دوفصلنامهٔ حقوق قراردادها و فناوری‌های نوین، دورهٔ اول، شمارهٔ ۱، بهار و تابستان ۱۳۹۹، صفحهٔ ۲۹۷-۳۲۲

مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی

فاطمه قناد[۱] امیره علیقلی[۲]

تاریخ دریافت: ۱۳۹۹/۵/۲۰ تاریخ پذیرش: ۱۳۹۹/۶/۲۷

چکیده

پیشرفت فنّاوری، در کنار مزیت‌های فراوان خود، به‌تنهایی به خسارات و جرایم بسیاری در این عرصه منجر شده است. نقض داده‌های شخصی توجه قانونگذاران و افراد درگیر در این حوزه را بسیار جلب کرده است، چراکه از شروع پیشرفت‌های فنّاورانه تا امروز به‌طور گسترده خسارات و جرایم جبران‌ناپذیری به بار آورده است که قانونگذاران را مجبور به توجه و تصویب قوانین جدید در این راستا کرده است. اگرچه حریم خصوصی از دیرباز در قوانین سنتی نیز مورد حمایت بوده است، داده‌های شخصی که بخشی از حریم خصوصی محسوب می‌شود در فضای وب امروز نیاز به قوانین جدید و مطابق با شرایط جدید دارد؛ ازاین‌رو وجود قوانین مطابق با نیازهای روز همواره مورد توجه بوده و هست.

در این نوشتار، با بررسی مفهوم حریم خصوصی در مقررات اتحادیهٔ اروپا و نظام حقوقی ایران، چنین تحلیل شده که قوانین نیاز به روزآمدی بیشتری نسبت به پیشرفت‌های عصر دیجیتال دارد و باید مفهوم حریم خصوصی و داده‌های شخصی به‌طور مشخص در بطن قوانین معرفی و مورد حمایت قرار گیرد. این درحالی است که در هیچ‌یک از قوانین بررسی‌شدهٔ نظام حقوقی داخلی تعریف جامع و منسجمی از داده‌های شخصی وجود ندارد و این خلأ در قوانین ایران باید بررسی شود. در نهایت تعریفی جامع از دادهٔ شخصی ارائه شده است.

واژگان کلیدی: حریم خصوصی، دادهٔ شخصی، فضای مجازی، مقررهٔ عمومی حمایت از داده‌های شخصی

---

۱. دانشیار و مدیر گروه کارشناسی ارشد حقوق تجارت الکترونیکی، دانشگاه علم و فرهنگ (نویسندهٔ مسئول)؛ ghanad@usc.ac.ir

۲. دانش‌آموختهٔ کارشناسی ارشد حقوق تجارت الکترونیکی، دانشگاه علم و فرهنگ؛ amire.aligholi@gmail.com

مقدمه

در قوانین و مقررات مختلف از حریم خصوصی و داده‌های شخصی تعاریف متفاوتی ارائه شده است. در حقوق بین‌المللی حق حریم خصوصی یکی از حقوق بنیادین حقوق بشر محسوب شده و در مقررات و دستورالعمل‌های مختلف مورد حمایت قرار گرفته است. داده‌های شخصی نیز یکی از ابعاد حریم خصوصی است که در این نوشتار بیشتر این بعد از حریم خصوصی مورد توجه قرار گرفته است.

داده‌های شخصی به هر موردی گفته می‌شود که به‌تنهایی یا در کنار شناسه‌ای دیگر به شناسایی موضوع داده منجر می‌شود. دادهٔ شخصی از مسائل و مواردی است که از دیرباز در قوانین و ادیان و فرهنگ‌های گوناگون مورد توجه قرار گرفته است، اما امروزه با رشد و توسعهٔ فنّاوری و گسترش استفاده از شبکهٔ جهانی وب اطلاعات و داده‌های شخصی افراد بیشتر از گذشته نیاز به حمایت دارد، چراکه دسترسی به این اطلاعات بسیار ساده‌تر از گذشته صورت می‌گیرد و سوءاستفاده از این اطلاعات و دسترسی غیرمجاز به آن به‌مراتب بیشتر است. این روزها، با اتصال هر گوشی تلفن همراه به اینترنت و البته ذخیره‌سازی حجم زیادی از داده‌های شخصی در این ابزارهای فنّاورانه، یکی از مهم‌ترین نگرانی‌های هر کسی افشانشدن این دسته از اطلاعات است. این نگرانی با رعایت برخی نکات ایمنی کاهش خواهد یافت، اما مرور برخی از حمایت‌های قانونی که در این زمینه وجود دارد نیز از نظر روانی مفید است. ضمن این‌که آگاهی از آن نقطهٔ آغاز پیگیری در صورت بزه‌دیده‌شدن در زمینهٔ افشای اطلاعات شخصی خواهد بود.

در این نوشتار، در طی دو بخش بررسی می‌شود که اهمیت داده‌های شخصی در دوران فنّاوری چقدر است و مفهوم این مهم در این دوران دستخوش چه تغییر و تحولاتی شده است؛ ضمن این‌که دیدگاه‌های حمایتی سنتی و نوظهور از داده‌های شخصی نیز بررسی خواهد شد. همچنین، مهم‌ترین رسالت این مقاله بررسی و تبیین تعاریف متفاوت دادهٔ شخصی و حریم خصوصی در متون و قوانین حقوقی ایران و مقررات بین‌المللی است.

۱. مفهوم و اهمیت حریم خصوصی و دیدگاه‌های مربوط به آن

اهمیت و ضرورت حمایت از حریم خصوصی از دیرباز در نظام‌های حقوقی دنیا مورد توجه قرار گرفته است و در مقررات مختلف تعاریف متفاوتی از حریم خصوصی ارائه شده است. با گسترش فنّاوری و پیشرفت استفاده از فضای مجازی اهمیت حریم خصوصی و داده‌های شخصی دوچندان شده است، تا جایی که علاوه‌بر قوانین سنتی، قوانین مدرن نیز به تعریف و تبیین داده‌های شخصی پرداخته‌اند. در نظام حقوقی ایران حریم خصوصی به‌صورت مشخص مورد حمایت قرار نگرفته است، اما به‌طور ضمنی در متن قوانین این حمایت دیده می‌شود، در نظام حقوقی بین‌المللی، اسناد سازمان همکاری اقتصادی و توسعه (OECD)[۱] و مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا (GDPR)[۲] متناسب با پیشرفت‌های فنّاورانه به حمایت از داده‌های شخصی پرداخته‌اند. در این نوشتار مفاهیم حریم خصوصی و داده‌های شخصی در قوانین و مقررات مذکور مورد بررسی قرار خواهد گرفت.

۱ـ۱. مفهوم حریم خصوصی در مقررات ایران

از دیرباز حریم خصوصی در فرهنگ‌ها و قوانین گوناگون بشری مورد حمایت قرار گرفته و یکی از دغدغه‌های قانونگذاران در اعصار مختلف بوده است. در نظام حقوقی ایران حریم خصوصی به‌صورت مشخص حمایت نشده است. حقوق و آزادی‌هایی که تحت عنوان حریم خصوصی حمایت می‌شوند به‌طور ضمنی و در بطن سایر قواعد حقوقی ایران مورد حمایت قرار گرفته‌اند. داده‌های شخصی و حریم خصوصی یکی از حقوق اساسی و بنیادین بشر است که باید از طریق قانون حمایت شود.

قانون اساسی، قانون مجازات اسلامی و قانون آیین دادرسی کیفری در زمرهٔ قوانین و مقرراتی هستند که در نظام حقوقی ایران از حریم خصوصی در فضای سنتی به‌طور ضمنی حمایت کرده‌اند. در قوانین بین‌المللی نیز نخستین مقرره‌گذاری در حمایت از

۱. Organization for Economic Co-operation and Development

۲. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88
ICO, Guide to the General Data Protection Regulation (GDPR), https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

حریم خصوصی از سوی سازمان همکاری اقتصادی و توسعه در دههٔ ۱۹۷۰ آغاز شد. میثاق بین‌المللی حقوق مدنی و سیاسی که دولت ایران نیز به آن ملحق شده است از دیگر منابعی است که صریحاً بر حمایت از حریم خصوصی تأکید دارد. خانه مهم‌ترین مصداق حریم خصوصی در فضای سنتی است. ازاین‌رو دربارهٔ بازرسی از خانه تشریفات خاصی وضع شده است، ازجمله این‌که بازرسی باید با ارائهٔ مجوز قانونی باشد، ضرورت داشته باشد، در صورت امکان در روز انجام شود، با حضور صاحب‌خانه باشد و... . در غیراین صورت، ورود افراد عادی و همچنین مأموران و مقامات غیرقضایی به منزل افراد ممنوع است و متخلفان به مجازات مقرر در قانون محکوم می‌شوند (احمدی ناطور، ۱۳۹۱، ص ۷).

حریم خصوصی از بنیادی‌ترین حقوق اساسی بشر است که تحت‌تأثیر پیشرفت‌های فنّاورانه قرار گرفته است. ظهور فنّاوری‌های جدید سبب شده است که همهٔ آحاد جامعه با دسترسی به بسیاری از وسایل پیشرفته به جمع‌آوری و ضبط و انتشار حجم انبوهی از اطلاعات مربوط به حریم خصوصی افراد اقدام کنند. درواقع، در کنار مزیت‌های گسترده‌ای که این فضا به همراه دارد، استفادهٔ نادرست از آن پیامدهای نامطلوبی را نیز به‌دنبال دارد که یکی از آن‌ها نقض حریم خصوصی افراد با استفاده از این فنّاوری‌ها از سوی برخی اشخاص و سازمان‌ها یا حتی دولت‌هاست که با اهدافی متفاوت صورت می‌گیرد (همان).

قانون اساسی ایران، درحکم مرجع تمامی قوانین، از حریم خصوصی صریحاً حمایت نکرده است، بلکه در برخی اصول این حمایت به‌صورت ضمنی است آن‌هم نه با نام حریم خصوصی، بلکه تحت عناوینی چون حریم خلوت و تنهایی، حریم مکانی، حریم اطلاعات، حریم ارتباطات و حریم جسمانی. در تحلیل چند اصل قانون اساسی همچون اصول ۱۹، ۲۰، ۲۲، ۲۳، ۲۴، ۲۵، ۲۶، ۲۷، ۲۸، ۳۰، ۳۲، ۳۳، ۳۵، ۳۸، ۳۹ و ۴۰ به‌وضوح می‌توان توجه خاص اما ناکافی به مفهوم حریم خصوصی را مشاهده کرد. برخلاف قوانین اساسی کشورهایی که از حریم خصوصی به‌صورت مشخص و در قالب اصل یا اصول خاصی حمایت کرده‌اند، در قانون اساسی ایران اصل خاصی که مشخصاً از حریم خصوصی حمایت کند وجود ندارد. به‌طور کلی، اگر حریم خصوصی را حریم خلوت و

تنهایی، حریم مکانی، حریم اطلاعات، حریم ارتباطات و حریم جسمانی دسته‌بندی کنیم، در قانون اساسی ایران:

۱. داشتن حریم خصوصی حق اساسی شناخته نشده است.

۲. حریم خلوت و تنهایی نه به‌صورت صریح و نه ضمنی حمایت نشده است.

۳. آزادی اطلاعات جز به‌صورت مضیق در اصل ۲۴ در جای دیگری مطرح نشده است. در اصل ۲۵ نیز، بدون تصریح به آزادی ارتباطات، به استثناهای این آزادی اشاره شده و از حریم خصوصی ارتباطات درمورد شایع‌ترین وسایل ارتباطی حمایت شده است. اصل ۲۵ از اصول مهمی است که از حریم خصوصی ارتباطات صریحاً حمایت کرده است.

۴. در دیگر اصول ذکرشده در قانون اساسی نیز به‌صورت ضمنی به حمایت از حریم خصوصی جسمانی و حفظ کرامت انسانی و حفظ مال و مسکن پرداخته شده است (واعظی، ۱۳۸۹، ص ۱۳۸).

در قوانین ایران، کامل‌ترین تعریف از داده‌های شخصی در قانون انتشار و دسترسی آزاد به اطلاعات به این نحو بیان شده است: «اطلاعات شخصی، اطلاعات فردی نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است.»

۱ـ۲ حریم خصوصی در مقررات بین‌المللی

داده‌های شخصی و حریم خصوصی یکی از حقوق اساسی و بنیادین بشر است که باید از طریق قانون حمایت شود. تعاریف متعددی از داده‌های شخصی وجود دارد که یکی از کامل‌ترین آن‌ها در مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا آمده است. در بند ۱ مادهٔ ۴ مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا دادهٔ شخصی تعریف شده است.[۱] این مقرره محدودهٔ داده‌های شخصی را گسترده کرده و چنین بیان می‌کند: «... یک شخص حقیقی قابل شناسایی کسی است که مستقیم یا غیرمستقیم، به‌ویژه با اشاره به یک شناسهٔ خاص مانند نام، شمارهٔ شناسایی، اطلاعات مکان، شناسهٔ آنلاین یا

۱. General Data Protection Regulation, (GDPR), op.cit. and http://www.oecd.org/internet/digital-government/open-government-data.htm
https://gdpr-info.eu

شناسایی یک یا چند عامل و ویژگی فیزیکی، فیزیولوژیکی، ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی قابل شناسایی باشد. این تعریف تمامی جنبه‌های شخصیتی یک فرد را که عامل شناسایی اوست بیان می‌کند. در اسناد سازمان همکاری اقتصادی و توسعه نیز، با وجود تعریف حریم خصوصی، باز هم تعریفی به جامعیت تعریف مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا دیده نمی‌شود اگرچه این سند نیز به حریم خصوصی اهمیت ویژه‌ای می‌دهد.

دستورالعمل‌های سازمان همکاری اقتصادی و توسعه در سال ۱۹۸۰ برای حفاظت از حریم خصوصی و جریان‌های دادهٔ شخصی موافقت کشورهای عضو برای اداره و حفاظت از اطلاعات شخصی را دریافت کرد. دستورالعمل‌ها به علت نگرانی دربارهٔ پیامدهای قوانین حفاظت از داده‌های متناقض یا رقابتی که در پاسخ به روش‌های جدید و خودکار پردازش اطلاعات به‌وجود آمده‌اند ایجاد شده است. دستورالعمل‌ها تأکید دارند که کشورهای عضو سازمان همکاری اقتصادی و توسعه[۱] منافع مشترک در حفاظت از حریم خصوصی و آزادی‌های فردی دارند. درعین‌حال، هدف دیگر این بود که اطمینان حاصل شود که گسترش قوانین حریم خصوصی نباید جریان‌های اطلاعاتی بین مرزها و مزایای اقتصادی و اجتماعی آن‌ها را بیش از حد محدود کند. سازمان همکاری اقتصادی و توسعه، در مواجهه با نگرانی‌های دوگانه از نقض حریم خصوصی به علت استفادهٔ بیشتر از داده‌های شخصی در عصر جدید و خطرهای احتمالی برای اقتصاد جهانی ناشی از محدودیت جریان اطلاعات، یکی از دستورالعمل‌های برجستهٔ خود درجهت حمایت از حریم شخصی و اصول آن را تهیه کرد. تمرکز بر خطرهای احتمالی در حفظ حریم خصوصی با استفاده از فنّاوری اطلاعات و ارتباطات (ICT) برای ذخیره و پردازش اطلاعات شخصی تأثیری بر قانونگذاری در دههٔ ۱۹۷۰ داشت. مراجعات متعدد به کتب و مطالعاتی که در زمینهٔ حریم خصوصی نگاشته شده بود و تمرکز گسترده بر این حق بنیادین بشر به قانونگذاری در این زمینه انجامید.[۲]

۱ـ۳. دیدگاه‌ها و نگرانی‌های مربوط به حریم خصوصی در عصر دیجیتال

۱. ۳۵ کشور عضو سازمان همکاری و توسعهٔ اقتصادی هستند.

۲. OECD (2011). The OECD Privacy Guideline. http://www.oecd.org/sti/ ieconomy/49710223.pdf.

Recitals of General Data Protection Regulation. https://uk.practicallaw.thomsonreuters.com/w0133003?transitionType=Default&contextData=(sc.Default)&firstPage=true, p. 14

در عصر فنّاوری اطلاعات و با توسعهٔ فضای مجاز، حریم خصوصی بیش از هر زمان دیگری در خطر است و دراین‌میان شبکه‌های اجتماعی در گرفتن و جمع‌آوری و استفاده از اطلاعات اشخاص در فضای مجازی وضعیت ممتازی دارند. این شبکه‌ها، با رصدکردن رفتار افراد در شبکه و افزودن این اطلاعات به بانک داده‌های خود، مجموعه‌ای از اطلاعات را جمع‌آوری می‌کنند و از راه داده‌کاوی، پروفایل‌های شخصی برای اعضا می‌سازند که حاوی اطلاعات بسیار زیادی از زندگی خصوصی افراد است. به این ترتیب به حریم خصوصی تعداد بیشتری از مردم جهان نفوذ می‌کند. حساسیت به نقض حریم خصوصی در فضای دیجیتال در سطح بین‌المللی و منطقه‌ای و ملی ایجاد شده، ولی هنوز مقررات کافی برای حفاظت مناسب از حریم خصوصی وجود ندارد. در ایران این فقر قانونی چشمگیرتر است و نیاز به تصویب مقررات حمایت‌کننده از حریم خصوصی و داده‌های شخصی با توجه به اصول موردپذیرش بین‌المللی احساس می‌شود (حبیبی، ۱۳۹۵، ص ۳۹)

حریم خصوصی را می‌توان به دو گروه اطلاعات خصوصی و داده‌های شخصی تقسیم کرد. اطلاعات خصوصی به شیوه‌های جمع‌آوری، ضبط، دسترسی و آزادسازی اطلاعات اشاره دارد. در عصر دیجیتال، تعداد زیادی از سوابق افراد در پایگاه‌های داده وجود دارد. از زمان ظهور سوابق الکترونیکی، حفاظت از اطلاعات خصوصی به یکی از مهم‌ترین مسائل و دغدغه‌های قانونگذاران و کنترل‌کننده‌ها تبدیل شده است. مهم‌ترین قدم در راستای مقرره‌گذاری برای حمایت از این داده‌ها از سوی سازمان همکاری اقتصادی و توسعه در دههٔ ۱۹۷۰ اغاز شد. داده‌های شخصی مربوط به حریم شخصی و فضای خصوصی فرد است؛ این داده‌ها ممکن است با جعل تصاویر یا تصویرسازی با فتوشاپ یا ضبط فیلم و عکس‌برداری در مکان‌های عمومی و خصوصی مورد نقض قرار گیرد (Davidson, 2009, p. 218).

در جامعهٔ امروز، بیشتر مردم فقط نام و نام خانوادگی، جزئیات حساب‌های بانکی و آدرس پستی خود را اطلاعات شخصی می‌دانند. اگرچه این تصور درست است، اما اطلاعات متنوع دیگری هم هست که حفظ آن از اهمیت بسیاری برخوردار است. اگر همهٔ افراد حاضر در فضای مجازی بدانند که تمام اطلاعات آن‌ها در این فضا نظاره و

تمام رفتارها و حرکات آن‌ها دنبال می‌شود برای حریم خصوصی خود و حفظ آن اهمیت بیشتری قائل می‌شوند. این واقعیت ترسناک در عصر امروز وجود دارد که ما در دنیایی شیشه‌ای زندگی می‌کنیم و همه می‌توانند زندگی ما را نظاره کنند. ابعاد مختلف زندگی امروز ما از راه فضای وب و هوش مصنوعی کنترل می‌شود و تأثیر پردازش اطلاعات شخصی بر اقتصاد و سیاست باورناپذیر است. نقض داده‌های شخصی ممکن است تأثیرات جبران‌ناپذیر اجتماعی به دنبال داشته باشد. به همین علت مشاهده می‌شود که مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا نقض داده‌های شخصی را پیش‌بینی و حمایت می‌کند: «نقض داده‌های شخصی به معنای نقض امنیت است که منجر به نابودی، ازدست‌دادن، تغییرات غیرقانونی و افشای غیرمجاز یا دسترسی به اطلاعات شخصی فرد می‌شود. این نقض ممکن است در نتیجهٔ اعمالی که سهواً یا عمداً رخ می‌دهد صورت پذیرد. این بدان معنا است که نقض در اینجا آثاری به‌مراتب بیشتر از صرف ازدست‌دادن داده‌های شخصی دارد.»

افراد در طول روز مدام درحال ارائهٔ اطلاعات خصوصی خود به کسانی هستند که هیچ تعهدی برای ارائهٔ اطلاعات شفاف از خود ندارند. افراد جامعه دائماً درحال خودافشایی به حکومت‌ها هستند. حکومت‌های امروز خیلی راحت می‌توانند به بهانهٔ ارائه خدمات به اطلاعات خصوصی افراد دسترسی داشته باشند. آن‌ها می‌توانند از طریق برنامه‌هایی که خودشان تعیین می‌کنند حریم خصوصی افراد را نقض کنند. مواردی همچون تعیین اجباری هویت، آزمایش مواد مخدر، تجسس بدنی و شخصی یا جست‌وجو در خانه، حفظ و پردازش مشخصات افراد در پایگاه‌های داده، انجام آزمایش‌های ژنتیک و دروغ‌سنجی که نوعی تفتیش عقیده به‌شمار می‌رود از جملهٔ این برنامه‌ها است. به عبارت دیگر، افراد مجبورند اطلاعاتی از خود به دولت بدهند، اما گرفتن اطلاعات از دولت به این آسانی نیست (احمدی ناطور، ۱۳۹۱).

به‌رغم آنچه بیان شد، ضرورت تدوین قانون خاص برای رعایت حریم خصوصی در ایران احساس می‌شود، چراکه قانون اساسی به‌صورت کلی و منشور حقوق شهروندی و موارد دیگر به‌صورت ضمنی و غیرصریح به این موضوع پرداخته‌اند و تعیین جزئیات آن بر عهدهٔ قانون عادی گذاشته شده تا در آن به حد و حدود این حریم و جنبه‌های

مختلف آن و همچنین تعیین مجازات‌ها توجه شود. شایان ذکر است، قوانین تجارت الکترونیکی و جرایم رایانه‌ای دو قانون مهمی است که به‌منزلهٔ نقطهٔ عطف قانونگذاری در ایران مورد توجه قرار گرفته و تحولات این دوره را تا حدودی مدنظر قرار داده است. دادهٔ شخصی تا حدودی در این قوانین تعریف شده است. همان‌طور که در اسناد سازمان همکاری اقتصادی و توسعه و مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا تعریف دادهٔ شخصی بررسی و ارائه شده است، در قوانین ایران نیز باید تعریف دادهٔ شخصی کامل شود و شاید بتوان گفت تعریف ارائه‌شده در مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا کامل‌ترین و جامع‌ترین تعریف از دادهٔ شخصی است. این مقرره محدودهٔ داده‌های شخصی را گسترده کرده و اطلاعاتی چون نام، شمارهٔ شناسایی، اطلاعات مکان، شناسهٔ آنلاین یا شناسایی یک یا چند عامل و ویژگی فیزیکی، فیزیولوژیکی، ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی را که با استفاده از آن بتوان شخص را شناسایی کرد از موارد دادهٔ شخصی عنوان می‌کند. این درحالی است که قانون تجارت الکترونیکی ایران از دادهٔ شخصی با عنوان داده‌پیام یاد می‌کند و آن را این‌گونه تعریف می‌کند: «داده‌پیام هرنمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فنّاوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.» نکتهٔ حائز اهمیت در دوران حاضر این است که شرکت‌های بزرگ و پلتفرم‌هایی چون فیسبوک یا اینستاگرام و گوگل و امثال آن‌ها با استفاده از داده‌های شخصی به کسب درآمد می‌پردازند و از آن‌ها برای تبلیغات استفاده می‌شود. این تبلیغات صرفاً جنبهٔ تجاری ندارد و گاهی بر زندگی سیاسی و اجتماعی افراد نیز تأثیرات عمده‌ای می‌گذارد که از چشم همگان پنهان می‌ماند، اما تمامی زندگی اشخاص را تحت تأثیر قرار می‌دهد.

۱ـ۴. نقش فضای مجازی و عصر دیجیتال در نقض داده‌های شخصی

اگرچه دوران برده‌داری به اتمام رسیده است، می‌توان گفت فضای مجازی و کنترل‌کنندگان این فضا همچون حاکمانی رفتار می‌کنند که کاربران را بردهٔ خویش می‌سازند. در این دنیای مدرن فقط با واردکردن برخی از اطلاعات شخصی می‌توان حکم بردگی خود را صادر کرد. البته با این تفاوت که چون کاربران از واقعیات و پشت پرده‌های آن اگاهی ندارند، با کمال رضایت این کار را انجام می‌دهند چراکه مزیت‌ها و جذابیت‌های

این فضا چنان زیاد است که می‌توان گفت اشخاص را ناخوداگاه وادار به استفاده از آن می‌کند. چنان‌که امروزه مشاهده می‌کنیم، طیف گسترده‌ای از اشخاص در سنین متفاوت، از کودک و نوجوان تا سالمند، را مجذوب خود کرده است. بنابراین اگر فضای مجازی را یک ملت مستقل درنظر بگیریم، نیاز به حکومتی مستقل و البته دموکراسی‌مآبانه دارد تا بتواند به این فضا نظم بخشد و آن را کنترل کند.

امروزه فضای مجازی تجاوز و تعدی به حریم خصوصی اشخاص حقیقی را که از بنیادی‌ترین و اساسی‌ترین حقوق بشری تلقی می‌شود و با شخصیت افراد ارتباط تنگاتنگ دارد بیش‌ازپیش آسان کرده است؛ به‌گونه‌ای که مجرمان در اقصانقاط جهان، فارغ از مرزهای جغرافیایی، حق تنهابودن و با خود بودن و به دور از چشم و نگاه کنترل‌کنندهٔ دیگران و رها از تفتیش و تجسس دیگران زیستن انسان را مورد تعرض قرار می‌دهند. اگر پیش از ظهور فنّاوری رایانه‌ای توانایی ورود به حریم خصوصی اشخاص و سرقت اطلاعات محدود بود، با ظهور آن امکان طرح‌ریزی و هتک حریم خصوصی و سرقت اطلاعات سری و خصوصی اشخاص فراهم شد که پیش از آن تصورش هم نمی‌رفت. همچنین، اگر پیش از این جاسوسان اطلاعات با مشکلاتی مواجه بودند و چندان امیدی به اقدامات مجرمانهٔ خود نداشتند، این سیستم‌ها امکاناتی فراهم کرده‌اند که در کمترین زمان ممکن و با دقت و وضوح بسیار بالا اطلاعات سری و غیرسری موردنظر خود را به‌دست آورند. اگر شنود و استراق‌سمع فقط این مفهوم را داشت که باید شخصی پنهان در جایی یا با تماسی تلفنی اطلاعات دیگران را کسب کند و درواقع فقط از این طریق بود که مجرمان می‌توانستند به آنچه از فعل مجرمانهٔ خود دنبال می‌کردند برسند، سیستم‌های رایانه‌ای این امکان را فراهم آورده که، در ورای مرزها و اقصانقاط جهان، اطلاعات دیگران را بدون این‌که خودشان متوجه شوند سرقت کنند و ارزش ذاتی آن را از بین ببرند و از حالت خصوصی و سری‌بودن خارج کنند. رایانه همچون تیغی است که منحرفان اجتماعی از لبهٔ تیز آن علیه بشریت استفاده می‌کنند (فتحی و شاهمرادی، ۱۳۹۶، ص ۲۳۵)

کشورهای پیشرفته سال‌هاست به فکر نظم‌بخشیدن به این فضا هستند و به‌مراتب قوانین روزآمدتری را نیز تصویب و اجرا نموده‌اند تا جنبه‌های مختلف آن را تحت

حاکمیت و کنترل درآورند، از جمله حریم خصوصی اشخاص که بخش قابل‌ملاحظه و اساسی در این فضاست. همان‌طور که بیان شد، از سال‌های ۱۹۷۰ تا کنون، سازمان همکاری اقتصادی و توسعه و معاهدات و دستورالعمل‌های اتحادیهٔ اروپایی این مهم را مد نظر قرار داده و قوانین متنوعی در این زمینه به تصویب رسانده‌اند تا به نسخهٔ پیشرفته و تکامل‌یافتهٔ قوانین، یعنی مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا، دست یافته‌اند.

در دوران مدرن، با رشد تفکرات انسان‌گرایانه، فرد اهمیت می‌یابد و همین موضوع خود را در حریم خصوصی نشان می‌دهد. حال توجه به این نکته جالب و ضروری است که همین فرد تأثیرگذارترین عنصر در فضای مجازی است. فرد است که به اینترنت به‌مثابهٔ کاربر آن هویت می‌بخشد. این موضوع به‌ویژه در سال‌های جدید و با ظهور شبکه‌های اجتماعی شکل تازه‌ای به خود گرفته است، چون در شبکهٔ اجتماعی، آن که در مرکز توجه است همین کاربر یا به‌عبارتی فرد است. اوست که تولید محتوا می‌کند، نظر می‌دهد و جریان می‌سازد. ازاین‌روست که گفته می‌شود حریم خصوصی با فضای مجازی و شبکه‌های اجتماعی گره خورده است، بنابراین باید جهت جلوگیری از نقض حریم خصوصی در فضای اینترنت به بسترهای مناسب پرداخته شود (همان).

رفتار کاربران نیز نقش مهمی دراین‌میان دارد تا جایی که برخی بر این باورند که رفتار کاربران این فضا به‌مراتب اهمیت بیشتری از قانونگذاری در این عرصه دارد. اولین مشکل به رفتار کاربران مربوط می‌شود که بسیاری از اوقات بدون آگاهی از گسترهٔ عمل خود دست به انتشار عمومی یا نیمه‌عمومی اطلاعاتی می‌زنند که به‌طور طبیعی جزئی از اطلاعات شخصی و خصوصی به‌شمار می‌رود. این رفتار غیرمحتاطانه ممکن است ناشی از بی‌توجهی به ویژگی‌های شبکه‌های اجتماعی و اینترنت باشد. درواقع، بسیاری از استفاده‌کنندگان از شبکه‌ها، با قیاس ارتباطات رو در رو یا مخابراتی مانند تلفن، تصور می‌کنند که آنچه در ارتباطات دو یا چندجانبه در اینترنت به اشتراک گذاشته شده است محرمانگی خود را حفظ خواهد کرد. حال آن‌که ماهیت ارتباطات در این شبکه‌ها متفاوت است و چنین پیش‌فرضی از ابتدا نادرست است. شاید به همین علت باشد که برخی نویسندگان بر این نظرند که قانونگذاران بیش از آن‌که وقت خود را صرف تدوین قوانین

حفاظت از حریم خصوصی کنند باید تلاش کنند تا استفاده‌کنندگان به این ویژگی شبکه‌های اجتماعی پی ببرند. البته مسئولان شبکه‌ها بی‌تقصیر نیستند؛ آن‌ها بسیاری اوقات عامدانه و برای این‌که شبکهٔ اجتماعی گسترش و تأثیر بیشتری پیدا کند سعی بر این دارند که اطلاعات حتی‌المقدور به شکلی عمومی منتشر شود؛ بنابراین شبکه‌ها را طوری طراحی می‌کنند که اطلاعات عمومی باشد، بنابراین کاربر باید به اطلاعاتی که افشا می‌کند و در اختیار عموم قرار می‌دهد توجه داشته باشد. گاه لازم است کاربران با انجام تغییرات در تنظیمات پیش‌فرض شبکه از حریم خصوصی خود حفاظت کنند (Walther, 2011, p. 3).

در آخر این گفتار گفتنی است که مفهوم حریم خصوصی در فضای سنتی و فضای مجازی به سبب تفاوت این دو فضا تا حدودی با یکدیگر متفاوت است، اگرچه اشتراکاتی نیز با یکدیگر دارند. در فضای سنتی اموری همچون اطلاعات شخصی مانند نام، نام خانوادگی، شمارهٔ شناسنامه، کد ملی، آدرس پستی، اطلاعات شغلی و تحصیلی از جمله داده‌های شخصی به‌شمار می‌رود و برخی از این اطلاعات به انضمام آدرس پست الکترونیکی، آدرس (IP) سیستم شخص و هر آنچه در دنیای دیجیتال شخص را قابل‌شناسایی کند از داده‌های شخصی فضای مجازی محسوب می‌شود. لذا شیوهٔ قانونگذاری باید منطبق بر مبنای تعریف ارائه‌شده قرار گیرد و از آن حمایت کند.

۲. انواع حمایت از حریم خصوصی و داده‌های شخصی

فضای سایبری، همانند فضای حقیقی، تهدیدها و آسیب‌پذیری‌هایی دارد که انسان در برخورد با آن شرایطی را برای مصونیت در یک چرخهٔ دائمی شکل می‌دهد. فضای سایبری، هم از آن جهت که همهٔ امور آدمی را دربر می‌گیرد و هم از آن جهت که مبانی انسان‌شناختی فضای تولید فنّاوری و محتوا را دربر گرفته، مخاطراتی را متوجه انسان و جامعه می‌کند. فضای جدید درحال دربرگرفتن همهٔ شئون زندگی آدمی از تلاش و ادارهٔ خانواده و محیط زندگی، تربیت فرزند و حتی فکرکردن را دربر می‌گیرد.

در این فضا، همانند فضای حقیقی، تأمین امنیت کاربران و صیانت از آن‌ها مورد توجه قرار گرفته و برخی از آموزه‌های عمومی تأمین امنیت در این محیط به‌کار می‌رود. اما، به علت ماهیت متفاوت فضای مجازی از فضای مادی، تأمین امنیت و پیشگیری از

جرایم ارتکابی در فضای جدید شیوه‌ها و فنون خاصی را می‌طلبد که باید دقیق‌تر بررسی شود.

با توجه به رویکرد کلی مقابله با جرایم که در دهه‌های اخیر شاهد تحولات شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد: اقدامات کیفری و غیر کیفری.

در زمینهٔ اقدامات کیفری سعی می‌شود، از طریق جرم‌انگاری هنجارشکنی‌ها و سوءاستفاده‌های جدید یا تجدیدنظر در قوانین کیفری گذشته، رعب بیشتری در مجرمان بالقوه یا مکرر ایجاد شود تا از ارتکاب جرم باز داشته شوند. حال آن‌که در جرایم الکترونیکی بهتر است از تدابیر مسئولیت مدنی به‌جای مسئولیت کیفری استفاده شود.

در زمینهٔ اقدامات غیرکیفری نیز سعی می‌شود با اعمال تدابیری همچون تدابیر نظارتی، تدابیر صدور مجوز، استفاده از ابزارهای ناشناس‌کننده و رمزگذاری، به‌کارگیری سیستم‌های امنیتی مناسب و به‌روز، پرهیز از رفتارهای پرخطر و حضور نیروهای حفاظتی تا حد ممکن حریم خصوصی افراد محفوظ بماند. در ایران، از سال ۱۳۸۱، واحدی تخصصی به نام واحد مبارزه با جرایم رایانه‌ای در پلیس آگاهی شکل گرفته و گشت اینترنتی پلیس از اواخر سال ۱۳۸۵ وارد فاز اجرایی شده است. این گشت قصد نفوذ به حریم خصوصی افراد را ندارد و در حالت کلی فقط بر بخش عمومی مثل فضای مجازی نظارت می‌کند. در اوایل بهمن ۱۳۸۹ نیز واحد پلیس فتا برای حضور فعال پلیس در فضای مجازی در ناجا تشکیل شد تا با نظارت کافی در فضای مجازی از اشخاص حقیقی و داده‌های شخصی افراد حمایت کند (احمدی ناطور، ۱۳۹۱، ص ۳۲)

اینترنت گسترشی افسارگسیخته یافته، اما ملاحظات آن نادیده گرفته شده است. جهانی‌سازی خود یکی از عوامل گسترش فنّاوری اطلاعات بوده است. مشکل از آن‌جا ناشی می‌شود که اینترنت از ابتدا با هدف بهره‌برداری نظامی و کنترل خارجی ابداع شده بود؛ حتی کسانی که مدافع توسعهٔ اینترنت هستند بر این باورند که زمانی اینترنت به ظرفیت کامل خود خواهد رسید و قواعد مسلمی بر آن حاکم خواهد شد (Davidson, 2009, p. 2)

ارتباط تنگاتنگ جرایم سایبری با استفاده از اطلاعات شخصی و محرمانهٔ حریم خصوصی اشخاص، به‌طور مستقیم و غیرمستقیم، آماج فعالیت‌های غیرقانونی قرار

می‌گیرد. بنابراین، اتخاذ راهکارهای پیشگیرانهٔ مستمر و روزآمد در این خصوص از مهم‌ترین پیش‌نیازهای توسعه در جامعهٔ اطلاعاتی است. اگرچه فنّاوری اطلاعات معمولاً یکی از عمده‌ترین علل نقض حریم خصوصی تلقی می‌شود، راه‌های گوناگونی نیز وجود دارد که از طریق آن‌ها خودِ فنّاوری از محرمانگی و پیشگیری از نقض آن حمایت کند. امروزه رهنمودها و شیوه‌های محافظت از حریم خصوصی که به روش‌های علمی طراحی شده است مورد استفاده قرار می‌گیرد. این امکانات طیف گسترده‌ای از تمهیدات و راهکارها را دربر می‌گیرد، از روش‌شناسی‌های طراحی‌شده بر مبنای اطلاع‌رسانی اخلاقی تا رمزنگاری به‌منظور محافظت از اطلاعات شخصی در مقابل استفادهٔ غیرمجاز (رنجبران، ۱۳۹۱، ص ۸۹)

در عین حالی که این فنّاوری‌ها فواید و منافع بسیاری را برای زندگی بشر به ارمغان آورده است، استفادهٔ نادرست از آن‌ها پیامدهای نامطلوبی همچون نقض حریم خصوصی افراد را نیز در پی داشته است که به دست برخی اشخاص و سازمان‌ها و حتی دولت‌ها با اهداف مختلف صورت می‌گیرد. بنابراین، با توجه به تهدیدهای فزاینده‌ای که از سوی افراد عادی و بخش خصوصی و دولت علیه حریم خصوصی وجود دارد، ضرورت حمایت از اشخاص و حریم داده‌های خصوصی افراد، به‌منزلهٔ یکی از جلوه‌های اصلی حریم خصوصی، در عصر حاضر بیش‌ازپیش احساس می‌شود.

از جمله موارد ضروری در حفظ حریم خصوصی، ارتقای سطح فرهنگی جامعه از طریق آموزش برای صیانت خود افراد از حریم خصوصی به‌ویژه در قبال فنّاوری‌های نوین، یاری‌جستن از مبانی اعتقادی در کاهش تعرض به حقوق دیگران، استفاده از روش‌های پیشگیری و قوانین جامع و گسترده و نهایتاً حمایت‌های کیفری برای اعمال اهداف مجازات در جامعه است. هرچند در برخی موارد ضمانت اجراهای غیرکیفری مؤثرتر عمل می‌کند، در برخی موارد مهم حمایت از حریم خصوصی مستلزم حمایت کیفری است. البته براساس میزان اهمیت حقی که مورد تعرض قرار گرفته و درجهٔ تهدیدی که از ناحیهٔ عوامل مختلف متصور است، واکنش حمایتی نیز متفاوت خواهد بود. نکتهٔ مهم این است که استفاده از راهکارهای کیفری درحکم آخرین راهکار نیز مقصود را به‌طور کامل تأمین نمی‌کند و نقش آن محدود است. به‌نظر می‌رسد این جنبه

از حقوق با اتخاذ رویکردی متعادل و استفادهٔ کمینه از آن در چارچوب اصل ضرورت و فرعی‌بودن، در کنار دیگر حمایت‌های حقوقی، قادر به تعامل با حقوق و آزادی‌های عمومی و خصوصی از جمله حریم خصوصی باشد (احمدی ناطور، همان، ص ۲۸)

در ایران نیز شورای عالی فضای مجازی طی حکمی از سوی مقام معظم رهبری تأسیس شد که رؤسای قوا و برخی دیگر از مسئولان نظام در آن عضوند. مسئولیتی که به عهدهٔ این نهاد گذاشته شده است ناشی از خلئی بود که در مسئلهٔ فضای مجازی و گسترش آن درجامعه و نفوذ آن در زندگی شخصی و اجتماعی افراد احساس می‌شد. مقام رهبری طی حکمی علت تشکیل شورا را بیان کردند: «گسترش فزایندهٔ فنّاوری‌های اطلاعاتی و ارتباطاتی به‌ویژه شبکهٔ جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی و لزوم سرمایه‌گذاری وسیع و هدفمند در جهت بهره‌گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه‌جانبهٔ کشور و ارائهٔ خدمات گسترده و مفید به اقشار گوناگون مردم؛ همچنین ضرورت برنامه‌ریزی و هماهنگی مستمر به‌منظور صیانت از آسیب‌های ناشی از آن اقتضا می‌کند که نقطهٔ کانونی متمرکزی برای سیاست‌گذاری، تصمیم‌گیری و هماهنگی در فضای مجازی کشور به‌وجود آید.» در ایران، تا کنون موضوعات مختلفی پیرامون جرایم رایانه‌ای در بخش حقوق جزای عمومی و اختصاصی مورد مطالعه قرار گرفته است که صرفاً به حیطهٔ جرایم رایانه‌ای یا بررسی نقش فنّاوری اطلاعات و ارتباطات در ارتکاب جرایم یا نقش این فنّاوری در پیشگیری از بزهکاری می‌پردازد و به سایر ناهنجاری‌های جامعهٔ اطلاعاتی از جمله تأثیر آن در نقض حریم خصوصی کمتر توجه می‌کند (احمدی، همان، ص ۷۵).

«مهم‌ترین عواملی که امروزه حریم خصوصی اشخاص به‌ویژه حریم خصوصی اطلاعاتی ایشان را به چالش کشیده است عبارت‌اند از:

۱. اینترنت

۲. توسعهٔ ظرفیت کامپیوترهای شخصی در انباشت و پردازش داده‌ها

۳. پایش مداوم و گستردهٔ شهروندان در اماکن عمومی (مثل دوربین‌های مداربستهٔ پلیس) و بعضاً خصوصی یا کنترل صحت و سقم اظهارات ایشان از طریق نرم‌افزارهای

دروغ‌سنج یا شنود مکالمات تلفنی ایشان یا کارگذاشتن میکروفن‌های مخفی برای کنترل مکالماتشان

۴. پایش جغرافیایی کاربران اینترنت سیار (مثل تلفن همراه)

۵. پیشرفت چشمگیر دانش‌های مرتبط با تشخیص هویت و ویژگی‌های شخصی(DNA) با شناسایی شخصیت از روی شبکیهٔ چشم، صدا، یک تار مو، دندان و...» (محسنی، ۱۳۹۶، ص ۳۲۶)

هیچ‌یک از افراد جامعه امروز نمی‌تواند ادعا کند که از هیچ‌کدام از موارد مذکور استفاده نکرده و حریم خصوصی وی حفظ شده یا داده‌ای از او انتشار نمی‌یابد، چراکه بسیاری از کارهای اشخاص از طریق اینترنت و در بستر اینترنت انجام می‌گیرد. بنابراین به‌ناچار باید پذیرفت که داده همهٔ اشخاص در این فضا در گردش است و برای حفظ آن و حراست از آن باید چاره‌ای اندیشید.

استفاده از فنّاوری اطلاعات و ارتباطات امروزه نه تفنن و انتخاب، بلکه نیازی حیاتی و تحمیل‌شونده در مسیر رشد و پیشرفت است. بدون برقراری نظامی دقیق و قاعده‌مند در باب حمایت از داده‌های شخصی، نه‌تنها توسعه و گسترش ابزارهای اطلاعاتی و ارتباطاتی نوین در درون اجتماع با کندی مواجه خواهد شد و از این رهگذر عقب‌ماندگی و توسعه‌نیافتگی اقتصادی، اجتماعی، فرهنگی و علمی را از درون به جامعه تحمیل خواهد کرد، بلکه با توجه به نیاز کشور به تبادل اطلاعاتی و علمی با جوامع پیشرفته، که خود ناشی از جایگاه نه‌چندان مناسب علمی کشور در رده‌بندی جهانی است، جریان اطلاعات از جوامع پیشرفته به داخل کشور با خطر جدی مواجه خواهد شد و تحریم اطلاعاتی کشور را در بلندمدت به دنبال خواهد داشت.[1] صرف‌نظر از مبانی نظری قابل‌ارائه در باب حمایت از داده‌ها، تردیدی نیست که حمایتی معقول و پذیرفتنی فواید علمی فراوانی به دنبال خواهد داشت و نبود آن ممکن است مشکلات بغرنجی برای جامعه در مسیر توسعه و پیشرفت در پی داشته باشد. همچنین، با عنایت به اهمیت حیاتی و نقش کلیدی چنین حمایتی، حاکمیت در جایگاه حافظ و نگهبان منافع اجتماع ناگزیر است که در این عرصه خود ابتکار عمل را به دست گیرد و علاوه‌بر قاعده‌گذاری و تبیین حداقل هنجارهای

۱. کاری که هم‌اکنون نیز از سوی برخی سایت‌های فرهنگی یا علمی نسبت به ایران اعمال می‌شود.

لازم‌الرعایه از سوی کاربران و به‌طور کلی شهروندان، نظارت بر حسن اجرای قانون و اعمال ضمانت اجراهای قانونی مناسب را بر عهده گیرد. البته این امر به هیچ وجه نافی امکان پیگیری شهروندان دربارهٔ حقوق تضییع‌شده‌شان نخواهد بود. درنتیجه، واگذاردن امری حیاتی و کلیدی نظیر حریم خصوصی شهروندان به حوزهٔ اخلاق و اکتفاکردن به ضمانت اجراهای اخلاقی و مبتنی بر اقناع درونی ایشان و صرف‌نظرکردن از ضمانت اجراهای بیرونی و حقوقی، با لحاظ طبع سودجو و زیاده‌خواه نوع بشر، عواقب وخیمی برای اجتماع به دنبال خواهد داشت. البته این سخن به هیچ وجه به معنای نفی فایدهٔ استفاده از ابزارهای اقناعی در کنار ابزارهای حقوقی و مبتنی بر اجبار نیست، بلکه برعکس اتخاذ چنین تدابیری موفقیت هرچه بیشتر در این حوزه را به همراه دارد. از سوی دیگر، فقدان حمایت کافی و معقول در این حوزه ممکن است به اتخاذ تدابیر احتیاطی و منع‌کنندهٔ جریان آزاد اطلاعات از سایر کشورها به ایران منجر شود و در نتیجه نوعی تحریم اطلاعاتی را برای کشور به دنبال داشته باشد (محسنی، همان، ص ۱۱۳)

ارتباط تلفنی متداول‌ترین راه ارتباطی اشخاص در جامعه است که روزانه با تلفن‌های ثابت و همراه انجام می‌شود. ازاین‌رو بیشترین حساسیت و نگرانی مربوط به مکالمات تلفنی است. استراق‌سمع و کنترل مکالمات تلفنی و سیگنال‌های رادیویی از رایج‌ترین موارد نقض حریم خصوصی ارتباطی است. پیشرفت‌های فنّاوری از مهم‌ترین عواملی است که شنود و رهگیری تلفن‌های معمولی، همراه و سلولی، کانال‌های رادیویی زمینی یا ماهواره‌ای و... را ممکن و تسهیل می‌کند. با گسترش استفاده از رایانه برای تولید و نگه‌داری و انتقال انواع داده‌ها که شامل داده‌های شخصی نیز می‌شود، این نگرانی ایجاد شده است که داده‌های مذکور از راه‌های گوناگون در اختیار دیگران قرار گیرد و اطلاعات شخصی افراد افشا شود. علاوه‌براین، استفادهٔ روزافزون از اینترنت و کارکردهای گوناگون آن سبب شده است که اینترنت رقیب جدی برای وسایل سنتی ارتباط از راه دور باشد و تحول مهمی در شکل و سرعت ارتباطات شخصی رخ دهد. امروزه هرکسی می‌تواند با استفاده از پست الکترونیک پیامی را به دیگری ارسال کند. پست الکترونیک این ظرفیت را دارد که جایگزین بسیاری از روش‌های خدمات پست سنتی و تلفن شود، ولی استفاده از این شیوهٔ جدید به‌طور طبیعی در معرض رهگیری و نظارت دیگران قرار دارد،

به‌طوری‌که شخص دیگری غیر از دریافت‌کنندهٔ پیام می‌تواند به آن پیام دسترسی پیدا کند و از مفاد آن اطلاع یابد (همان، ص ۱۸۵)

«در مجموع، ارائه‌دهندگان خدمات ارتباطات از راه دور ممکن است سه دسته از اطلاعات شخصی کاربران را جمع‌آوری یا رهگیری کنند:

۱. داده‌هایی که در زمان درخواست اشتراک در شبکه در اختیار ارائه‌دهندگان خدمات ارتباطات از راه دور قرار می‌گیرد، نظیر نام، نشانی و سایر مشخصات مشترک.

۲. داده‌هایی که در زمان برقراری تماس قابل جمع‌آوری یا رهگیری است، نظیر شماره‌هایی که کاربر با آن‌ها تماس می‌گیرد و مدت زمان مکالمات.

۳. محتوای ارتباطی که برقرار شده است اعم از صوت، متن یا تصویر.» (تبار، ۱۳۹۱، ص ۴۸)

در قانون تجارت الکترونیکی داده‌پیام این‌گونه تعریف شده است:

«داده‌پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فنّاوری جدید اطلاعات، تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.»

اصولاً در هر ارتباط چهار مؤلفهٔ اصلی وجود دارد: فرستنده، گیرنده، پیام و محیط ارتباطی. در حوزهٔ فنّاوری اطلاعات و ارتباطات بستر انتقال داده از فرستنده به گیرنده رسانه‌های ارتباطی است. فرستنده و گیرنده ماشین‌های الکترونیکی و کامپیوترها هستند. محیط ارتباطی و رسانه‌های ارتباطی نیز تنوع زیادی دارند: سیم، کابل، فیبر نوری، امواج الکترومغناطیسی، ماهواره و... رسانه‌های جابه‌جاکنندهٔ داده‌ها در بستر مبادلات الکترونیکی هستند. برای فنّاوری اطلاعات و ارتباطات تعاریف متفاوتی ارائه شده است. با توجه به تعاریف موجود می‌توان گفت فنّاوری اطلاعات و ارتباطات عبارت است از هرگونه عملیات اعم از مطالعه، طراحی، تولید، جمع‌آوری، پردازش، ذخیره‌سازی و... بر روی اطلاعات و تبادل، توسعه، مدیریت و پشتیبانی و خروجی اطلاعات به‌وسیلهٔ ارتباطات، همگام با پیشرفت‌های نرم‌افزاری و سخت‌افزاری. گرچه فنّاوری اطلاعات و ارتباطات به‌سرعت در جوامع درحال فراگیرشدن است و مزیت‌های زیادی را برای جامعه دارد، توسعه و بهره‌برداری از آن به‌نوبهٔ خود در حملات گسترده به رایانه‌ها و اعمال خرابکارانه‌ای همچون هک و کرک سایت‌ها بی‌تأثیر نیست. این عملیات با اندیشه‌های

سوء فعالیت‌های مجرمانهٔ مجازی خطرناکی را به دنبال خواهد داشت (نوحه‌خوان، ۱۳۹۱، ص ۱۱۴)

یکی از بحث‌های عمده در تجارت الکترونیکی بحث حمایت از داده‌های شخصی است. اطلاعات همواره در تجارت نقش بسیار مهمی دارد. بازاریابی، تعیین زمان و مکان خرید و فروش اجناس و تمامی فعالیت‌های مرتبط با تجارت رابطهٔ 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 حمایت کافی هستند انتقال نمی‌دهند و همان‌طور که پیش‌تر اشاره شد، این امر می‌تواند باعث تحریم اطلاعاتی و کاهش توان بازیابی و ارزیابی‌های دیگر تجار در کشورهای تحت تحریم اطلاعاتی شود. حمایت از داده‌های شخصی حتی در تجارت‌های داخلی نیز حائز اهمیت است.

قانونگذار در مادهٔ ۱ قانون جرایم رایانه‌ای و چند ماده از قانون تجارت الکترونیکی به بحث حمایت از داده‌ها پرداخته است. مادهٔ ۱ قانون جرایم رایانه‌ای در زمینهٔ حمایت از داده‌ها چنین مقرر می‌دارد: «هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیلهٔ تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.» این ماده، با هدف حمایت همه‌جانبه از اقدام اشخاص در اتخاذ تدابیر امنیتی برای سیستم یا داده‌های خود، دسترسی غیرمجاز را به‌صورت ساده جرم‌انگاری کرده است. ازآنجاکه هکرها و کرکرها دارای امکانات‌اند و جزای نقدی صرف قدرت پیشگیری ندارد، مجازات حبس نیز پیش‌بینی شده است که مسئولیت کیفری در چنین قوانینی از دیدگاه برخی مثبت و برخی دیگر منفی و قابل رد است. پیش‌تر دربارهٔ موافقان و مخالفان مجازات کیفری گفته شد.

در قانون تجارت الکترونیکی مصوب ۱۳۸۲ نیز قواعدی درخصوص حمایت از حریم خصوصی اطلاعات شخصی در فضای مجازی و محیط اینترنتی پیش‌بینی شده است و قانونگذار فصل سوم از باب سوم این قانون (مواد ۵۸ تا ۶۱) را به حمایت از داده‌پیام‌های شخصی اختصاص داده است. در مادهٔ ۵۸ این قانون، قانونگذار ذخیره و

پردازش و یا توزیع داده‌پیام‌های شخصی مبیّن ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده‌پیام‌های راجع‌به وضعیت جسمانی، روانی یا جنسی اشخاص را بدون رضایت صریح آن‌ها غیرقانونی می‌داند.

مادهٔ ۵۹ قانون مورد بحث ذخیره و پردازش و توزیع داده‌پیام‌های شخصی در بستر مبادلات الکترونیکی را در صورت رضایت اشخاص، به شرط آن‌که محتوای داده‌پیام موافق قوانین مصوب مجلس باشد، تابع شرایط زیر قرار داده است:

الف) اهداف آن مشخص باشد و به‌طور واضح شرح داده شده باشند.

ب) داده‌پیام باید فقط به اندازهٔ ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع داده‌پیام شرح داده شده جمع‌آوری شود و فقط برای اهداف تعیین‌شده به‌کار رود.

ج) داده‌پیام باید صحیح و روزآمد باشد.

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

ه) شخص موضوع داده‌پیام باید بتواند در هر زمان، با رعایت ضوابط مربوطه، محو کامل پروندهٔ رایانه‌ای داده‌پیام شخصی مربوط به خود را درخواست کند.

مواد ۷۱ تا ۷۳ این قانون نیز برای اشخاصی که مواد ۵۸ و ۵۹ پیش‌گفته را نقض کنند مجازات تعیین کرده است. درصورتی‌که این جرم را دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسئول مرتکب شوند، به حداکثر مجازات مقرر (سه سال حبس) محکوم خواهند شد. سرانجام، چنانچه جرم به علت بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی رخ دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی محکوم خواهد شد.

اگرچه فصل سوم از این قانون به عنوان حمایت از داده‌پیام‌های شخصی اختصاص یافته است، اساساً لفظ حریم شخصی که رکن اساسی در تجارت الکترونیکی است در این قانون مشخصاً تعریف نشده و حمایت از حقوق اشخاص درخصوص اطلاعات شخصی‌شان مورد بحث و حمایت قرار نگرفته است.

یکی از کمبودهای مهم این قانون سکوت دربارهٔ لزوم رعایت تدابیر امنیتی از سوی پردازشگر برای جلوگیری از نفوذ غیرمجاز و سایر اعمال ممنوع یا مجرمانه در بستر مبادلات الکترونیکی و بالاتر از آن عدم ذکر و تعیین اعمال ممنوع و مجرمانه در قانون است. همچنین بی‌توجهی به انتقال داده‌ها، اعم از این‌که انتقال داخلی یا خارجی یا به بخش خصوصی یا دولتی باشد، یکی دیگر از کاستی‌های این قانون است. این سکوت را می‌توان به معنای فقدان چنین حمایتی از داده‌ها و عدم ممنوعیت انتقال آن‌ها و مسئول‌شناختن مرتکب تعبیر کرد. هرچند تصویب این قانون، با وجود نواقص و کاستی‌های آن، نویدبخش آغاز قانونمندشدن فعالیت‌های اینترنتی در تجارت الکترونیکی و جامعهٔ ما بوده است، برای بهبود و پیشرفت و ارتقای آن باید تلاش کرد و توجه داشت که بستر قانونی برای توسعهٔ اینترنت و تجارت الکترونیکی به قوانین متعددی که با جامع‌نگری و توجه به سایر قوانین موجود در کشور تهیه شده باشند و نیز اصلاح قوانین موجود نیاز دارد.

«از دیگر قوانین موجود در زمینهٔ حمایت از ارتباطات الکترونیکی و داده‌پیام‌های شخصی، مقررات و ضوابط شبکه‌های اطلاع‌رسانی (مصوبات جلسات ۴۸۲ الی ۴۸۸ شورای عالی انقلاب فرهنگی) استت که مشتمل بر سه آیین‌نامه است. براساس این آیین‌نامه‌ها، واحدهای ارائه‌کنندهٔ خدمات اطلاع‌رسانی و اینترنتی از هرگونه دسترسی غیرقانونی به فعالیت‌های اینترنتی کاربران، افشای روابط خصوصی افراد و تجاوز به حریم اطلاعات شخصی آنان، انتشار اطلاعات حاوی رمزبانک‌های اطلاعاتی، نرم‌افزارهای خاص، صندوق‌های پست الکترونیکی یا روش شکستن آن‌ها، هرگونه نفوذ غیرمجاز به مراکز دارندهٔ اطلاعات خصوصی و محرمانه و تلاش برای شکستن قفل رمز سیستم‌ها و هرگونه تلاش برای انجام شنود و بررسی بسته‌های اطلاعاتی درحال گذر در شبکه که به دیگران تعلق دارد منع شده‌اند. همچنین دفاتر خدمات اینترنت نیز، که محلی برای ارائهٔ خدمات دسترسی حضوری به شبکه‌های اطلاع‌رسانی (اینترنت و اینترانت) هستند، از تجاوز به حریم خصوصی اطلاعاتی شهروندان، شنود و دسترسی غیرمجاز به داده‌های خصوصی ایشان منع شده‌اند. این آیین‌نامه‌ها، ضمن تأکید بر مصونیت حریم خصوصی کاربران، تجاوز به حریم خصوصی کاربران را مقیّد به یک سری ضمانت اجراهای اداری

کرده است. ضمن این‌که این ضمانت اجراها مانع طرح مورد در دادگاه‌ها و اعمال حقوق کیفری نخواهد بود. البته این آیین‌نامه‌ها فاقد شفافیت و وضوح کافی در تعیین ضمانت اجراهاست و علیرغم این‌که در این آیین‌نامه‌ها مصادیق مهمی از تجاوز به حریم خصوصی مانند شنود یا دسترسی غیرمجاز را تخلف شمرده‌اند، هنوز این موارد غیر از ضمانت اجراهای اداری این آیین‌نامه‌ها مشمول هیچ حکم کیفری نمی‌شوند.» (تبار، همان، ص ۵۵)

اگرچه در قانون ایران حفظ و نگه‌داری سابقهٔ ارتباطات اینترنتی مورد حمایت قرار گرفته است، دسترسی به آن فقط با حکم مقامات قضایی مجاز است. چنانچه پس از انقضای شش ماه قراری از جانب مقامات قضایی دایر بر تمدید مدت نگه‌داری سابقهٔ ارتباطات اینترنتی یک شخص حداکثر تا شش ماه دیگر به دایرکنندگان نقطه تماس بین‌المللی و رساها ابلاغ نشود، آن‌ها باید پس از انقضای موعد یا مواعد مذکور کلیهٔ سوابق ارتباطاتی را که ذخیره کرده‌اند از بین ببرند، وگرنه به مجازات مقرر برای نقض حریم خصوصی ارتباطات در این قانون محکوم خواهند شد. دایرکنندگان نقطه تماس بین‌المللی و رساها، جز با رعایت مقررات مربوط به حریم خصوصی اطلاعات شخصی در این قانون، حق جمع‌آوری اطلاعات شخصی مشترکان، استفاده از آن و افشای آن را ندارند (نوحه‌خوان، همان، ص ۱۵۶)

قوانین ایران در ارتباط با حمایت از حریم خصوصی همگام با تحولات پدیدآمده در این زمینه نیست. در سیاست کیفری ایران، چه در قانون اساسی و چه در قوانین عادی، به مفهوم حریم خصوصی صریحاً اشاره نشده است و چنین استنباط می‌شود که برخی از مصادیق آنچه در اصطلاح به حریم خصوصی معروف است در برخی مواد مورد توجه قرار نگرفته است. مجموع احکام پیش‌بینی‌شده در این مواد نشان می‌دهد که اولاً قانونگذار تمامی مصادیق حریم خصوصی را مدنظر قرار نداده است. ثانیاً، حتی در آن قسمت که مدنظر قرار داده، حمایت‌های لازم، چه کیفری و چه مدنی، از آن به عمل نیاورده است و این میزان از حمایت به هیچ وجه پاسخ‌گوی نیازهای جامعهٔ امروز و چالش‌های فراروی جامعه در عصر اطلاعات نیست. بنابراین تصویب قوانینی جامع و کامل درخصوص امر یا بازبینی و تکمیل قوانین موجود در کشور که حداقلِ آن ارائهٔ تعریفی صریح و دقیق از

مفهوم حریم خصوصی و تا حد امکان تعیین و تعریف دقیق محدوده و مصادیق آن است، امری ضروری و اجتناب‌ناپذیر به‌نظر می‌رسد (رستمی، ۱۳۹۴، ص ۷۰)

در نهایت می‌توان گفت، رویکرد قوانین ایران برای جلوگیری از نقض حریم خصوصی بیشتر جنبهٔ کیفری دارد و در برخی موارد به جبران خسارت و مسئولیت مدنی نیز اشاره کرده است. در اسناد سازمان همکاری اقتصادی و توسعه و مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا رویکرد اصلی غیرکیفری است و فقط به جریمهٔ نقدی در صورت نقض قوانین اشاره کرده است، اما برخلاف قوانین ایران مجازات حبس را برای مجازات نقض حریم خصوصی درنظر نگرفته است.

جدا از مجازات‌های مقرر در قوانین مذکور، این نکته نیز حائز اهمیت است که فرهنگ‌سازی و آماده‌کردن اشخاص برای اجرای قانون جدید تأثیر بسزایی در حاکمیت قانون داشته است. همان‌طور که درمورد مقررات حمایت از داده‌های عمومی اتحادیهٔ اروپا این فرهنگ‌سازی از زمان پیشنهاد قانون مذکور تا تصویب و اجرایی‌شدن آن مشاهده شد و تمام رسانه‌ها آن‌قدر در آگاه‌سازی مردم درخصوص مقررهٔ جدید نقش عمده‌ای داشتند که پس از اجرایی‌شدن آن تمامی مشمولان این مقرره شرایط و ضوابط خود را با آن هم‌راستا کردند و دربارهٔ حقوق و وظایف خود آگاهی کاملی داشتند. این مهم زمانی رخ می‌دهد که تمامی اقشار جامعه آگاه شوند. با آگاه‌سازی افراد دربارهٔ حقوق و وظایفشان می‌توان از خسارت‌های احتمالی بعدی جلوگیری کرد.

نتیجه‌گیری

تمامی بخش‌های زندگی اجتماعی بشر به قوانین و مقررات برای مدیریت و کنترل رابطهٔ افراد نیازمند است. فضای مجازی جنبهٔ جدیدی از زندگی است که نتیجهٔ توسعهٔ فنّاوری است. دهکدهٔ جهانی همهٔ کشورها را به یکدیگر نزدیک کرده است، بنابراین لازم است این فضا کنترل شود تا از جرایم جدی جلوگیری به عمل آید. از آنچه بیان شد می‌توان دریافت که حریم خصوصی محدوده‌ای است که فرد انتظار دارد از دسترس دیگران و حتی دولت‌ها مصون بماند. اسناد سازمان همکاری اقتصادی و توسعه، به‌عنوان اولین سندی که به حمایت از داده‌های شخصی پرداخته است، توجه قانونگذاران را به این

قسمت از فضای وب معطوف کرده و در دستورالعمل‌های خود به حمایت از حریم خصوصی پرداخته است.

حریم خصوصی وارد دنیای جدیدی شده و باید هم‌قدم با فنّاوری‌های روزانه اقدام به قانونگذاری مناسب کرد و از این راه از اشخاص حقیقی و داده‌های آنان حمایت کرد تا کاربران هم‌زمان از مزیت‌های عصر فنّاوری امروز با خاطری آسوده بهره ببرند و از قراردادن اطلاعات خود واهمه‌ای نداشته باشند. آنچه در قانونگذاری نیز حائز اهمیت است تعریف جامع و کامل از حریم خصوصی و دادهٔ شخصی است. این دقیقاً همان خلئی است که متأسفانه در قوانین ایران وجود دارد. با توجه به مقررات عمومی حفاظت از داده‌های شخصی، بهترین تعریف از دادهٔ شخصی را می‌توان این‌گونه بیان کرد:

دادهٔ شخصی هرگونه اطلاعات مربوط به شخص حقیقی شناخته‌شده یا قابل۲شناسایی است که به‌طور مستقیم یا غیرمستقیم، به‌تنهایی یا با استفاده از شناسه‌ای خاص مانند نام، شمارهٔ شناسایی، اطلاعات مکان، شناسهٔ آنلاین یا یک یا چند عامل خاص فیزیکی، فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی به شناسایی موضوع داده منجر می‌شود.

البته که تنها قانونگذاری نمی‌تواند از اشخاص و داده‌های آنان حمایت کند و فرهنگ جامعه و آموزش صحیح استفاده از ابزار فنّاوری نیز بسیار مهم و حیاتی است تا همهٔ این عوامل در کنار هم از داده‌های شخصی کاربران در فضای وب حمایت کنند. فرهنگ‌سازی و آموزش نحوهٔ درست استفاده از فضای مجازی نیز تأثیری کمتر از قانونگذاری ندارد و موجب می‌شود کاربران با حق و حقوق خود آشنا شوند و به‌درستی از حریم خود محافظت کنند.

منابع

احمدی ناطور، زهرا (۱۳۹۱). *نقش فنّاوری‌های نوین اطلاعاتی و ارتباطاتی در نقض حریم خصوصی و راهکارهای مقابله با آن در سیاست کیفری ایران*، پایان‌نامهٔ کارشناسی ارشد رشتهٔ جزا و جرم‌شناسی، دانشکدهٔ ادبیات و علوم انسانی، دانشگاه گیلان.

تبار، محسن (۱۳۹۱). *بررسی تطبیقی حق حریم خصوصی در ایران و آمریکا*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ حقوق بشر، دانشکدهٔ حقوق و علوم انسانی، دانشگاه تهران.

حبیبی، همایون (۱۳۹۵). «حق بر حریم خصوصی در شبکه‌های اجتماعی». مجلهٔ *تحقیقات حقوقی* دانشگاه شهید بهشتی، دورهٔ ۱۹، شمارهٔ ۷۳، ص ۳۹-۶۴.

رستمی، بهمن (۱۳۹۴). *بررسی تطبیقی حریم خصوصی در حقوق جزای ایران و اسناد بین‌المللی و حقوق فرانسه*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ جزا و جرم‌شناسی، دانشکدهٔ الهیات و علوم اسلامی، دانشگاه پیام نور.

فتحی، یونس و شاهمرادی، خیراله (۱۳۹۶). «گستره و قلمرو حریم خصوصی در فضای مجازی». *مجلهٔ حقوقی دادگستری*، سال هشتادویکم، شمارهٔ ۹۹، ص۲۲۹-۲۵۲.

رنجبران، مسلم (۱۳۹۱). *سیاست کیفری جمهوری اسلامی ایران در رابطه با نقض خلوت اشخاص*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ جزا و جرم‌شناسی، دانشگاه فردوسی مشهد.

محسنی، فرید (۱۳۹۶). *حریم خصوصی*. تهران: انتشارات دانشگاه امام صادق(ع)، چاپ دوم.

نوحه‌خوان، حنیفه (۱۳۹۱). *بررسی حریم خصوصی در حقوق کیفری ایران با نگاهی به اسناد بین‌المللی*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ جزا و جرم‌شناسی، دانشکدهٔ حقوق دانشگاه آزاد اسلامی، واحد تهران مرکزی.

واعظی، سیدمجتبی و علیپور، سیدعلی (۱۳۸۹). «بررسی موازین حقوقی حاکم بر حریم خصوصی و حمایت از آن در حقوق ایران». *نشریهٔ حقوق خصوصی دانشگاه تهران*، دورهٔ ۷، شمارهٔ ۱۷، ص ۱۳۳-۱۶۳.

Davidson, A. (2009). *The Law of Electronic Commerce*. Cambridge University Press.

OECD (2011). *The OECD Privacy Guideline*. http://www.oecd.org/sti/ieconomy/49710223.pdf.

Walther, J. B. (2011). "Introduction to Privacy Online". in *Privacy Online, Perspectives on Privacy and Self-Disclosure in the Social Web*. S. Trepte & L. Reinecke (eds).

The Notion and Importance of Personal Data and Privacy and Their Various Protections in Cyber Space

Fatemeh Ghanad[۱], Amireh Aligholi[۲]

Abstract

Electronic commerce has affected all aspects of life; it results from technological development and is still in progress. This development has some consequences and results for people. Breach of personal data and privacy is one of them. Cyberspace has targeted all aspects of personal data such as genetic, identity, physiological, behavioral, and religious beliefs information to achieve their political, economic, and social goals. This article aims to assess the legal protection of privacy in accordance with GDPR and Iranian laws. That is, whether these rules can prevent the violation of privacy on the Web, or whether in the digital age, it is the end of privacy and personal data protection. It is a significant issue that requires careful analysis and evaluation. In this paper, by examining the concept of privacy in EU regulations and the Iranian legal system, it is analyzed that laws need to be more up-to-date than developments in the digital age. The concept of privacy and personal data must be specifically introduced and protected within the law. To be placed. However, none of the domestic legal systems examined laws have a comprehensive and coherent definition of personal data, and this gap should be addressed in Iranian law. Finally, a broad definition of personal data is provided.

Keywords: Data Protection, Privacy, Web Space, Social Media, GDPR, Personal Data

۱ Associate Professor, University of science and culture, Tehran, Iran; (Corresponding Author); ghanad@usc.ac.ir

۲. Master of Electronic commerce Law, University of science and culture, Tehran, Iran; amire.aligholi@gmail.com