجو و نیز استفاده از

نرم‌افزارهای تلفن‌های هوشمند به‌ویژه شبکه‌های اجتماعی است، از همین رو، امروزه یکی از بسترهای اصلی و مهم نقض حریم خصوصی انحصار خدمات‌رسانی در اینترنت است. سرویس‌دهنده‌های برتر اینترنت چند شرکت معدود هستند. این شرکت‌ها با وضع قواعد پیچیده و غیر قابل تغییر به‌عنوان خط‌مشی حریم خصوصی، به صورت ظاهری با رضایت فرد اقدام به نقض حریم خصوصی کاربر می‌کنند (فتحی، ۱۳۹۶، ۲۳۸و ۲۳۹). فناوری‌های جدید امکان جمع‌آوری و نگهداری اطلاعات در مقیاس بسیار بزرگ را ایجاد کرده و فناوری اطلاعات این امکان را فراهم آورده است که این داده‌ها به انحای مختلف مورد واکاوی گیرد و اطلاعات دقیق و روشنی از زندگی افراد به دست آید و خطرات غیرقابل‌تصوری برای حریم شخصی افراد به همراه داشته باشد (حبیبی، ۱۳۹۵، ۴۱). شرکت‌های مختلفی در جهان هستند که یکی از منابع درآمدشان همین نقض حریم خصوصی یا استفاده از اطلاعات شخصی است. این شرکت‌ها با رصد فعالیت کاربران در محیط اینترنت، علاقه‌مندی‌ها و سایر اطلاعات کاربران را متوجه می‌شوند و آن‌گاه، با فروش این اطلاعات به شرکت‌های تولیدکنندهٔ کالا و خدمات، درآمد به دست می‌آورند. مثال بارز این موضوع جست‌وجو در گوگل است. وقتی شما یک برند را در گوگل سرچ کنید، گوگل می‌تواند، با اطلاع‌دادن این جست‌وجو به آن برند، نام شما را در زمرهٔ علاقمندان این شرکت درآورد و درنهایت کار شرکت برای تبلیغات هدفمند را ساده کند (فتحی، ۱۳۹۶، ۲۴۰).

۴- استفاده یا سوء استفاده از داده‌ها

وقتی یک برنامه را روی گوشی همراه خود دانلود می‌کنید، معمولاً انبوهی از اجازه‌ها را می‌خواهد تا بتواند به اطلاعات روی دستگاه دسترسی داشته باشد. تعداد کمی از مردم می‌پرسند که چرا یک بازی ساده باید محتوای دفتر نشانی‌ها را بداند و، از آنجا که کادر موافقت‌نامهٔ اجازه بر سر راه شروع بازی است، چیزی به نظر می‌رسد که به راحتی می‌توان از آن گذشت، به جای آنکه آن را خواند. اما طیف اطلاعاتی که این برنامه‌های بی‌آزار می‌توانند جمع کنند گسترده است. این مقدار شامل ایمیل‌ها و تلفن‌های ذخیره‌شده، فهرست تماس‌ها، اینترنت، تقویم و داده‌های موقعیت، آی‌دی اختصاصی دستگاه و داده‌های مربوط به چگونگی استفاده از دستگاه است (Summer, 2016, 77). قابلیت شبکه‌های اجتماعی به گونه‌ای است که به‌رغم تهدیدات فنی موجود، نه تنها امکان دست‌یابی اشخاص ثالث به اطلاعات خصوصی کاربران وجود دارد، بلکه امکان قرارگرفتن اطلاعات شخصی آن‌ها در دست شرکت‌های تجاری بزرگ یا نهادهای حکومتی نیز وجود دارد و این امکان را برایشان فراهم می‌کند که از طریق پروفایل کاربران به بسیاری از اطلاعات حساس آن‌ها دسترسی پیدا کنند (عبدی‌پور، ۱۳۹۴، ۱۱۱).

گوشی شما موقعیت مکانی شما را می‌داند. روال زندگی شما را می‌داند، اینکه کجا زندگی می‌کنید، در کدام کافی‌شاپ در راه نگه می‌دارید، و البته اینکه کجا کار می‌کنید. گوشی شما می‌داند از چه مسیری تردد می‌کنید. جزییات ارتباطات شما و تمام کسانی که می‌شناسید را می‌داند، و اگر برای ایمیل‌دادن از آن استفاده کنید هر چیزی را که برای دیگران می‌نویسید و پاسخ آنها را نیز می‌داند. گوشی حاوی عکس‌ها، فیلم‌ها و عادات وبگردی شماست. آنچه اینجا وضعیت را بغرنج‌تر می‌کند این واقعیت است که به طور معمول هرکس روی گوشی خود بیش از یک برنامه دارد و با ارتباط میان آنها ترکیبی از برنامه‌ها و وب‌سایت‌ها، که مجموعاً استفاده می‌کند، تمام فعالیت‌های او را ثبت و ضبط می‌کنند (Summer, 2016, 5).

با درنظرداشتن خودمختاری فردی و حق بر داشتن اندیشه‌ها، چالش‌های خاص معاصر نه دربارهٔ ایجاد اثری بازدارنده بلکه معطوف به تکنیک‌های اقناع و تحت تأیر قراردادن با استفاده از داده‌های شخصی بوده است. افراد به‌طور فزاینده با پیام‌های شخصی‌شده‌ای مواجه می‌شوند که از سوی عوامل خصوصی یا سازمان‌های دولتی فرستاده شده که برای اقناع و ایجاد تأثیر طراحی شده‌اند و ممکن است اعمال فردی مختلفی را هدف گرفته باشند، مانند خرید کالاها و خدمات جدید یا رأی‌دادن در انتخابات. این اهداف برای پردازش داده‌های شخصی ممکن است قانونی نباشند یا نیاز به رضایت صریح فرد داشته باشند. با این حال، روشن است که مرز روشنی برای حفاظت از خودمختاری فردی و حق داشتن عقیده هست که با رویه‌های اعمال نفوذ متأثر می‌شود و با خطر مواجه می‌شوند (Bakhoum, 2018, 14).

به هر حال باید توجه داشت که چگونگی بهره‌برداری از این اطلاعات مسئلهٔ مهمی است. اگر اطلاعات بدون نام و نشان باشد، به‌صورت آماری در مطالعات عمیق جامعه‌شناسی و اقتصادی و بازاریابی و امثال آن به کار می‌آید، ولی اگر بانام باشد، سوای آنکه می‌تواند به‌منظور تبلیغات و بازاریابی هدفمند به کار گرفته شود، می‌توان آن را به‌عنوان کالایی مستقل به فروش رساند. به عبارت دیگر، اطلاعات خصوصی افراد مانند کالا قابل‌فروش است. از تجار تا کارفرمایان تا دولت‌ها همه خریداران این کالا هستند (حبیبی، ۱۳۹۵، ۴۶).

۵- ضرورت مقررات‌گذاری و تنظیمگری در راستای حفظ حقوق بنیادین افراد

کاربران، وقتی پلتفرم‌هایی مانند فیس‌بوک در مورد تغییر تنظیمات حریم خصوصی آنان تصمیم می‌گیرند، انتخاب محدودی دارند. آنها گزینه‌ای برای تغییر خط‌مشی موجود برنامه‌ها و شبکه‌های اجتماعی ندارند؛ یا باید آن را بپذیرند یا به طور کلی از استفاده از آن سرویس صرف‌نظر کنند (که

در این صورت باز هم به این معنا نیست که فیس‌بوک نگه‌داری و فروش داده‌های آنها را متوقف می‌کند.) این یک اولتیماتوم است نه انتخاب (Summer, 2016, 95). ضررهای ناشی از نقض حریم خصوصی اشخاص بر حسب مورد ممکن است ضرر معنوی یعنی صدمات عاطفی و آسیب به سلامت روحی و روانی شخص یا کاهش اعتبار و تضییع حیثیت او باشد، که مورد اخیر ممکن است علاوه بر ضرر معنوی موجب ضرر مادی و کاهش ارزش بازاری نام و هویت شخص شود ، به ویژه در فرضی که نام شخص به عنوان نام تجاری او مورد استفاده قرار می‌گیرد. قسم دیگر از ضررهای ناشی از نقض حریم خصوصی ضرر ناشی از دسترسی به اسرار تجاری شخص و سوءاستفاده از آن است که امروزه به‌سان مالکیت‌های فکری، مال‌انگاری شده و ارزش تجاری دارند و طبیعتاً ضرر مادی محسوب شده و بنابر قانون باید جبران شوند (Von Bar, 2018, 3136). با توسعهٔ اینترنت و تکنولوژی همراه، حجم و سرعت جمع‌آوری داده‌های شخصی به سرعت رشد کرده است. هم‌زمان، موضوع داده‌ها بسیار ارزشمند و بااهمیت شده و حتی در بازارهای ثانونی معامله می‌شود (Sharma, 2020, 6). از این رو، یکی از موضوعاتی که قویاً نیاز به مداخلهٔ دولت و رکن مقررات‌گذار و تنظیمگر دارد، مسئلهٔ جمع‌آوری اطلاعات و چگونگی بهره‌برداری از آن است (حبیبی، ۱۳۹۵، ۴۱). مهم‌ترین شبکه‌های اجتماعی مطرح در جهان اغلب، به شکل فراملی عمل می‌کنند و به همین دلیل اعمال محدودیت‌های ملی بر آن‌ها معمولاً به‌تنهایی کافی نیست (همان، ۵۱). خودتنظیمی در موضوع موردبحث به شکل کدهای رفتاری و اعلامیه‌های خط‌مشی مؤسسه در قبال حریم خصوصی خودنمایی می‌کند. خودتنظیمی به‌ویژه از آن جهت اهمیت دارد که این شبکه‌های فرامرزی، به‌طور دقیق تحت مقررات ملی کشورها قرار نمی‌گیرند و مقررات ملی هیچ کشوری به‌طور مؤثری آن‌ها را محدود نمی‌کند. چون هنگامی قانون تصویب می‌شود که نیازی احساس شود و ایجاد نظم حقوقی زمانی لازم می‌آید که بی‌نظمی حس شود. بااین‌حال، باید پذیرفت که خودتنظیمی تابع شرایط حاکم بر ذی‌نفعان است و همواره منتج به بهترین نتایج نمی‌شود. به عبارت دیگر، هرچه یک مؤسسه تجاری خود را در موضع قدرت احساس کند، یعنی بداند که کشش خدماتش به‌گونه‌ای است که می‌تواند دسترسی به اطلاعات خصوصی و استفاده تجاری از آن را به مشترکین و کاربران تحمیل کند، در نبود مقررات محدودکننده از این کار دست نخواهد شست. این بدان معناست که، علی‌رغم ضرورت درنظرداشتن خودتنظیمی در برخی موارد، نمی‌توان این خدمات را به حال خود رها کرد. درنتیجه، مقررات‌گذاری در این زمینه و ورود نهادهای عمومی ضروری است (زرکلام،۱۳۸۶، ۱۷۴). نگرانی دیگری که ضرورت وضع مقررات را تقویت می‌کند مربوط به سیاست نحوهٔ بهره‌برداری از این اطلاعات است. در نبود مقررات محدودکننده، تنها نقطه‌اتکای استفاده‌کنندگان به قراردادهای بهره‌برداری و سیاست عملی

شرکت‌ها و ارائه‌دهندگان خدمات است. قراردادهای بهره‌برداری، که اغلب استفاده‌کنندگان آن را مطالعه نمی‌کنند، مانند هر قرارداد الحاقی دیگر، بیشترین حقوق را برای صاحبان این شرکت‌ها محفوظ می‌دارند. ولی تضمینی در خصوص حفظ سیاست‌ها و عدم تغییر آن وجود ندارد (حبیبی، ۱۳۹۵، ۵۱).

۶- رویکرد مقررات بین‌المللی و سایر کشورها در خصوص حمایت از داده‌های شخصی

کنوانسیون جرائم سایبری معروف به «کنوانسیون جرائم سایبری بوداپست» نخستین معاهدهٔ بین‌المللی است که به جرائم رایانه‌ای و اینترنتی می‌پردازد و می‌کوشد قوانین ملی را سازگار کند و روش‌های تحقیقات را ارتقا دهد و همکاری بین کشورها را بهبود بخشد. این کنوانسیون توسط شورای اروپا در سال ۲۰۰۱ ارائه شد و از ۲۳ نوامبر ۲۰۰۱ کشورها می‌توانستند آن را امضا کنند. از ابتدای ژوئیه ۲۰۰۴ کنوانسیون به اجرا درآمد. تا سال ۲۰۱۳، ۳۹ کشور از جمله کشورهای عضو اتحادیهٔ اروپا این کنوانسیون را مصوب نموده و ۱۲ کشور نیز آن را امضا کرده‌اند. «یکی از جنبه‌های مهم این کنوانسیون، که عملاً در اجرا مغفول مانده، این است که کنوانسیون صرفاً محدود به جرائم سایبری نیست بلکه به تمام جرائمی که آثار و شواهدش می‌تواند به‌طور الکترونیکی جمع‌آوری گردد، تسری می‌یابد» (رییسی دزکی، ۱۳۹۹، ۱۳۲). بسیاری از کنوانسیون‌های بین‌المللی همچون اعلامیهٔ جهانی حقوق بشر، کنوانسیون اروپایی حقوق بشر، منشور حقوق مدنی و سیاسی، کنوانسیون‌های منطقه‌ای حقوق بشر و نیز اعلامیهٔ حقوق بشر اسلامی، دولت‌های کشورهای جهان را به حفاظت فعال از حقوق شهروندانشان در خصوص حریم خصوصی‌شان ملزم کرده‌اند. متأسفانه بیشتر کشورهای دنیا از این نظر در وضعیت مناسبی به سر نمی‌برند. به‌طوری که یا قانونی در این زمینه به تصویب نرسانده‌اند یا قوانین بخشی و جزئی در آنها وجود دارد (تقوی فرد، ۱۳۹۶، ۳۰۲و ۳۰۳). سازمان ملل متحد در دسامبر ۲۰۱۳، به اتفاق آرا، رأی به گنجاندن حق حفظ حریم خصوصی اطلاعاتی افراد به عنوان یکی از بندهای حقوق بشر داده است تا انسان‌ها از این حقوق برخوردار باشند: الف) هرگونه ارتباطات برخط آنها مورد احترام قرار گرفته و حفاظت شود؛ ب) از تجاوز به حریم خصوصی آنها جلوگیری شده و قوانین ملی کشورها با حق حفظ حریم خصوصی آنان سازگاری داشته باشد؛ ج) فرایندها، رویه‌ها و قوانین نظارت بر انتقال اطلاعات و جمع‌آوری داده‌های شخصی باید با حق حفظ حریم خصوصی اطلاعاتی افراد تطابق داشته باشد؛ و د) مکانیزم‌هایی برای اطمینان از شفافیت و مناسب‌بودن اقدامات دولت‌ها در نظارت بر انتقال و جمع‌آوری داده‌های شخصی افراد به وجود آید (Sharwood, 2013, 1). همچنین شورای حقوق بشر سازمان ملل در قطعنامه ژوئیه سال ۲۰۱۲ میلادی، به لزوم رعایت حقوق بشر در فضای

دیجیتال و اهمیت توجه به حقوق بشر در فضای مجازی همچون دنیای واقعی تأکید کرد. پس از این تاریخ توجه به حقوق بشر در فضای مجازی در سازمان ملل اهمیت خاصی پیدا می‌کند (حبیبی، ۱۳۹۵، ۵۲). برای مثال سازمان همکاری و توسعهٔ اقتصادی[1] اصولی را در جهت حمایت از داده‌ها اعلام نموده است (تقوی فرد، ۱۳۹۶، ۳۱۳). علاوه بر این سازمان، سازمان همکاری‌های اقتصاد آسیا و اقیانوسیه نیز اصولی را برای حفاظت از داده‌های شخصی شهروندان کشورهای عضو پیشنهاد داده است (حبیبی، ۱۳۹۵، ۵۲). با این همه به طور خاص نمی‌توان سند واحد و مهم جهانی در کنترل شبکه‌های اجتماعی یا حتی حمایت از داده‌های شخصی ملاحظه کرد (حبیبی، ۱۳۹۵، ۵۳). البته مقررات منطقه‌ای به ویژه در اروپا، به نسبت مقررات بین‌المللی، پیشرفت‌های چشمگیرتری حاصل کرده‌اند و توجه مؤثرتری نسبت به حمایت از حق حریم خصوصی به‌ویژه در فضای مجازی داشته‌اند. از همین رو و با توجه به تجارب ارزشمندی که به‌ویژه در سطح اروپا در خصوص حمایت از حریم خصوصی افراد و داده‌های شخصی، در خلال تنظیم مقررات در این حوزه، به دست آمده است، ابتدائاً اشارهٔ مختصری به مقررات کشورها خواهیم داشت و سپس تجربهٔ اروپا را با تمرکز بر مقررات حفاظت از داده ۲۰۱۶ بررسی خواهیم نمود.

۶-۱- کشور ها

دولت‌ها در چگونگی مدیریت دریاچهٔ شناور اطلاعات راه‌حل‌های متفاوتی را برگزیده‌اند. برخی کشورها از جمله ایالات متحده و برخی کشورهای آسیایی، نظام‌های محدود مقررات‌گذاری را توسعه داده‌اند که بر توجه به بخش عمومی و صنایع حساس منتخب متمرکز بوده است و با اعمال و اجرای فشار برای خودتنظیمی در صنعت و ادارهٔ دولت نمود یافته است. اطلاعات شخصی به‌راحتی در اقتصاد در دسترس است و برای بسیاری از مجموعه‌ها برای مدل تجارتشان به عنصری مهم تبدیل شده است. در مقابل این نظام‌های محدود، سایر کشورها، از جمله اروپا، نگاه دیگری داشته‌اند که برتری را با حمایت از مصرف‌کننده و حریم خصوصی فرد در برابر کارآمدی و منافع اقتصادی بنگاه‌ها و مقامات عمومی دانسته است. از دههٔ ۱۹۷۰، جوامعی نظیر فرانسه و آلمان قواعد جامعی را در مورد حریم خصوصی داده در مورد دولت‌ها و صنایع به کار گرفتند. با تصویب مقررات حریم خصوصی داده اتحادیهٔ اروپا در سال ۱۹۹۵، تمام ۲۷ کشور عضو اتحادیهٔ اروپا قوانین جامع داشتند. این مقررات با تمرکز بر حفاظت از حریم خصوصی، شامل قواعد روشنی در مورد جمع‌آوری، انتقال و استفاده از اطلاعات شخصی بود که نظارت و اجرای آن از سوی نهادهای

[1] Organisation for Economic Co-operation and Development (OECD)

مقرراتی انجام می‌شد (Newman, 2008,1). به طور کلی، می‌توان گفت در رویکرد تقنینی کشورها نسبت به حریم خصوصی، دو تصویر کلی از رژیم حریم خصوصی وجود دارد: جامع و محدود. رژیم‌های جامع هر دو بخش عمومی و خصوصی را با مجموعهٔ یکسانی از اصول مربوط به حریم خصوصی به‌ویژه در مورد داده پوشش می‌دهند. این اصول توسط نهادهای تنظیمگر مستقل اعمال می‌شود که کارویژهٔ آنها حفاظت از حریم خصوصی است. رژیم‌های محدود بخش عمومی را با اصولی از حریم خصوصی پوشش می‌دهند که به‌روشنی قابل اجرا باشند، اما این اصول کلی را بر کل بخش خصوصی اقتصادی تحمیل نمی‌کنند. درعوض، راه‌حل‌های تجاری، به همراه برخی قوانین که تعدای از بخش‌های حساس را مستثنی می‌کنند، بر این حوزه مسلط هستند. رویکردهای محدود در خصوص حریم خصوصی به ندرت نهاد خاص اجرایی یا سازوکارهای جبران خسارت برای بخش خصوصی یا عمومی در حوزهٔ حریم خصوصی دارند (Newman, 2008, 23). در بنیادین‌ترین معنا، نظام‌های جامع پیش‌بینی می‌کنند که افراد، به دلیل عدم تقارن قدرت و اطلاعات، در ارزیابی ترجیحات خود برای حفاظت از حریم خصوصی با دشواری مواجه‌اند. بنابراین، این نظام‌ها مجموعه‌ای از هنجارهای حقوقی را ایجاد می‌کند و منافع حریم خصوصی افراد را در برابر منافع صنعتی و بوروکراتیک متعادل می‌کنند. رضایت فردی اغلب پیش از جمع‌آوری یا انتقال اطلاعات از سوی سازمان جمع‌آوری‌کننده به دیگران ضروری است. نهادهای دولتی فعالانه رفتار بخش عمومی و خصوصی را رصد می‌کنند و قدرت شناسایی و مجازات استفادهٔ نادرست از داده‌های شخصی را دارند. برخلاف کالایی‌شدن گستردهٔ داده در کشورهایی با قواعد محدود، کشورهای با نظام‌های جامع کمتر اطلاعات شخصی قابل شناسایی تولید می‌کنند و رویه‌های واضحی برای تشخیص استفادهٔ نادرست وجود دارد. به هر ترتیب، به دلیل اینکه وجود شبکه‌های دادهٔ دیجیتال انتقال سریع اطلاعات شخصی ورای مرزهای قانونی را تسهیل می‌کند، رویکردهای متفاوت به حریم خصوصی داده جوامع را به تضاد با یکدیگر کشانده است. اختلافات بر سر مقررات حریم خصوصی داده روابط تجاری را آشفته کرده و نگرانی‌های امنیتی جدید ایجاد کرده است که بابی مهم برای تحول نقشی که اروپا در شکل‌دهی قواعد اقتصاد جهانی دارد باز کرده است. در برابر سرسختی بی‌رحمانهٔ صنعت جهانی، مقررات اتحادیهٔ اروپا به هر حال به سرعت در جهان صنعت گسترش می‌یابند، با بیشترین تعداد اعضا برای سازمان همکاری و توسعهٔ اقتصادی (استثنای بزرگ آن آمریکاست)، که این مقررات را برای حمایت از حریم خصوصی یا تصویب قوانین به کار می‌گیرند (Newman, 2008, 2). از این رو، با وجود ساختار اداری متفاوت، بیش از ۴۰ کشور شکلی از مقررات فراگیر و جامع را به کار گرفته‌اند، از جمله کشورهایی که مدتی طولانی مقررات محدود

داشته‌اند مانند کانادا، استرالیا، و ژاپن. و حتی آمریکا نیز توافقی بین‌المللی امضا کرده است که بنگاه‌های آمریکایی را متعهد می‌کند در بازارهای اروپا با قواعد اروپایی انطباق یابند (Ibid, 4).

۶-۲- مقررات عمومی حفاظت از دادهٔ اروپا (GDPR)

اگر بخواهیم حمایت از حریم خصوصی در حوزهٔ داده‌های شخصی را از حیث سابقه بررسی نماییم، باید اشاره کرد که در سطح اروپا در سال ۱۹۹۵ ابتدائاً دستورالعملی در این باره به تصویب رسید و این موضوع را به طور خاص مورد توجه قرار داد. تا زمان به کارگیری GDPR، تنها مقررات حاکم بر حفاظت از داده‌ها ، دستورالعمل حفاظت از داده‌ها ۱۹۹۵ بود. مقررات ۱۹۹۵ اتحادیهٔ اروپا[1] سطح حفاظت در اروپا را ارتقا داد و انتقال اطلاعات از سوی دولت‌های عضو به کشورهای فاقد تأمین‌های متناسب را محدود کرد. این مقررات بدون پیش‌بینی جداگانه در نظام قانونی کشورهای عضو قابلیت اجرا نداشت. بدین ترتیب، تمامی دولت‌ها قوانین ملی جامع تصویب کردند که شامل بخش عمومی و خصوصی می‌شد (Newman, 2008, 94). با توجه به ضرورت بازبینی این مقررات، اتحادیهٔ اروپا در سال ۲۰۱۶ با بازنگری مقررات ۱۹۹۵، حمایت افراد در برابر پردازش داده‌های شخصی و انتقال آن را مورد تأکید قرار داد و مقرراتی را به تصویب رساند موسوم به GDPR[2] یا مقررات عمومی حفاظت از داده. برابر این سند، حق استفاده و پردازش داده‌های شخصی، بدون کسب رضایت صریح شخص، غیرمجاز است و در صورت کسب اجازه هم صرفاً برای هدف مورد رضایت شخص این داده‌ها می‌تواند مورد بهره‌برداری قرار گیرد (رییسی دزکی، ۱۳۹۹، ۱۳۰). با تصویب آیین‌نامهٔ عمومی حفاظت از دادهٔ اتحادیهٔ اروپا در سال ۲۰۱۶، سازوکاری جدید در دستور کار کمیسیون اتحادیهٔ اروپا قرار گرفت، که، برخلاف مبانی کلی موجود در نظام حقوقی کشورهای عضو اتحادیه، امکان جبران جمعی خسارات در دعاوی ناشی از نقض مقررات امنیتی آیین‌نامهٔ مذکور برای اتباع کشورهای عضو اتحادیه پدید آمد (فرحزادی، ۱۳۹۸، ۴۱۴). اگر چه این قانون در اتحادیهٔ اروپا وضع شده است، اما حوزهٔ سرزمینی آن محدود به اعضای اتحادیهٔ اروپا نیست و دایرهٔ شمول آن شرکت‌ها و سازمان‌هایی را نیز که در این اتحادیه مستقر نیستند می‌تواند در برگیرد. همچنین ماهیت این قانون و دید جامع و فراگیر آن در ارتباط با حریم خصوصی افراد و محافظت از داده‌ها باعث شده است که مطالعهٔ آن از منظر نیازهای امنیتی بسیار مهم باشد. هدف این مقررات اساساً اعطای کنترل داده‌ها به شهروندان و ساکنان منطقهٔ اروپا و ساده‌سازی محیط مقررات‌گذاری

[1] دستورالعمل شماره EC/۴۶/۹۵ اتحادیه اروپا

[2] The General Data Protection Regulation (GDPR) (EU) 2016/679

برای کسب‌وکارهای بین‌المللی از طریق یکسان‌سازی مقررات است. به عبارتی برای هماهنگ‌کردن جریان داده‌ها بین همهٔ کشورهای عضو و تقویت بعد حقوقی آن است تا شهروندان اتحادیهٔ اروپا نسبت به داده‌های خود، که در سازمان‌ها نگه داشته و پردازش می‌شود، قدرت کنترلی بیشتری داشته باشند. بدین ترتیب، فرایندهای کسب‌وکار، که اطلاعات شخصی را اداره می‌کنند، باید مبتنی بر «حفاظت اطلاعات از طریق طراحی و به‌طور پیش‌فرض» باشند؛ یعنی اطلاعات شخصی باید با استفاده از مستعارسازی یا بی‌نام سازی ذخیره شود و حداکثر محرمانگی به‌طور پیش‌فرض در نظر گرفته شود، به گونه‌ای که داده‌ها بدون رضایت صریح به‌طور عمومی در دسترس نباشد و بدون اطلاعات اضافی جداگانه برای تعیین هویت اشخاص قابل استفاده نباشد. هیچ اطلاعات شخصی نمی‌تواند پردازش شود، مگر آنکه تحت مبنای قانونی که به وسیله مقررات مشخص شده، انجام شود یا آنکه کنترل‌کننده یا پردازندهٔ داده‌ها اجازهٔ صریح مختارانهٔ صاحب داده‌ها را دریافت کرده باشد. صاحب داده‌ها می‌تواند در هر زمانی این اجازه را لغو کند. در این مقررات جدید، چگونگی کنترل اطلاعات مشتریان و کاربران توسط سازمان‌ها و شرکت‌ها مورد توجه قرار گرفته است. ضمن اینکه به حقوق اشخاص و اعطای نظارت آن‌ها روی اطلاعات شخصی‌شان در فضاهایی مثل اینترنت توجه بیشتری شده است. البته GDPR یک تغییر گام‌به‌گام در حفاظت از داده‌هاست و، بیش از اینکه به یک «انقلاب» شبیه باشد، به‌عنوان یک «تکامل» مطرح است. وب‌سایت رسمی GDPR در اروپا اعلام می‌دارد که این قانون برای «هماهنگی» قوانین حفاظت از داده در سراسر اروپا و اعطای حقوق و حفاظت بیشتر به اشخاص حقیقی طراحی شده است.[1] به کمک GDPR تغییرات گسترده‌ای در نحوهٔ نگه‌داری اطلاعات شخصی توسط شرکت‌ها، سازمان‌ها و بخش‌های مختلف اتفاق می‌افتد. مقررات عمومی حفاظت از داده، بر خلاف مقررات ۱۹۹۵ که از کشورهای عضو خواسته می‌شود تا قوانین داخلی خود را برای اجرای قوانین آن تهیه کنند، به طور خودکار برای همه ۲۸ کشور عضو اتحادیهٔ اروپا اعمال می‌شود و نیازمند تصویب جداگانه در پارلمان‌های کشورهای عضو نیست. هدف این آیین نامه این است که به مردم قدرت بیشتری نسبت به داده‌های خود ببخشد و عملکرد شرکت‌ها را در نحوه برخورد با اطلاعات حساس شفاف‌تر کند.

لازم به ذکر است که GDPR در قالب چندین اصل راهنما طراحی شده است که می‌توان آنها را اینگونه دسته‌بندی نمود:

الف) اصول محافظت از داده‌ها

[1] https://gdpr-info.eu/

تعریف GDPR از حوزهٔ داده‌های شخصی تا حد زیادی وسیع و گسترده است. اتحادیهٔ اروپا در ارتباط با حفاظت از حریم خصوصی افراد به شدت قاطع و محکم عمل می‌کند و امروز، با تصویب این مقررات جامع، مسیر جدیدی را برای محافظت از حقوق افراد شروع کرده است و با وضع جریمه‌های مالی سنگین، تا سقف ۴ درصد سود کل یک شرکت، که می‌تواند به راحتی شرکت‌ها را در بازار با چالش مواجه کند، از اجرای این قوانین پشتیبانی می‌کند. در این سند، حفاظت از داده‌های شخصی با پشتوانهٔ زمینهٔ حفاظت از حقوق و آزادی‌های بنیادین فردی توجیه شده است و به طور خاص بر حق بر حریم خصوصی و حق جدید بر حفاظت از داده‌های شخصی تأکید دارد (Bakhoum, 2018, 8). تعریف دادهٔ شخصی در این مقررات گسترش یافته است. براساس این سند، دادهٔ شخصی حاوی اطلاعاتی است که مبتنی بر آن یک شخص، به طور مستقیم یا غیرمستقیم، شناخته می‌شود. براساس تعریف جدید، شناساننده‌ها مانند آی پی آدرس و کوکی‌ها مشمول تعریف اطلاعات شخصی هستند (Tankard, 2016, 5). در کنار الزام شرکت‌ها و سازمان‌های جمع‌آوری‌کنندهٔ داده‌های شخصی به رعایت مقررات، GDPR به اشخاص نیز قدرت بیشتری برای دسترسی به داده‌هایی که به خودشان مربوط می‌شوند داده است. طبق GDPR، اشخاص می‌توانند از شرکت یا سازمان درخواست ارائهٔ اطلاعاتی را کنند که در موردشان ذخیره کرده است. اجابت این درخواست الزامی و رایگان خواهد بود. پس از ارائهٔ درخواست، شرکت باید ظرف مدت یک ماه، اطلاعات مورد نظر را جمع‌آوری کرده و تسلیم شخص کند.

GDPR مشخص می‌کند که سازمان‌ها باید فرایندهای مؤثری را برای حفاظت از داده‌ها توسعه دهند. این شامل استفاده از فناوری‌های مناسب، آموزش کارمندان و ایجاد روش‌های دقیق برای محافظت از داده‌ها است. براساس GDPR، اطلاعات شخصی که توسط یک سازمان جمع‌آوری می‌شود باید بادقت محافظت شود. بدین ترتیب، کلیهٔ داده‌ها می‌بایست:

- به صورت قانونی، منصفانه و شفاف پردازش شوند. (انصاف و قانونی‌بودن)
- برای یک هدف خاص و قانونی جمع‌آوری شده باشد. (محدودیت هدف)
- محدود به آنچه برای یک هدف خاص لازم است، باشد. (حداقلی‌بودن داده)
- با دقت حفظ شود و به‌روز باشد. (صحت)
- فقط تا زمانی که لازم است، ذخیره شود. (محدودیت ذخیره)

• ایمنی و محرمانه‌بودن آن با استفاده از فناوری‌های مناسب حفظ شود. (صداقت و محرمانگی)

ب) پردازش قانونی

یک تغییر کلیدی جی دی پی آر، در پردازش قانونی اطلاعات، وجود استاندارد لازم برای رضایت است. رضایت مبتنی بر جی دی پی آر باید آزادانه اعلام شود، معین، مبتنی بر آگاهی و مستند باشد که با عملی صریحاً ایجابی ابراز شده است. پردازش داده تنها زمانی منصفانه است که شفاف باشد، بدین معنا که باید در خلال ارتباط مؤثر با افراد از جمله با استفاده از هشدارهای اعلامی گشودگی در پردازش اطلاعات وجود داشته باشد (Goddard, 2017, 704). در مرحلهٔ به‌دست‌آوردن اطلاعات زمانی که اطلاعات یک شخص در اختیار دیگری قرار می‌گیرد، فقط آن شخص یا سازمان مجاز به استفاده بوده و در انتقال و افشای آن داده‌ها مجوزی ندارد (صابرنژاد، ۱۳۹۵، ۱۶). بنابراین، جز با رضایت شخص موضوع داده و تنها در یک یا دو موردی که او اجازه داده، نباید داده‌های شخصی پردازش شوند مگر حداقل یکی از مقدمات قانونی زیر فراهم باشد:

• برای منافع مشروع کنترل‌کنندهٔ داده یا یک شخص ثالث، مگر اینکه این منافع با منشور حقوق بنیادی اتحادیهٔ اروپا در تعارض باشد. (به ویژه در مورد کودکان)

• برای اجرای وظیفه‌ای در خدمت عموم یا یک مرجع رسمی

• برای رعایت تکالیف قانونی کنترل‌کنندهٔ داده

• برای تحقق الزامات قراردادی با شخص موضوع داده

• برای ایفای تعهداتی که به‌واسطهٔ درخواست شخص موضوع داده که در فرایند انعقاد قرارداد یا کنترل‌کنندهٔ داده قرار دارد.

• برای حفاظت از منافع حیاتی شخص موضوع داده یا یک شخص دیگر

ج) پاسخگویی و حاکمیت

پاسخگویی مستلزم آن است که سازمان‌ها معیارهای فنی و ساختاری متناسبی را به کار گیرند و بتوانند آنچه را انجام داده‌اند و کارآمدی آن را در صورت درخواست نشان دهند. این موضوع همچنین مشتمل بر استفاده از ارزیابی‌های مربوط به حریم خصوصی در پردازش‌های پرخطر است.

جی دی پی آر همچنین یک نظام الزام‌آور هشدار درز داده را معرفی می‌کند (Goddard, 2017, 703).

در این زمینه یک سازمان باید با موارد ذیل انطباق خود با GDPR را نشان دهد:

- ثبت سابقهٔ رضایت کاربران
- ثبت سوابق نحوهٔ جمع‌آوری، ذخیره و پردازش داده‌ها
- آموزش کارمندان بر اساس اصول GDPR
- تعیین یک مسئول حفاظت از داده
- مستندکردن سیاست‌های محافظت از داده

ذیل مقررات GDPR قواعدسختگیرانه‌ای برای چگونگی کسب رضایت سازمان‌ها از کاربران دارد. برای اینکه رضایت معتبر و مشروع تلقی شود باید شروط زیر را داشته باشد:

- درخواست‌های رضایت باید آسان فهم باشد.
- رضایت باید آزادانه و به روشی غیر مبهم ارائه شود.
- کاربر باید از نحوه استفاده شما از داده‌های آنها آگاه باشد.
- رضایت در هر زمان امکان پس گرفتن داشته باشد.
- سازمان‌ها باید شواهد رضایت کاربر را ذخیره کنند.

د) حق فردی برای حفظ حریم خصوصی

GDPR سطح بالاتری از حریم خصوصی را به افراد می‌دهد. این کار را با دادن حقوق زیر به آنها انجام می‌دهد:

- درخواست دسترسی به داده‌هایی که یک سازمان دارد
- امکان تغییر داده‌های نادرستی که یک سازمان دارد

• اعتراض به اطلاعات شخصی آنها که توسط یک سازمان نگهداری می‌شود

• پاک‌کردن داده‌های شخصی در صورت تقاضا

• انتقال داده‌های شخصی از یک ارائه دهنده به شرکت دیگر

• کاربران حق دارند دقیقاً بفهمند که سازمان چگونه می‌خواهد از اطلاعات استفاده کند و اینکه تا چه مدت آن را خواهد داشت.

ه) گزارش درز داده‌ها

هماهنگی در حفاظت از داده‌های شخصی می‌تواند با اعمال تکلیف بر این عاملان مستحکم شود. علاوه‌براین، می‌توان صریحاً عنوان کرد که کنترل‌کننده و پردازشگر مسئول زیرمجموعه‌های خود هستند. این مسئله تضمین می‌کند که موضوع داده‌ها همیشه می‌تواند در غیاب معیارهای متناسب امنیت حداقل از یک نهاد دادخواهی کند (Wolters, 2017, 14). پیش از اجرایی‌شدن جی دی پی آر، تعداد کمی از دولت‌های عضو اتحادیهٔ اروپا قوانین کلی هشدار درز داده داشتند. جی دی پی آر این موضوع را، با الزام هشدارهای درز داده، یکسان‌سازی کرد (مادهٔ ۳۳ و ۳۴ جی دی پی آر) GDPR (Custers, 2019, 207). از سازمان‌ها می‌خواهد تا نسبت به درز داده‌هایی که جمع‌آوری می‌کنند شفاف‌تر عمل کنند. درز داده‌ها باید ظرف ۷۲ ساعت از کشف به سازمان حفاظت از داده‌ها گزارش شود. در این گزارش اولیه باید ماهیت داده‌هایی را که تحت تأثیر قرار می‌گیرند، مشخص کند. اینکه تقریباً تا چه اندازه بر افراد تأثیر می‌گذارد، چه عواقبی برای آنها می‌تواند داشته باشد و چه اقداماتی قبلاً انجام شده یا اینکه چه برنامه‌ای برای پاسخگویی تدوین شده، باید عنوان شود. همچنین اگر خطرات زیادی برای حقوق و آزادی‌های کاربر وجود داشته باشد (مانند اطلاعات شخصی که می‌تواند به سرقت هویت منجر شود)، این سازمان باید به کاربران اطلاع دهد. به نظر می‌رسد اندیشهٔ اصلی در پس الزام هشدارهای درز داده تشهیر و بدنامی است: سازوکار پیش‌بینی‌شده این است که افشای درز داده‌ها (در برابر موضوع داده، یا عموم) به سوءشهرت کنترل‌کنندهٔ داده می‌انجامد و برای اجتناب از این خسارت معیارهای امنیتی را ارتقا خواهد داد (Custers, 2019, 207).

۷- رویکرد نظام داخلی در خصوص حمایت از داده‌های شخصی

در نظام حقوقی ایران، تا کنون برخی قوانین، در ارتباط با حوزهٔ فضای مجازی تصویب شده‌اند که از برخی قواعد آن می‌توان توجهی به حفاظت داده‌های شخصی را استنباط نمود. با این حال، نمی‌توان این قوانین را به طور مستقیم با حمایت از داده‌های شخصی مربوط دانست. چه آنکه، این حوزه، همان‌طور که دربررسی مقررات جی دی پی آر مشخص شد، ناگزیر از توجه به ظرائف و جزییاتی است که اشاره اجمالی یا غیرمستقیم به آن در خلال سایر قوانین نمی‌تواند وافی به مقصود حمایت و حفظ داده‌های شخصی باشد. در این بخش ضمن بررسی قانون جرایم رایانه‌ای و قانون تجارت الکترونیک به بررسی طرحی نیز خواهیم پرداخت که در سال‌های اخیر تحت عنوان «صیانت از داده‌های شخصی» طرح شده اما تاکنون تصویب نشده است.

۷-۱- قانون جرایم رایانه ای

در «قانون جرائم رایانه‌ای» مصوب ۱۳۸۸، مصادیق جرائم رایانه‌ای مشخص و برای ارتکاب آنها تدابیر کیفری پیش‌بینی شده است (تقوی فرد، ۱۳۹۶، ۳۰۳ و ۳۰۴). مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه‌ای جرم‌انگاری شده است عبارت‌اند از: دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا اکانت اشخاص (مادهٔ ۱)؛ شنود غیرمجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از نرم‌افزارهای شنود چت‌های اینترنتی (مادهٔ ۲)؛ دسترسی غیرمجاز به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن (مادهٔ ۳)؛ نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده (مادهٔ ۴)؛ در دسترس قراردادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت (مادهٔ ۵)؛ حذف یا تخریب یا مختل یا غیر قابل پردازش نمودن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده به طور غیرمجاز (مادهٔ ۸)؛ ازکارانداختن یا مختل نمودن سیستم‌های رایانه‌ای یا مخابراتی به‌طور غیرمجاز نظیر غیرفعال‌سازی دیتابیس تارنماها و ممانعت از دسترسی اشخاص به پایگاه اینترنتی‌های شخصی (مادهٔ ۹)؛ ممانعت از دسترسی اشخاص مجاز به داده‌های یا سیستم‌های رایانه‌ای یا مخابراتی به طور غیرمجاز (مادهٔ ۱۰)؛ ربودن داده‌های متعلق به دیگری به طور غیرمجاز (مادهٔ ۱۲)؛ هتک حیثیت از طریق انتشاریافتن صوت و فیلم تحریف شده دیگری به‌وسیلهٔ سیستم‌های رایانه‌ای یا مخابراتی (مواد ۱۶ و ۱۷)؛ نشر اکاذیب از طریق سیستم‌های

رایانه‌ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی (مادۀ ۱۸). هم چنین در تبصرۀ مادۀ ۴۸ این قانون آمده است «دسترسی به محتوای ارتباطات غیرعمومی ذخیره‌شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است.»

۷-۲- قانون تجارت الکترونیک

یکی از بحث‌های عمده در تجارت الکترونیک بحث حمایت از داده‌های شخصی است. اطلاعات همواره در تجارت نقش بسیار مهمی دارد. بازاریابی، تعیین زمان و مکان خریدوفروش اجناس و تمام فعالیت‌های مرتبط با تجارت رابطۀ نزدیکی با اطلاعات دارد. بخشی از این اطلاعات، داده‌های شخصی طرف‌های تجاری و نیز مصرف‌کنندگان است. برای انجام مبادلات تجاری بین‌المللی، کشورهای پیشرو اقتصادی، چنین داده‌هایی را به کشورهایی که فاقد سطح حمایت کافی هستند انتقال نمی‌دهند و این امر می‌تواند باعث تحریم اطلاعاتی و کاهش توان بازیابی و ارزیابی‌های دیگر تجار در کشورهای تحت تحریم اطلاعاتی شود (احمدی ناطور، ۱۳۹۵، ۸). مواد ۵۸ و۵۹ قانون تجارت الکترونیکی در زمینۀ داده‌های شخصی، برخی از اصول ناظر بر حمایت از حریم خصوصی داده‌ها و اطلاعات شخصی در محیط الکترونیکی را موردتوجه قرار داده است. از آن جمله می‌توان به اصل تحصیل قانونی و مبتنی بر رضایت سوژه یا شخص موضوع گردآوری و پردازش (مادۀ ۵۸)، اصل تحصیل مضیق و مرتبط (بندهای الف وب مادۀ ۵۹)، اصل درستی یا صحت داده‌های گردآوری‌شده) بند ج مادۀ ۵۹) ، اصل دسترسی (بند د مادۀ ۵۹) و اصل امحا (بند هـ مادۀ ۵۹) اشاره کرد. در قانون تجارت الکترونیک، آنچه در خصوص حمایت از حریم خصوصی و پیش‌بینی ضمانت‌اجرا برای نقض آن می‌تواند درخور توجه قرار گیرد جرم‌انگاری نقض حریم داده‌پیام‌های شخصی در تجارت الکترونیکی است. در مواد ۵۸ و ۵۹ این قانون آمده است:

«مادۀ ۵۸: ذخیره، پردازش و یا توزیع "داده پیام"های شخصی مبین ریشه‌های‌قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های‌راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هرعنوان غیرقانونی است.»

«مادۀ ۵۹: درصورت رضایت شخص موضوع داده‌پیام نیز به شرط آنکه محتوای‌داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع داده‌پیام‌های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت‌پذیرد:

الف) اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند.

ب) داده‌پیام باید تنها به‌اندازهٔ ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع داده‌پیام شرح داده شده جمع‌آوری گردد و تنها برای‌اهداف تعیین‌شده مورد استفاده قرار گیرد.

ج) داده‌پیام باید صحیح و روزآمد باشد.

د) شخص موضوع داده‌پیام باید به پرونده‌های رایانه‌ای حاوی داده‌پیام‌های‌شخصی مربوط به خود دسترسی داشته و بتواند داده‌پیام‌های ناقص و یا نادرست را محو یا اصلاح کند.

هـ) شخص موضوع داده‌پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پروندهٔ رایانه‌ای داده‌پیام‌های شخصی مربوط به خود را بنماید».

مادهٔ ۵۸ قانون مذکور سطح بالایی از حریم خصوصی را در فضای مجازی را به رسمیت شناخته که با توجه به خصوصیات این فضا و لزوم حمایت مؤثر از اطلاعات شخصی، قابل توجیه است. در مورد این داده‌ها رضایت صریح ضروری دانسته شده است. با توجه به مادهٔ ۵۹ همان قانون، حتی در صورت رضایت صریح شخص موضوع داده‌پیام، علاوه بر ضرورت انطباق محتوای داده‌پیام یا قوانین مجلس، رعایت شرطی ازجمله استفاده متناسب با اهداف جمع‌آوری، صحیح و روزآمدبودن داده‌ها و دسترسی شخص به پرونده رایانه‌ای خود و امکان حذف و اصلاح داده‌های ناقص یا نادرست و حق وی برای درخواست محو کامل پرونده خود لازم است. می‌توان نوعی حق فراموش‌شدن را برداشت نمود (قبولی درافشان، ۱۳۹۷، ۱۲۴). مادهٔ ۵۹ در اصل رکن قانونی نقض حریم داده‌پیام‌های شخصی در تجارت الکترونیکی است که مقرر نموده است: «ذخیره، پردازش و یا توزیع داده‌پیام‌های شخصی مبین ریشه‌های قومی و نژادی از دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده‌پیام‌های راجع به وضعیت جسمانی و روانی و یا جنسی اشخاص، بدون رضایت صریح آن‌ها، به هر عنوان غیرقانونی است.» به طور کلی می‌توان گفت در حوزهٔ حمایت از داده‌ها در فضای سایبر، قانون تجارت الکترونیک مصوب ۱۳۸۲ توانسته است تا حدودی نبود قانون ویژه حمایت از حریم خصوصی و داده‌ها را جبران کند. این قانون ضمن پیش‌بینی اصولی در مواد ۵۸ و ۵۹ خود که ملهم از اصول بین‌المللی پیش گفته است، در ماده ۷۱ نقض این مواد قانون را جرم محسوب کرده و ضمانت اجرای کیفیری یک تا سه سال حبس را برای آن مقرر کرده است (حبیبی، ۱۳۹۵، ۵۹).

۷-۳- طرح حمایت و حفاظت از داده و اطلاعات شخصی

در دی‌ماه ۱۳۹۶ پیش‌نویس لایحهٔ حمایت از داده و حریم خصوصی در فضای مجازی و در تیرماه ۱۳۹۷ پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی تهیه و برای اظهارنظر علمی در اختیار صاحب‌نظران قرارگرفته است. بعدتر در قالب طرح حمایت و حفاظت از داده و اطلاعات شخصی در اسفند ماه ۱۳۹۹ در مجلس اعلام وصول شده است.[1] هدف اصلی این طرح صیانت از حیثیت و کرامت اشخاص موضوع داده‌هاست که شامل تبیین حقوق اشخاص موضوع داده‌ها، به‌ویژه در تعامل با سایر حق‌های مشروع، ضابطه‌مندی فرایند پردازش داده‌های شخصی، مسئولیت‌پذیری پردازش، هم‌افزایی امور تنظیمی و نظارتی پردازش و جبران‌پذیری زیان‌ها و آسیب‌های پردازش است (مادهٔ ۱ طرح). در مادهٔ ۲ طرح صیانت و حفاظت از داده و اطلاعات شخصی، دادهٔ شخصی تعریف شده است. بر این اساس، دادهٔ شخصی عبارت است از «داده‌ای که به‌تنهایی یا به همراه داده‌های دیگر، شخصِ موضوعِ داده را می‌شناساند». این ماده همچنین به تعریف پردازش، کنترلگر و پردازشگر داده‌ها نیز پرداخته است. براساس مادهٔ ۳ این طرح، این قانون، در صورت تصویب، از یک سو شامل اتباع ایرانی حقیقی یا حقوقی عمومی یا خصوصی می‌شود، اعم از آنکه داده‌های شخصی آن‌ها درون یا بیرون از ایران پردازش شود، و از سوی دیگر، اتباع خارجی حقیقی یا حقوقی عمومی یا خصوصی را در بر می‌گیرد که داده‌های شخصی آن‌ها از سوی کنترلگر یا پردازشگر ایرانی پردازش می‌شود. در این طرح بر رضایت موضوع داده‌ها در مورد پردازش آن تأکید شده است. برای آنکه رضایت، براساس این قانون، معتبر تلقی شود می‌بایست پیش از پردازش باشد؛ بیانگر آگاهی شخص موضوع داده باشد؛ و استنادپذیر باشد. در مادهٔ ۷ این قانون نیز تأکید شده است که در صورت عدم اهلیت موضوع داده، رضایت قیم او ملاک است. این طرح پردازش داده‌ها بدون رضایت فرد را تنها در صورتی مجاز می‌داند که:

الف) برای صیانت از حیثیت، جان یا مال شخص موضوع داده ضروری باشد؛

ب) برای صیانت از حیثیت یا جان دیگری یا پیشگیری از زیان مالی شدید او ضروری باشد؛

ج) برای پیشگیری یا پاسخ به تهدیدهای نظم، ایمنی و امنیت عمومی ضروری باشد؛

د) برای کشف جرائم یا تخلفات یا شناسایی متهمان یا اجرای احکام قضایی و انتظامی ضروری باشد.

[1] https://rc.majlis.ir/fa/legal_draft/show/1675111

این طرح همچنین تحت شرایطی مطالبهٔ عدم پردازش داده ها از کنترلگر را نیز به رسمیت شناخته است. ضمن آنکه در مادهٔ ۷ این طرح آمده است که «درخواست انجام یا توقف پردازش داده‌های شخصی می‌تواند باهدف فراموشی مطرح شود، مشروط بر آنکه ذی‌نفع دیگری نباشد.» به عبارت دیگر، این طرح در رویکردی پیشروانه حق بر فراموش‌شدن را در چارچوبی مشخص و با درنظرداشتن حقوق احتمالی دیگران، به رسمیت شناخته است. براساس مادهٔ ۱۱، این طرح بهره‌برداری مالکانه از داده‌های شخصی را تنها در صورتی مجاز می‌داند که به طور پیشینی رضایت فرد جلب شده باشد، در غیر این صورت، چنانچه درعمل امکان جلب رضایت وجود نداشته باشد، تنها با حفظ گمنامی موضوع داده و با اطمینان از اینکه خسارت مالی یا معنوی برای او ایجاد نمی‌شود، امکان چنین استفاده‌ای وجود دارد. این طرح بر نظارت‌پذیری پردازش تأکید دارد و همچنین در راستای اعتمادپذیری پردازش چهار اصل شفافیت، تهدیدناپذیری (ایمنی و حفاظت)، پاسخگویی و استنادپذیری را شناسایی می‌کند. این طرح در نهایت برای نظارت بر مفاد آن و تنظیم و نظارت بر پردازش داده‌های شخصی، چهار رکن را معرفی می نماید، کمیسیون صیانت از داده‌های شخصی؛ هیئت نظارت؛ کارگروه‌های تخصصی؛ و دبیرخانهٔ اجرایی کمیسیون. در باب ضمانت اجرا نیز، این طرح، علاوه بر شناسایی مسئولیت مدنی و تأکید بر جبران خسارت مادی، نحوهٔ تقویم خسارات معنوی و اعادهٔ حیثیت را به تصمیم کمیسیون صیانت از داده واگذار کرده است. این طرح همچنین به پیش‌بینی ضمانت اجراهای کیفری نیز پرداخته است. مطابق مادهٔ ۶۸ این طرح، «مرتکبان ذیل به مجازات مقرر محکوم می‌شوند:

الف)نقض حق رضایت شخص موضوع داده، چنانچه داده‌های وضعیت‌ها و موقعیت‌های غیرعمومی پردازش شود، به مجازات درجه ۵ و چنانچه داده‌های وضعیت‌ها و موقعیت‌های عمومی پردازش شود، به مجازات درجه ۶؛

ب)ممانعت ازاستیفای همه یا بخشی از حق درخواست شخص موضوع داده درباره پردازش یا توقف آن یا انجام پردازش داده‌های شخصی به‌وسیله خود و یا نقض حق گمنامی، به یک یا هر دو مجازات درجه ۶؛

ج) نقض تعهدات اعتبارپذیری، اعتمادپذیری یا استنادپذیری پردازش داده‌های شخصی، به یک یا هر دو مجازات درجه ۵؛

د)استیفای ناروای حقوق مندرج در این قانون از سوی شخص موضوع داده، با توجه به‌شدت جرم و زیان‌ها و آسیب‌های وارده به یک یا هر دو مجازات درجه ۶؛

ه) کنترل غیرمجاز پردازش از سوی مقام صلاحیت‌دار دستگاه اجرایی، علاوه بر مجازات مقرر برای جرم موردنظر به انفصال‌ازخدمت از شش ماه تا سه سال؛

و) امتناع از اجرا یا اجرای نادرست یا اقدام به‌نحوی‌که اجرای همه یا بخشی از ضوابط این قانون یا دستور کمیسیون یا هیئت نظارت یا ناظر ویژه منتفی گردد، مانند عدم نگهداری همه یا بخشی از داده‌ها، حسب مورد یک یا هر دو مجازات درجه ۵.»

به طور کلی، می‌توان گفت این طرح به تجارب موفق در عرصهٔ حمایت از داده‌های شخصی و حفظ حریم خصوصی، همچون مقررات حفاظت از دادهٔ اروپا، نظر داشته است و به‌طور منطقی و طبیعی از اسناد موجود و تجربه‌شده در سطح بین‌المللی و سایر کشورها الگو گرفته است. تأکید بر اخذ رضایت موضوع داده‌ها، با توجه به تعدد روزافزون برنامه‌های ایرانی و داخلی که مورد استفادهٔ کاربران قرار می‌گیرند، تصمیمی بجاست که البته هر روز جای خالی آن، در خلال تعلل برای تصویب نهایی این طرح، احساس می‌شود. همچنین، با در نظر داشتن تجربه‌ای نظیر GDPR، به نظر می‌رسد این طرح می‌تواند حاوی جزئیات بیشتری در خصوص مسئولیت پردازشگر و کنترلگر و نحوهٔ مجاز پردازش داده‌های شخصی یا استفاده از آن باشد. به هر حال، بعد از رونمایی از متن اولیهٔ این طرح در سال ۱۳۹۷ و تقدیم آن به مجلس در سال ۱۳۹۹، موضع مشخص یا ارادهٔ مستحکمی در تصویب آن به چشم نمی‌خورد و مطابق آنچه در سوابق مربوطه در سایت مرکز پژوهش‌های مجلس ثبت شده است، حتی بررسی آن در دستور کار کمیسیون‌های مربوطه قرار نگرفته است.[1]

[1] https://rc.majlis.ir/fa/legal_draft/show/1675111

نتیجه گیری

بررسی تحول‌های صورت گرفته در نظام حقوقی کشورهای پیش‌رو، در زمینهٔ صنعت فناوری اطلاعات و ارتباطات، حاکی از آن است که این کشورها، به دنبال توسعه فناوری‌های اطلاعاتی و شکل‌گیری کسب‌وکارهای مبتنی بر داده، به سبب پیدایش چالش‌ها و مخاطرات گسترده‌ای در این زمینه، یک نهاد رسمی به عنوان «متولی داده» تشکیل داده‌اند. مسئولیت این نهادها، تنظیم و نظارت بر این حوزه، بر اساس قوانین و مقررات حمایت از داده است. حال آنکه نتایج بررسی اسناد بالادستی و رویه‌های اجرایی کشور، مؤید این مطلب است که در نظام حقوقی ایران، قانون جامعی در خصوص حفاظت از داده‌ها وجود ندارد و بالطبع، نهادی هم متولی رسمی داده در کشور نیست. این امر باعث شده تا علی‌رغم رشد فناوری‌های نوین، بسترهای قانونی مرتبط با حقوق داده در نظام حقوقی کشور تشکیل نشود. درنتیجه، رشد کسب‌وکارهای مبتنی بر داده نیز در ایران به کندی صورت خواهد گرفت (زارعیان، ۱۳۹۹، ۶۸). تنها سندی که در آن به این موضع توجه شده است لایحهٔ صیانت و حفاظت از داده‌های شخصی است که به تصویب نرسیده است و سرنوشت آن همچنان مبهم است. خلأ قوانین و مقرراتی حمایتی در موضوع مورد بحث در نظام حقوقی داخلی می‌تواند منشأ خسارات و آسیب‌های جبران‌ناپذیری باشد. این خسارات ممکن است هم از سوی شرکت‌های داخلی صورت گیرد و هم متأثر از فضای بین‌المللی باشد. به نظر می‌رسد تدوین مقرراتی جامع برای حمایت از داده‌های شخصی، با الگوگرفتن از تجارب موفق منطقه‌ای و بین‌المللی، نظیر GDPR، می‌تواند چارچوبی مناسب و امن برای فعالیت افراد در فضای مجازی فراهم آورد. اهمیت این موضوع آنجا روشن‌تر می‌شود که بدانیم، همان‌طور که در خلال این نوشتار تبیین شد، تمامی استفاده‌های روزمرهٔ افراد از دستگاه‌های هوشمند و برنامه‌های برخط می‌تواند منبعی برای جمع‌آوری و ذخیرهٔ داده باشد و در مواردی مورد استفاده سودآور پردازشگر یا کنترلگر قرار گیرد که اساساً فرد اطلاعی نسبت به آن ندارد. البته در پایان ذکر مجدد این نکته در ارتباط با مقررات‌گذاری داخلی ضروری است که، همان‌طور که بر اهمیت الگوپذیری از تجارب موفق بین‌المللی به‌ویژه GDPR تأکید شد، باید توجه داشت که، هرچند بسیاری از کشورها در قوانین داخلی به پیش‌بینی سازوکاری برای حمایت از حریم خصوصی در فضای مجازی و حفاظت از داده‌ها شخصی دست زده‌اند، با این حال نباید از این موضوع غافل بود که موفقیت مؤثر چنین مقرراتی، با توجه به فراگیری جهانی فضای مجازی، وابسته به گستردگی شمول مقرراتی است که حامی داده‌های شخصی است. اثرگذاری GDPR فارغ از محتوای آن، معطوف به آن است که، با دربرگیری دامنهٔ گسترده‌ای از صلاحیت، امکان وادارکردن شرکت‌های بزرگ پردازشگر یا کنترلگر

مانند گوگل، فیس‌بوک و... برای آن فراهم شده است. این بدان معناست که با توجه به تعداد بسیار قابل توجه کاربران شرکت‌های اصلی مقررات داخلی یک کشور به‌تنهایی نمی‌تواند در این حوزه اثرگذار باشد. از سوی دیگر، روی دیگر فراگیری تجربه‌ای مانند GDPR آن است که به ناگزیر بسیاری از کشورها را که در قوانین داخلی‌شان حامی حریم خصوصی داده نبوده‌اند با خود همراه کرده است. به عبارت دیگر، تدوین مقررات داخلی هماهنگ یا حداقل شکل‌گیری رویه‌های عملی هم‌سو با این مقررات خود نشان از ضرورت فراگیری مقررات یا تبعیت از مقررات فراگیر است.

منابع

۱- احمدی ناطور، زهرا، آقابابایی، حسین، (۱۳۹۵)، «مطالعهٔ تطبیقی جرائم علیه حریم خصوصی در فضای سایبری ایران و آلمان»، رسانه و فرهنگ، شماره‌ی اول، تابستان.

۲- اصلانی، حمیدرضا، (۱۳۸۹)، حقوق فناوری اطلاعات، میزان، چاپ دوم، تهران.

۳- انصاری، باقر، (۱۳۹۲)، «حمایت از حرمت اشخاص در برابر آزادی بیان»، رسانه، شمارهٔ ۳ (پیاپی ۹۱)، تابستان ۱۳۹۲

۴- آماده، مهدی، (۱۳۹۲)، حمایت از حریم خصوصی، نشر دادگستر، چاپ اول، تهران.

۵- باستانی، برومند، (۱۳۸۶)، جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، انتشارات بهنامی، چاپ سوم، تهران.

۶- تقوی‌فرد، محمدتقی، تقوا، محمدرضا، فقیهی، مهدی، جمشیدی، محمدجواد، (۱۳۹۶)، «مقایسه تطبیقی قوانین حمایت از حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب»، فصلنامه مجلس و راهبرد، شماره ۸۹، بهار.

۷- حبیبی، همایون، (۱۳۹۵)، «حق بر حریم خصوصی در شبکه‌های اجتماعی»، فصلنامه تحقیقات حقوقی، شماره ۷۵، پاییز.

۸- رییسی دزکی، لیلا، قاسم‌زاده لیاسی، فلور، (۱۳۹۹)، «چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر»، مجله حقوقی دادگستری، شماره ۱۱۰، تابستان.

۹- زارعیان، داود، واحد، فائزه، (۱۳۹۹)، «بررسی حقوقی رگولاتوری‌های حمایت از داده»، رسانه، شمارهٔ ۱، خرداد.

۱۰- زرکلام، ستار، (۱۳۸۶)، «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیهٔ اروپا)»، مجلهٔ معارف اسلامی و حقوق، شمارهٔ ۲۵، شهریور.

۱۱- صابر نژاد، علی، حسین‌پور، پری، (۱۳۹۶)، «تحلیل حقوقی گونه‌شناسی نقض حریم خصوصی در فضای سایبر»، جستارهای حقوقی عمومی ، شماره ۳ ، زمستان.

۱۲- عبدی‌پور، ابراهیم، (۱۳۹۴)، «رویکرد نظام‌های حقوقی نسبت به نقض حریم خصوصی اطلاعاتی در شبکه‌های اجتماعی مجازی»، فصلنامه پژوهشی تطبیقی حقوق اسلام و غرب، شماره ۳، بهار.

۱۳- فتحی، یونس، شاهمرادی، خیراله، (۱۳۹۶)، «گستره و قلمرو حریم خصوصی در فضای مجازی»، مجله حقوقی دادگستری، شماره ۹۹، پاییز.

۱۴- فرحزادی، علی‌اکبر، ناصر، مهدی، (۱۳۹۸)، «سازوکار جبران جمعی خسارات ناشی از نقض قواعد امنیتی آیین‌نامهٔ عمومی حفاظت از اطلاعات اتحادیهٔ اروپا و امکان‌سنجی اجرای آن در حقوق ایران»، حقوق خصوصی، شمارهٔ ۲، پاییز و زمستان.

۱۵- فروغی، فضل‌الله، برجی، محمدناصر، مصلحی، جواد، (۱۳۹۳)، «مبانی ممنوعیت نقض حریم خصوصی در حقوق ایران و آمریکا»، مجله مطالعات حقوقی دانشگاه شیراز، شماره ۳، پاییز.

۱۶- قبولی درافشان، سید محمدهادی، بختیاروند، مصطفی، آقا محمدی، اکرم، «حق فراموش‌شدن در ترازو: نیاز ناشی از فضای مجازی یا تهدیدی برای آزادی بیان»، فصلنامه پژوهش حقوق عمومی ، شماره ۵۸، بهار ۱۳۹۷

۱۷- نیکویی مهر، نفیسه، حسینی فرد، عاطفه، (۱۳۹۷)، «حفظ حقوق شهروند مجازی در راستای منشور حقوق شهروندی»، پژوهش‌های اخلاقی، شماره ۱، پاییز.

18- Bakhoum Mor et al, (2018), Personal Data in Competition, Consumer Protection and Intellectual Property Law, Springer, ed. 1, Germany

19- Belanger, F., J. S. Hiller, "A Framework for E-government: Privacy Implications", Business Process Management Journal, vol. 12, issue 1, 2006

20- Custers Bart et al, (2019), EU Personal Data Protection in Policy and Practice, Springer, Germany

21- Goddard Michelle, "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact", International Journal of Market Research, Vol. 59, Issue 6, 2017

22- Margetts, H., D. Sutcliffe, "Addressing the Policy Challenges and Opportunities of “Big data", Policy and Internet, vol.5, issue 2, 2013

ISSN: 2783-1329
شماره مجوز انتشار: ۸۷۰۱۹

23- Newman Abraham L., (2008), Protectors of Privacy, Cornell University Press, U.S.

24- Sharma Sanjay, (2020), Data Privacy and GDPR Handbook, Willy, U.S.

25- Sharwood, S., "United Nations Signs Off on 'right to Privacy in the Digital age", The Register, 2013

26- Summer Stuart, (2016), You: For Sale, Elsevier, U.S.

27- Tankard Colin, "What the GDPR means for businesses", Network Security, Volume 2016, Issue 6, 2016

28- The General Data Protection Regulation (GDPR) (EU) 2016/679

29- Von Bar Christian & Clive Eric, (2009), Principles, Definition and Model Rules of European Private Law (DCFR), Sellier European law publishers, Munich

30- Wolters P. T. J., "The security of personal data under the GDPR: a harmonized duty or a shared responsibility?", International Data Privacy Law, Volume 7, Issue 3, August 2017

www.jhvmn.ir
فصلنامه علمی حقوق و مطالعات نوین، دوره ۴، شماره ۱، پیاپی ۱۰، بهار ۱۴۰۲
ISSN: 2783-1329
شماره مجوز انتشار: ۸۷۰۱۹

Protecting personal data; The right of citizens, the duty of governments

Narges Nakhjavani[1]

Abstract

having the widespread use of virtual facilities and the provision of access to people's personal information and data, on the one hand, these data have become a valuable commodity for economic enterprises and governments, which provides them with the possibility of economic or security exploitation in various ways, and on the other hand, It has provided the basis for the invasion of people's privacy, for the simple reason that people may not be aware of the collection of this information about themselves or do not know the reason for the collection of information. The nature of application software in the continuous collection of user data and unannounced uses of this data, along with the need to protect privacy, has made government intervention and regulation in this area inevitable in order to protect the rights of citizens. The present article aims to examine the status of international regulations in this field and the approach of the domestic legal system, considering the protection of this data as a citizen's right and the duty of governments.

keywords: Privacy, personal data, general data protection regulations, protection of personal data.

[1] Doctorate in public law, Faculty of Law, Allameh Tabatabai University, Tehran. (Corresponding Author)
n.nkhjvn@gmail.com