مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

طرح پژوهشی جهت گذران فرصت مطالعاتی

عنوان طرح:

مطالعه الزامات قانون جامع حکمرانی و تنظیم‌گری حریم خصوصی و داده‌های شخصی در فضای مجازی در ایران

پژوهشگر: حسین حسنی

(عضو هیئت علمی پژوهشگاه فرهنگ، هنر و ارتباطات)

۱۴۰۳-۱۴۰۲

چکیده

هدف این پروژهٔ پژوهشی مطالعهٔ الزامات و ابعاد قانون حریم خصوصی در ایران، با ملاحظهٔ فضای مجازی و پلتفرم‌های رسانه‌های اجتماعی است. باوجود اهمیت یافتن فزاینده فضای مجازی و رسانه‌های اجتماعی در جامعهٔ ایران، به ابعاد گوناگون، از جمله حفاظت از حریم داده‌های شخصی و اطلاعات کاربران، توجهی نشده است. سابقه اقدام برای قانون‌گذاری درمورد حریم خصوصی در ایران به حدود اواسط دههٔ ۱۳۸۰ شمسی بازمی‌گردد؛ اما با گذشت حدود دو دهه و برخی اقدامات دیگر، مقررات جامعی برای حفاظت از حریم خصوصی در فضای مجازی در ایران تصویب نشده است. مسئله اصلی این پژوهش این بود که تدوین قانون جامع حکمرانی و تنظیم حریم خصوصی و داده‌های شخصی در فضای مجازی در ایران چه الزامات و چه ابعادی دارد؟. این مطالعه به روش کیفی انجام شد و اسناد و منابع گوناگون برای تحلیل گردآوری و به روش تحلیل محتوای کیفی صورت گرفت. تحلیل یافته‌ها در چند بخش ارائه شدند که عبارت‌اند از: مفهوم‌پردازی حریم خصوصی با مطالعهٔ ادبیات این حوزه، رویکرد دینی و فقهی به حریم خصوصی و نیز قوانین و رویکردهای حریم خصوصی در ایران پس از انقلاب اسلامی؛ سیاستهای حریم خصوصی در پلتفرم‌های بزرگ جهانی؛ حریم خصوصی در اسناد بین‌المللی؛ مرور مقررات وضع‌شده درباره حفاظت از داده‌های شخصی و نیز تحلیل لایحهٔ‌های پیشنهادی دربارهٔ حفاظت از حریم خصوصی و تحلیل داده در ایران. یافته‌های این مطالعه در قالب چکیدهٔ سیاسی و نیز پیش‌نویسی برای حفاظت از داده‌های شخصی و حریم اطلاعات در پلتفرم‌های دیجیتال ارائه‌شده است. درمجموع، توسعه فزاینده نقش پلتفرم‌ها و اقدامات حکمرانی درون‌پلتفرمی آنها برای حفاظت از داده‌های شخصی، لزوم حفاظت از حقوق کاربران ازجمله در حفاظت از داده‌های شخصی و عدم تجسس در حریم ارتباطی آن‌ها در پیام‌رسان‌ها، انتشار اخبار گوناگون دربارهٔ افشای اطلاعات شخصی کاربران و عدم مسئولیت‌پذیری پلتفرم‌های مختلف ایرانی در برابر افشای اطلاعات کاربران و درکل با ملاحظهٔ اینکه حفاظت از حریم خصوصی به‌منزله صیانت از کرامت ذاتی انسان‌ها و نوعی حق اساسی برای کاربران در جامعه است، ضرورت تدوین مقررات مرتبط را الزامی می‌کند.

فهرست

فصل اول

کلیات تحقیق

مقدمه

حفاظت از حریم خصوصی[۱] و محرمانگی داده‌های شخصی[۲] پس از گذار از عصر رسانه‌های آنالوگ و دیجیتال و سپس ظهور اینترنت و هم‌اکنون پلتفرمی‌شدن اینترنت[۳] (فلیو، ۲۰۲۱) که طی آن تعاملات، کنشها و ارتباطات بیش از پیش در شمار نسبتاً محدودی از پلتفرمهای بزرگ دیجیتال روی می‌دهد، بیش از گذشته دشوار و هرروز پیچیده‌تر می‌شود. درواقع، درهم‌تنیدگی فزاینده پلتفرم‌های دیجیتال و رسانه‌های اجتماعی با زندگی روزمره سبب می‌شود افراد به شکل خواسته یا ناخواسته داده‌های شخصی بیشتری را در فضای مجازی با طرفهای دیگر (شرکتها، دولتها، سازمانها، افراد) به اشتراک بگذارند. همچنین، پلتفرم‌های دیجیتال نیز بیش از پیش داده‌های شخصی ما را به مثابه مدل اصلی کسب و کار به کار می-بندند. پیامد همه این موارد، تسهیل و تعمیق مخاطره‌ها برای حریم شخصی افراد و دشوارترشدن کناره‌گیری از این روندهای اجباری–از جمله حق فراموش شدن[۴]– است. حریم خصوصی و داده‌های شخصی بیش از پیش به‌واسطه مدل کسب‌وکار شرکتهای پلتفرمی جهانی مورد خدشه قرار می‌گیرد؛ زیرا یکی از منابع عمده درآمدزایی این پلتفرم‌ها تحلیل داده‌های کلان کاربران است و نیز رویه‌های شخصی‌سازی و سفارشی‌سازی نیز به تحلیل و استخراج الگوهای رفتاری کاربران بر مبنای داده‌هایی که آنها به اشتراک می‌گذارند بستگی دارد. این موارد صرفاً برخی از نمونه‌های درهم‌تنیدگی حریم شخصی کاربران با عملکرد پلتفرم‌ها است. همانطور که فن دایک (۱۳۸۶) می‌گوید، مأموریت فیس‌بوک یعنی گشوده‌تر کردن و متصل‌تر کردن جهان در قالب اشتراک‌گذاری محقق می‌شود؛ معنای اجتماعی این اصطلاح در تقابل با اصطلاح حقوقی حریم خصوصی قرار می‌گیرد که مبتنی بر حق انزوا و کناره‌گیری از اجتماع است.

کاریسا ولیز (۲۰۲۰) در کتاب *حریم خصوصی قدرت*[۵] است، نشان می‌دهد که چگونه تمامی کنشها، اعمال، گفتار، انتخابها، عادتها، مصرف کالاها، سفر، بیماری و به طور تمام ساحت‌های زیست شخصی و خصوصی ما توسط پلتفرم‌ها و اپلیکیشن‌ها به مثابه داده ثبت و ضبط می‌شوند و پس از تحلیل به طرفهای گوناگون از نهادهای امنیتی تا شرکتهای بیمه و کارفرمایان ما فروخته می‌شوند؛ وضعیتی که ما را وارد یک جامعه نظارتی[۶] کرده است. علت این موضوع این است که «اینترنت در اصل

---

[1] .privacy
[2] .data privacy
[3] . platformization of the internet
[4] .right to be forgotten
[5] .Privacy is Power
[6] .privacy

به‌وسیله گردآوری، تحلیل و تجارت داده تأمین مالی می‌شود–اقتصاد داده. بخشی زیادی از این داده‌ها، داده‌های شخصی هستند» (ولیز، ۲۰۲۰: ۶). توسعه فزاینده فناوریهای متصل به وب همانند ساعتهای هوشمند، فناوریهای شناسایی چهره و اینترنت اشیا سبب شده است تا داده‌های شخصی به عنوان یک منبع ارزشمند مورد توجه پلتفرمهای بزرگ و شرکتهای طرف سوم قرار گیرد. بنابراین، حفاظت از داده‌های شخصی و حفظ حریم خصوصی بیش از پیش دشوار می‌شود.

حریم خصوصی و ضرورت احترام به آن یکی از مهمترین بحثهای رایج سیاسی و حقوقی است و مصونیت این حوزه زندگی شهروندان از جمله بدیهی‌ترین حقوق آنها به شمار می‌رود (اسماعیلی، ۱۳۹۶). اسماعیلی (۱۴۰۰) در کتاب حقوق آزادی اطلاعات در ایران، اطلاعات مرتبط با حریم خصوصی یا اطلاعات شخصی را از مهمترین استثنائات اصل آزادی اطلاعات معرفی کرده است و معتقد است احترام به حریم خصوصی افراد ازجمله حقوق اولیه و بدیهی انسانها است که نباید قربانی حقوق دیگر همانند آزادی اطلاعات شود. به طور کلی حریم خصوصی یکی از حدود مهم آزادی بیان و اطلاعات است که در اسناد بین المللی مختلف همانند اعلامیه جهانی حقوق بشر و میثاق بین المللی حقوق مدنی و سیاسی و قوانین اساسی بسیاری از کشورها مورد حمایت قرار گرفته است و طرفهای گوناگون از جستجو، گردآوری، تکثیر، انتشار و اشاعه اطلاعات مربوط به امور خصوصی افراد منع شده‌اند (انصاری، ۱۴۰۱).

طرح مسئله

در مجموعه‌ای از اسنادی که توسط شورای عالی فضای مجازی و مرکز ملی فضای مجازی مصوب شده است، به شکلهای گوناگون بر اهمیت حفظ حریم خصوصی کاربران تأکید شده است. در سند راهبردی جمهوری اسلامی ایران در فضای مجازی (مرکز ملی فضای مجازی، ۱۴۰۱) که شامل ارزشها، چشم‌انداز، اهداف و اقدامات کلان است و با هدف تحکیم و تقویت حکمرانی و اعمال حق حاکمیت بر فضای مجازی و پلتفرمهای دیجیتال و رسانه‌های اجتماعی تصویب شده است، صیانت از حریم خصوصی و حقوق عامه به مثابه یک ارزش مورد تأکید قرار دارد. در این سند، قاعده‌مندسازی دسترسی به داده‌های خصوصی، عمومی و کلان داده‌ها به عنوان یک هدف کلان بیان شده است. در همین راستا طراحی نظام حکمرانی داده‌ها ازجمله در مورد حریم خصوصی یکی از اقدامات کلانی است که باید پیگیری شود.

سند سیاستها و اقدامات سازماندهی پیام‌رسان‌های اجتماعی که مصوبه شورای عالی فضای مجازی در سال ۱۳۹۶ است، به طور خاص بر حکمرانی بر پیام‌رسانهای اجتماعی تأکید دارد. در این سند «اعتمادسازی و صیانت از حقوق شهروندی، حریم خصوصی، امنیت ملی و عمومی» به عنوان یک سیاست کلان ذکر شده است. هدف این سند فراگیرکردن پیام‌رسان‌های ایرانی و سازماندهی پیام‌رسانهای اجتماعی خارجی است (شورای عالی فضای مجازی، ۱۳۹۶). براین اساس می‌توان مدعی شد حفاظت از جریم خصوصی و داده‌های شخصی کاربران و رفع نگرانی آنها نسبت به دسترسی طرف‌های سوم به این داده‌ها، تا چه اندازه برای اعتماد کاربران به یک پیام‌رسان اهمیت دارد.

سایر اسناد مصوب شورای عالی فضای مجازی نیز به شکلهای مختلف بر اهمیت حفظ حریم خصوصی تأکید کرده‌اند. در سند تبیین الزامات شبکه ملی اطلاعات (شورای عالی فضای مجازی، ۱۳۹۵) صیانت از حریم خصوصی، حقوق عمومی و آزادی مسئولانه به مثابه یکی از الزامات سالم سازی و امنیت شبکه ملی اطلاعات ذکر شده است. همچنین حمایت ویژه از حریم خصوصی و حقوق عمومی یکی از نیازمندهای ارائه خدمات ایمن در قالب شبکه ملی اطلاعات ذکر شده است. در سند نظام هویت معتبر در فضای مجازی نیز صیانت از حریم خصوصی یکی از الزامات زیست بوم هویت معتبر ذکر شده است (شورای عالی فضای مجازی، ۱۳۹۶). در سند الزامات حاکم بر اینترنت اشیاء در شبکه ملی اطلاعات (۱۳۹۷)، حریم خصوصی یکی از الزامات ارائه خدمات در این قلمرو ذکر شده است.

باوجود تأکید اسناد بالادستی گوناگون به اهمیت حریم خصوصی و ضرورت ایجاد سازوکارهای حفاظت از داده‌های شخصی افراد، در شبکه ملی اطلاعات تا پیام‌رسان‌های ایرانی و پلتفرم‌های رسانه اجتماعی خارجی، اقدام عملی در راستای تدوین اسناد جامع مرتبط با حفاظت از داده و حریم خصوصی در ایران صورت نگرفته است.

طی دو دهه گذشته در مجلس شورای اسلامی به عنوان نهاد اصلی قانونگذاری در نظام جمهوری اسلامی ایران و نیز دولت جمهوری اسلامی اقداماتی درجهت ارائه یک لایحه جامع مرتبط با حریم خصوصی انجام شده است که تاکنون به تدوین یک قانون جامع حفاظت از داده‌ها و حریم خصوصی در ایران منجر نشده است. از جمله نخستین اقدامات می توان به لایحه «حمایت از حریم خصوصی» اشاره کرد که در سال ۱۳۸۳ در کمیسیون لوایح دولت تصویب شد اما در مهر ۱۳۸۴ پس از طرح در مجلس شورای اسلامی، رد شد و تصویب نشد. این طرح دارای ۸۰ ماده قانونی بوده است و در مقدمه آن آمده است:

با الهام از احکام شرع مبین اسلام و به منظور حمایت از جسم افراد، اماکن خصوصی و منازل، حریم خلوت و تنهایی افراد، محلهای کار، اطلاعات شخصی و ارتباطات خصوصی و تبیین نحوه اجرای اصول (۲۲) و (۲۵) قانون اساسی، شفاف‌سازی اختیارات و مسئولیتهای ارکان و اجزای مختلف حکومت در زمینه رعایت حریم خصوصی و با عنایت به تعهدات بین المللی دولت، قانون «حمایت از حریم خصوصی» به شکل زیر به تصویب می رسد.

در ماده ۲ این طرح پیشنهادی، حریم خصوصی به این شکل تعریف شده است:

قلمرویی از زندگی هر شخص که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند و یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند. جسم، البسه و اشیاء همراه افراد، امکان خصوصی و منازل، محلهای کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می‌شود (فصلنامه میزان، ۱۳۸۶).

به عنوان نمونه‌ای از اقدامات دیگر نیز باید گفت که در سال ۱۳۹۶ وزارت ارتباطات پیش‌نویس لایحه صیانت و حفاظت از داده های شخصی را تهیه و پس از انتشار آن در مرداد ۱۳۹۷ از صاحب‌نظران درخواست شد نظرات خود را درباره آن بیان کنند[1]. این پیش‌نویس به طور کلی بر داده‌های شخصی متمرکز است و نسبت این مفهوم با حریم خصوصی مشخص نشده است. برخی از اهداف این قانون در ماده ۱ بیان شده است عبارتند از: 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. این پیش‌نویس را می‌توان اساساً یک نوع نسخه‌برداری و یا تبعیت از تصویب از قانون مقررات عمومی حفاظت از داده‌ها[2] تلقی کرد که بر اساس رویکردهای تنظیم‌گرانه اتحادیه اروپا در سال ۲۰۱۸ تصویب شد. در این پیش‌نویس به رابطه میان حریم خصوصی و حریم داده و نسبت میان آنها اشاره‌ای نشده است.

[1] . https://peivast.com/wp-content/uploads/laehehhefazatazdadeh.pdf
[2] .GDPR

این پیش‌نویس شامل ۷۸ ماده است و به موارد همانند حقوق اشخاص، دامنه تعهدات کنترل‌گران، تنظیم و نظارت بر پردازش داده‌های شخصی و مسئولیت و ضمانت اجرا پرداخته شده است. در بیان توجیه این قانون به برخی از اصول قانون اساسی (۱۹، ۲۰، ۲۲، ۲۳، ۲۵، ۲۶، ۳۸ و ۳۹)، سیاستهای کلی نظام ابلاغی مقام معظم رهبری و قوانین دیگری همانند قانون انتشار و دسترسی آزاد به اطلاعات، قانون تجارت الکترونیک، قانون مجازات اسلامی، قانون تجارت و نیز عمل به فتوای مقام معظم رهبری مبنی بر حرام شرعی بودن نقض حریم خصوصی اشاره شده است. به ظاهر این اقدام به نتیجه خاصی منجر نشده است.

در دی ماه ۱۴۰۱ نیز وزیر کنونی ارتباطات و فناوری اطلاعات اعلام کرده است که پیش‌نویس لایحه قانون حمایت و حفاظت از داده‌های شخصی نهایی و به کارگروه ویژه اقتصاد دیجیتال ارسال شده است. این کارگروه در سال ۱۴۰۰ به منظور هماهنگی و راهبری توسعه اقتصاد دیجیتال با تصویب هیئت وزیران تشکیل شده است[۱]. بنابراین نهادی که وظیفه اصلی خود را توجه به مسائل اقتصاد و کسب وکارهای دیجیتال متولی نهایی‌سازی لایه حفاظت از داده‌های شخصی شده است و تاکنون نتیجه بررسی این پیش‌نویس در این کارگروه اعلام نشده است[۲]. گرچه بر اساس سند راهبردی جمهوری اسلامی ایران در فضای مجازی وزارت ارتباطات و فناوری اطلاعات، به عنوان دستگاه متولی طراحی نظام حکمرانی داده‌ها معین شده است و نهادهای حکومتی و دولتی دیگر از جمله قوه قضاییه، ستاد کل نیروهای مسلح، سازمان صداوسیما و برخی وزارتخانه‌های دیگر دستگاه همکار محسوب می‌شوند.

بر اساس مرور اقدامات قانونی فوق مشخص می‌شود که فارغ از دلایل مختلفی که سبب شده است تا تاکنون در ایران یک قانون جامع حریم خصوصی تصویب نشود، در مورد تعریف خصوصی و حریم داده اختلاف نظر اساسی وجود دارد و نسبت میان آنها مشخص نیست. هرچند بر اساس مطالعه مرکز پژوهشهای مجلس در مورد خلاءهای قانونی حفاظت از داده‌ها ارتباط میان به این شکل توضیح داده شده است:

---

[1] . https://rc.majlis.ir/fa/law/show/1680343

[۲] . عیسی زارع‌پور وزیر ارتباطات و فناوری اطلاعات در اوایل مرداد ۱۴۰۳ اعلام کرد که تدوین و تصویب لایحه «حفاظت از داده‌های شخصی»، ابتدا قریب به یکسال در کارگروه ویژه اقتصاددیجیتال بررسی و تصویب و سپس درچندین جلسه کمیسیون حقوقی و قضایی دولت بررسی و نهایی شده و هفته قبل در دولت تصویب و برای سیر مراحل قانونی به مجلس ارسال شد.

حریم خصوصی و حفاظت از داده[1] دو موضوع مرتبط با یکدیگر در حکمرانی اینترنت هستند. در منابعی که به تمایز این دو مفهوم اعتقاد دارند، حفاظت از داده‌ها را سازوکار حقوقی می‌دانند که حریم خصوصی را تضمین می‌کند. حریم خصوصی نیز معمولاً حق شهروندان در کنترل اطلاعات شخصی آنها و تصمیم در مورد (افشا یا عدم افشا) آن هستند. به بیان دیگر حریم خصوصی داده تعریف می کند که چه کسی به داده دسترسی داشته باشد درحالی که حفاظت از داده ابزارها و سیاستهایی برای محدود کردن بالفعل دسترسی به داده‌ها وضع می‌کند. گرچه منابع معتبر دانشگاهی تمایز میان حریم خصوصی و حفاظت از داده‌ها را تمایزی با منشا اروپایی می‌دانند. یعنی در مطلعات تطبیقی کشورها مرز میان حفاظفت از داده و حریم خصوصی داده ها کمرنگ می شود و اصولاً حریم خصوصی و حفاظت از داده‌ها در احکام قانونی تفکیک‌ناپذیر نیستند. زیرا حکم حقوقی که درزمینه حفاظت از داده ها تدوین می شود، اصولاً ضوابط حریم خصوصی را تعیین می کند (مرکز پژوهشهای مجلس، ۱۴۰۲: ۸).

قناد و علیقلی (۱۳۹۹) در مورد نسبت داده‌های شخصی و حریم خصوصی بحث کرده‌اند. از نظر آنها داده‌های شخصی یکی از ابعاد حریم خصوصی است. به نظر آنها «داده‌های شخصی به هر موردی گفته می شود که به تنهایی یا در کنار شناسه‌ای دیگر به شناسایی موضوع داده منجر می‌شود» (ص.۲۹۸). آن دو در مقاله دیگری، حریم خصوصی را به دو گروه اطلاعات خصوصی و داده های شخصی تقسیم کرده‌اند. اطلاعات خصوصی به شیوه‌های جمع آوری، ضبط، دسترسی و آزادسازی اطلاعات اشاره دارد. اما داده‌های شخصی مربوط به حریم شخصی و فضای خصوصی فرد است (قناد و علیقلی، ۱۳۹۸). بنابراین، تعریف دقیق هرکدام از این مفاهیم و وجوه شباهت و افتراق آنها یک موضوع محوری است که باید مورد توجه قرار گیرد.

آنچه تاکنون گفته شد، مروری بر برخی اقدامات قانونگذاری و مقررات گذاری توسط قوه مجریه و قوه قضائیه برای تعریف و تعیین حدود حریم خصوصی و یا داده‌های شخصی به طور کلی و در عرصه‌های رسانه‌ای و فضای مجازی بوده است. این اقدامات ذیل رویکرد کلی «حکمرانی بر اینترنت و فضای مجازی» قابل درک است. اما از سوی دیگر باید توجه داشت که امروزه بخش مهمی از حکمرانی حریم خصوصی توسط پلتفرم‌های رسانه‌های اجتماعی انجام می‌شود. این امر دلایل گوناگونی دارد که مهمترین آنها عبارتند از: عدم تمایل دولتها برای خدشه در آزادی بیان، به‌ویژه در مدل بازار–محور

[1] .data protection

حکمرانی پلتفرمها که در آمریکا رواج دارد، عقب‌افتادگی نهادهای قانونگذار برای وضع قوانین مرتبط برای حفاظت از حریم خصوصی در پلتفرمها که ناشی از تحولات شتابان این حوزه فناوری اطلاعاتی و ارتباطی است و نیز حجم غول‌آسای محتواهای کاربرساخته[1] که توسط کاربرانی از زمینه‌های فرهنگی–اجتماعی و زبانی متنوع در سطح جهان به اشتراک گذاشته می‌شود. بخش قابل توجه از این محتواها مرتبط با حریم خصوصی (از جمله نقض آن) هستند.

بنابراین رویکرد دیگری که با عنوان «حکمرانی به‌وسیله پلتفرم‌ها» و یا توسط برخی صاحبنظران دیگر بازبینی محتوا[2] (ژیلسپی، ۲۰۱۸) نامیده شده است، شامل مجموعه‌ای از اسناد و دستورالعمل‌های تدوین شده توسط مالکان و مدیران پلتفرم‌ها و نیز رویه‌های بازبینی، نظارت و نیز حذف و یا تعدیل محتواهای زیان‌آور از جمله محتواهای ناقض حریم خصوصی و داده‌های شخصی است که توسط عاملان انسانی و ماشینی به طور مستمر در حال وقوع است.

سلستی و همکارانش (۲۰۱۸) برای تحلیل مناقشه‌هایی که در مورد نحوه صیانت قانونی از حقوق بنیادین انسانها در پلتفرم-ها ایجاد شده است، از عبارت از اصطلاح‌های حکمرانی خرد[3] و حکمرانی کلان[4]استفاده می‌کنند. بنابراین آنها به جای تعدیل (بازبینی) محتوا از حکمرانی محتوا استفاده می‌کنند که ناظر بر مداخله و مشارکت ذی‌نفعان گوناگون در حکمرانی پلتفرم‌ها است. منظور آنها از حکمرانی خرد شامل مجموعه‌ای از «قواعد استانداردشده، سازوکارهای نهادینه‌شده بازبینی محتوا و کنشگران حرفه‌ای درگیر در تعدیل محتواهای برخط» (ص.۱۰) و یا هنجارها و ساختارهای داخلی است که پلتفرمها برای مقابله با محتواهای نابهنجار به کار می‌گیرند. اما منظور از حکمرانی کلان شامل سازوکارهایی که درنتیجه پیوند و همکاری با کنشگران بیرونی همانند دولتها و گروه‌های مدافعه‌گر به وجود می‌آید.

حفاظت از حریم خصوصی به عنوان یکی از حقوق بنیادین انسانها و کاربران یکی از مهمترین کردارها و بخش مهمی از اسناد تعدیل محتوا در پلتفرم‌ها یعنی شرایط ارائه خدمت[5]است. به‌طوری‌که نظام‌نامه یا خط‌مشی حریم خصوصی و حریم داده شامل مجموعه‌ای مقررات دقیق، پیچیده و پرجزئیات در بیشتر پلتفرم‌های بزرگ همانند پلتفرم‌های وابسته به متا (واتس‌اپ، فیس‌بوک و اینستاگرام)، ایکس (توئیتر) و یوتیوب وابسته به گوگل است. در این اسناد طیفی از مقررات گوناگون

---

[1] .UGC
[2] .content moderation
[3] .micro governance
[4] .macro governance
[5] .Terms of service (TOS)

از مجموعه داده‌های شخصی که از کاربران گردآوری می‌شود تا نحوه استفاده از این داده‌ها به طور کامل توضیح داده شده است.

بر اساس آنچه گفته شد، در سیاستگذاری و تنظیم‌گری حریم خصوصی و حفاظت از داده‌ها در فضای مجازی به طور کامل و عمده‌ترین مظاهر تعامل و اجتماع کاربران یعنی پلتفرم‌های رسانه‌های اجتماعی و پیام‌رسان‌ها و برخی از خدمات دیگر نظیر موتورهای جستجو هم باید مجموعه اسناد و مقررات و قوانین حاکم بر پلتفرم‌ها و هم اسناد و مقررات درونی پلتفرم‌ها مورد ملاحظه قرار گیرد. نکته اخیر ناظر بر جایگاه انکارناپذیر پلتفرم‌ها و سازوکارهای درونی آنها برای حفاظت و صیانت از حریم خصوصی کاربران است. ظهور امپریالیسم پلتفرمی (جین، ۲۰۱۵) که شکل نوینی از امپریالیسم جهانی بدون ملاحظه حق حاکمیت دولتها، مرزهای جهانی، قانون اساسی دولت–ملتها و هنجارهای اجتماعی، فرهنگی و اخلاقی را تداعی می‌کند و اساساً در آن حوزه قضایی به چالش کشیده شده است، یک تهدید اساسی برای مفاهیم محلی حریم خصوصی است. در همین جهت پازن[1] (۲۰۱۸) مفهوم مشروعیت استبدادی[2] را برای توصیف نحوه اعمال قواعد بازبینی محتوا توسط فیس بوک به کار می‌برد و سلستی (۲۰۱۹) اعتقاد دارد که اسناد شرایط ارائه خدمت توسط پلتفرمهای برخط همانند نوعی قانون اساسی خصوصی عمل می‌کند و آنها اعمال حقوق کاربران در این فضاهای مجازی را تنظیم می‌کنند.

علاوه بر پلتفرم‌های بزرگ جهانی که امروزه بخش مهمی از تعاملات و ارتباطات و تبادلات خدماتی کاربران در سطح جهان و ازجمله ایران به‌واسطه آنها انجام می‌شود، تعدادی پلتفرم محلی نیز در قلمروهای سرزمینی مختلف همانند ایران رشد و توسعه پیدا کرده‌اند. این پلتفرم‌ها یا بر اساس روند «طبیعی» رشد شرکتهای نوآور (استارتاپ) از مرحله پیش‌بذری تا بلوغ را طی می‌کنند و می‌توانند «توجه» کاربران عادی را به خود جلب کنند و بر مبنای اثر شبکه رشد کنند و حتی به یونیکورن تبدیل شوند و یا این دولت–حامی هستند و بنابراین اقتضائات گوناگون با انواع حمایت از تأمین مالی گرفته تا ایجاد انحصار توسعه داده می‌شوند تا کاربران در قالب پروژه اقتباس اجباری[3] از خدمات آنها استفاده کنند. در مورد پلتفرم‌های محلی، فارغ از شیوه فراگیری آنها، از آنجا که خط‌مشی حریم خصوصی آنها–با هر میزان از توسعه و پیچیدگی و اعمال–با قوانین،

[1] .Pozen
[2] . authoritarian constitutionalism
[3] .coersive adoptation

مقررات و هنجارهای اخلاقی جامعه تا حد زیادی هم‌پوشانی دارد، تعریف و اعمال انواع حقوق از جمله حق حریم خصوصی آسان‌تر است.

حق داشتن حریم خصوصی[1] یکی از حقوق بنیادین همه انسانها و به‌ویژه حقوق مخاطبان رسانه‌ها و محصولات فرهنگی و رسانه‌ای است و در کنار حق بر آگاهی که اسماعیلی (۱۴۰۱) آنرا به مثابه یکی از حقوق اساسی مخاطبان مورد بحث قرار داده است، از جمله وجوه اساسی حقوق مخاطبان است. بنابراین توانایی و امکان حفاظت از حریم خصوصی اشخاص در فضای مجازی و پلتفرم‌های رسانه‌های اجتماعی به این معنا است که یک بعد محوری از حقوق مخاطبان مورد توجه و تأکید قرار دارد.

بر اساس آنچه گفته شد و به‌ویژه ملاحظه کوشش‌های نافرجام برای ارائه یک قانون جامع حریم خصوصی در ایران، تحولات در اینترنت و پلتفرمی‌شدن آن، رویکردهای کلان به حکمرانی محتواهای پلتفرم‌های اجتماعی و اقتصاد دیجیتال و به ویژه سه رویکرد کلان بازار–محور آمریکایی، دولت–محور در چین و حقوق–مدار در اتحادیه اروپا که هر کدام مبتنی بر نظریه‌های مختلفی درباره بین بازار، دولت، فرد و حقوق جمعی هستند مسئله اصلی این پژوهش این است که «**تدوین قانون جامع حکمرانی و تنظیم‌گری حریم خصوصی و داده‌های شخصی در فضای مجازی در ایران چه الزامات و چه ابعادی دارد؟**».

پرسشهای فرعی این پژوهش عبارتند از:

۱. مبانی نظری و مفهومی حریم خصوصی در ایران چیست؟

۲. تا کنون چه اقداماتی (قوانین و مقررات و اسناد) برای صیانت از حریم خصوصی (در ایران انجام شده است) است؟

۳. تاکنون چه تحولاتی (قوانین و مقررات) در سایر کشورهای جهان برای حمایت از حریم خصوصی و مقابله با نقض آن انجام شده است؟

۴. با ملاحظه اهمیت حکمرانی در پلتفرم‌ها، پلتفرمهای بزرگ جهانی تاکنون چه اسناد و مقرراتی را برای حفاظت از حریم خصوصی و داده‌های شخصی ارائه کرده‌اند و از چه سازوکارهایی را برای صیانت از حقوق حریم خصوصی کاربران در پلتفرم‌های خود انجام تعبیه کرده‌اند؟

[1] .right to privacy

در مجموع، هدف نهایی این پروژه ارائه یک خلاصه سیاستی و ارائه پیش‌نویس قانون جامع حریم خصوصی در ایران با توجه به تمام ملاحظات نظری–مفهومی، فرهنگی–اجتماعی و نیز فناورانه است.

اهمیت، ضرورت و اهداف تحقیق

حفاظت و صیانت از حریم خصوصی یکی از حقوق اولیه همه انسانها است که در متون دینی، قوانین بین‌اللمل و نیز قوانین اساسی بسیاری از کشورها از جمله ایران به رسمیت شناخته شده و مورد تأکید قرار گرفته است. همه انسانها این حق را دارند که جدای از محیط اجتماعی یک فضای شخصی برای خود داشته باشند و دسترسی دیگران را به اطلاعات خود محدود کنند.

گسترش فناوریهای اطلاعاتی از جمله اینترنت و توسعه آنها بیش از پیش این حریم و فاصله‌گذاری را که در دنیای فیزیکی با سهولت بیشتری امکان پذیر بود به چالش کشیده است. رسانه‌های نوین و به طور خاص رسانه‌های اجتماعی و پلتفرمهای برخط اساساً و تا حد زیادی در تقابل با ایده حریم خصوصی قرار دارند. رسانه‌های اجتماعی تصویری همانند تیک تاک و اینستاگرام با انگیزه اشتراک‌گذاری زندگی شخصی و خصوصی افراد به بهای صمیمیت بیشتر، بیش از به حریم شخصی افراد تجاوز می‌کنند.

از آنجا که بخش مهمی از اطلاعات شخصی و خصوصی افراد به انواع گوناگون داده تبدیل می‌شوند، این داده‌ها در نهایت به کالا تبدیل می‌شوند. به همین دلیل است که مدل تجاری پلتفرم های عمده جهانی مبتنی بر اقتصاد داده است. میل به انباشت بیشتر سرمایه، پلتفرم‌ها را برمی‌انگیزد تا بیش از پیش و با وسعت بیشتری داده‌های شخصی افراد را گردآوری کنند. به دلیل مخاطره افکندن شدن زندگی شخصی و نیز استفاده تجاری از داده‌های شخصی کاربران و شهروندان ضرورت داد تا صیانت از حریم خصوصی خواه به شکل حکمرانی بر پلتفرم‌ها و یا حکمرانی در پلتفرم‌ها در دستور کار نهادهای سیاستگذار و قانون‌گذار در ایران قرار گیرد. به طور خاص اتحادیه اروپا در این امر یا حکمرانی مبتنی بر مقررات پیشگام است و پلتفرم-های بزرگ را وا داشته تا نسبت به حفظ داده‌های کاربران اروپایی اقدامات لازم را انجام دهد. گرچه گسترش جهانی پلتفرمهای جهانی و نفوذ آنها به حوزه قضایی جوامع مختلف ازجمله در ایران صیانت از داده‌های شخصی را به یک معضل

اساسی تبدیل کرده است، اما از سوی دیگر، تلاشهایی که طی دو دهه گذشته برای ارائه قانون جامع حفاظت از حریم خصوصی در فضای مجازی آغاز شده به سرانجام نرسیده است.

با ملاحظه لزوم حفظ حریم اشخاص، خانوادهها و گروههای اجتماعی در ایران بر اساس تأکیدات قانونی و شرعی و لزوم حکمرانی دادهها، به عنوان یک منبع ارزشمند، ضروری است تا هرچه سریعتر اقدامات تقنینی و اجرایی برای حفاظت و حراست از حریم خصوصی و دادههای شهروندان ایرانی مورد توجه قرار گیرد. این امر پیش از هرچیز نیازمند تعریف جامع و دقیق از حریم خصوصی، ابعاد گوناگون آن و نسبت آن با مفاهیم نزدیک همانند حریم دادههای شخصی است.

بنابراین این تحقیق اهداف مختلفی را پیگیری می کند که ازجمله آنها می‌توان به این موارد اشاره کرد: تعریف و مفهوم-سازی حریم خصوصی و دادههای شخصی؛ مرور مطالعات پیشن درباره حریم خصوصی در ایران؛ مرور پیش‌نویس لایحه‌ها، قوانین و اسناد مرتبط با حریم خصوصی؛ استخراج مبانی نظری حریم خصوصی در فقه، قانون اساسی، قوانین بین الملل، قوانین گوناگونی که به نحوی به مسئله حریم خصوصی توجه کرده‌اند؛ مطالعه قوانین و مقررات مرتبط با حریم خصوصی در کشورهای دیگر؛ مطالعه سیاستهای حریم خصوصی در پلتفرمهای بزرگ جهانی که عموماً در شرایط ارائه خدمت، سیاست حریم خصوصی و حریم داده آنها منعکس شده است؛ و درنهایت ارائه یک سند راهبردی یا پیش‌نویس لایحه جامع حریم خصوصی در پلتفرمهای رسانه‌های اجتماعی.

سازماندهی پژوهش (فصل‌بندی):

فصل اول: کلیات تحقیق (مقدمه و طرح مسئله)

فصل دوم: مبانی نظری و مفهومی

فصل سوم: روش‌شناسی

فصل چهارم: تحلیل یافته‌ها

فصل پنجم: نتیجه‌گیری و ارائه پیشنهادات

فصل دوم

چارچوب نظری

مقدمه

این پژوهش مبتنی بر یک منظومه مفهومی است که ابعاد و سطوح گوناگون حریم خصوصی و داده‌های شخصی را دربرمی‌گیرد. از یک منظر، تأکید بر وجه حکمرانی و تنظیم‌گری حریم خصوصی است. این نگاه جایگاهی محوری دارد و بر طبق آن باید برای فهم حریم خصوصی با ملاحظه حرکت از اینترنت به عنوان مفهومی عام به پلتفرمی‌شدن اینترنت، از دو منظر حکمرانی بر پلتفرم‌ها و حکمرانی توسط پلتفرم‌ها به موضوع تنظیم‌گری حریم خصوصی توجه شود. به عبارت دیگر، ایده مبنایی این پژوهش این است که با توجه به سلطه پلتفرم‌ها، از شبکه‌های اجتماعی گرفته تا پیام‌رسان‌ها و پلتفرم‌های خدمات‌رسان، هر نوع مقررات‌گذاری درباره حفاظت از داده‌ها و حریم خصوصی باید با ملاحظه این تحول اساسی باشد. بنابراین، قابلیت‌های فنی و اقدامات تنظیم‌گرانه آنها درمورد حریم خصوصی و حفاظت از داده‌ها اهمیت دارد. هرچند باید در نظر داشت که علاوه بر سازوکارهای پلتفرم‌ها در مورد بهره‌برداری از داده‌های شخصی، مقررات دولتها و نهادهای قانون‌گذار که در قالب *حکمرانی بر پلتفرم‌ها* بیان می‌شود و هدف نهایی این پژوهش کمک به این روند است، نیز مورد توجه قرار دارد.

توجه به ملاحظات مرتبط با حکمرانی و تنظیم‌گری حریم خصوصی و داده‌های شخصی (حکمرانی محتوا)، الگوی حکمرانی مقررات–مدار و حفاظت‌گرا برای پاسداشت حریم خصوصی به مثابه یک حق بنیادین، اسناد جهانی مرتبط با حریم خصوصی، رویکرد مصلحت اجتماعی در فقه، مبانی دینی مرتبط با حریم خصوصی، فتوای رهبری مبنی بر اهمیت حفظ حریم خصوصی در فضای مجازی و حق حاکمیت دیجیتال، چارچوب مفهومی این پژوهش را تشکیل می‌دهند. بر این اساس باید گفت که سیاستگذاری و تنظیم‌گری حریم خصوصی مستلزم توجه به منظومه‌ای درهم‌تنیده از الزامات فنی، مقررات جهانی–ملی، مفاهیم دینی و ارزشهای اجتماعی و فردی است.

الف) حکمرانی و حریم خصوصی

حکمرانی فضای مجازی: از حکمرانی اینترنت تا حکمرانی پلتفرمی

هدف این بخش مفهوم‌پردازی حکمرانی اینترنت و حکمرانی پلتفرم‌ها با تمرکز بر حفاظت از داده‌های شخصی و حریم خصوصی است. ایده محوری این بخش این است که طی دو دهه گذشته با فراگیر شدن پلتفرم‌های رسانه‌های اجتماعی،

مسائل و چالش‌های مرتبط با نحوه تنظیم‌گری حریم خصوصی و حفاظت از داده‌های شخصی از اینترنت به شکل عام به سمت حکمرانی اینترنت گرایش پیدا کرده است. بنابراین تلاش می‌شود ضمن مفهوم‌سازی حکمرانی اینترنت و گذار آن به حکمرانی پلتفرمی، بحث‌های مرتبط با حریم خصوصی به‌مثابه موضوع کانونی این تحول نیز واکاوای شود.

-حکمرانی اینترنت

حکمرانی اینترنت به مجموعه‌ای از قوانین، سیاست‌ها و رویه‌هایی گفته می‌شود که نحوه عملکرد اینترنت را شکل می‌دهند. اینترنت یک اکوسیستم پیچیده با ذی‌نفعان مختلف است و هیچ نهاد حاکم واحدی مانند دولت وجود ندارد که همه چیز را دیکته کند.

حکمرانی اینترنت (حکومت اینترنت) یک مفهوم پیچیده و چندوجهی است که شامل تنظیم و هماهنگی جنبه های مختلف اینترنت می شود. طبق گفته لورا دناردیس[1]، از پژوهشگران برجسته در این زمینه، حکمرانی اینترنت شامل «ایجاد، اجرا و تحول نهادها و سازمان هایی است که توسعه پروتکل های فنی، تأمین زیرساخت شبکه، تخصیص فضای آدرس شبکه و هماهنگی استانداردها و شیوه های فنی را شکل می دهند» (دناردیس، ۲۰۱۴، ص ۶). کوربالیجا[2]، یکی دیگر از پژوهشگران برجسته در زمینه حکمرانی اینترنت، این دیدگاه را تأیید می کند و استدلال می کند که حکمرانی اینترنت شامل «توسعه و اجرای اصول، هنجارها، قوانین، رویه های تصمیم گیری و برنامه های مشترکی است که تکامل و استفاده از اینترنت را شکل می دهد» (کوربالیجا، ۲۰۱۶، ص ۱۵).

حکمرانی اینترنت شامل تنظیم و هماهنگی جنبه های مختلف اینترنت، از جمله استانداردهای فنی، زیرساخت شبکه و تنظیم محتوا می شود. رویکرد ذینفعان متعدد به حکمرانی اینترنت ضروری است، زیرا امکان مشارکت ذینفعان مختلف را فراهم می کند و تضمین می کند که علایق و دیدگاه های متنوع در نظر گرفته شود.

ظهور اینترنت مزایای فراوان و چالش‌هایی را به همراه داشته است، اما همچنین نگرانی هایی را در مورد حریم خصوصی و محافظت از داده های شخصی ایجاد کرده است. با توجه به اینکه اینترنت به طور فزاینده ای به مرکز زندگی روزمره ما تبدیل می شود، مکانیزم های حکمرانی اینترنت نقش اساسی در رسیدگی به این نگرانی ها و اطمینان از رعایت حقوق

[1].Leura Denardis
[2] . Jovan Kurbalija

کاربران در زمینه حریم خصوصی ایفا می کنند. حریم خصوصی یک مسئله مهم در حکمرانی اینترنت است که پیامدهایی برای حقوق فردی، امنیت و عملکرد کلی اینترنت دارد.

–حکمرانی اینترنت و بحث حریم خصوصی و حفاظت از داده‌ها

همانطور که رادو (۲۰۱۹) بحث کرده است، رشد تصاعدی اهمیت حکمرانی اینترنت به دلیل مسائلی همانند کنترل‌های شبکه، امنیت سایبری و نگرانی‌ها نسبت به حریم خصوصی، افزایش قدرت واسطه‌های خصوصی و ظهور دستورکار دیپلماسی سایبری روی داده است. کوربالیجا (۲۰۱۶) در بحث خود در مورد تحولات حکمرانی اینترنت طی دهه گذشته، به مسائلی اشاره می‌کند که با محوریت یافتن حریم خصوصی ارتباط پیدا می‌کند. مهم‌ترین تحول در سال ۲۰۱۰، تأثیر رشد سریع رسانه‌های اجتماعی بر بحث‌های مربوط به حکمرانی اینترنت، به ویژه در زمینه حفاظت از حریم خصوصی کاربران پلتفرم‌های رسانه‌های اجتماعی مانند فیس‌بوک بود. در سال ۲۰۱۳ نیز برخی موضوعات برجسته شد. مهم‌ترین تحول در سیاست دیجیتال جهانی، افشاگری‌های اسنودن در مورد برنامه‌های نظارتی مختلفی بود که توسط آژانس امنیت ملی ایالات متحده[1] و سایر سازمان‌ها اداره می‌شد. افشاگری‌های اسنودن توجه عموم مردم جهان را به نحوه‌ی حکمرانی اینترنت جلب کرد. تمرکز اصلی این افشاگری‌ها روی حق حریم خصوصی و حفاظت از داده‌ها بود.

کوربالیجا (۲۰۱۶) مسائل گوناگون مرتبط با حکمرانی اینترنت را در هفت دسته گوناگون تقسیم‌بندی کرده است. این گروه‌ها عبارتند از:

–زیرساخت

–امنیت

–حقوقی

–اقتصادی

–توسعه

–اجتماعی–فرهنگی

–حقوق بشر

[1]. US National Security Agency (NSA)

کوربالیجا (۲۰۱۶) حریم خصوصی را زیر گروه یا سبد حقوق بشر مورد بحث قرار داده است. حریم خصوصی و حفاظت از داده، با چندین سبد از سبدهای حکمرانی اینترنت مرتبط هستند: حقوق بشر، زیرساخت (توسعه استانداردهایی برای مدیریت داده)، امنیت (دسترسی به داده برای حفاظت از امنیت ملی و مبارزه با جرم) و اقتصاد (پردازش داده به عنوان مبنایی برای یک مدل کسب و کار).

حریم خصوصی و حفاظت از داده دو مسئله به هم مرتبط در حکمرانی اینترنت هستند. حریم خصوصی معمولاً به عنوان حق شهروندان برای کنترل اطلاعات شخصی خود و تصمیم‌گیری در مورد افشای آن یا عدم افشا تعریف می‌شود. حفاظت از داده یک مکانیسم حقوقی است که حریم خصوصی را تضمین می‌کند.

حریم خصوصی یک حق اساسی بشر است. این حق در اعلامیه جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی و بسیاری از کنوانسیون‌های دیگر حقوق بشر بین‌المللی و منطقه‌ای به رسمیت شناخته شده است.

فرهنگ‌های ملی و شیوه‌های مختلف زندگی بر رویه‌ی حریم خصوصی تأثیر می‌گذارند. حریم خصوصی به طور خاص در جوامع غربی اهمیت ویژه‌ای دارد، به عنوان مثال، آلمانی‌ها اهمیت زیادی برای حریم خصوصی قائل هستند. شیوه‌های مدرن حریم خصوصی بر حریم خصوصی ارتباطات (عدم نظارت بر ارتباطات) و حریم خصوصی اطلاعات (عدم رسیدگی به اطلاعات مربوط به افراد) تمرکز دارند. به طور سنتی، نگرانی‌های مربوط به حریم خصوصی با نظارت دولت مرتبط بوده است. با این حال، به طور فزاینده‌ای، مسائل حریم خصوصی به نقض آن توسط بخش خصوصی نیز مربوط می‌شود (کوربالیجا، ۲۰۱۶).

درمجموع درمورد نسبت میان حکمرانی اینترنت و حریم خصوصی باید گفت، با توجه به افزایش حجم داده‌های شخصی تولید شده، جمع‌آوری شده و پردازش‌شده به صورت آنلاین، حریم خصوصی و حفاظت از داده نقشی حیاتی در حکمرانی اینترنت ایفا می‌کنند. از آنجایی که اینترنت به بخش جدایی‌ناپذیر زندگی روزمره ما تبدیل شده است، تضمین حفاظت از داده‌های شخصی افراد به جنبه‌ای اساسی در حکمرانی اینترنت بدل گشته است. در اینجا به برخی دلایل کلیدی که چرا حریم خصوصی و حفاظت از داده در حکمرانی اینترنت ضروری هستند، اشاره می‌کنیم:

–حقوق بشر: حریم خصوصی یک حق اساسی بشر است که در قوانین و معاهدات بین‌المللی مختلف، مانند اعلامیه جهانی حقوق بشر و کنوانسیون اروپایی حقوق بشر (بایگریو، ۲۰۱۴)، ذکر شده است. حفاظت از حریم خصوصی و داده‌های شخصی برای حفظ کرامت و استقلال افراد در عصر دیجیتال ضروری است.

–اعتماد و اطمینان: تضمین حریم خصوصی و حفاظت قوی از داده برای حفظ اعتماد و اطمینان در فضای آنلاین حیاتی است. کاربران زمانی بیشتر در فعالیت‌های آنلاین مشارکت کرده و اطلاعات شخصی خود را به اشتراک می‌گذارند که احساس کنند داده‌هایشان محافظت می‌شود و حریم خصوصی‌شان مورد احترام قرار می‌گیرد (دناردیس، ۲۰۱۴).

–نوآوری و رشد اقتصادی: یک چارچوب قوی برای حفاظت از داده می‌تواند با ترویج شفافیت، پاسخگویی و رقابت عادلانه در بازار دیجیتال، نوآوری و رشد اقتصادی را تقویت کند. شرکت‌هایی که اولویت را به حریم خصوصی و حفاظت از داده می‌دهند، به احتمال زیاد اعتماد و وفاداری مشتریان را جلب می‌کنند (بایگریو، ۲۰۱۴).

–جلوگیری از آسیب: نقض حریم خصوصی و حفاظت از داده می‌تواند آسیب‌های قابل توجهی به افراد وارد کند، از جمله سرقت هویت، خسارات مالی، لطمه به اعتبار و پریشانی روحی. قوانین محکم حریم خصوصی و حفاظت از داده به کاهش این خطرات و ایجاد یک محیط آنلاین امن‌تر کمک می‌کند (دناردیس، ۲۰۱۴).

ایجاد توازن بین منافع: حکمرانی اینترنت باید در چارچوب حریم خصوصی و حفاظت از داده، تعادل بین منافع مشروع افراد، کسب‌وکارها و دولت‌ها برقرار کند. این امر نیازمند گفت‌وگوی مداوم، همکاری و تدوین سیاست‌ها و مقررات مؤثری است که منعکس‌کننده چشم‌انداز در حال تحول دیجیتال باشد (بایگریو، ۲۰۱۴).

در نتیجه، حریم خصوصی و حفاظت از داده‌ها اجزای حیاتی حکمرانی اینترنت هستند، زیرا به محافظت از حقوق افراد، حفظ اعتماد در فضای آنلاین، تقویت نوآوری، جلوگیری از آسیب و ایجاد تعادل بین منافع رقابتی کمک می‌نمایند. حکمرانی مؤثر اینترنت باید اطمینان حاصل کند که حریم خصوصی و حفاظت از داده در تمامی سطوح تعامل دیجیتال رعایت و مورد احترام قرار می‌گیرند.

باوجود اقدامات بین‌المللی برای حکمرانی جهانی اینترنت که یکی از مهمترین نمودهای آن حکمرانی چندذی‌نفعی بوده است، تلاش دولتها برای احیاء حق حاکمیت بر فضای مجازی و نیز بحث‌های جدیدی که بر اساس توسعه پلتفرم‌ها شکل گرفته است، این تلاش‌ها را دچار افول کرده است. باوجود برخی کوششها و تمایل باطنی برخی دولتها و رهبران سیاسی، هم‌پوشانی کامل حق حاکمیت در فضای واقعی و فضای مجازی، به لحاظ فناورانه و نیز شکل‌گیری شیوه زیست جهان‌گرایانه کاربران تا حد زیادی دور از ذهن، غیرمنطقی و غیرمنطقی است.

–چندپاره‌شدن اینترنت و برجسته شدن حق حاکمیت بر فضای مجازی

مفاهیم شبکه چندپاره و بالکانیزاسیون اینترنت[1] به قطعه‌قطعه شدن اینترنت به شبکه‌های جداگانه و منزوی اشاره دارند که تحت کنترل نهادهای مختلف مانند دولت‌ها یا شرکت‌ها قرار می‌گیرند. این پدیده ماهیت باز و به هم پیوسته‌ی اینترنت را که برای ارتباطات جهانی، نوآوری و پیشرفت حیاتی بوده است، به چالش می‌کشد.

به طور کلی، شبکه‌ی چندپاره به جدایی اینترنت به شبکه‌های متمایز اشاره دارد، در حالی که بالکانیزاسیون اینترنت مفهومی مرتبط است که تقسیم اینترنت به بخش‌های کوچک‌تر، منزوی و اغلب ناسازگار را توصیف می‌کند (مالکومسون[2]، ۲۰۱۶). هر دو فرآیند تحت تأثیر عوامل مختلفی از جمله ژئوپلیتیک، نگرانی‌های امنیت ملی و منافع تجاری هدایت می‌شوند.

میلتون مولر[3]، پژوهشگر برجسته در حوزه حکمرانی اینترنت، در آثار خود به مفهوم «بالکانیزاسیون اینترنت» پرداخته است. مولر از این اصطلاح برای توصیف فرآیند تکه‌تکه شدن اینترنت به شبکه‌های جداگانه و ناسازگار به دلیل عوامل مختلفی از جمله رقابت بر سر استانداردهای فنی، محدودیت‌های اعمال‌شده توسط دولت‌ها و منافع تجاری استفاده می‌کند.

مولر معتقد است که بالکانیزاسیون اینترنت، با تهدید ماهیت باز و به هم پیوسته‌ی اینترنت که برای تسهیل ارتباطات جهانی، نوآوری و پیشرفت ضروری بوده است، به یک دغدغه رو به رشد تبدیل شده است (مولر، ۲۰۱۷). از نظر او، این پدیده ناشی

[1] .Internet Balkanization
[2] . Malcomson
[3] . Milton Mueller

از اعمال حاکمیت ملی بر اینترنت است که منجر به اجرای سیاست‌ها و مقررات ملی می‌شود و در نهایت اینترنت جهانی را به شبکه‌های جداگانه تحت کنترل محلی تکه‌تکه می‌کند.

مفهوم مرتبط دیگر ملی‌گرایی اینترنت[1] است. ملی‌گرایی اینترنت به ایده‌ای اشاره دارد که اینترنت، به‌عنوان پلتفرمی جهانی برای برقراری ارتباط و به اشتراک گذاری اطلاعات، می‌تواند تحت تأثیر منافع ملی، سیاست‌ها و مقررات ملی قرار گیرد. این مفهوم شامل اعمال حاکمیت ملی بر اینترنت در داخل مرزهای یک کشور است که می‌تواند منجر به اجرای اقدامات مختلف برای کنترل و حکمرانی بر فضای دیجیتال شود. ملی‌گرایی اینترنت به چند طریق نمود پیدا می‌کند:

کنترل زیرساخت اینترنت: دولتی‌ها ممکن است برای تضمین امنیت ملی و استقلال استراتژیک، به دنبال اعمال کنترل بر زیرساخت فیزیکی اینترنت، مانند مراکز داده، کابل‌های زیردریایی و نقاط تبادل اینترنت باشند (دناردیس، ۲۰۱۴).

فیلترینگ و سانسور محتوا: دولت‌های ملی ممکن است اقداماتی برای فیلتر کردن یا مسدود کردن انواع خاصی از محتوای آنلاین که مضر، غیرقانونی یا از نظر سیاسی حساس تلقی می‌شوند، انجام دهند. این می‌تواند آزادی بیان و دسترسی به اطلاعات را محدود کند (دناردیس، ۲۰۱۴).

محلی سازی و حاکمیت بر داده‌ها[2]: دولت‌ها ممکن است از شرکت‌های اینترنتی بخواهند داده‌های کاربران را در داخل مرزهای ملی ذخیره کنند و آن‌ها را تابع قوانین و مقررات محلی قرار دهند. این عمل با عنوان بومی‌سازی داده‌ها شناخته می‌شود و می‌تواند بر حریم خصوصی و امنیت کاربران تأثیر بگذارد (مولر، ۲۰۱۷).

موضوع دیگر، حق حاکمیت و نیز حق حاکمیت دیجیتال است که طی سالیان اخیر بخش محوری در مباحث حکمرانی اینترنت را تشکیل می‌دهد.

-حق حاکمیت و حکمرانی اینترنت

[1] .internet nationalism
[2] . Localization and data sovereignty

احیاء حق حاکمیت درفضای مجازی یکی از دل‌مشغولی‌های اساسی رهبران سیاسی و برخی از فعالان و صاحبنظران سیاستگذاری اینترنت است. این رویکرد ازبرخی جهات در تقابل با *آزادی‌خواهی اینترنت*[1] قرار دارد. عبارت «*آزادی‌خواهی اینترنت*» به دیدگاهی ایدئولوژیک اشاره دارد که طرفدار حداقل دخالت و تنظیم دولت در فضای مجازی است.

در درون قلمروهای سرزمینی کنترل و نظارت بر فعالیت شهروندان و نهادها و در معنای ساده اداره کلیه امور اجتماعی-سیاسی و اقتصادی تحت اراده یک دولت مستقر مرکزی بوده است. قدرت مطلقه حاکم درون مرزهای خود اعمال حکمرانی می‌کند و طیفی از وظایف گوناگون از تأمین منابع تا حفظ نظم و صیانت از امنیت مرزهای ملی را، در تقابل با حاکمیت بیرونی، با توسل به راهبردها و فن‌های گوناگون بر عهده دارد. بااین‌همه طی دهه‌های اخیر و به‌طور خاص پس از دهه ۱۹۹۰ میلادی، به دنبال تحولات فناورانه و دیجیتال و به‌ویژه توسعه اینترنت این نظم مستقر به‌طور اساسی به چالش کشیده شد و هم مرزهای ملی کم‌رنگ- در تخیل و در واقعیت- شدند و هم پایه‌های قدرت مطلقه حاکم-دست کم به شکلی ظاهری-متزلزل شدند (حسنی، ۱۴۰۰). اما همانطور که اشاره شد اکنون این دیدگاه اساساً با چالش‌های اساسی مواجه شده است و برخی دولتها تلاش کرده‌اند تا با اتخاذ موضع فعالانه فعالیت پلتفرم‌های جهانی را در قلمرو سرزمینی خود ضابطه‌مند و آنها را وادار کنند از ارزشهای محلی و قوانین فعالیت شرکت‌های رسانه‌ای و فناورانه تبعیت نمایند. برای نمونه، قانون اجرای شبکه آلمان که ناشی از استیصال از مدل خودحکمرانی بود (مقامات آلمان معتقد بودند که شرکتهای پلتفرمی آمریکایی نظیر توئیتر و فیس بوک به درخواستهای آنها بسیار دیر و ناکافی پاسخ می‌دهند)، مقرر می‌دارد که شرکتهای پلتفرمهای بزرگ و غیرآلمانی باید مطالب «آشکارا غیرقانونی» را ظرف مدت کمتر از ۲۴ ساعت پس از طرح شکایت حذف کنند یا اینکه مشمول جریمه خواهند شد (حسنی، ۱۴۰۱: ۱۶۸).

باید خاطرنشان کرد که مجموعه اقدام‌ها و کوشش‌ها به منظور احیاء حق حاکمیت دولت‌ها در قلمرو مجازی «درحال شکل‌گیری» و حتی در ابتدای راه هستند و البته با ملاحظه تحولات پیچیده ناشی از افزایش سیطره پلتفرم‌ها بیش از پیش پیچیده‌تر می‌شود. برای نمونه، میلتون مولر به عنوان یکی از صاحب‌نظران حکمرانی اینترنت میلتون مولر، چالش ها و تناقضات اعمال حاکمیت در حاکمیت اینترنت را مورد توجه قرار داده است. مولر استدلال می‌کند که ویژگی‌های منحصربه‌فرد فضای سایبر، از جمله ماهیت جهانی و استقلال آن از قلمرو فیزیکی، اعمال مؤثر حاکمیت سنتی دولت-ملت

[1]. Libertarian Intenet

را دشوار می‌سازد. او بر اهمیت به رسمیت شناختن فضای مجازی به عنوان یک حوزه متمایز با مجموعه قوانین و هنجارهای خاص خود، به جای تلاش برای وادار کردن آن به چارچوب‌های حاکمیتی از پیش موجود، تأکید می‌کند (مولر، ۲۰۱۸).

درخاتمه این بحث باید اشاره کرد که مفهوم حکمرانی دیدگاهی «غیرمتمرکز» را در مورد تنظیم مقررات ارائه می دهد که صرفاً از دولت نشأت نمی گیرد، بلکه از مجموعه های (پیچیده و تعاملی) بازیگران بخش دولتی و خصوصی شکل می‌گیرد. یک موضوع دیگر رابطه حکمرانی و تنظیم‌گری است. همانطور که بللی (۲۰۱۶؛ ۲۰۱۹) اشاره کرده است، حکمرانی را می‌توان مجموعه ای از فرآیندها و نهادهایی در نظر گرفت که مقایسه ایده‌ها و دیدگاه‌های ناهمگون را سازماندهی می‌کند و در حالت ایده‌آل، پیشنهاد مشترک ابزارهای نظارتی جدید را برای حل مشکلات خاص ترویج می‌دهد. برعکس، تنظیم مقررات را می‌توان به عنوان مجموعه‌ای از ابزارهای نظارتی مختلف در نظر گرفت که محصول حکمرانی هستند (نقل شده در لیرسن، ۲۰۲۱).

در بخش پیش تلاش شد تا برخی اقدامات برای احیاء حق حاکمیت دولتها در فضای مجازی نشان داده شوند. توضیح داده شد که چگونه از گفتمان‌های «اینترنت باز[1]» در دهه ۱۹۹۰ به «بازگشت دولت تنظیم‌گر» (فلیو، ۲۰۲۴)، در حال حاضر رسیده‌ایم. یکی از نمونه‌های برجسته این تحول و چرخش سیاستگذاری[2]، مفهوم حق حاکمیت دیجیتال است که به طور خاص در سطح اتحادیه اروپا برجسته شده است.

-حق حاکمیت دیجیتال

حق حاکمیت دیجیتال در راستای احیاء حق حاکمیت در فضای مجازی قابل فهم است. به گفته پال و تیل (۲۰۲۰) مفهوم حاکمیت دیجیتال به یک اصطلاح قدرتمند در گفتمان سیاسی تبدیل شده است که به دنبال بازگرداندن جایگاه دولت ملی، از جمله اقتصاد ملی و شهروندان کشور، به عنوان یک مقوله مرتبط در حاکمیت جهانی زیرساخت‌های دیجیتال و توسعه فناوری‌های دیجیتال است. به عبارت دیگر، اصطلاح حاکمیت دیجیتال توسط دولت‌ها برای بیان این ایده استفاده شده

[1] .Open Intenet
[2]. policy turn

است که دولت‌ها باید دوباره قدرت خود را بر اینترنت تثبیت کنند و از شهروندان و کسب‌وکار خود در برابر چالش‌های متعدد برای تعیین سرنوشت در حوزه دیجیتال محافظت کنند.

حق حاکمیت دیجیتال به طور خاص در سطح اتحادیه اروپا مطرح و پیگیری شده است. رهبران وقت چهار کشور اروپایی شامل آلمان، فنلاد، استونی و دانمارک طی یک بیانیه در مارس ۲۰۲۱ مشترک به رئیس کمیسیون اروپا خواستار تسریع در حق حاکمیت دیجیتال و ایجاد بازارمشترک دیجیتال شدند. راهبران این چهار کشور نوشته بودند که «حاکمیت دیجیتال» به معنای افزایش توان فناورانه اروپا و توانایی آن در برقراری ارزش‌ها و قواعد در دنیایی است که محوریت آن فناوری است و در حال حاضر تحت سلطه کشورهای دیگر قرار دارد. در این نامه آمده است:

«ما می‌خواهیم ظرفیت‌ها و قابلیت‌های خود را در زمینه‌هایی که به دنبال افزایش خوداتکایی با شرکای دموکراتیک در سراسر جهان و بر اساس روابط قوی ورای اقیانوس اطلس هستیم، توسعه دهیم. در عین حال، ما می‌خواهیم همکاری و هم‌افزایی‌های متقابل را تقویت و توسعه دهیم. حاکمیت دیجیتال در مورد تکیه بر نقاط قوت ما و کاهش وابستگی‌های استراتژیک ما است، نه در مورد حذف دیگران یا اتخاذ رویکرد حمایت‌گرایانه. ما بخشی از دنیای جهانی با زنجیره‌های تأمین جهانی هستیم که می‌خواهیم به نفع همه توسعه دهیم.» (ای‌آرآرنیوز[1]، ۲۰۲۱).

فلمینگ (۲۰۲۱) می‌نویسد که این چهار رهبر کشور به همراه تعداد فزاینده‌ای از درخواست‌ها برای یک سیستم مبتنی بر قوانین که امکان مالکیت بیشتر بر دارایی‌های فناوری حیاتی در سطح محلی، ملی و منطقه‌ای را فراهم می‌کند، وارد عمل شده‌اند. از نظر وی، برای برجسته کردن چالشی که اروپا در کنترل سرنوشت دیجیتالی خود با آن مواجه است، این نامه بر سه حوزه کلیدی تأکید کرده است: ۱) شناسایی نقاط قوت بالقوه و ضعف‌های استراتژیک اروپا در حوزه فناوری؛ ۲) گسترش استفاده از بازارهای باز و زنجیره‌های تأمین برای جلوگیری از وابستگی بیش از حد به سیستم‌های اختصاصی و ۳) ایجاد یک چارچوب ارزیابی برای اطمینان از اینکه استفاده از فناوری همچنان با آرمان‌های گسترده‌تر اروپا برای ارائه منافع اجتماعی، علمی و اقتصادی مطابقت دارد.

یکی از دلایل عمده طرح ایده حق حاکمیت دیجیتال در اتحادیه اروپا نگرانی نسبت به سلطه پلتفرم‌های بزرگ و به‌ویژه آمریکایی بر داده‌های شهروندان اروپایی بوده است. این موضوع که در فهرست بیست پلتفرم بزرگ جهانی هیچ نام اروپایی

[1]. ERR News, 2021

به چشم نمی‌خورد و بیش از ۹۰ درصد از داده‌های داده‌های غربی در آمریکا میزبانی می‌شود، نگرانی‌های عمده برای طرح حق حاکمیت اروپا بر بازار دیجیتال و نیز حاکمیت داده بوده‌اند.

در گزارشی که پارلمان اروپا (۲۰۲۰) درباره حاکمیت دیجیتال منتشر کرده است، حریم خصوصی و حفاظت از داده‌ها به عنوان یکی از نگرانی‌های اصلی برای پیشبرد این ایده در سطح اتحادیه اروپا معرفی شده است. این نگرانی پیش از هرچیز ناشی از نفوذ شرکتهای غیراروپایی بیان می‌شود. همانطور که در صفحه سوم این گزارش می‌خوانیم:

شرکت‌های فناوری در حال جمع‌آوری انبوهی از داده‌های شخصی هستند و مدل اقتصادی مورد استفاده گوگل، اپل، فیس‌بوک، آمازون و مایکروسافت – که گاهی اوقات با عنوان «غول‌های پنج‌گانه» شناخته می‌شوند – تا حد زیادی بر جمع‌آوری و بهره‌برداری از داده‌های کاربران آنلاین برای ایجاد درآمد تبلیغاتی استوار است. رسوایی کمبریج آنالیتیکا نشان داد که چگونه پلتفرم‌های آنلاین همچنین قادر به استخراج داده‌های شخصی برای اهداف سیاسی هستند. این روندها، که اغلب با عنوان «سرمایه‌داری نظارتی» شناخته می‌شوند، در نهایت منجر به از دست دادن تدریجی کنترل شهروندان اروپا بر اطلاعات شخصی و حریم خصوصی آن‌ها می‌شود. نگرانی در اتحادیه اروپا در مورد چگونگی بازیابی کنترل شهروندان بر داده‌های دیجیتال (یا «ردپای» آن‌ها) در محیطی آنلاین که اکنون عمدتاً تحت سلطه شرکت‌های فناوری غیر اتحادیه اروپا قرار دارد، افزایش یافته است. نمونه اخیر، جنجال مربوط به توسعه راه‌حل‌های ردیابی تماس برای کنترل شیوع ویروس کرونا است. انتخاب‌های فناورانه‌ای که اپل و گوگل انجام داده‌اند، توانایی برخی از کشورهای عضو را برای طراحی راه‌حل‌های ردیابی تماس خودشان (مانند «استوپ کووید» در فرانسه) را با مشکل مواجه کرده و تلاش برای دستیابی به حاکمیت دیجیتال را تقویت کرده است. در دنیای پس از همه‌گیری کرونا، جایی که فناوری بدون شک نقش مهم‌تری ایفا خواهد کرد، چالش برای سیاست‌گذاران اتحادیه اروپا همچنان یافتن تعادل مناسب بین کنترل و حقوق حفظ حریم خصوصی باقی خواهد بود (پارلمان اروپا، ۲۰۲۰: ص.۳).

اتحادیه اروپا تاکنون چارچوبی بسیار سختگیرانه برای حفظ حریم خصوصی و داده ها اتخاذ کرده است که در راس آن، مقررات عمومی حفاظت از داده‌ها قرار دارد. این اتحادیه همچنین برای تقویت کنترل افراد بر داده‌های خود، حق "فراموش شدن[1]" و حق انتقال داده‌ها[2] را معرفی کرده است. این مجموعه اقدامات را در بخش تحلیل یافته‌ها مورد توجه قرار خواهیم داد.

[1]. right to be forgotten
[2] .data portability right

-محلی(بومی)سازی داده‌ها

یک مفهوم مرتبط دیگر در مورد حفاظت از داده‌ها که در راستای روند کلی حاکمیت داده‌ها قرار می‌گیرد، محلی‌سازی[1] داده‌ها است. بومی‌سازی داده، مفهومی که در سال‌های اخیر مورد توجه قرار گرفته است، به فرآیند ذخیره و پردازش داده‌ها در مرزهای ملی کشوری که در آن تولید شده‌اند اشاره دارد. این رویکرد توسط چندین کشور به عنوان ابزاری برای اعمال حاکمیت داده و ارتقاء حریم خصوصی، امنیت و دسترسی دولت به داده‌ها (هورل و لوباتو، ۲۰۱۸) اتخاذ شده است. با این حال، این رویکرد سوالات مهمی را در مورد تأثیر آن بر تجارت بین‌المللی، نوآوری و اقتصاد دیجیتال جهانی نیز مطرح می‌کند.

طرفداران بومی‌سازی داده استدلال می‌کنند که این امر کشورها را قادر می‌سازد تا از داده‌های شهروندان خود در برابر نظارت خارجی، تهدیدات سایبری و سوءاستفاده احتمالی بهتر محافظت کنند (هورل و لوباتو، ۲۰۱۸). همچنین به دولت‌ها اجازه می‌دهد تا انطباق با قوانین و مقررات ملی را تضمین کنند و همچنین از طریق سرمایه‌گذاری در زیرساخت و خدمات داده داخلی، توسعه اقتصادی محلی را تقویت کنند (دولت هند، ۲۰۱۸).

بومی‌سازی داده برای اعمال حاکمیت داده استفاده می‌شود. یکی از روش‌های رایج برای یک ملت برای اعمال حاکمیت داده، به ویژه اگر آن کشور در موقعیت غالب قدرت ژئوپلیتیکی نباشد، تصویب اقدامات بومی‌سازی داده است. به طور کلی، دولت‌ها می‌خواهند حاکمیت داده‌های شهروندان خود را بدون توجه به محل یا توسط چه کسی ذخیره می‌شود، مطالبه کنند. به معنای دقیق کلمه، بومی‌سازی اجباری داده به این معنی است که داده‌هایی که در داخل مرزهای ملی ایجاد می‌شوند باید در همان مرزها باقی بمانند (وو، ۲۰۲۱). همانطور که (وو، ۲۰۲۱) می‌گوید:

ذخیره‌سازی داخلی داده‌ها به دنبال افزایش کنترل بر اطلاعات شهروندان با انتقال تصمیم‌گیری و حق دسترسی به درون مرزهای قضایی است. همچنین این کار باعث می‌شود شرکت‌های خارجی نسبت به شرکت‌های داخلی در وضعیت نامناسب‌تری قرار بگیرند. این سیاست معمولا توسط دولت‌ها وضع می‌شود و تمامی سازمان‌هایی که در آن کشور فعالیت می‌کنند ملزم به رعایت آن هستند. دسترسی به این داده‌ها به ویژه در جریان تحقیقات جنایی یا فعالیت‌های نظارتی اهمیت ویژه‌ای دارد. علاوه بر این، با افزایش مشارکت شهروندان در حوزه محصولات فناوری و

[1] .data localization

سیاست‌های مرتبط با آن، تعهد سیاسی به حریم خصوصی افراد می‌تواند در صندوق‌های رأی تأثیرگذار باشد. زمانی که داده‌ها به صورت محلی ذخیره یا پردازش نمی‌شوند، سردرگمی و نگرانی زیادی در مورد اینکه قوانین کدام کشور حاکمیت در چه شرایطی بر آن داده‌ها اعمال می‌شود، به وجود می‌آید. بومی‌سازی داده به دنبال ساده‌سازی این موضوع است (وو، ۲۰۲۱: ۹).

از سوی دیگر، منتقدان بر این باورند که بومی‌سازی داده می‌تواند جریان داده‌های فرامرزی را محدود کند، هزینه‌ها را برای کسب‌وکارها افزایش دهد و اقتصاد دیجیتال جهانی را تکه‌تکه کند (مرکز اروپایی برای اقتصاد سیاسی بین‌المللی، ۲۰۱۷). علاوه بر این، ممکن است نتواند به طور مؤثر به نگرانی‌های مربوط به حریم خصوصی رسیدگی کند، زیرا ذخیره‌سازی داده‌های داخلی به طور خودکار امنیت بهتر داده‌ها را تضمین نمی‌کند (چاندر و له، ۲۰۱۵).

با توجه به این دیدگاه‌های رقابتی، برای سیاستگذاران ضروری است که مزایا و معایب بومی‌سازی داده را به دقت بررسی کنند و راه‌حل‌های متوازنی را برای حفظ حاکمیت داده بدون مانع اتصال جهانی جستجو کنند. استراتژی‌های بالقوه ممکن است شامل اجرای قوانین قوی حفاظت از داده، تقویت همکاری‌های بین‌المللی در زمینه امنیت سایبری و حکمرانی داده، و ترویج قابلیت حمل و قابلیت همکاری داده (هورل و لوباتو، ۲۰۱۸) باشد.

این دلایل ما را به بحث درباره شبکه ملی اطلاعات در ایران متصل می‌کند. بنابراین، با ملاحظه موضوع حریم خصوصی و امنیت داده بحث خواهیم کرد که شبکه ملی اطلاعات را چگونه می‌توان در راستای احیای حق حاکمیت دولت ایران و نیز محلی‌سازی داده‌های ایرانیان مورد توجه قرار دارد. مهمترین اقدام دولت ایران برای تثبیت حق حاکمیت خود در فضای سایبر، ایده شبکه ملی اطلاعات است. بخش بعد کاوشی در ابعاد و معنای شبکه ملی اطلاعات است.

-نقش شبکه ملی اطلاعات در حفاظت از حریم خصوصی، حفاظت از داده‌ها و حکمرانی داده

شبکه ملی اطلاعات همچنین به عنوان اینترنت ملی ایران یا اینترنت ملی شناخته می شود، پروژه ای است که توسط دولت ایران برای توسعه زیرساخت امن و باثبات اینترنت ملی آغاز شده است. هدف این شبکه ایجاد یک شبکه مستقل و محلی است که از اینترنت جهانی جدا شده و در برابر حملات سایبری خارجی آسیب پذیرتر باشد و همچنین کنترل دولت بر محتوای آنلاین و ارتباطات درون ایران را افزایش دهد.

راه‌اندازی شبکه ملی اطلاعات یکی از سیاست‌های کلی مورد تأکید مقامات ارشد ایران بوده است. نگرانی در مورد انتشار محتواهای نامناسب به‌واسطه ارتباط بدون مانع با شبکه جهانی اینترنت و نیز ضرورت‌های امنیتی از دلایل اصلی اقدام در جهت راه‌اندازی شبکه ملی اطلاعات بوده است. برای مثال، آیت‌الله خامنه‌ای رهبر انقلاب اسلامی ایران همواره بر «مدیریت» فضای مجازی تأکید دارد و از «رها بودن» فضای مجازی انتقاد می‌کند. وی در اول فروردین ۱۴۰۰ می‌گوید، «همه کشورهای دنیا روی فضای مجازی خودشان دارند اعمال مدیریت می‌کنند، درحالی‌که ما افتخار می‌کنیم به اینکه ما فضای مجازی را ول کرده‌ایم! این افتخار ندارد. فضای مجازی را بایستی مدیریت کرد». وی همچنین در خرداد ۱۳۹۶ تحقق شبکه ملی اطلاعات را مهمترین مسئله فضای مجازی ایران اعلام می‌کند که در زمینه تحقق آن کوتاهی شده است و نقش شبکه ملی اطلاعات را کنترل فضای مجازی در راستای ارزشهای اجتماعی بیان کرده است. وی در شهریور ۱۳۹۹ نیز مجدداً از عدم توسعه شبکه ملی اطلاعات انتقاد کرده است (آیت‌الله خامنه‌ای، ۱۴۰۰). در نوامبر ۲۰۲۲ وزیر ارتباطات وقت اعلام کرده بود که فقط ۵۹ درصد از شبکه ملی اطلاعات تاکنون محقق شده است و تحقق کامل آن به دو سال زمان دیگر نیاز دارد (آستانه، ۱۴۰۱). آقامیری دبیر شورای عالی فضای مجازی در مصاحبه‌ای در اواخر اسفند ۱۴۰۲ اعلام کرد میزان پیشرفت اهداف عملیاتی شبکه ملی اطلاعات تا پایان بهمن سال ۱۴۰۲ و براساس شاخص‌های جدید تعیین شده توسط مرکز ملی فضای مجازی، ۵۹,۱۸ است (آقامیری، ۱۴۰۲).

طرح «اینترنت ملی» درس سال ۱۳۸۴ با هدف کاهش وابستگی به شبکه جهانی اینترنت دنبال شد و باید طی سه سال راه‌اندازی می‌شد. در این دوره بازنمایی نادرست از این پروژه کلان به منزله یک شبکه داخلی و مجزا از شبکه جهانی اینترنت سبب واکنش منفی افکار عمومی شد. درنتیجه در سال ۱۳۸۹ پروژه اینترنت ملی در قانون برنامه پنجم توسعه ایران گنجانده شد و به «شبکه ملی اطلاعات» تغییر نام داد (فیروزآبادی، ۱۳۹۹).

طی دهه اخیر، کشمکش بر سر تعاریف مفهومی و ابعاد این شبکه ادامه داشته است و نهادهای گوناگون و به طور خاص شورای عالی فضای مجازی و مرکز ملی فضای مجازی تلاش کرده‌اند، ابعاد، زیرساختها و اهداف این شبکه را تعریف و تبیین کنند. شورای عالی فضای مجازی دو سند مهم را درباره شبکه ملی اطلاعات تصویب کرده است: سند «تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات» (۱۳۹۲) و سند «تبیین الزامات شبکه ملی اطلاعات» (۱۳۹۵) که در سال ۱۳۹۹ پس از بررسی مجدد ابلاغ شده است.

در سند«تبیین الزامات شبکه ملی اطلاعات» شبکه ملی اطلاعات به این شکل تعریف شده است: "شبکه ملی اطلاعات، به عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه ای مبتنی بر قرارداد اینترنت به همراه سوئیچ ها و مسیریاب ها و مراکز داده ای -است به صورتی که درخواست های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می شوند به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه های اینترانت و خصوصی و امن داخلی در آن فراهم شود" . (معاونت قوانین، ۱۳۹۵)[1]

بر اساس این سند، شبکه ملی اطلاعات زیرساخت فضای مجازی ایران و شبکه همه شبکه‌های ایران تعریف شده است که مستقل بودن در آن یک اصل اساسی دیگر است که باید امکان رصد، اشراف و اعمال سیاستهای حاکمیتی (اعمال سیاست های حاکمیتی (اقتصادی، فرهنگی، احتماعی و...) در زیرساخت و پشتیبانی از اعمال سیاستهای حاکمیتی در لایه‌های خدمات و محتوا) بر تمام ابعاد و لایه‌های شبکه را فراهم کند. این شبکه باید به شبکه های غیراز خود برای تامین زیرساختها، خدمات ارتباطی و پایه کاربردی مورد نیاز در داخل ایران متکی نباشد و ظرفیت و امکانات لازم را برای ارائه خدمات بومی و محتوای اسلامی و ایرانی فراهم کند.

فیروزآبادی (۱۳۹۹) یکی از دلایل اساسی راه‌اندازی شبکه ملی اطلاعات در ایران را، حفاظت از استقلال و امنیت در فضای مجازی ذکر می‌کند؛ وی اعتقاد دارد شبکه ملی اطلاعات نقش برجسته‌ای در تأمین آن دارد. خارجی بودن خدمات پایه و کاربردی همانند وابستگی به موتور جستجوی گوگل به معنای عدم استقلال در فضای مجازی مجازی و ناتوانی در اعمال حاکمیت است و درنتیجه برای حفظ استقلال، امنیت و مرزهای جمهوری اسلامی ایران در فضای مجازی تحقق شبکه ملی اطلاعات، همانند تجربه چین و روسیه، یک ضرورت اساسی است.

بر اساس سند «تبیین الزامات شبکه ملی اطلاعات»، این شبکه از لایه‌های مختلفی تشکیل شده است. از پایین به بالا این لایه‌ها عبارتند از: لایه زیرساخت، لایه خدمات شبکه ملی اطلاعات، لایه خدمات کاربردی و درنهایت لایه محتوا است که درمجموع دو لایه زیرساخت و خدمات را شکل می‌دهند و نظام حکمرانی (سیاستگذاری و تنظیم‌گری) بر کلیت آن اعمال می‌شود. با این همه، در فهرست خدمات شبکه ملی اطلاعات به انواع گوناگون خدمات اشاره شده است. خدماتی همانند خدمات زیرساختی ارتباطی، خدمات امنیت وسالم سازی، رصد و کنترل هوشمند و نیز خدمات پایه کاربردی می‌توان اشاره

[1] . https://qavanin.ir/Law/PrintText/259464

کرد؛ در این بخش بر عناصری همانند مرورگر بومی، پیام‌رسان و شبکه اجتماعی؛ سیستم عامل داخلی، رایانه داخلی، جویشگر داخلی و...اشاره شده است (فیروزآبادی، ۱۳۹۹) که درنهایت هدف خوداتکایی و بومی‌سازی اینترنت را دنبال می-کند.

با ملاحظه هدف این پژوهش، توجه به حریم خصوصی و حفاظت از داده‌ها در اسناد مرتبط با شبکه ملی اطلاعات الزامی است. در سند طرح کلان و معماری شبکه ملی اطلاعات برخی اهداف عملیاتی ذکر شده است. هدف ۲۷ در این سند «اجرای الزامات صیانت از حریم خصوصی و حقوق عامه در سطح شبکه ملی اطلاعات در چارچوب طرح مصوب شورای عالی فضای مجازی و قوانین کشور» است. این تنها اشاره به موضوع حریم خصوصی و داده است. اما در مقابل در مقدمه سند تبیین الزامات شبکه ملی اطلاعات، «حفاظت از اطلاعات و ارتباطات کاربران ایرانی دربرابر تهدیدات علیه امنیت و حریم خصوصی» مورد توجه قرار گرفته است. همچنین در بحث از سلامت محتوا بر صیانت از حریم خصوصی تأکید شده است. همچنین در ارائه خدمات ایمن در شبکه ملی اطلاعات، بر حمایت ویژه از حریم خصوصی و حقوق داده تأکید شده است. در سند راهبردی جمهوری اسلامی ایران در فضای مجازی، صیانت از حریم خصوصی و حقوق عامه به عنوان یکی از ارزشهای اساسی راهبرد جمهوری اسلامی در فضای مجازی برجسته شده است.

-برآمدن پلتفرم‌های جهانی و چالش‌های جدید حکمرانی

دومین روند کلان در حکمرانی اینترنت، علاوه بر مباحث ملی‌گرایی اینترنت، رشد فزاینده پلتفرم‌های جهانی و سیطره آنها بر ساحت‌های گوناگون اینترنت و نیز توسعه و تثبیت پلتفرم‌های محلی–از پلتفرم‌های ارتباطی تا پلتفرم‌های خدماتی–است. در عصر دیجیتال، پلتفرم‌ها به زیرساخت‌های ضروری‌ای تبدیل شده‌اند که تعاملات، اقتصاد و جوامع ما را شکل می‌دهند. این نهادهای دیجیتال، از شبکه‌های اجتماعی گرفته تا پلتفرم‌های تجارت الکترونیک، بر جنبه‌های مختلف زندگی ما تأثیر قابل توجهی دارند. با افزایش نفوذ آنها، نیاز به سازوکارهای حکمرانی مؤثر برای تضمین پاسخگویی، عدالت و حمایت از حقوق کاربران نیز افزایش می‌یابد.

تری فلیو (۲۰۲۱) برخی از تحولاتی را که به «دگرگونی بنیادین» در نگرشها نسبت به تنظیم‌گری محیط‌های آنلاین منجر شده است، با خوبی تشریح کرده است:

در ایالات متحده، این نگرانی‌ها را می‌توان در دوره‌ی انتقال از دولت اوباما به ریاست جمهوری ترامپ و طیف نگرانی‌هایی که انتخابات ریاست جمهوری ۲۰۱۶ برانگیخت، از انتشار اخبار جعلی در پلتفرم‌های رسانه‌های اجتماعی تا ادعاهای دخالت انتخاباتی توسط قدرت‌های خارجی مشاهده کرد. اتحادیه اروپا تصمیم گرفت در مورد نگرانی‌های گسترده در مورد سوء استفاده از داده‌های شخصی آنلاین اقدام کند؛ مقررات عمومی حفاظت از داده‌ها در سال ۲۰۱۶ تصویب شد و در سال ۲۰۱۸ به قانون تبدیل شد و مقرراتی را در مورد چگونگی استفاده پلتفرم‌های دیجیتال و سایر نهادهای آنلاین از مطالبی که توسط «افراد موضوع داده» آنلاین ارائه می‌شود، وضع کرد....مقررات عمومی حفاظت از داده‌ها از نظر زمانی مقدم بر رسوایی کمبریج آنالیتیکا بود – یعنی افشاگری‌های کریستوفر ویلیِ[۱] سوت‌زن، نزد روزنامه‌نگار گاردین، کارول کادوالادر[۲]، در سال ۲۰۱۸، در مورد چگونگی فروش داده‌های جمع‌آوری‌شده از طریق فیس‌بوک به کمپین‌های سیاسی مانند گروه «رأی به خروج[۳]» در همه‌پرسی برگزیت ۲۰۱۶ در بریتانیا و کمپین ترامپ در ایالات متحده. با این حال، این رسوایی طیف وسیعی از نگرانی‌هایی را که در مورد قدرت پلتفرم‌های دیجیتال و امکان سوء استفاده از آن وجود داشت، به طور قابل توجهی برجسته کرد. بحث در مورد «حمله جهانی به شرکت‌های بزرگ فناوری[۴]» و ظهور FAANG یا FAMGA – مخفف فیس‌بوک، اپل، آمازون، نتفلیکس و گوگل، یا در نسخه‌ای متفاوت، فیس‌بوک، اپل، مایکروسافت، گوگل و آمازون – به امری عادی تبدیل شد (فلیو، ۲۰۲۱: ۱۳).

همانند رویکرد فلیو در کتاب خود، استدلال این پژوهش این است که درخواست و الزام فزاینده برای تنظیم بیشتر اینترنت، ازجمله تنظیم‌گری حریم خصوصی به طور جدایی‌ناپذیری به *پلتفرمی‌شدن*[۵] اینترنت مرتبط است – یعنی فرآیندی که از طریق آن، تعاملات و مشارکت‌های آنلاین به طور فزاینده‌ای بر تعداد نسبتاً کمی از پلتفرم‌های دیجیتال متمرکز می‌شود (فلیو، ۲۰۲۱). بنابراین، برای فهم بهتر نحوه تنظیم‌گری حریم خصوصی و حفاظت از داده‌ها به جای تکیه به مفاهیم عامی همانند فضای مجازی و اینترنت باید بر تحولات ناشی از جایگیر شدن پلتفرم‌ها تمرکز کرد. به‌عبارت دیگر، پلتفرم‌ها قابلیت‌ها و سازوکارهایی را ایجاد کرده‌اند که کاربران خودخواسته انواع گوناگون داده‌ها و تمام اطلاعات خود را با دیگران به اشتراک می‌گذارند.

---

1. Christopher Wylie
2. Carole Cadwalladr
3. Vote Leave group
4. global techlash
5. platformization

-حکمرانی پلتفرم‌ها: حکمرانی در و بر پلتفرم‌ها

اینترنت، که زمانی به عنوان یک آرمان‌شهر غیرمتمرکز تصور می‌شد، تحت سلطه‌ی تعداد معدودی از پلتفرم‌های قدرتمند قرار گرفته است. این پلتفرم‌ها، مانند فیس‌بوک، گوگل و آمازون، اساساً نحوه‌ی تعامل، مصرف اطلاعات و حتی انجام تجارت ما را تغییر داده‌اند. این تغییر اساسی، ارزیابی مجدد و انتقادی حکمرانی را ضروری می‌کند – اینکه این پلتفرم‌ها چگونه در درون خود عمل می‌کنند (حکمرانی توسط پلتفرم‌ها) و چگونه توسط بازیگران خارجی پاسخگو نگه داشته می‌شوند (حکمرانی پلتفرم‌ها).

پلتفرم‌های اینترنت به بازیگران کلیدی در حاکمیت بر فضاهای دیجیتال و شکل‌دهی تعاملات آنلاین تبدیل شده‌اند. حکمرانی پلتفرم‌ها را می‌توان ترکیبی از «حکمرانی توسط پلتفرم‌ها» و «حکمرانی پلتفرم‌ها» در نظر گرفت (گوروا[1]، ۲۰۱۹) که اولی بر رویه‌های داخلی پلتفرم‌ها و دومی بر مقررات خارجی تمرکز دارد.

حکمرانی *توسط پلتفرم‌ها*[2] شامل قوانین، مقررات و سیاست‌هایی است که توسط پلتفرم‌ها تدوین می‌شود و کاربران، محتوا و داده‌ها را مدیریت می‌کند. پلتفرم‌ها از طریق شرایط خدمات، استانداردهای جامعه، سیاست‌های تعدیل محتوا و مدیریت الگوریتمی، تجربیات آنلاین را شکل می‌دهند (دناردیس و هاکل، ۲۰۱۵). با اجرای این اقدامات، پلتفرم‌ها می‌توانند به عنوان تنظیم‌کننده‌های خصوصی عمل کرده و نفوذ خود را فراتر از قوانین و مقررات ملی گسترش دهند (گوروا، ۲۰۱۹). این جنبه از حکمرانی، نگرانی‌هایی را در مورد تمرکز قدرت در پلتفرم‌ها و تأثیر آن بر حقوق و آزادی‌های کاربران ایجاد می‌کند.

حکمرانی توسط پلتفرم‌ها اشکال مختلفی به خود می‌گیرد. برخی از شناخته‌شده‌ترین اشکال آن، تدوین و اجرای قوانین و استانداردهای کلی مانند «دستورالعمل‌های اجتماع[3]» و «شرایط ارائه خدمت[4]»، و همچنین رویه‌های «تعدیل محتوا» است که ادعا می‌شود برای اجرای این اصول به کار گرفته می‌شوند (لیرسن[5]، ۲۰۲۱).

حکمرانی *پلتفرم‌ها*[6] به تنظیم پلتفرم‌ها توسط ذینفعان خارجی مانند دولت‌ها، سازمان‌های جامعه مدنی و مردم مربوط می‌شود. این می‌تواند شامل ایجاد و اجرای قوانین و مقررات مربوط به حریم خصوصی، ضد انحصار و مسئولیت واسطه باشد

---

[1] .Gorwa
[2] . Governance by Platforms
[3] . Community Guidelines
[4] .Terms Of Service (TOS)
[5] .Leerssen
[6] . Governance of Platforms

(دناردیس و هاکل، ۲۰۱۵). علاوه بر این، از راه‌حل‌های قانونی و فشار عمومی می‌توان برای تحت تأثیر قرار دادن شیوه‌های پلتفرم‌ها و تضمین پاسخگویی استفاده کرد (گوروا، ۲۰۱۹).

تارلتون ژیلسپی[1] (۲۰۱۸) با مفهوم «سرپرستی[2]»، پیچیدگی‌های حکمرانی پلتفرم‌ها را بیشتر توضیح می‌دهد. این مفهوم پلتفرم‌ها را به عنوان میزبان و میانجی محتوای آنلاین به رسمیت می‌شناسد. ژیلسپی استدلال می‌کند که پلتفرم‌ها از طریق تعدیل محتوا[3] و مدیریت الگوریتمی، گفتمان آنلاین را مدیریت می‌کنند و بر گفتمان عمومی تأثیر می‌گذارند و سوالاتی را در مورد آزادی بیان و حاکمیت دیجیتال مطرح می‌کنند.

تعامل بین این ابعاد از حکمرانی پلتفرم‌ها، نیاز به چارچوب‌های فراگیر و دموکراتیک را که شفافیت، پاسخگویی و حمایت از حقوق کاربران را تقویت می‌کند، برجسته می‌کند (دناردیس و هاکل، ۲۰۱۵). رویکرد سرپرستی گلسپی بر اهمیت درک مسئولیت‌ها و نقش‌های پلتفرم‌ها در شکل‌دهی به فضای عمومی آنلاین تأکید می‌کند و بر لزوم بحث‌های دقیق در مورد حکمرانی پلتفرم‌ها تاکید می‌کند (ژیلسپی، ۲۰۱۸).

-تعدیل محتوا

به عنوان نکته‌ای مهم باید اشاره شود که حکمرانی توسط پلتفرم‌ها–همانطور که اشاره شد–عمدتاً تحت فرایند و سازوکار تعدیل محتوا انجام می‌شود. همانطور که لیرسن (۲۰۲۱) نیز اشاره کرده بود، تعدیل محتوا دراصل با هدف اجرای دستورالعمل های اجتماع و شرایط ارائه خدمت به اجرا گذاشته می‌شود. سیاست‌های داده[4] و نیز سیاست حریم خصوصی[5]دو مورد از مهمترین دستورالعمل‌هایی هستند که در بیشتر پلتفرم‌های بزرگ جهانی جزئیات گسترده‌ای را در مورد اطلاعات گردآوری‌شده از کاربران گرفته تا نحوه محافظت از داده‌های شخصی کاربران درآن ذکر شده است. بنابراین فهم اسناد و سازکارهای تعدیل محتوا در پلتفرم‌ها افق‌های گسترده‌ای در مورد حفاظت از حریم خصوصی پیش روی ما می‌گشاید.

---

[1]. Tarletton Gillespie
[2] . Custodianship
[3] .Content moderation
[4]. Data policy
[5] .Privacy policy

تعدیل محتوا به فرآیندها و رویه‌هایی گفته می‌شود که پلتفرم‌های دیجیتال برای مدیریت محتوای تولید شده توسط کاربران به کار می‌گیرند تا اطمینان حاصل شود که این محتوا با سیاست‌های پلتفرم و اصول کلی جامعه مطابقت دارد (ژپلسپی، ۲۰۱۸). با رشد تصاعدی محتوای آنلاین، اهمیت تعدیل محتوا در شکل‌دهی به فضاهای دیجیتال و گفتمان عمومی نیز افزایش یافته است.

به گفته گریملمن[1] (۲۰۱۵) تعدیل محتوا را می‌توان نتیجه‌ی تصمیمات تحریری فردی دانست که بر فضایی که اطلاعات در آن منتشر می‌شود، حاکمیت دارد. تعدیل همچنین به عنوان «مکانیزم‌های حکومتی که مشارکت در یک جامعه را برای تسهیل همکاری و جلوگیری از سوءاستفاده ساختار می‌دهند» تعریف شده است (نقل شده در دی‌گریگریو، ۲۰۲۱).

در یک تعریف دقیق‌تر، فلیو، مارتیتن و سازور[2] (۲۰۱۹).تعدیل محتوا را به این شکل تعریف شده است:

با توجه به سیاست‌های مرتبط نحوه ارتباط و انتشار مطالب مرتبط، غربالگری، ارزیابی، دسته‌بندی، تأیید، یا حذف/پنهان‌سازی محتوای آنلاین (...) برای حمایت و تقویت رفتارهای ارتباطی مثبت و به حداقل رساندن پرخاشگری و رفتارهای ضداجتماعی در فضای آنلاین (نقل شده در دی‌گریگریو، ۲۰۲۱).

درمجموع، فرایند تعدیل محتوا که به کمک عوامل انسانی و ناانسانی ازجمله یادگیری ماشین و هوش مصنوعی انجام می‌شود، مهمترین ابزار مدیران پلتفرم‌ها برای تنظیم گفتار و کردار در پلتفرم تحت حکمرانی و مدیریت آنها است. که البته، طی سالیان اخیر و با تثبیت بیشتری اینترنت تنظیم‌شده، برخی از پلتفرم‌ها همانند متا برخی از قوانین و مقررات ملی را نیز در شرایط ارائه خدمت خود گنجانده‌اند و خود را موظف با تبعیت از آن می‌دانند.

رویکرد سوم در حکمرانی پلتفرم‌ها، سازوکارهای خودتنظیم‌گری نیز نامیده می‌شودکه شامل سازوکارهای خودتنظیمی است که توسط خودِ اپراتورهای پلتفرم اجرا می‌شود. این سازوکارها شامل سیاست‌های داخلی، کدهای رفتاری و تعهدات داوطلبانه‌ای است که با هدف تنظیم رفتار پلتفرم و ترویج شیوه‌های مسئولانه به کار گرفته می‌شوند. پلتفرم‌ها اغلب برای مدیریت محتوای منتشر شده، رهنمودهای جامعه و توافقنامه‌های کاربر، سیاست‌هایی را وضع می‌کنند تا رفتار و محتوای

[1]. Grimmelman

[2]. Flew; Martin; Suzor, 2019

کاربران را کنترل کنند. رویکردهای خودتنظیمی بر استقلال، انعطاف‌پذیری و پاسخگویی پلتفرم‌ها به نیازهای کاربران تأکید دارند. این رویکردها به پلتفرم‌ها اجازه می‌دهند تا به‌سرعت با شرایط در حال تغییر سازگار شوند و در شیوه‌های حکمرانی نوآوری داشته باشند. با این حال، در مورد اثربخشی خودتنظیمی در پرداختن به مسائل سیستمی مانند سخنان نفرت‌انگیز، اطلاعات نادرست و سوگیری‌های الگوریتمی، تردیدهایی وجود دارد. منتقدان استدلال می‌کنند که خودتنظیمی ممکن است از شفافیت، پاسخگویی و نظارت مستقل برخوردار نباشد.

در نتیجه، حکمرانی پلتفرم‌ها همچنان یک موضوع پیچیده است که نیازمند تعادل ظریفی بین رویه‌های داخلی پلتفرم‌ها و مقررات خارجی است. بحث جاری پیرامون حکمرانی پلتفرم‌ها با بررسی پویایی قدرت، حقوق کاربران و گفتمان عمومی، نقشی اساسی در شکل‌دهی به آینده چشم‌انداز دیجیتال دارد[1].

موضوع حریم خصوصی افراد و صیانت از داده‌های کاربران که اکنون به یک دارایی باارزش با کاربردهای اقتصادی و سیاسی تبدیل شده است، برای برخی دولتها دارای محوریت مرکزی است، همانند اتحادیه اروپا، و برخی دولتها ازجمله دولت ایران نیز در تقابل با نشست گسترده اطلاعات شخصی کاربران در پلتفرم‌ها[2]، واکنش حداقلی و تلاش قانونگذارانه کند و با تأخیر را در پیش گرفته‌اند.

حکمرانی در پلتفرم‌ها، قابلیت‌های پلتفرم‌ها و سیاست حریم خصوصی و حفاظت از داده‌های شخصی

حفاظت از حریم خصوصی و داده‌های کاربران در پلتفرم‌ها متأثر از دو عامل است. از منظر نخست، دولتهای ملی، منطقه‌ای و نهادهای بین‌المللی مقرراتی را برای حفاظت از داده‌ها و حریم شخصی تدوین و بر پلتفرم‌های مختلف اعمال می‌کنند. ازجمله مهمترین این قوانین که برای همه شناخته شده است، مقررات عمومی حفاظت از داده‌ها در سطح اتحادیه اروپا است که پیشتر به طور مختصر درباره آن سخن گفته شده و به طور مفصل در بخش تحلیل یافته‌ها مورد بحث قرار می‌گیرد. اما یک بخش که کمتر در مورد آن سخن گفته شده است، حکمرانی در پلتفرم‌ها و نسبت آن با حریم خصوصی است. نظر به نو بودن، پیچیدگی و کمتر شناخته شده بودن آن در اینجا تلاش می‌شود تا تصویری از سازوکارهای فنی–فرهنگی پلتفرم‌ها و

[1] . در کتابها و مقاله‌های مختلف باجزئیات به این تفکیک پرداخته‌ام، بنابراین از توضیح بیشتر در مورد آنها خودداری می‌کنم.

[2] . نمونه آن افشای گسترده اطلاعات کاربران در اسنپ فود و هک برخی سازمانهای دولتی در سال ۱۴۰۲ است.

حریم شخصی ارائه شود. بعد فنی به عواملی همانند قابلیت‌های پلتفرم‌ها مرتبط است و بعد فرهنگی به کردارهایی همانند ضرورت خودافشایی برمی‌گردد که پیش‌شرط ارتباط در شبکه‌های اجتماعی بیان شده است و در سطحی وسیع‌تر به شکل‌گیری فرهنگ اشتراک‌گذاری منجر شده است.

قابلیت‌های پلتفرم[1] اصطلاحی است که برای توصیف ویژگی ها، امکانات و کارکردهای یک پلتفرم به کار می رود که بر تعاملات و رفتارهای کاربران تأثیر می گذارد و آن ها را محدود می کند. این مفهوم برگرفته از نظریه قابلیت‌های جیمز جی گیبسون[2] در روانشناسی، در بستر تعامل انسان و محیط زیست است. این مفهوم به ما کمک می کند تا بفهمیم که پلتفرم‌های دیجیتال چگونه بر شیوه تعامل کاربران با آنها تأثیر می‌گذارند (هلموند و باچر[3]، ۲۰۱۸).

یکی از قابلیت‌های مهم پلتفرم‌های رسانه‌های اجتماعی، اتصال و پیوند است که به کاربران امکان می‌دهد روابطی را با دیگران در سراسر مرزهای جغرافیایی ایجاد و حفظ کنند. این پلتفرم‌ها حس جامعه و تعلق را تقویت می‌کنند و به افراد اجازه می‌دهند تجربیات شخصی، افکار و احساسات خود را به اشتراک بگذارند (الیسون و همکاران، ۲۰۰۷). با این حال، این اشتراک مداوم اطلاعات شخصی ممکن است به سلب شدن حریم خصوصی منجر شود، زیرا کاربران ممکن است ناخواسته جزئیات حساس در مورد زندگی خود را فاش کنند.

قابلیت دیگر پلتفرم‌های رسانه‌های اجتماعی، قابلیت دیده‌شدن است که به کاربران صحنه‌ای برای به نمایش گذاشتن خلاقیت، عقاید و دستاوردهایشان می‌دهد (پاچراسی، ۲۰۰۹). در حالی که این قابلیت دیده شدن، کاربران را برای ابراز وجود و ساختن تصویر عمومی خود توانمند می‌کند، آن‌ها را در معرض نظارت بالقوه، توجه ناخواسته و حتی قلدری سایبری نیز قرار می‌دهد. علاوه بر این، ردپای دیجیتالی ماندگاری که در این پلتفرم‌ها باقی می‌ماند، می‌تواند پیامدهای درازمدتی برای شهرت و فرصت‌های آینده کاربران داشته باشد.

علاوه بر این، تنظیم الگوریتمی محتوا ازجمله قابلیت‌هایی است که تعامل کاربر را با شخصی‌سازی محتوا بر اساس ترجیحات و علایق فردی افزایش می‌دهد (باچر و هلموند، ۲۰۱۸). با این حال، این ویژگی به دلیل جمع‌آوری داده‌های گسترده و ایجاد پروفایل که برای شخصی‌سازی مبتنی بر الگوریتم مورد نیاز است، نگرانی‌هایی را در مورد حریم خصوصی

[1] . Platform affordance
[2] . James J. Gibson
[3] . Bucher & Helmond

ایجاد می‌کند (باچر و هلموند، ۲۰۱۸). چنین رویه‌هایی ممکن است منجر به از دست دادن کنترل کاربران بر اطلاعات شخصی خود شود و به سوء استفاده بالقوه از داده‌ها، نقض یا اشتراک‌گذاری غیرمجاز با اشخاص ثالث منجر شود.

در نهایت، ماهیت تعاملی پلتفرم‌های رسانه‌های اجتماعی به کاربران امکان می‌دهد در بحث‌ها شرکت کنند، در پروژه‌های مختلف همکاری داشته باشند و در اقدامات جمعی مشارکت کنند (باچر و هلموند، ۲۰۱۷). با این حال، این فعالیت‌ها اغلب شامل به اشتراک گذاشتن داده‌های شخصی، عقاید و ارتباطات است که خطرات مربوط به حریم خصوصی را بیشتر می‌کند. در نتیجه، امکانات پلتفرم‌های رسانه‌های اجتماعی نحوه برقراری ارتباط، ابراز وجود و تعامل ما با اطلاعات را متحول کرده است. با این حال، این امکانات همچنین چالش‌های جدیدی را برای حریم خصوصی ایجاد می‌کنند، زیرا عمل به اشتراک گذاشتن اطلاعات شخصی به طور فزاینده‌ای با ارتباطات اجتماعی، قابلیت دیده شدن و تعامل درآمیخته می‌شود. با تداوم روند تکامل رسانه‌های اجتماعی، برای کاربران، ارائه دهندگان پلتفرم و سیاستگذاران، رسیدگی مشترک به این نگرانی‌های مربوط به حریم خصوصی و تلاش برای ایجاد یک محیط دیجیتال امن‌تر و محترمانه‌تر ضروری است.

یک موضوع بااهمیت دیگر در حکمرانی به‌وسیله پلتفرم‌ها، تعدیل محتوا و ارتباط آن با خط‌مشی داده و حریم خصوصی است. تعدیل محتوا به جنبه‌ای ضروری برای حفظ یک محیط آنلاین سالم تبدیل شده است. با این حال، شیوه‌های مدیریت محتوا باید همراه با سیاست‌های قوی داده و حریم خصوصی باشد تا از حقوق و منافع کاربران محافظت شود.

از سوی دیگر، سیاست داده، نحوه جمع‌آوری، استفاده و به اشتراک گذاشتن داده‌های کاربر توسط پلتفرم‌ها را مشخص می‌کند. برای کاربران مهم است که بدانند چه داده‌هایی در مورد آنها جمع‌آوری می‌شود و برای چه اهدافی (بوید و کرافورد، ۲۰۱۲). سیاست‌های شفاف داده به کاربران کمک می‌کند تا درباره فعالیت‌های آنلاین خود تصمیمات آگاهانه بگیرند و پلتفرم‌ها را برای شیوه‌های مسئولانه داده پاسخگو کنند. این امر با توجه به حجم عظیمی از اطلاعات شخصی به اشتراک گذاشته شده در رسانه‌های اجتماعی و سایر پلتفرم‌های آنلاین، به‌ویژه اهمیت دارد.

سیاست حفظ حریم خصوصی که ارتباط نزدیکی با سیاست داده دارد، نحوه محافظت پلتفرم‌ها از حریم خصوصی کاربران و رسیدگی به اطلاعات حساس را بیان می‌کند. سیاست‌های حفظ حریم خصوصی باید اقدامات انجام شده برای محافظت از داده‌های کاربران در برابر دسترسی غیرمجاز، سوءاستفاده یا نقض را به طور واضح بیان کنند (سولوف[1]، ۲۰۱۳). علاوه بر

[1]. Solove

این، آنها باید به کاربران کنترل بر تنظیمات حریم خصوصی خود ارائه دهند و آنها را قادر سازد تا انتخاب کنند که چه اطلاعاتی و با چه کسی به اشتراک گذاشته شود.

در بخش پیش از منظر حکمرانی پلتفرمی به بحث حفاظت از حریم خصوصی و حریم داده‌ها توجه شد. در بخش بعد، رویکردهای نظری کلان مرتبط با حریم خصوصی و حفاظت از داده‌ها مورد ملاحظه قرار می‌گیرد.

ب) حکمرانی حریم خصوصی: رویکردهای کلان

از رویکرد حفاظت‌گرا تا مصلحت اجتماعی

رویکرد حفاظت‌گرا

برای فهم جامع حریم خصوصی و تدوین مقررات مرتبط بر اساس زمینه اجتماعی ایران، لازم است تا رویکردی کل‌نگر مد نظر قرار گیرد. بنابراین مجموعه‌ای از قوانین و مقررات بین‌المللی و منطقه‌ای، برخی قوانین ملی که بر فعالیت پلتفرم‌های جهانی نظارت دارند، اسناد درون‌پلتفرمی که حاصل ابتکار شرکتهای دیجیتالی گرداننده پلتفرمهای رسانه‌های اجتماعی و خدمات برخط است، مجموعه قوانین بالادستی در سطح ملی همانند قانون اساسی، منابع دینی (همانند برخی آیات قرآن و نیز فتوای رهبر انقلاب درباره پاسداشت حریم خصوصی در فضای واقعی)، قوانین گوناگون، شرایط ارائه خدمت پلتفرمهای ایرانی، مجموعه اقداماتی که تاکنون برای ارائه قانون حریم خصوصی در ایران انجام شده و مجموعه مطالعات گوناگون برای تدوین پیشنهاد، ارائه راهکارهای سیاستی و حتی ارائه پیش‌نویس حفاظت از حریم خصوصی و داده در ایران چارچوب مفهومی این پژوهش را تشکیل می‌دهند.

از میان سه رویکرد کلان حکمرانی پلتفرمها و اقتصاد دیجیتال در سطح جهان که بردفورد (۲۰۲۳) معرفی کرده است، یعنی مدل بازارمدار آمریکا[1]، دولت‌مدار چین[2] و حقوق مدار[3] در اتحادیه اروپا[1]، ما بر مدل اروپایی تمرکز می‌کنیم؛ زیرا محور آن

[1] .Market-driven regulatory model
[2] .Chinese State-driven regulatory model
[3] .European rights-driven regulatory model

حقوق شهروندان اروپایی و حفاظت از این حقوق و ارزشها است و با رویکرد مصلحت‌گرایانه در فرهنگ دینی ایران تا حدی ارتباط دارد.

رویکرد اتحادیه اروپا در حفاظت از حقوق بنیادین شهروندان خود، «حفاظت‌گرایانه» نیز نامیده شده است. هدف این رویکرد از یک طرف حفاظت از حقوق اساسی اروپاییان ازجمله حریم خصوصی آنها و از طرف دیگر مقابله با سلطه‌جویی پلتفرم‌های آمریکایی است (سلستی و همکاران، ۲۰۲۳). به همین دلیل آنها مجموعه مقررات گوناگونی را در این راستا تصویب کرده‌اند. حفاظت‌گرایی یا حمایت‌گرایی دیجیتال در این زمینه زمانی به وجود می‌آید که آن دولت‌ها اقداماتی را برای محافظت از داده‌های داخلی و بخش‌های فناوری خود در برابر نفوذ خارجی ارائه می‌کنند. این می‌تواند شامل الزامات ذخیره‌سازی داده‌های محلی، قوانین محلی‌سازی داده‌ها و محدودیت‌هایی در انتقال داده‌های مرزی باشد. هدف اولیه این اقدامات تضمین امنیت ملی، حفاظت از حریم خصوصی شهروندان و ترویج رشد صنایع فناوری داخلی است (کومرسکولگویم، ۲۰۲۰).

در نتیجه در عصر افزایش دیجیتالی شدن و جهانی شدن، رابطه بین حمایت گرایی، حریم خصوصی و حفاظت از داده ها همچنان در حال تکامل است. از آنجایی که کشورها تلاش می کنند از حقوق دیجیتالی شهروندان خود محافظت کنند، باید پیامدهای گسترده تر سیاست های خود را بر تجارت، نوآوری و همکاری بین المللی نیز در نظر بگیرند. ایجاد تعادل مناسب برای تضمین یک آینده دیجیتالی ایمن و باز بسیار مهم خواهد بود.

اتحادیه در زمینه مقررات گذاری درباره اقتصاد دیجیتال و حفاظت از داده های شهروندان پیشگام و پیشرو است. حمایت گرایی دیجیتال در اتحادیه اروپا با حمایت از حقوق اساسی پیوند تنگاتنگی دارد. برای مثال، مقررات عمومی حفاظت از داده‌ها به دنبال حمایت از حق حفظ حریم خصوصی و حفاظت از داده ها است که در ماده ۸ منشور حقوق اساسی ذکر شده است. به طور مشابه، دستورالعمل ان.آی.اس از حق امنیت با تقویت وضعیت امنیت سایبری اتحادیه اروپا و کشورهای عضو آن حمایت می کند. این اقدامات نشان دهنده تعهد اتحادیه اروپا به حفاظت از حقوق شهروندان خود در دنیای دیجیتالی فزاینده است (کونر، ۲۰۱۵).

---

[1]. در بخش چارچوب مفهومی این سه رویکرد شرح داده می‌شوند.

موضوع مهمی که در اینجا باید به آن اشاره شود، اهمیت حریم خصوصی در منشور حقوق اساسی اتحادیه اروپا است. منشور حقوق اساسی اتحادیه اروپا یک سند اساسی است که حقوق اساسی شهروندان اتحادیه اروپا را تدوین می‌کند و حمایت و ارتقای آنها را در همه کشورهای عضو تضمین می‌کند. در میان ارزش‌های اصلی مندرج در منشور، حریم خصوصی جایگاه برجسته‌ای دارد که نشان‌دهنده تعهد اتحادیه اروپا به حفاظت از زندگی شخصی و داده‌های شخصی افراد است. حریم خصوصی به عنوان یک حق اساسی در این منشور به رسمیت شناخته شده است. ماده ۷ منشور حقوق اساسی اتحادیه اروپا می گوید: «هر کس حق دارد به زندگی خصوصی و خانوادگی، خانه و ارتباطاتش احترام گذاشته شود». علاوه بر این، ماده ۸ بر حق حفاظت از داده های شخصی تأکید می کند و الزام می کند که این داده ها به طور منصفانه و برای اهداف قانونی پردازش شوند. این مقررات حریم خصوصی را به عنوان یک حق اساسی تعیین می کند و اهمیت آن را برای استقلال فردی، کرامت انسانی و عملکرد جوامع دموکراتیک به رسمیت می شناسد (گوتویرث و دیگران، ۲۰۰۹).

به رسمیت شناختن حریم خصوصی به عنوان یک حق اساسی در منشور چندین پیامد برای شهروندان اتحادیه اروپا دارد: محافظت در برابر مداخلات خودسرانه: شهروندان اتحادیه اروپا در برابر نفوذهای غیرقانونی به زندگی خصوصی، خانه و ارتباطات خود محافظت می شوند، مگر در مواردی که توسط قانون پیش بینی شده و در یک جامعه دموکراتیک ضروری است؛ کنترل بر داده های شخصی: افراد حق اعمال کنترل بر اطلاعات شخصی خود را دارند و اطمینان حاصل می کنند که به طور قانونی و شفاف پردازش می شوند؛ و راهکارهای جبران تخلفات: در صورت نقض حریم خصوصی، شهروندان اتحادیه اروپا این حق را دارند که از طریق دادگاه های ملی و اروپایی به دنبال راه حل موثر و جبران خسارت باشند.

حریم خصوصی و مصلحت در زمینه اجتماعی–حقوقی ایران

برای زمینه‌مند کردن چارچوب مفهومی بومی تعریف حریم خصوصی در ایران، با بسط استعاری مفهوم حفاظت‌گرایی به زمینه اجتماعی، فرهنگی و دینی جامعه ما می‌توانیم به مفهوم مصلحت نیز اشاره کنیم. منظور از مصلحت در اینجا مصلحت اجتماعی و به عبارت دیگر مصلحت اجتماعی است که گاهی سبب می‌شود مصلحت فردی و حقوق وی تحت‌الشعاع مصلحت اجتماعی قرار گیرد. به عبارت دیگر «همواره مصلحت نوعی و اجتماعی بر مصالح فردی تقدم دارد» (عزیزی و فلاح زاده، ۱۴۰۰). این اصل، نافی ضرورت حفظ و حراست از حریم شخصی افراد به عنوان یک اصل مورد تأکید بر منابع

دینی نیست. بلکه بر اساس این دیدگاه حفاظت از داده‌های شخصی و داده‌های عمومی به طور توامان باید مورد تأکید قرار گیرد. از سوی دیگر، برخی مصالح اجتماعی کلان همانند امنیت ملی به عنوان اصل خدشه‌ناپذیر این الزام–بیشتر موقت– را ایجاد می‌کند که در زمان رویدادهای بحران و تنشها، حریم شخصی فدای یک مصلحت کلان اجتماعی یعنی حفظ امنیت ملی به عنوان امنیت جامعه و شهروندان شود. البته، امنیت ملی با امنیت صاحبان قدرت در تعارض قرار دارد. مصلحت اجتماع نباید به منزله دستاویزی در دستان قدرتمندانی قرار گیرد که به جایگاه‌های کلیدی تنظیم‌گری فناوریهای ارتباطی دسترسی دارند و آزادیهای فردی را مورد تعرض قرار دهند. مصلحت همانگونه که از معنای این واژه برمی‌آید، بیانگر موقتی بودن و مشروط بودن در شرایط بحرانی است که امکان دارد کلیت یک جامعه و استقلال ملی به مخاطره افکنده شود.

دانش‌پور (۱۳۹۵) با بحث از اینکه دو خصلت «تنهایی‌دوستی» و «معاشرت‌جویی» در نهاد انسان پیوند نزدیکی با هم دارند، بحث می‌کند که حمایت از حریم خصوصی در فقه اسلامی به عنوان یک حق اساسی به رسمیت شناخته شده است و در قالب مصادیقی همانند منع تجسس و تفتیش، منع آزاررسانی به دیگران به آن تأکید شده است. بر این اساس، «مادام که ضرروت مبرم اجتماعی ایجاب نکند، مصلحت آن است که از افشای امور خصوصی افراد اجتناب شود». دربرخی موارد با انگیزه‌هایی همانند حفظ امنیت و منافع ملی و حکومتی، حفظ حوزه اخلاق اجتماعی، حفظ حقوق کار و حفظ بهداشت عمومی با تکیه بر برخی مستندات مثل تقدم اهم بر مهم، جلوگیری از اختلال نظام و حفظ دین، از طریق سازوکارهایی حدود و تغوری برای مصلحت فردی تعیین شده است و دفاع از حوزه عمومی و تقدم مصلحت جمعی را بر مبانی فقهی پشتیبان حریم خصوصی همچون سلطه، عدم ولایت، رازداری، ممنوعیتتجسس و مواردی نظیر امر حسبه مقدم داشته است (صص. ۱۵–۱۶).

در راستای نکته اخیر باید توجه داشت که همانطور که انصاری (۱۴۰۱) به روشنی بحث کرده است، توجه به حریم خصوصی ناشی از حمایت از آزادی و استقلال فردی در برابر دولت است و یکی از جنبه‌های حریم خصوصی، استقلال عمل و خودمختاری در حوزه خصوصی است. درنتیجه شناسایی حق حریم خصوصی در بیشتر موارد مستلزم آن است که اختیارات حکومت محدود شود تا حق دولت برای دخالت در امور خصوصی افراد تا حد ممکن محدود شود.

حریم خصوصی در نظام حقوقی بین‌المللی

حق حریم خصوصی، که بنیاد قوانین حفاظت از داده‌ها را تشکیل می‌دهد، در قوانین و کنوانسیون‌های بین‌المللی به طور قابل توجهی تکامل یافته است، که نشان‌دهنده‌ی اهمیت فزاینده‌ی آن در دنیای به هم پیوسته‌ی امروزی است. حق حریم خصوصی، که جنبه‌ای بنیادین از خودمختاری انسان به شمار می‌رود، در عرصه حقوق بین‌الملل، سفری قابل توجه را طی کرده است. در حالی که ریشه‌های آن را می‌توان در دکترین‌های حقوقی قدیمی‌تر جستجو کرد، به رسمیت شناختن صریح و تکامل آن در چارچوب اسناد حقوق بشر بین‌المللی، تحولی نسبتاً جدید محسوب می‌شود.

پیش از قرن بیستم، حمایت‌های قانونی از حریم خصوصی عمدتاً در نظام‌های حقوقی ملی وجود داشت و اغلب بر جنبه‌های خاصی مانند مصونیت خانه یا مکاتبات متمرکز بود. مفهوم جامع «حق حریم خصوصی» در سطح بین‌المللی به رسمیت شناخته نشده بود. با این حال، پیامدهای جنگ جهانی دوم شاهد یک تغییر اساسی در گفتمان حقوق بشر بود. جنایات ارتکابی در طول جنگ، یادآوری تلخی از ضرورت حفاظت از کرامت و خودمختاری بنیادین انسان به شمار می‌رفت.

مجموعه‌ای از اسناد و قوانین بین‌المللی از حق حریم خصوصی دفاع کرده و آنرا به عنوان یک اصل خدشه‌ناپذیر مورد تأکید قرار داده‌اند. امروزه، یک امروزه نوعی اجماع جهانی در مورد حق حریم خصوصی در تمام کشورها و در سطح بین‌الملل در مورد وجود حق حریم خصوصی وجود دارد (اسماعیلی، ۱۳۹۶) درواقع بسیاری از اسناد منطقه‌ای و بین‌المللی وجود دارند که بیانگر این است که حریم خصوصی یک جنبه حقوقی هم دارد و نباید در الزام‌آور بودن آن تردید کرد. برای مثال، ماده ۱۲ اعلامیه حقوق بشر مقرر کرده است که «احدی در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود نباید مورد مداخله خودسرانه واقع شود و شرافت و اسم و رسمش نباید مورد حمله قرار گیرد. هرکس حق دارد که در مقابل این گونه مداخلات و حملات مورد حمایت قانون قرار بگیرد» (نقل شده در اسماعیلی، ۱۴۰۱: ۱۱۴).

در سایر اسناد بین‌اللملی هم حمایت از حریم خصوصی مورد تأکید قرار گرفته است. ازجمله آنها می‌توان به ماده ۱۸ اعلامیه اسلامی حقوق بشر، ماده ۵ کنسوانسیون بین المللی منابع کلیه اشکال تبعیض نژادی ۱۹۶۶، ماده ۱۰ کنسوانسیون اروپایی حمایت از حقوق بشر و آزادی های اساسی و نیز مقررات عمومی حفاظت از داده‌ها مصوب سال ۲۰۱۸ اشاره کرد که کاملترین قانون مرتبط با حفاظت از داده های شخصی است (قناد و شریف، ۱۴۰۰).

در عصر اتصال دیجیتال و تولید داده های بی سابقه، حفاظت از حریم خصوصی و داده های شخصی به عنوان یک نگرانی مهم برای افراد، مشاغل و دولت ها در سراسر جهان مطرح شده است. با افزایش حجم جریان داده های فرامرزی، قوانین بین المللی نقش مهمی در تعریف استانداردهای حریم خصوصی و تقویت همکاری بین کشورها برای مقابله با چالش های نوظهور حفاظت از داده ایفا می کنند.

برای تعیین استانداردهای حریم خصوصی و حفاظت از داده، چندین ابزار و چارچوب بین المللی ایجاد شده است: اعلامیه جهانی حقوق بشر[1]: این اعلامیه که در سال ۱۹۴۸ توسط مجمع عمومی سازمان ملل متحد تصویب شد، یک سند بنیادی است که حریم خصوصی (ماده ۱۲) را به عنوان یک حق اساسی بشر به رسمیت می شناسد (سازمان ملل متحد، ۱۹۴۸).

میثاق بین المللی حقوق مدنی و سیاسی[2]: این میثاق در ماده ۱۷ صراحتاً حق حریم خصوصی را به رسمیت می شناسد و از کشورهای عضو می خواهد از افراد در برابر دخالت های خودسرانه یا غیرقانونی محافظت کنند (سازمان ملل متحد، ۱۹۶۶).

کنوانسیون برای حفاظت از افراد در خصوص پردازش خودکار داده های شخصی (کنوانسیون، ۲۰۱۸): این کنوانسیون که توسط شورای اروپا در سال ۱۹۸۱ تدوین و در سال ۲۰۱۸ به روز شد، تنها معاهده الزام آور بین المللی است که از حقوق افراد در زمینه پردازش خودکار داده ها محافظت می کند (شورای اروپا، ۲۰۱۸).

چارچوب حریم خصوصی سازمان همکاری و توسعه اقتصادی[3]: چارچوب حریم خصوصی سازمان همکاری و توسعه اقتصادی که در ابتدا در سال ۱۹۸۰ منتشر شد و در سال ۲۰۱۳ به روز شد، به عنوان راهنمایی برای کشورهای عضو برای توسعه قوانین و سیاست های حریم خصوصی عمل می کند (او.ای.سی.دی، ۲۰۱۳).

در حالی که کنوانسیون های بین المللی مبنایی برای حفاظت از حریم خصوصی را فراهم می کنند، اجرای استانداردهای جهانی حریم خصوصی و حفاظت از داده به دلیل تعامل پیچیده بین حاکمیت ملی و همکاری بین المللی همچنان چالش برانگیز است. هر کشوری دارای زمینه های فرهنگی، تاریخی و سیاسی منحصر به فردی است که رویکرد آن به حریم خصوصی و حفاظت از داده را شکل می دهد (گرینلیف، ۲۰۱۴).

---

[1] . UDHR
[2]. ICCPR
[3] . OECD

در سال های اخیر شاهد افزایش بومی سازی داده بوده ایم، زیرا کشورها نیاز دارند داده ها در داخل مرزهای ملی آنها ذخیره و پردازش شوند. این استراتژی تمایل به اعمال حاکمیت ملی بر داده ها را نشان می دهد، اما نگرانی هایی را در مورد تجزیه جریان داده های جهانی و افزایش موانع تجارت بین المللی ایجاد می کند (هوفبائر و لو، ۲۰۲۱).

برای آشتی دادن حاکمیت ملی و همکاری بین‌المللی، کشورها باید وارد گفتگو و مذاکره شوند تا مقررات هماهنگ حریم خصوصی و حفاظت از داده را ایجاد کنند. این امر از طریق توافق نامه های دوجانبه و چندجانبه، سازوکارهای اجرایی فرامرزی و اتخاذ چارچوب های قابل همکاری حفاظت از داده قابل دستیابی است (بردفورد، ۲۰۲۰).

چشم‌انداز حریم خصوصی و حفاظت از داده در قوانین بین المللی نیازمند یک تعادل ظریف بین ایجاد استانداردهای جهانی و احترام به حاکمیت ملی است. در حالی که کنوانسیون ها و چارچوب های بین المللی مبنایی برای حفاظت از حقوق افراد فراهم می کنند، کشورها باید برای رسیدگی مؤثر به چالش‌های نوظهور حفاظت از داده همکاری کنند. در راستای دستیابی به یک دنیای دیجیتال امن و به هم پیوسته، گفتگو و همکاری مستمر برای شکل دادن به آینده حریم خصوصی و حفاظت از داده ها در سراسر مرزها ضروری خواهد بود.

مباحث حریم خصوصی در ایران

بحثهای مرتبط با حریم خصوصی در ایران در دو دسته اساسی قرار می‌گیرند. بخشی از آنها برگرفته از قرآن و آیات و روایات هستند. دسته دیگر شامل مجموعه قوانینی هستند که به شکلهای گوناگون به حریم خصوصی توجه کرده‌اند. در همین زمینه به طور خاص می‌توان به فتوای آیت‌الله خامنه‌ای رهبر معظم انقلاب اسلامی اشاره کرد. رهبر انقلاب اسلامی با ابراز خرسندی از تبدیل شدن مطالبه ایجاد پیام‌رسان‌ها و شبکه‌های اجتماعی داخلی به مطالبه عمومی گفته‌اند: «مسئولان باید امنیت و حریم داخلی مردم و کشور را حفظ کنند. تعرض به امنیت و حریم مردم در پیام‌رسان‌های داخلی حرام شرعی است». همچنین ایشان در پاسخ به یک استفتاء اعلام کرده‌اند که «تجسس در امور شخصی و خصوصی دیگران جایز نیست و فرقی بین فضای مجازی و حقیقی نیست».

–حمایت از حریم خصوصی در اسلام) احترام به حریم خصوصی از توصیه‌های مؤکد اسلام است؛ به طوری که در منابع اسلامی ازجمله قرآن، سنت و اجماع، احکام مختلفی درباره مقوله‌های گوناگون حریم خصوصی وجود دارد. اصلاح حریم

خصوصی در آیات قرآن وجود ندارد و موضوع اسلام در مورد حریم خصوصی تحویل گرایانه است. به این معنا که در قالب احاله به حقوق و آزادی های دیگر همانند حق مالکیت، منع تجسس، اصل برائت، ممنوعیت اشاعه فحشا و منکر، منع سب و هجو و ...از آن حمایت شده است (انصاری، ۱۴۰). بر این اساس می‌توان مباحث مرتبط با حریم خصوصی در آیات و روایت را با عناوین ذیل دسته‌بندی کرد:

۱) ممنوعیت تجسس و تحسس و تفتیش (آیه ۱۲ سوره حجرات)؛ ۲) ممنوعیت ورود به منازل بدون استیذان (آیه ۲۷ سوره نور)؛ ۳) ممنوعیت استراق سمع و بصر؛ ۴) ممنوعیت سوءظن؛ ۵) ممنوعیت نمیمه و غیب؛ ۶) ممنوعیت اشاعه فحشا و هتک ستر (انصاری، ۱۴۰۱).

–حمایت از حریم خصوصی در قوانین) هم اکنون یک قانون جامع در مورد حریم خصوصی در ایران وجود ندارد. اما به برخی قوانین که بخشی از آنها به حریم خصوصی مرتبط هستند می توان اشاره کرد. از جمله آنها می توان اصطلاحات «اسرار شخصی» (قانون مطبوعات)، «اسرار مردم» (قانون مجازات اسلامی)، «داده‌های شخصی» و «حریم خصوصی» (قانون آزادی اطلاعات)، «صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری» (قانون جرایم رایانه ای) و نیز «حریم خصوصی» (مصوبات شورای عالی انقلاب فرهنگی و مجمع تشخیص مصلحت نظام) ذکر کرد (انصاری، ۱۴۰۱). به نظر می‌رسد اصطلاح «حریم خصوصی» در ایران متأخر و تابع تحولات بیرونی ازجمله توجه در سطح جهان به این حق و قانون با توجه به توسعه اینترنت و نگرانی نسبت به نقض این آن به واسطه توسعه پیچیده فناوری، و بازتاب آن در محافل دانشگاهی، رسانه‌ای و قانونگذاری ایران، روی داده است.

یکی از مهمترین اصول قانونی اساسی که با حریم خصوصی ارتباط دارد، اصل ۲۵ است که آشکارا از حریم خصوصی ارتباطات حمایت شده است: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون».

هرکدام از قوانین فوق به نحوی به حریم خصوصی پرداخته‌اند. در قانون اساسی به شکل مستقیم به حریم خصوصی اشاره نشده است. بلکه به شکل ضمنی و با اصطلاحات دیگری همانند حریم خلوت و تنهایی، حریم مکانی، حریم اطلاعات، حریم ارتباطات و حریم جسمانی به آن اشاره شده است (قناد و علیقلی، ۱۳۹۹). اصلهای ۱۹، ۲۰، ۲۲، ۲۳، ۲۴، ۲۶، ۲۷، ۲۸، ۳۰، ۳۲، ۳۳، ۳۵، ۳۸، ۳۹ و ۴۰ نیز به مفهوم حریم خصوصی اشاره کرده‌اند. درمجموع می توان گفت که درصورتی که

حریم خصوصی را به منزله حق خلوت و تنهایی، حریم مکانی، حریم اطلاعات، حریم ارتباطات و حریم جسمانی دسته بندی کنیم، در قانون اساس، داشتن حریم خصوصی به عنوان یک حق اساسی به رسمیت شناخته نشده است، از حریم خلوت و تنهایی حمایت نشده، از حریم خصوصی ارتباطات صریحاً حمایت شده و از حریم خصوصی جسمانی و حفظ کرامت انسانی و حفظ مال مسکن نیز به شکل ضمنی دفاع شده است (قناد و علیقلی، ۱۳۹۹).

در بخش تحلیل یافته‌ها به طور مفصل حریم خصوصی در ایران و قوانین اسلام مورد بحث قرار می‌گیرد. بنابراین به همین میزان از بحث مختصر بسنده می‌شوند.

در ادامه برخی دیگر از مفاهیم

حق (بر) حریم خصوصی

حق حریم خصوصی[1] یک حق بنیادین انسانی است که افراد را از دخالت یا تجاوز بی دلیل به زندگی شخصی، اطلاعات و حریم خصوصی آنها محافظت می کند. این حق شامل جنبه های مختلف زندگی فردی از جمله خودمختاری شخصی، تمامیت جسمانی، ارتباطات خصوصی و حفاظت از داده ها است. به عنوان یک حق به رسمیت شناخته شده جهانی، حریم خصوصی تضمین می کند که افراد توانایی کنترل و محدود کردن دسترسی به اطلاعات شخصی، افکار، احساسات و تجربیات خود را داشته باشند. این شامل حق آزادی از بازرسی و ضبط غیرمعقول، حق حفظ محرمانه بودن داده ها و ارتباطات شخصی و حق تصمیم گیری در مورد بدن و روابط شخصی بدون نفوذ یا اجبار خارجی نامناسب است.

همانطور که فلو (۲۰۲۱) می‌نویسد، حق حریم خصوصی به عنوان یک حق ذاتی انسانی در نظر گرفته می شود، هرچند که این حق در عمل با سایر حقوق، وظایف و هنجارهای رقیب محدود می شود. الکساندرا رِنگِل در بررسی تاریخی و فلسفی این مفهوم، دریافت که حق حریم خصوصی می تواند به موارد مختلفی اشاره داشته باشد، از جمله: حق تنها ماندن[2]، توانایی حفاظت از خود در برابر دسترسی ناخواسته دیگران، حق بر رازداری، کنترل بر اطلاعات شخصی، حفاظت از شخصیت، فردیت و کرامت فرد، و کنترل بر روابط صمیمانه یا جنبه هایی از زندگی فردی (رِنگِل، ۲۰۱۳). تعریفی که به طور معمول مورد استفاده قرار می گیرد، از عبارت "حق تنها ماندن" استفاده می کند که این عبارت از مقاله تأثیرگذار ساموئل وارن و

[1] .right to privacy
[2]. the right to be let alone’

لویی براندیس[1] که در سال ۱۸۹۰ در *مجله حقوقی هاروارد* منتشر شد، گرفته شده است. این مقاله به دلیل چالش هایی که عکاسی برای حفاظت از خود و حق خودداری از ارائه اطلاعات و اجتناب از مشاهده ایجاد می کرد، نوشته شد (فرانسیس و فرانسیس، ۲۰۱۷). (نقل شده در فلو، ۲۰۲۱).

ولیز (۲۰۲۴: ۱۷۸) استدلال می‌کند که حق حریم خصوصی، حق برخورداری از یک امتیاز با تقاضای قوی و الزام‌آور است (یعنی دارای مطالبات خلاف واقع یا احتمالی است). هنگامی که از حق حریم خصوصی برخوردار هستیم، اطمینان داریم که حریم خصوصی ما نه تنها در حال حاضر، بلکه در دنیای ممکن مرتبط (مثلاً مستقل از درآمد، یا دیدگاه‌های سیاسی یا مذهبی ما) نیز مورد احترام قرار خواهد گرفت. در مقابل، حریم خصوصی امتیازی است که به صورت گذرا (یعنی در حال حاضر) از آن برخوردار می‌شویم. به عبارت دیگر، حریم خصوصی و حق حریم خصوصی می‌توانند از هم جدا شوند. فردی می‌تواند حریم خصوصی داشته باشد و در عین حال حق حریم خصوصی او نقض شود. برعکس، ممکن است حق حریم شخصی کسی مورد احترام قرار گیرد در حالی که حریم خصوصی خود را از دست داده باشد.

موسی زاده و مصطفی‌زاده (۱۳۹۱) اعتقاد دارند که جایگاه «حق بر حریم خصوصی» در نظام حقوقی یک کشور از دو منظر قابل بررسی است: یکی از منظر حمایتی؛ یعنی می‌توان با جرم‌انگاری رفتارهای ناقض این حق و نیز اقدامات قضایی به مقابله با کسانی پرداخت که زندگی خصوصی و خلوت شهروندان را مورد تعرض قرار می‌دهند. دیگری از منظر مداخله و تهدید؛ یعنی دولت ممکن است در قلمرو خلوت و حریم خصوصی شهروندان اقدام به مداخله، ایجاد محدودیت و جرم‌انگاری در برابر اختیار و انتخاب آنها نماید یا ممکن است این حریم توسط مقامات کیفری و امنیتی در راستای کشف و تحقیق جرائم مورد نقض و تعرض قرارگیرد یا حتی ممکن است پیشگیری از وقوع جرم یا حفظ نظم اجتماعی، اخلاقی، بهداشتی و سیاسی موجبات دخالت در خلوت و زندگی خصوصی شهروندان را فراهم کند.

در بستر فناوری‌های دیجیتال و جوامع مبتنی بر داده، حق حریم خصوصی اهمیت فزاینده‌ای پیدا کرده است، زیرا اطلاعات شخصی افراد در مقیاسی بی‌سابقه جمع‌آوری، ذخیره و تحلیل می‌شود.

[1]. Samuel Warren and Louis Brandeis

نتیجه‌گیری

در این فصل موضوع حریم خصوصی و حریم داده بیشتر از منظر حکمرانی مورد ملاحظه قرار گرفت. در این فصل بحث شد که تغییر رویکرد کلی از موضوع حکمرانی اینترنت به حکمرانی پلتفرم‌ها سبب شده است تا بخش عمده بحث‌های با حریم خصوصی و حفاظت از داده‌ها با قابلیت‌های این پلتفرم‌های رسانه‌های اجتماعی درهم‌تنیده شود. از سوی دیگر، موضوع حکمرانی تنظیم‌گری حریم داده‌های کاربران نیز تا حد زیادی تابع سازوکارهای تعدیل محتوا یا خودتنظیم‌گری این پلتفرم‌ها شده است. البته، نباید فراموش کرد که در هر صورت از منظر حکمرانی بر پلتفرم‌ها، دولتها و نهادهای قانون‌گذار نقش مهمی در تنظیم مقررات مرتبط با حفاظت از داده‌ها و حریم خصوصی دارند. ازجمله آنها تلاش می‌کنند تا با مبنا قرار دادن مقررات بین‌المللی مرتبط با حریم خصوصی از یک طرف و نیز قوانین و مقررات محلی خود، پلتفرم‌ها را وادار کنند تا حقوق شهروندان و کاربران حفاظت کنند.

فصل سوم

روش‌شناسی

روش انجام پژوهش

این پژوهش از نوع تحلیلی و کیفی است. در انجام این پژوهش از رویکرد چند روشی[1] استفاده خواهد شد. رویکرد چندروشی شامل استفاده از روش‌های مختلف برای انجام یک پژوهش کیفی است که با روش‌شناسی ترکیبی[2] یا آمیخته از این حیث تفاوت دارد که رویکرد اخیر شامل استفاده از روش‌های پژوهشی کمی و کیفی با یکدیگر است (میک–میر[3]، ۲۰۲۰). در این پژوهش از روش تحلیل اسنادی و هم از روش تحلیل مضمون استفاده شده است. به عبارت دیگر، در این پژوهش برای گردآوری داده‌ها از روش تحلیل اسنادی و نیز برای تحلیل یافته‌ها از روش تحلیل مضمون استفاده کرده‌ایم. تحلیل اسنادی یا پژوهش اسنادی روشی است که در آن پژوهشگر برای جمع‌آوری داده‌ها و اطلاعات، به بررسی و تحلیل اسناد و مدارک موجود می‌پردازد. این اسناد می‌توانند شامل کتاب‌ها، مقالات علمی، گزارش‌ها، روزنامه‌ها، مجلات، مصاحبه‌ها، تصاویر، فیلم‌ها و هر نوع مدرک کتبی یا تصویری دیگری باشند که به موضوع پژوهش مرتبط باشند. در پژوهش حاضر ما عمدتاً از اسناد و منابع مکتوب شامل کتابها، مقالات علمی، گزارشها، مطالب مجله‌ها و نیز مصاحبه‌های مدیران و کارشناسان مرتبط با موضوع حریم خصوصی استفاده کرده‌ایم. تلاش شده است تا حد ممکن جستجو در پایگاه‌های اطلاعات علمی مختلف به زبان‌های فارسی و انگلیسی انجام شود تا داده‌های گردآوری شده از جامعیت لازم برخوردار باشند. بنابراین، از کلیدواژه‌های مختلفی استفاده شد و تمامی کتابها و مقاله‌های علمی مرتبط گردآوری و در صورت سودمندی در تحلیل مورد استفاده قرار گرفتند.

ایده گذران فرصت مطالعاتی از اوایل سال ۱۴۰۲ مطرح شد و این دوره از ابتدای اسفند ۱۴۰۲ تا اواخر مرداد ۱۴۰۳ به درازا کشید. پیش از آن مراحل نگارش نگارش طرحنامه و تصویب در شورای پژوهشی پژوهشگاه فرهنگ، هنر و ارتباطات انجام شده است. بنابراین، از طی چند ماه پیش از آغاز دوره فرصت مطالعاتی، که البته همراه با انجام برخی تعهدات پژوهشی دیگر نیز بوده است، مراحل گردآوری داده‌ها و آشنایی با ادبیات موضوع، شناسایی چهره‌های اصلی، درک مجموعه اقدامات انجام شده تا این دروان درباره موضوع حریم خصوصی در ایران، ازجمله برخی طرحها و لوایح به سرانجام نرسیده، آغاز شد و البته در طول دوره شش ماهه به اوج خود رسید.

---

1. Multi-method
2. Mixed-method
3. Mik-Meyer

بر اساس تعهدات ارائه شده در طرحنامه و برای پاسخگویی به مسئله اصلی پژوهش و نیز پرسشهای فرعی آن لازم بود تا گام‌ها و مراحل مختلفی طی می‌شود. بنابراین، این مطالعه یک طیف گسترده از فهم مفهوم حریم خصوصی و تاریخچه آن تا درک اقدامات کلان جهانی برای حفاظت از حریم خصوصی و حریم داده‌ها را دربرمی‌گیرد. در همین راستا، یک بخش از این مطالعه شامل مرور مجموعه مطالعاتی که در ایران درباره حریم خصوصی انجام شده است. علاوه بر بر اساس منابع موجود مفهوم حریم خصوصی در فقه و نیز قوانین و اسناد بالادستی و قوانین مرتبط از قانون اساسی گرفته تا اسناد شورای عالی فضای مجازی و نیز قوانین گوناگون و همینطور پیش‌نویس‌هایی که تاکنون درباره حریم خصوصی ارائه شده است، تحلیل و مضامین آنها استخراج می‌شود تا چه حریم خصوصی در قوانین ایران چه ابعاد دارد و چه ابعادی مورد غفلت واقع شده است. تحلیل رویکرد دینی به حریم خصوصی به ما کمک می‌کند تا یک رویکرد محوری را در تدوین مقررات حریم خصوصی شناسایی کنیم. یک بخش دیگر تحقیق تحلیل قوانین حریم خصوصی (با ملاحظه اینترنت و رسانه های اجتماعی) کشورها و مناطق پیشگام است. علاوه بر این اسناد حریم خصوصی برخی از پلتفرمهای بزرگ همانند گوگل، متا و توئیتر نیز به روش تحلیل محتوای کیفی مورد مطالعه قرار می‌گیرند. مجموع این مطالعات به ما کمک می کند تا تصویر مناسبی از قوانین کنونی مرتبط با حریم خصوصی و حریم داده در سطح جهان کسب کنیم و برای تهیه یک پیش‌نویس جامع قانون اساسی به کار بگیریم.

در این پژوهش برای تحلیل یافته‌ها از روش تحلیل مضمون استفاده شده است. برای انجام تحلیل مضمون از روشی که براون و کلارک در سال ۲۰۰۶ معرفی کرده‌اند استفاده شده است. آن دو در مقاله خود، روشی جامع و انعطاف‌پذیر برای تحلیل داده‌های کیفی به نام تحلیل مضمون یا تماتیک ارائه می‌دهد. تحلیل تماتیک به شناسایی، تحلیل، و گزارش الگوها (یا تم‌ها) در داده‌ها می‌پردازد و می‌تواند به شیوه‌ای ساختارمند انجام شود. مراحل اصلی تحلیل تماتیک شامل این موارد است: ۱) آشنایی با داده‌ها: در این مرحله، محقق باید خود را با داده‌ها آشنا کند. این شامل خواندن چندباره داده‌ها، یادداشت‌برداری و شناسایی ایده‌های اولیه است. هدف از این مرحله درک عمیق و جامع از داده‌ها می‌باشد؛ ۲) کدگذاری اولیه: در این مرحله، محقق بخش‌هایی از داده‌ها که به نظرش مهم هستند را کدگذاری می‌کند. این کدها می‌توانند عباراتی کوتاه باشند که مفهوم کلی قطعه‌ای از داده را توضیح می‌دهند. هدف این مرحله تفکیک داده‌ها به اجزای کوچک‌تر و قابل مدیریت است؛ ۳. جستجوی تم‌ها: در این مرحله، محقق کدهای ایجاد شده را بررسی کرده و آن‌ها را در دسته‌هایی که

تم‌های بالقوه هستند، سازماندهی می‌کند. تم‌ها باید نمایانگر الگوها و معانی درون داده‌ها باشند؛ ۴. بازبینی تم‌ها: در این مرحله، محقق تم‌های شناسایی‌شده را بازبینی و پالایش می‌کند. برخی از تم‌ها ممکن است کنار گذاشته شوند یا با تم‌های دیگر ادغام شوند. در این مرحله، محقق مطمئن می‌شود که تم‌ها با داده‌های اصلی هماهنگی دارند و به بهترین شکل نمایانگر معنای داده‌ها هستند؛ ۵. تعریف و نام‌گذاری تم‌ها: پس از پالایش تم‌ها، محقق هر تم را تعریف و توضیح می‌دهد. همچنین به هر تم یک نام مشخص و معنادار داده می‌شود که نمایانگر مضمون کلی آن باش؛ و ۶. نوشتن گزارش نهایی: در مرحله آخر، محقق یافته‌های خود را در قالب یک گزارش نهایی ارائه می‌دهد. این گزارش باید به وضوح چگونگی و چرایی شناسایی تم‌ها را توضیح دهد و نشان دهد که تم‌ها چگونه به سوال تحقیق پاسخ می‌دهند. بران و کلارک تأکید می‌کنند که تحلیل تماتیک روشی انعطاف‌پذیر و قابل تطبیق است و می‌تواند به محققان در استخراج معانی و الگوها از داده‌های کیفی کمک کند.

از آنجا که این پژوهش دارای بخشهای مختلفی است، بنابراین در هر بخش مضامین اصلی گوناگونی استخراج و مورد تحلیل قرار نگرفته‌اند. به عبارت دیگر، این پژوهش، برای مثال، شامل انجام مصاحبه با کارشناسان نبوده است تا مجموعه‌ای از مضامین اصلی و فرعی و کدهای استخراج شده معرفی و توضیح داده شوند. با این حال، درنهایت، مضامین اصلی هر بخش، در قالب یک مدل و الگوی کلی ارائه می‌شوند تا بتوانند تصویری جامع از مضامین عمده و فراگیر در اختیار ما قرار دهند تا بتوانیم از آنها برای جمع‌بندی و نتیجه‌گیری نهایی استفاده کنیم.

فصل چهارم

تحلیل یافته‌ها

بخش اول

مفهوم و ابعاد حریم خصوصی

(حریم داده و اطلاعات)

مقدمه

هدف این بخش فهم رویکرد کلی به حریم خصوصی در ایران است. علاوه براین، بر اساس منابع موجود مفهوم حریم خصوصی در فقه و نیز قوانین و اسناد بالادستی و قوانین مرتبط از قانون اساسی گرفته تا اسناد شورای عالی فضای مجازی و نیز قوانین گوناگون و همینطور پیش‌نویس‌هایی که تاکنون درباره حریم خصوصی ارائه شده است، تحلیل و مضامین آنها استخراج می‌شود تا چه حریم خصوصی اطلاعات و ارتباطات در قوانین ایران چه ابعاد دارد و چه ابعادی مورد غفلت واقع شده است.

همانطور که در بخش روش‌شناسی گفته شد، در هر کدام از مباحث مضامین اصلی و فرعی را ذکر می‌کنیم و بر اساس ادبیات موجود، نمونه‌هایی را که بیانگر کدهای زیرمجموعه هرکدام از این مضامین است، بیان می‌کنیم. سپس در خاتمه هربخش نیز آنها در قالب یک جدول ارائه می‌کنیم.

مفهوم حریم خصوصی

ما در تعریف امر خصوصی مجموعه‌ای

–حریم خصوصی به‌مثابه امری غریزی

انسان‌ها بنا بر فطرت خود، قلمروهایی را محدوده خصوصیِ خویش می‌دانند و در آن پناه می‌گیرند. در این پناه‌گاه امنِ خصوصی است که زندگی و حیات برای آنان میسور می شود و (انسانیت) معنا و مفهوم می یابد: شخصیت و آبرو، ناموس، خانه و محل کار و اموال از آن جمله اند. ورود خود سرانه و بی ضابطه به این قلعه مقدس در حکمِ کشتن افراد و فرو ریختنِ دیوار انسانیت آنان است (مهریزی، ۱۳۷۸).

-حریم خصوصی به عنوان امری تاریخی

به گفته علمای علوم اجتماعی نیاز به حریم خصوصی امری بسیار ریشه‌دار و نیازی فطری است که تنها به انسان‌ها محدود می‌شود و گونه‌های دیگر را نیز شامل می‌شود. از این می‌توان گفت که تفکیک حوزه خصوصی از حوزه عمومی به قدمت حیات انسان سابقه دارد. مطالعات مردم‌شناسی حاکی از این است که در تمام جوامع و در تمام دوره‌ها و حتی در جوامع ابتدایی، قواعد اجتماعی، ورود به برخی امکان را محدود و حضور در برخی امکان را ممنوع کرده است (محسنیان، ۱۴۰۰).

ولیز (۲۰۲۴) با تأکید بر غریزی بودن میل به حریم خصوصی بحث می‌کند که انسان‌ها به همان اندازه که به اجتماع نیاز دارند، به حریم خصوصی نیز نیازمندند. نیاز ما به معاشرت با خود خطرات و زیان‌هایی به همراه دارد که به نوبه خود باعث ایجاد نیاز به فضا و زمانی دور از دیگران می‌شود. ولیز در ادامه می‌گوید، زمانی که افراد سعی در کم اهمیت جلوه دادن حریم خصوصی دارند، اغلب از آن به عنوان یک اختراع فرهنگی یاد می کنند، که نشان می دهد این یک ترجیح مشروط است که به اجتماعی شدن بستگی دارد و نه یک نیاز عمیق انسانی. اما او معتقد است که حریم خصوصی ریشه در منبعی قدیمی‌تر از ترجیحات فرهنگی دارد. ریشه حریم خصوصی مهم است زیرا ترجیحات فرهنگی را می‌توان تغییر داد، گاهی اوقات بدون تأثیر منفی یا با تأثیر منفی کمی بر رفاه مردم، در حالی که نیازهای حیوانی اینطور نیست. وی بر این اساس اعتقاد دارد که حریم خصوصی ریشه در نیازهای انسانی یا غریزی انسان دارد.

-حریم خصوصی به مثابه نیاز به خلوت و جدایی از اجتماع

فارغ از منشاء غریزی حریم خصوصی، وستین (۱۹۶۷) به طور خاص در مورد چهار مبنا را برای حریم خصوصی افراد بیان می‌کند که عبارتند از:

۱. خلوت و تنهایی[1]: در این صورت افراد از گروه جدا شده، دور از چشم دیگر اشخاص زندگی می‌کنند.

۲. صمیمیت و الفت[2]: گاهی افراد به عنوان عضوی از یک واحد کوچک همانند خانواده عمل می‌کنند که درصدد است با ایجاد خلوت و تنهایی فیزیکی بتواند الفت و رابطه‌ای بسیار نزدیک و صمیمی میان دو یا چند فرد برقرار کند.

[1] .solitude
[2] .intimacy

۳. ناشناس ماندن[1]: این وضعیت هنگامی حادث می‌شود که فردی در عین حضور در مکانی عمومی، بخواهد آزادی خود را در اینکه ناشناس و مصمون از نظارت دیگران باشد حفظ کند.

۴. تحفظ[2]: این وضع هنگامی حادث می‌شود که نیاز افراد به محدود ساختن مخابره اطلاعات مربوط به آنها به دیگران و به‌ویژه به کسانی که روابط شخصی با آنها دارند مورد حمایت قانون قرار می‌گیرد (نقل شده در انصاری، ۱۴۰۰: ص.۱۵).

-تعریف حریم خصوصی

در این بخش قصد داریم تا حریم خصوصی را تعریف کنیم. تعریف حریم خصوصی و ارتباط آن با حریم داده‌ها در اینجا اهمیت دارد. همچنین باید توجه داشت که درنهایت حریم خصوصی در اینترنت، فضای مجازی و در عرصه پلتفرم‌های رسانه‌های اجتماعی مدنظر قرار دارد. بنابراین، درنهایت با تلفیق دیدگاه‌ّهای مختلف به حریم خصوصی، به تعریفی از حریم خصوصی خواهیم رسید که دربردارنده مفهومی جامع از حریم خصوصی باشد.

-حریم خصوصی به‌مثابه کنترل بر اطلاعات شخصی

حریم خصوصی یک مفهوم بنیادی است که به *توانایی افراد برای کنترل دسترسی و توزیع اطلاعات شخصی*، افکار و اعمالشان اشاره دارد. این مفهوم حق فرد را برای در امان بودن از جستجوی غیر منطقی، مزاحمت و افشای عمومی مسائل شخصی در بر می گیرد. حریم خصوصی به افراد این امکان را می دهد تا حس استقلال خود را حفظ کرده و زندگی شخصی خود را از زیر نظر گرفتن یا دخالت بی مورد دیگران محافظت کنند. در بستر فناوری و دنیای دیجیتال، حریم خصوصی شامل مدیریت امن داده‌ها است، به این معنی که اطلاعات شخصی بدون رضایت یا مجوز مناسب جمع آوری، به اشتراک گذاشته یا مورد استفاده قرار نمی گیرد. حفظ حریم خصوصی برای امنیت شخصی، عزت نفس و اعتماد در جنبه های مختلف زندگی از جمله تعاملات اجتماعی، ارتباطات و تراکنش های دیجیتال ضروری است.

همانطور که در بالا مشخص است، بین حریم خصوصی و حفاظت یا صیانت از داده‌ها رابطه مستقیمی وجود دارد. حفاظت از داده بر رویه ها و مقررات خاصی که بر نحوه مدیریت داده‌های شخصی حاکم است، تمرکز دارد. این امر عمدتاً بر اطمینان

[1] .anonymity
[2] .reserve

از پردازش، ذخیره سازی و انتقال امن اطلاعات برای جلوگیری از دسترسی غیرمجاز، سوء استفاده یا از دست رفتن آن متمرکز است. هدف از حفاظت از داده، حمایت از حقوق و آزادی های اساسی افراد، به ویژه حق آنها بر حریم خصوصی، با اطمینان از پردازش داده‌ها به روشی منصفانه، قانونی و شفاف است. به طور خلاصه، حریم خصوصی مفهومی گسترده تر است که حق فرد برای کنترل اطلاعات شخصی خود را در بر می گیرد، در حالی که حفاظت از داده بر اجرای اقدامات و مقرراتی برای اطمینان از رعایت و احترام به این حق در عمل تمرکز می کند. حفاظت موثر از داده، از حریم خصوصی پشتیبانی و تسهیل می کند و هر دو مفهوم برای ایجاد اعتماد و امنیت در عصر دیجیتال ضروری هستند.

حریم خصوصی، حق کنترل اطلاعات شخصی و فضایی که در آن زندگی می‌کنیم، همواره سنگ بنای یک جامعه آزاد و امن بوده است. با این حال، در عصر دیجیتال، این حق اساسی با چالش‌های بی‌سابقه‌ای روبرو است. جمع‌آوری و تحلیل مداوم داده‌های ما توسط شرکت‌ها، دولت‌ها و حتی افراد دیگر، دیوارهای زندگی خصوصی ما را فرسوده می‌کند و سوالات اساسی را در مورد کنترل، امنیت و ماهیت حریم خصوصی مطرح می‌کند.

نادو (۲۰۰۰) رویکردی جامع به حریم خصوصی دارد که انواع مختلف حریف خصوصی را دربردارد. به گفته وی، حریم خصوصی به عنوان مفهومی سیال شامل آزادی وجدان و اندیشه، کنترل بر جسم، داشتن خلوت و تنهایی در زمان و مکان خصوصی، کنترل بر اطلاعات شخصی، رهایی از نظارت‌های سمعی و بصری دیگران، حمایت از حیثیت و اعتبار خود و حمایت در برابرتفتیش، تجسس و رهگیری را شامل می‌شود (نقل شده در انصاری، ۱۴۰۰: ۱۱).

انصاری (۱۴۰۰) اعتقاد دارد که حق حریم خصوصی به معنای حق زندگی بر اساس میل و سلیقه فردی و حداقل مداخله دیگران در آن و به عبارت دیگر تعیین میزان دسترسی دیگران درباره اطلاعات آنها است. از این منظر توانایی کنترل فرد بر میزان اطلاعاتی که درباره خود به اشتراک می‌گذارد یک حق و اصل بنیادی است.

دو رویکرد در میان صاحبنظران درباره حریم خصوصی وجود دارد. یک رررویکرد منکر وجود حق مستقلی به نام حق حریم خصوصی و معتقد هر امری خصوصی مورد حمایت حق حریم خصوصی در ذیل حقوق دیگر مانند حق مالکیت و حق امنیت قابل تحقق است و رویکرد دیگری که حریم خصوصی را مستقل از سایر حقوق فردی قلمداد می‌کند. این رویکرد در انگلستان و آمریکا و کشورهای عضو خانواده کامن لا غلبه دارد و تعاریف مختلف شش‌گانه را از حریم خصوصی بیان کرده‌اند که عبارتند از:

۱. حریم خصوصی عبارتست از حق بر تنها ماندن؛

۲. حریم خصوصی یعنی دسترسی محدود دیگران به انسان و توانایی ایجاد مانع در برابر دسترسی‌های ناخواسته و ناخوانده به انسان؛

۳. حریم خصوصی یعنی محرمانگی و پنهان ساختن برخی امور از دیگران؛

۴. حریم خصوصی یعنی کنترل بر اطلاعات شخصی؛

۵. حریم خصوصی یعنی حق بر عالم صمیمیت و کرامت انسان (انصاری، ۱۴۰۰: صص. ۱۲-۱۳).

سروش (۱۳۹۸) نیز می‌گوید تعاریفی که از حریم خصوصی ارائه شده است بر یکی از این وجوه است: حق تنها ماندن؛ توانایی ایجاد مانع در دسترسی دیگران به انسان؛ پنهان ماندن از دیگران و محرمانه نگه‌داشتن برخی امور؛ کنترل بر اطلاعات شخصی؛ حمایت از کرامت و شخصیت؛ و نزدیکی و صمیمیت (ص.۱۲).

احمدلو (۱۴۰۰) تعریفی از حریم خصوصی ارائه می‌دهد که با رویکرد این پژوهش تمرکز بر بعد اطلاعاتی حریم خصوصی همخوانی دارد. به گفته او «حریم خصوصی عبارتست از از مجموعه اطلاعات و مسائل حوزه‌های خصوصی-فردی که شخص نمی‌خواهد کسی بدون تمایل و اطلاع وی نسبت به آن دسترسی حاصل و به آنها تعرض شود» (احمدلو، ۱۴۰۰: ۳۴).

-حریم خصوصی به مثابه دسترسی

دسته دوم تعاریف حریم خصوصی کنترل-مبنا هستند. این تعاریف حریم خصوصی را به‌منزله دسترسی محدود تعریف می‌کنند. از این منظر، به جای تمرکز بر محدودسازی اطلاعات باید بر «حریم خصوصی به‌منزله محدودیت دسترسی دیگران به یک فرد» (گاویسون، ۱۹۸۰: ۴۲۸) تمرکز شود (نقل شده در ولیز، ۲۰۲۴: ۸۱).

به گفته ولیز (۲۰۲۴) طرفداران نظریه‌های دسترسی استدلال می‌کنند که حریم خصوصی شامل محدود کردن یا جلوگیری از دسترسی به اطلاعات شخصی است. از این دیدگاه، هنگامی که چنین اطلاعاتی در اختیار دیگران قرار می‌گیرد، حریم خصوصی از بین می‌رود. یک مزیت کلیدی نظریه‌های دسترسی، تأکید آن‌ها بر نقض حریم خصوصی است، زمانی که کسی به اطلاعات شخصی دست یابد یا بدون توجه به اینکه فرد کنترل را حفظ می‌کند یا خیر، به فضای شخصی او تجاوز کند. برعکس، نظریه‌های کنترل بر اهمیت حفظ کنترل بر اطلاعات شخصی تأکید می‌کنند و این مفهوم را بیان می‌دارند که

به خطر انداختن این کنترل توسط دیگران، حتی زمانی که به اطلاعات دسترسی ندارند، اشتباه است. برای مثال، اگر دوستی دفترچه خاطرات شخصی را بدزدد، حتی اگر نتواند محتوای آن را رمزگشایی کند، نقض حریم خصوصی رخ داده است که نظریه‌های دسترسی ممکن است در پرداختن به آن با مشکل مواجه شوند. در نتیجه، یک نظریه کافی درباره حریم خصوصی باید هم دسترسی و هم کنترل را در نظر بگیرد تا حفاظت جامع را تضمین کند. ولیز (۲۰۲۴) درنهایت می‌گوید: «مفهوم حریم خصوصی و فقدان آن را بهتر می‌توان با نظریه دسترسی تبیین کرد، در حالی که حق حریم خصوصی و نقض آن را بهتر می‌توان با توسل به کنترل توضیح داد». (ص.۹۸).

ولیز (۲۰۲۴: ۹۹–۱۰۰) می‌گوید:

ضرورت گنجاندنِ هر دو مفهوم دسترسی و کنترل در یک نظریه جامع در مورد حریم خصوصی، در عصر دیجیتال از اهمیت بیشتری برخوردار شده است، زیرا بخش قابل توجهی از داده‌هایی که از دست می‌دهیم، ممکن است هرگز توسط انسان دیگری قابل دسترسی نباشند. سازمان‌های اطلاعاتی سراسر جهان و هزاران شرکت، ممکن است داده‌های شخصی شما را جمع‌آوری، ذخیره و به الگوریتم‌ها اجازه دهند تا آن‌ها را تحلیل کرده و در مورد زندگی شما تصمیم‌گیری کنند. من استدلال می‌کنم که هنگامی که کسی اطلاعات شخصی شما را سرقت می‌کند، حتی زمانی که به آن داده‌ها دسترسی پیدا نمی‌کند، حق حریم خصوصی شما را نقض کرده است.

ولیز (۲۰۲۴) در توضیح روایت پیوندی از حریم خصوصی می‌گوید که این مفهوم شامل «دسترسی‌نشده‌بودن اطلاعات شخصی و «فضای حسی» شخصی است[1]» (ص.۹۸). به بیان دیگر:

شما نسبت به فرد دیگر تا آن حدی حریم خصوصی دارید که آن فرد به اطلاعات شخصی و فضای فیزیکی شما دسترسی پیدا نکرده باشد؛ یعنی تا جایی که او هیچ چیز شخصی درباره شما نمی داند و نمی تواند شما را در موقعیت هایی که افراد دلیلی برای نخواستن توجه دیگران دارند، ببیند، ببوید، لمس کند یا بشنود. اطلاعات شخصی، اطلاعاتی درباره خود فرد است که افراد در یک جامعه خاص دلیلی برای نخواستنِ آگاهیِ دیگران (به جز خودشان و گاهی تعداد بسیار محدودی از

[1] . Privacy is the quality of having one’s personal information and one’s personal “sensorial space” unaccessed

افراد انتخابی شان) از آن دارند (مثلاً به این دلیل که آن ها را در برابر سوءاستفاده های قدرت از سوی دیگران آسیب پذیر می کند). (ولیز، ۲۰۲۴: ۹۸).

ولیز (۲۰۲۴) درنهایت تعریفی از حریم خصوصی می‌دهد که به این شرح است:

این متن، حریم خصوصی را بر اساس دسترسی به اطلاعات شخصی و فضای فیزیکی تعریف می‌کند که نکات کلیدی آن به شرح زیر است:

فردی (س) در رابطه با موضوعی (پ) در مقابل فرد دیگری (ع) دارای حریم خصوصی است، اگر و تنها در صورتی که ع به (پ) دسترسی پیدا نکرده باشد. (پ) می‌تواند شامل اطلاعات شخصی در مورد (س) یا فضای فیزیکی او باشد. حریم خصوصی کامل به این معنی است که (ع) هیچ اطلاعی از اطلاعات (س) ندارد و به فضای او دسترسی ندارد. این تعریف تفاوت‌های فرهنگی (آنچه مردم خصوصی می‌دانند) را در نظر می‌گیرد، اما همچنین عینیت نسبی را نیز به آن تزریق می‌کند. انسان‌ها برای محافظت از خود در برابر فشارهای تعاملات اجتماعی و سوءاستفاده احتمالی از قدرت، نیاز ذاتی به حریم خصوصی دارند.

از دیدگاه ولیز (۲۰۲۴) صرف *دسترسی‌پذیر بودن* اطلاعات برای از دست دادن حریم خصوصی کفایت نمی‌کند، بلکه باید شخص دیگر به آن دسترسی پیدا کند تا از اطلاعات شخصی شما آگاه شود. وی در مثال خود توضیح می‌دهد که اگر شخصی دفترچه خاطرات شما را در اختیار دارد (برای دسترسی‌پذیر است) اما هرگز آنرا نخواند، شما حریم خصوصی خود را از دست نداده‌اید که همان دسترسی‌نشده‌بودن است.

-انواع حریم خصوصی

در مورد اینکه حریم خصوصی چه انواعی دارد بحث‌های مختلفی مطرح است که ساده‌ترین آنها حریم مکانی است. یک فضای بسته که در اصطلاح یک در مرز آن با فضای عمومی است و امکان خلوت و تنهایی و کناره‌گیری از اجتماع را فراهم می‌کند. در این فضای بسته است که فرد به طور کامل بر محیط خود احاطه دارد و امکان تبادل اطلاعات مرتبط با خود (جسم، اندیشه‌ها، عقاید و...) با دیگران را مسدود می‌کند.

–اهمیت مکان در تعاریف حریم خصوصی

با توجه به اینکه انسانها پیش از حضور در فضای مجازی، در محیط فیزیکی زندگی کرده‌اند و می‌توان مفهوم مکان و فضای فیزیکی نقش مهم در تعاریف حریم خصوصی داشته است.

سروش (۱۳۹۸) انواع حریم خصوصی را به این شکل بیان کرده است:

۱. حریم مکانی: این حریم به فضای فیزیکی هر شخص اشاره دارد که در آن افراد دارای حریم حق حریم خصوصی است و بدون اجازه امکان ورود به آن وجود ندارد. نقض حریم مکانی صرفاً با حضور فیزیکی در مکان شخصی دیگران اتفاق نمی‌افتد و کاربرد ابزار سمعی–بصری همانند دوربین‌های مداربسته نیز می‌تواند ناقض حریم خصوصی تلقی شود.

۲. حریم جسمی: حریم جسمانی شخص بخشی از حریم خصوصی است و هرنوع اقدام ازجمله توقیف، بازرسی و نیز انجام آزمایش‌های پزشکی و گردآوری داده‌ها نسبت به جسم دیگری باید با رضایت وی انجام شود.

۳. حریم شخصیت: اهمیت حریم مکانی و حریم جسمانی بازتاب حریم قائل شدن برای شخصیت انسان است. بر این اساس هر نوع ورود به شخصیت دیگران و تعرض به آن ممنوع است.

۴. حریم خانواده: خانواده در قلمرو حریم خصوصی است و تصمیم شخص برای تشکیل خانواده، زمان انجام آن، اینکه چه کسی را به همسری برگزیند به خود وی مربوط است(سروش، ۱۳۹۸: ۱۶–۲۵)..

–حریم خصوصی به مثابه امری اطلاعاتی

از بین انواع حریم‌های خصوصی فوق توجه ویژه ما به حریم خصوصی ارتباطات و حریم اطلاعات شخصی متمرکز است. امروزه ارتباطات شخصی از مثال‌های فوق تا حد زیادی به سوی ارتباطات در پلتفرم‌های رسانه‌های اجتماعی و پیام‌رسان‌ها تغییرجهت داده است. افراد اطلاعات شخصی زیادی را نیز در انواع پلتفرم‌ها و سامانه‌ها به دلایل گوناگون از جمله ثبت نام گرفته تا دریافت خدمات منتشر می‌کنند و از خود برجای می‌گذارند که امروزه بیشتر تحت عنوان داده‌های شخصی شناخته می‌شود. این داده‌ها در قالب کلان داده (بیگ دیتا) گردآوری و تحلیل می‌شوند و یکی از ابزارهای درآمدزایی یا یکی از مدلهای کسب‌وکار پلتفرم‌های بزرگ است. کلان‌داده‌ها در شکل غیرتقلیل‌یافته نقض حریم داده‌های شخصی افراد به شمار می‌رود. انواع حریم‌های دیگر نیز قابل تسری به فضای مجازی است و می‌توان با توسعه و تعمیم تعریف حریم خصوصی آنرا

در فضای مجازی نیز تعریف و از آن حفاظت کرد. هرچند برخی از آنها مناقشه‌برانگیز است. مثلاً بر اساس تنظیمات حریم شخصی یک شبکه اجتماعی ما بتوانیم صفحه خود را خصوصی کنیم به این معنا است که آنجا یک فضای خصوصی محسوب می‌شود یا یک مکان (فضای) عمومی، چالش‌برانگیز است.

حریم اطلاعات شخصی یکی از انواع حریم خصوصی است است برخلاف گذشته، دسترسی سریع و گسترده به اطلاعات شخصی افراد به‌واسطه فناوری‌های پیشرفته امکان‌پذیر شده است و درنتیجه انواع داده‌های شهروندان در دسترس سازمان‌ها و نهادهای دولتی و شخصی قرار دارد. به همین دلیل کشورهای مختلف، قوانین و مقررات خاصی را برای حمایت از داده‌های شخصی تصویب و اجرا کرده‌اند (سروش، ۱۳۹۸: ۱۶-۲۵).

همچنین باید به حریم ارتباطات شخصی نیز اشاره شود که بر اساس باید گفت ارتباطات میان اشخاص به شکلّ‌های مختلفی صورت می‌گیرد که نامه، تلفن، نمابر، بی‌سیم و اینترنت در جنبه خصوصی‌شان، دارای مخاطب خاص است و هیچکس مجاز نیست از آنها مطلع باشد (سروش، ۱۳۹۸: ۱۶-۲۵).

محسنیان (۱۴۰۰) در قالب تعریف تحلیلی، مفهوم حریم شخصی را به این شکل تعریف کرده است: «اطلاعات، ارتباطات، فضاها و متعلقاتی که خواه از نظر فطری و خواه از نظر فرهنگی در وهله نخست به فرد معینی اختصاص دارد و پیش از این به طور علنی و عمومی منتشر نشده است» (ص.۱۸)؛ که عناصر تشکیل‌دهنده این تعریف عبارتند از:

۱. اطلاعات (داده) یا حریم اطلاعات: اطلاعات شخصی همانند اطلاعات مالی، پزشکی و دولتی افراد بخشی از اطلاعات را تشکیل می‌دهد.

۲. ارتباطات یا حریم ارتباطات: طیفی از کنشهای کلامی و غیرکلامی همانند پست الکترونیک، تلفن، پست و سایر اشکال (محسنیان، ۱۴۰۰: ۱۸-۱۹).

محسنیان می‌گوید ممکن است برخی از اطلاعات خصوصی فرد بنا به رضایت خود و یا موقعیت و پایگاه اجتماعی و یا به مصلح عمومی در اختیار عموم یا برخی مراجع قرار گیرد اما پیش از هرچیز این اطلاعات به وی اختصاص دارد. ویژگی دوم اختصاص اطلاعات شخصی به یک شخص معین است و بنابراین اسرار تجاری و اطلاعات محرمانه سازمانهای نظامی و اطلاعاتی در این تعریف نمی‌گنجد. و سوم اینکه باید اطلاعات در دسترس همه قرار نگرفته باشد. اگر اطلاعاتی پیشتر به

هر شکل در دسترس همگان قرار گرفته باشد، حتی اگر کاملاً شخصی باشند، دیگر در دسته اطلاعات حریم خصوصی فرد قرار نمی‌گیرند (محسنیان، ۱۴۰۰).

از مصادیق حریم اطلاعاتی به گفته محسنیان (۱۴۰۰: ۲۱–۲۲) عبارتند از:

۱. نام و سایر مشخصات شناسنامه‌ای

۲. نشانی اعم نشانی محل سکونت یا نشانی الکترونیکی

۳. تصویر یا حق تصویر

۴. وضعیت سلامتی فرد (جسمی، روحی و روانی)

۵. سطح تحصیلات فرد

۶. وابستگی صنفی و مذهبی

۷. عقاید و دیدگاه‌های سیاسی و اجتماعی

۸. اوقات فراغت و چگونگی گذاران آن

۹. منابع و شیوه تأمین نیازهای مالی و معیشتی

۱۰. روابط خانوادگی

۱۱. موقعیت خانوادگی

۱۲. روابط دوستانه

۱۳. زندگی عاطفی–احساسی

۱۴. شیوه ادامه تحصیلات فرزندان او

۱۵. گذشته اشخاص

۱۶. اعضای بدن، برخی نواحی و اندام جسمی افراد

۱۷. شغل افراد

۱۸. تمایلات و آرزوها

۱۹. محل سکونت افراد (منزل و ماوای افراد یا محل اقامت و آسایش آنها)

۲۰. مکاتبات و مراودات مخابراتی یا کتبی و امثال آن و نیز مرسولات پستی

۲۱. خانواده فرد

همین مصداق‌ها به توجه روشن‌تر به بحث حریم خصوصی کمک می‌کند. از آنجاکه توجه اساسی این پژوهش بر حریم خصوصی ارتباطات و اطلاعات است، توجه جزئ‌تر به ابعاد گوناگون حریم خصوصی اطلاعات کمک می‌کند. آقابایی (۱۳۹۷) دربحث انواع گوناگون حریم خصوصی اطلاعات بیان می‌کند که «همه تعرض‌ها به حریم خصوصی درحقیقت دست‌اندازی به اطلاعاتی است که فرد تمایل ندارد بدون اجازه وی آشکار شود و یا قوانین حمایت‌کننده حریم خصوصی در مقام تحدید و ضابطه‌مند نمودن دسترسی به اطلاعاتی است که افراد تمایل دارند از تعرض دیگران مصون مانده و افشاء نشود» (ص.۱۸۸). با وجود این، حریم خصوصی اطلاعات (داده‌ها) را می‌توان به دسته‌های مختلفی تقسیم کرد. اولین آنها شامل اطلاعات شخصی است که مصادیق آن بر اساس بند ب ماده یک «قانون انتشار و دسترسی آزاد به اطلاعات» عبارتست از: 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. دسته دوم شامل اطلاعات پزشکی–درمانی است که طی آن حریم خصوصی بیماران و عدم افشای اسراسر و اطلاعات پزشکی آنها را دربرمی‌گیرد. دسته سوم شامل اطلاعات مستخدمان و متقاضیان شغل است. در این حوزه منافع و ترجیحات کارفرمایان برای دستیابی به اطلاعات خصوصی پرسنل خود از یک سو و کرامت و حقوق متقاضیان کار از سوی دیگر در تعارض قرار دارد. دسته دیگر شامل اطلاعات قضایی و سجل کیفری است. با وجود عدم اشاره به اطلاعات قضایی در قوانین ایران به‌عنوان اطلاعات شخصی، تردیدی در اضافه کردن این اطلاعات در رده اطلاعات شخصی نیست و باید توجه داشت که اطلاعات مربوط به پرونده و سوابق افراد در مراجع قضایی و پلیسی از جمله اطلاعات شخصی حساس هستند که بر اساس مصالح فردی و اجتماعی باید دسترسی و انتشار آنها ضابطه‌مند باشد. دسته آخر اطلاعات تصویر و صدای افراد است. رسانه‌ها از طریق چاپ و انتشار تصویر و اظهارات افراد و یا به اشتراک‌گذشتن آنها و تجسس در گذشته و سوابق افراد عاملی مهمی در نقض حریم خصوصی افراد محسوب می‌شوند. آنها با توجه به رشد ابزارهای جدید جمع‌آوری خبر و تصویر و امکان تبادیل و ذخیره اطلاعات، امکان تعرض به حریم خصوصی افراد را افزایش داده‌اند.

در اوایل دهه ۲۰۰۰، با توجه به ریسک‌های مرتبط با توسعه اینترنت تجاری و رشد سریع تجارت الکترونیک، حریم خصوصی به دغدغه‌ای مهم در علم ارتباطات تبدیل شد. در طول این دوره، کارهای علمی عمدتاً بر تنظیم‌گری فردی و

تجارت الکترونیک متمرکز بود و درک افراد از حریم خصوصی و نقض آن را در بستر اینترنت، فضای مجازی یا محیط‌های شبکه‌ای بررسی می‌کرد. با این حال، این مطالعات عمدتاً بر تعاریف سنتی حریم خصوصی تکیه داشتند و جنبه‌های منحصر به فرد دنیای آنلاین را در نظر نمی‌گرفتند. تنها زمانی که رسانه‌های اجتماعی به شهرت رسیدند، محققان به ضرورت تعریف‌های خاص حریم خصوصی آنلاین پی بردند، با در نظر گرفتن شیوه‌ها و تجربیات خاصی که با پلتفرم‌های رسانه‌های اجتماعی و برنامه‌های آنلاین مرتبط است. در نهایت، تعریف حریم خصوصی آنلاین در پاسخ به شیوه‌های رسانه‌های اجتماعی تکامل یافت و این اصطلاح در نهایت جنبه‌هایی مانند افشای اطلاعات شخصی، مرزهای اجتماعی و تعادل بین باز بودن و حریم خصوصی در فضاهای دیجیتال را در بر گرفت (ترپته و ماسور، ۲۰۲۳).

-قابلیت‌های رسانه‌های اجتماعی و حریم خصوصی

همانطور که در مطلب مشخص است و ما نیز در بحث‌های خود اشاره کردیم، عمده بحث‌هایی که درباره حریم خصوصی و ابعاد گوناگون مرور کردیم، گرچه از اطلاعات و ارتباطات سخن گفته‌اند، اما از قابلیت‌ها و ویژگی‌های خاص عصر رسانه‌های اجتماعی غفلت شده است. به این دلیل که این تصور وجود دارد که فضای مجازی نیز نوعی رسانه است و همان مفاهیم و تعاریف و درک از حریم خصوصی را می‌توان به این فضا نیز تسری دارد.

روش‌های حفظ حریم خصوصی ذاتا با زیرساخت‌های فنی و پویایی‌های اجتماعی پلتفرم‌های رسانه‌های اجتماعی درهم‌تنیده شده‌اند. برای درک کامل چگونگی درک، اجرا و مدیریت حریم خصوصی توسط کاربران، بررسی دقیق این زمینه‌های منحصر به فرد و موقعیت‌های مختلف ناشی از آن‌ها ضروری است (ترپته و ماسور، ۲۰۲۳).

بر این اساس برای فهم حریم خصوصی در رسانه‌های اجتماعی توجه به چند موضوع اهمیت دارد-برخی از آنها در ادامه فصل ذکر می‌شود-که مهمترین آنها بحث *قابلیت*[1] و پیامد آن بر حریم خصوصی است. مفهوم قابلیت چندوجهی است. این مفهوم که در ابتدا در زمینه روان‌شناسی اکولوژیک (گیبسون، ۲۰۱۵) توسعه یافت و بعدها در مطالعات طراحی (نورمن، ۱۹۸۸) مورد پذیرش قرار گرفت، به طور کلی برای توصیف آنچه مصنوعات مادی مانند فناوری‌های رسانه‌ای به افراد اجازه می‌دهند انجام دهند، به کار می‌رود (تریم، زونن، سیوونن، ۲۰۲۳). در زمینه رسانه‌های اجتماعی، قابلیت به معنای انواع

[1] .affordance

گوناگون عملکردها و ویژگی‌هایی است که توسط پلتفرم‌ها ارائه می‌شود و به کاربران امکان می‌دهد تا به شکلهای گوناگون تعامل، برقراری ارتباط و خلق محتوا اقدام کنند.

همانطور که ترپته و ماسور (۲۰۲۳) توضیح داده‌اند پلتفرم‌های رسانه‌های اجتماعی قابلیت‌های متنوعی ارائه می‌دهند که استراتژی‌های تنظیم حریم خصوصی کاربران را شکل می‌دهند. این قابلیت‌ها، حاصل تعامل بین کاربران و ویژگی‌هایی است که پلتفرم در اختیار آن‌ها قرار می‌دهد. قابلیت‌های کلیدی شامل ناشناسی، ویرایش‌پذیری، ارتباط‌سازی و ماندگاری هستند. ناشناسی، به کاربران اجازه می‌دهد تا با سطوح مختلف از قابل شناسایی بودن تعامل داشته باشند، اما ممکن است بیان خود را محدود کند. ویرایش‌پذیری، کاربران را قادر می‌سازد تا اعمال و محتوای خود را تغییر دهند. ارتباط‌سازی، تعامل با دیگران را ترویج می‌کند و باعث ایجاد ارتباط می‌شود که به رضایت و رفاه کاربر کمک می‌کند. ماندگاری، به در دسترس بودن محتوا در طول زمان اشاره دارد. این قابلیت‌ها ذاتاً اجتماعی هستند و طراحی پلتفرم برای تعاملات اجتماعی را منعکس می‌کنند. شیوه‌ها و تعاملات کاربران بر اثربخشی این قابلیت‌ها در شکل‌دهی استراتژی‌های تنظیم حریم خصوصی در پلتفرم‌های رسانه‌های اجتماعی تأثیر می‌گذارد. این قابلیت‌ها کاربران را قادر می‌سازد تا حریم خصوصی خود را از طریق مکانیسم‌های مختلف ازجمله کنترل، اعتماد، هنجارها و ارتباطات بین‌فردی تنظیم کنند. محققان و کاربران اذعان دارند که کنترل تنها یکی از جنبه های تنظیم حریم خصوصی در رسانه های اجتماعی است. اعتماد و هنجارها نیز مکانیسم های ضروری برای کاربران برای محافظت از حریم خصوصی خود هستند.

تریم، زونن و سیوونن (۲۰۲۳) تلاش کرده‌اند تا رابطه قابلیت‌های رسانه‌های اجتماعی و حریم خصوصی را بسط بدهند. آنها ایده خود را به این شکل شرح داده‌اند:

با ظهور رسانه های اجتماعی، محققان این سوال را مطرح کرده اند که آیا این فناوری ها امکاناتی را برای کاربران فراهم می‌کنند که در بسترهای ارتباطی دیگر وجود نداشته باشد؟ یک دیدگاه مفید برای بررسی این موضوع، چارچوب قابلیت است که بر توانایی‌های کنشگری بازیگران (کاربران) در یک محیط اجتماعی–مادی خاص تمرکز دارد. در بررسی آنچه که برای بازیگران در استفاده از رسانه های اجتماعی ممکن یا غیرممکن است، محققان اغلب بر نحوه شکل گیری حریم خصوصی از طریق استفاده از رسانه های اجتماعی و میزان مدیریت، حفظ و به خطر افتادن آن در بسترهای آنلاین مختلف تمرکز کرده اند. مدیریت حریم خصوصی، برای درک ارتباطات در محیط های اجتماعی–مادی که ماهیت نمایشی دارند (مانند رسانه های اجتماعی)، یک دغدغه اصلی است. کاربران اغلب در مورد اینکه چه چیزی را به اشتراک بگذارند و چه چیزی را به اشتراک نگذارند، تصمیم گیری می‌کنند، در حالی که اغلب مخاطبان نهایی ارتباطات آنها ناشناخته هستند. ادبیات موجود، حریم

خصوصی را هم به عنوان یک امکان مجزا برای کاربران رسانه های اجتماعی و هم به عنوان پیامد سایر امکاناتی که از طریق استفاده از رسانه های اجتماعی به وجود می آیند، توصیف می کند. بررسی تقاطع استفاده از رسانه های اجتماعی و حریم خصوصی از طریق چارچوب قابلیت، اهمیت در نظر گرفتن حریم خصوصی را در بستر رسانه های اجتماعی و پویایی آن را که تحت تاثیر انتخاب های فعال بازیگران، مادیات موجود در استفاده از فناوری های رسانه های اجتماعی و مهارت ها و توانایی های کاربران این رسانه ها شکل می گیرد، به رسمیت می شناسد (تریم، زونن و سیوونن، ۲۰۲۳: ص.۹۱).

ایوانز و همکارانش (۲۰۱۷) استدلال می‌کنند که قابلیت‌ها باید سه معیار را در هنگام ارزیابی فناوری‌های ارتباطی داشته باشند: الف) آنها اشیا یا ویژگی‌های اشیاء نیستند، ب) آنها پیامد نیستند، و ج) دارای تنوع هستند. با بکارگیری این معیارها، نویسندگان به این نتیجه رسیدند که گرچه حریم خصوصی یک ویژگی فناوری ارتباطات نیست، و شکل‌های متنوعی دارد، به عنوان پیامد کنش‌های دیگر است و درنتیجه به عنوان یک قابلیت متمایز وجود ندارد در نتیجه، اغلب تحقیقات حریم خصوصی را به عنوان یک نتیجه حاصل از استفاده از ویژگی‌های خاص پلتفرم رسانه‌های اجتماعی تلقی می‌کنند (نقل شده در ترپته و ماسور، ۲۰۲۳).

تعریف و رویکرد ترپته (۲۰۲۱) به حریم خصوصی در رسانه‌های اجتماعی که برخلاف رویکرد ولیز (۲۰۲۴)–که به حریم خصوصی به طور کلی اختصاص داشت و بصیرت‌های مهمی را برای فهم حریم داده در فضای مجازی در اختیار ما قرار داد–به رسانه‌های اجتماعی اختصاص دارد. وی در رویکرد خود به حریم خصوصی بر کنترل و قابلیت تمرکز دارد. کنترل به عنوان یک جزء حیاتی در نظریه های تاریخی و معاصر حریم خصوصی به طور گسترده مورد توجه قرار گرفته است. بسیاری از پژوهشگران حریم خصوصی، کنترل را به عنوان ابزار اصلی برای افراد جهت تنظیم و دستیابی به حریم خصوصی در نظر می گیرند، با این فرض که افزایش کنترل بر دسترسی به داده های شخصی، منجر به بهبود تجربه های مرتبط با حریم خصوصی می شود.

ترپته (۲۰۲۱: ۱۳) سپس تعریف خود را از حریم خصوصی در رسانه‌های اجتماعی به این شکل اعلام می‌کند:

من حریم خصوصی را بر اساس ارزیابی‌های فردی از (الف) میزان دسترسی به این فرد در تعامل یا رابطه با دیگران (افراد، شرکت‌ها، مؤسسات) و (ب) در دسترس بودن سازوکارهای کنترل، ارتباط بین فردی، اعتماد و هنجارها برای شکل‌دهی به این سطح دسترسی از طریق (ج)

خودافشاگری به عنوان تنظیم‌گری رفتاری حریم خصوصی (تقریباً شهودی) و (د) کنترل، ارتباط بین فردی و بررسی به عنوان ابزاری برای اطمینان از تنظیم (تا حدودی مفصل‌تر) حریم خصوصی تعریف می‌کنم. سپس، در رسانه‌های اجتماعی، در دسترس بودن سازوکارهایی که برای اطمینان از حریم خصوصی قابل اعمال هستند، به‌طور اساسی تحت تأثیر محتوایی است که به اشتراک گذاشته می‌شود و توانمندی‌های رسانه‌های اجتماعی که نحوه استفاده بیشتر از این محتوا را تعیین می‌کنند، قرار می‌گیرد.

گرچه، بر اساس ایده محوری این پژوهش که طی اینترنت و فضای مجازی تا حد زیادی پلتفرمی شده است و ما اکنون در جامعه پلتفرمی زندگی می‌کنیم، ما بر *حقوق حریم خصوصی کاربران تمرکز داریم*؛ یعنی سوژه‌های انسانی که با تولید محتواهای کاربرساخته، نقش اصلی را در پلتفرم‌های زیرساختی ایفا می‌کنند و از طرف بسیاری از خدمات از انواع پلتفرم‌ها دریافت می‌کنند. بنابراین، تعریف ما از حریم خصوصی در فضای مجازی با تمرکز بر حریم کاربر خواهد بود و بر دو نوع حریم خصوصی یعنی حریم داده و حریم ارتباطات تمرکز خواهد داشت و انواع دیگر حریم خصوصی را نیز–تا حد ممکن از نظر منطقی– در این تعریف گنجانده خواهد شد.

-حریم خصوصی به مثابه حریم کاربران

از آنجا که ما بر دو شکل خاص از حریم خصوصی یعنی حریم داده و حریم ارتباطات تمرکز داریم، که در پلتفرم‌ها نقش محوری دارند، به لحاظ اینکه کاربران نقش اصلی را در ایفا می‌کنند و کنش و گفتار آنها و محتوایی که تولید می‌کنند، مبنای عمل پلتفرم‌های زیرساختی است، در این بخش بر حریم کاربران می‌پردازیم. از نظر ما حریم خصوصی کاربران شامل دو بخش است: حریم خصوصی اطلاعات (داده) کاربران و حریم خصوصی ارتباطات کاربران. بنابراین، برخلاف مقررات عمومی حفاظت از داده‌ها که بر حریم اطلاعات تمرکز دارد، در اینجا ما حریم خصوصی ارتباطات کاربران را نیز مد نظر قرار داده‌ایم. همچنین ذکر این نکته ضروری است که حقوق حریم خصوصی کاربران در پلتفرم‌های رسانه‌های اجتماعی شامل حقوق ارتباطات نیز هست اما در انواع دیگر پلتفرم‌ها ازجمله پلتفرم‌های خدماتی همانند اجاره اقامت‌گاه، سفر کوتاه‌مدت درون‌شهری و همانند اینها تمرکز عمدتاً بر حریم داده معطوف است.

حریم خصوصی داده‌های کاربران و حریم خصوصی ارتباطات، جنبه‌های مرتبط اما متمایز از مفهوم کلی حریم خصوصی هستند. حریم خصوصی داده‌های کاربران به محافظت و مدیریت صحیح اطلاعات شخصی‌ای اشاره دارد که افراد هنگام استفاده از پلتفرم‌های آنلاین، سرویس‌ها یا دستگاه‌های الکترونیکی به اشتراک می‌گذارند. این شامل طیف گسترده‌ای از داده‌ها مانند جزئیات دموگرافیک، ترجیحات، موقعیت مکانی، تاریخچه مرور و موارد دیگر می‌شود. حریم خصوصی داده‌های کاربران درگیر مسائلی مانند جمع‌آوری، ذخیره‌سازی، استفاده و به اشتراک گذاری داده‌ها توسط شرکت‌ها و اشخاص ثالث، و همچنین کنترل کاربران بر اطلاعات خودشان است. از طرف دیگر، حریم خصوصی ارتباطات به‌طور خاص بر محرمانگی و امنیت پیام‌ها، مکالمات و تعاملات بین افراد یا گروه‌ها تمرکز دارد. این جنبه از حریم خصوصی برای حفظ اعتماد و گفتگوی باز در محیط‌های مختلف مانند روابط شخصی، معاملات تجاری یا مباحثات سیاسی ضروری است. حریم خصوصی ارتباطات شامل محافظت در برابر دسترسی غیرمجاز، شنود یا نظارت بر مکالمات است و می‌تواند با رمزگذاری، پلتفرم‌های پیام‌رسان امن و سایر فناوری‌های بهبوددهنده حریم خصوصی امکان‌پذیر شود.

به طور خلاصه، در حالی که حریم خصوصی داده‌های کاربران با موضوع گسترده‌تر مدیریت اطلاعات شخصی در پلتفرم‌های دیجیتال سروکار دارد، حریم خصوصی ارتباطات بر محرمانگی تبادلات بین افراد یا گروه‌ها تمرکز محدودتری دارد. هر دو برای حفظ استقلال فردی، تقویت اعتماد و حفظ سلامت تعاملات دیجیتال ضروری هستند.

-حریم خصوصی اطلاعات کاربران (حریم داده‌های شخصی)

یکی از بحث‌های مهم در مورد حریم خصوصی اطلاعات یا داده‌ها، حریم اطلاعات کاربران است. حریم خصوصی داده‌های کاربران در عصر رسانه‌های اجتماعی و پلتفرم‌های آنلاین، جایی که کاربران حجم عظیمی از اطلاعات شخصی را به اشتراک می‌گذارند، به یک دغدغه جدی تبدیل شده است. با گذراندن زمان بیشتر به صورت آنلاین، افراد ردپای دیجیتالی از خود به جا می‌گذارند که می‌تواند توسط شرکت‌ها و اشخاص ثالث جمع‌آوری، تحلیل و کسب درآمد شود. این امر سوالاتی را در مورد استفاده اخلاقی از داده‌های شخصی و میزان کنترل افراد بر حضور آنلاینشان ایجاد می‌کند.

پلتفرم‌هایی مانند فیس‌بوک، اینستاگرام و گوگل به دلیل نحوه مدیریت داده‌های کاربران مورد انتقاد و نظارت قرار گرفته‌اند. این شرکت‌ها اغلب از الگوریتم‌های پیچیده و تکنیک‌های استخراج داده برای استخراج اطلاعات ارزشمند از اطلاعات کاربر استفاده می‌کنند که می‌تواند برای هدف قرار دادن تبلیغات و شکل‌دهی تجربیات آنلاین به کار رود. علاوه بر این، نقض داده‌ها و دسترسی غیرمجاز به اطلاعات حساس، نگرانی‌ها را در مورد امنیت و حفاظت از داده‌های کاربران افزایش داده است. برای کاربران و تنظیم‌کننده‌ها ضروری است که در حفاظت از حریم خصوصی داده‌ها و اطمینان از شفافیت در نحوه جمع‌آوری و استفاده از اطلاعات شخصی در فضای دیجیتال هوشیار باشند.

مرور بحث‌های فوق نشان می‌دهد که حقوق کاربران در فضای مجازی و رسانه‌های اجتماعی و انواع پلتفرم‌ها در ایران تاکنون مورد توجه قرار نگرفته است. مفهوم حقوق مخاطب که به عصر رسانه‌های جمعی اختصاص دارد کم‌وبیش بحث‌هایی را ایجاد کرده است اما حقوق کاربران که به عصر پلتفرم‌ها تعلق دارد، در بحث‌های مرتبط با حقوق رسانه‌ها و ارتباطات ناچیز است و انصار و عطار (۱۴۰۲) عمده‌ترین تلاش در ایران برای توسعه این بحث است. با این‌همه، بخش عمده بحث‌های مرتبط با حریم خصوصی داده‌ها در سطح بین‌الملل بدین سو، جهت‌گیری کرده است زیرا اکنون بخش ارتباطات ارتباطات اینترنتی، ارتباطات پلتفرم–مبنا است. پلتفرم‌هایی که صرفاً شامل رسانه‌های اجتماعی نیستند و انواع پلتفرم‌ها را شامل می‌شوند.

کارا (۲۰۲۱) در یک تقسیم‌بندی فراگیر انواع پلتفرم‌ها را به سه دسته تقسیم کرده است. این سه دسته عبارتند از: پلتفرم‌های رسانه‌های اجتماعی، پلتفرم‌های استریمینگ و پلتفرم‌های لجستیک. پلتفرم‌های شبکه‌های اجتماعی بر اساس ایجاد یک شبکه اجتماعی حول تولید و به اشتراک گذاشتن محتوا ساخته می‌شوند. این موارد شامل پلتفرم‌هایی مانند فیس‌بوک، اینستاگرام و اسنپ‌چت می‌شوند. پلتفرم‌های استریم بر اساس انتشار و استریم ویدیو و صدا ساخته می‌شوند. این موارد شامل پلتفرم‌هایی مانند نتفلیکس و اسپوتیفای می‌شوند. پلتفرم‌های لجستیکی بر اساس ارائه کالا و خدمات ساخته می‌شوند. این موارد شامل پلتفرم‌هایی مانند گوگل و آمازون می‌شوند.

ما در این بخش به طور خاص دو دسته پلتفرم رسانه‌های اجتماعی و لجستیک (یا خدمات) مورد بحث قرار خواهیم داد. چون کاربران در آنها نقش ویژه‌ای دارند. همانطور که سوجون (۲۰۲۱) بحث کرده است، شبکه های اجتماعی تقریباً در تمام جنبه های زندگی ما نفوذ کرده اند و حضور پررنگی در اینترنت، دستگاه های ما و روابط شخصی ما ایجاد کرده اند. ما از

این پلتفرم ها برای تعامل با شخصیت های عمومی، دسترسی به اخبار و تعامل با دنیای اطرافمان استفاده می کنیم. آنها همچنین بر روابط عاشقانه و خانوادگی ما تأثیر می گذارند، هویت حرفه ای و شخصی ما را شکل می دهند و به عنوان مجرایی برای ارتباط و قطع ارتباط عمل می کنند. در عصر حاضر، شبکه‌های اجتماعی فراتر از صرفاً سرگرمی و فرار از واقعیت شده‌اند؛ آن‌ها به فضایی حیاتی برای ارتباط انسانی و محرکی کلیدی برای تبادل فرهنگی و اقتصادی تبدیل شده‌اند. همانطور که کارا (۲۰۲۱) بحث می‌کند، یکی از مهمترین ویژگیهای پلتفرم‌های رسانه‌های اجتماعی گردآوری داده است. پلتفرم‌های شبکه‌های اجتماعی برای هدایت الگوریتم‌های توصیه و هدفمندسازی محتوا، به جمع‌آوری داده‌های کاربران وابسته‌اند. کاربران فعال با تعاملات اجتماعی، محتوا و داده‌هایی که تولید می‌کنند در این امر سهیم هستند و پلتفرم‌ها از این داده‌ها برای جلب توجه و ایجاد درآمد استفاده می‌کنند. این پلتفرم‌ها با جمع‌آوری اطلاعات متنوعی مانند موقعیت مکانی، علایق و ارتباطات اجتماعی، محتوا را به صورت لحظه‌ای برای کاربران شخصی‌سازی می‌کنند. این حجم عظیم از جمع‌آوری داده که توسط پلتفرم‌های شبکه‌های اجتماعی به عنوان واسطه تسهیل می‌شود، با امکان‌دادن به کارگزاری داده‌ها و بسته‌بندی آن‌ها برای اهداف مختلف، نقش مهمی در اقتصاد دیجیتال ایفا می‌کند. بدین ترتیب، پلتفرم‌های شبکه‌های اجتماعی به بازیگران کلیدی در جمع‌آوری، تحلیل و کسب درآمد از داده‌های مربوط به زندگی روزمره تبدیل شده‌اند.

درواقع، این ویژگی خود به امری چالش‌برانگیز در حوزه حریم خصوصی تبدیل شده و مسائل نوظهوری متعددی را باعث شده است.

-پلتفرم‌های ایرانی و بی‌توجهی به حفاظت از داده‌های شخصی

عدم اتخاذ راهکارهای امنیت سایبری در پلتفرم‌ها گاهی در ایران مسئله‌ساز می‌شود. این چالش بیشتر در مورد پلتفرم‌های خدماتی یا بنا به تقضای مصرف‌کننده روی می‌دهد. برخلاف انتظار، رخته و نفوذ به پیام‌رسان‌های ایرانی تاکنون گزارش نشده است. یک نمونه آن هک و در معرض فروش دادن داده‌های شخصی حدود بیست میلیون نفر از کاربران پلتفرم اسنپ‌فود در دی‌ماه ۱۴۰ است که طی آن هکر ادعا کرده بود بیش از ۲۰ میلیون کاربر شامل نام کاربری، پسورد، ایمیل، نام و نام خانوادگی، شماره موبایل، تاریخ تولد و همچنین اطلاعات بیش از ۸۸۰ میلیون سفارش محصول را استخراج کرده‌اند

(آستانه، ۱۴۰۲). اما درنهایت، پس از فروکش کردن توجه افکار عمومی، هیچ‌گونه مجازاتی متوجه این پلتفرم نشد. درواقع، این رسوایی درز گسترده اطلاعات، برای کاربران، صاحبان این پلتفرم و نیز قوه قضاییه چندان اهمیت نداشت. و صرفاً اسنپ‌فود وعده داد حداکثر تلاش خود را برای جلوگیری از انتشار داده‌های کاربران، از طریق مذاکره با این گروه هکری به کار خواهد گرفت. این اتفاق پیشتر توسط همین گروه در مورد خدمت سفر آنلاین تپسی نیز اتفاق افتاده بود.

در تازه‌ترین مورد از افشاء داده‌های کاربران ایران، در ۱۹ تیر ۱۴۰۳ و در زمان تدوین این گزارش، همان گروه هکری مدعی شده بود که خدمت اجاره اقامتگاه اتاقک را هک کرده است. این گروه در کانال تلگرامی خود اعلام کرده بودند: «به اتاقک ۲۴ ساعت فرصت میدهیم تا جهت جلوگیری از فروش اطلاعات، با ما وارد مذاکره شوند و مانند سازمان حج و تپسی تکرار اشتباه نکنند!».

بخشی از داده‌های کاربران اتاقک که در دسترس این گروه هکری قرار گرفته بودند، عبارت بودند از:

-اطلاعات رزرواسیون؛ شامل نام و نام‌خانوادگی، تاریخ رزرو، مدت اقامت، هزینه پرداختی، کد ملی، شماره تماس، ایمیل و... .

-اطلاعات تسویه حساب؛ شامل مبلغ، اطلاعات بانکی، توضیحات، تاریخ

-پیام‌ها و چت‌ها؛ شامل کد فعال‌سازی یا کلمه‌عبور، پیام‌های پشتیبانی و... .

-اطلاعات کاربری؛ شامل نام کاربری، پسورد، نام و نام‌خانوادگی، جنسیت، شماره تماس، کد ملی، آی‌پی آدرس، یوزر ایجنت و... .

-اطلاعات پرداخت؛ شامل توضیحات پرداخت، تاریخ پرداخت، مبلغ، اطلاعات پرداخت کننده

-اطلاعات دقیق اماکن قابل رزرو؛ شامل آدرس دقیق، طول و عرض جغرافیایی، شهر، کد پستی و... .

-اطلاعات جستجوی کاربران؛ شامل شهر، استان، فیلترهای جستجو، بازه زمانی جستجو، مبلغ، یوزر آیدی، آی‌پی آدرس و... .

-اطلاعات بانکی؛ شامل نام و نام‌خانوادگی صاحب حساب، نام کاربری، شماره شبا، نام بانک، شماره کارت

– کوپن‌های تخفیف و کلی اطلاعات دیگر

جالب توجه است که برخلاف «دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی» مصوب سال ۱۴۰۲ که طی آن این پلتفرم‌ها ملزم شده‌اند تا سیاست حریم خصوصی خود را به شکل شفاف اعلام نمایند، در وب‌سایت اتاقک چنین اقدامی انجام نشده

است. بنابراین مشخص نیست که ضمانت اجرایی این نوع دستورالعمل‌ها چیست و چرا برخلاف رویه پیش‌بینی‌شده برای نظارت بر اجرا، اقدام لازم انجام نشده است.

این نمونه‌ها بیانگر این است که پلتفرم‌ها در حفاظت از داده‌های شهروندان دچار قصور هستند و اینکه عدم مجازات انتشار داده‌های شخصی و بی‌توجهی عمومی به آن، زمینه تکرار این اعمال را ایجاد کرده است.

-حفاظت از داده‌ها[1]

حریم اطلاعات شخصی، حریم داده و حفاظت از داده‌ها مفاهیم نزدیک به هم هستند. در ادبیات حقوقی ایران بیشتر از عبارت حریم خصوصی اطلاعات و یا حریم اطلاعات شخصی (انصاری، ۱۴۰۰) استفاده شده است. در مقررات عمومی حفاظت از داده‌ها در سطح اتحادیه اروپا که پیشروترین قانون در این حوزه است، از اصطلاح «اطلاعات شخصی» و «حفاظت از داده‌ها» استفاده شده است. در مورد تفاوت این عبارتها، گاه توضیحات متناقضی مشاهده می‌شود. برای نمونه، سیندهایاچ (۲۰۲۳: ۱)، حفاظت از داده را به این شکل تعریف کرده است: «مفهوم «حمایت از داده» اصطلاحی گسترده است که تدابیر و مقررات وضع شده برای محافظت از حریم خصوصی اطلاعات و داده‌های افراد را دربرمی‌گیرد. همچنین از این اصطلاح برای اطمینان از این موضوع استفاده می‌شود که شرکت‌ها از داده‌ها به شیوه‌هایی که حریم خصوصی یا حقوق قانونی کاربران را نقض کند، استفاده نمی‌کنند». در اینجا حفاظت از داده به معنای محافظت از حریم خصوصی اطلاعات و داده‌های افراد تعریف شده است و صرفاً بر بر «داده‌های شخصی» متمرکز نیست و رویکردی کلی به آن دارد.

از طرف دیگر، اوستوین (۲۰۱۶) بر تفاوت‌های بین حریم خصوصی و حفاظت از داده‌ها تأکید می‌کند و خاطرنشان می‌سازد که اگرچه این اصطلاحات اغلب به جای یکدیگر استفاده می‌شوند، اما مفاهیمی مجزا با ویژگی‌های منحصر به فرد هستند. در اینجا خلاصه‌ای کوتاه آورده شده است:

حریم خصوصی، حق بنیادینی است که از دیرباز بر محافظت از حریم شخصی افراد در برابر تجاوز تمرکز داشته است و در ابتدا با هدف حراست افراد در برابر دخالت دولت شکل گرفته است. حفاظت از داده‌ها، مفهومی جدیدتر است که اخیراً در

[1] .data protection

اتحادیه اروپا به عنوان یک حق اساسی شناخته شده است و بر کنترل و حفاظت از اطلاعات شخصی متمرکز است. این مفهوم هم برای نهادهای دولتی و هم خصوصی قابل اعمال است.

حریم خصوصی دامنه وسیع‌تری نسبت به حفاظت از داده‌ها دارد و نه تنها اطلاعات شخصی، بلکه فضاهای فیزیکی و انتخاب‌های شخصی را نیز در بر می‌گیرد. در عین حال، حریم خصوصی محدودتر است، زیرا حفاظت از داده‌ها حتی در شرایطی که دخالتی در حریم شخصی فرد صورت نگرفته باشد، قابل اعمال است. برای تعیین اینکه آیا حریم خصوصی در خطر است، زمینه جمع‌آوری یا پردازش داده‌ها و تأثیر آن بر زندگی خصوصی، عوامل مهمی هستند. داده‌های عمومی همچنان می‌توانند تحت حق حریم خصوصی قرار گیرند. در نتیجه، در حالی که حریم خصوصی و حفاظت از داده‌ها اشتراکاتی دارند، مفاهیمی مجزا با پیشینه‌های تاریخی، اهداف و دامنه‌های متفاوت هستند. درک این تفاوت‌ها در بستر مباحثات معاصر در مورد نظارت، انحصار اطلاعات و ردیابی آنلاین بسیار مهم است.

با این‌همه منظور ما از حریم اطلاعات همان حریم داده‌های شخصی است که یکی از انواع حریم خصوصی به شمار می‌رود و تمرکز بر حفاظت یا حمایت از داده‌های شخصی است که طی آن مقرراتی برای پردازش اطلاعات شخصی کاربران وضع می‌شود.

مقررات عمومی حفاظت از داده‌ها یکی از مهمترین مقررات مرتبط با حفاظت از اطلاعات شخصی کاربران در سطح جهان است که در آن حقوق حریم خصوصی کاربران مورد خاص توجه قرار دارد. حق حفاظت از داده، حقی بنیادین است که در منشور حقوق اساسی اتحادیه اروپا مورد توجه قرار دارد و مقررات عمومی حفاظت از داده‌ها نیز مبتنی بر آن تدوین شده است. متن منشور حقوق بنیادین اتحادیه اروپا یک سند الزام آور قانونی است که حاوی لیست جامع حقوق بنیادینی است که در اتحادیه اروپا به رسمیت شناخته شده و مورد حمایت قرار می گیرد. این منشور در سال ۲۰۰۰ اعلام شد و با اجرای پیمان لیسبون در سال ۲۰۰۹ الزام قانونی پیدا کرد.

منشور حقوق بنیادین جزء ضروری چارچوب حقوقی و سیاسی اتحادیه اروپا است و مکمل قانون اساسی کشورهای عضو و ابزارهای بین المللی حقوق بشر می باشد. این منشور طیف گسترده‌ای از حقوق مدنی، سیاسی، اقتصادی و اجتماعی را در خود جای داده است و تضمین می کند که این حقوق در سیاست ها و قوانین اتحادیه اروپا مورد احترام و ارتقاء قرار گیرند.

این منشور به شش بخش تقسیم می شود: کرامت انسانی، آزادی ها، برابری، همبستگی، حقوق شهروندی و عدالت. برخی از حقوق بنیادین مندرج در این منشور عبارتند از حق حیات، ممنوعیت شکنجه و رفتار غیر انسانی یا تحقیرآمیز، حق آزادی و امنیت، حق دادرسی عادلانه، حق حریم خصوصی، حق حمایت از داده‌ها، آزادی بیان، آزادی اندیشه، وجدان و مذهب، و ممنوعیت تبعیض بر اساس دلایل مختلف. منشور حقوق بنیادین اتحادیه اروپا نقش اساسی در تضمین حمایت و رعایت حقوق شهروندان اتحادیه اروپا در چارچوب نظام های حقوقی و سیاسی اتحادیه اروپا ایفا می‌کند.

ماده ۸ منشور حقوق اساسی اتحادیه اروپا که به حفاظت از داده‌های شخصی اختصاص دارد، بیان می‌دارد:

۱. هر فردی حق دارد از داده‌های شخصی مربوط به خود محافظت شود.

۲. چنین داده‌هایی باید به صورت منصفانه و برای اهداف مشخص و بر اساس رضایت فرد ذینفع یا سایر مبنای قانونی مقرر توسط قانون پردازش شود. هر فرد حق دسترسی به داده‌هایی را دارد که در مورد وی جمع‌آوری شده است و حق دارد آن را اصلاح کند.

۳. رعایت این قوانین باید تحت نظارت یک مرجع مستقل باشد (اتحادیه اروپا، ۲۰۲۴).

این بدان معنی است که هر فردی حق دارد اطلاعات شخصی خود را به صورت ایمن نگهداری کند، به طور عادلانه و قانونی مورد استفاده قرار گیرد و در صورت درخواست نسخه ای از آن برای وی در دسترس باشد. اگر فردی احساس کند که اطلاعات شخصی او اشتباه است، حق دارد درخواست اصلاح آن اطلاعات را داشته باشد.

در مقررات عمومی حفاظت از داده‌ها حریم داده شخصی به این شکل تعریف شده است:

«داده‌های شخصی» به هرگونه اطلاعاتی در رابطه با یک شخص حقیقی شناسایی شده یا قابل شناسایی (سوژه داده) گفته می‌شود؛ یک شخص حقیقی قابل شناسایی کسی است که به طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به شناسه‌ای مانند نام، شماره شناسایی، داده‌های مکان، شناسه آنلاین یا به یک یا چند عامل خاص مربوط به هویت جسمی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی یا اجتماعی آن شخص حقیقی قابل شناسایی باشد (ماده ۴ (۱) مقررات عمومی حفاظت از داده‌ها)[۱].

[۱]. علاوه بر این مفهوم «پردازش» به این شکل تعریف شده است:
«پردازش» به معنای هر عملیاتی است که روی داده‌های شخصی یا مجموعه‌های داده‌های شخصی انجام می‌شود، چه به صورت خودکار و چه به صورت غیر خودکار، مانند جمع‌آوری، ضبط، سازماندهی، ساختاردهی، ذخیره‌سازی، تطبیق یا تغییر، بازیابی، مشورت، استفاده، افشا از طریق انتقال، انتشار یا در دسترس قرار دادن به روش‌های دیگر، هم‌ترازی یا ترکیب، محدودسازی، پاک‌سازی یا نابودی (ماده ۴ (۲)).

در مقررات عمومی حفاظت از داده‌ها، کاربر با عنوان سوژه داده[1]تعریف شده است. در چارچوب مقررات عمومی حفاظت از داده، سوژه داده به فرد حقیقی شناسایی شده یا قابل شناسایی اشاره دارد که داده‌های شخصی وی توسط کنترل‌گر داده[2] یا پردازشگر داده[3] پردازش می‌شود. این سوژه شامل هر فردی در اتحادیه اروپا می‌شود که اطلاعات شخصی وی، مانند نام، شماره شناسایی، داده‌های مکان، شناسه‌های آنلاین یا سایر عوامل خاص هویت فیزیکی، فیزیولوژیکی، ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی او جمع‌آوری، ذخیره یا پردازش می‌شود[4]. با تنظیم نحوه مدیریت سازمان‌ها بر داده‌های شخصی و اطمینان از پردازش شفاف، ایمن و قانونی چنین اطلاعاتی، به دنبال محافظت از حقوق و آزادی‌های افراد سوژه داده است.

بنابراین، در این قانون دو بحث محوری باید مورد توجه قرار گیرد. نخستین آن حقوقی است که برای کاربر در نظر گرفته شده است و بحث دوم، نواع داده‌های گردآوری‌شده از کاربر است؛ که مورد نخستین در اینجا مورد بحث قرار می‌گیرد.

هفت دسته‌بندی زیر اطلاعات دقیق‌تری در مورد حقوق فردی کاربران تحت حفاظت از داده‌ها و نحوه اعمال آن حقوق برای کاربران ارائه می‌دهد:

حق دسترسی به اطلاعات[5]

حق اطلاع (شفافیت)[6]

حق اصلاح[7]

حق پاک کردن[8]

---

[1] .data subject
[2] .data controller
[3] . data processor
[4]. در مورد انواع داده‌های گردآوری‌شده بر اساس مقررات عمومی حفاظت از داده در بخش مرتبط با بررسی آن بحث خواهد شد.
[5] . The right to access information
[6] . The right to access information
[7] .the right to rectification
[8] .the right to erasure

حق انتقال داده‌ها[1]

حق اعتراض به پردازش داده‌های شخصی[2]

حق محدودیت[3]

-حق دسترسی به اطلاعات (ماده ۱۵):

ماده ۱۵ مقررات عمومی حفاظت از داده‌ها حق سوژه داده را برای دریافت تأیید از کنترلر داده در رابطه با پردازش داده‌های شخصی آنها مشخص می کند. پس از تأیید، سوژه داده حق دسترسی به داده‌های شخصی خود و اطلاعات مرتبط، از جمله موارد زیر را دارد:

اهداف پردازش

دسته بندی های داده‌های شخصی

گیرندگان یا دسته های گیرندگان

دوره ذخیره سازی پیش بینی شده یا معیارهای مورد استفاده برای تعیین آن

حقوق مربوط به اصلاح، حذف، محدودیت پردازش یا اعتراض

حق ارائه شکایت به مقام ناظر

منبع داده‌های شخصی در صورت عدم جمع آوری مستقیم از سوژه داده

وجود تصمیم گیری خودکار، از جمله پروفایل سازی

سوژه داده حق دارد با درخواست، یک نسخه رایگان از داده‌های شخصی خود را دریافت کند، با امکان دریافت نسخه های اضافی با هزینه معقول. در صورت درخواست الکترونیکی، اطلاعات باید در یک فرم الکترونیکی رایج ارائه شود. این حق

[1] .the right to data portability
[2] .the right to object to processing of personal data
[3] .the right of restriction

دسترسی به اطلاعات مشروط به حقوق و آزادی های دیگران بوده و بر آنها مقدم نیست. در ادامه خلاصه‌ای از ماده‌های طولانی و اصل ماده‌های کوتاه مرتبط با این حقوق ذکر می‌شود.

-حق اطلاع (شفافیت) ماده ۱۳ و ۱۴

ماده ۱۳ مقرارت عمومی حفاظت از داده‌ها، اطلاعاتی را که باید هنگام جمع‌آوری اطلاعات شخصی به افراد سوژه داده ارائه شود، مشخص می‌کند. مسئولین کنترل داده باید در زمان جمع آوری داده، جزئیات زیر را ارائه دهند:

-هویت و اطلاعات تماس مسئول کنترل و در صورت وجود، نماینده آنها.

-اطلاعات تماس مسئول حفاظت از داده، در صورت وجود.

-اهداف پردازش داده و مبنای قانونی پردازش.

-منافع مشروع دنبال شده توسط مسئول کنترل یا اشخاص ثالث، در صورت وجود.

-گیرندگان یا دسته های گیرندگان اطلاعات شخصی، در صورت وجود.

-اطلاعات مربوط به انتقال اطلاعات شخصی به کشورهای ثالث یا سازمان های بین المللی، از جمله وجود یا عدم وجود تصمیم کفایت توسط کمیسیون یا ضمانت های مناسب.

اطلاعات اضافی مورد نیاز برای پردازش منصفانه و شفاف شامل موارد زیر است:

-دوره نگهداری داده یا معیارهای تعیین کننده آن.

-حقوق سوژه داده در رابطه با دسترسی، اصلاح، پاک کردن، محدودیت پردازش، اعتراض و قابلیت انتقال داده.

-حقِ پس گرفتن رضایت و حقِ ثبت شکایت نزد یک مرجع نظارتی.

-اینکه آیا ارائه داده‌های شخصی یک الزام قانونی، قراردادی یا الزامی است و عواقب عدم ارائه چنین داده‌هایی چیست.

-اطلاعات در مورد تصمیم گیری خودکار و ایجاد پروفایل، از جمله منطق، اهمیت و عواقب آن برای سوژه داده.

مسئولین کنترل داده همچنین باید موضوعات داده را از هرگونه پردازش بیشتر برای اهدافی غیر از جمع آوری اولیه مطلع کنند و قبل از انجام چنین پردازشی، اطلاعات اضافی مرتبط را ارائه دهند. با این حال، این الزام در صورتی که سوژه داده از قبل اطلاعات مورد نیاز را داشته باشد، اعمال نمی شود.

ماده ۱۴ آیین نامه عمومی حمایت از داده‌های شخصی (جی.دی.پی.آر) به اطلاعاتی اشاره می‌کند که کنترل‌کننده‌های داده باید زمانی که داده‌های شخصی را مستقیماً از خود افراد دریافت نکرده‌اند، در اختیار آن‌ها قرار دهند. در چنین مواردی، کنترل‌کننده‌ها باید جزئیات زیر را ارائه دهند:

-هویت و اطلاعات تماس کنترل‌کننده و نماینده آن‌ها (در صورت وجود).

-اطلاعات تماس مسئول حفاظت از داده (در صورت وجود).

-اهداف پردازش داده‌ها و مبنای قانونی برای پردازش.

-دسته‌بندی‌های داده‌های شخصی مورد نظر.

-گیرندگان یا دسته‌بندی‌های گیرندگان داده‌های شخصی، در صورت وجود.

-اطلاعات مربوط به انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی، از جمله وجود یا عدم وجود تصمیم کفایت توسط کمیسیون یا ضمانت‌های مناسب.

اطلاعات اضافی مورد نیاز برای پردازش منصفانه و شفاف شامل موارد زیر است:

۱.دوره ذخیره سازی داده یا معیارهای تعیین کننده آن.

۲.منافع مشروع دنبال شده توسط کنترلر یا اشخاص ثالث، در صورت لزوم.

۳.حقوق سوژه داده در مورد دسترسی، اصلاح، حذف، محدودیت پردازش، اعتراض و انتقال داده.

۴.حق لغو رضایت و حق شکایت به مرجع نظارتی.

۵.در صورت وجود، ذکر منبع داده‌های شخصی و اینکه آیا از منابع قابل دسترسی عموم است.

۶.اطلاعات مربوط به تصمیم گیری و پروفایل سازی خودکار، از جمله منطق، اهمیت و پیامدهای آن برای سوژه داده.
ارائه این اطلاعات تضمین می کند که موضوعات داده از حقوق خود و فعالیت های پردازشی مرتبط با داده‌های شخصی خود، حتی زمانی که به طور مستقیم از آنها به دست نیامده باشد، آگاه هستند.

-حق اصلاح (ماده‌های ۱۶ و ۱۹)

متن ماده ۱۶: سوژه داده حق دارد بدون تأخیر غیر ضروری از مسئول کنترل، اصلاح داده‌های شخصی نادرست مربوط به خود را درخواست نماید. همچنین با در نظر گرفتن اهداف پردازش، سوژه داده حق دارد داده‌های شخصی ناقص را تکمیل کند، از جمله با ارائه یک بیانیه تکمیلی.
متن ماده ۱۹: مسئول کنترل، هرگونه اصلاح یا پاک کردن داده‌های شخصی یا محدودیت پردازش انجام‌شده مطابق با ماده ۱۶، ماده ۱۷(۱) و ماده ۱۸ را به هر گیرنده‌ای که داده‌های شخصی به او افشا شده است، باید اطلاع دهد، مگر اینکه این امر غیرممکن باشد یا مستلزم تلاش نامتناسب باشد. در صورتی که سوژه داده درخواست کند، مسئول کنترل باید آن گیرندگان را به اطلاع سوژه داده برساند.

موضوع اصلی این ماده حول محور حقوق صاحبان داده در رابطه با صحت و کامل بودن داده‌های شخصی آنها می چرخد. صاحبان داده حق دارند در اسرع وقت درخواست اصلاح و دریافت هرگونه داده شخصی نادرست را از کنترلر داده داشته باشند. علاوه بر این، آنها حق دارند داده‌های شخصی ناقص را با در نظر گرفتن اهداف پردازش، تکمیل کنند. این ممکن است شامل ارائه اطلاعات تکمیلی برای اطمینان از اینکه داده‌ها به طور دقیق وضعیت، ترجیحات یا سایر جنبه های مرتبط با موضوع را منعکس می کند.

-حق پاک کردن (حق نادیده گرفته شدن[1]) (ماده‌های ۱۷ و ۱۹)

[1] .right to be forgotten

متن ماده ۱۷ (بخش اول): ۱. سوژه داده حق دارد بدون تأخیر غیر منطقی از مسئول کنترل، پاک کردن داده‌های شخصی مربوط به خود را درخواست کند و مسئول کنترل موظف است در صورت وجود یکی از موارد زیر، بدون تأخیر غیر منطقی داده‌های شخصی را پاک کند:

–داده‌های شخصی دیگر برای اهدافی که برای آنها جمع آوری یا به نحو دیگری پردازش شده اند، ضروری نباشد.

–سوژه داده رضایت خود را که مبنای پردازش بر اساس بند (الف) ماده ۶(۱) یا بند (الف) ماده ۹(۲) است، پس بگیرد و هیچ مبنای قانونی دیگری برای پردازش وجود نداشته باشد.

–سوژه داده بر اساس ماده ۲۱(۱) با پردازش مخالفت کند و هیچ مبنای قانونی موجه برای پردازش وجود نداشته باشد، یا سوژه داده بر اساس ماده ۲۱(۲) با پردازش مخالفت کند.

–داده‌های شخصی به طور غیرقانونی پردازش شده باشند.

–داده‌های شخصی برای رعایت تعهد قانونی در حقوق اتحادیه یا دولت عضو که مسئول کنترل تابع آن است، باید پاک شوند.

–داده‌های شخصی برای ارائه خدمات جامعه اطلاعاتی موضوع ماده ۸(۱) جمع آوری شده باشند.

ماده ۱۹: مسئول کنترل، هرگونه اصلاح یا پاک کردن داده‌های شخصی یا محدودیت پردازش انجام‌شده مطابق با ماده ۱۶، ماده ۱۷(۱) و ماده ۱۸ را به هر گیرنده‌ای که داده‌های شخصی به او افشا شده است، باید اطلاع دهد، مگر اینکه این امر غیرممکن باشد یا مستلزم تلاش نامتناسب باشد. در صورتی که سوژه داده درخواست کند، مسئول کنترل باید آن گیرندگان را به اطلاع سوژه داده برساند.

–حق انتقال داده‌ها (ماده ۲۰)

متن ماده ۲۰: ۱. سوژه داده حق دارد داده های شخصی مربوط به خود را که به کنترلر ارائه کرده است، در قالبی ساختارمند، به طور معمول استفاده شده و قابل خواندن توسط ماشین دریافت کند و حق انتقال آن داده ها به کنترلر دیگری را بدون مانع از کنترلری که داده های شخصی به آن ارائه شده است، داشته باشد، در صورتی که:

–پردازش بر اساس رضایت موضوع بند (الف) ماده ۶(۱) یا بند (الف) ماده ۹(۲) یا بر اساس قرارداد موضوع بند (ب) ماده ۶(۱) باشد؛ و

–پردازش به صورت خودکار انجام می شود.

۲. سوژه داده در اعمال حق انتقال داده خود بر اساس بند ۱، حق دارد که داده های شخصی را در صورت امکان فنی، به طور مستقیم از یک کنترلر به کنترلر دیگر منتقل کند.

۳. اعمال حقی که در بند ۱ این ماده به آن اشاره شده است نباید خللی به ماده ۱۷ وارد کند. ۲ این حق در مورد پردازشی که برای انجام وظیفه‌ای که در راستای منافع عمومی یا در اعمال اختیارات رسمی تفویض شده به کنترلر انجام می‌شود، اعمال نمی‌شود.

۴. حق مذکور در بند ۱ نباید به حقوق و آزادی های دیگران لطمه بزند.

– حق اعتراض به پردازش داده‌های شخصی (ماده ۲۱)

متن ماده ۲۱: ۱. سوژه داده حق دارد هر زمان به دلایل مربوط به وضعیت خاص خود، با پردازش داده های شخصی مربوط به خود که بر اساس بند (e) یا (f) ماده ۶(۱) است، از جمله پروفایل سازی بر اساس آن مفادیر، اعتراض کند. مسئول کنترل دیگر اطلاعات شخصی را پردازش نخواهد کرد مگر اینکه مسئول کنترل دلایل قانونی و قانع کننده ای برای پردازش ارائه دهد که بر منافع، حقوق و آزادی های سوژه داده یا برای تأسیس، اعمال یا دفاع از دعاوی حقوقی غلبه کند.

۲. در صورتی که داده های شخصی برای اهداف بازاریابی مستقیم پردازش شوند، سوژه داده حق دارد در هر زمان با پردازش داده های شخصی مربوط به خود برای چنین بازاریابی، که شامل پروفایل سازی تا حدی که به چنین بازاریابی مستقیم مرتبط است، مخالفت کند.

۳. در صورتی که سوژه داده با پردازش برای اهداف بازاریابی مستقیم مخالفت کند، داده های شخصی دیگر برای چنین اهدافی پردازش نخواهند شد.

۴. حداکثر در زمان اولین ارتباط با سوژه داده، حق مذکور در بندهای ۱ و ۲ به صراحت به اطلاع سوژه داده خواهد رسید و به طور واضح و جداگانه از سایر اطلاعات ارائه خواهد شد.

۵. در زمینه استفاده از خدمات جامعه اطلاعاتی، و بدون لطمه به دستورالعمل[1] ای.سی/۲۰۰۲/۵۸ سوژه داده می تواند حق اعتراض خود را با استفاده از وسایل خودکار با استفاده از مشخصات فنی اعمال کند.

۶. در صورتی که داده های شخصی برای اهداف تحقیقات علمی یا تاریخی یا اهداف آماری مطابق با ماده ۸۹(۱) پردازش شوند، سوژه داده حق دارد به دلایل مربوط به وضعیت خاص خود، با پردازش داده های شخصی مربوط به خود مخالفت کند، مگر اینکه پردازش برای انجام وظیفه ای به دلایل منافع عمومی ضروری باشد.

-حق محدودسازی پردازش (ماده ۱۸):

متن ماده ۱۸: حق دسترسی به محدودیت پردازش برای سوژه داده در صورتی وجود دارد که یکی از موارد زیر اعمال شود:

-سوژه داده صحت داده‌های شخصی را به چالش بکشد، برای مدتی که به کنترلر امکان تأیید صحت داده‌های شخصی را بدهد.

-پردازش غیرقانونی باشد و سوژه داده با پاک کردن داده‌های شخصی مخالفت کند و به جای آن درخواست محدودیت استفاده از آنها را داشته باشد.

[1] . Directive 2002/58/EC

–کنترل‌کننده دیگر برای اهداف پردازش به داده‌های شخصی نیاز ندارد، اما سوژه داده برای اثبات، اعمال یا دفاع از دعاوی حقوقی به آنها نیاز دارد.

–سوژه داده طبق ماده ۲۱(۱) تا زمان بررسی اینکه آیا دلایل مشروع کنترلر بر دلایل سوژه داده اولویت دارد، به پردازش اعتراض کرده است.

۲. در صورتی که پردازش بر اساس بند ۱ محدود شده باشد، چنین داده‌های شخصی، به استثنای ذخیره‌سازی، تنها با رضایت فرد سوژه داده یا برای تأسیس، اعمال یا دفاع از دعاوی حقوقی یا برای حمایت از حقوق شخص حقیقی یا حقوقی دیگر یا به دلایل منافع مهم عمومی اتحادیه یا یک کشور عضو، پردازش خواهد شد.

۳. فرد سوژه داده‌ای که طبق بند ۱ محدودیت پردازش را به دست آورده است، قبل از رفع محدودیت پردازش، توسط مسئول کنترل مطلع خواهد شد.

یکی دیگر از انواع حقوق تصریح شده در مقررات عمومی حفاظت از داده‌ها، رضایت[1] است. این حق مهم، امکان کنترل کاربر بر داده‌های خود را فراهم می‌کند. به طور کلی پردازش داده های شخصی ممنوع است، مگر اینکه به صراحت توسط قانون مجاز باشد، یا موضوع داده رضایت به پردازش داده باشد. رضایت در حالی که یکی از شناخته‌شده‌ترین مبانی قانونی برای پردازش داده‌های شخصی است، تنها یکی از شش مبنایی است که در مقررات عمومی حفاظت از داده ذکر شده‌است. موارد دیگر عبارتند از: قرارداد، الزامات قانونی، منافع حیاتی موضوع داده، منافع عمومی و منافع مشروع همانطور که در ماده ۶ (۱) مقررات عمومی ذکر شده است. مراحل اساسی برای اثربخشی رضایت قانونی معتبر در ماده ۷ تعریف شده و در مقدمه ۳۲ مقررات عمومی بیشتر توضیح داده شده است. رضایت باید به صورت داوطلبانه، خاص، آگاهانه و صریح داده شود. برای به دست آوردن رضایت داوطلبانه، باید به صورت داوطلبانه داده شود. عنصر «آزاد» حاکی از انتخاب واقعی توسط سوژه داده است. هرگونه فشار یا نفوذ نامناسبی که بر نتیجه آن انتخاب تأثیر بگذارد، رضایت را نامعتبر می کند. بدین ترتیب، متن حقوقی عدم تعادل خاصی را بین کنترل‌گر و سوژه داده در نظر می‌گیرد.

آنچه گفته شد مجموعه حقوقی بود که برای اصطلاحاً سوژه داده در مقررات عمومی حفاظت از داده‌ها ذکر شده بود. این اقدامات همراستا با منشور حقوق اساسی اتحادیه اروپا برای حفاظت از حق حریم خصوصی کاربران اروپایی بوده است.

[1] .Consent

پیش از بحث درباره حریم داده در رسانه‌های اجتماعی و پلتفرم‌ها بحث حریم اطلاعات یا داده را مورد بحث بیشتری قرار می‌دهیم.

باقری (۱۴۰۰) در کتاب حق دسترسی به اطلاعات، حریم خصوصی را یکی از استثناءهای حق دسترسی به اطلاعات معرفی می‌کند که طی آن موسسات عمومی و خصوصی باید از افشاء و ارائه اطلاعاتی که زیرعنوان حریم خصوصی قرار می‌گیرند امتناع کنند. از آنجا که مبنای حق دسترسی به اطلاعات، به طور خاص اطلاعات موجود در مؤسسات عمومی است، از این منظور از داده‌های شخصی نیز اطلاعاتی است که افراد برای مقاصد گوناگون در اختیار نهادهای دولتی قرار می‌دهند و منظور داده‌ای کاربران در فضای مجازی نیست. هرچند باید توجه داشت که امروزه عموماً داده‌های شهروندان در فضاهای دیجیتال و برخط نگهداری می‌شوند و ماهیت شبکه‌ای اینترنت، دسترسی به داده‌های شخصی در اختیار نهادها و سازمان‌ها را به شکل‌های مختلف از جمله هک و نفوذ محتمل کرده است. بنابراین، منظور از داده‌های شخصی کلیت داده‌هایی است که در فضای مجازی به اشتراک گذاشته شده است.

در هر صورت، هریک از شهروندان به شکل‌های خواسته یا ناخواسته داده‌های زیادی را در اختیارها دولتها و مؤسسات خصوصی قرار می‌دهند که بخشی از آن به دلیل ضرورت دسترسی به خدمات عمومی است. اما دو خطر عمده جمع‌آوی و استفاده از داده‌های شخصی را تهدید می‌کند که باید به آن توجه شود. یکی گردآوری داده‌هایی است که دریافت خدمات لازمه آنها نیست و دوم، داده‌های گردآوری شده برای اهدافی غیر از ارائه خدمات مورد سوءاستفاده قرار بگیرند (انصاری، ۱۴۰۰). در شکل اخیر، پردازش داده‌های شهروندان بدون اطلاع و رضایت آنها به عنوان دو حق اساسی ناقض حقوق انسانی و برخلاف قانون است.

انصاری (۱۴۰۰) برخی اصول را برای حمایت و حفاظت از داده‌های شخصی کرده است که می‌تواند برای تدوین مقررات حفاظت از داده‌ها به عنوان اصول راهنما به کار رود. اول اصل، جمع‌آوری داده‌های شخصی است. طبق این اصل نباید به شکل گسترده اقدام به گردآوری داده‌ای شهروندان شود و تنها در صورت ضرورت باید داده‌های شهروندان گردآوری شوند. همچنین اطلاعات باید تا جای ممکن از افرادی که داده مرتبط به آنها است[1]گردآوری شوند. اصل دوم، استفاده از داده‌های

[1]. سوژه داده بنا بر تعریف مقررات عمومی حفاظت از داده‌ها

شخصی است. اصل دوم استفاده از داده‌های شخصی است. امکان دارد داده‌های گردآوری شده برای مقاصد ثانویه به کار روند و مثلاً داده‌های شهروندان در اختیار طرف‌های ثالث ازجمله شرکت‌های تبلیغاتی قرار بگیرد. بنابراین باید نسبت به هر نوع سوءاستفاده از داده‌های شهروندان حساس بود و تدابیر لازم در مورد آن اندیشیده شود. اصل سوم، گردش داده‌های شخصی است[۱]. هر نوع عملیات بر روی داده‌ها به معنای گردش داده‌های شخصی است و بر اساس این است لازم است که افشای هویت افرادی که داده مربوط به آنها است اجتناب شود[۲]. اصل چهارم جریان فرامرزی داده‌های شخصی است. فرامرزی بودن وسایل ارتباطی و اطلاعاتی سبب شده است تا داده‌های شخصی به‌آسانی به فراسوی مرزهای کشورها راه پیدا کنند که این امر به شکل ناخواسته نگرانی‌هایی را در مورد سوءکاربرد داده‌های یک کشور در کشورهای دیگر ایجاد کرده است.

یک مفهوم مرتبط در این زمینه محلی‌سازی داده‌ها است. محلی سازی داده ها به یک الزام قانونی یا اداری اجباری اشاره دارد که به طور مستقیم یا غیرمستقیم تصریح می کند که داده ها به طور انحصاری یا غیر انحصاری در یک حوزه قضایی مشخص ذخیره یا پردازش شوند. به عبارت دیگر، قوانین محلی سازی داده ها، انتقال برون مرزی داده ها را محدود می کند (دیوین، ۲۰۲۳).

هدف اصلی محلی‌سازی داده، اعمال کنترل بیشتر بر داده‌ها، حفظ امنیت ملی، صیانت از حریم خصوصی و ارتقای منافع اقتصادی در یک حوزه قضایی خاص است. دولت‌ها با الزام به ذخیره و پردازش محلی داده‌ها، تلاش می‌کنند اطمینان حاصل کنند که اطلاعات حساس در محدوده دسترسی قانونی و نظارتی آن‌ها باقی می‌ماند. این می‌تواند شامل اعمال محدودیت بر انتقال داده‌های فرامرزی یا الزام به ذخیره داده‌ها روی سرورهای محلی باشد. حریم خصوصی و حفاظت از داده‌ها نیز در بومی‌سازی داده‌ها نقش دارند. برخی از کشورها برای اطمینان از اینکه داده‌های شخصی شهروندانشان تحت قوانین داخلی حمایت از داده‌هایشان قرار می‌گیرد، اقدامات بومی‌سازی را اجرا می‌کنند. این امر اغلب به عنوان راهی برای تقویت حریم خصوصی و جلوگیری از دسترسی غیرمجاز یا سوء استفاده از اطلاعات شخصی تلقی می‌شود.

درنهایت، همانطور که انصاری (۱۳۹۷) نوشته است، اصل پنجم، اصل دسترسی به داده‌های شخصی و تصحیح آنها است. این اصل بیان می‌کند:

---

[۱]. به‌نظر می‌رسد منظور از آن پردازش داده‌های شخصی است.

[۲]. این اصل هنگام بحث در مورد مقررات عمومی حفاظت از داده‌ها مفصلاً مورد بحث قرار می‌گیرد.

داده‌های جمع‌آوری شده در مورد یک فرد ممکن است از خود وی جمع‌آوری نشده باشند و درنتیجه درست نباشند. یا ممکن است در زمان جمع‌آوری درست بوده باشند اما به مرور زمان و تغییر اوضاع و احول، دیگر درست نباشند و اصلاح ضرورت داشته باشد. به همین دلیل، باید امکان دسترسی اشخاص به داده‌های شخصی خودشان فراهم باشد تا از اعتراضی نسبت به صحت و درستی آنها دارند اعلام کنند و مانع از این شوند که استفاده از داده‌های غلط یا به گردش افتادن آنها، سبب ضررهای مادی یا معنوی آنان شود (انصاری، ۱۳۹۷: ۲۴۵).

همه این اصول به عنوان راهنمای تدوین هر نوع قانونی برای حفاظت از داده‌های شخصی می‌تواند سودمند باشد. همانطور که گفته شد، مفهوم گردش و یا به عبارت بهتر، پردازش اطلاعات در مباحث مرتبط با حریم خصوصی جایگاهی محوری دارد. گودرزی (۱۴۰۰) در بحث از حریم خصوصی اطلاعات شخصی می‌گوید، بحث‌های مرتبط به حریم خصوصی که در برخی نظام‌های حقوقی تحت عنوان حمایت از داده‌ها مورد تحقیق قرار دارد، دربرگیرنده قوانین حاکم بر پردازش داده‌ها و اطلاعات است. تعریف پردازش نشان می‌دهد که این حوزه به ظهور فناوری‌های اطلاعاتی و ارتباطی رابطی ندارد و امکان نقض آن پیش‌نیز وجود داشته است اما پیدایش این فناوری‌ها سبب سهولت و ترویج این قابلیت در مقیاسی کلان شده است و به همین دلیل جامعه بیش از پیش نگران سوءآثار نقض اطلاعات خصوصی است.

یکی از موضوعاتی که در اینجا باید به آن اشاره شود، موضوعات مرتبط با حریم داده کلان داده[1] است. حریم خصوصی کلان‌داده به محافظت از اطلاعات شخصی و داده‌های حساس در بستر گردآوری، ذخیره‌سازی و تحلیل داده‌های حجیم اشاره دارد. این مفهوم، طیف وسیعی از مسائل و دغدغه‌ها را در بر می‌گیرد که مربوط به حریم خصوصی، امنیت و استفاده اخلاقی از حجم عظیمی از داده‌های تولید شده از طریق منابع مختلف مانند رسانه‌های اجتماعی، تراکنش‌های آنلاین و دستگاه‌های متصل (اینترنت اشیا) است. همانطور که اسمیت (۲۰۱۳) و همکارانش اشاره کرده‌اند، کلان داده (بیگ دیتا) چالش‌های مهمی را برای حفظ حریم خصوصی ایجاد می‌کند. در اینجا برخی از مسائل کلیدی وجود دارد:

۱. گردآوری داده و نظارت: تلاش برای جمع‌آوری حجم عظیمی از داده‌ها برای تجزیه و تحلیل می‌تواند به نظارت دیجیتال منجر شود. این امر به طور بالقوه منجر به افشاگری‌های شخصی ناخواسته، سرقت هویت و تبعیض در بخش‌هایی مانند اشتغال و خدمات مالی می‌شود.

[1] .big data privacy

۲. حذف اطلاعات شناسایی و پنهان‌سازی: سازمان‌ها باید برای حفظ ناشناسی، داده‌های حساس را به طور مؤثر پنهان یا از آن‌ها اطلاعات شناسایی شخصی را حذف کنند. حذف اطلاعات شناسایی شخصی برای جلوگیری از افتادن داده‌ها به دست افراد غیرمجاز ضروری است.

۳. تبلیغات هدفمند: در حالی که تبلیغات شخصی‌سازی‌شده می‌توانند تجربه کاربری را بهبود بخشند، اما زیاده‌روی در تبلیغات هدفمند می‌تواند به حریم خصوصی افراد لطمه بزند. برقراری تعادل بین شخصی‌سازی و محافظت از حریم خصوصی ضروری است.

۴. استفاده غیرمجاز از داده: استفاده از داده بدون رضایت مناسب می‌تواند حقوق مربوط به حریم خصوصی را نقض کند. اطمینان از اینکه استفاده از داده‌ها مطابق با مجوزهای کاربر باشد، امری حیاتی است.

۵. خطرات امنیتی: منابع کلان داده (به عنوان مثال، شهرهای هوشمند، دستگاه‌های اینترنت اشیا، رسانه‌های اجتماعی) فرصت‌هایی را برای سوءاستفاده از داده‌ها توسط مهاجمین به منظور سود مالی فراهم می‌کند. محافظت در برابر نقض امنیتی امری حیاتی است.

در کل باید گفت که منظور از اطلاعات خصوصی شامل هر نوع اطلاعات مربوط به اشخاص ازجمله اطلاعات مربوط به علایق و منابع مالی و درآمد، اطلاعات مربوط به نیازهای فردی و وابستگی‌های قومی–نژادی، هویت فرهنگی و به طور کلی هر قسم اطلاعاتی را که بالقوه قابل استناد به ضرر شخص موضوع اطلاعات یا حداقل بهبود اشخاص دیگر باشد دربرمی‌گیرد (گودرزی، ۱۴۰۰).

ما تاکنون درباره حریم داده‌های شخصی به طور کلی بحث کردیم که تا حد زیادی به مفهوم‌سازی، فهم وجوه، اصول بنیادین و نیز حقوق اشخاص یا کاربران نسبت به داده‌های خود کمک کرد. منابعی که تاکنون مرور شد، به طور مستقیم حریم داده‌ها در رسانه‌های اجتماعی و پلتفرم‌های گوناگون دیجیتال را هدفگیری نکرده بودند. بنابراین در بخش به حریم اطلاعات در این دسته از رسانه‌های نوظهور می‌پردازیم.

رسانه‌های اجتماعی، پلتفرم‌های دیجیتال و حریم داده

در ادامه این بخش بر حریم داده در شبکه‌های اجتماعی تمرکز خواهیم کرد. موضوعی که در ادبیاتی که تاکنون مرور کرده‌ایم مورد غفلت واقع شده است. ما بحث خواهیم کرد که چگونه قابلیت‌ها، مکانیزم‌ها و الزامات کنش رفتاری در شبکهّای اجتماعی می‌تواند حریم خصوصی را مورد خدشه قرار دهد و مهمتر اینکه نشان خواهیم داد که چگونه خودافشایی

که به معنای تبادل داده‌های صمیمانه درباره خود است، اکنون به یک سازوکار اصلی در اقتصاد توجه و جلب نظر و نگاهداشت به اصطلاح دنبال‌کنندگان تبدیل شده است.

شبکه‌های اجتماعی به بخش جدایی‌ناپذیر زندگی ما تبدیل شده‌اند و فضایی را برای کاربران فراهم می‌کنند تا با هم ارتباط برقرار کنند، گفتگو داشته باشند و جنبه‌های مختلف تجربیات روزانه خود را به اشتراک بگذارند. زیربنای اصلی شبکه‌های اجتماعی در عمل به اشتراک گذاری ریشه دارد – از عکس‌ها و داستان‌های شخصی گرفته تا نظرات و ایده‌ها.

اشتراک‌گذاری در شبکه های اجتماعی به فرآیند توزیع انواع محتوا مانند پست های متنی، عکس ها، فیلم ها و لینک ها با شبکه ای از دوستان، دنبال کنندگان یا عموم مردم از طریق پلتفرم های رسانه های اجتماعی اشاره دارد. هدف اصلی از به اشتراک گذاری محتوا در شبکه های اجتماعی، ارتباط با دیگران، ابراز عقیده، تبادل اطلاعات و به نمایش گذاشتن تجربیات شخصی، علایق یا دستاوردها است. با این حال، با گسترش دامنه به اشتراک گذاری، مفهوم حریم خصوصی به دغدغه‌ای اساسی برای کاربران و همچنین این پلتفرم‌ها تبدیل شده است.

فن دایک (۱۳۹۶) در کتاب *فرهنگ اتصال* توضیح می‌دهد که چگونه مأموریت اعلام‌شده فیس‌بوک برای ایجاد دنیایی «بازتر و متصل‌تر» می‌تواند برای حفاظت از حریم خصوصی کاربران چالش‌برانگیز باشد. این مأموریت بر مفهوم «اشتراک‌گذاری» بنا شده است که تبادل اطلاعات شخصی بین کاربران و همچنین توزیع آن اطلاعات را به اشخاص ثالث ترویج می‌دهد. با این حال، این تأکید بر اشتراک‌گذاری، نگرانی‌هایی را در مورد حریم خصوصی ایجاد می‌کند، زیرا سهولت اشتراک‌گذاری اطلاعات می‌تواند با انتظارات کاربران از حریم خصوصی و کنترل بر داده‌های شخصی‌شان در تضاد باشد. مدیران ارشد فیس‌بوک بارها بر تعهد این شرکت به بازبودن و اتصال تأکید می‌کنند، اما این موضع با مفهوم حریم خصوصی در تضاد است و اغلب نشان‌دهنده‌ی وجود تنش بین این دو ارزش است.

عمل به اشتراک گذاری در رسانه های اجتماعی، چالش های مهمی را در زمینه حریم خصوصی ایجاد می کند. با به اشتراک گذاشتن اطلاعات شخصی، کاربران خود را در معرض خطرات مختلفی مانند سرقت هویت، قلدری سایبری و آزار و اذیت آنلاین قرار می دهند. علاوه بر این، حجم عظیم داده های به اشتراک گذاشته شده در رسانه های اجتماعی می تواند توسط تبلیغ کنندگان، کارگزاران اطلاعات و حتی دولت ها برای بازاریابی هدفمند، ایجاد پروفایل و نظارت مورد سوء استفاده قرار گیرد. همچنین، ماندگاری محتوای به اشتراک گذاشته شده در رسانه های اجتماعی، نگرانی هایی را در مورد حریم

خصوصی بلندمدت کاربران ایجاد می کند، زیرا پست های گذشته می توانند دوباره ظاهر شوند و عواقب ناخواسته ای برای روابط شخصی و حرفه ای داشته باشند.

برای حفظ تعادل سالم بین اشتراک‌گذاری و حریم خصوصی در رسانه‌های اجتماعی، کاربران و پلتفرم‌ها می‌توانند اقدامات مختلفی انجام دهند. کاربران باید نسبت به تنظیمات حریم خصوصی خود هوشیار باشند و از کنترل‌های موجود برای محدود کردن دیده شدن پست‌هایشان و مدیریت ردپای دیجیتال خود استفاده کنند. علاوه بر این، آن‌ها باید با خودداری از ارسال اطلاعات شخصی حساس یا محتوایی که می‌تواند به شهرت یا روابطشان آسیب بزند، اشتراک‌گذاری مسئولانه را تمرین کنند.

پلتفرم‌های رسانه‌های اجتماعی نیز مسئولیت محافظت از حریم خصوصی کاربران را دارند و شفافیت در شیوه‌های جمع‌آوری داده را تضمین می‌کنند و تنظیمات حریم خصوصی واضح و کاربرپسند را ارائه می‌دهند. همچنین آن‌ها باید روی تدابیر امنیتی قوی برای جلوگیری از نقض داده‌ها سرمایه‌گذاری کنند و اصول «حریم خصوصی با طراحی» را در معماری پلتفرم خود پیاده‌سازی نمایند.

موضوعی دیگری که می‌تواند حریم خصوصی را در شبکه‌های اجتماعی مورد تهدید قرار دهد، خودافشایی است. پلتفرم‌های رسانه‌های اجتماعی اساساً شیوه‌ی تعامل، ارتباط و به اشتراک گذاشتن تجربیات شخصی با دوستان، خانواده و جامعه‌ی آنلاین گسترده‌تر را متحول کرده‌اند. یک جنبه‌ی کلیدیِ این تعامل اجتماعیِ دیجیتال، عملِ «خودافشاگری» است – یعنی به اشتراک گذاشتنِ داوطلبانه‌ی اطلاعات شخصی، افکار و احساسات با دیگران. در حالی که خودافشاگری می‌تواند منجر به ایجاد ارتباطات عمیق‌تر و درک متقابل شود، اما همچنین پیامدهای قابل توجهی برای «حریم خصوصی» در حوزه‌ی رسانه‌های اجتماعی به همراه دارد.

نقض حریم خصوصی زمانی رخ می‌دهد که اطلاعات شخصی فرد بدون رضایت یا اطلاع او مورد دسترسی، استفاده یا توزیع قرار گیرد. پلتفرم‌های رسانه‌های اجتماعی، بر اساس ماهیت طراحی و گستردگی استفاده‌شان، محیطی را ایجاد می‌کنند که در آن اطلاعات افشا شده توسط خود افراد به راحتی قابل دسترسی و سوءاستفاده توسط بازیگران مختلف است:

خود پلتفرم‌های رسانه‌های اجتماعی: این پلتفرم‌ها اغلب داده‌های کاربران را برای بازاریابی هدفمند و سایر اهداف، جمع‌آوری، تجزیه و تحلیل کرده و با تبلیغ‌کنندگان و نهادهای ثالث به اشتراک می‌گذارند. این روش، با توجه به اینکه

اطلاعات شخصی به اشتراک گذاشته شده با حسن نیت می‌تواند بدون رضایت صریح برای اهداف دیگری مورد استفاده مجدد قرار گیرد، سوالاتی را در مورد حریم خصوصی کاربران ایجاد می‌کند.

کاربران دیگر: اطلاعات به اشتراک گذاشته شده در پلتفرم‌های رسانه‌های اجتماعی به راحتی توسط سایر کاربران قابل دسترسی و کپی‌برداری است که بالقوه می‌تواند منجر به توزیع مجدد غیرمجاز، قلدری سایری[1] یا سایر اشکال آزار و اذیت آنلاین شود.

بازیگران مخرب: هکرها، کلاهبرداران و سایر بازیگران مخرب می‌توانند از اطلاعات افشا شده توسط خود افراد در رسانه‌های اجتماعی برای سرقت هویت، باج‌گیری یا سایر اهداف شوم سوءاستفاده کنند.

در کل باید گفت شبکه‌های اجتماعی، ذاتا به اشتراک گذاری حجم عظیمی از اطلاعات شخصی تسهیل می‌کنند. افراد می‌توانند با چند کلیک، تصاویر را پست کنند، افکار شخصی خود را به اشتراک بگذارند و حتی کل مکالمات را ضبط کنند. با این حال، این داده‌ها همیشه به خوبی که باید محافظت نمی‌شوند و در نتیجه در برابر سوءاستفاده و کاربردهای نادرست آسیب‌پذیر هستند. برای اطمینان از امنیت داده‌های کاربران، باید اقداماتی برای تضمین حریم خصوصی اطلاعات به اشتراک گذاشته شده از طریق رسانه‌های اجتماعی وجود داشته باشد (سیندهایاچ، ۲۰۲۳).

یک بحث دیگر که باید در اینجا بر آن تأکید شود، حریم فضایی است. مفهوم حریم شخصی (فضایی) معمولاً به قلمرو فیزیکی اشاره دارد که مربوط به محافظت از فضای شخصی و کنترل بر محیط اطراف فرد است. با این حال، این مفهوم را می توان به طور مفهومی برای در بر گرفتن حریم خصوصی حساب های کاربری در فضاهای دیجیتال، مانند پلتفرم های رسانه های اجتماعی و خدمات آنلاین، گسترش داد.

در بستر پلتفرم های دیجیتال، حساب کاربری یک کاربر را می توان فضای دیجیتال شخصی او در نظر گرفت که حاوی اطلاعات شخصی، محتوا و تعاملات او است. کاربران اغلب انتظار و تمایل به کنترل بر این فضای دیجیتال دارند، از جمله توانایی تعیین اینکه چه کسی می تواند به اطلاعات آنها دسترسی داشته باشد و با آنها ارتباط برقرار کند.

[1] . cyberbullying

تعمیم ایده حریم شخصی فضا به حساب های کاربری در پلتفرم های دیجیتال، اهمیت کنترل کاربر و نیاز پلتفرم ها به ارائه تنظیمات امنیتی قوی برای حریم شخصی را برجسته می کند. کاربران باید بتوانند تصمیم بگیرند که آیا می خواهند حساب آنها عمومی یا خصوصی باشد، اتصالات خود را مدیریت کنند و کنترل دسترسی به اطلاعات و فعالیت های خود را داشته باشند.

در حالی که تعمیم مفهوم حریم شخصی فضا به پلتفرم های دیجیتال از لحاظ مفهومی مفید است، مهم است که چالش ها و پیچیدگی های منحصر به فرد مرتبط با حریم شخصی در فضای دیجیتال را درک کنیم. این چالش ها شامل جمع آوری داده، ردیابی آنلاین و پتانسیل به اشتراک گذاری غیرمجاز یا سوء استفاده از اطلاعات شخصی است. رسیدگی به این مسائل نیازمند رویکردی جامع به حریم شخصی است که هم کنترل کاربران بر فضاهای دیجیتال آنها و هم مسئولیت پلتفرم ها در محافظت از داده‌های کاربران و حفظ حقوق حریم شخصی را در بر می گیرد. درک فضایی از حریم خصوصی به جای حریم مکانی، همانطور که پیشتر با مفهوم فضای حسی ولیز (۲۰۲۴) نیز توضیح دادیم، به ما کمک می‌کند که بحث کنترل و دسترسی حریم خصوصی را به پروفایل یا حساب کاربری افراد بسط بدهیم و در مورد حفاظت از داده‌های شخصی بحث کنیم.

در کل باید گفت که بحث حریم خصوصی در رسانه‌های اجتماعی و پلتفرم‌ها دو جنبه دارد. یک جنبه آن بحث حکمرانی و تنظیم‌گری داده‌ها و حریم خصوصی کاربران است که در بخش قبل در مورد آن به طور مفصل بحث کردیم و بحث دیگر، کردارهای مرتبط با کنش‌های کاربران در این فضا است و اینکه چگونه مجموعه‌ای از کردارها و الزامات تعامل، ارتباط و اجتماع‌سازی در این فضا سبب شده است تا اشتراک‌گذاری داده‌های شخصی و خودافشایی چالش‌های جدیدی را برای حفاظت از داده‌ای افراد ایجاد کند.

-حریم خصوصی ارتباطات

یک مبحث دیگر که باید به آن توجه شود، بحث حریم خصوصی ارتباطات است. حریم خصوصی ارتباطات با حریم اطلاعات یا داده‌ها ارتباطی نزدیکی دارد اما برخی تفاوت‌های عمده در میان آنها مشاهده می‌شود. درواقع، حفاظت از داده‌ها در حریم ارتباطات هم اهمیت دارد اما جنبه‌های دیگری در حریم ارتباطات مطرح است که آنرا از حریم داده‌ها متمایز

می‌کند. در یک تعریف کلی می‌توانیم حریم ارتباطات یا ارتباط امکان برقراری ارتباط بین فردی بدون مداخله دیگری و آگاهی آن از محتوای پیام‌های مبادله شده تعریف کرد. دیگری می‌تواند یک شخص، سازمان و یا نهاد همانند نهادهای امنیتی باشد که به دلایل گوناگون ازجمله استراق سمع در جریان ارتباط دوسویه محرمانه، به شکل غیرقانونی و بدون رضایت طرفین ارتباط وارد می‌شود.

-حریم ارتباطات در ارتباطات سنتی

ما در اینجا ابتدا مباحث به اصطلاح سنتی‌تر حریم ارتباطات را مرور می‌کنیم و سپس حریم ارتباطات را در رسانه‌های اجتماعی و پیام‌رسان‌ها مورد بحث قرار می‌دهیم. امکان رمزگذاری پیام‌های مبادله‌شده در پیام‌رسان‌ها یکی از مزیت‌های پیام‌رسان‌ها تلقی می‌شود که دیگران را از درک محتوای ارتباطات در این فضاهای ارتباطی محروم می‌کند. از سوی دیگر، مشاهده شده است که یکی از نگرانی‌های کاربران ایرانی پیام‌رسان‌های داخلی امکان دسترسی بدون ضابطه مقامات امنیتی و قضایی به محتوای مبادله شده در این دسته‌پیام‌رسان‌ها است. پس از بحث‌های کلی به این موارد خواهیم پرداخت.
انصاری (۱۴۰۰) در بحث حریم ارتباطات خصوصی، ارتباط جمعی و یا عمومی را از ارتباط خصوصی تفکیک می‌کند و ارتباطی را که مخاطبان آن اشخاص محدود و معین باشد ارتباط خصوصی تلقی می‌کند. بر اساس این تفکیک وی توضیح می‌دهد:

چنانچه برقرارکننده ارتباط، عموم را مخاطب خود قرار دهد آنچه او بیان کرده است تابع آزادی بیان و ارتباطات بوده، برای شخص دیگری قابل استفاده و ارجاع است. درباره چنین ارتباطی اصل بر این است که بدون اجازه بیان‌کننده می‌توان اظهارات شفاهی یا مکتوب او را آزادانه اشاعه داد. اما چنانچه شخصی قصد داشته باشد پیام خود را صرفاً به شخص یا اشخاص محدود و معینی برساند، دستیابی به چنین پیامی تابع اصل محرمانگی و رعایت حریم خصوصی است. بنابراین، اصل بر این است که اشخاص ثالث حق رهگیری ارتباط مذکور را ندارند و دریافت‌کننده پیام نیز بدون رضایت صریح یا ضمنی ارسال‌کننده آن، حق افشاء و اشاعه آن را ندارد (انصاری، ۱۴۰۰: ۲۸۴).

انصاری بر اهمیت احترام به حریم خصوصی و رضایت در زمینه به اشتراک گذاشتن پیام یا اطلاعات تاکید می‌کند. این نوشته خاطرنشان می کند که اگر شخصی قصد ارسال پیامی برای افراد خاص یا مخاطبان محدود را داشته باشد، دسترسی

و انتشار چنین پیامی توسط اشخاص ثالث نقض حریم خصوصی است. طبق آن، اصل بر این است که اشخاص ثالث حق دخالت یا انتشار چنین ارتباطاتی را ندارند. علاوه بر این، گیرنده پیام حق ندارد بدون رضایت صریح یا ضمنی فرستنده، محتوا را فاش یا منتشر کند. این نوشته بر اهمیت رفتار اخلاقی و مسئولانه هنگام برخورد با پیام ها و اطلاعات شخصی تأکید می‌کند.

ارتباطات خصوصی شکل‌های مختلفی دارد که ازجمله می‌توان به ارسال نامه پستی، تلفن، تلکس، فکس، بی‌سیم و وسایل رادیویی مشاهده و اینترنت اشاره کرد. در تمام انواع ارتباطات مذکور این خطر وجود دارد که یک غریبه اعم از دولتی یا غیردولتی پیام خصوصی یک فرد را پنهانی رهگیری کند. ارتباطات رایانه‌ای و اینترنتی که جایگزین بسیاری از روش‌های سنتی انتقال پیام همانند ارتباطات تلفنی و پستی شده است، ذاتاً در معرض رهگیری و نظارت دیگران قرار دارد و دیگران به جز دریافت کننده می‌توانند به راحتی به آن دسترسی پیدا کنند و از مفاد آن مطلع شوند (انصاری، ۱۴۰۰). بحث‌های دیگر انصاری درباره باز کردن و تفتیش مرسولات پستی و رهگیری تلفن‌ها و سیگنالهای رادیویی است که به فضای مجازی ارتباط ندارند.

سروش (۱۳۹۸) نیز اعتقاد دارد شکلهای مختلف ارتباطات اشخاص نظیر نامه پستی، تلفن، نمابر، بی‌سیم، اینترنت و برخی شیوه‌های دیگر، وقتی در آنها ارتباط جنبه خصوصی پیدا می‌کند و دارای مخاطب خاص است، باید محرمانه تلقی شود و هیچ‌کس مجاز به اطلاع یافتن از محتوای آن نیست. اما توسعه ارتباطات سبب شده تا برای استراق سمع و رهگیری به شکلی گسترده از این روش که تسهیل شده است، استفاده شود و بسیاری از دولتها در خصوص مسائل امنیتی خود را محق می‌دانند که از این ابزارها استفاده کنند و استفاده از چنین شیوه‌هایی در همه کشورها برای رهگیری عناصر جاسوسی و باندهای تبهکاری قانونی است. اما در مورد احزاب و گروه‌های قانونی و نیز نویسندگان و منقدان، نمی‌توان با اطمینان از عدم نقض حریم ارتباطی سخن گفت و چون این روش‌ها به شکل محرمانه انجام می‌شود، برای عموم شهروندان قابل تشخیص و شناسایی نیست.

روشن است که کاربرد این شیوه‌ها برای شناسایی گروه‌های تروریستی و موارد مشابه وجاهت قانونی دارد اما معضل زمانی حادث می‌شود که حریم ارتباطی شهروندان عادی بدون دلیل موجه و بدون مجوز قانونی نقض شود. با توجه به پنهانی بودن

این نوع مداخله، ضرورت دارد که برای قانونی بودن آن تدابیری اندیشیده شود و تا حد ممکن نیز محدود به موارد استثنائی شود.

گودرزی (۱۴۰۰) در خصوص حریم خصوصی ارتباط اینترنتی می‌نویسد که به طور کلی ضبط، ذخیره یا انواع دیگر رهگیری ارتباطات خصوصی افراد بدون رضایت آنها مجاز نیست و منظور از ارتباط خصوصی اینترنت هر نوع ارتباطی است که فرد برقرارکننده ارتباطت پیام خود را به دریافت‌کننده معین در ایران ارسال کرده و انتظار دارد تا پیام مذکور فقط توسط فرد مذکور دریافت شود. در ماده دوم قانون جرایم رایانه‌ای پیش‌بینی شده است که هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سیستم‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم می‌شود.

-حریم ارتباطات در رسانه‌های اجتماعی

با توسعه اینترنت و رسانه‌های اجتماعی، شکل عمده ارتباط خصوصی از پست الکترونیک به برقراری ارتباط از طریق پیام‌رسان‌های اجتماعی منتقل شده است. در ابتدای دهه ۱۳۹۰ که پیام‌رسان‌ّها در ایران کم‌کم توسعه پیدا می‌کردند، یک نگرانی عمده امکان برقراری ارتباط صوتی و تصویری توسط خدمت اُ.تی.تی[1]بود. برنامه‌های پیام‌رسان مبتنی بر اُ.تی.تی، پلتفرم‌های پیام‌رسانی هستند که به جای شبکه مخابرات از اتصال اینترنت برای انتقال ارتباطات استفاده می‌کنند. این نگرانی از یک طرف به کاهش سطح درآمد شرکت مخابرات مربوط می‌شد. اما یک نگرانی دیگر، کاهش امکان نظارت بر محتوای مبادله‌شده در این پیام‌رسان‌ها به‌ویژه از منظر امنیتی بود. موضوعی که سالها بعد به شکل کاربرد پیام‌رسان تلگرام توسط برخی گروه‌ها و افراد مخالف جمهوری اسلامی در برخی از ناآرامی‌های دهه ۱۳۹۰ بروز و ظهور پیدا کرد و یکی از دلایل فیلترینگ این پیام‌رسان بود.

-تبادل پیام در پیام‌رسان‌ها به مثابه حریم خصوصی ارتباطات

[1] .OTT (over-the-top)

در سال های اخیر، برنامه های پیام رسان به عنوان روش اصلی ارتباطات شخصی ظهور کرده اند و تا حد زیادی جایگزین روش های سنتی مانند پیامک، تماس تلفنی و ایمیل شده اند. این برنامه ها که امکان ارسال پیام های متنی، صوتی و تصویری به صورت آنلاین و لحظه‌ای را فراهم می کنند، به دلیل راحتی، مقرون به صرفه بودن و چند کارکردی بودن، محبوبیت زیادی به دست آورده اند. با افزایش روزافزون تعداد کاربران تلفن هوشمند در سراسر جهان، برنامه های پیام رسان راهی آسان و در دسترس را برای افراد برای برقراری ارتباط با دوستان، خانواده و همکاران ارائه می دهند و ارتباطات شخصی و حرفه ای را در سراسر جهان تقویت می کنند.

-رمزگذاری به عنوان پیش‌نیاز حریم ارتباطی

پذیرش گسترده برنامه‌های پیام‌رسان را می‌توان به تأکید آن‌ها بر حریم خصوصی و امنیت نیز نسبت داد. بسیاری از برنامه‌های پیشرو مانند واتس‌اپ، سیگنال و تلگرام از رمزگذاری سرتاسری[1] استفاده می‌کنند تا اطمینان حاصل شود که فقط فرستنده و گیرنده می‌توانند به محتوای پیام‌های خود دسترسی داشته باشند. این رمزگذاری قوی، اطلاعات حساس را از دسترسی غیرمجاز محافظت می‌کند و به کاربران این آرامش خاطر را می‌دهد که بدوند مکالمات شخصی آن‌ها خصوصی باقی می‌ماند. علاوه بر این، برنامه‌های پیام‌رسان حس صمیمیت و کنترلی را ارائه می‌دهند که سایر اشکال ارتباطات دیجیتال ممکن است فاقد آن باشند و به کاربران این امکان را می‌دهند تا تنظیمات خود را سفارشی کنند، گروه‌های خصوصی ایجاد کنند و نحوه تعامل با مخاطبین خود را انتخاب کنند.

جونز، ماتاموروس-فرناندز و بالچ (۲۰۲۴) در کتاب *واتس‌اپ* توضیح می‌دهند که چگونه این پیام‌رسان، به‌منزله نوعی پیام خصوصی تلقی شده است. موضوعی که در حریم ارتباطات که پیشتر مورد بحث قرار گرفت، اهمیت دارد. به گفته آنها، در ادبیات دانشگاهی، واتس‌اپ عموماً به عنوان یک برنامه برای ارتباطات خصوصی شناخته می‌شود. در ابتدا، این برنامه به عنوان پلتفرمی برای برقراری ارتباط شخصی و مکالمه بین دوستان و خانواده طراحی شد. بر خلاف سایر پلتفرم‌های رسانه‌های اجتماعی مانند توییتر و فیس‌بوک، واتس‌اپ داده‌های کاربران را برای پیش‌بینی رفتار و نمایش تبلیغات هدفمند جمع‌آوری نمی‌کرد. ویژگی گروهی که در سال ۲۰۱۱ معرفی شد، با امکان برقراری ارتباط در یک محیط کنترل‌شده‌تر، از

[1]. end-to-end encryption

این دیدگاه ارتباط خصوصی پشتیبانی می‌کرد. با این حال، این ویژگی همچنین نقطه عطفی در تحول واتس‌اپ از یک ابزار پیام‌رسانی فرد به فرد به یک پلتفرم ارتباطی جامع در سطح جهانی بود.

اما موضوع حریم خصوصی و امنیت پیام‌های مبادله شده موضوعی اساسی برای کاربران است. به‌طوری‌که گرچه در سال های اخیر، محبوبیت برنامه های پیام رسان موبایل و تماس صوتی اینترنتی (VoIP) برای تلفن های هوشمند به شدت افزایش یافته است، اما این موضوع همچنین سبب افزایش علاقه به تحقیقات مرتبط با امنیت و حریم خصوصی این برنامه ها شده است (مولر و همکاران، ۲۰۱۴).

رمزگذاری یکی از ویژگی‌های مهمی است که سبب شده است تا پیام‌رسان‌ها ازجمله واتس‌اپ، یک فناوری برای ارتباط شخصی و خصوصی هستند (جونز، ماتاموروس–فرناندز و بالچ، ۲۰۲۴). به گفته پوجالت (۲۰۲۴) رمزگذاری در ارتباطات دو طرفه مانند تبدیل پیام های شما به کدهای سری است که فقط افراد مورد نظر می توانند آن را بفهمند. این فرآیند، کلمات شما را بهم ریخته می‌کند تا در صورت گوش دادن فرد دیگری، او هیچ چیزی متوجه نشود.

در حالی که رمزگذاری برای حفظ حریم خصوصی ارتباطات ضروری است، اما در برقراری تعادل بین امنیت و دسترسی نیز چالش هایی ایجاد می کند. رمزگذاری قوی گاهی اوقات می تواند تحقیقات اجرای قانون را مختل کند یا شناسایی و حذف محتوای مضر را برای ارائه دهندگان پلتفرم دشوار سازد.

از طرف دیگر، ضعیف کردن رمزگذاری یا فراهم کردن درهای پشتی برای مقامات، به طور بالقوه می تواند حریم خصوصی کاربران را به خطر بیندازد و راه را برای بازیگران مخرب جهت سوء استفاده از آسیب پذیری ها باز کند. بنابراین، دستیابی به تعادل مناسب بین محافظت از حریم خصوصی افراد و اجازه دسترسی لازم برای اجرای قانون، همچنان یک موضوع مورد بحث است.

با این حال، اجرای رمزگذاری قوی در برنامه های پیام رسانی اُ.تی.تی همچنین چالش هایی را در برقراری تعادل بین حریم خصوصی و نیاز به دسترسی قانونی توسط سازمان های اجرای قانون ایجاد می کند. در حالی که رمزگذاری برای حفظ حریم خصوصی کاربران ضروری است، اما می تواند تحقیقات را مختل کند یا شناسایی و جلوگیری از انتشار محتوای مضر را برای ارائه دهندگان پلتفرم دشوار کند.

به طور کلی، ترکیب برنامه های پیام رسانی اُ.تی.تی و رمزگذاری قوی، پتانسیل افزایش قابل توجه حریم خصوصی ارتباطات در عصر دیجیتال را دارد. دستیابی به تعادل مناسب بین محافظت از حریم خصوصی کاربران و امکان دسترسی قانونی برای حفظ اعتماد و امنیت این پلتفرم ها حیاتی خواهد بود.

- پروفایل رسانه‌های اجتماعی به مثابه فضای خصوصی

مفهوم حریم خصوصی فیزیکی به طور کلی به محافظت از فضای شخصی در دنیای واقعی، مانند خانه، محل کار یا سایر مکان های فیزیکی اشاره دارد. با این حال، می توان بین حریم خصوصی فیزیکی و حریم خصوصی پروفایل های کاربر در پلتفرم های رسانه های اجتماعی مشابهت هایی قائل شد.

در بستر رسانه های اجتماعی، پروفایل کاربر را می توان فضای دیجیتال شخصی او در نظر گرفت که ممکن است بخواهد از دسترسی غیرمجاز، نفوذ یا افشا محافظت کند. کاربران اغلب این امکان را دارند که پروفایل های خصوصی ایجاد کنند، جایی که می توانند کنترل کنند چه کسی محتوای آنها را ببیند و با آنها ارتباط برقرار کند. این را می توان به عنوان بسط حریم خصوصی فیزیکی به دنیای دیجیتال در نظر گرفت، جایی که افراد به دنبال حفظ حریم شخصی و کنترل بر محیط آنلاین خود هستند.

در حالی که شباهت هایی بین حریم خصوصی فیزیکی و حریم خصوصی پروفایل های رسانه هـای اجتمـاعی وجـود دارد، ضروری است که تشخیص دهیم فضای دیجیتال دارای ویژگی ها و چالش های منحصر بـه فـردی اسـت. نگرانـی هـای مربوط به حریم خصوصی دیجیتال فراتر از دسترسی فیزیکی به یک پروفایل است و شامل مسائلی مانند جمـع آوری داده، ردیابی آنلاین و پتانسیل به اشتراک گذاری غیرمجاز یا سوء استفاده از اطلاعات شخصی می شود.

در نتیجه، در حالی که از نظر مفهومی می توانیم حریم خصوصی فیزیکی را به پلتفرم های رسانه های اجتماعی گسترش دهیم، ضروری است که پیامدهای گسترده تر و چالش های مرتبط با حریم خصوصی دیجیتال را درک کنیم و برای رفع موثر این نگرانی ها، استراتژی های جامع توسعه دهیم.

در کل با ملاحظه هدف این فصل که مفهوم‌سازی حریم خصوصی بوده است، مضمون اصلی و مضامین فرعی شناسایی شدند که در جدول ۲-۱ آمده است. این مضامین به تدوین چارچوبی برای حفاظت از داده و حریم خصوصی در فضای مجازی و پلتفرم‌های رسانه‌های اجتماعی کمک می‌کنند.

مفهوم و ابعاد حریم خصوصی	-حریم خصوصی به مثابه امری غریزی؛ -حریم خصوصی به مثابه امری اجتماعی؛ حریم خصوصی به مثابه امری تاریخی؛ -حریم خصوصی به مثابه کنترل -حریم خصوصی به مثابه دسترسی -حریم خصوصی به مثابه امری ارتباطی -قابلیت‌های رسانه‌های اجتماعی و حریم خصوصی -حریم خصوصی به مثابه حریم کاربران -پلتفرم‌های ایرانی و بی‌توجهی به حفاظت از داده‌های شخصی حق دسترسی به اطلاعات حق اطلاع (شفافیت) حق اصلاح حق پاک کردن حق انتقال داده‌ها حق اعتراض به پردازش داده‌های شخصی حق محدودیت -حریم خصوصی ارتباطات -حریم ارتباطات در ارتباطات سنتی

	–حریم ارتباطات در رسانه‌های اجتماعی –تبادل پیام در پیام‌رسان‌ها به مثابه حریم خصوصی ارتباطات –رمزگذاری به عنوان پیش‌نیاز حریم ارتباطی – پروفایل رسانه‌های اجتماعی به مثابه فضای خصوصی

جدول ۴–۱) مضامین بخش مفهوم‌سازی حریم داده و اطلاعات به طور کلی و در پلتفرم‌های رسانه‌های اجتماعی

نتیجه‌گیری

در این بخش، تلاش شد تا حریم خصوصی به‌ویژه با تمرکز بر حریم داده و حریم ارتباطات مفهوم‌سازی شود. در این بخش با تمرکز بر مفهوم حقوق کاربر و ارتباط دادن آن به پلتفرم‌های رسانه‌های اجتماعی، تلاش شد تا از مفهوم شخص یا موضوع داده به مفهومی فراگیر در عصر رسانه‌های اجتماعی برسیم و بنابراین، تدوین مقررات مرتبط با داده‌های شخصی بر داده‌های شخصی و حق ارتباط کاربر متمرکز شود.

بخش دوم

حریم داده و اطلاعات در اسلام، قوانین ایران و اسناد بین‌الملل

مقدمه

هدف این بخش مروری بر بحث‌های مرتبط با حریم خصوصی در منابع دینی و فقهی است. با وجود این تمرکز عمده بر حریم اطلاعات (داده) و ارتباطات خواهد بود. ما تاکنون بحث‌های مفصل درباره انواع حریم خصوصی انجام دادیم، می‌توان حریم خصوصی را به دو دسته حریم مادی (مشتمل بر حریم مکانی، جسمانی و اموال) و حریم معنوی (حریم اطلاعات، ارتباطات و حیثیت اجتماعی) نیز تقسیم کرد (فاطمی، نوابی و عبدالهی‌نژاد، ۱۴۰۱). تمرکز این بخش بر دسته دوم و بسط آن بر اساس مبانی دینی و حقوقی است. حفظ شأن و کرامت انسان یکی از بنیان‌های اساسی بحث‌های حریم خصوصی در اسلام است. همانطور که خاکی، محقق داماد و درگاهی (۱۴۰۲) بحث کرده‌اند، انسان دارای کرامت ذاتی است و از این جهت جان و مال و آبروی او باید محترم شمرده شده و از تعرض مصون بماند. ازجمله اموری که به حریم شخصیتی انسان مرتبط می‌شود، نوع اطلاعات و ارتباطات او با دیگران است که از طریق ابزارهای ارتباطی گوناگون صورت می‌گیرد. هدف این بخش این است که علاوه بر رویکردهایی که عمدتاً در منابع غربی درباره ابعاد گوناگون حریم داده وجود داریم، دریابیم چه ابعادی دیگری را با ملاحظه ادبیات فوق می‌توان برای بسط حریم داده به کار گرفت. بنابراین، بعدی اطلاعاتی و ارتباطی حریم خصوصی و نیز بر چه مبنایی امکان ورود به حریم خصوصی مجاز شمرده شده، کلیت بحث این بخش را تشکیل می‌دهد.

- حریم خصوصی در اسلام

-حریم خصوصی به‌مثابه حفظ کرامت انسانی

انصاری (۱۴۰۰) در مورد حریم خصوصی در حقوق اسلام بحث می‌کند که برخلاف سابقه کوتاه غرب در حمایت از حریم خصوصی، حمایت از حریم خصوصی در حقوق اسلام قدمت بسیار زیادی دارد و پیش از آنکه حریم خصوصی در کنوانسیون‌ها و اسناد بین‌المللی حقوق بشر به رسمیت شناخته شود، در منابع اسلامی مورد تأکید بسیاری قرار گرفته است.

به عبارت دیگر، اسلام به کرامت و حرمت آدمیان اهمیت فراوان داده است و حریم خصوصیِ افراد را با وسواس و باریک بینیِ فراوان پاس داشته است. در آیات قرآنی و نیز احادیث معصومان(ع) و هم چنین در سخنان پیشوایان دینی توصیه های فراوانی است که آدمیان را از ورود به حریم خصوصی افراد اکیداً باز داشته است (مهریزی، ۱۳۷۸).

گرچه، با وجود این سابقه طولانی توجه به حریم خصوصی در اسلام، در نظام حقوقی ایران و سایر کشورهای مسلمان، در تدوین قوانین و مقررات مرتبط با حریم خصوصی به آن به اندازه کافی توجه نشده است. این درحالی است که برای حمایت از حریم خصوصی و مقوله‌های مختلف آن، در نظام حقوقی اسلام مبانی محکمی وجود دارد که برای حمایت از حقوق خصوصی کفایت می‌کند (انصاری، ۱۴۰۰). این هدف در این پژوهش دنبال می‌شود. به عبارت دیگر، قصد داریم رویکرد اسلامی به حریم خصوصی، به‌ویژه با تمرکز حریم داده و ارتباط را مورد ملاحظه قرار دهیم و به عنوان مبنایی برای ارائه پیش‌نویس مقررات جامع حریم خصوصی و داده ایران به کار بریم.

دین اسلام نیز به عنوان یکی از بزرگترین ادیان جهان اهتمام ویژه ای به حریم خصوصی انسانها و حفظ آن داشته است. خداوند به صراحت در آیات ۱۲سوره حجرات؛ ۱۸۹ سوره بقره ؛ ۱۹ و ۲۷ الی ۳۰ سوره نور درباره لزوم رعایت حریم خصوصی افراد سخن گفته است. همچنین روایتهای بسیاری از پیامبر(ص) و امامان معصوم (ع) درباره حرمت حریم خصوصی افراد نقل شده است (فکری، ۱۳۹۷).

گرچه باید توجه داشت که اصطلاح «حریم خصوصی» در آیات و روایات وجود ندارد و موضع اسلام نسبت به حریم خصوصی «تحویل‌گرایانه» است یعنی حریم خصوصی در قالب احاله به حقوق و آزادی‌های دیگر نظیر حق مالکیت، منع تجسس، اصل برائت، منع سوء ظن و اشاعه فحشا و سب و هجو و قدف و نمیمه و غیبت و خیانت در امانت حمایت شده است (انصاری، ۱۴۰۰).

به عبارت دیگر، از نظر تاریخی اسلام پیش از غرب حریم خصوصی را به عنوان یک اصل مهم و با مبانی متعدد و محکم از طریق ضمانتهای اجرایی دنیوی و اخروی مورد حمایت قرار داده و موضع حمایت‌گرایانه خویش را در قالب احاله به حقوق و

آزادی‌های دیگر همانند منع تجسس، سوءظن و نیز اصولی همانند سلطه و عدم ولایت به‌گونه‌ای تلوییحی تبیین کرده است (دانش‌پور، ۱۳۹۵: ص.۴۰).

-مصداق‌های حریم خصوصی در اسلام

چون هدف در نهایت برقراری نسبت میان رویکردها به حریم خصوصی در اسلام و ابعاد گوناگون حریم خصوصی است. موارد و اصطلاحات مرتبط با حریم خصوصی در آیات و روایات را در قالب دسته‌بندی زیر می‌توان بیان کرد:

۱. ممنوعیت تجسس و تحسس و تفتیش؛

۲. ممنوعیت ورود به منازل بدون استیذان؛

۳. ممنوعیت استراق بصر؛

۴. ممنوعیت استراق سمع؛

۵. ممنوعیت سوءظن؛

۶. ممنوعیت نعیمه و غیبت؛

۷. ممنوعیت سب و هجو قذف؛

۸. ممنوعیت خیانت در امانت (انصاری، ۱۴۰۱).

از میان دسته فوق، ممنوعیت ورود به منازل بدون استیذان نخستین تصور از حریم خصوصی یعنی حریم مکانی را به ذهن متبادر می‌کند. ممنوعیت تجسس و تحسس و نیز استراق سمع و بصر نیز با حریم اطلاعاتی و ارتباطی تداعی می‌شود. به همین دلیل این سه دسته از اصطلاحات را که با رویکرد پژوهش حاضر ارتباط دارند، اندکی مورد بحث و بررسی بیشتر قرار می‌دهیم.

-ممنوعیت تجسس

در قران کریم حرمت تجسس مورد تاکید بوده و سوره مبارکه حجرات با عبارت لاتجسسوا صراحتاً تجسس در امور دیگران را منع نموده است. در صدر اسلام نیز این آیه شریفه به معنای عدم تجسس در حریم خصوصی مردم فهم میشده است. در این زمینه در تفسیر مجمع البیان در ذیل این آیه این گونه نوشته شده که خلیفه دوم با عبدالرحمن شبی به تجسس پرداختند، دیدند در خانه ای دود آتش بلند است. رفتند در آن خانه را کوبیدند و با اجازه داخل گردیدند. مردی را با زنی دیدند که در دست آن مرد کاسه ای نیز بوده است، عمر پرسید: این زن کیست؟ مرد گفت: زوجه من است سپس پرسید در میان آن کاسه چیست؟ گفت: آب است سپس پرسید شعری که آن زن با آواز می‌خواند چگونه شعری است؟

مرد مزبور آن اشعار را برای عمر خواند بعد از این پرسش‌ها آن مرد رو به عمر کرد و گفت: مگر نمی‌دانی که خداوند در قرآن فرموده: «وَلاتَجَسَّسُوا». عمر گفت: راست می‌گوئی و از آن خانه بیرون آمد (محبی، ۱۳۹۷).

ممنوعیت تجسس در آیات و روایت‌های مختلفی مورد تأکید قرار گرفته است. خداوند در آیه ۱۲ سوره حجرات می‌فرماید: «يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيراً مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضًا». که معنای آن این است: «ای کسانی که ایمان آورده اید از بسیاری از گمان ها بپرهیزید که برخی از گمان ها گناه است و از یکدیگر تجسس نکنید و غیبت نکنید».

به نظر می‌رسد این روایت از دو منظر با حریم خصوصی ربط پیدا می‌کند. نخست، ممنوعیت نقض حریم مکانی و دوم، ممنوعیت گردآوری اطلاعات یا داده‌های شخصی. درواقع، به نظر می‌رسد هدف اصلی تجسس گردآوری داده‌ها و اطلاعاتی است که شخص دوست ندارد دیگران از آن مطلع شوند.

-ممنوعیت استراق سمع و بصر

در فقه اسلامی مکرراً به عدم تجاوز به حریم خصوصی دیگران از طریق استراق سمع اشاره شده است. استراق بصر نیز همانند استراق سمع ممنوع است (خاکی، محقق داماد و درگاهی، ۱۴۰۲). هتک ستر و نگاه کردن به هرآنچه نوعاً یا شخصاً در قلمرو حریم خصوصی قرار می‌گیرد ممنوع است و فقه اسلامی سرشار از توصیه‌هایی درزمینه عدم تجاوز به حریم خصوی اشخاص از طریق نگاه کردن است. ازجمله اینکه طبق تعالیم اسلامی هیچکس نمی‌تواند بدون اذن همسایه به خانه او پنجره باز کند (انصاری، ۱۴۰۰).

امروزه، در رسانه‌های اجتماعی، به‌ویژه رسانه‌های اجتماعی تصویری همانند اینستاگرام و تیک‌تاک، نقض حریم خصوصی افراد به راحتی رواج پیدا کرده است. بسیاری از افراد عامدانه بسیاری از امور و اقداماتی را که پیشتر در حوزه حریم درون‌خانگی آنها قرار داشت، آگاهانه در معرض دید دیگران قرار می‌دهند. اما درصورتی‌که افراد تنظیمات خود را به شکل خصوصی درآورند، می‌توان ادعا کرد که چنانچه افرادی به این حریم به هر شکلی نفوذ کنند، مرتکب استراق بصر شده‌اند.

از سوی دیگر، استراق سمع نیز در سنت اسلامی ممنوع شده است و پیامبر اکرم نیز از مجازات روز قیامت برای افرادی خبر داده است که بدون رضایت دیگران به مکالمات خصوصی آنها گوش می‌دهند (۱۴۰۰). امروزه افراد فایل‌های صوتی خود را که بخشی از آنها خصوصی است در رسانه‌های اجتماعی به اشتراک می‌گذارند. برای مثال از طریق پیام‌رسان‌ها برای دیگران پیام صوتی ارسال می‌کنند و یا اینکه از طریق برخی ابزارهای نصب شده در گوشی‌های تلفن همراه امکان گوش دادن پنهانی به مکالمات خصوصی دیگران وجود دارد. گوش دادن پنهانی به هرشکلی نوعی استراق سمع و نقض حریم خصوصی محسوب می‌شود.

استراق سمع و بصر در دسته حریم ارتباطی قرار دارند. ارتباطات اشخاص در زمره مصادیق حریم خصوصی است که افراد تلاش می‌کنند دیگران را از دسترسی به آنها منع کنند اما پیشرفت‌های فناورانه سبب سهولت دسترسی به اطلاعات افراد شده و روابط دیگران در گوش‌رس و دیدرس دیگران قرار گرفته است که مورد حمایت حقوق اسلامی است (احمدلو، ۱۴۰۰).

بحث‌های مرتبط با حریم خصوصی در اسلام بسیار مفصل است و طیفی از مسائل گوناگون ازجمله ادله نقلی نظار بر حریم خصوصی، آیات مرتبط با حریم خصوصی، ادله عقلی و قواعد فقهی، ازجمله قاعده سلطه «الناس مسلطون علی اموالهم» و قاعده «اصل عدم ولایت» را دربرمی‌گیرد (خاکی، محقق داماد و درگاهی، ۱۴۰۲). این مباحث، بسیار گسترده هستند با اینهمه، ما به طور گذرا به مصادیق ارتباطی حریم خصوصی از منظر اسلام پرداختیم و در بخش نیز جواز نقض حریم خصوصی بر اساس مبانی اسلامی را مرور می‌کنیم.

حدود اختیار دولت برای ورود به حریم خصوصی

همانطور که بحث شد حریم خصوصی به عنوان یک حق اساسی در دین اسلام به رسمیت شناخته شده است و اکیداً مورد تأکید قرار گرفته است و افراد از ورود به حریم خصوصی دیگران منع شده‌اند. با وجود این برخی شرایط ایجاب می‌کند که حریم افراد در معرض نقض قرار بگیرد و این نقض توجیه‌پذیر می‌شود. اما ملاحظات آن باید مد نظر قرار بگیرد. به عبارت دیگر، با بررسی ادله فقهی و نیز مواد قانونی به حرمت و ممنوعیت نقض حریم خصوصی پی می‌بریم اما در صورت تزاحم مصلحت فردی با مصالح اجتماعی و با تشخیص حاکم و مجوز قانونی امکان ورود به حریم خصوصی با رعایت ضوابط وجود دارد.

حریم خصوصی به معنای محدود معقولی است که یک فرد انتظار دارد از دسترسی دیگری که شامل دولت و حاکمیت هم هست، مصون بماند. وجود قوانین حریم خصوصی در یک جامعه مردم‌سالار الزامی است و سبب می‌شود تا از دخالت حاکمیت‌های تمامیت‌خواه و اقتدارگرا در آن جلوگیری شود (فاطمی، نوابی، عبدالهی‌نژاد، ۱۴۰۱).

–مصلحت به مثابه جواز ورود به حریم خصوصی

یکی از جوازهای ورود به حریم خصوصی مصلحت است. مصلحت در لغت به معنای خیر و نیکی و نیز جلب منفعت و دفع ضرر و به تعبیر عزالی، مصلحت به معنای محافظت از مقصود شرع است است که مقصود شرع هم بر اصول حفظ دین، جان، نسل و مال مردم استوار شده است. از سوی دیگر در جامعه اسلامی باید بین مصلحت‌های دنیوی همانند لذت‌جویی و فایده‌گرایی و مصلحت‌های معنوی همانند تقوا و خویشتن‌داری تعادل برقرار شود. تأمین مصالح عمومی وظیفه حکومت است و در نظام اسلامی، «مصلحت عمومی» در چهارچوب مقاصد دین و موازین شریعت، مبنای تمام احکام حکومتی است. مصلحت انواع گوناگونی دارد (فاطمی، نوابی، عبدالهی‌نژاد، ۱۴۰۱):

۱. مصالح ضروری: مصالح ضروری مصالحی است که مقصود اصلی شرعیت حفظ آنها است که عبارتند از: حفظ دین، نفس، عقل و مال انسانها. این مصالح از آن جهت ضروری‌اند که حیات بشری و سعاد دنیوی و اخروی انسان در گرو وجود آنها است، به‌گونه‌ای که فقدان آنها موجب اختلال در نظام زندگی انسانی می‌گردد. لذا حفظ این مصالح بر همه چیز مقدم است.

۲. مصالح حقیقی: مصالح حقیقی در برابر مصالح وهمی می‌آید و آن در جایی است که یک کار به طو حقیقی جلب منفعت یا دفع ضرر نماید و تشریع حکم طبق آنها به مصلحت و نفع شخص و یا جامعه باشد. مانند الزام به ثبت رسمی معاملات مربوط به زمین در اداره ثبت و اسناد که باعث کاهش دعاوی مربوط به زمین می‌گردد و نوعی امنیت و ثبات در معاملات ایجاد می‌کند.

۳. مصالح شخصی (مصالح فردی): مصالح شخصی در برابر مصالح عام قرار دارد و عبارت است از مصالح مربوط به افراد یا گروه‌های خاص در برابر مصالح مربوط به عموم یا بیشتر افراد جامعه. در مصالح مرسله[۱] آنچه واجب است رعایت مصالح عموم است و در تعارض میان مصلحت اشخاص و مصلحت عموم، مصلحت اشخاص نادیده گرفته می‌شود مانند اینکه اگر خانه شخصی در مسیر خیابانی که برای عموم مردم شهر لازم است قرار گیرد، مصالح جامعه مقدم می‌گردد و منزل وی تخریب می‌شود.

۴. مصالح تحسینی: مصالح تحسینی نوعی از مصالح هستند که رعایت آنها، بهبود و بهتر شدن زندگی را در پی دارد ولی عدم رعایت آنها باعث سختی و دشواری در زندگی انسان نمی‌شود، مانند به دست کردن انگشتر و استعمال بوی خوش، که نه وجود آنها برای زندگی انسانها ضرورت دارند و نه سب رفع مشقت و حرج می‌گردند (فاطمی، نوابی، عبدالهی‌نژاد، ۱۴۰۱).

منابع تشخیص مصلحت شامل کتاب، سنت، عقل و اجماع است و منابع عمده تشخصیص آن شامل شرع، عقل، علم، تجربه و عرف است. استنباط مصلحت در فقط شیعی به سه صورت انجام می‌شود. اول، گاهی مصلحت موضوع حکم شرعی است که با از بین رفتن مصلحت، حکم آن هم منتفی می‌شود و هرگاه دوباره آن مصلحت محقق شود حکم آن نیز فعلیت می‌یابد. دوم، در فقه شیعی حاکم اسلامی می‌توند بر اساس مصالحه، حکمی ولایی برخلاف حکم ثابت یک موضوع جعل کند اما این حکم حکومتی به هیچ‌وجه حکم ثابت آنرا تغییر نمی‌دهد. به‌عبارت دیگر، در فقه شیعه مصلحت یکی از مصادر حکم حکومتی است نه حکم شرعی. سوم، بسیای از موارد تعارض احکام شرعی (تکلیفی یا وضعی) با احکام حکومتی، از باب تزاحم در مقام احرا و امتثال است. در این موارد حکم حاکم مشروع بر اساس مصلحت و یا بر اساس اولویت دادن به مصلحت برتر یا اهم، تعیین‌کننده امتثال حکم یک طرف تزاحم میان مصلحت انجام امر واجب خواهد شد. در حکم تعطیلی انجام امر واجب حج در صورت ترتب انجام آن بر تضعیف نظام اسلامی، ممکن است امر واجب حج با مصلحت حفظ اقتدار و تمامیت نظام اسلامی، تعطیل شود. اما در این‌صورت، نه هیچ یک از مصالح فوق تغییر کرده است و حکم حاکم نیز به تغییر حکم اولی شرعی وجوب تعلق نگرفته است (فاطمی، نوابی، عبدالهی‌نژاد، ۱۴۰۱: ص.۶۳۹۳).

دانش‌پور (۱۳۹۵) در بحث از اهتمام شریعت به مصلح جمعی در حریم خصوصی، اعتقاد دارد که در فقه شیعه با طرح ابوابی مانند «مصلحت اجتماعی»، «مصلحت حکومتی» و «مصلحت نظام»، به موضوع ترجیح مصالح احتماعی و عمومی بر مصالح فردی و خصوصی که مبتنی بر مبانی شرعی و عقلی است، توجه شده است. به طور خاص، درباره حریم شخصی

[۱]. مصالح مرسله مصالحی است که شارع آن مصالح را معتبر دانسته است.

افراد، با وجود حمایت همه‌جانبه اسلام از این حوزه، مواردی از این مصلحت‌سنجی در تلاقی با مصالح عامه و حقوق جمعی در تزاحم قرار می‌گیرد و تعیین مرزهای صحیح قانونی بین آنها اهمیت حیاتی دارد و بنابراین در صورت به خطر افتادن منافع و کیان جامعه باید به شکل دیگری عمل کرد. وی سپس برخی از مصادیق تقدم مصالح اجتماعی بر مصلحت فردی و مهمترین موارد جواز نقض حریم خصوصی را برمی‌شمرد. اول تقدم مصلحت جمعی بر اصل رازداری است که مصادیق متعددی دارد. ازجمله ۱) ارتکاب جرایم علیه امنیت. در مواردی که عدم افشاء اطلاعات فرد موجب لطمه یا زیان اساسی به سلامت جان و بقاء افراد دیگر و جامعه می‌شود، نمی‌توان با استناد به آزادی‌های فردی و ضرورت حفظ حریم شخصی او در زمینه اطلاعات حقوق جمع را تضییع کرد. در مواردی همانند ارتباط غیرمجاز با بیگانگان، جاسوسی، آدم‌ربایی، آلوده کردن منابع آب، سرقت و غیره، شنود مکالمات یا کنترل رفت‌وآمد توسط حکومت به‌مثابه نقض حریم شخصی تلقی نمی‌شود. بنابراین، در تزاحم میان حریم خصوصی و امنیت، غالباً و یا در بیشتر اوقات امنیت در اولویت قرار می‌گیرد. بحث دیگر، حفظ بهداشت عمومی است. گرچه در پزشکی، اصل بر حفظ اطلاعات خصوصی بیمار و عدم دسترسی همگانی به آن است اما گاهی میان این حق و منافع و مصالح اجتماعی تزاحم ایجاد می‌شود و برای پیشرفت علمی، حمایت از بهداشت عمومی و دیگر اهداف اجتماعی، ضرورت پیدا می‌کند که افراد از حق شخصی خود بر اطلاعات محرمانه پزشکی گذشت کنند. به‌ویژه در مورد بیماری‌های واگیردار و خطرناک، تا حد امکان ضمن حفظ حریم خصوصی فرد، باید سلامت و امنیت اجتماعی در اولویت قرار بگیرد. مورد سوم، پیگری و کشف جرایم است. تزاحم حق خلوت با مصالح و منافع مربوط به پیگری کشف جرم، در این بحث قابل طرح است. هم جامعه حق دارد از وقوع جرایم مطلع شود و هم اینکه سوابق مربوط به اتهامات و محکومیت افراد دارای جنبه خصوصی است. بحث چهارم حقوق کار است که طی آن کارفرمایان به هنگام دسترسی به اطلاعات درباره کارگران باید از افشای اطلاعات مربوط به آنها خودداری کنند و نیز صاحبان برخی حرفه‌ها همانند وکلا و نیز روان‌شناسان باید رازدار باشند اما گاهی اوقات آنها به اطلاعاتی دسترسی پیدا می‌کنند که با امور مهم اجتماعی مرتبط است و مصالح اجتماعی ایجاب می‌کند که بخش‌های خاصی از جامعه از آن آگاه شوند. یک بحث اساسی دیگر، تقدم مصلحت جمعی بر اصول ممنوعیت تجسس و غیبت است. گاهی استثناءپذیری حریم خصوصی تا اصل ممنوعیت تجسس را هم شامل می‌شود. ازجمله می‌توان به مواردی همانند آگاهی حاکمان اسلامی و قضات، تحقیق و تفحص در امر ازدواج،

تجسس از کودکان و نوجوان و جوان توسط ولی امر، تجسس بر پایه انگیزه و غرض شرعی و عقلایی صحیح و تجسس در ادای تکلیف واجب اشاره کرد که در تمام آنها مصلحت جمعی بر مصلحت فردی اولویت دارد.

-قاعده حفظ نظام و مصلحت و ورود به حریم خصوصی

در راستای بررسی رابطه مصلحت و حریم خصوصی، کشتگر و جاور (۱۴۰۰) تأثیر قاعده فقهی «حفظ نظام» بر حق حریم خصوصی را واکاوی کرده‌اند. به گفته آنها در شرایط معمول و در شرایط غیراستثنایی همانند اضطرار، حوزه زندگی خصوصی افراد باید محترم شمرده شود و از تعرض مصون بماند. قاعده حفظ نظام را می‌توان برای تدوین الزامات حقوقی مرتبط با حق حریم شهروندان به کار برد. قاعده حفظ نظام به شکل یک طیف است که بسته به مقوله آن دارای شدت و ضعف است. هرقدر نظمی که درصدد حمایت از آن هستیم قوی‌تر باشد، احکام مربوط از قوت بیشتری برخوردار است. زمانی که یک مصلحت عمومی قوی‌تر با حریم خصوصی افراد در تزاحم قرار گیرد، حفظ نظام برتر مبنایی برای تحدید حریم خصوصی افراد است. بر این اساس، حفظ نظام در سه ساخت ملاک تعیین ضوابط و احکام مرتبط با حریم خصوصی است. نخست، ساخت شناسایی حق حریم خصوصی است که طبق آن مبنای حفظنظام هرگونه مداخله (اعم از اطلاع یا انتشار) در امور محرمانه و پنهانی افراد که باعث شود سامان زندگی و حیات مردم مخدوش شود ممنوع است. دوم، تحدید حریم خصوصی است که مبتنی بر قاعده حفظ نظام چنانچه مصلحت عمومی قوی‌تر با حق حریم خصوصی افراد در تزاحم قرار گیرد، حفظ نظام برتر، مبنایی برای تحدید حریم خصوصی افراد محسوب می‌شود. سوم، ساخت تحدید نسبی حریم خصوصی که مبتنی بر قاعده حفظ نظام، مبادرت به دخالت بیش از میزان ضرورت مجاز نیست.

در توضیح بیشتر باید گفت ازآنجا که تحصیل محتوای محرمانه زندگی افراد و اشاعه و انتشار اطلاعات خصوصی آنها سبب مخدوش شدن امنیت روانی انسانها می‌شود و موجب تزلزل روابط اجتماعی می‌شود، مداخله خودسرانه در حوزه زندگی خصوصی افراد با مفاد قاعده حفظ نظام در تعارض است. به عبارت دیگر، مداخله خودسرانه در حریم خصوصی افراد و انتشار اطلاعات محرمانه زندگی آنها که می‌تواند مقدمه‌ای برای زائل ساختن نظم عمومی، اخلاقی و فرهنگی شود، حرام است (کشتگر و جاور، ۱۴۰۰).

بحث بعد شرایط تحدید حق حریم خصوصی در پرتو قاعده حفظ نظام است. امکان تقیید حریم خصوصی دارای شرایطی است و از برخی مصالح عمومی و ملاحظات عقلی تبعیت می‌کند. در تعارض میان مصلحت فردی و مصلحت اجتماعی، حکومت موظف است تا مصالح عمومی را بر مصالح افراد مقدم بدارد که قاعده فقهی تقدیم اهم بر مهم مبنای آن است. همچنین برخی معتقدند که محدوده ممنوعیت تحریم حریم خصوصی فقط اسرار، عیوب و لغزش‌های شخصی و خانوادگی است که با مصالح عمومی هیچ ارتباطی ندارد اما مسائل و اموری که به مصالح عمومی جامعه و حفظ نظام مسلمین بستگی دارد، به ناچار باید مورد بازرسی و مراقبت قرار گیرد. به‌طوری که باید تحرکات دولتها و ملت‌های بیگانه و ایادی آنها مورد رصد قرار بگیرد و لازم است مصالح عمومی کشور و مردم بر آزادی‌های فردی ترجیح داده شود. اما در حدود نقض حریم خصوصی باید به برخی امور ازجمله اکتفا به قدر ضرورت در نض حریم خصوصی، لزوم رعایت نسبیت در نشر، ارزش اثبانی نداشتن دلایل ناشی از نقض بلاوجه و ممنوعیت نشر داده‌های حساس و مرتبط با امور عفافی توجه شود. بر اساس اصل اول، مبادرت به دخالت بیش از حد ضرورت جایز نیست و بر اساس قاعده فقهی الضرورات تقدر بقدرها تنها تا رفع حالت ضرورت و به تناسب خطر و تهدید انجام فعل اضطراری مجاز است. لزوم رعایت نسبیت در نشر به این معنا است که جواز نشر داده‌های شخصی، در موارد مجاز، باید صورت محدود باشد و شرایط مکانی، زمانی و موضوع عمل و نظایر آن مد نظر قرار گیرد. در بحث ارزش اثباتی نداشتن دلایل ناشی از نقض بلاوجه باید گفت صرف آگاهی اشخاص از حرمت منزل و ممنوعیت تجسس از محلهای خصوصی و منع انتشار داده‌های حساس کافی نیست و باید با تدابیری انگیزه ارتکاب به این اعمال از بین برود و بنابراین، به طور مثال، اطلاعاتی که از طریق غیرمشروع حاصل شده باشد، در محاکم فاقد ارزش تلقی شود. نکته آخر ممنوعیت نشر داده‌های حساس و مرتبط با امور منافی است. انتشار داده‌های مرتبط با امور عفاف حتی اگر به شکل قانونی تحصیل شده باشد یا فرد به دلخواه آنها را در معرض انتشار قرار داده باشد، مجاز نیست و صرف دسترسی آشکار یا حتی مجاز به این نوع داده‌ها با جواز نشر آنها ملازمه ندارد. زیرا انتشار این نوع داده‌ها با نظم فرهنگی جامعه در تعارض است. (کشتگر و جاور، ۱۴۰۰).

حریم خصوصی پس از انقلاب اسلامی

به طور کلی پیروزی انقلاب اسلامی سبب ایجاد یک حکومت مبتنی بر اصول دینی شد. با گذر زمان و پس از تصویب قوانین گوناگون مبتنی بر آموزه‌های دین اسلام، بحث‌های مرتبط با حقوق شهروندان ازجمله حریم خصوصی نیز مورد توجه قرار گرفت. همانطور که رجایی و فکری (۱۳۹۰) بحث کرده‌اند، انقلاب اسلامی با پیروزی خود ساختارها، ارزش‌ها و تعاریف جدیدی از موضوعات و مفاهیم عرضه کرد. یکی از این موضوعات مهم مفهوم آزادی و حقوق بشر به طور اعم و حریم خصوصی و عمومی شهروندان به طور خاص بود.

-فرمان هشت ماده‌ای امام خمینی

همانطور که فکری (۱۳۹۷) نوشته است، نظر امام خمینی درباره حریم خصوصی را باید به عنوان نظر یک فقیه بررسی کرد، نه فیلسوفی سیاسی یا اندیشمندی اجتماعی. فیلسوفان و اندیشمندان سیاسی ـ اجتماعی با مبانی فکری خاصی که برگرفته از جریان تاریخی و اندیشه‌ای تاریخ غرب است، به موضوع حقوق انسانها پرداخته‌اند و امام خمینی(ره) در مقام فقیهی سیاسی که معتقد و مقید به دین اسلام است، با مبانی فکری و اعتقادی اسلام به موضوعات و مباحث نگریسته است. به دلیل جایگاه رهبری امام، نظر و عمل ایشان در باب حقوق و آزادیهای فردی به هم پیوند خورده است؛ یعنی ایشان زمانی که قیام را شروع کردند، به بیان نظراتشان درباره حقوق و آزادیهای فردی هم پرداختند و پس از پیروزی انقلاب اسلامی نیز که در جایگاه رهبر دینی و سیاسی جامعه قرار گرفتند، از موضع رهبری با صدور فرمانها و دستوراتی از جمله فرمان هشت ماده‌ای سعی در عملی کردن اندیشه‌های اسلامی در جامعه داشتند.

پس از پیروزی انقلاب اسلامی، امام خمینی به عنوان رهبر انقلاب مصاحبه‌ها و سخنرانی‌های خود بارها به موضوعات آزادی و حریم خصوصی اشاره کرده‌اند. امام خمینی(ره) معتقد بودند پس از انقلاب اسلامی، یکی از تحولات اساسی، اعتقاد به این امر است که مردم دارای حق هستند و حکومت وظیفه دارد این حق را رعایت کند و حرمت آن را نگه دارد. بر همین اساس از مهمترین توصیه‌های امام در دیدارهای مکرری که با مردم و مسئولان داشتند، توجه به حقوق مردم و عدم تجاوز به آن و جلوگیری از وارد شدن ظلم به افراد جامعه است (فکری، ۱۳۹۷)

و به طور کل در اندیشه و سیره ایشان موضوع حریم عمومی و خصوصی شهروندان جایگاه مهمی‌داشته است، فرمان هشت ماده‌ای که ایشان در سال ۱۳۶۱ خطاب به مسئولین اجرایی و قضایی صادر فرمودند صریح‌ترین دیدگاه ایشان در خصوص موازین این موضوع حیاتی برای جامعه و عموم مردم است (رجایی و فکری، ۱۳۹۰).

از نظر امام حریم خصوصی زندگی افراد دربرگیرنده حوزه‌های مختلفی است که برخی از آنها عارتست از:

-حوزه اعتقادات (آزادی عقیده)

-آزادی بیان و قلم

-آزادی در محل سکونت و کار (به نقل از فکری، ۱۳۹۷).

حریم اندیشه و حریم مکانی برای امام خمینی اهمیت والایی داشته است و هرگونه تفتیش عقیده و نیز نقض محل سکونت که متمایزکننده حریم خصوصی از حوزه عمومی مورد تأکید قرار دارد. بر این اساس، خانه اهمیت بسیاری دارد و هرگونه تعرض به آن ممنوع است و ساکنان خانه دارای آزادی مطلق هستند و جز برخی استثناءها هر فرد و یا حکومتی حق تعرض به آن را ندارد.

-حق حریم خصوصی به مثابه حق بنیادین در حکومت اسلامی از منظر امام خمینی

فرمان ۸ ماده ای امام خمینی برای تامین امنیت اجتماعی و قضایی در ۲۴ آذر ۱۳۶۱ در روزنامه کیهان منتشر شد. رهبر انقلاب در این فرمان بر رعایت قانون و حقوق مردم در تمام شئون فردی و اجتماعی تأکید کردند. یکی از این حقوق، حق حریم خصوصی است و اشاره به آن بیانگر اهمیت این حق بنیادین در حکومت اسلامی است. ماده ششم این فرمان به حریم خصوصی اختصاص دارد:

هیچ کس حق ندارد به خانه یا مغازه و یا محل کار شخصی کسی بدون اذن صاحب آنها وارد شود یا کسی را جلب کند، یا به نام کشف جرم یا ارتکاب گناه تعقیب و مراقبت نماید، و یا نسبت به فردی اهانت نموده و اعمال غیرانسانی – اسلامی مرتکب شود، یا به تلفن یا نوار ضبط صوت دیگری به نام کشف جرم یا کشف مرکز گناه گوش کند، و یا برای کشف گناه و جرم هر چند گناه بزرگ باشد، شنود بگذارد و یا دنبال اسرار مردم باشد، و تجسس از گناهان غیر نماید یا اسراری که از غیر به او رسیده ولو برای یک نفر فاش کند. تمام اینها جرم (و) گناه است و بعضی از آنها چون اشاعه‌ی فحشا و گناهان از کبایر بسیار بزرگ است، و مرتکبین هر یک از امور فوق مجرم و مستحق تعزیر شرعی هستند و بعضی از آنها موجب حد شرعی می‌باشد (امام خمینی، ۱۳۶۱).

–امنیت عمومی به‌مثابه تنها جواز نقض حریم خصوصی افراد

امام خمینی، چند ممنوعیت دیگر را ذکر است. ازجمله در ماده چهار این فرمان هشت ماده‌ای، ممنوعیت توقیف یا احضار افراد بدون حکم قاضی، در ماده پنج بر ممنوعیت دخل و تصرف در مال افراد بدون حکم حاکم شرع نیز مورد تأکید قرار دارد. اما در ماده هفت عنوان می‌کند که این ممنوعیت‌ها در «رابطه با توطئه‌ها و گروهک‌های مخالف اسلام و نظام جمهوری اسلامی است که در خانه‌های امن و تیمی برای براندازی نظام جمهوری اسلامی و ترور شخصیت‌های مجاهد و مردم بیگناه کوچه و بازار و برای نقشه‌های خرابکاری و افساد فی‌الارض اجتماع می‌کنند و محارب خدا و رسول می‌باشند» صدق نمی‌کند. اما در ادامه تأکید می‌نماید که «در عین حال مأمورین باید خارج از حدود مأموریت که آن هم منحصر است به محدوده سرکوبی آنان حسب ضوابط مقرره و جهت شرعیه، عملی انجام ندهند. و موکداً تذکر داده می‌شود که اگر برای کشف خانه‌های تیمی و مراکز جاسوسی و افساد علیه نظام جمهوری اسلامی از روی خطا و اشتباه به منزل شخصی یا محل کار کسی وارد شدند و در آنجا با آلات لهو یا آلات قمار و فحشا و سایر جهات انحرافی مثل مواد مخدره برخورد کردند، حق ندارند آن را پیش دیگران افشا کنند، چرا که اشاعه‌ی فحشا از بزرگترین گناهان کبیره است و هیچ کس حق ندارد هتک حرمت مسلمان و تعدی از ضوابط شرعیه نماید» (امام خمینی، ۱۳۶۱).

نکته اخیر به خوبی اهمیت حفظ حریم خصوصی به‌ویژه حریم مکانی را در نظام اسلامی متذکر می‌شود. اینکه باید حرمت افراد حتی اگر مجرم باشند حفظ شود. به نظر می‌رسد در این فرمان حریم خصوصی اطلاعاتی و مکانی مورد تأکید قرار گرفته است. موضوع دیگر، امکان ورود به حریم خصوصی افراد است که به طور مطلق منوط به کسب مجوز قضایی است و به عبارت دیگر، هرگونه دخل و تصرف در حریم اطلاعاتی و مکانی افراد باید مبنای قانونی داشته باشد.

در کل امام خمینی در سخنرانی‌ها و فرمان‌هایشان توجه ویژه‌ای به حفظ شأنیت انسان‌ها و احترام به حریم خصوصی شهروندان داشته‌اند و فرمان تاریخی هشت ماده‌ای ایشان از مهم‌ترین مصادیق توجه ایشان به حریم خصوصی و حقوق شهروندی افراد است، به عقیده ایشان فقط چنانچه در حریم خصوصی افراد توطئه‌ای علیه اسلام، نظام و جان مردم درحال شکل‌گیری بود به شرط اطمینان بایست مانع از آن شد؛ آن هم نه توسط هر شخصی بلکه فقط توسط مقامات مسئول و فقط با حکم قضایی، در غیر این‌صورت کسی نمی‌تواند در حریم خصوصی افراد مداخله کند. همچنین نکتهٔ مهم در تحلیل نظرات امام این است که ایشان شرط دخالت در حریم خصوصی افراد را اطمینان و حصول یقین از اینکه در خفا عملی

خلاف مصلحت و امنیت نظام یا فسادی آشکار در حال انجام است، می‌دانند و تجاوز به حریم خصوصی افراد را تنها بر مبنای شک و تردید باطل می‌دانند. در صورتی هم که مردم از وجود فساد و توطئه در مکانی مطمئن شدند در این صورت هم تنها مقامات قضایی با صدور مجوزهای قانونی لازم می‌توانند به حریم خصوصی افراد وارد شوند و جلوی فساد و توطئه را بگیرند (رجایی و فکری، ۱۳۹۰: ص.۹۹).

به گفته مهریزی (۱۳۷۸) یکی از شاخصه های مهم (رهبر دینی) اصرار او بر امن بودنِ حریم خصوصی افراد است. با همین ملاک و شاخصه است که می توان میزانِ اسلامیِ بودنِ یک پیشوا را سنجید. امام خمینی(ره) که توانست در تمامی عرصه ها با معیارهای اسلامی مشی کند در این وادی نیز با قوّت و در حساسیّتِ مثال زدنی وارد شد و حریم خصوصی مردم را پیامبرانه پاس داری کرد و همه مسئولان را به رعایت آن فرمان داد.

بر اساس مفاد فرمان امام می‌توان استدلال کرد که چند اقدام در مکتب اسلام حرام است و همه مذاهب در مورد آن اتفاق نظر دارند که عبارتند از:

۱- تصرف در ملک دیگری و حریم او بدون رضایت مالک و صاحب حریم؛

۲-سلب آزادی و حقوق فردی همانند احضار، توقیف و حبسِ

۳. تجسس و جست‌وجو برای یافتن گناهان و لغزش‌های دیگران

۴. اشاعه فحشاء، انتشار گناهان و اسرار و لغزش‌های دیگران

در کل، مهریزی با ملاحظه آیات و روایات و نیز سنت ائمه و ملاحظه فرمان امام خمینی نتیجه می‌گیرد که حریم خصوصی شهروندان در دولت اسلامی مصمون است و هیچکدام از شهروندان و دولت‌مردان حق نقض آنرا ندارد و دو استثناء می‌توان ذکر کرد که اولی شامل تزاحم حریم خصوصی با حقوق شهروندان دیگر است و دیگری تزاحم حریم خصوصی با مصالح عمومی (مهریزی، ۱۳۷۸).

بنابراین، تأکید بر حریم مکانی و اطلاعاتی و نیز استثناء مصالح عمومی و حفظ امنیت ملی از مهمترین مفاد فرمان هشت‌ماده‌ای امام خمینی است.

علاوه بر این امام خمینی در حکمی که خطاب به ستاد پیگیری تخلفات قضایی و اداری (فرمان هشت ماده ای) در تاریخ ۱۵ دی ۱۳۶۱ با موضوع انحلال هیأتهای گزینش در سراسر کشور، و تأسیس هیأتهای دارای صلاحیت صادر کردند، فرموده‌اند:

۵. تجسس از احوال اشخاص در غیر مفسدین و گروههای خرابکار مطلقاً ممنوع است، و سؤال از افراد به اینکه چند معصیت نمودی، چنانچه بنا به بعضی گزارشات این نحوه سؤالات می شود، مخالف اسلام وتجسس کننده، معصیت‌کار است. باید در گزینش افراد این نحوه امور خلاف اخلاق اسلامی و خلاف شرع مطهر ممنوع شود (امام خمینی، ۱۳۶۱؛ صحیفه امام، ۱۴۰۳: ص.۲۱۹).

-حریم خصوصی در اندیشه رهبر انقلاب اسلامی

-ضرورت حفظ حریم خصوصی در پیام‌رسان‌ها از منظر رهبر انقلاب

رهبر انقلاب اسلامی در مناسب‌ها و به شکل‌های گوناگون بر اهمیت حفظ حریم خصوصی تأکید کرده‌اند. شاید مهمترین آن تأکید بر حفظ حریم خصوصی در پیام‌رسان‌ها باشد که بازتاب فراوانی پیدا کرد. در خصوص لزوم حفظ حریم شخصی شهروندان در پیام رسان‌ها، رهبر معظم انقلاب اسلامی در دیدار با جمعی از مدیران نظام فرموده‌اند که «مسئولان باید امنیت و حریم داخلی مردم و کشور را حفظ کنند؛ تعرض به امنیت و حریم داخلی مردم حرام شرعی است و نباید انجام شود».

بنابراین، این سخن رهبر انقلاب که طی آن نقض حریم خصوصی کاربران در پیام‌رسان‌های داخلی را حرام شرعی خوانده‌اند، بیانگر اراده حکومت و رهبری برای عدم دسترسی به اطلاعات مردم است.

همچنین ایشان در حکم انتصاب اعضای شورای عالی فضای مجازی در سال ۱۳۹۶، بر «اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبه فضای مجازی کشور و نیز حفظ حریم خصوصی آحاد جامعه و مقابله مؤثر با نفوذ و دست‌اندازی بیگانگان در این عرصه» تأکیده کرده‌اند (خامنه‌ای، ۱۳۹۴).

بخشی از توجه ایشان به حریم خصوصی را می‌توان از استفتائات صورت گرفته از ایشان نیز مشاهده کرد. ایشان در پاسخ به پرسشی در زمینه تجسّس در امور شخصی و غیر شخصی کارمندان می‌فرمایند «تجسس در کار دیگران و یا تحقیق در اعمال و رفتار کارمندان برای کشف اسرار آنان در خارج از حدود و ضوابط قانونی برای آن مأموران هم جایز نیست».

همچنین ایشان درخصوص تجسس در امور خصوصی دیگران و تفاوت آن بین فضای واقعی و مجازی این‌چنین پاسخ داده‌اند: «تجسس در امور شخصی و خصوصی دیگران چه در فضای حقیقی و چه در فضای مجازی جایز نیست» (خامنه‌ای، ۱۴۰۲).

به طور کلی، اگرچه رهبر انقلاب کمتر درباره حریم خصوصی سخن گفته‌اند، اما ممنوعیت تجسس و نیز لزوم حمایت و صیانت از داده‌های کاربران در پیام‌رسان‌های اجتماعی و عدم نقض حریم خصوصی کاربران در فضای مجازی مورد تأکید ایشان قرار دارد.

حریم خصوصی در قوانین ایران

-عدم حمایت صریح از حریم خصوصی در قانون اساسی

در نظام حقوقی ایران، حریم خصوصی به صورت مشخص و حمایت نشده و در واقع، موضع حقوق موضوعه ایران در مواجهه با حریم خصوصی، تحویل گرایانه است. حقوق و آزادی ها به منزله حریم خصوصی به طور ضمنی و در میان سایر قواعد حقوقی، به طور ناقص، مورد حمایت قرار گرفته اند. قانون اساسی، قانون مجازات اسلامی، قانون آیین دادرسی کیفری، قانون آزادی اطلاعات، قوانین و مقررات مربوطه به ارتباطات پستی، تلفنی و قانون مطبوعات در زمره قوانین و مقرراتی هستند که گاه ضمنی و گاه صریحاً از برخی مصادیق حریم خصوصی حمایت کرده اند. البته برخلاف قوانین اساسی کشورهایی که از حریم خصوصی به صورت مشخص و در قالب اصل یا اصول خاصی حمایت کرده اند، در قانون اساسی ایران متن خاصی که از حریم خصوصی، تحت این عنوان حمایت کرده باشد، وجود ندارد (واعظی و علیپور، ۱۳۸۹).

تا حدود یک دهه پیش، قوانین و مقررات روشنی در حمایت از حریم خصوصی اطلاعات و ارتباطات در نظام حقوقی ایران وجود نداشت. پس از ورود برخی فناوری‌های نو و سوءاستفاده از آنها برای افشای امور خصوصی و هتک حرمت افراد برخی قوانین و مقررات در این خصوص به تصویب رسید. در قوانین ایران از تعابیر مختلفی برای حریم خصوصی اطلاعات و ارتباطات استفاده می‌شود که از جمله آنها می‌توان به «اسرار شخصی» در قانون مطبوعات، «اسرار مردم» در قانون مجازات اسلامی، «داده‌های شخصی» و «حریم خصوصی» در قانون آزادی اطلاعات، «صوت و تصویر یا فیلم خصوصی یا

خانوادگی یا اسرار دیگری» در قانون جرایم رایانه‌ای و نیز عبارت «حریم خصوصی» در مصوبات شورای عالی انقلاب فرهنگی و مجمع تشخیص مصلحت نظام اشاره کرد (انصاری، ۱۴۰۱).

عدم وحدت رویه در کاربرد یک اصطلاح برای حریم خصوصی و حریم داده و ارتباطات، یکی از معضلات اساسی در تعریف دقیق مفاهیم است که، همانند بسیاری از موارد دیگر، به فهم نادرست آن منجر شده است. نگاه دینی و اخلاقی به حریم خصوصی در نزد عامه مردم و عدم اشاره صریح قانونی به آن از یکی از معضلاتی است که بحث حریم خصوصی در ایران با آن مواجه بوده است. بنابراین، ضرورت دارد حق حریم خصوصی به عنوان یک حق اساسی شهروندان به رسمیت شناخته شود تا حقوق و مسئولیت‌های ناشی از نقض آن آشکارا وجهی قانونی پیدا کند. بنابراین، مرور رویکرد قوانین ایران به حریم خصوصی چشم‌انداز روشنی از آن به دست می‌دهد.

-قانون اساسی

در قانون اساسی جمهوری اسلامی ایران اصطلاح حریم خصوصی ذکر نشده است. با اینهمه اگر همانطور که پیشتر اشاره شد، حفظ شأن و کرامت انسان را یکی از بنیان‌های اساسی بحث‌های حریم خصوصی در اسلام تلقی کنیم، در این‌صورت می‌توان حفظ کرامت انسان را به مثابه یک اصل پذیرفته شده در قانون اساسی مورد ملاحظه قرار دهیم که به طور ضمنی، حمایت از حریم خصوصی وی نیز مورد تأیید و تأکید در قانون اساسی است. چنانچه در بند ششم اصل دوم قانون اساسی «کرامت و ارزش والای انسان و آزادی توأم با مسئولیت او در برابر خدا» به عنوان یکی از مبانی جمهوری اسلامی بیان شده است. در بند ۱۴ اصل سوم قانون اساسی، «تأمین حقوق همه جانبه افراد از زن و مرد و ایجاد امنیت قضایی عادلانه برای همه و تساوی عموم در برابر قانون» یکی از شرایط دستیابی به کرامت انسان ذکر شده است. بنابراین، می‌توان استنباط کرد که حمایت از حریم خصوصی به‌مثابه یکی از پیش‌شرط‌های حفظ کرامت انسان ایرانی به رسمیت شناخته شده است.

-توجه به حریم خصوصی ارتباطات در قانون اساسی

مهمترین اصل قانون اساسی که تا حد زیادی به شکل مستقیم با حریم خصوصی در ارتباط دارد، اصل بیست و پنجم است. طبق این اصل «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون».

بر اساس بحث‌هایی که انجام شد، این اصل یک بعد از حریم خصوصی را دربرمی‌گیرد: حریم ارتباطات.

-لزوم قانون‌مند بودن ورود به حریم خصوصی از منظر قانون اساسی

در اصل بیست و دوم نیز می‌خوانیم، «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز کند». این اصل دربردارنده برخی از وجوه حریم خصوصی از جمله حریم مکانی، حریم جسمانی و نیز شأن و کرامت انسان و حریم شغلی است. یک نکته مهم دیگر اینکه، این اصل، آشکارا مجوز قانونی را تنها ملاک نقض حریم خصوصی افراد قلمداد می‌کند و صراحتاً هرنوع تجاوز به برخی از انواع حریم خصوصی شهروندان ایران را ممنوع می‌کند. علاوه بر این باید به اصل بیست و سوم اشاره کنیم که طبق آن، تفتیش عقاید ممنوع است و هیچ‌کس را نمی‌توان به صرف داشتن عقیده‌ای مورد تعرض و مؤاخذه قرار داد.

همچنین همانطور که انصاری (۱۴۰۰) گفته است، می‌توانیم به اصل صدوشصت‌وپنجم اشاره کنیم که طی افراد مجاز هستند برای ممانعت از افشای امور خصوصی خود از دادگاه درخواست کنند، محاکمه آنها به شکل غیرعلنی برگزار شود.

بنابراین درمجموع باید اذعان کرد که حریم خصوصی داده‌ها و اطلاعات شخصی به هیچ‌وجه در قانون اساسی مورد توجه قرار نگرفته است (احمدلو، ۱۴۰۰).

حریم خصوصی در قوانین و مقررات ایران

در این بخش، بر اساس سنت این پژوهش، به طور گذرا به مباحث مرتبط با حریم خصوصی در قوانین و مقررات ایران خواهیم پرداخت. زیرا این بحث‌ها به شکل مفصل در منابع گوناگون قابل مشاهده است. همچنین تمرکز اصلی بر حریم اطلاعات و ارتباطات خواهد بود.

-قانون مجازات اسلامی

-ممنوعیت نقض حریم خصوصی توسط کارکنان دولتی

در این قانون چند ماده به نحوی حریم خصوصی ارتباط دارد. در فصل دهم با عنوان در تقصیرات مقامات و مأمورین دولتی، در ماده ۵۷۰ می‌خوانیم:

هر یک از مقامات و مأمورین وابسته به نهادها و دستگاههای حکومتی‌که برخلاف قانون، آزادی شخصی افراد ملت را سلب کند یا آنان را از حقوق مقرر در قانون‌اساسی جمهوری اسلامی ایران محروم نماید علاوه بر انفصال از خدمت و محرومیت یک تا پنج سال از مشاغل حکومتی به حبس از دو ماه تا سه سال محکوم خواهد شد.

این ماده به طور کلی به سلب آزادی اشخاص توسط مقامات دولتی توجه کرده و در آن از حریم خصوصی سخن نگفته است. اما در ماده ۵۸۲ قانون مجازات اسلامی به صراحت بیان شده است:

«هر یک از مستخدمین و مامورین دولتی، مراسلات یا مخابرات یا مکالمات تلفنی اشخاص را در غیر مواردی که قانون اجازه داده حسب مورد مفتوح یا توقیف یا معدوم یا بازرسی یا ضبط یا استراق سمع نماید یا بدون اجازه صاحبان آنها مطالب آنها را افشاء نماید به حبس از یک سال تا سه سال و یا جزای نقدی از شش تا هیجده میلیون ریال محکوم خواهد شد».

آشکارا، این ماده با حریم ارتباطات سروکار دارد که در بیشتر مقررات ایران در مورد آنها بحث شده است. نکته مهم آن ممنوع کردن دسترسی غیرقانونی به محتوای ارتباطات شهروندان است. ماده‌های ۵۸۰، ۶۹۴ و نیز ۶۹۱ و ۶۹۲ نیز به نوعی مرتبط به نقض حریم مکانی هستند. به نظر می‌رسد از ماده ۶۶۹ این قانون موضوع حریم اطلاعات شخصی را استنباط کرد. این ماده ذیل فصل بیست و دوم، اکراه و تهدید، قرار دارد. طبق این ماده:

هر گاه کسی دیگری را به هر نحو تهدید به قتل یا ضررهای نفسی یا شرفی یا مالی و یا به افشاء سری نسبت به خود یا بستگان او نماید، اعم از اینکه به این واسطه تقاضای وجه یا مال یا تقاضای انجام امر یا ترک فعلی را نموده یا ننموده باشد به مجازات شلاق تا (۷۴) ضربه یا زندان از دوماه تا دو سال محکوم خواهد شد.

بر اساس این ماده قانون مجازات اسلامی، تهدید به افشای اطلاعات خصوصی شهروندان توسط فرد دیگر، می‌توان به مجازات منجر شود. البته، موضوع اصلی این ماده تهدید و تحت فشار قرار دادن غیرقانونی دیگران است و به طور مستقیم به مجازات نقض حریم شخصی دیگران نپرداخته است.

قانون آیین دادرسی کیفری

آیین دادرسی کیفری مجموعه مقررات و قواعدی است که برای کشف جرم، تعقیب متهم، تحقیقات مقدماتی، میانجیگری، صلح میان طرفین، نحوه رسیدگی، صدور رأی، طرق اعتراض به آراء، اجرای آراء، تعیین وظایف و اختیارات مقامات قضایی و ضابطان دادگستری و رعایت حقوق متهم، بزه‌دیده و جامعه وضع می‌شود (ماده ۱ قانون آیین دادرسی کیفری).

به گفته انصاری (۱۴۰۱) قانون آیین دادرسی کیفری که به قانون تضمین‌کننده حقوق و آزادی‌های تعیین‌شده مرسوم است، مهمترین قانون برای حمایت از حریم خصوصی است و با ملاحظه اجمالی برخی از مفاد این قانون می‌توان میزان حمایت واقعی آن از حریم خصوصی را دریافت. این قانون، قدرت حکومت و مأموران دولت در تعرض به حقوق و آزادی‌های فردی و اجتماعی را محدود می‌کند.

–ممنوعیت ورود به حریم خصوصی بدون حکم قانون

در این قانون، برخلاف قوانینی که تاکنون بررسی کردیم، به صراحت اصطلاح «حریم خصوصی» ذکر شده است. ماده ۴ قانون آیین دادرسی کیفری می‌گوید:

اصل، برائت است. هرگونه اقدام محدودکننده، سالب آزادی و ورود به حریم خصوصی اشخاص جز به حکم قانون و با رعایت مقررات و تحت نظارت مقام قضایی مجاز نیست و در هر صورت این اقدامات نباید به گونه‌ای اعمال شود که به کرامت و حیثیت اشخاص آسیب وارد کند.

از این ماده قانونی چنین استنباط می‌شود که اصل در حکومت اسلامی عدم ورود حکومت به حوزه حریم خصوصی و محدود کردن آزادی‌های شخصی در قلمرو حریم خصوصی است. همچنین در این قانون تأکید فراوانی بر قانونی بودن ورود به حریم خصوصی افراد شده است و تلاش شده است تا حد امکان ورود محدود و به طور کامل با رعایت ضوابط قانونی باشد. درنهایت، تصریح شده است که ورود به حریم خصوصی مطلقاً مجوزی برای خدشه وارد کردن به کرامت انسانی نیست. پیشتر نیز گفته شد که در قوانین اسلام اصل حفظ کرامت و تکرمی مقام انسان است و نقض حریم شخصی وی پیش از هرچیزی خدشه به حرمت و کرامت انسانی اوست.

ماده ۶۵۳ این قانون که به ارائه اطلاعات قضایی از درگاه ملی قوه قضائیه اختصاص دارد، پیش‌بینی کرده است که «آراء صادره از سوی محاکم درصورتی که به تشخیص قاضی اجرای احکام خلاف عفت عمومی یا امنیت ملی نباشد به صورت برخط (آنلاین) برای تحلیل و نقد صاحب‌نظران و متخصصان با حفظ حریم خصوصی اشخاص» (بند ت)، ارائه شود. در این ماده پیش‌بینی شده است که اطلاعات شخصی حقوقی مرتبط با افراد مورد صیانت قرار گیرد..

برخی از ماده‌های دیگر این قانون به صیانت از حریم خصوصی در دفاتر خدمات الکترونیک قضایی اختصاص دارد. بر اساس ماده ۶۵۸ این قانون، «قوه قضائیه موظف است تمهیدات فنی و قانونی لازم را برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان، در چهارچوب اقدامات این بخش فراهم آورد». در این ماده قانونی از امنیت داده‌های شخصی افراد سخن گفته شده است و از این منظر بدیع است. همچنین در ماده ۶۶۰ این قانون می‌خوانیم، «چنانچه اشخاصی که داده‌های موضوع این بخش را در اختیار دارند، موجبات نقض حریم خصوصی افراد یا محرمانگی اطلاعات را فراهم آورند یا به طور غیرمجاز آنها را افشاء کرده یا در دسترس اشخاص فاقد صلاحیت قرار دهند، به حبس از دو تا پنج سال یا جزای نقدی از بیست تا دویست میلیون ریال و انفصال از خدمت از دو تا ده سال محکوم خواهند شد».

اهمیت قانون آیین دادرسی کیفری از این جهت که برخلاف قوانینی که تاکنون بررسی کردیم، صراحتاً اصطلاح حریم خصوصی را به کار برده است و همچنین منظور از حریم خصوصی در آن حریم داده‌های شخصی یا حریم اطلاعاتی است. زیرا بیشتر قوانینی که تاکنون مورد توجه قرار گرفت، بر حریم اطلاعاتی تأکید داشتند. البته برخی ماده‌های دیگر هم به نحوی به حفظ حریم خصوصی مرتبط هستند–ماده ۹۶–که کمتر موضوع بحث ما است. اما در کل قانون آیین دادرسی کیفری از حیث توجه به حریم داده‌های شخصی در ایران استثناء است.

قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند

این قانون به طور کلی در اوایل دهه ۱۳۸۰ خورشیدی تصویب شده است. زمانی که هنوز آثار سینمایی و هنری در قالب سنتی سی.دی و دی.وی.دی عرضه می‌شدند و حتی استفاده از ابزارهای حافظه (فلش مموری) به شکل کنونی رایج نبود، چه برسد به قابلیت انتشار محتوا در فضای مجازی و پلتفرم‌های مختلف.

با این حال، برخی از مفاد آن به نحوی با حریم خصوصی در ارتباط هستند. همانطور که انصاری (۱۴۰۱) بحث کرده است، این قانون با هدف حمایت از آبرو و حیثیت افراد، ایجاد هرگونه اثر سمعی–بصری از دیگران را که زمینه اخاذی و تهدید را فراهم می‌کند، مستوجب مجازات دانسته است و بنابراین قلمرو خاص و محدودی ازحریم خصوصی را مورد حمایت قرار می‌دهد. دو ماده ۴ و ۵ این قانون به این موضوع ارتباط دارند.

–مجرمانه بودن توسل به اطلاعات شخصی برای تهدید دیگران

ماده ۴:

هرکس با سوءاستفاده از آثار مبتذل و مستهجن تهیه شده از دیگری، وی را تهدید به افشا و انتشار آثار مزبور نماید و از این طریق با وی زنا نماید به مجازات زنانی به عنف محکوم می‌شود ولی اگر عمل ارتکابی غیر از زنا و مشمول حد باشد حد مذبور بر وی جاری می‌گردد و در صورتی که مشمول تعزیر باشد به حداکثر مجازات تعزیری محکوم خواهد شد.

ماده ۵ نیز مرتکبان برخی از جرایم مرتبط را به دو تا پنج سال حبس و ده سال محرومیت از حقوق اجتماعی و هفتاد و چهار ضربه شلاق محکوم کرده است:

الف) وسیله تهدید قرار دادن آثار مستهجن به منظور سوءاستفاده جنسی، اخاذی، جلوگیری از احقاق حق یا هر منظور نامشروع و غیرقانونی دیگر.

ب) تهیه فیلم یا عکس از محل‌هایی که اختصاصی بانوان بوده و آنها فاقد پوشش مناسب می‌باشند مانند حمام‌ها و استخرها و یا تکثیر و توزیع آنها.

ج) تهیه مخفیانه فیلم یا عکس مبتذل از مراسم خانوادگی و اختصاصی دیگران و تکثیر و توزیع آن.

این مواد قانونی به طور خاص به زنان اختصاص دارد و بیشتر از حریم خصوصی نسبت به حریم جسمانی آنها تمرکز دارد. هرچند درنهایت این نوع محتواها به شکل داده شخصی قابل انتشار و اشتراک‌گذاری در فضای مجازی است و بنابراین می‌توان از بحث‌های مرتبط با حریم مکانی و جسمانی به حریم داده نیز گذار کرد.

قانون جرایم رایانه‌ای

قانون جرایم رایانه‌ای مصوب ۵ خرداد ۱۳۸۸ مجلس شورای اسلامی است و در تاریخ ۱۰ تیر ۱۳۸۸ توسط رییس جمهور وقت ابلاغ شده است. این قانون از این جهت که توجه به بحث داده‌ها و محرمانگی داده‌ها می‌کند، اهمیت بسیاری دارد. هرچند این قانونی زمانی نوشته شده است که کاربرد رایانه‌ها توسعه پیدا کرده است و مفهوم شبکه و نیز اینترنت و رسانه‌های اجتماعی در ایران در ابتدای راه بودند. با وجود این، می‌توان آنرا مبنایی برای نگارش قانونی مرتبط و به‌روز در این خصوص در نظر گرفت. ما از این قانون را صرفاً از منظر حریم داده‌ها (داده‌های شخصی) بررسی می‌کنیم.

فصل یکم این قانون–جرایم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی–شامل سه مبحث دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه‌ای است. در مفاد این مباحث به طور خاص به داده‌های شخصی توجه نشده است. آنچه مطرح شده، برای مثال در ماده ۱)، شامل «داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده» است. بنابراین، می‌توان استنباط کرد که هدف این قانون بیشتر فعالیت‌های نفوذگران و خرابکارانی است که به شبکه‌های ارتباطی و مخابراتی نفوذ می‌کنند است و نه حمایت از داده‌های شخصی.

–مجرمانه بودن نقض اطلاعات شخصی

ماده پنج این قانون نیز بر مسئولیت افراد متولی در حفاظت از داده‌ها و مجازات آنها در صورت اهمال در انجام وظیفه‌شان تأکید دارد:

چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سیستم‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سیستم‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سیستم‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

فصل پنجم قانون جرایم رایانه‌ای با عنوان هتک حیثیت و نشر اکاذیب با مباحث حریم خصوصی ارتباط بیشتری دارد. طبق ماده ۱۷ قانون مذکور:

هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

این قانون حمایت از حریم خصوصی را به حیثیت و اعتبار اشخاص پیوند زده است و افشای صوت، تصویر یا مسائل خصوصی افراد را تنها درصورتی‌که عرفاً موجب ضرر به افراد باشند مستوجب و موجود مسئولیت مدنی دانسته است. همچنین ماده مذکور افشای امور خصوصی یک فرد را چنانچه بدون رضایت او باشد، کافی برای تحقق نقض حریم خصوصی نمی‌داند، بلکه افشای بدون رضایت را که منجر به ضرر شود، منع می‌کند (انصاری، ۱۴۰۱: صص. ۱۷۴–۱۷۵).

قانون انتشار و دسترسی آزاد به اطلاعات

قانون انتشار و دسترسی آزاد به اطلاعات در ۶ بهمن ۱۳۸۷ در مجلس شورای اسلامی تصویب و در ۱۱ بهمن ۱۳۸۷ ابلاغ شده است. این قانون از برخی جهت برای پژوهش حاضر اهمیت دارد. در این قانون اطلاعات شخصی (و نه داده‌های شخصی) تعریف شده است–هرچند باید در نظر داشت که در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا نیز داده‌های شخصی به معنای «هر نوع اطلاعات» درنظر گرفته شده است تا به قدر کافی فراگیر باشد. بنابراین، داده اصطلاح جامع و دربردارنده اطلاعات است. در هرصورت در قانون انتشار، اطلاعات شخصی به این شکل تعریف شده است:

فصل اول: تعاریف و کلیات. بند اول: تعاریف. ب) 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.

بند سوم فصل اول به حق دسترسی به اطلاعات مرتبط است. در ماده ۶ آن می‌خوانیم:

درخواست دسترسی به اطلاعات شخصی تنها از اشخاص حقیقی که اطلاعات به آنها مربوط می گردد یا نماینده قانونی آنان پذیرفته می شود.

بنابراین صرفاً خود فرد می‌تواند به اطلاعات شخصی خود دسترسی پیدا کند و یا اینکه نماینده قانونی وی این اختیار را خواهد داشت. در این قانون اطلاعات مرتبط با حریم خصوصی به عنوان یکی از استثنائات حق دسترسی به اطلاعات بیان شده است. در بند دوم (حمایت از حریم خصوصی) از فصل چهارم که مربوط به استثنائات دسترسی به اطلاعات است، در ماده چهاردهم چنین آمده است:

چنانچه اطلاعات درخواست شده مربوط به حریم خصوصی اشخاص باشد و یا در زمره اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود.

بنابراین، در کل اسناد طبقه‌بندی‌شده دولتی، اطلاعات مرتبط به حریم خصوصی تنها استثنائات دسترسی به حریم خصوصی هستند. دسترسی به این اطلاعات تنها برای افراد خاص مجاز است. در ماده ۱۵ آمده است:

ماده۱۵- مؤسسات مشمول این قانون درصورتی که پذیرش درخواست متقاضی متضمن افشای غیرقانونی اطلاعات شخصی درباره یک شخص حقیقی ثالث باشد باید از در اختیار قرار دادن اطلاعات درخواست شده خودداری کنند، مگر آن که:

الف) شخص ثالث به نحو صریح و مکتوب به افشاء اطلاعات راجع به خود رضایت داده باشد.

ب) شخص متقاضی، ولی یا قیّم یا وکیل شخص ثالث، در حدود اختیارات خود باشد.

ج) متقاضی یکی از مؤسسات عمومی باشد و اطلاعات درخواست شده در چارچوب قانون مستقیماً به وظایف آن به عنوان یک مؤسسه عمومی مرتبط باشد.

قانون مدیریت داده‌ها و اطلاعات ملی

قانون مدیریت داده‌ها و اطلاعات علمی تاکنون مرتبط‌ترین قانونی است که برای مدیریت داده‌ها و اطلاعات در ایران تصویب شده است. این قانون در ۳۰ شهریور ۱۴۰۱ در مجلس شورای اسلامی تصویب و در تاریخ ۳ آبان ۱۴۰۱ توسط رئیس جمهور وقت–ابراهیم رئیسی–ابلاغ شده است.

براساس ماده۲ این قانون، «سیاستگذاری و تصویب راهبردهای کلان نظام تولید، نگهداری، پردازش، دسترسی، یکپارچه سازی، تبادل و امنیت داده‌ها و اطلاعات ملی با هدف افزایش قدرت حکمرانی، ساماندهی و انسجام‌بخشی به نظام تبادل داده‌ها و اطلاعات، گسترش تبادل اطلاعات میان دستگاهها و نهادهای مشمول این قانون و تسهیل دسترسی به اطلاعات پایه برای کسب وکارهای بخش خصوصی برعهده «شورایعالی فضای مجازی» است.

همچنین بر اساس ماده ۳ این قانون، «کارگروه تعامل پذیری دولت الکترونیکی» مصوب شورای عالی فضای مجازی موظف است در تصمیم‌گیری‌های خود به استثنای امر قضاء نسبت به اعمال سیاست‌ها و راهبردهای کلان و نظارت و مدیریت بر نحوه نگهداری، پردازش، دسترسی، یکپارچه‌سازی، امنیت و به‌ویژه تبادل و به‌اشتراک‌گذاری داده‌ها و اطلاعات موضوع این قانون اقدام نماید».

به جز تعیین مسئول و متولی تبادل داده‌ها در سطح ملی که شورای عالی فضای مجازی و نیز کارگروه تعامل‌پذیری دولت الکترونیکی است، در چند جای این قانون به اصل رعایت حریم داده‌ها توجه شده است. ازجمله در ماده۴ آن می‌خوانیم که «داده‌ها و اطلاعات ملی با لحاظ مسائل امنیتی و با رعایت محرمانگی اطلاعات اشخاص در اختیار دولت جمهوری اسلامی ایران است». در تبصره آن نیز ذکر شده که مکان دسترسی و تبادل داده ها و اطلاعات ملی صرفاً براساس سطوح دسترسی تعیین‌شده توسط کارگروه تعامل‌پذیری دولت الکترونیکی فراهم شود. فارغ توجهبه اصل محرمانگی و نیز تعیین سطح دسترسی، اما این نکته که اطلاعات اشخاص که در زمره داده‌های شخصی است، چگونه تحت مالکیت دولت قرار می‌گیرد، هرچند محرمانگی آن مراعات شود، محل اشکال است.

در ماده پنجم آن نیز صراحتاً بیان شده است که «دستگاهها و نهادهای مشمول این قانون که بر اساس شرح وظایف مقرر در قوانین مربوط و نیز تکالیف ناشی از این قانون موظف به تولید، نگهداری، پردازش داده‌ها و اطلاعات می‌باشند، مکلفند در امر تولید، نگهداری، پردازش، حفظ امنیت و صیانت از داده‌های شخصی و تبادل و اشتراک‌گذاری و تکمیل و به‌روزرسانی داده‌ها و اطلاعات ملی، سیاست‌ها و نظامات مصوب شورای عالی فضای مجازی و مصوبات کارگروه تعامل‌پذیری دولت الکترونیکی را اعمال و اجراء نمایند».

در ماده ششم قانون بار دیگر بر صیانت و محرمانگی داده‌ها تأکید شده است: «اعمال تدابیر حفاظتی و امنیتی جهت صیانت از داده‌ها و اطلاعات و حفظ محرمانگی داده‌ها و اطلاعات اشخاص برعهده دستگاهها و نهادهای مشمول این قانون و ارائه‌دهندگان خدمات ذیل تنظیم‌گران بخشی است که مسؤول تولید، نگهداری یا پردازش‌کننده داده ها و اطلاعات هستند». همانطور که در این ماده مشاهده می‌کنیم، دستگاه‌هایی که مسئولیت تولید و پردازش داده‌ها و اطلاعات را برعهده دارند، مکلفند نسبت به صیانت از داده‌ها نیز اقدام کنند (مرکز پژوهش‌های مجلس، ۱۴۰۱).

سند راهبردی جمهوری اسلامی ایران در فضای مجازی

مصوبه شورای عالی فضای مجازی کشور در خصوص «سند راهبردی جمهوری اسلامی ایران در فضای مجازی- اهداف و اقدامات کلان» در تاریخ ۸ شهریور ۱۴۰۱ توسط سید ابوالحسن فیروز آبادی، دبیر وقت شورای عالی فضای مجازی ابلاغ شد.

در این سند کلان، «صیانت از حریم خصوصی» به عنوان یکی از ارزشهای کلان جمهوری اسلامی ایران در فضای مجازی معرفی شده است. در چشم‌انداز این سند، صیانت از حقوق مردم-که حق حریم خصوصی نیز یکی از آنها به شمار می‌رود-به عنوان یکی از مبانی حکمرانی جمهوری اسلامی در بهره‌گیری از فضای مجازی بیان شده است. همچنین یکی از اقدامات کلان در این سند «محافظت از داده‌های ملی و اشتراک داده‌ها با حفظ حریم خصوصی» است.

آنچه مشخص است گرچه در این سند بر صیانت از حریم خصوصی تأکید شده است اما حمایت از داده‌ها به‌ویژه داده‌های شخصی در آن مورد غفلت واقع شده است. با این همه یکی از اقدامات کلانی که در این سند پیش‌بینی شده است و متولی

اصلی آن وزارت ارتباطات و فناوری اطلاعات است، طراحی نظام حکمرانی داده‌ها است که انبارش، پردازش، تبادل، اشتراک‌گذاری، بهره‌برداری، تنظیم‌گری، امنیت، مالکیت، حریم خصوصی، طبقه‌بندی داده‌ها و کلان‌داده‌ها را دربرمی‌گیرد.

دستورالعمل اجرایی حفاظت از حریم خصوصی کاربران

مسئله تأمین و حفاظت از امنیت داده‌های کاربران در فضای مجازی یکی از موضوعات مهم است که به‌ویژه پس از حمله‌های سایبری متعدد به سامانه‌های دولتی و پلتفرم‌ها در چند وقت اخیر بیشتر مورد توجه قرار گرفته است. هرچند در سال‌های اخیر حمله‌های سایبری یک داستان طولانی و ادامه‌دار بوده است، اما اقدام مؤثری جهت تقویت امنیت با هدف ارتقای سطح حفاظت از داده‌ها و اطلاعات کاربران در فضای مجازی انجام نشده است. پس از حمله سایبری به اسنپ‌فود و مسئله به خطر افتادن امنیت اطلاعات کاربران موضوع تقویت امنیت و سطح حفاظت برای مسئولین و نهادها جدی‌تر شده است (مهری، ۱۴۰۲).

-ضرورت اخذ رضایت کاربران برای تحلیل داده‌های آنها

یکی از اقدامات اخیر ابلاغ دستورالعمل حفاظت از حریم خصوصی کاربران است. دستورالعمل اجرایی «بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی» در کمیسیون عالی تنظیم مقررات فضای مجازی کشور (۱۱ دی ۱۴۰۲) تصویب شده است. هدف این دستورالعمل کاهش بخشی از مخاطرات مرتبط با نقض حریم خصوصی کاربران و نیز الزام اشخاص حقوقی غیردولتی و دستگاه‌های اجرایی کشور، به رعایت شرایط مرتبط با شیوه‌های جمع‌آوری، پردازش و نگهداری داده‌های کاربران در سامانه‌ها و سکوهای فضای مجازی است.

مفاد این دستورالعمل به شرح زیر است:

در راستای تقویت حفاظت از داده‌های کاربران، مرکز ملی فضای مجازی دستورالعمل‌های جدیدی را منتشر کرده است که الزام‌آورنده‌ی تمامی ارائه دهندگان خدمات آنلاین به افشای شفاف و واضح سیاست‌های حفظ حریم خصوصی و اخذ رضایت

صریح کاربران است. این دستورالعمل‌ها که بخش نخست از سند مادر سیاست‌ها و الزامات حفاظت از داده‌ها را تشکیل می‌دهند، هدفشان توانمندسازی کاربران برای کنترل بیشتر بر اطلاعات شخصی آن‌ها است.

فرصت اجرای دو ماهه با اعمال سختگیرانه

برای اجرای این دستورالعمل‌ها، سکوهای آنلاین از دو ماه مهلت برخوردار هستند. عدم رعایت مفاد تعیین شده در این بازه زمانی، منجر به تعلیق فعالیت آن‌ها خواهد شد. این دستورالعمل‌ها که به تصویب کمیسیون عالی تنظیم مقررات فضای مجازی رسیده است، بر شفافیت در شیوه‌های جمع‌آوری و استفاده از داده‌ها تأکید می‌کند.

دستورالعمل روشن برای جمع‌آوری، پردازش و نگهداری داده‌ها

این دستورالعمل چارچوبی جامع را برای مدیریت داده‌ها، شامل جمع‌آوری، پردازش و نگهداری اطلاعات کاربران، ترسیم می‌کند. آن‌ها تصریح می‌کنند که ارائه دهندگان خدمات تنها مجاز به جمع‌آوری حداقل داده‌های مورد نیاز برای اهداف مشخص و از پیش تعیین شده هستند. علاوه بر این، کاربران باید بتوانند بدون قید و شرط، کل یا بخشی از داده‌های خود را بنا به درخواست حذف کنند، مشروط بر اینکه با مفاد قانون آیین دادرسی کیفری مطابقت داشته باشد.

نظارت بر انطباق و اعمال آن

برای اطمینان از رعایت این دستورالعمل‌ها، اپراتورهای پلتفرم و سامانه‌ها باید تحت ارزیابی دقیق توسط تنظیم‌گری بخشی و مراجع صدور مجوز قرار گیرند. تنها در صورتی که با استفاده از سازوکارهای نظارتی تدوین شده توسط مرکز ملی فضای مجازی، رعایت کامل دستورالعمل‌ها تأیید شود، به سکوها اجازه ادامه ارائه خدمات یا تمدید مجوزهایشان داده خواهد شد.

نکات کلیدی

–ارائه‌دهندگان خدمات آنلاین باید سیاست‌های حفظ حریم خصوصی خود را به طور واضح افشا کرده و رضایت صریح کاربران را کسب کنند.

-پلتفرم‌ها تنها مجاز به جمع‌آوری حداقل داده‌های مورد نیاز برای اهداف خاص هستند.

-کاربران حق دارند کل یا بخشی از داده‌های خود را بنا به درخواست حذف کنند.

-رعایت دستورالعمل‌های حفظ حریم خصوصی داده‌ها برای ادامه فعالیت الزامی است (مرکز ملی فضای مجازی، ۱۴۰۲).

برنامه هفتم پیشرفت

در آبان‌ماه ۱۴۰۲ و در جریان بررسی برنامه هفتم توسعه در مجلس شورای اسلامی نمایندگان با بند «ب» ماده ۷۵ این لایحه برنامه هفتم توسعه-که اکنون قانون برنامه هفتم پیشرفت نامیده شده است-موافقت کردند. بندی که بر اساس آن وزارت فرهنگ و ارشاد اسلامی مکلف شده است تا نسبت به راه‌اندازی سامانه رصد، پایش و سنجش مستمر شاخص‌های فرهنگ عمومی، سبک زندگی مردم، مرجعیت رسانه‌ای و وضعیت ارتباطات کشور اقدام کند. متن این بند بدین شرح است:

بند ب) به‌منظور احصای دقیق و برخط داده‌های آماری مورد نیاز به جهت تسهیل پردازش، تحلیل دقیق و ایجاد بستر مناسب برای آینده‌پژوهشی روندهای سبک زندگی جامعه ایرانی، شناخت تحولات فرهنگی-ارتباطی و همچنین انتشار آنها، وزارت فرهنگ و ارشاد اسلامی مکلف است با همکاری سازمان صداوسیمای جمهوری اسلامی ایران و مرکز آمار ایران و راهبری و نظارت مرکز رصد و برنامه‌ریزی و ارزیابی دبیرخانه شورای عالی انقلاب فرهنگی و با رعایت اصل بیست‌وپنجم (۲۵) قانون اساسی و قانون مدیریت داده‌ها و اطلاعات ملی نسبت به راه‌اندازی سامانه رصد، پایش و سنجش مستمر شاخص‌های فرهنگ عمومی، سبک زندگی مردم، مرجعیت رسانه‌ای و وضعیت ارتباطات کشور اقدام نماید. دستگاه‌های اجرائی و دارندگان پایگاه‌های داده موضوع این بند به جز دستگاه‌هایی که مستقیماً زیرنظر مقام معظم رهبری هستند، موظفند نسبت به ارائه مستمر و جامع داده‌ها به این سامانه به‌صورت برخط اقدام کنند. وزارت فرهنگ و ارشاد اسلامی مکلف است ضمن برقراری دسترسی برخط مجلس به سامانه فوق، گزارش تغییرات شاخص‌های فرهنگ عمومی را سالانه به کمیسیون فرهنگی مجلس ارسال نماید (قانون برنامه پنج‌ساله هفتم پیشرفت جمهوری اسلامی ایران، ۱۴۰۳: صص. ۲۰۲-۲۰۳).

در زمان بررسی و تصویب این بند در مجلس شورای اسلامی، بحث‌های مختلفی در رسانه‌ها مطرح شد و افکار عمومی نسبت به نقض حریم خصوصی شهروندان ابراز نگرانی کردند. با اینکه این بند گردآوری داده‌ها را منوط به رعایت مفاد اصل ۲۵ قانون اساسی می‌کند که طی آن ورود به حریم خصوصی فقط با مجوز قانون امکان‌پذیر است اما موضوع کسب

مجوزهای قانونی و نیز عبارت «ارائه مستمر و جامع داده‌ها...به صورت برخط» بحث‌برانگیز هستند. زیرا اولاً به نظر می‌رسد مجوز قانونی به شکل موردی صادر می‌شود و مشخص نیست که برای گردآوری مستمر داده‌ها تنها یک حکم قانونی کفایت می‌کند یا خیر. دوم اینکه، منظور از جامعیت داده مشخص نیست. همانطور که در فصل‌های پیشین بحث شد، معمولاً اشتراک‌گذاری داده‌ها به شکل تقلیل‌یافته است و کلان‌داده‌ها به شکلی که جزئیات سوژه یا دارنده داده مشخص نباشد، با طرف‌های ثالث با اهداف گوناگون به اشتراک گذاشته می‌شوند. بنابراین، مشخص نیست که منظور قانون‌گذار کدامیک از شکلّ‌های داده است. اگر دریافت داده بدون ملاحظه فوق صورت گیرد، این اقدام آشکارا نقض حریم داده‌های شخصی است. سوم اینکه در این بند، به مفهوم پردازش اشاره شده است که در قوانین ایران سابقه ندارد. هرچند در مقررات جهانی همانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا بحث‌های مهمی درباره این مفهوم و کیفیت آن وجود دارد. بنابراین ضروری است به جزئیات آن به منظور تطابق با حق حریم خصوصی شهروندان ایرانی توجه شود.

حمایت از حریم خصوصی در اسناد بین‌المللی

حریم خصوصی، که زمانی مفهومی حاشیه‌ای تلقی می‌شد، به عنوان حقی بنیادین از حقوق بشر در اسناد حقوقی متعدد بین‌المللی ذکر شده است. این بخش به بررسی چشم‌انداز در حال تحول حریم خصوصی در حقوق بین‌الملل می‌پردازد.

-ممنوعیت دخالت در حریم خصوصی افراد

بنیان حقوق بین‌المللی حریم خصوصی در اعلامیه جهانی حقوق بشر در سال ۱۹۴۸ نهفته است. ماده ۱۲ حق حریم خصوصی را اعلام می‌کند و بیان می‌دارد که «هیچ‌کس نباید در معرض دخالت خودسرانه در زندگی خصوصی، خانه یا خانواده‌اش قرار گیرد و همچنین نباید مورد اهانت به حیثیت و شهرت خود قرار گیرد.» این اصل اساسی در اسناد بین‌المللی بعدی نیز طنین‌انداز شده است.

عهدنامه (میثاق) بین‌المللی حقوق مدنی و سیاسی مصوب ۱۹۶۶ بر این حق بیشتر تأکید می‌کند. ماده ۱۷ جزئیات مربوط به حمایت در برابر دخالت غیرقانونی یا خودسرانه در حریم خصوصی را شرح می‌دهد که شامل خانه، خانواده، مکاتبات و حیثیت

فرد می‌شود. با این حال، این میثاق محدودیت‌هایی را برای این حق قائل است و اجازه محدودیت‌هایی را می‌دهد که در یک جامعه دموکراتیک و به نفع امنیت ملی یا نظم عمومی ضروری باشد.

فراتر از این اعلامیه‌های جهانی، ابزارهای منطقه‌ای نیز از حمایت‌های حریم خصوصی پشتیبانی کرده‌اند. برای مثال، کنوانسیون اروپایی حقوق بشر مصوب سال ۱۹۵۰ حق احترام به زندگی خصوصی و خانوادگی را با محدودیت‌های مشابهی برای امنیت عمومی و امنیت ملی تضمین می‌کند. ازجمله ماده کنوانسیون اروپایی حقوق بشر آمده است: «هرکس نسبت به حریم زندگی خصوصی و خانوادگی، منزل و ارتباطات خود واجد حق است». (انصاری، ۱۴۰۰: ۶۰).

ظهور سریع عصر دیجیتال چالش‌های جدیدی را برای حریم خصوصی ایجاد کرده است. حجم عظیم داده‌های شخصی که به صورت آنلاین جمع‌آوری می‌شوند، همراه با ابزارهای قدرتمند تجزیه و تحلیل داده‌ها، نگرانی‌هایی را در مورد نظارت گسترده و از بین رفتن حریم خصوصی ایجاد می‌کند. حقوق بین‌الملل در تلاش است تا خود را با این چشم‌انداز در حال تحول وفق دهد.

کنوانسیون جرائم سایبری شورای اروپا مصوب ۲۰۰۱ به تکنیک‌های تحقیقاتی در فضای سایبر می‌پردازد و وجود ضمانت‌هایی برای حمایت از داده‌ها در طول تحقیقات را الزامی می‌داند. مجمع عمومی سازمان ملل متحد نیز قطعنامه‌هایی را در مورد حق حریم خصوصی در عصر دیجیتال به تصویب رسانده و از کشورها خواسته است که حق حریم خصوصی را در فضای آنلاین رعایت و از آن حمایت کنند.

با این حال، چارچوب حقوقی بین‌المللی برای حریم خصوصی در عصر دیجیتال همچنان پراکنده و مورد مناقشه است. نگرانی‌های امنیت ملی اغلب با حقوق حریم خصوصی افراد در تضاد است و سرعت بالای توسعه فناوری چالش‌های جدیدی را ایجاد می‌کند. به عنوان مثال، مسئله انتقال داده‌ها از مرزها، مسائل پیچیده‌ای را در مورد اینکه قوانین حریم خصوصی کدام حوزه‌های قضایی اعمال می‌شود، مطرح می‌کند.

در نتیجه، حق حریم خصوصی به ویژگی‌ای برجسته‌تر در حقوق بین‌الملل تبدیل شده است. از اصول اساسی اعلام‌شده در اعلامیه جهانی حقوق بشر تا رژیم‌های پیچیده حفاظت از داده در اتحادیه اروپا، حقوق بین‌الملل نشان‌دهنده شناخت فزاینده‌ای از اهمیت حریم خصوصی است. با این حال، عصر دیجیتال چالش‌های جدید و پیچیده‌ای را ایجاد می‌کند که نیازمند تکامل مستمر و همکاری بین کشورها برای اطمینان از یک چارچوب قوی برای حمایت از این حق اساسی در قرن

بیست و یکم است. هدف این فصل مفهوم‌سازی و تحلیل حریم داده و اطلاعات در اسلام، قوانین ایران و اسناد بین‌الملل بوده است. بر این اساس برخی مضامین شناسایی شدند که در جدول ۴-۲ ذکر شده است.

حریم خصوصی و داده در اسلام، قوانین ایران و قوانین بین‌الملل	– حریم خصوصی در اسلام –حریم خصوصی به‌مثابه حفظ کرامت انسانی –مصداق‌های حریم خصوصی در اسلام حدود اختیار دولت برای ورود به حریم خصوصی –مصلحت به مثابه جواز ورود به حریم خصوصی ––قاعده حفظ نظام و مصلحت و ورود به حریم خصوصی حریم خصوصی پس از انقلاب اسلامی –حق حریم خصوصی به مثابه حق بنیادین در حکومت اسلامی از منظر امام خمینی –امنیت عمومی به‌مثابه تنها جواز نقض حریم خصوصی افراد –ضرورت حفظ حریم خصوصی در پیام‌رسان‌ها –عدم حمایت صریح از حریم خصوصی در قانون اساسی –توجه به حریم خصوصی ارتباطات در قانون اساسی –لزوم قانون‌مند بودن ورود به حریم خصوصی از منظر قانون اساسی حریم خصوصی در قوانین و مقررات ایران –ممنوعیت نقض حریم خصوصی توسط کارکنان دولتی ––ممنوعیت ورود به حریم خصوصی بدون حکم قانون –مجرمانه بودن توسل به اطلاعات شخصی برای تهدید دیگران

	-مجرمانه بودن نقض اطلاعات شخصی -ضرورت اخذ رضایت کاربران برای تحلیل داده‌های آنها حمایت از حریم خصوصی در اسناد بین‌المللی -ممنوعیت دخالت در حریم خصوصی افراد

جدول ۴-۲) مضامین حریم خصوصی و داده در اسلام، قوانین ایران و قوانین بین‌الملل

نتیجه‌گیری

در این بخش تلاش شد تا مبانی فقهی و دینی حریم خصوصی در ایران مورد بررسی قرار گیرد. سپس حریم خصوصی به‌ویژه حریم داده و ارتباطات را در قوانین ایران و درنهایت در قوانین بین‌الملل بررسی کردیم. ازجمله این مرور نشان داد که گرچه در منابع غربی از حریم خصوصی به عنوان یک حق اساسی نام برده شده است اما در منابع اساسی حفظ حریم خصوصی با شأنیت و کرامت انسان و لزوم پاسداشت آن پیوند خورده است. از طرف دیگر، در منابع دینی از مصلحت عمومی به‌عنوان مجوزی برای ورود به حریم خصوصی انسان‌ها نام برده شده است، اما در قوانین بین‌المللی بیشتر مبنا قانون و مجوز قانونی است. از سوی دیگر، فقدان یک تعریف واحد از حریم خصوصی و داده و اطلاعات در قوانین ایران، یک نقص بزرگ در صیانت از حریم داده و اطلاعات در ایران است.

بخش سوم

اصول بنیادین و اقدامات حفاظت از حریم خصوصی و حریم داده در پلتفرم‌های جهانی

مقدمه

هدف این بخش مطالعه اصول بنیادین حاکم و اقداماتی است که پلتفرمهای بزرگ جهانی شامل گوگل، متا و توئیتر (ایکس) نسبت به داده‌های کاربران اتخاذ کرده‌اند. مطالعه این سیاستها برای تدوین اصول مشابه برای پلتفرم‌های ایرانی کمک شایانی خواهد کرد. سیاستهای مرتبط با حریم خصوصی و نحوه حفاظت از داده‌ها یکی از بخش‌های اصلی حکمرانی پلتفرمی یا تعدیل محتوا (گوروا، ۲۰۱۴) است. پس از مطالعه توصیفی-تحلیلی هرکدام از این پلتفرم‌ها، نتایج حاصل در قالب یک جدول مضامین ذکر می‌شود. اولین پلتفرم، گوگل است.

پلتفرم گوگل

نخستین پلتفری که سیاستهای حریم خصوصی و داده آنرا مورد بررسی قرار می‌دهیم، گوگل است. گوگل یک شرکت چند ملیتی فناوری است که در سال ۱۹۹۸ توسط لری پیج و سرگی برین تأسیس شد. مأموریت گوگل سازماندهی اطلاعات جهان و در دسترس و مفید ساختن آن برای همه است. این شرکت از آن زمان به یک رهبر جهانی در بخش‌های مختلف فناوری، از جمله جستجوی آنلاین، تبلیغات، رایانش ابری، نرم‌افزار و سخت‌افزار تبدیل شده است. موتور جستجوی گوگل به ابزاری ضروری برای میلیاردها کاربر در سراسر جهان تبدیل شده است و به مردم کمک می‌کند تا به سرعت و به طور مؤثر به اطلاعات مورد نظر خود دست پیدا کنند.

در طول سال‌ها، گوگل با خرید و توسعه پلتفرم‌ها و خدمات محبوب مختلف مانند یوتیوب، جیمیل، گوگل درایو، گوگل مپ و کروم، دامنه فعالیت خود را گسترش داده است. تعهد این شرکت به نوآوری در سرمایه‌گذاری آن در فناوری‌های نوظهور

مانند هوش مصنوعی، رایانش کوانتومی و خودروهای خودران مشهود است. مجموعه محصولات، خدمات و ابتکارات گوگل آن را به نامی آشنا و یکی از بازیگران اصلی در شکل‌دهی چشم‌انداز دیجیتال مدرن تبدیل کرده است.

این تحلیل در اصل با تکیه بر اسناد خود گوگل و سایر مطالعات نهادها و پژوهشگران مختلف درباره سیاست حریم خصوصی گوگل انجام می‌شود. این تحلیل به شکل تحلیل اسنادی و تحلیل محتوای کیفی انجام می‌شود. به این معنا که اسناد مرتبط با تکیه بر اسناد خود پلتفرم‌ها تحلیل می‌شوند تا مقوله‌ها یا مضمون‌های اصلی که شکل‌دهنده اصول حاکم بر این پلتفرم هستند، استخراج شوند. این تحلیل ابتدا به شکل توصیفی و تحلیلی انجام می‌شود. در مورد سایر پلتفرم‌ها نیز به همین روش اقدام خواهد شد.

حریم خصوصی در گوگل اسناد

به مثابه بخشی از رویکرد کلی حکمرانی در پلتفرم، گوگل اسناد بالادستی مختلفی را برای اعلام شروط و پیش‌شرط فعالیت کاربران در این پلتفرم اعلام کرده است. گوگل شرایط سیاست حریم خصوصی و شرایط ارائه خدمت خود[1]را در یک بخش معرفی کرده است[2]. سیاست حریم خصوصی (و یا در ترجمه فارسی گوگل از آن خطمشی رازداری) از شرایط (ارائه) خدمت متمایز هستند. شرایط ارائه خدمت گوگل در ۲۲ مه ۲۰۲۴ گوگل به‌روزرسانی شده است و در آن به صراحت اعلام می‌شود که سیاست حریم خصوصی بخشی از شرایط ارائه خدمت نیست اما مطالعه آن به درک بهتر اینکه گوگل چگونه اطلاعات کاربران را به‌روزرسانی، مدیریت، صادر و حذف می‌کند، کمک‌کننده است (شرایط ارائه خدمت گوگل، ۲۰۲۴). شرایط ارائه خدمت نوعی توافقنامه میان کاربران و این شرکت به هنگام استفاده از خدمات گوگل و به تعبیر گوگل بیانگر انتظارات کاربران از خدمات گوگل و انتظارات کاربران از شرکت گوگل است.

- اصل حفظ حریم خصوصی بر اساس طراحی یا حفظ حریم خصوصی به صورت پیش‌فرض

[1] .Google Privacy and Terms
[2] . https://policies.google.com/privacy?hl=en

در یک مرور کلی بخش سیاست حریم خصوصی و شرایط خدمت گوگل شامل این دو بخش پیش‌گفته و نیز مرکز ایمنی گوگل[۱]، حساب کاربری گوگل[۲]، اصول حریم خصوصی و ایمنی ما[۳] و راهنمای حریم حریم خصوصی محصولات گوگل[۴] است. همانطور که مشخص است، بحث حریم خصوصی در سطوح گوناگون ارائه خدمت در گوگل اهمیت فراوانی دارد. ازجمله در حساب کاربری گوگل، توجه به داده‌های شخصی اهمیت فراوانی دارد. با توجه به اینکه اکنون برای اتصال به بسیاری از خدمات آنلاین و حتی خدمات پلتفرم‌های هوش مصنوعی، امکان ثبت‌نام از طریق گوگل به جای ثبت‌نام‌های متعدد فراهم شده است و حساب کاربری گوگل به یک حساب کاربری فراگیر و جهانی تبدیل می‌شود، حفاظت از داده‌های شخصی کاربران گوگل بیش از پیش اهمیت پیدا می‌کند. به نظر می‌رسد تعبیه‌شدگی گسترده اصول و سازوکارهای حفاظت از داده‌های شخصی کاربران و حریم خصوصی تابع اصل حفظ حریم خصوصی بر اساس طراحی[۵] یا حفظ حریم خصوصی به صورت پیش‌فرض[۶] است.

حریم خصوصی بر اساس طراحی و حریم خصوصی به صورت پیش‌فرض دو اصل مکمل هستند که برای محافظت از حریم خصوصی کاربران با هم کار می کنند. مفهوم حریم خصوصی بر اساس طراحی بر ادغام فعالانه ملاحظات مربوط به حریم خصوصی در توسعه محصولات و خدمات از همان ابتدا تأکید دارد. در عمل، چنانچه یک پلتفرم رسانه اجتماعی با در نظر گرفتن حریم خصوصی طراحی شده باشد، مهندسان در طول فرآیند توسعه، ویژگی‌هایی مانند رمزگذاری قوی، کنترل‌های دقیق حریم خصوصی و راه‌هایی برای به حداقل رساندن جمع‌آوری داده‌ها را در نظر می‌گیرند.

مفهوم حریم خصوصی به صورت پیش‌فرض بر اطمینان از این موضوع تمرکز دارد که تنظیمات پیش‌فرض یک محصول یا خدمت، حداکثر سطح محافظت از حریم خصوصی را بدون نیاز به تغییر هیچ تنظیماتی به کاربران ارائه دهد. چنانچه مثال پلتفرم رسانه‌های اجتماعی را در نظر بگیریم، حریم خصوصی به صورت پیش‌فرض تضمین می‌کند که پروفایل‌های کاربری به صورت پیش‌فرض خصوصی باشند، اشتراک‌گذاری موقعیت مکانی خاموش باشد و جمع آوری داده‌ها برای تبلیغات هدفمند به صورت پیش‌فرض غیرفعال باشد. کاربران در صورت تمایل می‌توانند برای به اشتراک گذاشتن اطلاعات بیشتر،

---

[1] .Google Safety Center
[2] .Google Account
[3] .Our Privacy and security Principles
[4] .Google Product Privacy Guide
[5] .privacy by design
[6] .privacy by default

رضایت خود را اعلام کنند. این دو اصل با هم حریم خصوصی را به جای یک فکر پسینی، به هسته اصلی یک سیستم تبدیل می‌کنند. این دو اصل با اولویت قرار دادن به حریم خصوصی، کاربران را توانمند می‌کنند.

این اصول به‌ویژه در دنیای امروزی که مبتنی بر داده مهم هستند و اغلب توسط مقررات حفظ حریم خصوصی داده مانند مقررات عمومی حفاظت از داده الزام‌آور هستند–این موضوع اخیر در بخش‌های دیگر و به طور خاص هنگام بررسی مقررات عمومی حفاظت از داده‌ها با جزئیات بررسی می‌شود.

کاووکیان (۲۰۰۹) هفت اصل را به عنوان اصول بنیادی حریم خصوصی بر اساس طراحی برشمرده است که عبارتند از:

۱. پیشگیرانه به جای واکنشی؛ پیشگیری به جای درمان

پیش بینی، شناسایی و جلوگیری از وقوع حوادث نقض حریم خصوصی قبل از وقوع آن‌ها.

۲. حریم خصوصی به عنوان تنظیمات پیش‌فرض

بالاترین سطح از حریم خصوصی را به عنوان تنظیمات پیش‌فرض برای هر سیستم یا رویه تجاری اعمال کنید. این کار باعث حفظ حریم خصوصی کاربر حتی در صورت عدم انجام هیچ اقدامی می‌شود.

۳. تعبیه حریم خصوصی در طراحی

تنظیمات حریم خصوصی را در طراحی و معماری سیستم‌های فناوری اطلاعات و شیوه‌های کسب و کار تعبیه کنید، به جای اینکه آن‌ها را به عنوان یک افزودنی پس از طراحی، اجرا نمایید.

۴. عملکرد کامل– مجموع مثبت، نه مجموع صفر

تمامی علایق و اهداف مشروع را به شیوه‌ای مثبت در نظر بگیرید تا تعادلی بین حریم خصوصی و امنیت ایجاد کنید، زیرا دستیابی به هر دو مورد امکان‌پذیر است.

۵. امنیت جامع–حفاظت از کل چرخه عمر

اقدامات امنیتی قوی را در کل چرخه عمر داده‌ها برای اطمینان از مدیریت ایمن اطلاعات از ابتدا تا انتها، تعبیه کنید.

۶. قابلیت مشاهده و شفافیت–آن را باز نگه دارید

به ذینفعان اطمینان دهید که استانداردهای حریم خصوصی باز، شفاف و قابل تأیید مستقل هستند.

۷. احترام به حریم خصوصی کاربر–آن را کاربرمحور نگه دارید

با ارائه پیش‌فرض‌های قوی حریم خصوصی، اطلاع رسانی مناسب و توانمندسازی گزینه‌های کاربرپسند، از منافع کاربران محافظت کنید.

ادعای گوگل این است که اصل کلی حریم خصوصی بر اساس طراحی جزو اصول لاینفک این شرکت فناوری است. گوگل در بخش اصول حریم خصوصی خود ادعا می‌کند «ما محصولاتی می‌سازیم که برای همه به شکل خصوصی بر اساس طراحی هستند» و منظور از آن این است که این شرکت برای داده‌هایی که استفاده می‌کند، نحوه استفاده از آنها و نحوه حفاظت از آنها به شکل ملاحظه‌کارانه عمل می‌کند (مرکز ایمنی گوگل (اصول حریم خصوصی گوگل)، ۲۰۲۴).

بنابراین مفهوم محوری یا مضمون کلیدی اصول حریم خصوصی گوگل، حریم خصوصی بر اساس طراحی است که راهنمای عمل گوگل در طراحی و تولید محصولات، فرایندها و نیز کارکنان آن برای حفظ و ایمن نگه‌داشتن داده و فراهم کردن امکان کنترل کاربران بر اطلاعات‌شان است. بنابراین توانمندسازی کاربران در حفاظت از داده‌ها اهمیت ویژه‌ای دارد. اصول حریم داده‌های کاربران دارای شش اصل اساسی که به شکل نامی که ما به آن اصل می‌دهیم، خود اصل و نیز تعریف گوگل در قالب جدول ۳–۴) بیان می‌شوند.

مفهوم	اصل	تعریف و توضیح
عدم فروش اطلاعات به شخص ثالث	ما هرگز اطلاعات شخصی شما را به کسی نمی فروشیم.	ما از داده‌ها برای کاربردی‌تر کردن محصولات گوگل در لحظات مهم استفاده می‌کنیم. برای مثال، به شما کمک می‌کنیم تا یک رستوران نزدیک یا مسیری کم‌مصرف‌تر برای رسیدن به خانه پیدا کنید. همچنین از داده‌ها برای نمایش تبلیغات مرتبط‌تر استفاده

		می‌کنیم. در حالی که این تبلیغات به ما امکان می‌دهند محصولات را به صورت رایگان برای همه ارائه دهیم، مهم است که تأکید کنیم ما هرگز اطلاعات شخصی شما را به هیچکس، حتی برای اهداف تبلیغاتی، نمی‌فروشیم. این موضوع به طور کامل منتفی است.
شفاف‌سازی در مورد اطلاعات گردآوری شده	ما در مورد اینکه چه داده هایی را جمع آوری می کنیم و چرا شفاف هستیم.	می‌خواهیم بدانید چه داده‌هایی را جمع‌آوری می‌کنیم، چگونه از آن‌ها استفاده می‌کنیم و چرا. شفافیت برای ما مهم است، بنابراین یافتن و درک این اطلاعات را برای شما آسان می‌کنیم. به این ترتیب، می‌توانید در مورد نحوه استفاده از محصولات گوگل تصمیمات آگاهانه بگیرید.
تسهیل کنترل اطلاعات شخصی	کنترل اطلاعات شخصی خود را برای شما آسان می کنیم.	این به معنای آن است که به راحتی می‌توانید تنظیمات حریم خصوصی مناسب خود را انتخاب کنید و هر زمان که بخواهید اطلاعات شخصی که با گوگل به اشتراک گذاشته‌اید را کنترل کنید – از جمله بررسی داده‌های خود، دانلود و انتقال آن به سرویس دیگری در صورت تمایل یا حذف کامل آن.
تقلیل[1] داده‌های شخصی	ما برای محافظت بیشتر از حریم خصوصی شما، داده‌هایی را که استفاده می کنیم تقلیل می دهیم.	ما هرگز از محتوایی که شما در برنامه‌هایی مانند درایو، جیمیل و عکس‌ها ایجاد و ذخیره می‌کنید برای مقاصد تبلیغاتی استفاده نمی‌کنیم و همچنین هرگز از اطلاعات حساس مانند سلامتی، نژاد، مذهب یا گرایش جنسی برای شخصی‌سازی تبلیغات برای شما استفاده نمی‌کنیم.

[1] .reduction

		علاوه بر این، کنترل‌های حذف خودکار را به عنوان پیش‌فرض تنظیم کرده‌ایم، بنابراین به‌طور منظم داده‌های فعالیت آنلاین شما را که به حساب گوگل شما مرتبط است، مانند مواردی که جستجو کرده‌اید و تماشا کرده‌اید، حذف می‌کنیم. هنگامی که از محصولات ما استفاده می‌کنید، اطلاعات خود را به ما می‌سپارید و وظیفه ما این است که به درستی از آن محافظت کنیم. به همین دلیل، ما از یکی از پیشرفته‌ترین زیرساخت‌های امنیتی جهان برای محافظت از داده‌های شما استفاده می‌کنیم.
تضمین ایمنی با ساخت محصولات ایمن به شکل پیش‌فرض	ما با ساخت محصولاتی که به طور پیش فرض امن هستند از شما محافظت می کنیم.	محصولات ما به گونه‌ای طراحی شده‌اند که به صورت پیش‌فرض ایمن باشند و ما دائماً اقدامات امنیتی خود را برای شناسایی و محافظت در برابر تهدیدات آنلاین در حال تکامل، مانند بازیگران مخربی که سعی در سرقت اطلاعات شخصی شما دارند، قبل از اینکه به دست شما برسد، تقویت می‌کنیم. حفظ اینترنت به صورت باز، خصوصی و امن، هسته اصلی تمام کارهایی است که ما انجام می‌دهیم.
ساخت و توسعه فناوری‌های پیشرفته حفاظت از حریم خصوصی	ما فناوری‌های پیشرفته حفظ حریم خصوصی را توسعه می‌دهیم و آن‌ها را با دیگران به اشتراک می‌گذاریم.	امنیت آنلاین شما نباید با گوگل متوقف شود – بلکه باید به کل اینترنت گسترش یابد. به همین دلیل است که ما به نوآوری در فناوری‌های حفظ حریم خصوصی ادامه می‌دهیم و آن‌ها را به‌طور گسترده در دسترس قرار می‌دهیم. ما یافته‌ها، تجربیات و ابزارهای خود را با شرکا، سازمان‌ها و رقبا به اشتراک می‌گذاریم، زیرا حفظ امنیت اینترنت نیازمند همکاری همگان است.

جدول ۳-۴) اصول راهنمای گوگل برای حفاظت از داده‌ها و حریم شخصی (منبع وب‌سایت گوگل، ۲۰۲۴).

درمجموع، دو رویکرد اساسی حریم خصوصی بر اساس طراحی و حریم خصوصی به شکل پیش‌فرض، در کنار ممنوعیت فروش داده‌های شخصی به دیگران، شفاف‌سازی در مورد اطلاعاتی که پلتفرم گوگل گردآوری می‌کند، تقلیل و یا به عبارت دیگر زدودن جزئیات داده‌های شخصی افراد، تأکید بر ساخت محصولات و خدمات بر اساس حفظ حریم خصوصی به شکل پیش‌فرض و توسعه فناوری‌های حفظ حریم خصوصی از جمله اصول راهنمایی هستند که می‌توانند برای تدوین قواعد و مقررات مرتبط با حفاظت از داده‌ها در فضای مجازی و پلتفرم‌های رسانه‌های اجتماعی مورد تأکید قرار گیرند. موضوع حائز اهمیت دیگری که در اصول حفظ حریم خصوصی بر اساس طراحی مورد تأکید قرار گرفت، توانمندسازی کاربران است. به این معنا که کاربران باید این حق و اختیار را داشته باشند که بتوانند میزان انتشار و یا اشتراک‌گذاری محتوا را کنترل کنند و تصمیم بگیرند که کدامیک از داده‌های آنها می‌تواند در اختیار کاربران دیگر، شرکت پلتفرمی و نیز شرکت‌های ثالثی قرار گیرد که مدل کسب و کار آنها مبتنی بر تحلیل داده‌های کاربران است.

مرکز ایمنی گوگل و حریم خصوصی

ایمنی (امنیت) و حریم خصوصی ارتباط نزدیکی با یکدیگر دارند. به همین دلیل است که در بحث‌های مرتبط با ایمنی به حریم خصوصی نیز توجه می‌شود. همانطور که کوریا و رودریگز (۲۰۲۳) گفته‌اند، امنیت و حریم خصوصی رشته‌های به هم وابسته‌ای هستند. حریم خصوصی تا حد زیادی در مورد امنیت، به ویژه محرمانگی اطلاعات شخصی و شناساگرهای شخصی است. از طرف دیگر، همانطور که ویپل و شریتویز (۲۰۲۳) می‌گویند، امنیت به وضعیتی از یک سیستم اشاره دارد که در برابر تهدیدات و ریسک‌های بالقوه محافظت شود؛ مفهوم خاص آن به الزامات امنیتی بستگی دارد. اما حریم خصوصی حق اساسی فرد برای تعیین و محدود کردن دسترسی دیگران به اطلاعات و تجربیات شخصی اوست که این امر توانایی فرد در حفظ مرزهای شخصی، محرمانگی و آزادی از نظارت غیرمجاز را تضمین می‌کند.

-ایمنی و حریم خصوصی

حریم خصوصی و امنیت مفاهیمی به هم مرتبط هستند که اغلب در زمینه فناوری‌های دیجیتال و تعاملات آنلاین با هم در ارتباط هستند. در حالی که آنها معانی متمایزی دارند، هر دو برای اطمینان از محافظت از افراد و اطلاعات شخصی آنها ضروری هستند. در اینجا نحوه ارتباط این دو مفهوم آمده است

۱. هدف مشترک محافظت حریم خصوصی و امنیت یک هدف مشترک برای محافظت از کاربران و اطلاعات آنها دارند. حریم خصوصی بر روی محافظت از اطلاعات شخصی در برابر دسترسی غیرمجاز و اطمینان از کنترل افراد بر نحوه استفاده و به اشتراک گذاشتن داده‌هایشان تمرکز دارد. امنیت از سوی دیگر، شامل محافظت از داده‌ها، دستگاه‌ها و شبکه‌ها در برابر تهدیداتی مانند هک کردن، سرقت و دسترسی غیرمجاز است.

۲. اقدامات و شیوه‌های همپوشانی بسیاری از اقدامات و شیوه‌ها به هر دو حریم خصوصی و امنیت کمک می‌کنند. برای مثال، رمزگذاری می‌تواند هر دو حریم خصوصی (با محافظت از محتوای ارتباطات شخصی) و امنیت (با جلوگیری از دسترسی غیرمجاز به داده‌های حساس) را افزایش دهد. به طور مشابه، مکانیسم‌های احراز هویت قوی، کنترل دسترسی و به‌روزرسانی‌های منظم نرم‌افزار می‌توانند هم حریم خصوصی و هم امنیت را بهبود بخشند.

۳. رابطه تکمیلی دستیابی به حریم خصوصی قوی اغلب به زیربنایی از شیوه‌های امنیتی قوی نیاز دارد و بالعکس. برای مثال، سیستم‌های امن به محافظت از اطلاعات شخصی کمک می‌کنند و در نتیجه به حفظ حریم خصوصی کمک می‌کنند. برعکس، احترام به حریم خصوصی با به حداقل رساندن جمع‌آوری و نگهداری داده‌های حساس می‌تواند به کاهش خطر نقض امنیتی و آسیب‌های بالقوه ناشی از افشای داده کمک کند.

۴. برقراری تعادل بین حریم خصوصی و امنیت در برخی موارد، ممکن است بین حریم خصوصی و امنیت تعارض وجود داشته باشد. برای مثال، اقدامات امنیتی خاص، مانند نظارت بر ترافیک شبکه یا جمع‌آوری داده‌های کاربران برای شناسایی تهدید، ممکن است نگرانی‌هایی را در مورد حریم خصوصی ایجاد کند. سازمان‌ها و افراد باید بین این دو الزام، با در نظر گرفتن زمینه خاص و خطرات درگیر، تعادل برقرار کنند.

به طور خلاصه، در حالی که حریم خصوصی و امنیت مفاهیم متمایزی هستند، آنها در هدف خود برای محافظت از افراد و اطلاعاتشان به هم مرتبط هستند. آنها اغلب در عمل همپوشانی دارند و نیازمند رویکردی متعادل برای اطمینان از ایمن بودن فناوری‌های دیجیتال و احترام به حریم خصوصی کاربر هستند.

مرکز ایمنی[1] یکی از بخش‌های دیگر گوگل است که در آن بحث‌هایی درباره نحوه تنظیم‌گری حریم خصوصی در این پلتفرم مورد تأکید قرار دارد. یکی از شعارهای گوگل در این بخش این است که «ما ابزارهای حریم خصوصی‌ای را می‌سازیم که شما در جایگاه کنترل‌کننده قرار دهد» (مرکز ایمنی گوگل، ۲۰۱۴). این گفته به طور آشکار رابطه بین حفظ ایمنی در گوگل و حریم خصوصی را نشان می‌دهد و بر اهمیت آنها تأکید می‌شود. در این بخش نقل قولی از سوندار پیچای مدیرعامل گوگل نقل شده است

ما اطلاعات آنلاین شخصی شما را خصوصی، امن و مطمئن نگه می داریم. تمامی محصولات ما تحت هدایت سه اصل مهم قرار دارند با داشتن یکی از پیشرفته‌ترین زیرساخت‌های امنیتی جهان، محصولات ما به طور پیش فرض امن هستند. ما به شدت از شیوه‌های مسئولانه داده‌های آنلاین پیروی می‌کنیم، بنابراین هر محصولی که می‌سازیم به صورت خصوصی طراحی شده‌است. و ما تنظیمات حریم خصوصی و امنیت داده‌ای را ایجاد می‌کنیم که استفاده از آن‌ها آسان است تا شما کنترل داشته باشید (پیچای، ۲۰۲۱).

همانطور که مضمون این نقل قول نشان می‌دهد، چند اصل مورد تأکید قرار دارد حریم خصوصی به شکل پیش‌فرض و بر اساس طراحی؛ مسئولیت نسبت به حفظ ایمنی داده‌های کاربران و لزوم توانمندسازی کاربران برای کنترل داده‌هایشان. این اصول مبنای ادعایی رویکرد گوگل نسبت به حفظ حریم خصوصی کاربرانش است.

-رمزگذاری به عنوان ابزار حفظ ایمنی

همچنین گوگل بر حریم داده تأکید کرده است که ابزار اصلی تحقق آن استفاده از فناوری‌های پیشرفته‌ای است که از پیش‌تعبیه اند[2]. درواقع کاربرد فناوری‌های امنیتی با هدف حفظ ایمنی داده‌ها رخ می‌دهد. ساختار امنیتی پیشرفته گوگل، به

[1] .Safety Center
[2] .built-in

طور خودکار تهدیدات آنلاین را شناسایی و از آنها جلوگیری می کند، بنابراین افراد می‌توانند اطمینان داشته باشند که اطلاعات خصوصی آنها در وضعیت ایمنی قرار دارد. یکی از موارد کاربرد فناوری پیشرفته برای حفظ محرمانگی داده‌ها رمزگذاری[1] است.

باید اشاره شود که رمزگذاری روشی است که در آن اطلاعات به یک کد مخفی تبدیل می‌شود تا معنای واقعی آن پنهان شود. رمزگذاری از دیرباز برای محافظت از اطلاعات حساس به کار می‌رفته است. در دوران مدرن، از رمزگذاری برای محافظت از داده‌ها در دو حالت سکون و انتقال استفاده می‌شود. داده‌های در سکون، اطلاعاتی هستند که روی رایانه‌ها و ابزارهای ذخیره‌سازی نگهداری می‌شوند. داده‌های در حال انتقال، به اطلاعاتی گفته می‌شود که بین دستگاه‌ها و روی شبکه‌ها در حال جابه‌جا شدن هستند. رمزگذاری نقشی حیاتی در ایمن سازی انواع مختلف دارایی های فناوری اطلاعات و اطلاعات قابل شناسایی شخصی ایفا می کند. هدف اصلی رمزگذاری محافظت از محرمانه بودن داده های دیجیتالی است که در سیستم های رایانه ای ذخیره شده یا از طریق اینترنت یا سایر شبکه های رایانه ای منتقل می شوند. برای محافظت از طیف گسترده ای از داده‌ها، از اطلاعات شناسایی شخصی گرفته تا دارایی‌های حساس شرکت تا اسرار دولتی و نظامی استفاده می‌شود. سازمان‌ها با رمزگذاری داده‌های خود، خطر افشای اطلاعات حساس را کاهش می‌دهند (شلدون، لاشین و کاب، ۲۰۲۴).

همانطور که گوگل اعلام کرده است

رمزگذاری باعث محرمانگی و امنیت داده‌ها در هنگام انتقال می‌شود. رمزگذاری باعث افزایش امنیت و حریم خصوصی خدمات ما می‌شود. هنگامی که ایمیلی ارسال می‌کنید، ویدیویی به اشتراک می‌گذارید، از وب‌سایتی بازدید می‌کنید یا عکس‌های خود را ذخیره می‌کنید، داده‌هایی که ایجاد می‌کنید بین دستگاه شما، خدمات گوگل و مراکز داده ما جابجا می‌شود. ما از این داده‌ها با چندین لایه امنیتی از جمله فناوری رمزگذاری پیشرو مانند اچ.تی.تی.پی.اس[2] و لایه امنتی انتقال[3] محافظت می کنیم (مرکز ایمنی گوگل، ۲۰۲۴).

[1] .Encryption
[2] . HTTPS
[3] . Transport Layer Security

نکته مهم دیگری که باید بر اساس بحث‌های مطرح شده در مرکز ایمنی گوگل به آن اشاره کنیم، اهمیت دادن به امکان کنترل کاربران بر حریم خصوصی و داده‌های خودشان است (مرکز ایمنی گوگل، ۲۰۲۴). ما می‌توانیم به دلایل مختلف بحث کنیم که چرا این قابلیت از منظر ایمنی و حریم خصوصی دارای اهمیت است

محافظت از اطلاعات شخصی با امکان کنترل تنظیمات حریم خصوصی توسط کاربران، آن‌ها می‌توانند انتخاب کنند که چه اطلاعاتی و با چه کسانی به اشتراک گذاشته شود. این امر به جلوگیری از دسترسی غیرمجاز به داده‌های حساس، مانند اطلاعات شخصی، اطلاعات مالی و موقعیت مکانی کمک می‌کند.

جلوگیری از نقض داده‌ها زمانی که کاربران امکان مدیریت تنظیمات حریم خصوصی خود را داشته باشند، خطر نقض داده‌ها کاهش می‌یابد. کاربران می‌توانند میزان در معرض دید قرار گرفتن داده‌های خود را محدود کنند و بدین ترتیب، آن‌ها را در برابر حملات سایبری بالقوه، تلاش‌های هک و دسترسی‌های غیرمجاز آسیب‌پذیرتر سازند.

-فراهم کردن امکان کنترل کاربران

اعتماد و رضایت کاربر هنگامی که کاربران احساس کنند حریم خصوصی آن‌ها مورد احترام قرار می‌گیرد و بر داده‌های خود کنترل دارند، به احتمال زیاد به پلتفرم اعتماد می‌کنند، با آن تعامل برقرار می‌کنند و اطلاعات را به اشتراک می‌گذارند. این امر رضایت کاربر را بهبود می‌بخشد و می‌تواند منجر به نرخ ماندگاری بالاتر کاربران در یک پلتفرم و توصیه به دیگران باری کاربرد یک پلتفرم خاص شود.

همچنین امکان ارائه پیشنهادهای شخصی‌سازی‌شده نیز وجود دارد که سبب افزایش ایمنی حساب کاربری کاربران گوگل می‌شود. همه این موارد بر امکان توانمندی کاربران برای حفاظت از حریم خصوصی‌شان دلالت دارد.

یکی از مهمترین اسنادی که از طریق آن می‌توانیم به رویکرد پلتفرم گوگل درباره گردآوری داده‌ها تا حفاظت از داده‌های کاربران پی ببریم، خط مشی یا سیاست حریم خصوصی گوگل است که نسخه آخر آن از ۲۸ مارس ۲۰۲۴ به اجرا گذاشته شده است. حریم خصوصی گوگل سندی جامع است که روش‌های جمع‌آوری، استفاده و محافظت از اطلاعات کاربران توسط گوگل در سراسر محصولات و خدمات مختلف آن را شرح می‌دهد. طی سالهای مختلف این سند به روزرسانی شده

است. اولین نسخه سیاست حریم خصوصی گوگل که در دسترس قرار دارد، به ماه ژوئن ۱۹۹۹ برمی‌گردد. در این سند رویکرد کلی گوگل به این شکل شرح داده شده است

سیاست گوگل در قبال وب‌سایت‌های تحت مالکیت و کنترل کامل ما، احترام و محافظت از حریم خصوصی کاربرانمان است. گوگل عمداً هیچ گونه اطلاعاتی که به طور شخصی قابل شناسایی باشد راجع به مشتریان خود، بدون دریافت اجازه قبلی از آن مشتری، به هیچ شخص ثالثی افشا نخواهد کرد. این بیانیه خط مشی به شما می‌گوید که چگونه اطلاعات را از شما جمع‌آوری می‌کنیم و چگونه از آن استفاده می‌کنیم (سیاست حریم خصوصی گوگل، ۱۹۹۹).

-اصل تقلیل داده‌های کاربران

موضوع دیگری که از همان ابتدا مورد تأکید گوگل دررابطه کاربردهای تجاری داده‌های کاربران قرار داشته است، اصل تقلیل داده‌های کاربران است

گوگل ممکن است اطلاعات مربوط به کاربران را با تبلیغ کنندگان، شرکای تجاری، اسپانسرها و سایر طرف های ثالث به اشتراک بگذارد. با این حال، ما *فقط* در مورد کاربران خود به صورت کل، نه به صورت جداگانه صحبت می کنیم. برای مثال، ممکن است فاش کنیم که یک کاربر معمولی گوگل چند بار به گوگل مراجعه می‌کند، یا اینکه کدام کلمات پرسش دیگری اغلب با کلمه پرسش «مایکروسافت» استفاده می‌شود (سیاست حریم خصوصی گوگل، ۱۹۹۹).

ملاحظه این نکته اساسی در هنگام تنظیم‌گری پلتفرم‌ها در ایران اهمیت اساسی دارد. تنظیم مقررات حریم خصوصی باید پلتفرم‌ها را ملزم کند تا از انتشار داده‌های کاربران که کاربر را شناسایی‌پذیر می‌کند، اجتناب نماید و در صورت کاربرد داده‌ها کاربران بر تقلیل داده‌ها یا ارائه آنها به شکل مجموع‌شده تأکید شود. تقلیل داده شکلهی مختلفی دارند که مهمترین آنها عبارتند از ناشناس‌سازی داده[1] یعنی تغییر یا حذف اطلاعات شخصی قابل شناسایی از مجموعه داده‌ها برای محافظت از

[1] . Data anonymization

حریم خصوصی افراد و کاهش خطر دسترسی غیرمجاز یا سوء استفاده و نیز تجمیع داده[1] که به معنای ترکیب یا خلاصه کردن داده‌ها در سطح بالاتر برای کاهش جزئیات و حجم اطلاعات ذخیره شده است. آخرین نسخه سیاست حریم خصوصی گوگل به چند بخش اصلی تقسیم می‌شود که عبارتند از

-اطلاعاتی که گوگل جمع‌آوری می‌کند این بخش جزئیات انواع اطلاعات شخصی را که گوگل از کاربران جمع‌آوری می‌کند، از جمله جزئیات حساب کاربری، اطلاعات دستگاه، داده‌های موقعیت مکانی و اطلاعات سرویس‌های جانبی را توضیح می‌دهد.

-چرا گوگل داده‌ها را جمع‌آوری می‌کند در اینجا، گوگل اهدافی را که برای آن داده‌های کاربران را جمع‌آوری می‌کند، مانند ارائه و بهبود خدمات خود، محافظت از حساب‌های کاربری و شخصی‌سازی محتوا را توضیح می‌دهد.

-چگونه گوگل از داده‌ها استفاده می‌کند این بخش نحوه پردازش و استفاده گوگل از داده‌های کاربر را شرح می‌دهد، از جمله ترکیب اطلاعات از چندین سرویس، به اشتراک گذاری داده‌ها با شرکت‌های تابعه و شرکا و مدیریت داده‌ها مطابق با الزامات قانونی.

-شفافیت و کنترل این بخش از خط مشی ابزارها و منابعی را که گوگل برای کمک به کاربران برای درک، مدیریت و کنترل تنظیمات حریم خصوصی و داده‌هایشان ارائه می‌کند، مانند داشبورد گوگل، فعالیت من و ابزارهای بررسی حریم خصوصی را مشخص می‌کند.

-اشتراک‌گذاری و افشای داده‌ها در اینجا، گوگل توضیح می‌دهد که چه زمانی و با چه کسانی ممکن است داده‌های کاربر را به اشتراک بگذارد، از جمله شرایط مربوط به درخواست‌های قانونی، محافظت از حقوق کاربر و اجرای سیاست‌های خود.

-نگهداری و حذف داده‌ها این بخش نحوه نگهداری داده‌های کاربر توسط گوگل و معیارهای مورد استفاده برای تعیین دوره‌های نگهداری، و همچنین نحوه حذف یا درخواست حذف داده‌های کاربران را شرح می‌دهد.

-حقوق و مسئولیت‌های کاربران این بخش حقوق و مسئولیت‌های کاربران را در قبال داده‌هایشان، مانند دسترسی، به‌روزرسانی و مدیریت اطلاعاتشان، و همچنین رعایت شرایط خدمات و خط‌مشی‌های گوگل را شرح می‌دهد.

[1] . Data aggregation

-خط‌مشی یا سیاست اشتراک‌گذاری داده‌های کاربران

درک سیاست پلتفرم بزرگ برای نحوه اشتراک‌گذاری داده‌های کاربران اهمیت زیای دارد و روشنگر است. درحالیکه همه محتواها و داده‌های به اشتراک گذاشته شده یا جستجو شده در همه خدمات زیرمجموعه گوگل به شکل آشکار همراه با نام برای گوگل مشخص است، وقتی گوگل تصمیم می‌گیرد اطلاعات کاربران را به اشترک بگذارد، این اشتراک‌گذاری با شرکتها، سازمانها یا افراد خارج از گوگل مبتنی بر برخی رویه‌ّها است. مهمترین رویه یا اقدام *کسب رضایت کاربران* است.

-کسب رضایت کاربران

همانطور که در سیاست حریم خصوصی گوگل می‌خوانیم

چنانچه شما رضایت داشته باشید، اطلاعات شخصی را خارج از گوگل به اشتراک خواهیم گذاشت...همچنین کنترل‌هایی را برای بررسی و مدیریت برنامه‌ها و سایت‌های شخص ثالثی که به داده‌های موجود در حساب گوگل خود اجازه دسترسی به آنها داده‌اید، در اختیار شما قرار می‌دهیم. ما برای به اشتراک گذاشتن هرگونه اطلاعات شخصی حساس، به طور صریح رضایت شما را خواهیم گرفت (سیاست حریم خصوصی گوگل، ۲۰۲۴).

اگرچه، دلایل *قانونی یا حقوقی* سبب می‌شوند تا گوگل بدون نیاز به کسب رضایت کاربران اقدام به افشای اطلاعات شخصی کاربران نماید. این دلایل به این شکل بیان شده‌اند

اطلاعات شخصی را در خارج از گوگل به اشتراک خواهیم گذاشت، اگر به حسن نیت اعتقاد داشته باشیم که افشای اطلاعات برای موارد زیر معقولانه ضروری است

-پاسخ به هر قانون، مقررات، روند قانونی یا درخواست قابل اجرای دولتی

-اجرای شرایط خدمات قابل اجرا، از جمله تحقیق در مورد نقض احتمالی قانون

-کشف، پیشگیری یا رسیدگی به تقلب، امنیت یا مشکلات فنی کشف، پیشگیری یا رسیدگی به تقلب، امنیت یا مشکلات فنی کشف.

-محافظت در برابر آسیب به حقوق، اموال یا امنیت گوگل، کاربران ما یا عموم.

پلتفرم متا (فیس‌بوک)

شرکت متا پلتفرمز، که در ابتدا با نام فیسبوک، در فوریه ۲۰۰۴ تأسیس شد، از یک پلتفرم ساده شبکه‌های اجتماعی به یک غول چندملیتی فناوری با حضور قوی در سطح جهانی تبدیل شده است. تأسیس این شرکت انقلابی در نحوه تعامل و برقراری ارتباط افراد به صورت آنلاین ایجاد کرد و راه را برای عصر رسانه‌های اجتماعی هموار ساخت.

زیرمجموعه‌های اصلی متا شامل چندین برنامه و پلتفرم پرکاربرد است، از جمله

۱. فیسبوک یک پلتفرم شبکه‌های اجتماعی که به کاربران امکان ایجاد پروفایل، برقراری ارتباط با دوستان و خانواده، به اشتراک گذاری محتوا و مشارکت در جوامع آنلاین را می‌دهد.

۲. اینستاگرام یک پلتفرم اشتراک گذاری عکس و ویدیو که بر محتوای بصری تمرکز دارد و به کاربران امکان ایجاد، به اشتراک گذاری و تعامل با پست‌های دیگران را می‌دهد.

۳. واتس‌اپ یک سرویس پیام‌رسان فوری و صدا روی پروتکل اینترنت که از چند پلتفرم پشتیبانی می‌کند و به کاربران امکان برقراری ارتباط امن از طریق پیام‌های متنی، تماس‌های صوتی و تصویری را می‌دهد.

۴. مسنجر یک برنامه پیام‌رسان مستقل که با فیسبوک ادغام شده و به کاربران امکان برقراری ارتباط، به اشتراک گذاری محتوا و برقراری تماس صوتی یا تصویری با مخاطبین فیسبوک خود را می‌دهد.

در اکتبر ۲۰۲۱، فیسبوک، تغییر نام تجاری قابل توجهی را تجربه کرد و نام شرکتی خود را به متا پلتفرمز تغییر داد. این تغییر در هویت به منظور نشان دادن تمرکز فزاینده شرکت بر ساخت متاورس – یک محیط مجازی و فراگیر که رسانه‌های اجتماعی، واقعیت افزوده و واقعیت مجازی را ترکیب می‌کند – انجام شد.

در طول فرآیند تکامل متا، این شرکت همواره بر اهمیت حریم خصوصی کاربر و حفاظت از داده‌ها تأکید کرده است. با افزایش نگرانی‌ها در مورد حریم خصوصی دیجیتال، متا تلاش‌هایی را برای بهبود کنترل‌های حریم خصوصی در پلتفرم‌های خود انجام داده است تا اطمینان حاصل شود که کاربران کنترل بیشتری روی اطلاعات شخصی خود و نحوه به اشتراک

گذاری آن دارند. تعهد مستمر این شرکت به حریم خصوصی و امنیت نقش اساسی در ایجاد اعتماد کاربر و حفظ یکپارچگی پلتفرم‌های دیجیتال آن دارد.

حریم خصوصی در متا

به طور کلی حریم خصوصی یکی از زیرمجموعه‌های بخش شرایط ارائه خدمت در پلتفرم‌های متا است. دو بخش مرکز حریم خصوصی و سیاست حریم خصوصی عمده‌ترین محل‌هایی هستند که می‌توانیم سیاست کلی حریم خصوصی متا را درک کنیم. مارک زاکربرگ فیس بوک را بر اساس این ایده تأسیس کرد که برقراری ارتباط با افراد اساساً چیز خوبی است – و راهی برای کسب سود خوب. اما از همان ابتدا، فیس‌بوک هم به خاطر نحوه مدیریت حریم خصوصی کاربران و هم به خاطر نحوه مدیریت محتوای تولید شده توسط کاربر مورد انتقاد قرار گرفت. این دو موضوع پس از انتخابات ریاست‌جمهوری ایالات متحده در سال ۲۰۱۶، پس از نقش فیس‌بوک در انتشار اطلاعات نادرست سیاسی و نشت اطلاعات کاربران فیس‌بوک به شرکت‌های مشاوره سیاسی، با هم ادغام شدند (یافی و فیشر، ۲۰۲۰).

شرکت متا در موارد متعدد به اتهام نقض محرمانگی داده‌ها جریمه شده است. ازجمله در این شرکت در سال ۲۰۲۳ به دلیل نقض قوانین حفاظت از داده اتحادیه اروپا، مبلغ ۲.۱ میلیارد یورو (۳.۱ میلیارد دلار) جریمه شد و ملزم به توقف انتقال داده‌های جمع‌آوری‌شده از کاربران فیس‌بوک در اروپا به ایالات متحده شد (ساتاریانو، ۲۰۲۳). همچنین مهمترین مورد نقض حریم خصوصی کاربران توسط فیس‌بوک، رسوایی کمبریج آنالتیکا است که طی آن اطلاعات شخصی کاربران این پلتفرم برای کارزارهای انتخاباتی مورد استفاده قرار گرفت.

دو بخش اساسی در مرکز حریم خصوصی متا شامل موضوعات حریم خصوصی و نیز سیاست یا خط‌مشی حریم خصوصی است که مورد بررسی قرار خواهیم داد. علاوه بر این در بخش درباره متا نیز اسناد و اطلاعاتی درباره خط‌مشی حریم خصوصی متا قابل مشاهده است که در مورد آنها نیز بحث خواهد شد. بحث ما با مراجعه به این بخش آغاز می‌شود.

اصول بنیادین متا

میشل پراتی (۲۰۲۲)، مدیر ارشد حریم خصوصی متا، مطلبی را در سایت متا نوشته و در آن در مورد بروزرسانی حریم خصوصی و شرایط ارائه خدمت این پلتفرم توضیحاتی را بیان کرده است

از امروز، متا اعلان‌هایی را منتشر می‌کند تا به کاربران اطلاع دهد که ما «سیاست حریم خصوصی» خود را که قبلاً به عنوان «سیاست داده» شناخته می‌شد، به‌روزرسانی کرده‌ایم. ما با الهام از بازخورد کاربران فناوری‌های ما و کارشناسان حریم خصوصی، سیاست حریم خصوصی خود را بازنویسی کرده‌ایم تا درک آن آسان‌تر شود و محصولات جدیدی را که ارائه می‌دهیم منعکس کند. در حالی که متن در بسیاری از نقاط متفاوت به نظر می‌رسد، متا بر اساس این به‌روزرسانی سیاست، داده‌های شما را به روش‌های جدید جمع‌آوری، استفاده یا به اشتراک نمی‌گذارد و ما همچنان اطلاعات شما را نمی‌فروشیم (پراتی، ۲۰۲۲).

چند نکته از این نوشته قابل فهم است. نخست اینکه متا سیاست حریم خصوصی خود را از داده به حریم خصوصی تغییر داده است که البته علت آن بیان نشده است. دوم اینکه، ساده‌سازی ادبیات حریم خصوصی برای قابل فهم‌تر شدن آن برای عموم کاربران این پلتفرم است و تأکید بر اینکه متا داده‌های کاربران را با دیگران به اشتراک نمی‌گذارد و نمی‌فروشد. به ظاهر، این موضوع در راستای انتقادها نسبت به انتشار و فروش داده‌های کاربران بیان شده است.

پراتی (۲۰۲۴) همچنین در مطلبی درباره سرمایه‌گذاری متا در حریم خصوصی سخن گفته است. «از سال ۲۰۱۹، ۵.۵ میلیارد دلار در برنامه حفظ حریم خصوصی خود سرمایه گذاری کرده‌ایم و تیم‌های متمرکز بر حفظ حریم خصوصی را به بیش از ۳۰۰۰ نفر افزایش داده‌ایم». یکی از اقدامات متا برای ارتقاء حریم خصوصی ایجاد *زیرساخت آگاه نسبت به حریم خصوصی*[1] است که متخصصان این شرکت امکان می‌دهد تا به هنگام تولید محصولات به شکلی آسان‌تر الزامات مرتبط با حریم خصوصی را مدنظر قرار دهند. یک موضوع کلیدی دیگر تولید محصولاتی که در آنها از ابتدا به حریم خصوصی[2] توجه می‌شود. این رویکرد شامل استفاده از رمزگذاری پایان به پایان[3] برای پیام‌های شخصی و برقراری در مسنجر و فیس‌بوک

[1] .privacy-aware infrastructure
[2] .Privacy-First Products
[3] .default end-to-end encryption

است که ارتباط نزدیکی با مفهوم حریم خصوصی بر اساس طراحی دارد (پراتی، ۲۰۲۴) که پیشتر در مورد گوگل درباره آن بحث کردیم.

- اصول بنیادین حریم خصوصی متا

گرچه به طور خاص بخشی به بیان اصول بنیادین متا درباره حریم خصوصی اختصاص نیافته است اما در بخش به‌روزرسانی بهبود حریم خصوصی[1] بیان شده است که برای توسعه محصولات، خدمات و کردارهای جدید برخی ملاحظات راهنما درباره حریم خصوصی وجود دارد. این اصول را می‌توان به‌منزله اصول راهنمای متا نسبت به حریم خصوصی در نظر گرفت

محدودیت هدف پردازش داده تنها برای اهداف محدود و مشخص که برای مردم ارزش ایجاد می کند، انجام شود.

کاهش داده حداقل میزان داده مورد نیاز برای پشتیبانی از اهداف مشخص، جمع آوری و ایجاد شود.

نگهداری داده ها تنها تا زمانی که برای پشتیبانی از اهداف مشخص، واقعاً مورد نیاز هستند، نگهداری شوند.

سوء استفاده خارجی از داده محافظت از داده در برابر سوء استفاده، از دست رفتن تصادفی و دسترسی اشخاص ثالث غیرمجاز.

شفافیت و کنترل رفتار محصول و شیوه های داده را به طور پیشگیرانه، واضح و صادقانه اطلاع رسانی کنید. در صورت امکان و مناسب بودن، به مردم کنترل بر شیوه های ما بدهید.

دسترسی و مدیریت داده به افراد امکان دسترسی و مدیریت داده هایی را که در مورد آنها جمع آوری یا ایجاد کرده ایم، بدهید (به‌روزرسانی بهبود حریم خصوصی، ۲۰۲۴).

بنابراین اصولی کلی همانند تقلیل داده، کاربرد هدفمند و محدود داده‌ها، جلوگیری از دسترسی خارجی به داده‌ها، شفافیت، فراهم کردان امکان کنترل داده‌ها را می‌توان به عنوان اصول بنیادین حفاظت از محرمانگی داده‌ها در متا در طراحی محصولات بیان کرد. حکمرانی متا درباره حریم خصوصی مبتنی بر این اصول است.

از منظری دیگر، رویکرد متا به حریم خصوصی توسط چندین اصل اساسی هدایت می‌شود که محصولات، خدمات و تجربه کاربری آن را شکل می‌دهد. این اصول عبارتند از

[1] . Privacy progress update

کنترل و شفافیت کاربر: متا تلاش می کند تا ابزارهای آسان برای استفاده و اطلاعات شفاف در مورد تنظیمات حریم خصوصی را در اختیار کاربران قرار دهد تا آنها را قادر سازد تا انتخاب های آگاهانه در مورد داده های خود داشته باشند امنیت متا با سرمایه گذاری در فناوری های پیشرفته و بهترین شیوه ها برای محافظت در برابر دسترسی غیرمجاز و سوء استفاده بالقوه، امنیت داده های کاربر را در اولویت قرار می‌دهد.

تقلیل داده: متا به دنبال جمع آوری و نگهداری تنها اطلاعاتی است که برای ارائه خدمات و ارائه تجربیات شخصی سازی شده ضروری است. این رویکرد به حداقل رساندن افشای بالقوه داده های حساس کمک می‌کند.

پاسخگویی و انطباق: متا خود را مسئول رعایت مقررات، قوانین و استانداردهای صنعتی حریم خصوصی می داند و همچنین با تنظیم کننده ها و ذینفعان برای اطمینان از حفظ حریم خصوصی کاربران همکاری می‌کند.

حفظ حریم خصوصی از طریق طراحی و به صورت پیش‌فرض: متا ملاحظات مربوط به حریم خصوصی را در فرآیند توسعه محصولات و خدمات جدید ادغام می کند تا حریم خصوصی را از همان ابتدا به عنوان یک جنبه اساسی از محصولات خود قرار دهد.

منافع کاربر: متا در عین احترام و محافظت از حریم خصوصی کاربران، تلاش می کند تا تجربیات کاربری ارزشمند و خدمات شخصی سازی شده ایجاد کند. این شرکت به دنبال ایجاد تعادل بین نوآوری و حفظ حریم خصوصی است

بهبود مستمر: متا اذعان دارد که حریم خصوصی یک تعهد مستمر است و دائماً رویه ها، سیاست ها و فناوری های خود را برای رسیدگی به چالش های نوظهور حریم خصوصی ارزیابی و تکامل می بخشد.

با پایبندی به این اصول اساسی حریم خصوصی، متا هدف خود را بر ایجاد یک محیط آنلاین خصوصی‌تر و امن‌تر برای کاربران خود، تقویت اعتماد و ارتقای کلی تجربه کاربری در سراسر پلتفرم های خود قرار داده است (متا، ۲۰۲۳).

برخی از اصول بنیادین که در اینجا به آن اشاره شده است، ازقبیل تقلیل داده‌ها، کنترل کاربران، حفظ حریم خصوصی از طریق و به شکل پیش‌فرض ازجمله اصولی هستند که در پلتفرم متا مورد تأکید قرار دارد و در گوگل نیز بر آنها تأکید شده بود.

حریم خصوصی و امنیت در متا

بخشی از رویکرد کلی متا به حریم خصوصی در این بخش قابل مشاهده است. همانطور که در صفحه این بخش مشاهده می‌کنیم، متا ادعا می‌کند

ما متعهد هستیم که به شما کنترل حریم شخصی و محافظت از اطلاعاتتان را بدهیم تا بتوانید از تجربیات باارزش خود در محصولات ما لذت ببرید. به همین دلیل است که ما ابزارهایی را برای کمک به شما در ایمن سازی اطلاعاتتان و انتخاب های درست در زمینه حفظ حریم شخصی، با رعایت استانداردهای سختگیرانه صنعت برای حفظ حریم شخصی و محافظت از داده هایتان، ساخته ایم (حفاظت از حریم خصوصی و داده متا، ۲۰۲۴).

دو نکته محوری در این مطلب کوتاه قابل توجه است. نخست تأکید بر اینکه کاربران توانایی *اعمال کنترل* بر حریم خصوصی خود را دارند. موضوعی که مورد تأکید پلتفرم گوگل نیز هست. نکته دوم، توسعه *فناوری‌های حفظ حریم خصوصی* است. حفظ حریم خصوصی و محرمانگی داده‌ها در پلتفرم‌ها، مستلزم توسعه فناوری‌های متناسب است. پلتفرم‌ها باید متعهد شوند تا از تمام ابزارها برای حفاظت از حریم خصوصی کاربرانشان استفاده کنند و این یک روند مستمر و الزام تعهدآور است.

موضوعات حریم خصوصی

موضوعات مرتبط با حریم خصوصی شامل ایمنی، امنیت حساب کاربری، مخاطب، موقعیت جغرافیایی، تبلیغات، گردآوری اطلاعات و نحوه کاربرد اطلاعات است.

-اهمیت ایمنی در حریم خصوصی

نخستین بخش از موضوعات حریم خصوصی متا ایمنی است. ایمنی امکانات کاربرد اعمال کنترل بر اشتراک‌گذاری اطلاعات شخصی را در اختیار کاربرد قرار می‌دهد. در این بخش کاربران می‌توانند محدودیت‌هایی را برای اینکه چه کسانی می‌توانند اطلاعات به اشتراک‌گذاشته شده توسط آنها را مشاهده کنند، اعمال نمایند. همچنین افراد می‌توانند از پیامها و

اطلاعات شخصی خود محافظت کنند. همچنین اگر کاربران مورد آزار و قلدری قرار می‌گیرند می‌توانند مورد حمایت شرکت متا قرار بگیرند. بنابراین مضمون محوری در این بخش *مدیریت اشتراک‌گذاری اطلاعات توسط کاربر* است.

دو بخش حائزاهمیت دیگر نحوه گردآوری داده و نحوه استفاده از داده‌های شخصی است. در این بخش نخست، کاربر می‌تواند اطلاعاتی را که متا درباره او گردآوری می‌کند مشاهده و مدیریت کند. در بخش استفاده توضیح داده شده است که کاربر در این بخش یاد می‌گیرند متا با اطلاعاتی که درباره کاربر گردآوری می‌کند و یا اطلاعاتی را درباره او دریافت می‌کند چه می‌کند. آگاهی بیشتر درباره این کردارهای حریم خصوصی به سیاست حریم خصوصی گوگل ارجاع داده شده است.

سیاست حریم خصوصی متا

سیاست و خط‌مشی حریم خصوصی در ۲۶ ژوئن ۲۰۲۴ به روزرسانی شده است. در ابتدای این گزارش آمده است: «ما در متا از شما می‌خواهیم که بدانید چه اطلاعاتی را جمع‌آوری می‌کنیم و چگونه از آن استفاده می‌کنیم و به اشتراک می‌گذاریم» (سیاست حریم خصوصی متا، ۲۰۲۴). بر این اساس می‌توان گفت که هدف از این سند بیان کردارهای متا درباره نحوه گردآوری داده‌های کاربران، چگونگی استفاده از آن و نیز نحوه اشتراک‌گذاری این محتواها است. همچنین هدف این حریم خصوصی آگاه کردن کاربران از حقوق‌شان نسبت به حریم داده‌هایشان است. علاوه بر این، همانطور که متا می‌گوید: «برای ما مهم است که بدانید چگونه حریم خصوصی خود را کنترل کنید، بنابراین به شما نشان می دهیم کجا می توانید اطلاعات خود را در تنظیمات محصولات متا که استفاده می کنید مدیریت کنید» (سیاست حریم خصوصی متا، ۲۰۲۴). بنابراین، نکته‌ای که در اینجا بر آن تأکید می‌شود، *امکان کنترل کاربر بر حریم خصوصی خود* است.

ما در اینجا برای فهم سیاست حریم خصوصی متا در موارد کلیدی فوق آنها را در مقوله‌های جداگانه مورد بررسی قرار می‌دهیم.

اطلاعات گردآوری شده در متا

یکی از بخش‌های اصلی سیاست حریم خصوصی داده از منظر امنیت اطلاعات، آگاهی از اطلاعاتی است که متا درباره کاربران گردآوری می‌کند. شناخت این گستره این این اطلاعات نشان می‌دهد که شرکت متا چه میزان بر داده‌های ما

دسترسی دارد. یک نکته مهم دیگر این است که گردآوری اطلاعات در متا مبتنی بر محصول مورد استفاده است. یعنی « اگر مبلمان‌تان را در بازار بفروشید، اطلاعات متفاوتی نسبت به ارسال یک ریل در اینستاگرام جمع آوری می‌کنیم» (سیاست حریم خصوصی متا، ۲۰۲۴).

چیستی اطلاعات	انواع اطلاعات گردآوری شده	جزییات اطلاعات
گردآوری شده	-فعالیت و اطلاعاتی که کاربران ارائه می‌کنند:	محتوائی که شما ایجاد می کنید، مانند پست ها، نظرات یا صدا محتوایی که از طریق ویژگی دوربین ما یا تنظیمات رول دوربین خود یا از طریق ویژگی‌های صوتی ما ارائه می‌دهید. درباره آنچه از این ویژگی‌ها جمع‌آوری می‌کنیم و نحوه استفاده از اطلاعات دوربین برای ماسک‌ها، فیلترها، آواتارها و افکت‌ها بیشتر بدانید. پیام‌هایی که ارسال و دریافت می‌کنید، از جمله محتوای آنها، با رعایت قوانین قابل اجرا. ما نمی توانیم محتوای پیام های رمزگذاری شده سرتاسر را ببینیم مگر اینکه کاربران آنها را برای بررسی به ما گزارش دهند. بیشتر بدانید. داده های متا در مورد محتوا و پیام ها، با رعایت قوانین قابل اجرا انواع محتوا، از جمله تبلیغاتی که مشاهده یا با آنها تعامل دارید و نحوه تعامل شما با آنها برنامه‌ها و ویژگی‌هایی که استفاده می‌کنید و اقداماتی که در آن‌ها انجام می‌دهید. نمونه ها را ببینید. خریدها یا سایر تراکنش‌هایی که انجام می‌دهید، مانند

		خرید از طریق متا، از جمله اطلاعات کارت اعتباری. بیشتر بدانید. هشتگ هایی که استفاده می کنید زمان، فرکانس و مدت فعالیت های شما در محصولات ما

	–دوستان، دنبال‌کنندگان و رابطه‌های دیگر	ما در مورد دوستان، دنبال کنندگان، گروه ها، حساب ها، صفحات فیسبوک و سایر کاربران و جوامعی که به آنها متصل هستید و با آنها تعامل دارید، اطلاعات جمع آوری می کنیم. این شامل نحوه تعامل شما با آنها در سراسر محصولات ما و اینکه با کدام یک بیشتر تعامل دارید، می شود. اطلاعاتی که در مورد مخاطبین جمع آوری می کنیم ما همچنین اطلاعات مخاطبین شما را مانند نام و آدرس ایمیل یا شماره تلفن آنها جمع آوری می کنیم، در صورتی که انتخاب کنید آنها را از یک دستگاه دیگر آپلود یا وارد کنید، مانند همگام سازی دفترچه آدرس. اگر از محصولات متا استفاده نمی کنید یا بدون حساب کاربری از آنها استفاده می کنید، ممکن است اطلاعات شما همچنان جمع آوری شود. در مورد نحوه استفاده متا از اطلاعات تماس آپلود شده توسط دارندگان حساب، بیشتر بدانید. نحوه آپلود و حذف مخاطبین در فیسبوک و اینستاگرام یا نحوه اتصال لیست مخاطبین دستگاه خود در فیسبوک را بیاموزید. اطلاعاتی که بر اساس فعالیت دیگران در مورد شما جمع آوری یا استنتاج می کنیم

		ما بر اساس فعالیت دیگران، اطلاعاتی در مورد شما جمع آوری می کنیم. ما همچنین بر اساس فعالیت دیگران چیزهایی در مورد شما استنتاج می کنیم. برای مثال: ممکن است از طریق ویژگی «افرادی که ممکن است بشناسید» فیسبوک، دوستی را به شما پیشنهاد کنیم، اگر هر دوی شما در لیست مخاطبینی ظاهر شوید که شخصی آن را آپلود کرده است. هنگامی که پیشنهاد می کنیم به یک گروه بپیوندید، در نظر می گیریم که آیا دوستان شما به آن گروه تعلق دارند یا خیر.
	اپ (کارافزار)، مرورگر و اطلاعات وسیله	

		اطلاعاتی که در مورد دستگاه شما جمع‌آوری و دریافت می‌کنیم شامل موارد زیر است: دستگاه و نرم‌افزاری که استفاده می‌کنید، و سایر مشخصات دستگاه. کاری که روی دستگاه خود انجام می‌دهید، مانند اینکه آیا برنامه ما در حال اجرا است یا خیر و یا اینکه آیا ماوس شما در حال حرکت است (که می‌تواند به تشخیص انسان از ربات کمک کند). شناسه‌هایی که دستگاه شما را از دستگاه‌های کاربران دیگر متمایز می‌کند، از جمله شناسه‌های دستگاه خانواده. سیگنال‌های ارسال‌شده از دستگاه شما. اطلاعاتی که از طریق تنظیمات دستگاه با ما به اشتراک گذاشته‌اید، مانند موقعیت مکانیGPS ، دسترسی به دوربین، عکس‌ها و موارد دیگر. اطلاعات مربوط به شبکه‌ای که دستگاه خود را به آن متصل می‌کنید و اتصال شما، از جمله آدرس IP شما. برخی از اطلاعات موقعیت مکانی، حتی در صورتی که خدمات موقعیت مکانی در تنظیمات دستگاه شما خاموش باشد. این شامل استفاده از آدرس‌های IP برای تخمین موقعیت مکانی کلی شما است. اطلاعات مربوط به عملکرد محصولات ما روی دستگاه شما. اطلاعات حاصل از کوکی‌ها و فناوری‌های مشابه.

	اطلاعات از شرکا، فروشندگان و سایر طرفهای ثالث	ما اطلاعاتی را از منابع مختلف شامل شرکا، موسسات نظرسنجی و بازاریابی در مورد فعالیت‌ها و اطلاعات متنوع شما در داخل و خارج از محصولات خود جمع‌آوری و دریافت می‌کنیم. در اینجا چند نمونه از اطلاعاتی که در مورد شما دریافت می‌کنیم آورده شده‌است: اطلاعات تماس شما وب‌سایت‌هایی که بازدید می‌کنید و داده‌های کوکی، مانند پلاگین‌های اجتماعی یا پیکسل متا اپلیکیشن‌هایی که استفاده می‌کنید بازی‌هایی که انجام می‌دهید خریدها و تراکنش‌هایی که خارج از محصولات ما با استفاده از روش‌های پرداخت غیر از متا انجام می‌دهید اطلاعات جمعیت‌شناختی شما، مانند سطح تحصیلات تبلیغاتی که می‌بینید و نحوه تعامل شما با آنها نحوه استفاده شما از محصولات و خدمات شرکای ما، به صورت آنلاین یا حضوری هم چنین اطلاعاتی مانند آدرس ایمیل، و شناسه دستگاه تبلیغاتی را با ما به اشتراک می‌گذارند. این به ما

		کمک می‌کند فعالیت‌های شما را با حساب کاربری‌تان، در صورت داشتن حساب، مطابقت دهیم. ما این اطلاعات را دریافت می‌کنیم، چه وارد حساب کاربری خود شده باشید یا در محصولات ما حساب کاربری داشته باشید. در مورد نحوه اتصال اطلاعات از شرکا به حساب کاربری خود را بخوانید. همچنین شرکا در صورتی که به ما دستور دهند خدماتی را به کسب و کارشان ارائه دهیم، مانند کمک به مدیریت ارتباطاتشان، ارتباطات خود را با شما با ما به اشتراک می‌گذارند. برای اینکه بدانید یک تجارت

جدول ۴-۴) انواع اطلاعات گردآوری‌شده توسط متا

همانطور که جدول ۴-۴ نشان می‌دهد داده‌های که متا درباره کاربران خود گردآوری می‌کند طیف بسیار گسترده‌ای از داده‌ها را دربرمی‌گیرد و تمامی کنش‌ها و فعالیت‌های ما زیرنظر شرکت متا قرار دارد.

نحوه استفاده از اطلاعات گردآوری شده توسط متا

متا برای ارائه یک تجربه شخصی‌شده برای کاربران ازجمله برای شخصی‌سازی آگهی‌ها و نیز به دلایل گوناگون از اطلاعات گردآوری شده از کاربران استفاده می‌کند. به این منظور متا هم از اطلاعاتی که کاربران در محصولات مختلف این کشور ارائه کرده‌اند و نیز اطلاعاتی که از طریق وسایل ارتباطی کاربران قابل دسترسی است استفاده می‌کنند. با وجود این متا مدعی است که این شرکت برای اینکه از اطلاعاتی که مربوط به یکایک کاربران است کمتر استفاده کند، از این اطلاعات هویت‌زدایی می‌کند و یا آنها را انبوهه‌سازی[1] می‌کند تا قابل شناسایی نباشند. بنابراین یک رویکرد برای حفاظت از

[1] .aggregate

داده‌های شخصی کاربران *ناشناس‌سازی و یا تقلیل داده‌ها* است. در جدول ۵-۴) نحوه استفاده از اطلاعات توسط متا نشان داده شده است.

نحوه استفاده از اطلاعات گردآوری شده	**برای ارائه محصولات، شخصی‌سازی و بهبود محصولاتمان**	ما از اطلاعاتی که داریم برای ارائه و بهبود محصولات و خدمات خود استفاده می‌کنیم. این شامل شخصی‌سازی ویژگی‌ها، محتوا و تبلیغات، مانند جستجوهای شما، علایق، استوری‌ها و تبلیغاتی که می‌بینید، می‌شود. ما از اطلاعاتی که شما انتخاب می‌کنید برای این اهداف استفاده می‌کنیم، اما از آن‌ها برای نمایش تبلیغات به شما استفاده نمی‌کنیم.
	برای ارتقای امنیت، حفاظت و یکپارچگی	ما از اطلاعاتی که جمع‌آوری می‌کنیم برای کمک به محافظت از افراد در برابر آسیب و ارائه محصولات امن و مطمئن استفاده می‌کنیم.
	برای ارائه خدمات اندازه‌گیری، تحلیل و کسب‌وکار	بسیاری از افراد برای اداره یا تبلیغ کسب و کار خود به محصولات ما اعتماد می‌کنند. ما به آن‌ها کمک می‌کنیم تا میزان اثربخشی تبلیغات و سایر محتوا، محصولات و خدماتشان را بسنجند.
	برای برقراری ارتباط با شما	ما با استفاده از اطلاعاتی که به ما داده‌اید،

		مانند اطلاعات تماس که در پروفایل خود وارد کرده‌اید، با شما ارتباط برقرار می‌کنیم.
	برای تحقیق و نوآوری برای خیر اجتماعی	برای انجام و پشتیبانی از پژوهش، از اطلاعات موجود خود، اطلاعات حاصل از پژوهشگران و مجموعه داده‌های منابع در دسترس عموم، گروه‌های حرفه‌ای و گروه‌های غیرانتفاعی استفاده می‌کنیم.

جدول ۵-۴) نحوه استفاده از اطلاعات توسط متا

نحوه اعمال حقوق کاربران توسط متا درباره حریم خصوصی

متا برای فراهم کردن اعمال حق حریم خصوصی توسط کاربران، امکانّ‌های مختلفی را برای مدیریت یا حذف اطلاعات کاربران فراهم کرده است. متا امکان مشاهده، مدیریت، بارگیری و نیز حذف اطلاعات توسط کاربران را فراهم کرده است. یکی از امکان‌های مدیریت اطلاعات در متا، مشاهده تنظیمات هرکدام از محصولات متا است.

مبنای قانونی پردازش اطلاعات کاربران

بر اساس قوانین موضوعه برای حفاظت از داده‌ها، شرکتها برای پردازش اطلاعات شخصی باید بر مبنای مفاد قاناونی عمل کنند. منظور از پردازش داده‌های شخصی، روشهای گردآوری، استفاده و اشتراک‌گذاری داده‌های کاربران است که در سیاست حریم خصوصی متا بیان شده است.

مبنای حقوقی پردازش اطلاعات

همانگونه در سیاست حریم خصوصی متا مشاهده می‌شود، متا برای پردازش اطلاعات کاربران به قانون تکیه می‌کند تا اعمال خود را قانونی جلوه دهد:

ما برای پردازش اطلاعات شما برای اهداف شرح داده شده در این خط مشی رازداری به پایه‌های قانونی مختلفی متکی هستیم. بسته به شرایط، ما هنگام پردازش اطلاعات مشابه شما برای اهداف مختلف، به پایه‌های قانونی متفاوتی تکیه می‌کنیم. برای هر پایه قانونی در زیر، توضیح می‌دهیم که چرا اطلاعات شما را پردازش می‌کنیم. همچنین بسته به اینکه از کدام پایه قانونی استفاده می‌کنیم، حقوق خاصی برای شما در نظر گرفته شده است که ما در اینجا آنها را توضیح داده‌ایم. صرف نظر از اینکه چه پایه قانونی اعمال شود، شما همیشه حق دسترسی، اصلاح و حذف اطلاعات خود را دارید (سیاست حریم خصوصی متا، ۲۰۲۴).

-رضایت کاربران

مبانی قانونی پردازش اطلاعات کاربران فیس‌بوک بر چند محور استوار است. نخست قراردادی است که کاربران به هنگام عضویت در هرکدام از خدمات متا امضاء می‌کنند. ازجمله آنها می‌توان به شرایط ارائه خدمت، شرایط ارائه خدمت اینستاگرام، شرایط ارائه خدمت در فناوری‌های تکمیلی پلتفرم‌های متا، شرایط ارائه خدمت پرتال تکمیلی و شرایط ارائه خدمت نگرش تکمیلی فیس‌بوک[1]اشاره کرد که درمجموع شرایط ارائه خدمت نامیده می‌شوند. یکی مبنای قانونی دیگر *رضایت کاربران* است:

ما اطلاعات شما را در صورت رضایت شما پردازش می کنیم. برای مثال، شما می توانید به ما اجازه دهید تا تبلیغات شخصی سازی شده را بر اساس اطلاعاتی که تبلیغ کنندگان و دیگران به ما ارائه می دهند، به شما نشان دهیم. این شامل اطلاعات مربوط به فعالیت شما در وب سایت ها و برنامه های آنها و همچنین برخی تعاملات آفلاین مانند خرید است. شما می توانید رضایت خود را در هر زمان پس بگیرید (سیاست حریم خصوصی متا، ۲۰۲۴).

-منافع مشروع

چند مبنای قانونی دیگر برای پردازش اطلاعات وجود دارد. یکی از آنها *منافع مشروع* است. این منافع مشروع می‌تواند برای شرکت متا یا طرف‌های دیگر باشد. منافع شامل ارائه خدمتی نوآورانه، شخصی‌شده، ایمن و سودمند برای کاربران و شرکای متا و نیز پاسخگویی به درخواستهای حقوقی است. *اجبار قانونی* یک عامل دیگر است. درصورت درخواست نهادهای قانونی

[1] .Supplemental Facebook View Terms of Service

متا نسبت به پردازش اطلاعات کاربران اقدام می‌کند. *منفعت عمومی* یک مبنای قانونی دیگر به شمار می‌رود. برخی از این منافع عمومی شامل مواردی همانند انجام پژوهش یا ارتقاء ایمنی، امنیت یا همبستگی است.

درخواست‌های قانونی یکی از دلایل افشاء یا انتشار داده‌های کاربران است. در واکنش به درخواست‌های قانونی، همانند دستور دادگاه که از سوی نهادهای مختلف ازجمله مقامات دولتی صادر می‌شود، متا به این درخواست‌ها پاسخ می‌دهد.

آنچه گفته شد، تلاش درجهت ارائه تصویری از رویکرد و اقدامات متا برای حفاظت از حریم شخصی و داده‌های کاربرانش است. به طور کلی این شرکت مدعی است که افراد در طراحی محصولات این شرکت در اولویت قرار دارند (فیشر، ۲۰۲۲) و تلاش می‌شود تا حفاظت از حریم خصوصی بر اساس طراحی به پیش برود.

اعمال مقررات مرتبط با سیاست‌ها در متا

شرکت متا مجموعه‌ای از رویه‌ها را برای اعمال مقررات مرتبط با سیاستها ازجمله حریم خصوصی تعبیه کرده است که درکل ذیل تعدیل محتوا قابل فهم است. متا برای شناسایی، بررسی و اقدام نسبت به میلیون‌ها محتوا در فیس‌بوک و اینستاگرام هر روز از فناوری و تیم‌های بررسی‌کننده استفاده می‌کند. فناوری و تیم‌های بررسی به متا کمک می‌کنند تا محتوا و حساب‌های کاربری که بالقوه ناقض قوانین هستند را شناسایی و بررسی کنند. متا از یک رویکرد سه بخشی برای اعمال مقرارت در مورد محتوا استفاده می‌کند: حذف، کاهش و اطلاع‌رسانی. روشن است که این موضوع در مورد محتواهای ناقض حریم خصوصی نیز مصداق دارد.

بخش اول شامل حذف است. همانطور که در مرکز شفافیت متا آمده است:

اگر محتوای شما مغایر با استانداردهای انجمن فیس‌بوک یا دستورالعمل‌های انجمن اینستاگرام باشد، متا آن را حذف خواهد کرد. ما همچنین به شما اطلاع خواهیم داد تا بتوانید دلیل حذف محتوا و نحوه جلوگیری از ارسال محتوای نقض‌کننده در آینده را درک کنید. ما از یک سیستم امتیازدهی برای شمارش تخلفات و مسئول نگه داشتن شما در قبال محتوایی که ارسال می‌کنید استفاده می‌کنیم. بسته به اینکه محتوای شما با کدام خط‌مشی مغایرت دارد، سوابق قبلی تخلفات شما و تعداد امتیازهایی که دارید، حساب کاربری شما نیز ممکن است محدود یا غیرفعال شود (مرکز شفافیت متا، ۲۰۲۳).

بخش دوم کاستن از میزان انتشار محتوای مسئله‌دار است:

اگرچه محتوایی در فیسبوک، معیارهای انجمن فیسبوک را نقض نکند، اما همچنان ممکن است مشکل‌ساز یا به نوعی کم‌کیفیت باشد، متا می‌تواند توزیع آن را مطابق با کنترل‌های کاربر کاهش دهد. این، یکی از اجزای استراتژی کلی «حذف، کاهش، اطلاع‌رسانی» ماست که از سال ۲۰۱۶ به کار می‌بریم (مرکز شفافیت متا، ۲۰۲۳).

بخش سوم، اطلاع‌رسانی یا آگاهانیدن کاربران نسبت به یک محتوای خاص است:

یکی از روش‌هایی که متا جامعه امن و واقعی را ترویج می‌کند، اطلاع رسانی به افراد در مورد اینکه محتوا ممکن است حساس یا گمراه‌کننده باشد، حتی اگر صراحتا با استانداردهای انجمن فیسبوک یا دستورالعمل‌های انجمن اینستاگرام مغایرت نداشته باشد، است. در چنین مواقعی، ما زمینه بیشتری در مورد محتوا اضافه می‌کنیم تا به مردم در تصمیم‌گیری برای خواندن، اعتماد یا به اشتراک گذاشتن آن کمک کنیم (مرکز شفافیت متا، ۲۰۲۳).

در مجموع می‌توان گفت که یکی از پیشروترین و پیچیده‌ترین سازوکارهای مرتبط با حریم خصوصی و داده در متا مشاهده می‌شود. هرچند با وجود تمام این اسناد و اقدامات، متا همواره در معرض اتهام نقض حریم خصوصی کاربرانش قرار داشته است.

پلتفرم ایکس

توییتر، که اکنون با نام جدید ایکس شناخته می‌شود، یک پلتفرم پویای شبکه‌های اجتماعی است که به طور قابل توجهی نحوه ارتباط و به اشتراک گذاری اطلاعات مردم در سطح جهان را متحول کرده است. این پلتفرم که در سال ۲۰۰۶

راه‌اندازی شد، به ابزاری قدرتمند برای گفتگوهای لحظه‌ای، انتشار اخبار فوری و اتصال افراد از پیشینه‌های مختلف تبدیل شده است.

در ابتدا توییتر به عنوان پلتفرمی برای پیام‌های کوتاه یا توییت طراحی شد، ویژگی بارز آن توانایی تسهیل ارتباط مختصر و سریع بوده است، با محدودیت کاراکتر که کاربران را تشویق می‌کند تا افکار و اطلاعات را به طور خلاصه به اشتراک بگذارند. با گذشت زمان، توییتر قابلیت‌های چندرسانه‌ای را ادغام کرده است که به کاربران امکان می‌دهد برای غنی‌سازی محتوا و تعامل، تصاویر، ویدیوها و حتی پخش زنده را به اشتراک بگذارند.

حریم خصوصی در ایکس

قواعد و سیاستهای مرتبط با حریم خصوصی و داده در بخش حریم خصوصی ایکس[1] توضیح داده شده‌اند. این اسناد عبارتند از: شرایط ارائه خدمت، که قوانین کلی ایکس را توضیح می‌دهد و کارهایی که پلتفرم و کاربر می‌توانند انجام دهند را تشریح می‌کند؛ سیاست حریم خصوصی، که به کاربر کمک می‌کند تا داده‌هایی را که ایکس جمع آوری می‌کند، نحوه استفاده از آنها و زمان به اشتراک‌گذاری آنها را درک کند تا بتواند بهترین تصمیمات را در مورد اطلاعاتی که با ایکس به اشتراک می‌گذارید بگیرد؛ مطالب بیشتر درباره گردآوری داده، که به ایکس، «متن «سیاست حریم خصوصی» ما را تکمیل می‌کند و اطلاعات بیشتری در مورد نوع داده‌هایی که جمع‌آوری می‌کنیم، نحوه‌ی دریافت آن‌ها و چگونگی پردازش و اشتراک‌گذاری‌شان ارائه می‌دهد؛ مرکز کمک، «منابع اضافی مربوط به حفظ حریم خصوصی و امنیت که به شما کمک می‌کند تا نحوه استفاده از ایکس را بهتر درک کنید»؛ و و شرکای ما که اطلاعاتی درباره شرکت‌هایی که به ما کمک می‌کنند ارائه می‌کند.

شرایط ارائه خدمت که می‌توان آنرا سند اصلی هر پلتفرمی به شمار آورد، در پلتفرم ایکس، شامل حریم خصوصی نیز هست. به نوشته ایکس، شرایط ارائه خدمت «یک قرارداد الزام‌آور حقوقی است که نحوه استفاده کاربران از ایکس را مدیریت می‌کند» (شرایط ارائه خدمت ایکس، ۲۰۲۳). در اشرایط ارائه خدمت ایکس ذکر شده است که این شرکت حقوق گسترده‌ای برای اعمال قواعد خود دارد دارد و چنانچه کاربر شرایط را نقض کند این شرکت به اقدامات مختلفی دست می‌زند که

[1] .X Privacy (https://privacy.x.com/en)

ازجمله آنها می‌توان به حذف محتوا، کاهش میزان بازدید از آن، قطع دسترسی کاربر به ایکس یا اقدام حقوقی می‌توان اشاره کرد. این شرایط در مورد محتواهای ناقض حریم خصوصی نیز قابل اعمال است.

همانطور که در صفحه حریم خصوصی ایکس قابل مشاهده است[1]، ایکس خود را به قوانین مرتبط با حریم خصوصی و داده متعهد می‌داند که عبارتند از: مقررات عمومی حفاظت از داده‌ها، قانون حریم خصوصی مشتریان کالیفرنیا[2] و الحاقیه پردازش داده[3].

رویکرد ایکس به حریم خصوصی

به نحوی قابل توجه، ایکس رویکرد خود به حریم خصوصی را در صفحه مرتبط با مقررات عمومی حفاظت از داده‌ها توضیح داده شده است[4]:

حفاظت و دفاع از حریم خصوصی کاربران، هسته اصلی کار ما است. از محافظت از ناشناس بودن کاربران گرفته تا ارائه کنترل‌های معنادار حفظ حریم خصوصی و امنیت، و تعهد به شفافیت، اصول بنیادی ما در هسته اصلی ایکس تعبیه شده است (صفحه جی.دی.پی.آر ایکس، ۲۰۲۴).

در این بخش توضیح داده شده است که رویکرد ایکس به حریم خصوصی بسیار از فراتر از تبعیت از برخی قوانین است و پلتفرم قصد دارد تا امنیت داده و برنامه حریم خصوصی جامع خود را تقویت کند. همچنین این شرکت در پی این است تا به شکلی شفاف ابزارهایی را در اختیار کاربران قرار دهد تا به شکلی معنادار درباره داده‌های خود و داده‌هایی که درباره آنها گردآوری می‌شود، امکان اعمال کنترل داشته باشند.

[1] . https://privacy.x.com/en
[2] .California Consumer Privacy Act (CCPA)
[3] .Data Processing Addendum (Global DPA)
[4] . https://gdpr.x.com/

سیاست حریم خصوصی ایکس

آخرین به‌روزرسانی حریم خصوصی ایکس در تاریخ ۲۹ سپتامبر ۲۰۲۳ انجام شده است. در مقدمه این سند بر دو نکته تأکید شده است:

ایجاد یک سیاست حفظ حریم خصوصی که همه را راضی کند، کار بسیار دشواری است. اکثر افرادی که از ایکس استفاده می کنند، به دنبال متنی کوتاه و قابل فهم هستند. در حالی که دوست داشتیم همه چیزهایی را که نیاز دارید بدانید، در یک پست جا دهیم، مقررات از ما می خواهند که با توصیف همه آنها با جزئیات زیاد، تعهدات قانونی خود را برآورده کنیم.

با در نظر گرفتن این موضوع، ما تا حد امکان خط مشی حفظ حریم خصوصی خود را به سادگی نوشته ایم تا با اطمینان از درک و کنترل اطلاعاتی که جمع آوری می کنیم، نحوه استفاده از آنها و زمان به اشتراک گذاری آنها، شما را در هنگام استفاده از ایکس قادر سازیم تا تصمیمات آگاهانه بگیرید (حریم خصوصی ایکس، ۲۰۲۴).

- ساده‌سازی مفاد حریم خصوصی و -امکان اعمال کنترل کاربر

این مطلب بر دو نکته تأکید دارد. نخست *ساده‌سازی مفاد حریم خصوصی*. یکی از انتقادهایی که گاه به پلتفرم‌های بزرگ وارد می‌شود پیچیدگی بیش از حد جزئیات حریم خصوصی است که گاه عامدانه توسط صاحبان پلتفرم‌ها برای گریز از مسئولیت نسبت به حریم خصوصی کاربران صورت می‌گیرد (فن‌دایک، ۱۴۰۲). مورد دوم فراهم کردن *امکان اعمال کنترل کاربر* برای تصمیم‌گیری آگاهانه برای اشتراک‌گذاری اطلاعات شخصی است. موضوعی که مورد تأکید پلتفرم‌های مورد مطالعه دیگر قرار دارد. اعمال کنترل به دلایلی متعددی اهمیت زیادی دارد که ازجمله آنها می‌توان به حفاظت از حریم خصوصی، امنیت داده و توانمندسازی کاربران اشاره کرد.

در جدول ۶-۴) برخی از بخش‌های محور سند حریم خصوصی ایکس را مرور می‌کنیم. این امر از این حیث اهمیت دارد که در تدوین سند حریم خصوصی جامع برای پلتفرم‌ها می‌تواند مورد استفاده قرار گیرد.

اطلاعات گردآوری شده توسط ایکس	**اطلاعاتی که کاربران ارائه می‌کنند**	–اطلاعات ارائه شده به هنگام ثبت نام برای حساب کاربری (نام، نام خانوادگی، نام کاربری، گذرواژه، پست الکترونیک، تلفن همراه، موقعیت و...) –اطلاعات مربوط به حساب کاربری تجاری –ترجیحات کاربر –اطلاعات بیومتریک –اطلاعات شخصی همانند سابق استخدام، سوابق آموزشی، ترجیحات شغلی، مهارتها و توانایی‌ها، جستجوی شغل برای پیشنهاد شغل
	اطلاعات که هنگام کاربرد، پلتفرم ایکس گردآوری می‌کند	–هنگامی که از خدمات ما استفاده می کنید، ما اطلاعاتی در مورد چگونگی استفاده شما از محصولات و خدمات خود جمع آوری می کنیم. ما از آن اطلاعات برای ارائه محصولات و خدمات به شما، برای کمک به ایمن نگه داشتن [محصولات ما / X] به روشی محترمانه برای همه و مرتبطتر کردن آن با شما استفاده می‌کنیم. (هنگامی که از خدمات ما استفاده می کنید، ما اطلاعاتی در مورد چگونگی استفاده شما از محصولات و خدمات خود جمع آوری می کنیم. ما از آن اطلاعات برای ارائه محصولات و خدمات به شما، برای کمک به ایمن نگه داشتن

		محصولات ما به روشی محترمانه برای همه و مرتبط‌تر کردن آن با شما استفاده می‌کنیم.)
	اطلاعات به دست آمده از طرف‌های ثالث	–شرکای تجاری در زمینه تبلیغات، توسعه‌دهندگان و ناشر –طرف‌های ثالث دیگر، پیوندها با حساب کاربری و شرکتهای مرتبط

جدول ۶-۴) اطلاعات گردآوری شده توسط ایکس

نحوه استفاده از اطلاعات

توضیح دادن اینکه پلتفرم ایکس چگونه از اطلاعات جمع آوری شده استفاده می‌کند، به دلیل نحوه عملکرد سیستم هایی که خدمات ایکس را به کاربران ارائه می دهند، ساده نیست. برای مثال، ممکن است از یک قطعه اطلاعات خاص برای اهداف مختلف برای ارائه نهایی یک سرویس واحد استفاده شود. اما به پنج روش اصلی می‌توان نحوه استفاده از اطلاعات کاربران توسط پلتفرم را توضیح داد.

۱. انجام فعالیت خدمات ایکس، بهبود و نیز شخصی‌سازی آنها

۲. ارتقاء ایمنی و امنیت

۳. سنجش، اندازه‌گیری و بهبود خدمات ایکس

۴. برقراری ارتباط با کاربران درباره خدمات ایکس

۵. انجام پژوهش.

اعمال کنترل بر اطلاعات شخصی

امکان اعمال کنترل بر اطلاعات شخصی یکی از قابلیت‌هایی است که ایکس برای توانمندسازی کاربرانش فراهم کرده است. این موضوع در جدول ۷-۴ نمایش داده شده است.

	نحوه اعمال کنترل	
اعمال کنترل	دسترسی، تصحیح و قابلیت انتقال	–«شما می توانید با ویرایش پروفایل و تنظیم تنظیمات حساب کاربری خود، به اطلاعاتی که به ما ارائه کرده اید دسترسی پیدا کنید، آنها را اصلاح یا تغییر دهید». (ویرایش حساب کاربری) –شما می توانید در بخش داده های شما درباره اطلاعاتی که ما در مورد شما جمع آوری یا استنتاج کرده ایم، بیشتر بیاموزید و درخواست دسترسی به اطلاعات تکمیلی را بدهید.(درخواست ارائه جزئیات داده‌های گردآوری شده) –برای محافظت از حریم خصوصی و حفظ امنیت شما، ما قبل از اینکه به شما اجازه دسترسی به اطلاعات شخصی خود را بدهیم یا با درخواست حذف، انتقال یا سایر درخواست‌های مرتبط موافقت کنیم، اقداماتی را برای تأیید هویت شما انجام می‌دهیم. (احراز هویت به هنگام درخواست دسترسی به اطلاعات شخصی)
	حذف اطلاعات کاربران	–«اگر دستورالعمل‌های اینجا را دنبال کنید، حساب کاربری شما غیرفعال می‌شود و داده‌های شما برای حذف در صف قرار می‌گیرند. پس از غیرفعال شدن، حساب کاربری X شما، از جمله نام نمایشی، نام کاربری و پروفایل عمومی، دیگر در X.com، X برای iOS و X برای اندروید قابل مشاهده نخواهد بود». (امکان حذف حساب کاربری)

	اعتراض به رضایت، محدود کردن آن یا لغو رضایت	–شما می‌توانید تنظیمات حریم خصوصی و سایر ویژگی‌های حساب خود را در اینجا مدیریت کنید. اگر تنظیمات خود را تغییر دهید، ممکن است مدتی طول بکشد تا انتخاب‌های شما به طور کامل در سراسر سیستم‌های ما اعمال شود. همچنین ممکن است بسته به تنظیماتی که تنظیم کرده‌اید، تغییراتی را در تجربه خود یا محدودیت‌هایی در دسترسی به ویژگی‌های خاص مشاهده کنید (تغییر تنظیمات)
	درخواست‌های نماینده مجاز	برای ارسال درخواست مربوط به دسترسی، اصلاح یا حذف اطلاعات خود، یا اطلاعات شخص دیگری در صورت نماینده مجاز وی بودن، همچنین می توانید طبق روشی که در بخش "نحوه تماس" در بخش خط مشی رازداری ما در زیر آمده است با ما تماس بگیرید (درخواست اصلاح حریم خصوصی توسط نمایندگان مجاز)

جدول ۷-۴) نحوه اعمال کنترل کاربر محتوا در ایکس

حقوق متقابل

یکی از بخش‌های سیاست حریم خصوصی ایکس، حقوق متقابل کاربران و پلتفرم ایکس است که در آن تصریح شده است ایکس همه ابزارهای کنترل حریم خصوصی را برای کاربرانش در سطح جهان به شکل یکسان فراهم کرده است اما ایکس به الزامات و مقررات محلی نیز احترام می‌گذارد (سیاست حریم خصوصی ایکس، ۲۰۲۴). منظور این است که این پلتفرم خود را ملزم می‌داند به حق حاکمیت کشورها احترام بگذارد و قوانین محلی در خصوص حریم خصوصی و داده را نیز مورد توجه قرار دهد. یکی از این حقوق، عمل بر اساس مبنای قانون برای گردآوری، اشتراک‌گذاری و پردازش اطلاعات کاربران است. در بخشی با عنوان اطلاعات اضافی درباره پردازش داده که در مرکز کمک ایکس قرار دارد، به شکلی مفصل اطلاعات تکمیلی در مورد گردآوری و پردازش اطلاعات کاربران و مبنای قانونی آنها توضیح داده شده است. در یک جدول با جزئیات توضیحاتی درباره فهرستی از اهداف عمومی پردازش داده‌های شخصی بیان شده است. در این جدول به طور

خاص مبانی قانونی گردآوری داده‌های شهروندان اتحادیه اروپا، دولتهای عضو انجمن تجارت آزاد اروپا[1] و انگلستان مشاهده می‌شود (مرکز کمک ایکس، ۲۰۲۴).

اعمال مقررات درباره حریم خصوصی

ایکس اعتقاد دارد که این پلتفرم بازتاب‌دهنده‌ی گفتگوهای واقعی‌ای است که در دنیا رخ می‌دهد و این گاهی شامل دیدگاه‌هایی می‌شود که ممکن است برای دیگران توهین‌آمیز، جنجالی و یا متعصبانه باشد. بنابراین، رفتارهایی که دیگران را آزار می‌دهد، تهدید می‌کند یا از ترس برای خاموش کردن صدای دیگران استفاده می‌کند تحمل نمی‌شود. این فلسفه اعمال مقررات در پلتفرم ایکس است (مرکز کمک ایکس، ۲۰۲۴).

فلسفه اجرایی حول محور ترویج بحث‌های آزاد و توانمندسازی کاربران برای ابراز عقاید متنوع، از جمله دیدگاه‌های مخالف می‌چرخد. این امر باعث تشویق ضدسخن می‌شود که حقایق را ارائه می‌کند، اطلاعات نادرست را اصلاح می‌کند، تناقضات را برجسته می‌کند، در مورد عواقب هشدار می‌دهد و به تغییر دیدگاه‌ها کمک می‌کند. هنگام بررسی اقدامات اجرایی، زمینه اهمیت دارد و عواملی مانند هدف رفتار، منبع گزارش، سابقه تخلف کاربر، شدت تخلف و منافع عمومی بالقوه در نظر گرفته می‌شود.

اجرای سیاست‌ها بر ایجاد تعادل میان نظرات مختلف و محافظت کاربران در برابر رفتارهای توهین‌آمیز تمرکز دارد. برخی ملاحظات کلیدی عبارتند از:

هدف‌گیری: در صورتی که رفتار گزارش‌شده مستقیماً به سمت افراد یا گروه‌هایی جهت‌گیری شده باشد، سیاست‌ها اجرا می‌شوند. این هدف‌گیری ممکن است از طریق تگ کردن افراد (@)، تگ کردن عکس، یا روش‌های دیگر صورت گیرد.

منبع گزارش: بستر مکالمه و ظرافت‌های فرهنگی در نظر گرفته می‌شوند، به خصوص زمانی که گزارش‌ها از سوی ناظران ارائه شود. در برخی موارد، اقدامات اجرایی تنها پس از گزارش از سوی فرد هدف یا نماینده او انجام می‌پذیرد.

[1]. (EFTA States): اتحادیه تجارت آزاد اروپا با علامت اختصاری نام سازمانی منطقه‌ای است که به موجب کنوانسیون استکهلم در سال ۱۹۶۰ میلادی برای تسهیل تجارت میان کشورهای اروپایی و حذف تعرفه های گمرکی ایجاد شد و متشکل از چهار کشور ایسلند، لیختن اشتاین، نروژ و سوئیس است.

سابقه نقض قوانین کاربر: با فرض اینکه نقض قوانین غیرعمدی باشد، رویکرد با آموزش کاربران و دادن فرصت برای اصلاح رفتار آغاز می‌شود. با این حال، تکرار نقض قوانین منجر به اقدامات شدیدتری مانند محدودیت‌های موقت یا تعلیق دائمی حساب کاربری می‌شود.

شدت نقض: اقدامات بر اساس شدت نقض صورت‌گرفته تعیین می‌شوند. در موارد جدی مانند تهدید به خشونت، انتشار محتوای جنسی بدون رضایت یا سوءاستفاده از کودکان، تعلیق فوری و دائمی اعمال می‌شود. نقض‌های کمتر جدی ممکن است منجر به حذف محتوا یا محدودیت‌های موقت برای انتشار محتوا شوند.

در پلتفرم ایکس، سهل‌ترین و نزدیک‌ترین روشی که کاربران با سیاست حریم خصوصی این پلتفرم ارتباط برقرار می‌کنند، گزارش دادن یک گزارش دادن یک پست است. گزارش دادن یا علامت‌دهی اکنون به یک سازوکار رایج برای گزارش محتوای توهین‌آمیز و غیرقانونی به پلتفرم های آنلاین تبدیل شده است و به طور گسترده در اکثر سایت‌های محبوب شبکه‌های اجتماعی مورد استفاده قرار می‌گیرد. علامت‌دهی هم به عنوان راه حلی برای مشکل مدیریت مجموعه‌های عظیم محتوای ایجاد شده توسط کاربر و هم به عنوان توجیهی بلاغی برای مالکان پلتفرم هنگام حذف محتوا عمل می‌کند. علامت‌دهی به یک سازوکار فراگیر برای حکمرانی تبدیل شده است (کرافورد و ژیلسپی، ۲۰۱۶).

در پلتفرم ایکس، ذیل هر پست کاربران می‌توانند به حکمرانی محتوا از طریق گزارش یک پست کمک کنند و سپس ایکس تصمیم می‌گیرد آن محتوا را حذف کند یا خیر. یکی از موضوعات گزارشها مرتبط به حریم خصوصی است. بخش مربوط به حریم خصوصی دارای این توضیحات است:

اشتراک‌گذاری اطلاعات خصوصی، تهدید به اشتراک‌گذاری/ افشای اطلاعات خصوصی، اشتراک‌گذاری تصاویر محرمانه بدون توافق، اشتراک‌گذاری تصاویری از من که نمی‌خواهم در پلتفرم

-تهدید به اشتراک گذاری یا به اشتراک گذاری اطلاعات شخصی خصوصی بدون اجازه

-تهدید به اشتراک گذاری یا اشتراک گذاری عکس/فیلم جنسی، برهنه یا صمیمی از من یا شخصی بدون اجازه

-به اشتراک گذاری عکس/ویدیویی از من که نمی خواهم در پلتفرم (پلتفرم ایکس، ۲۰۲۴).

سپس کاربر باید مشخص کند که اطلاعات مربوط به وی است یا به فرد دیگری تعلق دارد. درمرحله بعد محتوای گزارش شده که ناقض حریم خصوصی تشخیص داده شده است، وارد فرایند تعدیل محتوا می‌شود.

در جدول ۴-۸) مجموعه مضامین این فصل که بیانگر اصول حاکم بر پلتفرم‌های جهانی برای حفاظت از حریم خصوصی کاربران است، ذکر می‌شود.

اصول حریم خصوصی در پلتفرم‌های گوگل، متا و فیس‌بوک	اصل حفظ حریم خصوصی بر اساس طراحی یا حفظ حریم خصوصی به صورت پیش‌فرض شفاف‌سازی در مورد اطلاعات گردآوری شده عدم فروش اطلاعات به شخص ثالث تسهیل کنترل اطلاعات شخصی تقلیل داده‌های شخصی تضمین ایمنی با ساخت محصولات ایمن به شکل پیش‌فرض ساخت و توسعه فناوری‌های پیشرفته حفاظت از حریم خصوصی -ایمنی و حریم خصوصی -رمزگذاری به عنوان ابزار حفظ ایمنی -فراهم کردن امکان کنترل کاربران -اصل تقلیل داده‌های کاربران -خطمشی یا سیاست اشتراک‌گذاری داده‌های کاربران کسب رضایت کاربران

	پلتفرم متا (فیس‌بوک) – اصول بنیادین حریم خصوصی متا کنترل و شفافیت کاربر تقلیل داده پاسخگویی و انطباق حفظ حریم خصوصی از طریق طراحی و به صورت پیش‌فرض منافع کاربر بهبود مستمر –چیستی اطلاعات گردآوری شده فعالیت و اطلاعاتی که کاربران ارائه می‌کنند –نحوه استفاده از اطلاعات گردآوری شده توسط متا برای ارائه محصولات، شخصی‌سازی و بهبود محصولات ارتقای امنیت، حفاظت و یکپارچگی ارائه خدمات اندازه‌گیری، تحلیل و کسب‌وکار برای برقراری ارتباط برای تحقیق و نوآوری برای خیر اجتماعی –مبنای حقوقی پردازش اطلاعات رضایت کاربران منافع مشروع پلتفرم ایکس رویکرد ایکس به حریم خصوصی

	-نخست ساده‌سازی مفاد حریم خصوصی -امکان اعمال کنترل کاربر نحوه استفاده از اطلاعات اعمال کنترل بر اطلاعات شخصی -دسترسی، تصحیح و قابلیت انتقال -حذف اطلاعات کاربران -اعتراض به رضایت، محدود کردن آن یا لغو رضایت

جدول ۴-۸) مضامین حریم خصوصی و داده در پلتفرم‌های جهانی

نتیجه‌گیری

در این بخش تلاش شد تا اصول بنیادین، رویکرد کلی و سازوکار حکمرانی داده‌ها و حریم خصوصی در سه پلتفرم بزرگ جهانی تشریح شود. در این بخش تلاش شد رویکرد کلی پلتفرم‌های جهانی بزرگ در مورد حریم خصوصی و حریم داده کاربران تشریح شود تا در نهایت بتواند به‌منزله راهنمایی برای تدوین سازوکار حفاظت از داده‌ها در پلتفرم‌های ایرانی عمل نماید. بنابراین، در اینجا نشان دادیم که برای تعریف بهتر و جامع‌تر حریم داده‌های شخصی یک روش سودمند مراجعه به پلتفرم‌ها، ملاحظه سیاست حریم خصوصی آنها و آگاهی از جزئیات داده‌هایی است که از کاربران جمع‌آوری می‌کنند.

بخش چهارم

مرور قوانین و مقررات جهانی مرتبط با حریم داده‌ها (اتحادیه اروپا، آمریکا و چین)

مقدمه

هدف این بخش مرور جزئیات مقررات و قوانین مصوب بین‌المللی درباره حفاظت از حریم داده‌ها است. قوانین و یا مقرراتی که در اینجا بررسی می‌شوند شامل مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، قانون حریم خصوصی مصرف‌کننده کالیفرنیا و قانون حفاظت از اطلاعات شخصی چین با مرور این مقررات می‌توان به الگویی برای نگارش پیش‌نویس قانون حفاظت از حریم خصوصی داده‌ها در ایران دست پیدا کرد و آنرا با متناسب با رویکردهای بومی (عموماً برگرفته از مفاهیم دینی) بازنویسی کرد.

مقررات عمومی حفاظت از داده‌ها

مقررات کلی حفاظت از داده‌های اروپا یک آیین‌نامه جامع در زمینه حریم خصوصی و حفاظت از داده‌ها است که تأثیر چشمگیری بر نحوه مدیریت داده‌های شخصی توسط سازمان‌ها در اتحادیه اروپا و فراتر از آن داشته است. این مقررات که در آوریل ۲۰۱۶ تصویب شد و از ماه مه ۲۰۱۸ به اجرا درآمد، جایگزین دستورالعمل حفاظت از داده‌های[1] ۱۹۹۵ شد تا با توجه به پیشرفت‌های فناوری و افزایش جریان داده‌های فرامرزی، از داده‌های شخصی شهروندان اتحادیه اروپا به صورت مدرن‌تر و قوی‌تری محافظت کند. این قانون شامل ۱۱ فصل و ۹۹ ماده است.

هدف اصلی جی.دی.پی.آر اعطای کنترل بیشتر به افراد بر روی داده‌های شخصی آنها است و همزمان اطمینان می‌دهد که سازمان‌ها، اولویت حفاظت از داده‌ها و حریم خصوصی را در عملکرد خود قرار دهند. این مقررات برای تمامی سازمان‌هایی

[1] . Data Protection Directive

که داده‌های شخصی شهروندان اتحادیه اروپا را پردازش می‌کنند، فارغ از مکان سازمان یا محل پردازش داده‌ها، اعمال می‌شود.

مقررات کلی حفاظت از داده‌های اروپا بر چند اصل کلیدی استوار است.

قانونی بودن، انصاف و شفافیت. داده‌های شخصی باید به صورت قانونی، منصفانه و شفاف در رابطه با افراد پردازش شوند.

محدودیت هدف. داده‌ها باید برای اهداف مشخص، صریح و مشروع جمع‌آوری شوند و به روشی که با آن اهداف سازگار نباشد، پردازش بیشتر نشوند.

تقلیل داده‌ها. داده‌های جمع‌آوری‌شده باید کافی، مرتبط و محدود به آنچه برای هدف پردازش ضروری است، باشد.

دقت. داده‌های شخصی باید دقیق و در صورت لزوم به روز نگه داشته شوند.

محدودیت ذخیره‌سازی. داده‌ها باید به شکلی نگهداری شوند که امکان شناسایی افراد را بیش از مدت زمان مورد نیاز برای اهداف پردازش، فراهم نکند.

یکپارچگی و محرمانگی. داده‌های شخصی باید به صورت امن پردازش شوند تا یکپارچگی و محرمانگی آن‌ها حفظ شود.

مسئولیت‌پذیری. کنترلرهای داده باید انطباق خود با اصول جی.دی.پی.آر را نشان دهند و مسئول فعالیت‌های پردازش داده خود باشند.

عدم انطباق با جی.دی.پی.آر می‌تواند منجر به جریمه‌های قابل توجهی تا سقف ۲۰ میلیون یورو یا ۴ درصد از گردش مالی سالانه جهانی شرکت، هرکدام که بیشتر باشد، شود.

به طور خلاصه، مقررات کلی حفاظت از داده‌های اروپا یک چارچوب قدرتمند است که هدف آن محافظت از حقوق شهروندان اتحادیه اروپا در رابطه با پردازش داده‌های شخصی آن‌ها است. این مقررات استانداردهای جدیدی را برای حفاظت از داده‌ها و حریم خصوصی ایجاد کرده و بر قوانین حفاظت از داده‌ها در سطح جهان تأثیر گذاشته است.

تحلیل جزئی‌تر جی.دی.پی.آر

بر اساس روش پژوهش تحلیل محتوای کیفی، ما به تحلیل محتوای این سند به شکل قیاسی اقدام می‌کنیم. همانطور که کوکارتز و ردیکر (۲۰۲۳) توضیح داده‌اند، در این روش، مقوله‌های پیشینی مستقل از داده‌های جمع‌آوری‌شده، اما بر اساس

یک سیستم‌بندی از پیش موجود، توسعه می‌یابند. این سیستم‌بندی می‌تواند یک نظریه یا فرضیه، و همچنین یک راهنمای مصاحبه یا یک سیستم موجود برای ساختارمند کردن محتوا باشد. بنابراین، ما بر اساس مرور ادبیات که تاکنون درباره مفاهیم، اصول، معیارها و دسته‌بندی حریم خصوصی و حمایت از داده‌ها انجام داده‌ایم، بر اساس برخی مقوله‌های پیشینی اقدام به مطالعه این سند و چهار سند دیگر خواهیم کرد.

حفاظت از حقوق اساسی شهروندان اروپایی از منظر داده‌های شخصی

فصل اول این قانون قواعد کلی[1] است که شامل چهار ماده است. ماده یک این قانون شامل موضوع و اهداف است.

۱. این مقررات، قواعد مربوط به حمایت از اشخاص حقیقی در قبال پردازش داده‌های شخصی و همچنین قواعد مربوط به جریان آزاد داده‌های شخصی را تعیین می‌کند.

۲. این مقررات از حقوق و آزادی‌های بنیادین اشخاص حقیقی و به‌ویژه حق *آن‌ها برای حمایت از داده‌های شخصی* محافظت می‌کند.

۳. جریان آزاد داده‌های شخصی در اتحادیه اروپا نباید به دلایل مرتبط با حمایت از اشخاص حقیقی در قبال پردازش داده‌های شخصی، محدود یا ممنوع شود.

بنابراین هدف این قانون *حمایت از اشخاص حقیقی در قابل پردازش داده‌های شخصی آنها، حمایت از حقوق و آزادی‌های اساسی افراد* و *عدم محدودسازی جریان آزاد اطلاعات* در سطح اتحادیه اروپا است.

ماده دوم که دامنه مادی[2] نامیده شده است، مقرر می‌دارد، «این مقررات بر پردازش داده‌های شخصی به صورت کاملاً خودکار یا نیمه‌خودکار و همچنین بر پردازش داده‌های شخصی به صورت غیر خودکار که بخشی از یک سیستم بایگانی هستند یا برای قرار گرفتن در یک سیستم بایگانی در نظر گرفته شده‌اند، اعمال می‌شود».

بنابراین، «پردازش داده‌های شخصی» محور این قانون است. دو مهفوم پردازش و داده شخصی باید تعریف شوند. اما پردازش می‌تواند به شکل کاملاً خودکار و یا نیمه‌خودکار و پردازش غیرخودکار داده‌های شخصی بایگانی شده تمرکز دارد. پردازش داده‌ها به شکل خودکار توسط پلتفرم‌ها و سامانه‌های کلان‌داده انجام می‌شود. از سوی دیگر پایگاه‌های داده شامل اطلاعات ذخیره شده شهروندان نیز نیز هست. در موارد زیر، این مقررات قابل اجرا نیستند.

–در جریان فعالیتی که خارج از حوزه قوانین اتحادیه اروپا قرار می‌گیرد (*دربردارنده حوزه قضایی اتحادیه اروپا*).

[1] .general provision
[2] .material scope

–توسط کشورهای عضو اتحادیه اروپا، هنگامی که فعالیت‌های آن‌ها در چارچوب فصل ۲ از عنوان پنجم معاهده اتحادیه اروپا باشد (مثتنی شدن فعالیتهای فصل دوم عنوان پنجم معاهده اتحادیه اروپا)

–توسط یک شخص حقیقی در جریان فعالیت‌های کاملاً شخصی یا خانوادگی (*عدم مشمول فعالیت‌های کاملاً شخصی*).

–توسط مقامات ذیصلاح به منظور پیشگیری، تحقیق، کشف یا تعقیب جرائم کیفری یا اجرای مجازات‌های کیفری، از جمله اقدامات پیشگیرانه در برابر تهدیدات علیه امنیت عمومی (*مستثنی شدن جرایم کیفری و تهدیدات علیه امنیت ملی*).

ماده سوم) قلمرو سرزمینی

۱) این مقررات در مورد پردازش داده‌های شخصی در چارچوب فعالیت‌های تأسیساتِ مسئول یا پردازشگرِ مستقر در اتحادیه اروپا، فارغ از اینکه پردازش در داخل اتحادیه انجام شود یا خیر، اعمال می‌گردد.

۲) این مقررات در مورد پردازش داده‌های شخصی افراد موضوع داده که در اتحادیه اروپا حضور دارند، توسط مسئولی یا پردازشگری که در اتحادیه اروپا مستقر نیست، در صورتی اعمال می‌شود که فعالیت‌های پردازش مرتبط با موارد زیر باشد.

الف) ارائه کالا یا خدمات، صرف نظر از اینکه پرداخت توسط فرد موضوع داده الزامی باشد، به چنین افرادی در اتحادیه اروپا؛ یا

ب) پایش رفتار آن‌ها تا زمانی که رفتارشان در داخل اتحادیه اروپا صورت گیرد.

۳) این مقررات در مورد پردازش داده‌های شخصی توسط مسئولی که در اتحادیه اروپا مستقر نیست، اما در مکانی که قوانین کشورهای عضو اتحادیه اروپا به موجب حقوق بین‌الملل عمومی اعمال می‌شود، نیز صدق می‌کند.

نکات کلیدی این ماده به این شرح است.

دامنه وسیع کاربرد جی.دی.پی.آر

مقررات عمومی حفاظت از داده‌های شخصی دامنه‌ی بسیار وسیعی دارد. این مقررات بر هر سازمانی که به پردازش داده‌های شخصی شهروندان اتحادیه اروپا اقدام می‌کند، صرف‌نظر از محل استقرار آن سازمان، اعمال می‌شود.

تمرکز بر فعالیت‌ها

جی.دی.پی.آر. بر ماهیت فعالیت‌های سازمان تمرکز می‌کند، نه صرفاً مکان فیزیکی پردازش داده‌ها. به عبارت دیگر، مهم نیست که داده‌ها در کجا پردازش می‌شوند، بلکه نوع فعالیت سازمان در قبال داده‌های شهروندان اتحادیه اروپا اهمیت دارد.

دو سناریو برای سازمان‌های خارج از اتحادیه اروپا

مقررات جی.دی.پی.آر. در دو سناریو برای سازمان‌های خارج از اتحادیه اروپا نیز اعمال می‌شود.

–ارائه کالا یا خدمات (رایگان یا با پرداخت هزینه) به شهروندان اتحادیه اروپا

–رصد رفتار شهروندان اتحادیه اروپا، مشروط بر اینکه این رفتار در داخل اتحادیه اروپا صورت گیرد.

موارد خاص

در موارد خاصی خارج از اتحادیه اروپا، زمانی که قوانین کشورهای عضو اتحادیه اروپا به موجب توافقات بین‌المللی جاری باشد، جی.دی.پی.آر. همچنان قابل اجرا است.

به بیان ساده‌تر، جی.دی.پی.آر. دارای دامنه‌ی وسیعی است و هدف آن محافظت از حریم خصوصی داده‌های شهروندان اتحادیه اروپا می‌باشد، حتی اگر سازمانی که داده‌ها را پردازش می‌کند، در خارج از اتحادیه اروپا مستقر باشد.

چیستی داده‌های شخصی

یک موضوع محوری مفهوم و تعریف داده‌های شخصی است. همانطور که به‌ویژه مرور ادبیات مرتبط با حریم اطلاعات و داده‌های شخصی در ایران نشان داد، در ایران در مورد کاربرد یک اصطلاح واحد برای حریم داده‌ها نیز اتفاق نظر وجود ندارد، چه برسد به اینکه این اصطلاح تعریف شود. بر این اساس، در بررسی این قانون و قوانین دیگر، نخست تعریف داده‌های شخصی اهمیت دارد. ماده چهار جی.دی.پی آر به تعریف اصطلاحات این قانون اختصاص دارد. در اینجا ۲۶ مفهوم تعریف شده‌اند که برخی از مهمترین آنها را ذکر می‌کنیم.

–مفهوم داده‌های شخصی

اولین مفهوم «داده شخصی» است که در راستای اهداف این قانون به این شکل تعریف شده است.

«داده‌های شخصی» به معنای هرگونه اطلاعاتی است که به یک شخص حقیقی شناسایی شده یا قابل شناسایی («موضوع داده[1]») مرتبط باشد. یک شخص حقیقی قابل شناسایی کسی است که به طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به شناسه‌هایی مانند نام، شماره شناسایی،

[1] .data subject

داده‌های مکان‌یاب، شناسه آنلاین یا به یک یا چند عامل خاص مربوط به هویت جسمی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی یا اجتماعی آن شخص حقیقی قابل شناسایی باشد.

در سایت کمیسیون اروپا در پاسخ به پرسش چیستی داده‌های شخصی این توضیح ذکر شده است.

مقررات عمومی حفاظت از داده‌های شخصی هرگونه اطلاعاتی را که به یک فرد زنده شناسایی‌شده یا قابل شناسایی مرتبط باشد، تحت پوشش قرار می‌دهد. همچنین قطعات مجزایی از اطلاعات که در کنار هم منجر به شناسایی یک فرد خاص شوند نیز داده‌های شخصی محسوب می‌گردند. داده‌های شخصی که ناشناس‌سازی، رمزنگاری یا مستعارسازی شده‌اند، اما همچنان قابل استفاده برای شناسایی مجدد فرد باشند، همچنان داده‌های شخصی به شمار می‌روند و مشمول جی.دی.پی.آر هستند.

داده‌های شخصی که به گونه‌ای کاملاً ناشناس شده باشند که فرد قابل شناسایی نباشد، دیگر داده شخصی محسوب نمی‌شوند. برای اینکه داده‌ها واقعاً ناشناس شوند، فرایند ناشناس‌سازی باید غیرقابل بازگشت باشد.

جی.دی.پی.آر از داده‌های شخصی، فارغ از فناوری مورد استفاده برای پردازش آن‌ها، محافظت می‌کند. این مقررات فناوری–خنثی بوده و بر هر دو پردازش خودکار و دستی داده‌ها، مشروط بر اینکه داده‌ها بر اساس معیارهای از پیش تعریف‌شده (به عنوان مثال، ترتیب حروف الفبا) سازماندهی شده باشند، اعمال می‌شود. همچنین نحوه ذخیره‌سازی داده‌ها (در یک سیستم فناوری اطلاعات، از طریق نظارت تصویری یا روی کاغذ) اهمیتی ندارد. در تمامی موارد، داده‌های شخصی مشمول الزامات حفاظتی مندرج در جی.دی.پی.آر هستند (کمیسیون اروپا، ۲۰۲۴).

کمیسیون اروپا (۲۰۲۴) نمونه‌هایی از داده‌های شخصی را به این شکل بیان کرده است.

نام و نام خانوادگی

آدرس منزل

آدرس ایمیل مانند نام.نام‌خانوادگی@شرکت.کام

شماره کارت شناسایی

داده‌های موقعیت مکانی (به عنوان مثال، عملکرد داده موقعیت مکانی روی تلفن همراه)

آدرس پروتکل اینترنت (آی.پی)

شناسه کوکی

شناسه تبلیغاتی تلفن همراه

اطلاعات نگهداری شده توسط بیمارستان یا پزشک، که می‌تواند شامل نمادی باشد که به طور منحصر یک فرد را شناسایی می‌کند.

همچنین، نمونه‌هایی از داده‌هایی که داده شخصی محسوب نمی‌شوند عبارتند از.

شماره ثبت شرکت

آدرس ایمیلی مانندinfo@company.com

داده‌های ناشناس (کمیسوین اروپا، ۲۰۲۴).

بر این اساس ما می‌توانیم بگوییم که داده‌های شخصی به هرگونه اطلاعاتی که به یک فرد شناسایی‌شده یا قابل شناسایی مربوط باشد، گفته می‌شود. این امر می‌تواند انواع مختلفی از اطلاعات را شامل شود، از جمله.

–شناساگرهای مستقیم. داده‌هایی که به طور مستقیم هویت یک فرد را نشان می‌دهند، مانند نام، کد ملی، داده‌های موقعیت مکانی یا شناسه آنلاین.

–شناساگرهای غیرمستقیم. داده‌هایی که می‌توان آن‌ها را با اطلاعات دیگر برای شناسایی یک فرد ترکیب کرد، مانند ویژگی‌های فیزیکی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی یا اجتماعی.

دادهٔای حساس[1]. دسته‌های خاصی از داده‌های شخصی که حساس در نظر گرفته می‌شوند، مانند نژاد یا قومیت، عقاید سیاسی، اعتقادات مذهبی یا فلسفی، عضویت در اتحادیه کارگری، داده‌های ژنتیکی، داده‌های بیومتریک، داده‌های بهداشتی و داده‌های مربوط به زندگی جنسی یا گرایش جنسی فرد.

برخی از نمونه‌های داده‌های شخصی عبارتند از.

–نام، آدرس، آدرس ایمیل و شماره تلفن

–تاریخ تولد، جنسیت و وضعیت تأهل

–اطلاعات موقعیت مکانی، آدرس‌های آی.پی و شناسه‌های دستگاه

–سابقه خرید، اطلاعات مالی و جزئیات حساب

[1] .sensetice data

–سابقه کاری، تحصیلات و صلاحیت‌های حرفه‌ای

–سوابق پزشکی، داده‌های بهداشتی و داده‌های بیومتریک

–عکس، فیلم و ضبط صدا

با ملاحظه اینکه امروز بخش مهمی از زیست روزمره ما در فضای مجازی سپری می‌شود و ما برای دریافت خدمات گوناگون، ارتباط و تعامل با پلتفرم‌ها سروکار داریم، پلتفرم‌های گوناگون عمده‌ترین پایگاه داده، داده‌های شخصی هستند که به طور مستمر داده‌های شخصی ما را دریافت می‌کنند. مهمترین ویژگی این داده‌های شخصی در پلتفرم‌ها این است که آنها دائماً به‌روزرسانی می‌شوند؛ بسیار گسترده‌تر از شیوه‌های سنتی گردآوری داده‌های شخصی عمل می‌کنند (مانند پایگاه داده سازمان ثبت احوال)؛ گستره داده‌ها دریافت‌شده توسط پلتفرم‌ها بسیار وسیع‌تر است و شامل داده‌های بسیار خصوصی‌تری است که افراد در حریم مکانی خود آنرا با نزدیکانشان حتی اعضای خانواده نیز به‌اشتراک نمی‌گذارند. بنابراین، در تعریف داده‌های شخصی ما باید این ملاحظات را مد نظر قرار دهیم. باید این موضوع با ملاحظه سیاست‌های گردآوری داده در پلتفرم‌های مطالعه شده بررسی شود–در فصل نتیجه‌گیری این موضوع مورد توجه قرار می‌گیردو این تعریف در فصل نتیجه‌گیری با همه این ملاحظات ارائه خواهد شد.

با توجه به ماهیت گسترده و عمیق داده‌های شخصی کاربران در پلتفرم‌های رسانه‌های اجتماعی، داده‌های شخصی در این زمینه را می‌توان مجموعه‌ای عظیم از اطلاعات تعریف کرد که ابعاد مختلفی از هویت، رفتارها، ترجیحات و تعاملات فرد در این محیط‌های آنلاین را در بر می‌گیرد. این داده‌ها شامل موارد زیر است.

–اطلاعات پروفایل کاربر. جزئیاتی مانند نام، سن، جنسیت، موقعیت مکانی، تحصیلات، سابقه کار و سایر اطلاعات بیوگرافی که توسط کاربران ارائه می‌شود.

–داده‌های محتوا و فعالیت. محتوای متنی، عکس‌ها، فیلم‌ها و سایر موارد چندرسانه‌ای که توسط کاربران به اشتراک گذاشته می‌شود، و همچنین اطلاعاتی در مورد فعالیت‌های آنها، مانند لایک‌ها، اشتراک‌گذاری‌ها، نظرات و پست‌ها.

ارتباطات و تعاملات اجتماعی. دوستان، دنبال‌کنندگان و ارتباطاتی که کاربر در پلتفرم‌های رسانه‌های اجتماعی دارد، از جمله پیام‌ها، تعاملات و محتوای مشترک آنها.

داده‌های موقعیت مکانی و دستگاه. اطلاعاتی در مورد موقعیت جغرافیایی کاربران و دستگاه‌هایی که برای دسترسی به پلتفرم‌های رسانه‌های اجتماعی استفاده می‌کنند، از جمله آدرس‌های آی.پی، شناسه‌های دستگاه و جزئیات مرورگر.

داده‌هایی در مورد رفتار و ترجیحات. اطلاعاتی استنتاج‌شده از فعالیت‌های آنلاین کاربران، مانند علایق، سرگرمی‌ها و ترجیحات آنها بر اساس تعامل با محتوا، سابقه مرور و تعامل با تبلیغات.

فراداده. داده‌های اضافی تولیدشده از طریق فعالیت کاربر، مانند برچسب‌های زمانی، جزئیات دستگاه و نرم‌افزار و سایر اطلاعات فنی.

در زمینه پلتفرم‌های رسانه‌های اجتماعی، داده‌های شخصی فراتر از اطلاعات جمعیت‌شناختی اولیه گسترش می‌یابد و شامل یک ردپای دیجیتال جامع می‌شود که نشان‌دهنده رفتار آنلاین، روابط و علایق کاربران است.

– چیستی حریم ارتباطات

از طرف دیگر، حریم ارتباطات نیز باید مورد ملاحظه قرار گیرد. بر این اساس ما اعتقاد داریم حریم خصوصی ارتباطات در پلتفرم‌های شبکه‌های اجتماعی اجتماعی به معنای محافظت و کنترلی است که کاربران بر اطلاعات شخصی، پیام‌ها و تعاملات خود در این محیط‌های آنلاین دارند. این مفهوم، جنبه‌های مختلفی از حفاظت از داده‌های کاربر و تضمین کانال‌های ارتباطی امن و خصوصی بین کاربران را در بر می‌گیرد. تعریفی از حریم خصوصی ارتباطات در پلتفرم‌های شبکه‌های اجتماعی می‌تواند به شرح زیر باشد:

حریم خصوصی ارتباطات در پلتفرم‌های شبکه‌های اجتماعی، توانایی کاربران برای اشتراک‌گذاری ایمن، محرمانه و کنترل‌شده اطلاعات شخصی و پیام‌ها است، با این اطمینان که تعاملات و محتوای آن‌ها در برابر دسترسی، استفاده یا افشای غیرمجاز محافظت می‌شود. این حریم خصوصی شامل عناصر کلیدی زیر است:

–پیام‌رسانی امن[1]: اجرای رمزنگاری همتا با همتا (سرتاسر) یا سایر اقدامات امنیتی برای اطمینان از اینکه پیام‌های رد و بدل شده بین کاربران قابل دسترسی، رهگیری یا دستکاری توسط طرف‌های غیرمجاز، از جمله خود ارائه‌دهندگان پلتفرم، نباشد.

–مکالمات خصوصی[2]: ارائه گزینه‌هایی برای کاربران برای شرکت در مکالمات خصوصی یا گروه‌های بسته که بدون رضایت صریح یا دعوت، برای عموم یا سایر کاربران پلتفرم قابل مشاهده نیستند.

[1] .secure messaging

[2] .private conversation

کنترل محتوا[1]: به کاربران اجازه می‌دهد تا تنظیمات حریم خصوصی خود را انتخاب کنند و کنترل کنند که چه کسی می‌تواند محتوای آن‌ها (پست‌ها، عکس‌ها، فیلم‌ها و غیره) را ببیند، به اشتراک بگذارد یا با آن تعامل داشته باشد.

محافظت از داده‌ها:[2]اطمینان از اینکه داده‌های شخصی کاربران، از جمله اطلاعات تماس، علایق و سابقه مرور آن‌ها، در برابر دسترسی، استفاده یا افشای غیرمجاز محافظت می‌شود.

شفافیت[3]: برقراری ارتباط شفاف در مورد شیوه‌های جمع‌آوری، ذخیره‌سازی و استفاده از داده‌های پلتفرم‌های شبکه‌های اجتماعی، و همچنین هرگونه به اشتراک‌گذاری یا فروش داده‌ها به اشخاص ثالث.

ناشناسی و نام مستعار[4]: به کاربران اجازه می‌دهد تا انتخاب کنند که آیا از نام واقعی خود استفاده کنند یا در حین شرکت در گفتگوها یا تعاملات آنلاین ناشناس یا با نام مستعار باقی بمانند.

در این تعریف حفاظت داده که ما به عنوان حفاظت از داده‌های شخصی مورد بررسی قرار داریم، به‌مثابه بخش یا زیرمجموعه حریم ارتباطات در پلتفرم‌ها تلقی شده است. ما بر این اساس حریم ارتباطات را به عنوان یک مفهوم کلی و حریم داده‌های شخصی را بخشی از آن درنظر می‌گیریم. تعریف حفاظت از داده‌های شخصی در بسترهای شبکه‌های اجتماعی، با در نظر گرفتن ارتباط آن با حریم خصوصی ارتباطات، به شرح زیر است:

حفاظت از داده‌های شخصی در بسترهای شبکه‌های اجتماعی به معنای اجرای اقدامات فنی، حقوقی و سازمانی مختلف برای صیانت از حریم خصوصی، امنیت و صحت اطلاعات شخصی کاربران، از جمله داده‌های ارتباطی، در این محیط‌های آنلاین است. این حفاظت که جزء اصلی حریم خصوصی ارتباطات به شمار می‌رود، شامل عناصر کلیدی زیر است:

ارتباط امن به کارگیری فناوری‌های رمزنگاری برای اطمینان از اینکه پیام‌های رد و بدل شده بین کاربران قابل دسترسی، رهگیری یا دستکاری توسط طرف‌های غیرمجاز نباشد.

کنترل کاربر: ارائه امکان دسترسی، مدیریت و کنترل اطلاعات شخصی کاربران به آن‌ها، مانند ویرایش یا حذف داده‌هایشان و تنظیم تنظیمات حریم خصوصی برای ویژگی‌های ارتباطی.

امنیت داده‌ها: اجرای اقدامات فنی و سازمانی مناسب برای محافظت از داده‌های شخصی کاربران، از جمله فرا داده و محتوای ارتباطات آن‌ها، در برابر دسترسی، استفاده، افشا، تغییر یا نابودی غیرمجاز.

---

[1] .content control
[2] .data protection
[3] .transparency
[4] . Anonymity and pseudonymity

-پردازش داده‌های شخصی

برخی از مفاهیم دیگر نیز برای فهم مقررات عمومی حفاظت از داده‌ها اهمیت دارند. یکی از این مفاهیم پردازش[1] است. پردازش در برخی از مقررات جدیدتر در ایران که مورد بررسی قرار گرفتند به کار رفته بود؛ ازجمله قانون مدیریت داده‌ها و اطلاعات ملی، سند راهبردی جمهوری اسلامی ایران در فضای مجازی و دستورالعمل بهبود حفاظت از حریم خصوصی کاربران؛ اما تعریفی از آن ارائه نشده است.

در جی.دی.پی.آر.، پردازش به این شکل تعریف شده است:

عبارت «پردازش» به معنای هر عملیاتی یا مجموعه عملیاتی است که روی داده‌های شخصی یا مجموعه‌هایی از داده‌های شخصی انجام می‌شود، خواه به صورت خودکار یا غیر خودکار، مانند: گردآوری، ثبت، سازماندهی، ساختاردهی، ذخیره‌سازی، تطبیق یا تغییر، بازیابی، مشورت، استفاده، افشا از طریق انتقال، انتشار یا در دسترس قرار دادن به هر طریق دیگر، هم‌راستا سازی یا ترکیب، محدودسازی، پاک کردن یا نابودی.

بنابراین، معادلی که انصاری (۱۴۰۱) برای پردازش یعنی گردش به کاربرده نادرست و نارسا است و مجموعه معناهای این اصطلاح را دربرنمی‌گیرد. برخی اصطلاحات دیگر نیز در این قانون به پردازش مرتبط هستند. اولین آنها «محدودسازی پردازش[2]» است:

«محدودسازی پردازش» به معنای علامت‌گذاری داده‌های شخصی ذخیره‌شده به منظور محدود کردن پردازش آنها در آینده است.

مفهوم دیگر «پروفایل‌سازی[3]» است:

پروفایل‌سازی به معنای هر شکلی از پردازش خودکار داده‌های شخصی است که شامل استفاده از داده‌های شخصی برای ارزیابی جنبه‌های شخصی خاص مربوط به یک فرد حقیقی می‌شود، به‌ویژه برای تجزیه و تحلیل یا پیش‌بینی جنبه‌هایی از عملکرد آن فرد در کار، وضعیت اقتصادی، سلامت، ترجیحات شخصی، علایق، قابلیت اطمینان، رفتار، موقعیت مکانی یا حرکات او.

---

[1] .processing
[2] . restriction of processing
[3] .profiling

«نام‌مستعارسازی[1]» به معنای پردازش داده‌های شخصی به روشی است که دیگر داده‌های شخصی را بدون استفاده از اطلاعات اضافی نمی‌توان به یک فرد مشخص (موضوع داده) نسبت داد، به شرطی که چنین اطلاعات اضافی به طور جداگانه نگهداری شود و تحت تدابیر فنی و سازمانی برای اطمینان از اینکه داده‌های شخصی به یک فرد حقیقی شناسایی شده یا قابل شناسایی نسبت داده نمی‌شوند، قرار گیرد.

«سامانه بایگانی[2]» به معنای هر مجموعه ساختارمند از داده‌های شخصی است که بر اساس معیارهای خاص قابل دسترسی باشد، خواه متمرکز، غیرمتمرکز یا پراکنده بر اساس عملکردی یا جغرافیایی.

«کنترل‌گر[3]» به معنای شخص حقیقی یا حقوقی، مرجع دولتی، سازمان یا نهاد دیگری است که به تنهایی یا به طور مشترک با دیگران، اهداف و ابزارهای پردازش داده‌های شخصی را تعیین می‌کند؛ در صورتی که اهداف و ابزارهای چنین پردازشی توسط قوانین اتحادیه یا دولت عضو تعیین شود، کنترل‌گرا یا معیارهای خاص برای تعیین آن ممکن است توسط قوانین اتحادیه یا دولت عضو پیش‌بینی شود.

«پردازشگر[4]» به معنای یک شخص حقیقی یا حقوقی، مرجع عمومی، سازمان یا نهاد دیگری است که به نمایندگی از کنترلر، داده‌های شخصی را پردازش می‌کند.

«گیرنده[5]» به معنای یک شخص حقیقی یا حقوقی، نهاد عمومی، سازمان یا نهاد دیگری است که داده‌های شخصی برای آن افشا می‌شود، خواه شخص ثالث باشد یا خیر. با این حال، مقامات عمومی که ممکن است در چارچوب یک تحقیق خاص و مطابق با قوانین اتحادیه یا دولت عضو، داده‌های شخصی را دریافت کنند، به عنوان گیرنده تلقی نمی‌شوند؛ پردازش این داده‌ها توسط آن مقامات عمومی باید مطابق با قوانین و مقررات قابل اجرا در زمینه حفاظت از داده و با توجه به اهداف پردازش باشد.

«طرف ثالث[6]» به معنای یک شخص حقیقی یا حقوقی، مرجع دولتی، سازمان یا نهاد به غیر از موضوع داده، کنترل‌گر، پردازشگر و افرادی است که تحت نظارت مستقیم کنترل‌گر یا پردازشگر مجاز به پردازش داده‌های شخصی هستند.

---

[1] . pseudonymisation
[2] .filing system
[3] .controller
[4] .Processor
[5] .recepient
[6] .third party

-رضایت کاربران

یک مفهوم مهم رضایت است که در ادبیات حریم خصوصی بر آن تأکید زیادی شده است. رضایت در فرهنگ معین به معنای قبول، رضامندی، خشنودی تعریف شده است. در معنای حقوقی رضایت به معنای «قصد انجام عملی بدون شائبه اکراه و اجبار» (تقی‌پوریان، نیک‌بین و اسماعیلی، ۱۴۰۰: ۴۳) تعریف شده است. ظاهراً در معنای رضایت نوعی آگاهی و قصد آگاهانه در شرایط متعارف و در وضعیت روانی و عقلانی متعارف برای پذیرش یک اندیشه یا عمل قابل استنباط است. فقدان اجبار برای یک اقدام به معنای رضایت است. رضایت شامل دادن اجازه برای انجام عملی به شکل خودخواسته و با آگاهی کامل از چیزی است که به آن رضایت می‌دهد و فقدان اجبار یک شرط اساسی است. در جی.دی.پی.آر. رضایت به این شکل تعریف شده است:

رضایت موضوع داده به معنای هرگونه نشانگرِ ارائه‌شده به صورت داوطلبانه، مشخص، آگاهانه و بدون ابهامِ خواسته‌های موضوع داده است که از طریق بیانیه (اظهار) یا یک اقدام تأییدیِ صریح، موافقت خود را با پردازش داده‌های شخصی مربوط به خود اعلام می‌کند.

بنابراین، یک رضایت معتبر باید واجد شرایط زیر باشد:

به صورت آزادانه داده شده باشد: افراد باید حق انتخاب واقعی در مورد ارائه رضایت خود داشته باشند و نباید تحت فشار یا اجبار به دادن آن قرار گیرند؛

مشخص: رضایت باید برای یک هدف خاص یا مجموعه اهداف مرتبط با پردازش داده‌ها اعطا شود و بدون رضایت اضافی نمی‌توان آن را به سایر فعالیت‌های نامرتبط گسترش داد.

آگاهانه: افراد باید درک روشنی از آنچه که به آن رضایت می‌دهند داشته باشند، از جمله انواع داده‌هایی که جمع‌آوری می‌شوند، اهدافی که برای آن استفاده می‌شوند و هرگونه پیامد بالقوه ناشی از ارائه یا عدم ارائه رضایت.

بدون ابهام: نباید هیچ تردید یا سردرگمی در مورد رضایت داده شده یا داده نشده وجود داشته باشد؛ این باید یک اقدام یا اظهار صریح از سوی فرد باشد.

قابل بازپس‌گیری: افراد باید حق داشته باشند در هر زمان رضایت خود را پس بگیرند و فرآیند انجام این کار باید به همان سادگی ارائه رضایت در وهله اول باشد.

«نقض داده‌های شخصی[1]» به معنای نقض امنیتی است که منجر به نابودی، فقدان، تغییر، افشای غیرمجاز، یا دسترسی به داده‌های شخصی منتقل‌شده، ذخیره‌شده یا به نحو دیگری پردازش‌شده، به صورت اتفاقی یا غیرقانونی می‌شود.

فصل دوم: اصول جی.دی.پی.آر

در ماده ۵ اصول مرتبط با پردازش داده‌های شخصی بیان شده است. این بخش هفت اصل[2] حاکم بر پردازش داده‌های شخصی را که در ماده ۵ جی.دی.پی.آر ذکر شده است، ارائه می‌کند: ۱) مشروعیت، انصاف و شفافیت؛ ۲) محدودیت هدف؛۳) به حداقل رساندن داده‌ها؛۴) دقت ؛ ۵) محدودیت نگهداری؛۶) یکپارچگی و محرمانگی؛ ۷) مسئولیت‌پذیری. خلاصه‌ای از این بند در ادامه آورده می‌شود تا این اصول توضیح داده شوند.

قانونی بودن، انصاف و شفافیت: پردازش داده‌ها باید قانونی، عادلانه و برای شخص داده شفاف باشد.

محدودیت هدف: داده‌ها باید برای اهداف مشخص، واضح و قانونی جمع‌آوری شوند و برای اهداف ناسازگار استفاده نشوند.

حداقل‌سازی داده‌ها: فقط داده‌های لازم باید جمع‌آوری و پردازش شوند.

دقت: داده‌ها باید دقیق و به‌روز باشند.

محدودیت ذخیره‌سازی: داده‌ها باید فقط تا زمانی که لازم است نگهداری شوند و به طور ایمن ذخیره شوند.

یکپارچگی و محرمانگی: داده‌ها باید در برابر دسترسی غیرمجاز، از دست رفتن یا آسیب محافظت شوند.

مسئولیت‌پذیری: سازمانی که مسئول داده‌ها است (کنترل‌گر) مسئول اطمینان از رعایت این اصول است.

در اصل، این اصول با ایجاد قوانین روشن برای نحوه مدیریت داده‌های شخصی، هدف از محافظت از حریم خصوصی و حقوق افراد را دارند.

فصل سوم، مادّه‌های مرتبط با حقوق سوژه داده را دربرمی‌گیرند. این بخش ماده ۱۲ تا ۲۳ را دربرمی‌گیرد. این حقوق را در بخش حریم خصوصی کاربر بررسی کردیم.

---

[1] . personal data breach

[2] . 1) lawfulness, fairness and transparency; 2) purpose limitation; 3) data minimisation; 4) accuracy; 5) storage limitation; 6) integrity and confidentiality; 7) accountability.

-کنترل‌گرا و پردازشگر

ماده ۲۴ مسئولیت کنترل‌گر را بیان می‌کند. بر اساس این ماده، کنترل‌گر داده باید اقدامات فنی و سازمانی مناسب را برای اطمینان از اینکه پردازش داده‌ها مطابق با قوانین و مقررات بوده و حقوق و آزادی‌های افراد را محافظت می‌کند، اجرا کند. این اقدامات باید متناسب با فعالیت‌های پردازش داده باشند و ممکن است شامل اتخاذ سیاست‌های مناسب حفاظت از داده‌ها باشد. کنترل‌گر داده باید این اقدامات را به طور مرتب بررسی و به‌روزرسانی کند. رعایت کدهای رفتاری یا مکانیسم‌های صدور گواهینامه تایید شده می‌تواند به عنوان مدرکی برای اثبات رعایت تعهدات مسئول پردازش داده استفاده شود.

خلاصه‌ای از نکات مهم ذکر شده در ماده ۲۸ را که مربوط به *کنترل‌گر* است، به شرح زیر می‌توان بیان کرد:

-کنترل‌گرا باید تنها از پردازشگرهایی استفاده کنند که بتوانند تضمین کنند اقدامات فنی و سازمانی مناسب برای رعایت الزامات قانونی و حفاظت از حقوق افراد داده شده را اجرا می‌کنند.

-پردازشگرها قبل از واگذاری پردازش به پردازشگر دیگر باید مجوز کتبی از کنترل‌گر دریافت کنند.

-در موارد مجوز کتبی عمومی، پردازشگرها باید کنترل‌گرا را از تغییرات مورد نظر در مورد پردازشگرهای دیگر مطلع کنند و به کنترل‌گرها فرصت اعتراض دهند.

-پردازش توسط یک پردازشگر باید تحت قرارداد یا عمل قانونی که جزئیات کلیدی مانند موضوع پردازش، مدت، ماهیت، هدف، انواع داده، دسته‌های افراد داده شده و تعهدات و حقوق مسئول پردازش را مشخص می‌کند، انجام شود.

-قرارداد یا عمل قانونی باید تعهدات خاصی را برای پردازشگر تعیین کند، از جمله:

- پردازش داده‌های شخصی صرفاً بر اساس دستورالعمل‌های مستند از کنترل‌گرا باید انجام شود.
- از اینکه افرادی که داده‌ها را پردازش می‌کنند، ملزم به حفظ محرمانگی هستند، باید اطمینان حاصل شود.
- اقدامات امنیتی لازم باید انجام شود.

پردازش داده از طریق طراحی و به صورت پیش‌فرض

یکی از نکته‌ّهای مهم در این بخش، پردازش داده از طریق طراحی و به صورت پیش‌فرض است. در فصل مربوط به پلتفرمها بحث کردیم که این دو اصل مهم در اصول حریم خصوصی پلتفرم‌ها مورد تأکید قرار گرفته است. به طور خلاصه، حفاظت از داده‌ها از طریق طراحی بر ضرورت ادغام اقدامات حفاظت از داده‌ها در طراحی سیستم‌ها، فرایندها و فناوری‌ها از همان ابتدا تأکید می‌کند. این مفهوم به معنای آن است که سازمان‌ها باید مسائل حفاظت از داده‌ها را در طول توسعه محصولات، خدمات و فرایندهای خود در نظر بگیرند و نه اینکه آن را به عنوان ایده‌ای که بعداً در مورد آن اقدام لازم صورت می‌گیرد قلمداد کنند. این رویکرد شامل اجرای اقدامات فنی و سازمانی مناسب مانند نام‌مستعارسازی، رمزنگاری و کنترل دسترسی برای اطمینان از امنیت و محافظت از داده‌ها در طول چرخه حیات آن است. دمفهوم حفاظت از داده‌ها به صورت پیش‌فرض به این معنی است که حفاظت از داده‌ها باید به صورت پیش‌فرض در سیستم‌ها، فرایندها و فناوری‌ها تعبیه شود بدون نیاز به اقدام خاصی از سوی فرد. این بدان معناست که سختگیرانه‌ترین تنظیمات حریم خصوصی باید هنگام استفاده اولیه از یک محصول یا خدمت اعمال شود و کاربر بتواند در صورت تمایل تنظیمات را کاهش دهد. این رویکرد تضمین می‌کند که داده‌های کاربران از ابتدا تا حد امکان محافظت شوند و خطر نقض داده‌ها یا دسترسی غیرمجاز به اطلاعات شخصی یابد.

در ماده ۲۵ این قاعده ذکر شده است که به طور خلاصه معنای آن این است که کنترل‌گر باید اقدامات فنی و سازمانی مناسب را برای اطمینان از ادغام موثر اصول حفاظت از داده‌ها، مانند حداقل‌سازی داده‌ها، در فعالیت‌های پردازش اجرا کند. این اقدامات باید به گونه‌ای طراحی شوند که از حقوق افراد داده شده محافظت کرده و تضمین کنند که به طور پیش‌فرض تنها داده‌های شخصی ضروری پردازش می‌شوند. این شامل محدود کردن حجم داده‌های جمع‌آوری شده، میزان پردازش، مدت زمان ذخیره‌سازی و دسترسی است. یک مکانیسم صدور گواهینامه تایید شده می‌تواند برای نشان دادن انطباق با این الزامات استفاده شود.

-انتقال داده‌های شخصی به طرفهای سوم یا سازمانهای بین‌المللی

فصل پنجم مقررات عمومی حفاظت از داده‌ها به انتقال داده‌های شخصی به کشورهای سوم یا سازمانهای بین‌المللی متمرکز شده است. ماده ۴۴ اصل کلی انتقال داده‌ها را به شرح زیر بیان کرده است:

هرگونه انتقال داده‌های شخصی که در حال پردازش هستند یا قصد پردازش آن‌ها پس از انتقال به یک کشور ثالث یا یک سازمان بین‌المللی وجود دارد، فقط در صورتی مجاز است که با رعایت سایر شروط این مقررات، شرایط تعیین‌شده در این فصل توسط کنترل‌گر و پردازشگر رعایت شود، از جمله برای انتقال‌های بعدی داده‌های شخصی از کشور ثالث یا یک سازمان بین‌المللی به کشور ثالث دیگر یا سازمان بین‌المللی دیگر. همه مقررات این فصل باید برای اطمینان از حفظ سطح حفاظت از افراد طبیعی تضمین شده توسط این مقررات اعمال شود.

در بخش نخست ماده چهل‌پنج، انتقال بر مبنای تصمیم‌گیری کفایت[1]، گفته شده است که:

انتقال داده‌های شخصی به یک کشور ثالث یا یک سازمان بین‌المللی ممکن است زمانی انجام شود که کمیسیون تصمیم گرفته باشد که کشور ثالث، یک قلمرو یا یک یا چند بخش مشخص در آن کشور ثالث یا سازمان بین‌المللی مورد نظر سطح حفاظت کافی را تضمین می‌کند.

یک پرسش اساسی این است که معیارهای خاص برای تصمیم‌گیری کفایت چیست؟ معیارهای خاص برای تصمیم‌گیری کفایت تحت جی.دی.پی.آر، همانطور که در ماده ۴۵(۲) آمده است، شامل چندین عنصر کلیدی است که کمیسیون اروپا باید هنگام ارزیابی اینکه آیا یک کشور ثالث یا سازمان بین‌المللی سطح کافی از حفاظت داده را فراهم می‌کند، در نظر بگیرد:

-حاکمیت قانون و حقوق بشر: کمیسیون حاکمیت قانون در کشور ثالث، از جمله احترام به حقوق بشر و آزادی‌های اساسی را ارزیابی می‌کند. این شامل قوانین مرتبط، اجرای آن و وجود حقوق موثر و قابل اجرا برای افراد داده شده و همچنین مکانیسم‌های اصلاح اداری و قضایی است.

-مقامات نظارتی مستقل: وجود و عملکرد موثر مقامات حفاظت از داده مستقل در کشور ثالث بسیار مهم است. این مقامات باید دارای اختیارات اجرایی کافی برای نظارت بر رعایت قوانین حفاظت از داده، کمک به افراد داده شده و همکاری با مقامات حفاظت از داده‌های کشورهای عضو اتحادیه اروپا باشند.

[1] .adequacy decision

-تعهدات بین‌المللی: کمیسیون تعهدات بین‌المللی که کشور ثالث یا سازمان انجام داده است را در نظر می‌گیرد، از جمله تعهدات ناشی از کنوانسیون‌های الزام‌آور قانونی یا مشارکت در سیستم‌های چندجانبه یا منطقه‌ای مرتبط با حفاظت از داده.

این معیارها تضمین می‌کنند که سطح حفاظت ارائه شده توسط کشور ثالث یا سازمان اساساً معادل سطح ارائه شده در اتحادیه اروپا است و امکان جریان آزاد داده‌های شخصی بدون اقدامات حفاظتی اضافی را فراهم می‌کند.

شرایط اصلی انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی چیست؟ ماده‌های ۴۴ تا ۵۰ مقررات عمومی حفاظت از داده‌ها به این موضوع اختصاص دارند که در ادامه خلاصه‌ای از مفاد آنها ذکر می‌شود.

انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی مشروط به شرایط خاصی است تا اطمینان حاصل شود که سطح حفاظت ارائه شده به داده‌های افراد تضعیف نمی‌شود. طبق مقررات عمومی حفاظت از داده(GDPR) ، شرایط اصلی برای چنین انتقال‌هایی عبارتند از:

۱) تصمیم کفایت: کمیسیون اروپا ممکن است تصمیم بگیرد که یک کشور ثالث، قلمرو یا سازمان بین‌المللی سطح کافی از حفاظت داده را تضمین می‌کند. در صورت وجود چنین تصمیمی در مورد کفایت، داده‌های شخصی می‌توانند بدون اقدامات حفاظتی اضافی منتقل شوند.

۲) ضمانت‌های مناسب: در غیاب تصمیم کفایت، داده‌ها می‌توانند همچنان در صورت ارائه ضمانت‌های مناسب منتقل شوند، مانند:

-بندهای قراردادی استاندارد[1]: قرارداد انتقال داده پیش‌تأیید شده بین صادرکننده و واردکننده داده که شامل ضمانت‌های حفاظت از داده‌های لازم است.

-قوانین شرکتی الزام‌آور[2] : کدهای رفتاری داخلی که توسط سازمان‌های چند ملیتی برای اطمینان از حفاظت کافی در طول انتقال‌های درون گروهی اتخاذ شده است.

-کدهای رفتار یا مکانیسم‌های صدور گواهینامه: این موارد همچنین می‌توانند برای ارائه ضمانت‌های مناسب برای انتقال استفاده شوند، مشروط بر اینکه توسط مقامات ذی‌ربط تأیید شده باشند.

[1] . Standard Contractual Clauses (SCCs)
[2] . Binding Corporate Rules (BCRs)

–استثنائات برای شرایط خاص: در غیاب تصمیم کفایت یا ضمانت‌های مناسب، انتقال ممکن است همچنان در شرایط خاصی انجام شود، مانند:

رضایت صریح: زمانی که شخص داده پس از اطلاع از خطرات آن، صریحاً به انتقال رضایت داده است.

اجرای قرارداد: اگر انتقال برای اجرای قرارداد بین شخص داده و مسئول پردازش داده ضروری باشد.

منافع عمومی یا ادعاهای قانونی: زمانی که انتقال برای دلایل مهم منافع عمومی یا برای ایجاد، اعمال یا دفاع از ادعاهای قانونی ضروری باشد.

–شرایط اضافی برای داده‌های حساس: برای دسته‌های خاصی از داده‌های شخصی، باید شرایط اضافی مانند رضایت صریح یا پردازش ضروری به دلایل مهم منافع عمومی رعایت شود.

ارزیابی مبنای قانونی مناسب برای انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی ضروری است تا اطمینان حاصل شود که حقوق افراد در طول فرآیند محافظت می‌شود.

–شرایط اضافی برای داده‌های حساس: برای دسته‌های خاصی از داده‌های شخصی، باید شرایط اضافی مانند رضایت صریح یا پردازش ضروری به دلایل مهم منافع عمومی رعایت شود.

ارزیابی مبنای قانونی مناسب برای انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی ضروری است تا اطمینان حاصل شود که حقوق افراد در طول فرآیند محافظت می‌شود.

فصل ششم مقررات عمومی حفاظت از داده‌ها به مقام نظارتی[1] اختصاص دارد. ماده‌های ۵۱ تا ۵۹ جزئیات مربوط به این موضوع را دربرمی‌گیرند. در ماده ۵۱ می‌خوانیم:

۱) هر کشور عضو باید یک یا چند مقام عمومی مستقل را برای مسئولیت نظارت بر اجرای این مقررات تعیین کند تا از حقوق و آزادی‌های اساسی افراد طبیعی در رابطه با پردازش محافظت کند و جریان آزاد داده‌های شخصی در اتحادیه را تسهیل کند («مقام نظارتی»).

۲) هر مقام نظارتی در اجرای ثابت این مقررات در سراسر اتحادیه مشارکت خواهد کرد. ۲ برای این منظور، مقامات نظارتی مطابق با فصل هفتم با یکدیگر و کمیسیون همکاری خواهند کرد.

[1] .supervisory authority

۳) در صورتی که بیش از یک مقام نظارتی در یک کشور عضو ایجاد شود، آن کشور عضو باید مقام نظارتی را که قرار است نماینده آن مقامات در هیئت باشد تعیین کند و مکانیسمی را برای اطمینان از رعایت مقررات مربوط به مکانیسم سازگاری مندرج در ماده ۶۳ توسط سایر مقامات تعیین کند.

۴) هر کشور عضو باید مقررات قانونی خود را که بر اساس این فصل تصویب می‌کند، تا ۲۵ مه ۲۰۱۸ و بدون تأخیر هرگونه اصلاحیه بعدی که بر آنها تأثیر می‌گذارد، به کمیسیون اطلاع دهد.

«استقلال» مقام نظارتی به عنوان یک موضوع مهم در ماده ۵۲ مورد تأیید قرار گرفته است. در بند او این ماده آمده است:

«هر مقام نظارتی در انجام وظایف و اعمال اختیارات خود مطابق با این مقررات با استقلال کامل عمل می‌کند».

در این مورد چند نکته حائز اهمیت است: بی‌طرفی: اعضای مقامات نظارتی باید از تعارض منافع اجتناب کنند؛ منابع: کشورهای عضو باید منابع کافی برای مقامات نظارتی فراهم کنند؛ استقلال کارکنان: مقامات نظارتی باید دارای کارکنان اختصاصی تحت نظارت انحصاری خود باشند؛ استقلال مالی: مقامات نظارتی باید دارای بودجه‌های جداگانه و کنترل مالی باشند که استقلال آن‌ها را به خطر نیندازد.

مقام نظارتی بر اساس ماده ۵۷ وظایف متعدی دارد. برخی از مهترین این وظایف عبارتند از:

-نظارت و اجرای اعمال این مقررات؛

-ترویج آگاهی عمومی و درک مخاطرات، قوانین، اقدامات حفاظتی و حقوق مربوط به پردازش. فعالیت‌های ویژه برای کودکان باید توجه خاصی دریافت کنند؛

-مشاوره با پارلمان ملی، دولت و سایر نهادها و سازمان‌ها در مورد اقدامات قانونی و اداری مربوط به حفاظت از حقوق و آزادی‌های افراد طبیعی در رابطه با پردازش، مطابق با قوانین کشورهای عضو؛

-ترویج آگاهی مسئولان پردازش و پردازشگرها از تعهدات خود تحت این مقررات؛

-ارائه اطلاعات به هر شخص داده شده در مورد اعمال حقوق خود تحت این مقررات، در صورت درخواست، و در صورت لزوم همکاری با مقامات نظارتی در سایر کشورهای عضو برای این منظور.

بر اساس ماده ۵۸) هر مقام نظارتی از اختیارات متعددی برخوردار است که شامل اختیار (قدرت) بازارسی، قدرت تصحیح‌گری، قدرت مشورتی. برای مثال، «دستور دادن به کنترل‌گر و پردازشگر و در صورت لزوم نماینده کنترل‌گر یا پردازشگر برای ارائه هر گونه اطلاعات مورد نیاز برای انجام وظایف خود» (بند۱ الف) (قدرت بازرسی)؛ «صدور اخطار به مسئول پردازش یا پردازشگر مبنی بر اینکه عملیات پردازش مورد نظر احتمالاً با مفاد این مقررات مغایرت دارد» (قدرت تصحیح‌گری) (بند ۲الف).

فصل ۷ مقررات عمومی حفاظت از داده‌ها بر همکاری و هماهنگی بین مقامات نظارتی در اتحادیه اروپا تمرکز دارد. هدف اصلی این فصل اطمینان از اجرای هماهنگ و یکنواخت قوانین حفاظت از داده در سراسر کشورهای عضو اتحادیه اروپا است.

در اینجا مروری بر سه بخش اصلی در فصل ۷ آورده شده است.

بخش ۱: همکاری

این بخش مکانیسم‌های همکاری بین مقامات نظارتی در موارد فرامرزی یا هنگام رسیدگی به شکایات از سوی افراد داده شده را تشریح می‌کند. این بخش شامل مقرراتی برای موارد زیر است:

–مقام نظارتی اصلی[1]: در پردازش فرامرزی، یک مقام نظارتی اصلی برای نظارت بر فعالیت‌های پردازش تعیین می‌شود.

–مکانیسم همکاری: چارچوبی برای تبادل اطلاعات، ارائه کمک متقابل و انجام تحقیقات مشترک بین مقامات نظارتی.

بخش ۲: یکپارچگی

این بخش یک مکانیسم یکپارچگی برای اطمینان از اعمال یکنواخت قوانین حفاظت از داده در سراسر اتحادیه اروپا ایجاد می‌کند. این شامل مقرراتی برای موارد زیر است:

–نظر یکپارچگی: فرآیندی برای درخواست نظر مقامات نظارتی از هیئت حفاظت از داده‌های اروپا[2] در مورد موضوعات مربوط به چندین کشور عضو.

–حل اختلاف: مکانیسمی برای حل اختلاف بین مقامات نظارتی از طریق هیئت حفاظت از داده‌های اروپا.

بخش ۳: هیئت حفاظت از داده‌های اروپا

[1] . Lead supervisory authority

[2] . European Data Protection Board (EDPB)

این بخش نقش و مسئولیت‌های هیئت حفاظت از داده‌های اروپا، یک نهاد مستقل اروپایی مسئول تضمین اجرای یکنواخت قوانین حفاظت از داده در سراسر اتحادیه اروپا را تشریح می‌کند. هیئت حفاظت از داده‌های اروپا این وظایف را برعهده دارد:

– ارائه راهنمایی و توصیه در مورد مسائل حفاظت از داده.

–صدور نظرات در مورد معیارهای صدور گواهینامه، کدهای رفتار و یکپارچگی.

–ارتقای همکاری و اجرای موثر بین مقامات نظارتی.

به طور کلی، فصل ۷ — ماده‌های ۶۰ تا ۷۶–مقررات عمومی حفاظت از داده‌ها با هدف ایجاد یک رویکرد مشارکتی و یکپارچه در حفاظت از داده‌ها در اتحادیه اروپا، اطمینان از حفاظت مؤثر از حقوق افراد و رعایت تعهدات سازمان‌ها تحت جی.دی.پی.آر است.

فصل ۸ مقررات عمومی حفاظت از داده مقررات مربوط به جبران خسارت، مسئولیت و مجازات در صورت عدم رعایت مقررات حفاظت از داده را تشریح می‌کند. این فصل شامل سه بخش اصلی است:

بخش ۱: جبران خسارت

این بخش بر حقوق افراد داده شده در صورتی که داده‌های شخصی آن‌ها به طور غیرقانونی پردازش شده است تمرکز دارد. این بخش شامل مقرراتی برای موارد زیر است:

–ثبت شکایت: افراد موضوع داده حق دارند در صورتی که معتقدند داده‌های آن‌ها با نقض جی.د.پی.آر پردازش شده است، شکایتی را به یک مقام نظارتی ثبت کنند.

– اقدامات قضایی: افراد موضوع داده حق دارند علیه تصمیمات مقامات نظارتی یا کنترل‌گر/پردازشگرهای داده که حقوق آن‌ها را تحت جی.د.پی.آر تحت تأثیر قرار می‌دهد، به دنبال یک اقدام قضایی مؤثر باشند.

–غرامت و مسئولیت: افراد موضوع داده می‌توانند در صورتی که به دلیل نقض جی.د.پی.آر متحمل خسارت مادی یا غیرمادی شوند، از کنترل‌گرها یا پردازشگرهای داده غرامت مطالبه کنند.

بخش ۲: مسئولیت کنترل‌گر و پردازشگر

این بخش مسئولیت کنترل‌گرها و پردازشگرها را برای هرگونه خسارت ناشی از پردازش غیرقانونی داده‌های شخصی مشخص می‌کند:

-کنترل‌گر مسئول خسارات ناشی از پردازشی است که توسط کنترل‌گر یا به نمایندگی از آن توسط یک پردازشگر انجام شده است.

-پردازشگر مسئول خسارات ناشی از پردازش است اگر تعهدات خود را تحت جی.د.پی.آر رعایت نکرده باشد یا خارج از یا خلاف دستورالعمل‌های قانونی کنترل‌گر عمل کرده باشد.

هر دو کنترل‌گر و پردازشگر می‌توانند در صورت مسئولیت هرگونه خسارت ناشی از پردازش، مسئولیت کامل را بر عهده بگیرند.

-بخش ۳: تحریم‌ها و مجازات‌ها

این بخش جریمه‌هایی را که می‌توان برای عدم رعایت جی.د.پی.آر اعمال کرد، تشریح می‌کند:

-مقامات نظارتی می‌توانند برای تخلفات شدید مانند نقض اصول حفاظت از داده یا قوانین انتقال داده‌های فرامرزی، جریمه‌های اجرایی تا ۲۰ میلیون یورو یا ۴ درصد گردش مالی جهانی سالانه یک شرکت را اعمال کنند، هر کدام که بیشتر باشد.

-جریمه‌های پایین‌تر تا ۱۰ میلیون یورو یا ۲ درصد گردش مالی جهانی سالانه یک شرکت را می‌توان برای تخلفات کمتر جدی مانند نگهداری ناکافی سوابق یا عدم همکاری با مقامات نظارتی اعمال کرد.

-قوانین ملی می‌توانند مجازات‌های اضافی مانند تحریم‌های کیفری برای برخی تخلفات را مشخص کنند.

در نتیجه، فصل ۸ جی.د.پی.آر به گونه‌ای طراحی شده است تا برای افراد موضوع داده که حقوق آن‌ها نقض شده است، اقدامات قانونی فراهم کند، مسئولیت کنترل‌گرها و پردازشگرهای داده را تعیین کند و با استفاده از جریمه‌های مالی قابل توجه، از عدم رعایت مقررات جلوگیری کند.

فصل نهم شامل ماده‌های ۸۶ تا ۹۱ مقررات مربوط به شرایط پردازش خاص را بیان کرده است:

ماده ۸۵: پردازش و آزادی بیان و اطلاعات

ماده ۸۶: پردازش و دسترسی عمومی به اسناد رسمی

ماده ۸۷: پردازش شماره شناسایی ملی

ماده ۸۸: پردازش در زمینه اشتغال

ماده ۸۹: ضمانت‌ها و استثنائات مربوط به پردازش برای اهداف بایگانی‌سازی به نفع عموم، اهداف تحقیقات علمی یا تاریخی یا اهداف آماری

ماده ۹۰: تعهدات رازداری

ماده ۹۱: قوانین موجود حفاظت از داده کلیساها و انجمن‌های مذهبی

در بند ۲ ماده ۸۵ که مربوط به پردازش و آزادی بیان و اطلاعات است می‌خوانیم: «دولت‌های عضو موظفند از طریق قانون، حق حفاظت از داده‌های شخصی مطابق با این مقررات را با حق آزادی بیان و اطلاعات، از جمله پردازش برای اهداف روزنامه‌نگاری و اهداف بیان علمی، هنری یا ادبی، هماهنگ کنند». ماده ۸۶ این قانون با عنوان پردازش و دسترسی عمومی به اسناد رسمی مقرر می‌دارد: «داده‌های شخصی موجود در اسناد رسمی که توسط یک مقام عمومی یا یک نهاد عمومی یا یک نهاد خصوصی برای انجام یک وظیفه در منافع عمومی نگهداری می‌شود، ممکن است توسط مقام یا نهاد مطابق با قوانین اتحادیه یا کشور عضو که مقام عمومی یا نهاد تابع آن است، به منظور سازگاری دسترسی عمومی به اسناد رسمی با حق حفاظت از داده‌های شخصی مطابق با این مقررات افشا شود».

مقررات عمومی دو فصل دیگر نیز دارد که شامل فصل دهم، تصمیمات تفویضی و اجرایی و نیز فصل یازدم مقررات نهایی است.

قانون حریم خصوصی مصرف‌کننده کالیفرنیا[1]

قانون حفاظت از حریم خصوصی مصرف‌کننده کالیفرنیا (سی.سی.پی.ای) در سال ۲۰۱۸ یک قانون جامع حفاظت از داده‌ها است که حقوق حریم خصوصی و حمایت از مصرف‌کننده را برای ساکنان ایالت کالیفرنیا افزایش می‌دهد. سی.سی.پی.ای که از اول ژانویه ۲۰۲۰ اجرایی شد، تأثیر قابل توجهی بر نحوه برخورد کسب‌وکارها با اطلاعات شخصی ساکنان کالیفرنیا دارد.

[1] . California Consumer Privacy Act

قانون حفاظت از حریم خصوصی مصرف‌کننده کالیفرنیا قانونی است که به مصرف‌کنندگان کالیفرنیا امکان محافظت از حریم خصوصی خود را فراهم می‌کند. از اول ژانویه ۲۰۲۰، مشاغلی که اطلاعات شخصی ساکنان کالیفرنیا را جمع‌آوری می‌کنند، باید با این تعهدات مطابقت کنند. رای دهندگان کالیفرنیا با رأی دادن به قانون حقوق خصوصی کالیفرنیا در انتخابات نوامبر ۲۰۲۰ قانون حفظ حریم خصوصی مصرف‌کنندگان کالیفرنیا را اصلاح و گسترش دادند. قانون جدید حفظ حریم خصوصی ایالت کالیفرنیا[1]، مفاد موجود سی.سی.پی.ای را تشریح می‌کند، حقوق مصرف کننده جدید ایجاد می کند، بر مشاغلی که اطلاعات شخصی مصرف کنندگان کالیفرنیا را جمع آوری می کنند، تعهدات اضافی تحمیل می کند و یک آژانس اجرایی جدید به نام آژانس حفاظت از حریم خصوصی کالیفرنیا[2] ایجاد کرده است. گرچه مسئولیت اجرای قانون حفاظت از حریم خصوصی مصرف‌کننده کالیفرنیا در اختیار دفتر دادستانی کل کالیفرنیا بوده اما بر اساس قانون حفاظت از حریم خصوصی کالیفرنیا آژانس حفاظت از حریم خصوصی کالیفرنیا[3] برای اعمال و اجرای قانون تأسیس شد که مسئولیت هایی از جمله اعمال و اجرای قانون و آموزش مردم در مورد حقوق مصرف کنندگان و تعهدات تجاری بر اساس قانون را بر عهده گرفت.

قانون حفظ حریم خصوصی مصرف کنندگان کالیفرنیا به مصرف کنندگان حقوق خاصی را در مورد اطلاعات شخصی که کسب و کارها درباره آنها جمع آوری می کنند اعطا می کند و از کسب و کارها می خواهد که مصرف کنندگان را در مورد نحوه جمع آوری، استفاده، افشا و حفظ اطلاعات شخصی خود آگاه کنند. این قانون مهم اولین قانون جامع حفظ حریم خصوصی مصرف کنندگان بود که در ایالات متحده تصویب شد.

مرور قانون حریم خصوصی مصرف‌کننده کالیفرنیا

ما در اینجا به شکل اجمالی قانون حریم خصوصی مصرف‌کننده کالیفرنیا را مرور می‌کنیم. مرور قانون حریم خصوصی مصرف‌کننده کالیفرنیا از این جهت اهمیت دارد که بر حریم داده‌ها تمرکز دارد. در این بخش مرور کلی بر این قانون انجام می‌شود. نسبت به مقررات عمومی حفاظت از داده‌های اتحادیه اروپا این تحلیل مختصرتر و به شکل مقایسه‌ای انجام خواهد

[1] . California Privacy Rights Act (CPRA)
[2] . the California Privacy Protection Agency
[3] . California Privacy Protection Agency

شد. این مقایسه از منظر تعاریف، حقوق مصرف‌کننده، مجازات‌ها و نهادسازی است. تمرکز بر این موضوعات امکان مقایسه و نیز امکان توجه به جزئیات بیشتر در ارائه پیشنهاد پیش‌نویس نهایی را فراهم می‌کند.

تعاریف

اولین موضوعی که به آن توجه می‌کنیم تعاریف است. ازجمله اینکه چه تعریفی از حریم داده ارائه شده است. در قانون مصرف‌کننده تعاریف، برخلاف جی.دی.پی.آر بر اساس حروف الفبا است و نه اهمیت مفهوم.

-تعریف اطلاعات شخصی

در این قانون «اطلاعات شخصی» به این شکل تعریف شده است:

«اطلاعات شخصی» به معنای اطلاعاتی است که یک مصرف‌کننده یا خانوار[1] را شناسایی می‌کند، به آن مرتبط است، آن را توصیف می‌کند، به شکلی معقول آنرا تداعی می‌کند و یا به شکل معقول می‌تواند به آن پیوند بخورد، به‌شکلی مستقیم و غیرمستقیم.

نکته جالب توجه در این تعریف، تعمیم سوژه‌ای که در مورد وی اطلاعات گردآوری می‌شود، از شخص به خانوار است. بنابراین، واحد گردآوری از شخص تا خانواده وی تعمیم پیدا می‌کند. از سوی دیگر، در این تعریف تلاش شده است تا تمام امکانّ‌های شناسایی فرد از طریق اطلاعات شخصی وی مورد توجه قرار گیرد. بنابراین، این قانون نسبت به جی.دی.پی.آر استحکام بیشتری از منظر شناسایی فرد دارد. اطلاعاتی که سبب شناسایی یک مصرف‌کننده می‌شوند، موضوع محوری این قانون است و طیف گسترده‌ای را دربرمی‌گیرند:

– شناسه‌هایی مانند نام واقعی، نام مستعار، آدرس پستی، شناسه شخصی منحصر به فرد، شناسه آنلاین، آدرس پروتکل اینترنت، آدرس ایمیل، نام حساب، شماره تامین اجتماعی، شماره گواهینامه رانندگی، شماره پاسپورت یا سایر شناسه‌های مشابه

– هر گونه اطلاعات شخصی که در بخش فرعی (ای) بخش ۱۷۹۸,۸۰ توضیح داده شده است[2].

[1] .household

[2]) که به نظر می‌رسد قانون حفاظت از حریم خصوصی کالیفرنیا California Civil Code 2009. منظور از آن نظام‌نامه (قانون) مدنی کالیفرنیا در سال ۲۰۰۹ است (نوعی اصلاحیه به آن باشد اما مبتنی بر آن نیست زیرا قانون حریم مصرف‌کننده کالیفرنیا به شکلی قابل ملاحظه نوع مقررات‌گذاری جدید است که با هدف توجه به چالشهای نوین حریم داده در عصر دیجیتال طراحی شده است. قانون مدنی کالیفرنیا مجموعه‌ای از قوانین ایالت کالیفرنیا است. این قانون از قوانینی تشکیل شده است که بر

–اطلاعات تجاری، از جمله سوابق دارایی شخصی، محصولات یا خدماتی که خریداری، اخذ یا مورد توجه قرار گرفته‌اند، یا سایر تاریخچه‌ها یا گرایش‌های خرید یا مصرف.

–اطلاعات بیومتریک.

–اطلاعات فعالیت اینترنتی یا شبکه الکترونیکی دیگر، از جمله اما نه محدود به تاریخچه مرور، تاریخچه جستجو و اطلاعات مربوط به تعامل مصرف‌کننده با یک وب‌سایت، اپلیکیشن یا تبلیغات اینترنتی.

– داده‌های موقعیت مکانی.

–اطلاعات صوتی، الکترونیکی، تصویری، حرارتی، بویایی یا مشابه.

–اطلاعات حرفه‌ای یا مربوط به اشتغال.

–اطلاعات آموزشی، تعریف‌شده به عنوان اطلاعاتی که به صورت عمومی در دسترس نیست و به عنوان اطلاعات شخصی قابل شناسایی در قانون حقوق آموزشی و حریم خصوصی خانواده.

–استنتاج‌های حاصل از هر یک از اطلاعات مشخص‌شده در این زیربخش برای ایجاد یک پروفایل در مورد مصرف‌کننده که منعکس‌کننده ترجیحات، ویژگی‌ها، گرایش‌های روانشناختی، مستعد بودن، رفتار، نگرش‌ها، هوش، توانایی‌ها و استعدادهای مصرف‌کننده است.

–اطلاعات شخصی حساس.

-معنای اطلاعات شخصی حساس

در این قانون منظور از اطلاعات شخصی حساس به این شکل بیان شده است:

اطلاعات شخصی حساس به این معنا است:

۱– اطلاعات شخصی که (موارد زیر را) افشاء می‌کند:

الف) شماره تامین اجتماعی، گواهینامه رانندگی، کارت شناسایی دولتی یا گذرنامه یک مصرف‌کننده.

ب) اطلاعات ورود به حساب، حساب مالی، کارت بدهی یا کارت اعتباری یک مصرف‌کننده همراه با هر کد امنیتی یا دسترسی مورد نیاز، رمز عبور یا اعتبارنامه برای دسترسی به حساب.

ج) موقعیت مکانی دقیق یک مصرف‌کننده.

تعهدات و حقوق عمومی افراد در حوزه قضایی کالیفرنیا حاکم است شناسه‌ّهای ذکر شده در بند ای بخش ۱۷۹۸,۸۰ قانون مدنی ۲۰۰۹ کالیفرنیا که در مورد تعریف اطلاعات شخصی است، عبارتند از: نام، امضا، شماره تامین اجتماعی، مشخصات فیزیکی یا توضیحات، آدرس، شماره تلفن، شماره پاسپورت، گواهینامه رانندگی یا کارت شناسایی دولتی، شماره بیمه نامه، تحصیلات، اشتغال، سابقه اشتغال، شماره حساب بانکی، شماره کارت اعتباری، شماره کارت نقدی، یا هر گونه اطلاعات مالی، اطلاعات پزشکی، یا اطلاعات بیمه درمانی دیگر. "اطلاعات شخصی" شامل اطلاعات در دسترس عموم نیست که به طور قانونی از سوابق فدرال، ایالتی یا دولت محلی در دسترس عموم قرار گرفته است.

د) نژاد یا قومیت، تابعیت یا وضعیت مهاجرتی، باورهای مذهبی یا فلسفی، یا عضویت صنفی یک مصرف‌کننده.

ه) محتوای نامه، ایمیل و پیام‌های متنی یک مصرف‌کننده مگر اینکه کسب‌وکار گیرنده مورد نظر ارتباط باشد.

و) داده‌های ژنتیکی یک مصرف‌کننده.

۲- پردازش اطلاعات بیومتریک برای شناسایی منحصر به فرد یک مصرف‌کننده.

الف) اطلاعات شخصی جمع‌آوری و تحلیل شده در مورد سلامت یک مصرف‌کننده.

ب) اطلاعات شخصی جمع‌آوری و تحلیل شده در مورد زندگی جنسی یا گرایش جنسی یک مصرف‌کننده.

در مورد اینکه کدام از دسته‌ها داده‌ها دیگر اطلاعات شخصی محسوب نمی‌شود، در این قانون شرایطی ذکر شده است. بر این اساس، «اطلاعات شخصی» شامل این موارد نمی‌شود: اطلاعاتی که به شکل عمومی در دسترس قرار گرفته‌اند یا اطلاعات واقعی که به طور قانونی به دست آمده و موضوع نگرانی عمومی است. برای اهداف این بند، «عمومی در دسترس» به معنای اطلاعاتی است که به طور قانونی از سوابق دولت فدرال، ایالتی یا محلی در دسترس قرار گرفته است، یا شامل اطلاعاتی است که یک کسب‌وکار دلایل قانونی دارد که آن اطلاعات به طور قانونی توسط مصرف‌کننده یا از طریق رسانه‌های گسترده در دسترس عموم قرار گرفته است و یا اینکه اطلاعات به دست آمده شامل اطلاعاتی است که فرد دارنده آن اطلاعات دسترسی به آنرا محدود نکرده است. «عمومی در دسترس» به معنای اطلاعات بیومتریک جمع‌آوری شده توسط یک کسب‌وکار در مورد یک مصرف‌کننده بدون اطلاع مصرف‌کننده نیست. و همچنین «اطلاعات شخصی» شامل اطلاعات مصرف‌کننده‌ای که ناشناس‌سازی شده یا اطلاعات جمعی مصرف‌کننده است، نمی‌شود.

بنابراین، اطلاعاتی که بر اساس برخی شرایط معقول در دسترس عمومی قرار گرفته‌اند یعنی اینکه به شکل عمومی در دسترس قرار دارند- از طریق مقامات یا رسانه‌های عمومی و اطلاعاتی که دسترسی به آنها توسط دارنده اطلاعات محدود نشده است، و یا اینکه اطلاعات ناشناس‌سازی شده باشند، شامل نمی‌شود.

-معنای پردازش اطلاعات شخصی

در این قانون **پردازش** یک تعریف محدود و فراگیر دارد. «پردازش» به معنای هرگونه عملیات یا مجموعه عملیاتی است که بر روی اطلاعات شخصی یا مجموعه‌هایی از اطلاعات شخصی انجام می‌شود، صرف نظر از اینکه این عملیات به صورت خودکار انجام شود یا نشود.

فروش داده نیز به این شکل تعریف شده است: واژه فروش «به معنای فروش، اجاره، انتشار، افشاء، پخش، در دسترس قرار دادن، انتقال یا به هر نحو دیگر ارتباط کلامی، کتبی یا الکترونیکی یا سایر روش‌ها، اطلاعات شخصی مصرف‌کننده توسط کسب‌وکار به شخص ثالث در ازای مبلغ یا ارزش مادی دیگر است».

در این قانون «طرف ثالث» ممکن است شامل دسته‌بندی سه‌گانه زیر شود:

-کسب‌وکاری که مصرف‌کننده به‌طور عمدی با آن تعامل دارد و آن کسب‌وکار در چارچوب این قانون، اطلاعات شخصی مصرف‌کننده را به‌عنوان بخشی از تعامل جاری مصرف‌کننده با کسب‌وکار جمع‌آوری می‌کند.

-ارائه‌دهنده خدمات به کسب‌وکارها.

-پیمانکار.

-مفهوم رضایت

رضایت در این قانون، به شکل مفصل و باجزئیات تعریف شده است:

رضایت به معنای هرگونه اعلامیه آزادانه، مشخص، آگاهانه و بدون ابهام از سوی مصرف‌کننده است که به موجب آن، مصرف‌کننده یا قیم قانونی مصرف‌کننده، فرد دارای وکالتنامه یا فردی که به عنوان قیم برای مصرف‌کننده عمل می‌کند، از جمله با یک بیانیه یا یک اقدام تأییدی روشن، موافقت خود را با پردازش اطلاعات شخصی مربوط به مصرف‌کننده برای یک هدف خاص و دقیق مشخص می‌کند. پذیرش شرایط عمومی یا گسترده استفاده یا اسناد مشابه که شامل توصیف پردازش اطلاعات شخصی همراه با اطلاعات دیگر و بی‌ربط است، رضایت محسوب نمی‌شود. حرکت دادن موس بر روی محتوا، قطع صدا، مکث یا بستن یک محتوای خاص رضایت محسوب نمی‌شود. همچنین، توافقی که از طریق استفاده از الگوهای تاریک به دست آمده است، رضایت محسوب نمی‌شود.

-وظایف کسب‌وکارها نسبت به داده‌های کاربران

وظایف کسب‌وکارها در برابر داده‌های مصرف‌کنندگان

بر اساس قانون حفاظت از حریم خصوصی مصرف‌کننده کالیفرنیا در سال ۲۰۱۸، کسب‌وکارهایی که اطلاعات شخصی مصرف‌کنندگان کالیفرنیا را جمع‌آوری می‌کنند، چندین وظیفه و مسئولیت عمومی دارند، از جمله:

ارائه اطلاعیه در هنگام جمع‌آوری: کسب‌وکارها باید مصرف‌کنندگان را در مورد دسته‌های اطلاعات شخصی جمع‌آوری شده و اهداف استفاده از این اطلاعات مطلع کنند. این اطلاعیه باید در زمان یا قبل از جمع‌آوری داده‌ها ارائه شود.

پاسخگویی به درخواست‌های مصرف‌کنندگان: کسب‌وکارها باید به مصرف‌کنندگان امکان درخواست دسترسی به اطلاعات شخصی خود، حذف اطلاعات شخصی خود و حق انتخاب عدم فروش اطلاعات شخصی خود را بدهند. آنها موظفند ظرف مدت مشخص، معمولاً ۴۵ روز، به این درخواست‌ها پاسخ دهند.

حفظ اقدامات امنیتی مناسب: کسب‌وکارها باید اقدامات امنیتی مناسب را اجرا و حفظ کنند تا از دسترسی، تخریب، استفاده، تغییر یا افشای غیرمجاز اطلاعات شخصی محافظت کنند.

عدم تبعیض: کسب‌وکارها نمی‌توانند علیه مصرف‌کنندگانی که از حقوق خود تحت CCPA استفاده می‌کنند، تبعیض قائل شوند، مانند امتناع از ارائه کالا یا خدمات، دریافت قیمت‌های متفاوت یا ارائه سطح یا کیفیت خدمات متفاوت.

به‌روزرسانی سیاست‌های حفظ حریم خصوصی: کسب‌وکارها باید سیاست‌های حفظ حریم خصوصی خود را به‌روزرسانی کنند تا شامل توصیفی از حقوق مصرف‌کنندگان تحت سی.سی.پی.ای، روش‌های ارسال درخواست‌ها و لیستی از دسته‌های اطلاعات شخصی جمع‌آوری، فروش یا افشا شده برای یک هدف تجاری طی دوازده ما گذشته.

آموزش کارکنان: کسب‌وکارها باید اطمینان حاصل کنند که کارمندان آنها برای پاسخگویی به درخواست‌های مصرف‌کنندگان و انطابق با الزامات سی.سی.پی.ای آموزش دیده‌اند.

به طور خلاصه، کسب‌وکارهایی که اطلاعات شخصی را گردآوری می‌کنند، موظفند نسبت به کردارهای گردآوری داده خود شفاف باشند و امکان کنترل مصرف‌کنندگان بر اطلاعات شخصی‌شان را فراهم کنند، داده‌ها را امن نگه دارند و از عدم تبعیض اطمینان حاصل کنند.

-حقوق مصرف‌کنندگان در برابر داده‌های شخصی

در این قانون برخی حقوق برای مصرف‌کنندگان درنظر گرفته شده است که به طور اختصار آنها را ذکر می‌کنیم:

- حق حذف اطلاعات شخصی مصرف‌کننده: یک مصرف‌کننده حق دارد درخواست کند که یک کسب‌وکار هرگونه اطلاعات شخصی در مورد مصرف‌کننده که کسب‌وکار از مصرف‌کننده جمع‌آوری کرده است را حذف کند.
- حق تصحیح اطلاعات شخصی نادرست مصرف‌کننده: یک مصرف‌کننده حق دارد از یک کسب‌وکاری که اطلاعات شخصی نادرستی در مورد مصرف‌کننده نگهداری می‌کند درخواست کند تا آن اطلاعات شخصی نادرست را اصلاح کند، با در نظر گرفتن ماهیت اطلاعات شخصی و اهداف پردازش اطلاعات شخصی.
- حق دانستن اینکه چه اطلاعات شخصی جمع‌آوری می‌شود: یک مصرف‌کننده حق دارد از یک کسب‌وکاری که اطلاعات شخصی در مورد مصرف‌کننده جمع‌آوری می‌کند درخواست کند موارد زیر را به مصرف‌کننده افشاء کند:۱) دسته‌های اطلاعات شخصی که در مورد آن مصرف‌کننده جمع‌آوری کرده است. ۲)دسته‌های منابعی که اطلاعات شخصی از آن‌ها جمع‌آوری شده است.۳) هدف مالی یا تجاری برای جمع‌آوری، فروش یا اشتراک‌گذاری اطلاعات شخصی. ۴) دسته‌های اشخاص ثالثی که کسب‌وکار اطلاعات شخصی را به آن‌ها افشاء می‌کند. ۵) قطعات خاص اطلاعات شخصی که در مورد آن مصرف‌کننده جمع‌آوری کرده است.
- حق دسترسی به اطلاعات شخصی: یک مصرف‌کننده حق دارد از یک کسب‌وکاری که اطلاعات شخصی مصرف‌کننده را می‌فروشد یا به اشتراک می‌گذارد یا آن را برای یک هدف تجاری افشاء می‌کند درخواست کند دسته‌های اطلاعات شخصی که کسب‌وکار در مورد آن مصرف‌کننده جمع‌آوری کرده است، افشاء کند.
- حق دانستن اینکه چه اطلاعات شخصی فروخته یا به اشتراک گذاشته شده و به چه کسی: یک مصرف‌کننده حق دارد در هر زمان، به یک کسب‌وکاری که اطلاعات شخصی مصرف‌کننده را به اشخاص ثالث می‌فروشد یا به اشتراک می‌گذارد، دستور دهد که اطلاعات شخصی مصرف‌کننده را نفروشد یا به اشتراک نگذارد. این حق ممکن است به عنوان حق انتخاب عدم فروش یا اشتراک‌گذاری نامیده شود.
- حق انتخاب عدم فروش یا اشتراک‌گذاری اطلاعات شخصی: یک مصرف‌کننده حق دارد هر زمان به کسب‌وکاری که اطلاعات شخصی حساس او را جمع‌آوری می‌کند، دستور دهد تا استفاده از اطلاعات شخصی حساس او را محدود به استفاده‌ای کند که برای ارائه خدمات یا کالاهای مورد انتظار از یک مصرف‌کننده متوسط که آن کالاها یا خدمات را درخواست می‌کند.

نهادسازی برای اجرای قانون حفاظت از حریم خصوصی کالیفرنیا

آژانس حفاظت از حریم خصوصی کالیفرنیا مسئول اجرای قانون و حفاظت از حریم خصوصی شهروندان ایالت کالیفرنیا است. همانطور که در بخش درباره ما این نهاد آمده است: قانون حقوق حریم خصوصی کالیفرنیا یک نهاد جدید به نام آژانس حفاظت از حریم خصوصی کالیفرنیا برای اعمال و اجرای قانون ایجاد کرد. این نهاد توسط یک هیئت پنج نفره

اداره می‌شود. مسئولیت‌های دیگر این نهاد که به طور اختصاری «آژانس» نامیده می‌شود شامل به‌روزرسانی مقررات کنونی و نیز تصویب مقررات جدید است.

وظایف عمده این نهاد را بر اساس قانون حفاظت از حریم خصوصی مصرف‌کنندگان به شرح زیر در جدول ۸-۴ خلاصه شده است:

نکات اصلی	توصیف
اجرای سی.سی.پی.ای	این آژانس مسئول اجرای قانون حفاظت از حریم خصوصی مصرف‌کننده کالیفرنیا (سی.سی.پی.ای) از طریق اقدامات اداری است.
ایجاد مقررات سی.سی.پی.ای	این آژانس اختیار وضع، اصلاح و لغو مقررات برای اجرای سی.سی.پی.ای را دارد.
حفاظت از حقوق حریم خصوصی مصرف‌کننده:	وظیفه این آژانس حفاظت از حقوق اساسی حریم خصوصی مصرف‌کنندگان در رابطه با استفاده از اطلاعات شخصی آن‌ها است.
ترویج آگاهی عمومی از حریم خصوصی:	این آژانس موظف است آگاهی و درک عمومی از حقوق و خطرات حریم خصوصی را ارتقاء دهد.
راهنمایی مصرف‌کنندگان و کسب‌وکارها	این آژانس مسئول ارائه راهنمایی به مصرف‌کنندگان و کسب‌وکارها در مورد حقوق و مسئولیت‌های آن‌ها تحت سی.سی.پی.ای است.
کمک به قانون‌گذاری در زمینه حریم خصوصی:	این آژانس می‌تواند به قوه مقننه در زمینه قوانین مربوط به حریم خصوصی مشاوره و کمک فنی ارائه دهد.
نظارت بر تحولات حریم خصوصی:	این آژانس موظف است تحولات مرتبط با حفاظت از اطلاعات شخصی را رصد کند.
همکاری با سایر مقامات حریم خصوصی:	این آژانس می‌تواند با سایر آژانس‌های دارای صلاحیت در قوانین حریم خصوصی برای اطمینان از اجرای یکسان حفاظت از حریم

	خصوصی همکاری کند.
ارائه برنامه انطباق اختیاری برای کسب‌وکارهای کوچک:	این آژانس می‌تواند برنامه‌ای ایجاد کند که به کسب‌وکارهای کوچک اجازه می‌دهد انطباق خود با سی.سی.پی.ای را به صورت اختیاری گواهی کنند.
توازن بین حریم خصوصی مصرف‌کننده و منافع تجاری:	این آژانس موظف است بین اهداف تقویت حریم خصوصی مصرف‌کننده و توجه به تأثیر آن بر کسب‌وکارها تعادل برقرار کند.

جدول ۸-۴) وظایف آژانس حفاظت از حریم خصوصی کالیفرنیا

برنامه استراتژیک سی.پی.پی.ای. ۲۰۲۴-۲۰۲۷[1] مأموریت و ارزش‌های اصلی سازمانی ما را بیان می‌کند و تعهد ما به حفاظت از حریم خصوصی مصرف‌کننده را از طریق اهداف و مقاصد روشن ارتقا می‌دهد (وب‌گاه آژانس حفاظت از حریم خصوصی کالیفرنیا، ۲۰۲۴).

بر اساس محتوای این برنامه راهبردی، قانون حفاظت از حریم مصرف‌کننده کالیفرنیا (۲۰۱۸) اولین قانون جامع حفاظت از حریم خصوصی در ایالات متحده است که آژانس حفاظت از حریم خصوصی کالیفرنیا برمبنای آن تأسیس شد که مأموریت آن اجرا، اعمال و آفزایش آگاهی درباره حفاظت از حریم خصوصی است. در این برنامه راهبردی ارکان این نهاد (بخش اداری، بخش حسابرسی (ممیزی)، بخش اجرای قانون، بخش اجرایی، بخش فناوری اطلاعات، بخش قانونی، بخش سیاستگذاری و قانونگذاری و بخش امور عمومی و خارجی است. در این برنامه راهبردی مجموعه‌ای از اهداف، چشم‌انداز، مأموریت و ارزشها ذکر شده است که عبارتند از:

چشم‌انداز

حفاظت از حریم خصوصی برای همه کالیفرنیایی‌ها

مأموریت

محافظت از حریم خصوصی کالیفرنیایی‌ها، اطمینان از آگاهی مصرف‌کنندگان از حقوق خود، آگاهی کسب‌وکارها از تعهداتشان، و اجرای جدی قانون علیه کسب‌وکارهایی که حقوق حریم خصوصی مصرف‌کنندگان را نقض می‌کنند.

[1] . CPPA 2024-2027

ارزش‌ها

ارزش‌های اصلی ما نشان‌دهنده نحوه تعامل ما با یکدیگر و ذینفعان ما است. آن‌ها رفتارهای روزانه و تصمیم‌گیری‌های ما را هدایت می‌کنند و به ما امکان می‌دهند به مأموریت مشترک خود دست یابیم.

برتری: ما برای خودمان استاندارد بالایی تعیین می‌کنیم؛ ما کیفیت و صداقت استثنایی را در همه کارهای خود به ارمغان می‌آوریم. ما فرهنگی از تعلق ایجاد می‌کنیم و از کارکنان دعوت می‌کنیم تا پتانسیل خود را به حداکثر برسانند.

ارتباطات: ما محیطی از صداقت و صداقت را تقویت می‌کنیم؛ ما با هدف و وضوح در داخل و خارج سازمان ارتباط برقرار می‌کنیم.

نوآوری: ما انعطاف‌پذیر، مبتکر هستیم و از ایده‌های متنوع استقبال می‌کنیم؛ ما برای حل مشکلات مهم در خدمت کالیفرنیایی‌ها از رویکردهای جدید استفاده می‌کنیم.

عدالت: ما قانون را با بی‌طرفی برای محافظت از حریم خصوصی مصرف‌کنندگان اجرا می‌کنیم. ما به کار گروهی اهمیت می‌دهیم و با همه با احترام و مهربانی رفتار می‌کنیم.

در این برنامه راهبردی چهار هدف کلان ذکر شده است که هدف اول و عناصر آن عبارتند از:

هدف اول: تقویت آموزش عمومی، اطلاع‌رسانی و مشارکت مردمی

(هدف این است که منابع، ابزارها و پشتیبانی لازم برای ارائه اطلاعات مرتبط، به موقع و دقیق به مصرف‌کنندگان و کسب‌وکارها فراهم شود.)

۱) توسعه یک کمپین آموزشی عمومی در سطح ایالت، با استفاده از کانال‌ها و ابزارهای ارتباطی مختلف برای افزایش آگاهی شهروندان کالیفرنیا از حقوق حریم خصوصی خود.

۲) انجام کمپین‌های اطلاع‌رسانی هدفمند برای جوامع آسیب‌پذیر و محروم، از جمله دانش‌آموزان، مهاجران، سالمندان، جوامع کم‌درآمد و گروه‌های در معرض خطر.

۳) توسعه مشارکت‌های استراتژیک با ذینفعان، اعضای رسانه‌ها و سایر گروه‌های جامعه برای تقویت آگاهی از حقوق و مسئولیت‌های حریم خصوصی.

۴)تسهیل انطباق از طریق راهنمایی‌های تجاری مکمل.

۵) آموزش جامعه حریم خصوصی در مورد تلاش‌های آژانس از طریق سخنرانی‌ها، رسانه‌های کسب‌شده و کانال‌های ارتباطی متعلق به آژانس.

سایر اهداف ذکر شده در این سند عبارتند از:

۲) اجرای قاطع قوانین حفاظت از حریم خصوصی: این هدف با هدف حفاظت از مصرف‌کنندگان در برابر نقض حقوق حریم خصوصی آن‌ها از طریق تعامل با جامعه تحت نظارت، تحقیقات به موقع و اقدامات اجرایی دنبال می‌شود. ۲) تقویت حقوق حریم خصوصی کالیفرنیایی‌ها: این هدف با هدف پیشبرد حقوق حریم خصوصی تمامی کالیفرنیایی‌ها با اطمینان از اینکه قوانین، مقررات، سیاست‌ها و رویه‌ها از ماموریت و وظایف آژانس حمایت و ارتقا می‌یابند، دنبال می‌شود. ۳) برتری عملیاتی این هدف با هدف اطمینان از رویکردی کارآمد و موثر در توسعه سازمانی، از جمله اجرای سیاست‌ها، برنامه‌ها و مقررات دنبال می‌شود (سلطانی، ۲۰۲۴).

قانون حفاظت از اطلاعات شخصی چین (پی.آی.پی.ال)[1]

قانون حفاظت از اطلاعات شخصی پی.آی.پی.ال در تاریخ ۱ نوامبر ۲۰۲۱ به اجرا درآمد و اولین قانون جامع حفاظت از داده‌های چین است. فعالیت‌های پردازش اطلاعات شخصی انجام شده توسط نهادها یا افراد در چین را تنظیم می‌کند و همراه با دو قانون کلیدی دیگر در مورد امنیت سایبری و حفاظت از داده‌ها؛ یعنی قانون امنیت سایبری و قانون امنیت داده‌ها رژیم جدیدی را برای حفاظت از داده‌ها در چین معرفی می‌کند[2].

همچنانکه در پایگاه نسخه غیررسمی این قانون ذکر شده است[3]، قانون حفاظت از اطلاعات شخصی (پی.آی.پی.ال) در سی‌امین جلسه کمیته دائمی سیزدهمین کنگره ملی خلق جمهوری خلق چین در تاریخ ۲۰ آگوست ۲۰۲۱ تصویب شد. پی.آی.پی.ال از ۱ نوامبر ۲۰۲۱ به اجرا درآمد. جمهوری خلق چین به سازمان‌ها چندین ماه فرصت داد تا اقدامات لازم برای رعایت پی.آی.پی.ال را آماده و اجرا کنند. پی.آی.پی.ال در مورد بسیاری از موضوعات از جمله قوانین پردازش اطلاعات شخصی و حساس، از جمله مبانی قانونی و الزامات افشای اطلاعات، جهت‌گیری می‌کند. پی.آی.پی.ال همچنین قوانینی را برای پردازنده‌های حفاظت از اطلاعات شخصی و همچنین حقوق موضوع داده معرفی می‌کند و الزامات مربوط به انتقال داده‌های بین‌المللی به اشخاص ثالث را تشریح می‌کند.

---

[1] . The China Personal Information Protection Law (PIPL)

[2] . https://www.dataguidance.com/notes/china-data-protection-overview

[3] . https://personalinformationprotectionlaw.com/

«قانون حفاظت از اطلاعات شخصی جمهوری خلاق چین» که به جای «داده» از اطلاعات استفاده کرده است، بخش‌های مختلفی دارد: مقررات کلی، قواعد پردازش اطلاعات شخصی، قواعد کلی، قواعدی درباره پردازش اطلاعات شخصی حساس، مقرات ویژه برای پردازش اطلاعات شخصی توسط نهادهای دولتی، قواعدی در مورد مقررات (تدارک) اطلاعات شخصی فرامرزی، حقوق افراد در فعالیت‌های پردازش اطلاعات شخصی، الزامات و پردازشگر اطلاعات شخصی، اداره‌هایی با وظایف حفاظت از اطلاعات شخصی، مسئولیت قانونی و مقررات تکمیلی. این قانون دارای هشت فصل و ۶۷ ماده است. هریک از فصلها، طیفی از موضوعات اساسی از حقوق افراد تا وظایف نهادهای مسئول حفاظت از داده‌های شخصی را دربرمی‌گیرد که به شکل جزئی مرور می‌کنیم.

-اصول حفاظت از داده‌های شخصی

فصل اول پی.آی.پی.ال ، مقررات کلی، ۱۲ ماده دارد. ماده ۱ که به هدف و قلمرو این قانون اشاره دارد که طی حفاظت از حقوق و منافع اطلاعات شخصی منطبق با قانونی اساسی چین است و تنظیم‌گری اطلاعات شخصی و ترویج استفاده معقول از داده‌های شخصی به عنوان هدف اصلی بیان می‌شود. مضمون ماده دوم، تأکید بر حفاظت قانون از اطلاعات شخصی عامه مردم و ممانعت از نقض آن توسط افراد و سازمانها اشاره دارد. طبق ماده سوم، این قانون مختص پردازش اطلاعات شخصی افراد درون قلمرو سرزمینی جمهوری خلق چین است و تحت شرایطی می‌تواند شامل پردازش اطلاعات شخصی شهروندان چین خارج از این کشور هم بشود.

صرفاً دو مفهوم در این قانون تعریف شده است-در مقایسه با تعریف‌های طولانی در جی.دی.پی.آو. و قانون حقوق حریم خصوصی مصرف کنندگان در کالیفرنیا-که عبارتن از اطلاعات شخصی و پردازش اطلاعات شخصی. همچنین باید توجه داشت که در این قانون به جای داده‌های شخصی از اطلاعات شخصی استفاده شده است[1]:

«اطلاعات شخصی» به معنای انواع اطلاعات مرتبط با شخص حقیقی شناسایی‌شده یا شناسایی‌پذیر است که به صورت الکترونیک یا ابزارهای دیگر ثبت شده است اما شامل اطلاعات ناشناس‌شده نیست.

[1]. نسخه انگلیسی که در اینجام مبنای تحلیل قرار گرفته است، ترجمه انگلیسی قانون حریم اطلاعات شخصی چین، در وب‌گاه کنگره ملی جمهوری خلق چین است. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

در این تعریف اطلاعات به شکل کلی درنظر گرفته است و در نگاهی سنتی از نگهداری الکترونیکی استفاده شده است. همچنین اطلاعاتی که دیگر قابل شناسایی نیستند، یعنی از طریق آن دیگر نمی‌توان یک فرد حقیقی را شناسایی کرد شامل نمی‌شود.

همچنین بر اساس این قانون، «پردازش اطلاعات شخصی»، ازجمله، شامل گردآوری، ذخیره‌سازی، استفاده، پردازش، انتقال، آماده‌سازی، افشاء و آماده‌سازی است.

مضامین اصلی قانون حفاظت از داده‌های شخصی چین

برخلاف قانون حریم مصرف‌کننده کالیفرنیا این تعریف محدود است اما قانون‌گذار با یک شرط هر نوع عملیات بر روی داده را به معنای پردازش اطلاعات تلقی کرده است. در جدول ۹-۴) مضامین دیگر این قانون آورده شده است:

مضمون	تعریف	ماده مرتبط
قانونی بودن، مستدل‌بودن، غیرفریبکارانه بودن	اطلاعات شخصی در مواقع لزوم و با دلایل موجه و با حسن نیت طبق قانون پردازش می‌شود و پردازش نباید متضمن گمراهی، تقلب، اجبار و موارد مشابه باشد	ماده ۵
مبتنی بر هدف روشن	پردازش اطلاعات شخصی باید بر اساس اهداف صریح و معقول و مستقیماً با آن اهداف مرتبط باشد و حداقل تأثیرات را بر حقوق و منافع افراد بگذارد	ماده۶
شفاف در بیان هدف پردازش	اصول باز بودن و شفافیت باید در پردازش اطلاعات شخصی رعایت شود، قوانین پردازش اطلاعات شخصی افشا شود و اهداف، ابزار و دامنه پردازش به صراحت ذکر شود	ماده ۷
جلوگیری از تأثیر پردازش بر حقوق افراد	کیفیت اطلاعات شخصی باید در پردازش اطلاعات شخصی تضمین شود تا از تأثیرات نامطلوب بر حقوق و منافع افراد ناشی از اطلاعات شخصی نادرست و ناقص جلوگیری شود	ماده ۸
مسئولیت‌پذیری	پردازشگرهای اطلاعات شخصی مسئولیت فعالیت‌های	ماده ۹

پردازشگرها	پردازش اطلاعات شخصی خود را بر عهده خواهند داشت و اقدامات لازم را برای اطمینان از امنیت اطلاعات شخصی که پردازش می‌کنند انجام می‌دهند	
ممنوعیت پردازش غیرقانونی اطلاعات شخصی	هیچ سازمان یا فردی نباید به طور غیرقانونی اطلاعات شخصی افراد دیگر را جمع آوری، استفاده، پردازش یا انتقال دهد، یا به طور غیرقانونی اطلاعات شخصی افراد دیگر را تجارت، ارائه یا افشا کند، یا در فعالیت های پردازش اطلاعات شخصی که امنیت ملی را به خطر می اندازد یا به منافع عمومی آسیب می رساند، شرکت کند.	ماده ۱۰
ایجاد سامانه حفاظت از داده‌ها	دولت باید سیستم حفاظت از اطلاعات شخصی را ایجاد و بهبود بخشد تا از نقض حقوق و منافع مربوط به اطلاعات شخصی جلوگیری و مجازات شود، تبلیغات و آموزش حفاظت از اطلاعات شخصی را تقویت کند، و محیط مساعد برای دولت، شرکت ها، سازمان های صنعتی مربوطه، و عموم مردم به طور مشترک در حفاظت از اطلاعات شخصی شرکت کنند	ماده ۱۱
تلاش دولت چین برای ارتقاء حفاظت از اطلاعات شخصی در سطح بین‌المللی	دولت فعالانه در توسعه قواعد بین المللی در مورد حفاظت از اطلاعات شخصی شرکت خواهد کرد، تبادلات بین المللی و همکاری در حفاظت از اطلاعات شخصی را ارتقاء خواهد داد و به رسمیت شناختن متقابل قوانین و استانداردهای حفاظت از اطلاعات شخصی را، از جمله از طریق همکاری با با سایر کشورها، مناطق، و سایر کشورها. سازمان های بین المللی تشویق خواهد کرد.	ماده ۱۲

جدول ۹-۴) مضامین اصلی قانون حفاظت از اطلاعات شخصی چین

شفافیت، قانونی بودن، مستدل‌بودن و مسئول‌بودن پردازش‌گرها در برابر پردازش اطلاعات شخصی، ازجمله مهمترین اصول پردازش اطلاعات شخصی در چین بیان شده است. علاوه‌براین، دولت چین موظف است تا سازوکار لازم را برای حفاظت از اطلاعات شخصی فراهم کند. این سامانه یا سازوکار دولتی برخی وظایف را برعهده دارد که عبارتند از: افزایش سواد اطلاعات شخصی شهروندان، بهبود حفاظت از داده‌های شخصی، جلوگیری از نقض حریم اطلاعات و ایجاد زمینه حفاظت از اطلاعات شخصی.

-اهمیت اخذ رضایت در پردازش داده‌ها

با ملاحظه تعریف فوق از پردازش اطلاعات، در ماده ۱۳ برخی شرایط برای اینکه پردازشگر برای پردازش اطلاعات، صرفاً بر اساس کفایت وجود یکی از این شرایط، مجاز باشد ذکر شده است. یک موضوع مهم در این بند ماده رضایت است:

۱) رضایت: یک پردازشگر اطلاعات شخصی می تواند اطلاعات شخصی یک فرد را در صورتی که رضایت فرد را کسب کرده باشد پردازش کند.

۲) تعهدات قراردادی: پردازش در صورتی مجاز است که برای انعقاد یا اجرای قراردادی که شخص طرف آن است و یا برای مدیریت منابع انسانی بر اساس قوانین و مقررات، کار ضروری باشد.

۳) وظایف قانونی: پردازش در صورت لزوم برای انجام وظایف یا تعهدات قانونی مجاز است.

۴) وضعیت های اضطراری: اطلاعات شخصی را می‌توان برای پاسخگویی به شرایط اضطراری بهداشت عمومی یا حفاظت از جان، سلامت و ایمنی اموال در طول شرایط اضطراری پردازش کرد.

۵) منافع عمومی: پردازش منطقی برای گزارش خبری، نظارت بر رسانه‌ها و سایر فعالیت‌هایی که در راستای منافع عمومی انجام می‌شود مجاز است.

۶) خود افشایی: اطلاعات شخصی افشاء شده توسط فرد یا اطلاعات افشاء شده قانونی طبق قانون قابل پردازش است.

۷) سایر شرایط: پردازش ممکن است تحت شرایط دیگری که توسط قوانین یا مقررات اداری مشخص شده است مجاز باشد.

درکل، برای انجام پردازش رضایت فردی همچنان مورد نیاز است مگر اینکه استثنائات مشخص شده (زیر بندهای ۲ تا ۷) اعمال شود.

ما ملاحظه اهمیت مفهوم رضایت برای پردازش اطلاعات شخصی، مادّه‌های ۱۴ تا ۱۶ به شرایط مرتبط با رضایت اختصاص یافته است.

ماده ۱۴:

شرایط رضایت فردی: داوطلبانه، صریح، کاملا مطلع شده.

سایر مقررات قانونی در مورد رضایت: رعایت رضایت جداگانه یا الزامات رضایت کتبی در سایر قوانین یا مقررات،

تغییر در هدف پردازش، روش‌ها یا دسته‌های اطلاعات شخصی: رضایت جدید باید از فرد گرفته شود.

ماده ۱۵:

-حق انصراف از رضایت

-تعهد پردازشگر اطلاعات شخصی: روش‌های سهلی برای پس گرفتن رضایت ارائه کند.

تأثیر لغو رضایت بر فعالیت‌های پردازش قبلی: هیچ تاثیری بر اعتبار فعالیت های پردازش گذشته ندارد

ماده ۱۶:

ممنوعیت امتناع از ارائه محصولات یا خدمات بر اساس رضایت خودداری شده یا پس‌گرفته شده، به استثنای اینکه

پردازش اطلاعات شخصی برای ارائه محصولات یا خدمات ضروری باشد.

به طور خلاصه، مواد ۱۴، ۱۵ و ۱۶ بر اهمیت رضایت فردی معتبر و آگاهانه به عنوان مبنایی برای پردازش اطلاعات شخصی تأکید می‌کنند. این ماده‌ها توضیح می‌دهند که هنگام تغییر اهداف پردازش، روش‌ها یا دسته‌های اطلاعات شخصی باید رضایت کسب شود. افراد حق دارند رضایت خود را پس بگیرند و پردازشگران اطلاعات شخصی باید این فرآیند را تسهیل کنند. در نهایت، آنها تأکید می‌کنند که وضعیت رضایت نمی‌تواند دلیلی برای اجتناب از ارائه محصولات یا خدمات باشد، مگر اینکه پردازش اطلاعات شخصی برای ارائه آنها ضروری باشد. همچنین بر اساس ماده ۱۷، پردازشگر اطلاعات شخصی پیش از پردازش اطلاعات باید به شکلی حقیقی، دقیق و کاملا فرد را به شکلی آسان‌هم از مواردی مانند نام و اطلاعات پردازشگر اطلاعات شخصی، هدف و وظایف پردازش اطلات شخصی و دسته‌بندی‌ها و دوره ذخیره‌سازی اطلاعات شخصی پردازش‌شده مطلع نماید. همچنین مدت زمان ذخیره‌سازی اطلاعت فرد باید در کوتاه‌ترین زمانی ممکن باشد (ماده ۱۹).

با ملاحظه اهمیت اطلاعات شخصی حساس، برخی ماده‌ها در این قانون به پردازش آن اختصاص یافته است. در این قانون «اطلاعات شخصی حساس» به معنای اطلاعاتی است که پس از افشا یا استفاده غیرقانونی، ممکن است به‌راحتی منجر به

تضییع حیثیت شخصی یک شخص حقیقی شود یا ممکن است امنیت یا دارایی شخصی او را به خطر بیندازد، که از جمله آنها می‌توان به اطلاعات مانند بیومتریک، اعتقادات مذهبی، هویت خاص، وضعیت سلامت پزشکی، حساب‌های مالی و محل اختفای شخص و همچنین اطلاعات شخصی افراد زیر ۱۴ سال اشاره کرد. یکی از ویژگی‌های پردازش اطلاعات شخصی این است که برای پردازش این نوع اطلاعات، باید برای هرکدام از آنها رضایت جداگانه گرفته شود (ماده ۲۹). همچنین برای پردازش اطلاعات افراد زیر چهارده سال باید رضایت والدین آنها و یا قیم آنها گرفته شود (ماده ۳۱).

خلاصه‌ای از پردازش اطلاعات شخصی توسط ارگان های دولتی

-اصول پردازش داده‌های شخصی توسط نهادهای دولتی

بر اساس ماده ۳۴، ارگان‌های دولتی باید اطلاعات شخصی را دقیقاً در چارچوب اختیارات و تشریفاتی که قانون تعیین می‌کند پردازش کنند و اطمینان حاصل کنند که آنها از محدودیت‌های لازم برای وظایف قانونی خود تجاوز نکنند؛ بحث دیگر تعهدات مرتبط با اطلاع‌رسانی است. ماده ۳۵ مقرر می‌دارد که ارگانهای دولتی موظفند در هنگام پردازش اطلاعات شخصی افراد را مطلع سازند، مگر اینکه استثنائاتی اعمال شود (طبق ماده ۱۸) یا اگر اطلاع‌رسانی مانع از انجام وظایف آنها شود. موضوع دیگرذخیره‌سازی داده‌ها و امنیت است. در ماده ۳۶ ذکر شده است که اطلاعات شخصی باید در چین ذخیره شود، در صورت نیاز به اشتراک‌گذاری این اطلاعات در خارج از کشور، ارزیابی امنیتی اجباری است و بخش‌های مربوطه در صورت نیاز پشتیبانی می‌کنند.

-حقوق افراد در فعالیت‌های پردازش اطلاعات شخصی

فصل چهارم به حقوق افراد در فرایند پردازش اطلاعات شخصی توجه دارد و ماده ۴۴ تا ۵۰ این قانون را شامل می‌شود. در ماده ۲۴ این قانون به حقوقی همانند حق آگاه شدن، حق تصمیم‌گیری در مورد پردازش اطلاعات شخصی و حق محدودسازی یا اجتناب از پردازش اطلاعات شخصی توسط دیگران، به جز الزام قانونی، اشاره شد. ماده ۴۵ بر حق افراد برای مشورت خواستن از پردازشگران اطلاعات و رونوشت گرفتن از اطلاعات خود تأکید دارد. ماده ۴۶ بر حق اصلاح اطلاعات شخصی در صورت آگاه شدن از نادرستی آن اطلاعات تأکید دارد. ماده ۴۷ بر اساس برخی شرایط مقرر داشته

است که فرد می‌تواند درخواست حذف یا پاک کردن اطلاعات خود را به پردازشگر اعلام نماید و پردازشگر نیز باید اقدام لازم را انجام دهد. ازجمله این شرایط زمانی که هدف پردازش محقق شده یا اکنون امکان تحقق ندارد و یا اینکه این اطلاعات برای دستیابی به هدف پردازش ضروری نیست؛ یا اینکه پردازشگر ارائه خدمات یا محصولات را متوقف کند؛ همچنین اگر فرد رضایت خود را پس بگیرد و یا اینکه پردازش اطلاعات توسط پردازشگر برخلاف قانون باشد، فرد می‌تواند درخواست نماید تا اطلاعات وی حذف شود.

نهادهای مسئول اجرای قانون

بر اساس ماده ۶۰ قانون حفاظت از اطلاعات شخصی چین، اداره ملی فضای مجازی مسئول برنامه‌ریزی و هماهنگی کلی حفاظت از اطلاعات شخصی و نظارت و اداره مربوطه خواهد بود. ادارات ذیربط شورای ایالتی مطابق این قانون و سایر قوانین و مقررات اداری مربوطه در حدود وظایف خود مسئولیت حفاظت از اطلاعات شخصی و نظارت و اداره مربوطه را بر عهده خواهند داشت. بر اساس ماده ۶۲، اداره ملی فضای مجازی، ادارات مربوطه را برای ارتقای حفاظت از اطلاعات شخصی از طریق اقدامات زیر مطابق با این قانون هماهنگ خواهد کرد:

۱) تدوین قوانین و استانداردهای خاص برای حفاظت از اطلاعات شخصی؛

۲) توسعه قوانین و استانداردهای ویژه حفاظت از اطلاعات شخصی برای پردازشگرهای اطلاعات شخصی کوچک، پردازش اطلاعات شخصی حساس، و فناوری ها و برنامه های جدید مانند تشخیص چهره و هوش مصنوعی؛

۳) حمایت از تحقیق و توسعه و ترویج کاربرد فناوری احراز هویت الکترونیکی امن و راحت و ارتقای خدمات عمومی برای احراز هویت شبکه؛

۴) ترویج توسعه یک سیستم خدمات حفاظت اطلاعات شخصی با مشارکت بخش‌های مختلف اجتماعی و حمایت از نهادهای مربوطه در ارائه خدمات ارزیابی و صدور گواهینامه حفاظت از اطلاعات شخصی؛ و

۵) بهبود مکانیسم شکایت و گزارش مربوط به حفاظت از اطلاعات شخصی.

درنهایت در ماده ۷۳ برخی اصطلاحات نیز تعریف شده‌اند که بر این اساس:

۱) پردازنده اطلاعات شخصی به سازمان یا فردی اطلاق می‌شود که به طور مستقل اهداف و ابزار پردازش اطلاعات شخصی را تعیین می‌کند:

۲) تصمیم‌گیری خودکار به فعالیت‌های تجزیه و تحلیل و ارزیابی خودکار رفتارهای شخصی، سرگرمی‌ها، یا وضعیت اقتصادی، بهداشتی و اعتباری از جمله از طریق برنامه‌های رایانه‌ای و تصمیم‌گیری اشاره دارد؛

۳) ناشناس‌سازی[1] به فرآیند پردازش اطلاعات شخصی برای غیرممکن کردن شناسایی افراد حقیقی خاص و غیرممکن کردن بازیابی اشاره دارد.

در نهایت در ماده ۷۴، اول نوامبر سال ۲۰۲۱ به عنوان تاریخ به اجرا گذاشته شدن این قانون بیان شده است.

در جدول ۴-۹) مجموعه مضامین این فصل که بیانگر اصول حاکم بر سه مورد از مقررات جهانی حفاظت از داده‌های شخصی کاربران است، ذکر شده است.

اصول حریم خصوصی در سه قانون پیشرو جهانی	-مقررات عمومی حفاظت از داده‌ها -اصول تحلیل داده‌ها قانونی بودن، انصاف و شفافیت - محدودیت هدف - تقلیل داده‌ها -محدودیت ذخیره‌سازی -یکپارچگی و محرمانگی -مفهوم داده‌های شخصی - چیستی حریم ارتباطات -پردازش داده‌های شخصی --رضایت کاربران -کنترل‌گرا و پردازشگر - پردازش داده از طریق طراحی و به صورت پیش‌فرض --انتقال داده‌های شخصی به طرفهای سوم یا سازمانهای بین‌المللی

[1] . anonymization

	– مسئولیت کنترل‌گر و پردازشگر --بخش ۳: تحریم‌ها و مجازات‌ها قانون حریم خصوصی مصرف‌کننده کالیفرنیا -تعریف اطلاعات شخصی -معنای اطلاعات شخصی حساس -معنای پردازش اطلاعات شخصی -وظایف کسب‌وکارها نسبت به داده‌های کاربران -حقوق مصرف‌کنندگان در برابر داده‌های شخصی – نهادسازی برای اجرای قانون حفاظت از حریم خصوصی قانون حفاظت از اطلاعات شخصی چین مضامین اصلی قانون حفاظت از داده‌های شخصی چین – قانونی بودن، مستدل‌بودن، غیرفریبکارانه بودن – مبتنی بر هدف روشن – شفاف در بیان هدف پردازش – جلوگیری از تأثیر پردازش بر حقوق افراد – مسئولیت‌پذیری پردازشگرها – ممنوعیت پردازش غیرقانونی اطلاعات شخصی – ایجاد سامانه حفاظت از داده‌ها – تلاش دولت چین برای ارتقاء حفاظت از اطلاعات شخصی در سطح بین‌المللی -اهمیت اخذ رضایت در پردازش داده‌ها -اصول پردازش داده‌های شخصی توسط نهادهای دولتی -حقوق افراد در فعالیت‌های پردازش اطلاعات شخصی

جدول ۴-۸) مضامین سه قانون مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، قانون حریم خصوصی مصرف‌کننده کالیفرنیا و قانون حفاظت از اطلاعات شخصی چین

نتیجه‌گیری

در این بخش، سه قانون جهانی مرتبط با حریم داده مورد ملاحظه قرار گرفت. همانطور که بحث شد، مقررات عمومی حفاظت از داده‌ها با جزئیات گسترده، پیشروترین مقررات مرتبط با حفاظت از داده‌های شخصی است و الگوی بسیاری از کشورها برای تدوین مقررات مرتبط است. دو قانون مورد بحث دیگر نیز اطلاعات سودمندی را برای تدوین قانون مشابه در ایران در اختیار ما می‌گذارند.

بخش پنجم

مرور سوابق لایحه‌های مشابه در ایران

مقدمه

در این بخش به طور کلی دو لایحه‌ای را که تاکنون در حوزه حریم خصوصی و داده‌های شخصی نهایی شده‌اند اما به قانون تبدیل نشده‌اند، مرور می‌کنیم. اول لایحه «حمایت از حریم خصوصی». و دوم لایحه «صیانت و حفاظت از داده‌های شخصی».

لایحه حمایت از حریم خصوصی

لایحه حمایت از حریم خصوصی که براساس پیشنهاد معاونت حقوقی و امور مجلس رییس جمهوری در نشست چهارم خرداد ماه ۱۳۸۴ هیات وزیران به تصویب رسیده بود، در ۲۲ مرداد ۱۳۸۴برای انجام تشریفات قانونی تقدیم مجلس شورای اسلامی شده بود. این لایحه که در هفت فصل تحت عنوانهای تعاریف و کلیات، حریم خصوصی جسمانی، حریم خصوصی اماکن و منازل، حریم خصوصی در محل کار، حریم خصوصی اطلاعات، حریم خصوصی ارتباطات و مسئولیتهای ناشی از نقض حریم خصوصی تنظیم شده بود، در راستای اجرای اصول ۲۲ و ۲۵ قانون اساسی در هیات وزیران به تصویب رسیده بود[1]. اما این لایحه در مهرماه ۱۳۸۴ چند روز پس از آغاز ریاست جمهوری محمود احمدی‌نژاد، از سوی نمایندگان مجلس شورای اسلامی وقت رد شد و تصویب نشد. یکی از دلایل عدم پیگری این لایحه به این شکل بیان شده بود که به علت وجود دستورجلسه‌ای در هیات دولت مبنی بر استرداد این لایحه از سوی دولت و هم‌چنین وارد آمدن اشکالاتی از سوی

[1] . https://www.irna.ir/news/6331500

مرکز پژوهش‌های مجلس به ۴۲ ماده از لایحه‌ی یاد شده، اعضای کمیسیون صنایع، لایحه حمایت از حریم خصوصی را رد کردند[1].

این لایحه در دوره‌ای که تهیه شده است که اینترنت در ابتدای گسترش خود بوده است و فضای مجازی به معنای کنونی آن شکل نگرفته بود، چه برسد به رسانه‌های اجتماعی. ماده یک این قانون که به نوعی مقدمه توجیهی آن است به شکل زیر می‌باشد:

ماده ۱: با الهام از احکام شرع مبین اسلام و به منظور حمایت از جسم افراد، اماکن خصوصی و منازل، حریم خلوت و تنهائی افراد، محل‌های کار، اطلاعات شخصی و ارتباطات و تبیین نحوه اجرای اول اصول (۲۲) و (۲۵) قانون اساسی، شفاف‌سازی اختیارات و مسئولیت‌های ارکان و اجزاء مختلف حکومت در زمینه رعایت حریم خصوصی و با عنایت به تعهدات بین‌المللی دولت، قانون حریم خصوصی به شرح زیربه تصویب می‌رسد[2].

این ماده آشفتگی مفهومی را به خوبی نشان می‌دهد. در این لایحه به جای ارائه رویکردی کلی به حریم خصوصی برخی از عرصه‌های خصوصی ذکر شده است.

-مفهوم حریم خصوصی

در این لایحه حریم خصوصی به این شکل تعریف شده است:

۱. حریم خصوصی: قلمروئی از زندگی هر شخص است که آن شخص یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند. جسم ، البسه و اشیاء همراه افراد ، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می‌شوند.

-حریم خصوصی به عنوان دسترسی به اطلاعات شخصی

در این تعریف از قانون اساسی دو موضوع برجسته است. اول، رویکرد دسترسی‌محور به محدوده حریم خصوصی و دوم تأکید بر مفهوم رضایت که در اکثر قوانین مورد مطالعه مورد تأکید قرار دارد. در این تعریف به حریم جسمانی، حریم مکانی، حریم اطلاعاتی و حریم ارتباطی توجه شده است. بر این اساس، ورود، نگاه، نظارت و کسب اطلاعات مستلزم کسب اجازه

[1] . https://www.isna.ir/news/8407-14298

[2] . https://www.moi.ir/news/109078

شخص شده است. در این تعریف امکان خصوصی و نیز منزل تعریف جداگانه دارند. درصورتی که در ادبیات اخیر، حریم مکانی به عنوان یکی از اشکال حریم خصوصی تعریف شده است.

-مفهوم اطلاعات شخصی

در این قانون از اصطلاح «اطلاعات شخصی» استفاده شده است. بر اساس آن اطلاعات شخصی «عبارتست از اطلاعات وابسته به شخصیت افراد نظیر وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی و شماره کارت‌های اعتباری» و نکته جالب توجه اینکه طبق این لایحه «اطلاعات مربوط به نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار و شماره‌های تلفن از شمول تعریف اطلاعات شخصی خارج می‌باشد».

همانطور که در بررسی برخی از قوانین مشاهده کردیم، اطلاعات مربوط به نام و ... دقیقاً در زمره داده‌های شخصی است. همچنین داده‌هایی که به نوعی سبب شناسایی فرد شوند و یا شناسه باشد در زمره حریم خصوصی محسوب می‌شوند اما در این تعریف از اطلاعات مرتبط با شخصیت افراد همانند وضعیت زندگی خانوادگی و عادت‌های فردی به عنوان حریم خصوصی نام برده شده است که به نظر می‌رسد که پیش از آنکه مرتبط با اطلاعات شخصی باشند مرتبط با وضعیت روان‌شناختی فرد است.

-اطلاعات شخصی حساس

اطلاعات شحصی حساس نیز به معنای «اطلاعات راجع به وضعیت زندگی جنسی، اعتقادات (اعم از فلسفی ، مذهبی و سیاسی) ، عضویت در احزاب یا تشکل‌های صنفی و وضعیت نژادی ، قومی قبیله‌ای افراد» تعریف شده است.

چند تعریف مهم در دیگر در این لایحه عبارتند از:

دسترسی به اطلاعات: اعم است از مشاهده سند و یاهر وسیله یا چیز دیگری از اطلاعات در آن ثبت یا ذخیره شده است و اطلاع از محتوای آن از طریق مطالعه یا استنساح یا تکثیر تمام یا برخی قسمت‌ها و یابا تهیه یک رونوشت کامل از آن.

دسترسی بر اساس این تعریف، شامل دسترسی به حریم ارتباطی است و نه حریم داده و اطلاعات. همچنین تعریف پایش که «عبارتست از کسب اطلاعات از طریق مختلف؛ مخفی یا آشکار و با وسیله یا بی‌وسیله، اعم از انکه رفتار، گفتار، نوشتار مورد پایش ضبط و ذخیره شود یا نشود» و رهگیری که «عبارتست از دستیابی به محتوای ارتباطات کلامی- حضوری یا

کتبی یا الکترونیکی یا سیمی با استفاده از هر نوع وسیله الکترونیکی، مکانیکی یا سایر وسائل مشابه بدون اطلاع طرف برقرارکننده ارتباط نظیر بررسی، شنود و ضبط ارتباطات» ناظر بر حریم ارتباطی است.

-حریم اطلاعات شخصی

فصل پنجم این لایحه به حریم خصوصی اطلاعات اختصاص دارد. بند اول این قانون درباره جمع‌آوری اطلاعات شخصی و نحوه استفاده و دسترسی به آنها است. در ماده ۳۱ این لایحه آمده است: «کلیه مؤسسات عمومی و مؤسسات خصوصی که خدمات عمومی ارائه می‌دهند نباید اطلاعات شخصی افراد را جمع‌آوری کنند مگر اینکه آن اطلاعات برای انجام وظایف و فعالیتهای قانونی –سازمانی آنها به طور متعارف ضرورت داشته باشد».

-اصول گردآوری اطلاعات شخصی حساس

اما گردآوری اطلاعات شخصی حساس بر اساس ماده ۴۲ این قانون منع شده و مؤسسات تحت شرایطی قادر خواهند بود اطلاعات شخصی حساس را گردآوری کنند که عبارتند از:

۱) آن افراد رضایت داده باشند

۲) جمع‌آوری یا استفاده صریحاً طبق قانون مجاز باشد

۳) جمع‌آوری یا استفاده، به طور متعارف برای جلوگیری از یک تهدید شدید قریب‌الوقوع نسبت به حیات یا سلامتی فرد و جامعه یا کاهش این تهدید ضروری باشد.

۴) جمع‌آوری یا استفاده برای تحقیق یا تحلیل آماری راجع به خدمات رفاهی یا آموزشی‌ای که از بودجه‌های دولتی استفاده می‌کنند ضروری باشد

۵) اطلاعات جمع‌آوری شده مربوط به اصل و نسب نژادی یا قومی یک فرد بوده و به منظور کمک به خدمات رفاهی یا آموزشی برخوردار از هزینه‌های دولتی جمع‌آوری شده باشد

تبصره– در اجرای بندهای (۴) و (۵)، نام و مشخصات شناسنامه‌ای و سایر مشخصاتی که به هر ترتیب منجر به شناسایی افراد می‌گردد نباید سؤال شود.

طبق این قانون، رضایت فرد و قانونی بودن صرفاً در مورد اطلاعات حساس یک پیش‌شرط الزامی است و نه اطلاعات شخصی به طور کل که از این منظر با قوانین مشابه در جهان در تعارض قرار دارد.

-ابعاد حریم ارتباطات

در فصل ششم که به حریم خصوصی ارتباطات اختصاص دارد، صراحتاً اعلام شده است که حریم خصوصی ارتباطات از تعرض مصون است و اجازه رهگیری که فقط با مجوز قانونی مجاز شمرده شده است. بند اول فصل ششم به ارتباطات پستی اختصاص دارد که در زمان تهیه لایحه اهمیت و جایگاه والایی داشته است و سه ماده به آن اختصاص دارد. بند دوم این قانون درباره ارتباطات از راه دور تلفن، تلگراف، تلکس، فکس اختصاص دارد که هرنوع پایش آن به رعایت قانون منوط شده است. در این بخش تلاش شده است تا با جزئیات فراوان نحوه و جزئیات پایش این نوع ارتباطات مشخص شود. این بخش از بخش‌های دقیق و جالب این لایحه بوده است و با دقت فراوان تلاش شده است تا از حریم ارتباطات از راه دور افراد صیانت شود. بند سوم این فصل به ارتباطات اینترنتی اختصاص دارد و طبق ماده ۶۹ : شنود ، ضبط ، ذخیره یا دیگر انواع رهگیری ارتباطات خصوصی اینترنتی اشخاص بدون رضایت وی مجاز نیست، مگر آنکه ماده (۶۴)[1] و شرائط پیش‌بینی شده در آن رعایت شود.. براس تبصره ۱ ماده ۶۵ منظور از «ارتباطات خصوصی اینترنتی» هر نوع ارتباطی است که اصل سازوکار آن در ایران است یا پیام خود را به دریافت‌کننده معینی در ایران ارسال کرده و انتظار متعارف دارد تا پیام مذکور تنها توسط شخص مورد نظر او دریافت شود. نظیر پست الکترونیکی، مکالمه تلفنی و اینترنتی و سایر ارتباطات اینترنتی که تنها با استفاده از کلمه عبور یا رمز قابل دریافت یا ارسال باشد.

---

[1]. ماده ۶۴ : در صورتی که مقام صلاحیت دار قضائی بنا به در خواست مراجع ذی صلاح ، برمبنای ظن قوی تشخیص دهد که رهگیری ارتباطات از راه دور یا ارتباطات کلامی ـ حضوری به جلوگیری از وقوع جرم ، کشف ادله جرم در حال وقوع یا واقع شده کمک موثر خواهد کرد ، اختیار دارد با صدور یک قرار که حاوی اوصاف زیر باشد مجوز رهگیری ارتباطات مذکور را صادر کند.

۱) مشخصات شخص یا اشخاصی که باید ارتباطات مورد نظر را رهگیری کند ؛

۲) مشخصات دقیق شخص یا سازمانی که باید ارتباطاتشان رهگیری شود ؛

۳) طرق و روش رهگیری؛

۴) مدت زمان اعتبار مجوز رهگیری؛

۵) تعداد دفعات رهگیری؛

۶) ساعاتی که رهگیری باید در آن ساعت به عمل آید؛

۷) موضوعی که باید اطلاعات راجع به آن از طریق رهگیری تحصیل شود؛

۸) استفاده کنندگان از اطلاعات تحصیل شده؛

تبصره : مرجع رهگیری‌کننده باید پس از اتمام رهگیری گزارش اقدامات خود را به مقام قضائی صادر کننده قرار ارائه نماید.

این رویکرد به حریم ارتباطات خصوصی اینترنت قابل تعمیم به ارتباطات میان‌فردی در پیام‌رسان‌ها است و می‌توان بر این اساس ادعا کرد که این قانون می‌توانسته است به عصر کنونی نیز تعمیم داده شود.

فصل هفتم این لایحه به مسئولیت‌های ناشی از نقض حریم خصوصی اختصاص دارد. از منظر رویکرد این پژوهش، که به حریم داده‌های شخصی و ارتباطات تمرکز دارد، ماده ۷۹ به آن اختصاص دارد. طبق این ماده «هر کس مقررات این قانون را در زمینه جمع‌آوری، نگهداری، استفاده و افشای اطلاعات شخصی نقض کند، به حبس از سه ماه تا یک سال محکوم خواهد شد. چنانچه مرتکب در زمره یکی از مقامات و مستخدمان و ماموران دولتی باشد، علاوه بر مجازات یاد شده به انفصال از خدمت و محرومیت سه تا پنج سال از مشاغل دولتی نیز محکوم می‌گردد».

با وجود آشفتگی در مفاهیم و برخی ضعف‌های این لایحه، عدم تعیین نهاد مسئول اجرای این لایحه، تصویب و قانونی شدن آن می‌توانست برخی مشکلات موجود را پاسخگو باشد.

لایحه «صیانت و حفاظت از داده‌های شخصی»

در ۶ مرداد ۳۹۷ همزمان با نمایشگاه الکامپ ۲۴، با حضور وزیر ارتباطات و فناوری اطلاعات، رییس مرکز پژوهشهای مجلس و رییس کمیته ارتباطات و فناوری اطلاعات مجلس از پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» رونمایی شد.

در تاریخ دی‌ماه ۱۳۹۶، وزارت ارتباطات با همکاری تعدادی از پژوهشگران اقدام به تهیه پیش‌نویس لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی کرد و پس از انتشار آن از صاحب‌نظران درخواست شد نظرات خود را درباره آن بیان کنند.

شش ماه بعد در خرداد ۱۳۹۷، محمدجواد آذری جهرمی وزیر وقت ارتباطات و فناوری اطلاعات در توییتی به زبان انگلیسی اعلام کرده بود که وی به دنبال ارسال لایحه‌ای برای حفاظت از داده‌ها در ماه‌های آتی به مجلس شورای اسلامی برای تصویب است (کربلایی، ۱۴۰۱). گرچه این لایحه به مجلس شورای اسلامی ارسال نشد و پس از پیگری‌های انجام شده در

دولت بعد و بررسی این لایحه در کمیسیون اقتصاد دیجیتال، سرانجام در مرداد ۱۴۰۳ لایحه جدیدی–که مفاد آن اعلام نشده است–برای بررسی و تصویب به مجلس شورای اسلامی ارسال شده است.

بر اساس نسخه‌ای از لایحه صیانت و حفاظت از داده‌های شخصی که در وب‌سایت وزارت ارتباطات و فناوری ارتباطات در دسترس است[1]، این لایحه پیشنهادی ۶ با و ۷۸ ماده دارد. باب یا فصل‌های مختلف این لایحه عبارتند از: کلیات، حقوق اشخاص موضوع داده‌ها، تعهدات کنترل‌گران و پردازشگران، تنظیم و نظارت بر پردازش داده‌های شخصی، مسئولیت‌ها و ضمانت اجراها و نسخ قوانین.

در این بخش برخی از قسمت‌های این لایحه که برای ما اهمیت دارند، به شکل کلی مرور می‌شوند. آنچه مسلم است و از توئیت انگلیسی آذری جهرمی وزیر وقت ارتباطات که در آن به کمیسیون اروپا بابت تصویب مقررات عمومی حفاظت از داده‌ها تبریک گفته بود، این لایحه تا حد زیادی متأثر از نسخه مادر اروپایی است و می‌توان آنرا خلاصه‌ای از جی.دی.پی.آر دانست. ازجمله استفاده از اصطلاح موضوع داده که به همان شکل شکل در جی.دی.پی.آر ذکر شده است. ماده یک هدف اصلی این قانون را «صیانت از حیثیت و کرامت اشخاص موضوع داده‌ها» ذکر کرده است. همچنین، 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 ازجمله اهداف این قانون ذکر شده است.

-تعریف داده‌های شخصی

ماده دوم این لایحه به تعاریف اختصاص دارد که طی آن شش اصطلاح تعریف شده است:

الف) داده شخصی عبارت است از داده‌ای که به تنهایی یا به همراه داده‌های دیگر، مستقیم یا غیرمستقیم شخص موضوع داده را از طریق ارجاع به یک شناسه می‌شناساند.

[1] . https://www.ict.gov.ir/fa/newsagency/21691

ب) داده شخصی حساس عبارت است از داده شخصی که ریشه قومی یا قبیله ای، نظرات سیاسی، مذهبی و فلسفی، مشخصات وراثتی یا اطلاعات سلامت شخص موضوع داده را آشکار می‌سازد.

ب) پردازش: هرگونه عملیات دستی یا خودکار بر داده‌های شخصی، شامل و نه محدود به ایجاد، ثبت، دریافت، گردآوری، نگهداری، جداسازی، تغییر، تجزیه و تحلیل، طبقه‌بندی، ساختاربندی، تطبیق، ذخیره‌سازی، اشتراک‌گذاری، فرستادن، توزیع و عرضه، انتشار و در دسترس قرار دادن و پاک کردن آن‌ها.

پ)کنترل‌گر: شخصی است که همه یا بخشی از هدف، سازوکار، شرایط، ویژگی‌ها و ابزارهای یک یا چند عملیات پردازش داده‌های شخصی در اختیار پردازشگر را تعیین می‌کند. مصوبات و تصمیمات مراجع صلاحیت‌دار در امور تنظیم‌گری، نظارت، ضابطین و دادرسی درباره پردازش داده‌های شخصی، جز در مواردی که جنبه فردی دارد، کنترل‌گری به شمار نمی‌آید.

ت) پردازشگر: شخص مأذون کنترل‌گر در پردازش است. در صورت نبود کنترل‌گر یا عدم امکان اتصاف پردازش به آن، پردازشگر به‌عنوان کنترل‌گر نیز شناخته می‌شود.

ث) ناظر ویژه: کسی است که پیرو حکم صادره از سوی کمیسیون، صلاحیت نظارت بر پردازش داده‌های شخصی را می‌یابد.

-رضایت به پردازش

بخش یک باب دوم که شامل حقوق اشخاص موضوع داده است، رضایت به پردازش است. بر اساس ماده ۴ این لایحه، « پردازش داده‌های شخصی مربوط به وضعیت‌ها یا موقعیت‌های غیرعمومی، منوط به رضایت شخص موضوع آن‌هاست» و اینکه بر اساس ماده ۶، پردازش داده‌های شخصی اشخاص موضوع داده درصورتی بلامانع است که «خودش داده‌ها را در معرض پردازش قرار داده باشد؛ یا پردازش داده‌های خود را منع یا محدود نکرده باشد».

یک بخش مهم که می‌تواند برای بحث درباره پردازش داده‌های شخصی کاربران ایرانی در پلتفرم‌های غیرایرانی اهمیت داشته باشد، بحث پردازش فرامرزی است. در ماده ۳۷ عنوان شده است که پردازش داده‌های شخصی در این شرایط فرامرزی انگاشته می‌شود: «هریک از کنترل‌گران یا پردازشگران تابعیت خارجی داشته باشند» و «سامانه‌های پردازنده داده‌ها در بیرون از قلمرو حاکمیتی جمهوری اسلامی ایران قرار داشته باشد». ماده ۳۸ نیز اظهار می‌دارد که برای پردازش داده‌های شخصی اتباع ایرانی رعایت برخی شرایط الزامی است:

الف) تنها در مراکز داده واقع در قلمرو حاکمیتی جمهوری اسلامی ایران یا مراکز داده خارجی مورد تأیید مراجع صلاحیت‌دار ذخیره شوند؛

ب) همه پردازنده‌های سخت‌افزاری و نرم‌افزاری از گواهی مراجع صلاحیت‌دار ذی‌ربط برخوردار باشند؛

پ) بر روی شبکه ارتباطی مطمئن جابه‌جا شوند؛

ت) صلاحیت کنترل‌گران و پردازشگران خارجی مورد تأیید مراجع ذی‌ربط قرارگرفته باشد؛

ث) پردازش‌های فرامرزی برپایه ضوابط مقرر به ثبت برسد.

-نهاد متولی تنظیم‌گری و نظارت بر پردازش داده‌های شخصی

در لایحه صیانت و حفاظت از داده‌های شخصی، تنظیم و نظارت بر پردازش داده‌های شخصی برعهده ارکان زیر گذاشته شده است:

الف) کمیسیون صیانت از داده‌های شخصی؛

ب) هیئت نظارت؛

پ) کارگروه‌های تخصصی؛ و

پ) دبیرخانه اجرایی کمیسیون.

بر اساس ماده ۴۰ اعضای این کمیسیون عبارتند از: ۱. وزیر ارتباطات و فناوری اطلاعات به‌عنوان رئیس کمیسیون؛ وزیر اطلاعات؛ وزیر کشور؛ وزیر دادگستری؛ وزیر فرهنگ و ارشاد اسلامی؛ وزیر اقتصاد و امور دارایی؛ دبیر شورای عالی و رئیس مرکز ملی فضای مجازی؛ معاون پیشگیری از وقوع جرم قوه قضائیه؛ رئیس کمیسیون اصل نودم مجلس شورای اسلامی؛ دادستان کل کشور؛ دبیر شورای اجرایی فناوری اطلاعات به‌عنوان دبیر کمیسیون. آشکارا، در این لایحه مسئولیت اصلی حفاظت از داده‌های شخصی در اختیار وزارت ارتباطات و فناوری اطلاعات قرار گرفته است. به‌طوری‌که وزای مختلف و حتی دبیر شورای عالی فضای مجازی در ذیل وزیر ارتباطات به عنوان رئیس کمیسیون قرار می‌گیرند. دبیرخانه کمیسیون نیز در محل وزارت ارتباطات و فناوری اطلاعات قرار دارد.

یکی از بخش‌های این لایحه تشکیل کارگروه‌های تخصصی صیانت از داده‌های شخصی است که طبق بر اساس بند مربوط به تشکیل کارگروه‌ها، در ماده ۴۷ پیش‌بینی شده است که کارگروه‌های تخصصی، متشکل از نمایندگان نهادهای متولی امور حاکمیتی مرتبط با صیانت از داده‌های شخصی به انجام وظایف مقرر در این قانون می‌پردازند.

-تشکیل هیئت نظارت بر داده‌های شخصی

علاوه‌براین، تشکیل هیئت نظارت بر داده‌های شخصی نیز مورد نظر قرار دارد. که بر اساس ماده ۵۱ اعضای هیئت نظارت عبارتند از: وزیر دادگستری به عنوان رئیس هیئت نظارت؛ رئیس کمیسیون اصل نود مجلس شورای اسلامی؛ رئیس مرکز ملی فضای مجازی و دبیر کمیسیون.

بر اساس ماده ۵۳ وظایف هیئت نظارت عبارتند از:

الف) نظارت بر حسن اجرای امور نظارتی کارگروه‌های تخصصی؛

ب) دریافت و رسیدگی به شکایات ذی‌نفعان صیانت از داده‌های شخصی؛

پ) شناسایی و معرفی ناظران ویژه به کمیسیون و نظارت بر امور و فعالیت‌های آن‌هابرپایه شیوه‌نامه مصوب کمیسیون؛

ت) نظارت بر تدوین شیوه‌نامه‌های اختصاصی استنادپذیری ادله ناظر به داده‌های شخصی از سوی کارگروه‌های تخصصی، تصویب در کمیسیون و ابلاغ پس از تأیید رئیس کمیسیون؛

ث) ایفای سایر امور محوله از سوی کمیسیون.

بر اساس ماده ۵۴، ناظر ویژه برای پردازش داده‌های شخصی حیاتی و حساس؛ پردازش کلان‌داده‌های شخصی و نیز در مورد زیان‌ها و آسیبهای جدی یا پرشمار بالقوه و بالفعل پردازش‌ها به داده‌های شخصی تعیین می‌شود.

در باب پنج که به مسئولیت‌ها و ضمانت اجراها می‌پردازد نیز دامنه مسئولیت کنترل‌گران و پردازش‌گران تعیین شده است که شامل مسئولیتهای مدنی (جبران مادی) و نیز مسئولیتّهای کیفری (جرایم و مجازاتّها) است.

در جدول ۴-۱۰) مجموعه مضامین این فصل که مفاهیم اصلی لایحه‌های پیشنهادی در ایران است، بیان شده است.

	-مفهوم حریم خصوصی -حریم خصوصی به عنوان دسترسی به اطلاعات شخصی -مفهوم اطلاعات شخصی -اطلاعات شخصی حساس -حریم اطلاعات شخصی -اصول گردآوری اطلاعات شخصی حساس

مضامین لایحه‌های پیشنهادی برای حفاظت از حریم خصوصی در ایران	-ابعاد حریم ارتباطات -حقوق اشخاص موضوع داده‌ها -تعهدات کنترل‌گران و پردازشگران - تنظیم و نظارت بر پردازش داده‌های شخصی - مسئولیت‌ها و ضمانت اجراها و نسخ قوانین -تعریف داده‌های شخصی -رضایت به پردازش -نهاد متولی تنظیم‌گری و نظارت بر پردازش داده‌های شخصی -تعریف داده‌های شخصی -رضایت به پردازش -نهاد متولی تنظیم‌گری و نظارت بر پردازش داده‌های شخصی -تشکیل هیئت نظارت بر داده‌های شخصی

جدول ۴-۱۰) مضامین لایحه‌های پیشنهادی برای حفاظت از حریم خصوصی در ایران

نتیجه‌گیری

گرچه اخیراً لایحه‌ای درباره حفاظت از حریم داده‌های شخصی از سوی دولت به مجلس شورای اسلامی ارسال شده است- اما ما به آن دسترسی نداشتیم- بنابراین، به طور خلاصه، دو لایحه یعنی لایحه حریم خصوصی سال ۱۳۸۳ و لایحه صیانت از داده‌های شخصی ۱۳۹۷ را مرور کردیم. هر دوی این لایحه‌ها با وجود اینکه در صورت می‌توانستند خلاء قانونی حفاظت از حریم خصوصی و داده‌های شخصی را در ایران مرتفع کنند اما هر دوی آنها دارای کاستی‌ّای اساسی از حیث مفهوم و ملاحظه تحولات فناورانه هستند.

فصل پنجم

نتیجه‌گیری

مقدمه

ساختار نتیجه‌گیری تحقیق به طور کلی از اجزای زیر تشکیل شده است: بیان مجدد مسئله و اهداف تحقیق برای ارائه زمینه؛ جمع‌بندی یافته‌های کلیدی و پرداختن به اهداف یا فرضیه‌های تحقیق؛ بحث در مورد پیامدهای یافته‌ها برای نظریه، عمل یا سیاست؛ و درنهایت ارائه یک پیش‌نویس برای حفاظت از داده‌های شخصی و حریم ارتباط در پلتفرم‌های دیجیتال.

مسئله پژوهش حاضر و اهداف کلیدی

این پروژه پژوهشی با هدف گذراندن یک دوره فرصت مطالعاتی شش ماهه در مرکز ملی فضای مجازی (پروهشگاه فضای مجازی) مطابق با شیوه‌های فرصت مطالعاتی اعضای هیئت علمی در جامعه و صنعت انجام شده است. موضوع، ابعاد و خروجی‌های مورد انتظار این طرح بر اساس مذاکره با رئیس پژوهشگاه فضای مجازی وابسته به مرکز ملی فضای مجازی تعیین شده است. هدف اولیه این طرح مطالعه الزامات و ابعاد یک قانون جامع حریم خصوصی در ایران با ملاحظه فضای مجازی و پلتفرم‌های رسانه‌های اجتماعی بود. بر اساس طرحنامه ارائه شده قصد داشتیم با ملاحظه مرور قوانین و مقررات بین‌المللی مرتبط با حریم خصوصی و حریم داده و تجربه کشورها و سازمانهای بین‌المللی، ادبیات حقوقی و فقهی حریم خصوصی، مجموعه اسناد و قوانین بالادستی همانند قانون اساسی، فتوای رهبری درباره حریم خصوصی، حریم خصوصی دربرخی قوانین و مقررات و اقدامات قانونی که تاکنون درباره تدوین یک لایحه جامع حفاظت از حریم خصوصی انجام شده و نیز مطالعه اسناد حریم خصوصی پلتفرمهای بزرگ جهانی، تصوری کلی از وضعیت موجود حریم خصوصی در ایران و جهان ارائه شود و سپس یک خلاصه سیاسی و پیش‌نویسی برای قانون جامع حفظ حریم خصوصی و حریم داده در اکوسیستم پلتفرمی ایران ارائه شود.

بر اساس آنچه گفته شد، مسئله اصلی این پژوهش این بود که «تدوین قانون جامع حکمرانی و تنظیم‌گری حریم خصوصی و داده‌های شخصی در فضای مجازی در ایران چه الزامات و چه ابعادی دارد؟».

برخی از پرسشهای فرعی این پژوهش عبارت بودند از:

۱. مبانی نظری و مفهومی حریم خصوصی در ایران چیست؟

۲. تا کنون چه اقداماتی (قوانین و مقررات و اسناد) برای صیانت از حریم خصوصی (در ایران انجام شده است) است؟

۳. تاکنون چه تحولاتی (قوانین و مقررات) در سایر کشورهای جهان برای حمایت از حریم خصوصی و مقابله با نقض آن انجام شده است؟ با ملاحظه اهمیت حکمرانی در پلتفرم‌ها، پلتفرمهای بزرگ جهانی تاکنون چه اسناد و مقرراتی را برای حفاظت از حریم خصوصی و داده‌های شخصی ارائه کرده‌اند و از چه سازوکارهایی را برای صیانت از حقوق حریم خصوصی کاربران در پلتفرم‌های خود انجام تعبیه کرده‌اند؟

بنابراین در این پژوهش برخی از اهداف کلیدی عبارت بودند از: تعریف و مفهوم‌سازی حریم خصوصی و داده‌های شخصی؛ مرور مطالعات پیشین درباره حریم خصوصی در ایران؛ مرور پیش‌نویس لایحه‌ها، قوانین و اسناد مرتبط با حریم خصوصی؛ استخراج مبانی نظری حریم خصوصی در فقه، قانون اساسی، قوانین بین الملل، قوانین گوناگونی که به نحوی به مسئله حریم خصوصی توجه کرده‌اند؛ مطالعه قوانین و مقررات مرتبط با حریم خصوصی در کشورهای دیگر؛ مطالعه سیاستهای حریم خصوصی در پلتفرمهای بزرگ جهانی که عموماً در شرایط ارائه خدمت، سیاست حریم خصوصی و حریم داده آنها منعکس شده است؛ و درنهایت ارائه یک سند راهبردی یا پیش‌نویس لایحه جامع حریم خصوصی در پلتفرمهای رسانه‌های اجتماعی.

تقسیم‌بندی یافته‌ها

همانطور که در فصل تحلیل یافته‌ها مشخص است، با ورود به میدان پژوهش و مطالعه اسناد و منابع گوناگون، مطالعه پیشینه پژوهش و تصوری کلی که از موضوع پژوهش حاصل شد، این مطالعه حول چند موضوع کلیدی سامان‌دهی شد: اول، مفهوم‌سازی و تلاش برای کنکاش در ابعاد گوناگون و زمینه‌های پیدایش حریم خصوصی و حریم داده، با تمرکز بر حریم اطلاعات و اطلاعات (داده)؛ دوم، تلاش برای زمینه‌مند مفهوم حریم خصوصی در ایران، با ملاحظه رویکرد دینی و فقهی به مفهوم حریم خصوصی، ابعاد مورد تأکید حریم خصوصی در منابع اسلامی و مرور رویکرد به حریم خصوصی و دو بعد اصلی یعنی حریم داده و ارتباطات در اسناد و قوانین و رویکردهای مقامات جمهوری اسلامی به حریم خصوصی؛ سوم، مرور سیاستهای حریم خصوصی و اسناد پلتفرم‌های بزرگ جهانی ازجمله گوگل، متا (فیس‌بوک) و توئیتر به حریم خصوصی، حریم داده و از جمله رویکرد کلی پلتفرم‌ها به نحوه حفاظت از حریم خصوصی ازجمله از منظر فنی که ازجمله شامل اصل حریم خصوصی بر اساس طراحی و اصول گردآوری و پردازش داده و اشتراک‌گذاری آن با طرف‌های سوم است؛ چهارم،

مرور و تحلیل جزئی سه قانون مطرح مهم جهانی برای حفاظت از داده‌ها از جمله مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا که سرمشق و الگوی بسیاری از کشورها برای تدوین قوانین مشابه بوده است و با رویکرد اتحادیه اروپا با مقررات‌محوری سازگاری دارد، قانون حفاظت از حریم خصوصی مصرف‌کننده ایالت کالیفرنیا و نیز قانون حفاظت از اطلاعات شخصی در چین.

در این پژوهش بر اساس پرسشهای مختلف که این پژوهش برای پاسخ به آنها انجام شد، تعدادی از مضامین مختلف استراج شدند. در انتهای هرکدام از بخشهای تحلیل یافته‌ها این مضامین در قالب یک جدول ذکر شدند. این مضامین در ایجاد یک منظومه مفهومی به کار رفتند که درنهایت برای فهم ابعاد دینی، تاریخی، قانونی، بین‌المللی و نیز فهم پیامدهای تحولات فناورانه و مقررات جهانی در این حوزه می‌توانند به کار گرفته شوند. پس از ترکیب این مضمون‌ها ما آنها را قالب یک جدول (جدول ۵-۱) ارائه می‌کنیم.

دسته اصلی	زیرشاخه‌ها
مفاهیم کلان حریم خصوصی	**حریم خصوصی به مثابه امری غریزی، حریم خصوصی به مثابه امری اجتماعی، حریم خصوصی به مثابه امری تاریخی، حریم خصوصی به مثابه کنترل، حریم خصوصی به مثابه دسترسی، حریم خصوصی به‌مثابه حفظ کرامت انسانی، حریم خصوصی به مثابه حریم کاربران، مفهوم حریم خصوصی، حریم خصوصی به مثابه امری ارتباطی**
اصول و چارچوب‌های حریم خصوصی	**اصل حفظ حریم خصوصی بر اساس طراحی یا پیش‌فرض، اصل تقلیل داده‌ها، قانونی بودن، انصاف و شفافیت، محدودیت هدف، محدودیت ذخیره‌سازی، یکپارچگی و محرمانگی، حق دسترسی به اطلاعات، حق اطلاع (شفافیت)، حق اصلاح، حق پاک کردن، حق انتقال داده‌ها، حق اعتراض به پردازش داده‌های شخصی، حق محدودیت**
سیاست‌ها و مقررات حریم خصوصی	**مقررات عمومی حفاظت از داده‌ها، قانون حریم خصوصی مصرف‌کننده کالیفرنیا، قانون حفاظت از اطلاعات شخصی چین، حریم خصوصی در قوانین و مقررات ایران، عدم حمایت صریح از حریم خصوصی در قانون اساسی، توجه به حریم خصوصی ارتباطات در قانون اساسی، ممنوعیت ورود به حریم خصوصی بدون حکم قانون، مجرمانه بودن نقض اطلاعات شخصی،**

	مصلحت به مثابه جواز ورود به حریم خصوصی
فناوری و ایمنی در حریم خصوصی	**ایمنی و حریم خصوصی، رمزگذاری به عنوان ابزار حفظ ایمنی، ساخت و توسعه فناوری‌های پیشرفته حفاظت از حریم خصوصی، تضمین ایمنی با ساخت محصولات ایمن به شکل پیش‌فرض**
مصادیق و رویکردهای سازمانی	**اصول بنیادین حریم خصوصی متا، نحوه استفاده از اطلاعات گردآوری شده، رویکرد ایکس به حریم خصوصی، پلتفرم‌های ایرانی و بی‌توجهی به حفاظت از داده‌های شخصی**
حقوق و تعهدات کنترل‌گران و پردازشگران	**تعهدات کنترل‌گران و پردازشگران، تنظیم و نظارت بر پردازش داده‌های شخصی، مسئولیت کنترل‌گر و پردازشگر، بخش ۳: تحریم‌ها و مجازات‌ها**
مصادیق و حریم خصوصی در اسلام	**حریم خصوصی در اسلام، مصداق‌های حریم خصوصی در اسلام، حدود اختیار دولت برای ورود به حریم خصوصی، حق حریم خصوصی به مثابه حق بنیادین در حکومت اسلامی از منظر امام خمینی**

جدول ۵-۱) مضامین نهایی اصلی و فرعی مرتبط با حریم خصوصی و حریم داده

نتایج کلی و یافتهّای اصلی انجام تحلیل

۱. این تحلیل با هدف کاربرد مبانی نظری اسلامی و دینی در تدوین مقررات حریم خصوصی در ایران انجام شد. مطالعه اسناد بین‌المللی و نیز مقررات فعلی در مورد حریم داده‌ها نشان می‌دهد که مبتنی کردن حق حفاظت از حریم خصوصی بر مبانی متقن و محکم بوده است. ازجمله مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا مبتنی بر منشور حقوق اساسی اتحادیه اروپا است. در این قانون حریم خصوصی به عنوان یک حق اساسی اشخاص حقیقی مدنظر قرار گرفته است. اما ملاحظه اسناد و منابع دینی نشان داد که در زمینه اجتماعی ایران، ملاحظه حق حریم خصوصی را می‌توان فراتر از آن به‌منزله پاسداشت کرامت و منزلت انسان مدنظر قرار دارد.

۲. در اسناد و قوانین گوناگون، امکان تعرض به حریم خصوصی صرفاً با مجوز قانون و حکم قانونی امکان‌پذیر است اما در ادبیات دینی، از مصلحت عمومی یا اجتماعی سخن گفته شده است. از این منظر گرچه مصلحت فرد در احترام به حریم

خصوصی وی است اما گاهی برخی مصالح عمومی و اجتماعی همانند حفظ امنیت به ناچار نقض حریم خصوصی را توجیه می‌کند. از این تقدم مصلحت عمومی بر مصلحت فردی می‌توان قوانین و مقررات متناسب را استناط و تدوین کرد.

۳. با ملاحظه گرایش کلی فضای مجازی به پلتفرمی‌شدن و توسعه انواع پلتفرم‌ها ازجمله پلتفرم‌های رسانه‌های اجتماعی، پلتفرم‌های پیام‌رسان و نیز انواع پلتفرم‌های خدمات‌رسان، بحث‌های مرتبط با «حریم خصوصی در فضای مجازی به حریم خصوصی در پلتفرم‌ها تغییرجهت داده است». به‌عبارت دیگر، از آنجا که بخش اعظم تعاملات، ارتباطات و تراکنش‌های افراد پلتفرم–مبنا شده است، حریم خصوصی و حریم داده نیز به‌ناچار تا حد زیادی به حریم خصوصی در پلتفرم‌ها متمرکز شده است. بر این اساس، با ملاحظه حجم گسترده‌تر محتواهای کاربرساخته در انواع پلتفرم‌ها، موضوع صیانت و حفاظت از حریم خصوصی (حریم داده و ارتباط) منوط به و وابسته به مقررات و کردارهای حکمرانی پلتفرم‌ها وابسته شده است. درک، امروزه یکی از حوزه‌های اساسی سازکار تعدیل محتوا یا حکمرانی محتوا در پلتفرم‌ها مربوط به حریم خصوصی است. درهمین راستا سیاست حریم خصوصی یکی از اسناد اصلی پلتفرم‌های بزرگ است که در آن تمام جزئیات مرتبط با نحوه گردآوری تا اشتراک‌گذاری و فروش اطلاعات و داده‌های شخصی کاربران ذکر شده است. این موضوع شامل قابلیت‌های خاص پلتفرم‌ها و نیز یکی از ویژگی‌های اساسی پلتفرم‌ها که شامل گردآوری داده‌های شخصی به شکل کلان‌داده و انتفاع از این منبع غنی و سودآور نیز می‌شود.

۴. برخلاف اسناد و مقرراتی که از موضوع داده یا شخص یا اشخاص حقیقی برای بحث در مورد نحوه پردازش داده‌ها سخن گفته‌اند، ما از مفهوم کاربر پلتفرم‌ها برای بحث درباره حقوق وی در گردآوری و پردازش داده‌ها استفاده کرده‌ایم. به این علت که وقتی از پلتفرم و رسانه اجتماعی سخن می‌گوییم، ما در اصل عمدتاً با محتوای کاربرساخته مواجه هستیم که محصول کنش کاربران در رسانه‌های اجتماعی است.

۵. ما در این پژوهش از میان انواع حریم خصوصی هم بر حریم داده و هم حریم ارتباط تمرکز کردیم. برخلاف اسنادی که صرفاً حریم داده را مدنظر قرار داده‌اند، ازآنجام که ما می‌خواهیم حفظ حریم خصوصی در پلتفرم‌های گوناگون ازجمله رسانه‌های اجتماعی و پیام‌رسان‌ّها را مدنظر قرار دهیم، تلاش کردیم تا در مورد حریم ارتباط نزدیک مفهوم پردازی کنیم. در مقررات فعلی حق ارتباط صرفاً در شبکه ارتباطات سنتی (همانند ممنوعیت استراق سمع در شبکه مخابرات یا ممنوعیت تفتیش مرسوله‌های پستی) مد نظر قرار گرفته بود اما ما با ملاحظه تحولات فناورانه کنونی آنرا به حفاظت از حق ارتباط در

پلتفرم‌ها ازجمله حق حریم خصوصی در ارتباطات میان‌فردی در پیام‌رسان‌ها نیز بسط دادیم. یعنی حق ارتباط را می‌توان به پیام‌رسان‌ها و نیز ارتباط میان‌فردی در رسانه‌های اجتماعی گسترش داد. همچنین ضمن بحث در مورد فضا و مکان لزوم حفظ حرمت حریم مکانی حساب کاربری کاربران در رسانه‌های اجتماعی را دارای حق حریم مکانی تلقی کردیم که در صورت انجام تنظیمات باید محترم شمرده شود.

۶. با وجود بحث‌های گسترده دینی در مورد حریم شخصی و لزوم حفاظت از آن، بخش عمده قوانین و مقررات ایران به این امر بی‌توجه بوده‌اند. حتی در قانون اساسی نیز حق حریم خصوصی به عنوان یک حق اساسی مورد غفلت واقع شده است و برخی اصول آن به شکل تلویحی به آن مرتبط هستند. یکی پیامدهای این موضوع، نبود اصطلاح واحد برای حریم داده و کاربرد اصطلاح مختلف برای آن است. ازجمله حریم داده‌های شخصی در قوانین و مقررات ایران وجود ندارد.

بر این اساس و با این ملاحظات، و ضمن ملاحظه این موضوع که اخیراً لایحه‌ای برای حفاظت از داده‌های شخصی پس از مدتها بررسی در حدود مرداد ۱۴۰۳ از سوی دولت به مجلس شورای اسلامی ارسال شده است که در دسترس پژوهشگر حاضر قرار ندارد، برخی پیشنهادهای سیاستگذارانه به شرح ذیل بیان می‌شود. همچنین به پیوست با ملاحظه نکات فوق و یافته‌های پژوهش و ملاحظه مقررات مشابه، پیش‌نویس یک لایحه قانونی با عنوان «**حفاظت از حریم داده‌های شخصی و حریم ارتباط در پلتفرم(سکو)های رسانه‌های اجتماعی و خدماتی**» ارائه می‌شود که با ملاحظه نتایج این پژوهش تدوین شده است که مهمترین ویژگی‌های آن عبارتند از: تمرکز بر کار، ملاحظه مبانی دینی در تدوین مقررات، ملاحظه سلطه پلتفرم‌ها بر فضای مجازی، ملاحظه درون‌مرزی و فرامرزی بودن حق ارتباط و حق حریم داده‌های شخصی و توجه به پلتفرم‌های داخلی و خارجی، ارائه تعاریف دقیق و فراگیر از مفاهیم اصلی. بنابراین، ما صرفاً حفاظت از داده‌های شخصی را به شکل را مدنظر قرار نداده‌ایم و آنرا به حریم ارتباط و ملاحظات مرتبط با پلتفرمی‌شدن نیز بسط داده‌ایم.

در پاسخ به پرسش اصلی مقاله و پرسش‌های فرعی توضیحاتی ذکر می‌شود.

به طور کلی تدوین مقررات و قوانین مرتبط با حریم خصوصی مستلزم ملاحظه ابعاد مختلف الهی، انسان‌شناختی، دینی، قانونی و فناورانه است. بنابراین، طیفی از رویکردهای اساسی به حقوق انسان، رویکردهای کلان نظری به این مقوله، مقررات پیشین در یک حوزه قضایی و فناورانه و نیز عوامل فراسرزمینی، از الزامات تقید به حقوق بین‌الملل تا تسری

تحولات فناورانه به قلمرو سرزمینی، ازجمله جهانی‌شدن پلتفرم‌های دیجیتال و رسانه‌های اجتماعی و آثار آن بر حق حاکمیت و درهم‌تنیده‌شدن بحث‌های مرتبط با حفظ حریم خصوصی درون قلمرو قضایی با سازوکارهای گردآوری و صیانت از داده‌ای شخصی در این پلتفرم‌ها است.

-مبانی تنظیم مقررات حریم خصوصی در ایران: حریم خصوصی به‌منزله یکی از پیش‌شرط‌های کرامت انسانی

یکی از ابعاد رویکردهای اساسی به انسان و حقوق آن، نحوه نگرش به حق حریم خصوصی است. در حقوق بین‌الملل که بر حقوق بشر تأکید ویژه‌ای می‌شود، حریم خصوصی به‌عنوان یک حق بنیادین یا اساسی به رسمیت شناخته شده است و مجموعه اقدامات حقوقی و قضایی نیز در راستای نیل به آن طی چندین دهه گذشته پیگیری شده است. ازجمله در مقررات عمومی حفاظت از داده‌ها که مبتنی بر منشور حقوق اساسی اتحادیه اروپا است، بر حق حریم خصوصی به عنوان یک حق اساسی تأکید شده است. بر این اساس، محترم شمردن انسان و حریم خصوصی وی مبتنی بر توافق و قراردادهای منعقده است اما مبنای حرمت حریم خصوصی انسان در اندیشه دینی ناشی از کرامت ذاتی وی است. به عبارت دیگر، انسان‌ها دارای مقام بالایی نسبت به دیگر موجودات هستند، و به اصطلاح دارای کرامت ذاتی هستند. کرامت انسانی ازچند جهت قابل توجه است. اول، بخش کرامت به انسان از سوی پروردگار: « «ما بنی‌آدم را کرامت بخشیدیم و آنان را بر صحرا و دریا مسلط کردیم و بر بسیاری از مخلوقات خویش برتری دادیم» (سوره اسراء، آیه ۱۷)؛ جانشین خدا بودن: «به یاد آور زمانی را که خداوند به فرشتگان فرمود: به راستی روی زمین جانشین قرار خواهم داد». (بقره، آیه ۳۰)؛ کارگزار بودن و در خدمت انسان بودن جهان: «آن‌چه در آسمان و زمین است، تسخیر شما قرار دادیم ...» (جائیه، ۱۳). بنابراین، نظر شأن و کرامت و منزله ذاتی الهی انسان و اینکه انسان جانشین خداوند بر روی زمین است، حرمت آزادی و به‌ویژه آزادی وی در حریم شخصی باید مورد احترام قرار گیرد. حفظ شأن و کرامت انسان یکی از بنیان‌های اساسی بحث‌های حریم خصوصی در اسلام است. از آنجا که انسان دارای کرامت ذاتی است و از این جهت جان و مال و آبروی او باید محترم شمرده شده و از تعرض مصون بماند. ازجمله اموری که به حریم شخصیتی انسان مرتبط می‌شود، نوع اطلاعات و ارتباطات او با دیگران است که از طریق ابزارهای ارتباطی گوناگون صورت می‌گیرد. در قانون اساسی جمهوری اسلامی ایران اصطلاح حریم خصوصی ذکر نشده است اگر حفظ شأن و کرامت انسان را یکی از بنیان‌های اساسی بحث‌های حریم خصوصی در اسلام تلقی کنیم، در این‌صورت می‌توان حفظ کرامت انسان را به مثابه یک اصل پذیرفته شده در قانون اساسی مورد ملاحظه قرار

دهیم که به طور ضمنی، حمایت از حریم خصوصی وی نیز مورد تأیید و تأکید در قانون اساسی جمهوری اسلامی ایران است. چنانچه در بند ششم اصل دوم قانون اساسی «کرامت و ارزش والای انسان و آزادی توأم با مسئولیت او در برابر خدا» به عنوان یکی از مبانی جمهوری اسلامی بیان شده است. در بند ۱۴ اصل سوم قانون اساسی، «تأمین حقوق همه جانبه افراد از زن و مرد و ایجاد امنیت قضایی عادلانه برای همه و تساوی عموم در برابر قانون» یکی از شرایط دستیابی به کرامت انسان ذکر شده است. بنابراین، می‌توان استنباط کرد که حمایت از حریم خصوصی به‌مثابه یکی از پیش‌شرط‌های حفظ کرامت انسان ایرانی به رسمیت شناخته شده است و نقض حریم شخصی وی پیش از هرچیزی خدشه به حرمت و کرامت انسانی اوست.

با وجود اهمیت انسان و احترام به حریم خصوصی وی در مبانی دینی و اسلامی، این موضوع آن‌چنان که باید و شاید در حکومت اسلامی جدی گرفته نشده است. برهمین اساس بود که امام خمینی، بنیان‌گذار انقلاب اسلامی، در سخنرانی‌ها و فرمان‌هایشان توجه ویژه‌ای به حفظ شأنیت انسان‌ها و احترام به حریم خصوصی شهروندان داشته‌اند و فرمان تاریخی هشت ماده‌ای ایشان در اوایل پیروزی انقلاب اسلامی صادر شد از مهم‌ترین مصادیق توجه ایشان به حریم خصوصی و حقوق شهروندی افراد است، اما حریم خصوصی و مقررات مربوط به آن چندان جدی گرفته نشده است؛ به‌طوری‌که در حدود ۲۵ سال پس از پیروزی انقلاب نخستین لایحه حفظ حریم خصوصی در مجلس شورای اسلامی مورد بررسی قرار گرفت و تصویب نشد و اکنون هم که حدود ۴۵ سال از انقلاب اسلامی می‌گذارد، همچنان قانون جامعی برای حریم خصوصی وجود ندارد.

اصول تدوین یک قانون جامع حریم خصوصی و داده‌های شخصی در ایران

برای تدوین یک قانون جامع حریم خصوصی و داده‌های شخصی در ایران، لازم است اصول زیر که برگرفته از مفاهیم کلیدی ارائه‌شده هستند، به‌عنوان پایه‌های اساسی مورد توجه قرار گیرند:

حریم خصوصی به‌مثابه یک حق بنیادین انسانی

قانون باید حریم خصوصی را به‌عنوان یکی از حقوق بنیادین انسان به رسمیت بشناسد. این حق باید فراتر از جنبه‌های فردی به‌عنوان یک عنصر مهم در حفظ کرامت انسانی و استقلال فردی تلقی شود. تضمین این حق، پایه‌ای برای تنظیم سایر اصول در قانون خواهد بود.

۲. حریم خصوصی در بستر اجتماعی، تاریخی، و فرهنگی

– به‌مثابه امری غریزی و اجتماعی: حریم خصوصی از نیازهای اساسی انسان است و باید به نحوی تنظیم شود که در تعاملات اجتماعی و زندگی روزمره به رسمیت شناخته شود.

– به‌مثابه امری تاریخی: قانون باید تغییرات تاریخی مفهوم حریم خصوصی را در نظر گیرد و با نیازهای روز جامعه و فناوری‌های نوین هماهنگ باشد.

۳. حریم خصوصی و کنترل داده‌ها

– حق کنترل و دسترسی: افراد باید بر داده‌های شخصی خود کنترل کامل داشته باشند و بتوانند تعیین کنند چه کسی و چگونه به این داده‌ها دسترسی پیدا کند.

– حق دسترسی به اطلاعات: قانون باید تضمین کند که کاربران بتوانند داده‌های گردآوری‌شده درباره خود را مشاهده و مدیریت کنند.

۴. حریم خصوصی و ارتباطات در فضای دیجیتال

– رسانه‌های اجتماعی و فضای مجازی: حریم خصوصی کاربران در پلتفرم‌های دیجیتال باید مورد توجه جدی قرار گیرد. این شامل محافظت از پروفایل‌های رسانه‌های اجتماعی، تبادل پیام‌ها، و تضمین رمزگذاری ارتباطات است.

– رمزگذاری به‌عنوان پیش‌نیاز حریم ارتباطی: قانون باید رمزگذاری قوی را برای حفاظت از ارتباطات شخصی کاربران الزامی کند.

۵. حقوق کاربران در مدیریت داده‌ها

– حق اطلاع و شفافیت: کاربران باید از نحوه گردآوری و پردازش داده‌های خود آگاه باشند.

– حق اصلاح، پاک کردن، و انتقال داده‌ها: قانون باید به کاربران اجازه دهد داده‌های نادرست خود را اصلاح کنند، داده‌های غیرضروری را حذف کنند، یا آن‌ها را به سایر ارائه‌دهندگان خدمات انتقال دهند.

– حق اعتراض و محدودیت پردازش: کاربران باید بتوانند از پردازش داده‌های خود جلوگیری کنند، مگر در شرایط خاص قانونی.

۶. محدودیت‌های قانونی در ورود به حریم خصوصی

– لزوم قانونی بودن ورود به حریم خصوصی: قانون باید محدودیت‌های دقیقی برای ورود به حریم خصوصی تعیین کند و این امر را به حکم قانونی مشروط کند.

– عدم نقض حریم خصوصی بدون حکم قانونی: نقض حریم خصوصی، به‌ویژه توسط نهادهای دولتی، باید به‌عنوان جرم شناخته شود.

۷. حریم خصوصی و مبانی اسلامی

– مطابقت با اصول اسلامی: قانون باید با مفاهیم اسلامی مانند کرامت انسانی و مصلحت عمومی هم‌راستا باشد.

– حریم خصوصی در حکومت اسلامی: دیدگاه‌هایی مانند حریم خصوصی به‌مثابه حق بنیادین از منظر امام خمینی باید مبنای تدوین قانون قرار گیرد.

– مصلحت عمومی و امنیت: مواردی که امنیت عمومی در خطر است، باید تنها با محدودیت‌های مشخص اجازه نقض حریم خصوصی را بدهند.

۸. تعهدات پردازشگران داده و نظارت

– مسئولیت‌پذیری پردازشگران داده: تمامی نهادها و سازمان‌هایی که داده‌های شخصی را پردازش می‌کنند، باید در برابر حفاظت از این داده‌ها پاسخگو باشند.

– نهاد نظارتی مستقل: قانون باید یک نهاد مستقل برای نظارت بر اجرای مقررات حریم خصوصی و رسیدگی به تخلفات تعیین کند.

۹. حفاظت از داده‌ها در سطح بین‌المللی

– هماهنگی با اسناد بین‌المللی: قانون باید با استانداردهای جهانی مانند مقررات عمومی حفاظت از داده‌ها (GDPR) همخوانی داشته باشد.

– ممنوعیت فروش داده‌ها به شخص ثالث: انتقال یا فروش داده‌های کاربران به اشخاص ثالث بدون رضایت آن‌ها باید به‌طور کامل ممنوع شود.

۱۰. ایمنی و امنیت در فضای دیجیتال

– محصولات امن به‌صورت پیش‌فرض: تمامی خدمات و محصولات دیجیتال باید با اصول ایمنی پیش‌فرض طراحی شوند تا حفاظت از داده‌ها در اولویت باشد.

– توسعه فناوری‌های پیشرفته حفاظت از داده‌ها: قانون باید مشوق توسعه فناوری‌های نوین برای افزایش حفاظت از داده‌ها باشد.

این اصول می‌توانند چارچوبی جامع برای تدوین یک قانون موثر و متناسب با نیازهای ایران ایجاد کنند و در عین حال حقوق افراد را در برابر چالش‌های ناشی از پیشرفت‌های فناوری تضمین نمایند.

–زمینه حقوقی مقررات و قوانین مرتبط با حریم خصوصی و حریم داده

در نظام حقوقی ایران، حریم خصوصی به صورت مشخص و معنون حمایت نشده و در واقع، موضع حقوق موضوعه ایران در مواجهه با حریم خصوصی، تحویل گرایانه است. حقوق و آزادی ها به منزله حریم خصوصی به طور ضمنی و در میان سایر قواعد حقوقی، به طور ناقص، مورد حمایت قرار گرفته اند. قانون اساسی، قانون مجازات اسلامی، قانون آیین دادرسی کیفری، قانون آزادی اطلاعات، قوانین و مقررات مربوطه به ارتباطات پستی، تلفنی و قانون مطبوعات در زمره قوانین و مقرراتی هستند که گاه ضمنی و گاه صریحاً از برخی مصادیق حریم خصوصی حمایت کرده اند. البته برخلاف قوانین اساسی کشورهایی که از حریم خصوصی به صورت مشخص و در قالب اصل یا اصول خاصی حمایت کرده اند، در قانون اساسی ایران متن خاصی که از حریم خصوصی، تحت این عنوان حمایت کرده باشد، وجود ندارد. مهمترین اصل قانون اساسی که تا حد زیادی به شکل مستقیم با حریم خصوصی در ارتباط دارد، اصل بیست و پنجم است. طبق این اصل «بازرسی و نرساندن

نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون». این اصل درواقع، بر اساس مباحثی که مطرح شد، فقط بر حریم ارتباطی به عنوان یکی از ابعاد حریم خصوصی توجه دارد. بنابراین درمجموع باید اذعان کرد که حریم خصوصی داده‌ها و اطلاعات شخصی به هیچ‌وجه در قانون اساسی مورد توجه قرار نگرفته است. همچنین مرور ادبیات مرتبط با حریم اطلاعات و داده‌های شخصی در ایران نشان داد، در مورد کاربرد یک اصطلاح واحد برای حریم داده‌ها نیز اتفاق نظر وجود ندارد، چه برسد به اینکه این اصطلاح تعریف شود. در قوانین ایران از تعابیر مختلفی برای حریم خصوصی اطلاعات و ارتباطات استفاده می‌شود که از جمله آنها می‌توان به «اسرار شخصی» در قانون مطبوعات، «اسرار مردم» در قانون مجازات اسلامی، «داده‌های شخصی» و «حریم خصوصی» در قانون آزادی اطلاعات، «صوت و تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری» در قانون جرایم رایانه‌ای و نیز عبارت «حریم خصوصی» در مصوبات شورای عالی انقلاب فرهنگی و مجمع تشخیص مصلحت نظام اشاره کرد. عدم وحدت رویه در کاربرد در کاربرد یک اصطلاح برای حریم خصوصی و حریم داده و ارتباطات، یکی از معضلات اساسی در تعریف دقیق مفاهیم است که، همانند بسیاری از موارد دیگر، به فهم نادرست آن منجر شده است. نگاه دینی و اخلاقی به حریم خصوصی در نزد عامه مردم و عدم اشاره صریح قانونی به آن از یکی از معضلاتی است که بحث حریم خصوصی در ایران با آن مواجه بوده است. بنابراین، به‌رسمیت شناخته شدن حق حریم خصوصی و دستیابی به اصطلاحی واحد یکی از الزامات تدوین قوانین مرتبط با حریم خصوصی در ایران است.

–علاوه بر پلتفرم‌های ایرانی همانند پیام‌رسان‌ها و نیز پلتفرم‌های خدماتی همانند پلتفرم‌های خدمات اقامتگاه و نیز توزیع غذا که داده‌های شهروندان را گردآوری می‌کنند و در چند مورد نیز به افشای گسترده اطلاعات شخصی کاربران ایرانی منجر شده است، کاربران داده‌های شخصی خود را در پلتفرم‌های بزرگ جهانی همانند اینستاگرام، تلگرام و واتس‌اپ نیز به اشتراک می‌گذارند. دسترسی شرکت‌های فراملی جهانی به داده‌های شهروندان کشورهای مختلف، بدون ضابطه روشن و نیز به شکل گسترده و بی‌وقفه، یکی از معضلاتی که در عصر پلتفرم‌ها با آن مواجه هستیم. حتی با وجود ایجاد نسخه‌های داخلی فراگیر از رسانه‌های اجتماعی و پیام‌رسان‌ها، امکان منع کامل شهروندان از حضور در رسانه‌های اجتماعی خارجی وجود ندارد، بلکه جریان و پردازش داده‌های شخصی به شکل فرامرزی یک چالش و نگرانی عمده نه تنها برای دولت ایران بلکه برای بسیاری از کشورهای جهان است. دست‌کم در وضعیت کنونی حکمرانی اینترنت و پلتفرم‌ها، این وضعیت قابل

اصطلاح کامل نیست، فقط می‌توان اقداماتی با تخفیف یا فرونشانی جریان خروشان داده‌های کلان به مراکز داده‌کاوی پلتفرم‌های جهانی انجام داد. در مورد پلتفرم‌های خدماتی که با الهام از نمونه‌ّای بزرگ جهانی همانند اوبر و ایر.بی.ان.بی توسعه یافته‌اند و نمونه‌ّای جهانی در بازار ایران حضور نداند وضعیت از منظر حفظ داده‌های شهروندان در قلمرو سرزمینی مناسب‌تر است اما با وجود این عدم اتخاذ اقدامات امنیت داده سبب شده است تا طی چند رخداد اخیر، نفوذگران به راحتی به داده‌های شخصی شهروندان دسترسی پیدا کنند و آنرا افشاء کنند. بنابراین، موضوع امنیت داده‌های شخصی در پلتفرم‌های ایرانی باید مورد ملاحظه جدی قرار گیرد، به‌ویژه زمانی که برخلاف رسانه‌های اجتماعی داده‌های شخصی آزادانه در دسترس شرکتهای خارجی قرار نمی‌گیرد. بنابراین، ملاحظات مرتبط با پلتفرمی‌شدن و فرامرزی شدن داده‌های شخصی در تدوین مقررات یک امر اساسی است که باید مورد توجه قرار گیرد.

-همانطور که گفته شد به جز برخی قوانین و مقررات بخشی همانند قانون جرایم رایانه‌ای و اشاره مختصر به حفاظت از داده‌های شخصی در برخی قوانین در مجموع سه اقدام کلان برای حفاظت از حریم خصوصی و حریم داده‌های شخصی در ایران انجام شده است. اول، لایحه حریم خصوصی سال ۱۳۸۳ و دوم لایحه صیانت از داده‌های شخصی ۱۳۹۷ و سوم لایحه «حفاظت از داده‌های شخصی» که اخیراً در مرداد ۱۴۰۳ در اواخر فعالیت دولت وقت به مجلس شورای اسلامی ارسال شده است. دو لایحه قبلی که به سرانجام نرسیده‌اند و لایحه سوم نیز به تازگی به مجلس ارسال شده است و بنابراین مراحل رسیدگی و تصویب آن فرایندی طولانی را سپری خواهد کرد. بررسی مفاد لایحه اول نشان داد که موضوع اصلی آن حفظ حریم خصوصی به طور کلی با ابعاد گوناگون آن ازجمله حریم مکانی، جسمانی، اطلاعاتی و ارتباطی با ملاحظه توسعه فناورانه در اوایل دهه ۱۳۸۰ شمسی بوده است. به مفاد لایحه سوم دسترسی پیدا نکردیم اما بررسی لایحه دوم نیز نشان داد که بخش عمده ارائه نسخه‌ای ناقص از مقررات عمومی حفاظت از داده‌های شخصی در اتحادیه اروپا است و به الزامات بومی در این زمینه توجه نشده است.

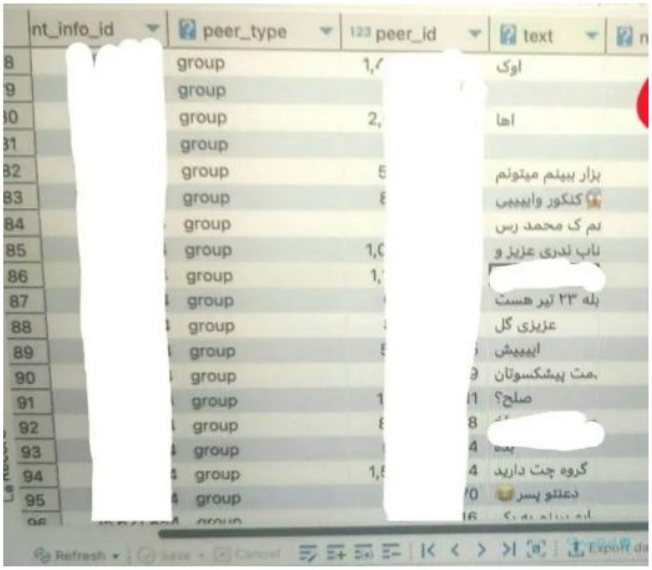
-همانطور که در تحلیل یافته‌ها به شکل مفصل بررسی شد، در سطح جهان تاکنون برخی اقدامات اساسی برای حفاظت از حریم داده‌های شخصی انجام شده است. مهمترین آنها مقررات عمومی حفاظت از داده‌ها در سطح اتحادیه اروپا است. این قانون کامل‌ترین و مفصل‌ترین مقررات مرتبط با پردازش داده‌های شخصی محسوب می‌شود. دو قانون دیگری که بررسی

شد، قانون حفاظت از حریم شخصی مصرف‌کنندگان کالیفرنیا و قانون حریم خصوصی چین است. اولی یک قانون ایالتی و دومی یک قانون ملی است که جزیئات آن در بخش تحلیل یافته‌ها قابل دسترسی است.

–مطالعه نحوه مواجهه پلتفرم‌های جهانی با حریم داده‌های شخصی نشان داد که این پلتفرم‌ها اسناد و نیز کردارهای گسترده‌ای را درخصوص حریم خصوصی داده‌های کاربران خود تصویب و در پیش گرفته‌اند. بخش عمده پلتفرم‌های بزرگ در قسمت شرایط ارائه خدمت و یا به طور خاص در سیاست حریم خصوصی خود به شکل مفصل در رویکردهای کلان، انواع اطلاعات گردآوری‌شده از کاربران، نحوه استفاده و پردازش آنها و نیز نحوه اشتراک‌گذاری با طرف‌های ثالث و الزامات قانونی و نیز اقدامات فنی آنها برای مثل از طریق حفاظت از حریم داده‌ها به شکل حفظ حریم خصوصی بر اساس طراحی توضیح داده شده است. گرچه برخی پلتفرم‌های ایرانی همانند ایتا نیز سیاست حریم خصوصی خود را اعلام کرده‌اند[1]، اما در مقایسه با نسخه‌های جهانی آنها بسیار مختصر هستند.

همچنین حفظ حریم ارتباطی در پیام‌رسان‌ها منوط به کاربرد فناوری رمزگذاری سرتاسری است تا محتوای پیام مبادله‌شده در یک ارتباط شخصی برای دیگران قابل مشاهده نباشد. اما انتشار تصویری از مشاهده محتوای پیام‌های مبادله شده در یکی از گروه‌های بله در اواخر تیر ۱۴۰۲ نگرانی نسبت به دسترسی به محتوای پیام‌های مبادله شده در این پیام‌رسان را افزایش داد.

[1] . https://eitaa.com/privacy/#id-7



در این تصویر محتواهای پیام به شکل کامل در دسترس قرار داشت. در واکنش به این موضوع، پیام‌رسان بله بیانیه‌ای صادر کرد و توضیحاتی ارائه کرد: بله در بیانیه خود عنوان کرده است موارد افشاء شده در این تصویر، در مورد محتواهای عمومی کانال‌های بیش از هزار کاربر مصداق دارد که محتوای آنها از سوی سایر کاربران به عنوان محتوای نامناسب گزارش شده و از سوی بله مورد بررسی قرار گرفته است[1].

در این بیانیه آمده است: «بله، به عنوان یک پلتفرم، مانند تمام پلتفرم‌های دیگر موظف است تدابیر لازم را برای جلوگیری از کلاهبرداری‌ها و حفظ امنیت، درباره فعالیت کاربران خود در پلتفرم، اتخاذ کند. از این رو طبق سند قوانین و شرایط استفاده از بله که در قوانین و شرایط استفاده از پیام‌رسان بانکی بله منتشر شده «برای کانال‌ها و بازوهایی که به صورت عمومی در دسترس هستند، بله از الگوریتم‌های خودکار برای آنالیز پیام‌ها برای جلوگیری از انتشار محتوای مجرمانه استفاده می‌کند. همچنین کاربران می‌توانند در صورت مشاهده این موارد، گزارش آن را به بازوی پشتیبانی ارسال یا از گزینه «گزارش محتوای نامناسب» استفاده کنند».

[1] . سازوکار پرچم‌زنی یا علامت‌دهی در پلتفرم‌ها که یکی از ابزارهای نظارت جمعی بر محتوای پلتفرم‌ها است و بیشتر پلتفرم‌های مبتنی بر محتوای کاربرساخته از آن برای مقابله با محتواهای نامناسب از آن استفاده می‌کنند.

در بخشی از این بیانیه گفته شده است: «آنچه در تصویر مذکور از صفحه مانیتور منتشر شده، مربوط به ابزار اجرایی همین موضوع است. این ابزار صرفاً حاوی محتوای منتشرشده در کانال‌های عمومی و گروه‌های بیش از هزار عضو است که به صورت سیستمی و حسب نیاز کارشناسی، جهت مقابله با کلاهبرداری از کاربران مورد بررسی قرار می‌گیرد. بدیهی است که اطلاعات خصوصی کاربران، آی‌دی و شماره فرستنده محتوا و مواردی از این قبیل در جهت حفظ حریم خصوصی کاربران به عنوان خط قرمز بله، در حیطه این ابزار وجود ندارد و فقط محتوا، آن هم به صورت بی‌نام، در آن وجود دارد.» (کربلایی، ۱۴۰۲).

در مورد این بیانیه چند نکته قابل ملاحظه است. نخست، اینکه پیام‌رسان‌ها بر اساس خط‌مشی تنظیم‌گری و حکمرانی خود اقدام به نقض حریم داده‌های شخصی کاربران کرده‌اند و اینکه برای این کار مجوز قانونی دارند یا خیر (حکمرانی بر پلتفرم)، مورد پرسش است. دوم، بر اساس ادعای پلتفرم بله اطلاعات خصوصی کاربران، آی‌دی و شماره فرستنده محتوا در اختیار ابزار ذکر شده یعنی بخش مانیتورینگ و پالایش وجود ندارد. اما به شکل ضمنی مشخص است که در رده‌های بالاتر به این نوع اطلاعات دسترسی وجود دارد. ضمن اینکه اطلاعات اخیر در بیشتر تعاریف حریم داده در زمره داده‌های شخصی هستند که باید از آن محافظت شود. بنابراین هم اصل رمزنگارانه محتوای پیام و هم اطلاعات موضوع داده (بنابر تعریف جی.دی.پی.آر) و کاربر پلتفرم به تعبیر ما با اصول حفظ حریم داده‌های کاربران در تناقض است.

گرچه سازمان فناوری اطلاعات اعلام کرده طی بررسی بخش‌های مختلف پیام‌رسان بله مشخص شده که اپراتور امکان مشاهده اطلاعات خصوصی کاربر ارسال‌کننده محتوا در کانال ها و گروه های عمومی مانند ایدی کاربر، نام ارسال کننده و شماره‌تلفن را ندارد؛ در نتیجه هیچگونه نقض حریم خصوصی مشاهده نشده و امنیت استفاده کاربران از پیام‌رسان بله همانند گذشته تأمین است (اسماعیلی، ۱۴۰۲).

پیشنهادهای سیاستگذارانه

با ملاحظات موارد فوق و مطالعه انجام شده برخی پیشنهادهای سیاستگذارانه درجهت حفاظت از داده‌های شخصی و نیز تدوین مقررات مرتبط به شرح ذیل اعلام می‌شود:

-در تدوین لایحه حفاظت از داده‌های شخصی به مبانی دینی و معرفتی از جمله حریم خصوصی به‌مثابه حرمت به کرامت انسانی توجه شود.

-لازم است با اتکاء به منابع دینی، حریم داده‌های شخصی در فضای مجازی بازتعریف شود و برخی مباحث قابل تعیمم در تدوین قانون لحاظ شود.

-در تدوین لایحه حریم داده‌های شخصی باید حریم ارتباطات نیز مدنظر قرار گیرد. زیرا امروزه حریم داده‌ها و اطلاعات در پلتفرم‌ها و رسانه‌های اجتماعی درهم‌تنیده شده‌اند.

-با مرور قوانین و مقررات و آشفتگی در کاربرد اصطلاح مناسب و تعاریف متفاوت لازم یک اصطلاح عمومی برگزیده و تعریف جامع و فراگیری از آن ارائه شود.

-با ملاحظه پلتفرمی‌شدن فزاینده زندگی روزمره و فعالیت افراد در این فضا، پیشنهاد می‌شود به جای اصطلاحاتی همانند موضوع داده (سوژه داده) و داده اشخاص، از حریم اطلاعات شخصی کاربران استفاده شود.

-در تدوین لایحه حریم اطلاعات شخصی باید حفاظت از حریم اطلاعات در پیام‌رسان‌ها و رسانه‌های اجتماعی مورد توجه قرار گیرد.

-لازم است به مسائل کلان همانند تفاوت پلتفرم‌های رسانه‌های اجتماعی ایرانی و پلتفرم‌های جهانی از منظر دسترسی به داده‌های شخصی کاربران توجه شود.

-در تدوین لایحه حریم داده‌های شخصی رضایت برای پردازش داده‌ها به عنوان یک اصل اساسی باید مورد توجه قرار گیرد.

-لازم است اصل مصلحت عمومی که بر مبنای آن می‌توان مجوز قانونی ورود به حریم خصوصی را صادر کرد مورد تأکید قرار گیرد.

-لازم است پلتفرم‌های داخلی، اصل رمزگذاری سرتاسری تبادیل پیام‌های شخصی را مراعات نمایند.

-در تدوین لایحه مربوط به حفاظت از داده‌ها، دو حوزه حریم خصوصی داده و امنیت داده می‌تواند با هم ترکیب شود. حریم داده‌ها به قوانین، دستورالعمل‌ها و بهترین شیوه‌های حاکم بر جمع‌آوری، استفاده، ذخیره‌سازی و به‌اشتراک‌گذاری داده‌های شخصی اشاره دارد. امنیت داده‌ها به جنبه‌های فنی محافظت از داده‌ها در برابر دسترسی غیرمجاز، سرقت، آسیب یا سایر

اشکال فعالیت‌های مخرب مربوط می‌شود. این شامل اجرای اقدامات امنیتی، ابزارها و پروتکل های مختلف برای حفاظت از داده‌ها است.

-هرگونه نظارت و پالایش محتوای شخصی کاربران در پیام‌رسان‌های ایرانی، حتی در فرایند تعدیل محتوا (پالایش محتوا) به‌منزله یکی از سازوکارهای حکمرانی درون‌پلتفرمی یا خودتنظیم‌گری، باید با کسب مجوز از مراجع قانونی صورت گیرد. به‌ویژه در مواردی که موضوع داده‌های شخصی حساس مطرح است.

-لازم است رده‌بندی سنی در حفاظت از داده‌های شخصی مورد توجه قرار گیرد. باید گردآوری داده‌های شخصی کاربران زیر سن قانونی (زیر ۱۳ سال و یا هر سن مقتضی دیگر) به طور کامل ممنوع شود.

-حریم ارتباطی کاربران باید از هر نوع مداخله مصون بماند، مگر به موجب دستور موردی و مشخص قانون.

-لازم است پلتفرم‌ها در برابر حفاظت از دادهٔای شخصی و حفظ امنیت دارای مسئولیت مطلق باشند. هر نوع نفوذ و افشای اطلاعات شخصی کاربران در این پلتفرم‌ها باید با مجازات‌های شدید و پیشگیری‌کننده همراه باشد.

پیوست ۱

خلاصه سیاستی

مقدمه

این پروژه پژوهشی با هدف مطالعه الزامات و ابعاد یک قانون جامع حریم خصوصی در ایران با ملاحظه فضای مجازی و پلتفرم‌های رسانه‌های اجتماعی انجام شده است. با وجود اهمیت یافتن فزاینده فضای مجازی و رسانه‌های اجتماعی در جامعه ایران، به ابعاد گوناگون از جمله حفاظت از حریم داده‌های شخصی و اطلاعات کاربران توجهی نشده است. درهم-تنیدگی فزاینده پلتفرم‌های دیجیتال و رسانه‌های اجتماعی با زندگی روزمره سبب می‌شود افراد به شکل خواسته یا ناخواسته داده‌های شخصی بیشتری را در فضای مجازی با طرفهای دیگر (شرکتها، دولتها، سازمانها، افراد) به اشتراک بگذارند. همچنین، پلتفرم‌های دیجیتال نیز بیش از پیش داده‌های شخصی ما را به مثابه مدل اصلی کسب و کار به کار می‌بندند. پیامد همه این موارد، تسهیل و تعمیق به مخاطره افکنده شدن حریم شخصی افراد و دشواری کناره‌گیری از این روندهای اجباری است. حریم خصوصی و داده‌های شخصی بیش از پیش به‌واسطه مدل فعالیت شرکتهای پلتفرمی جهانی مورد خدشه قرار می‌گیرد.

با وجود تأکید اسناد بالادستی گوناگون به اهمیت حریم خصوصی و ضرورت ایجاد سازوکارهای حفاظت از داده‌های شخصی افراد، در شبکه ملی اطلاعات تا پیام‌رسان‌های ایرانی و پلتفرم‌های رسانه اجتماعی خارجی، اقدام عملی در راستای تدوین اسناد جامع مرتبط با حفاظت از داده و حریم خصوصی در ایران صورت نگرفته است.

طی دو دهه گذشته در مجلس شورای اسلامی به عنوان نهاد اصلی قانونگذاری در نظام جمهوری اسلامی ایران و نیز دولت جمهوری اسلامی اقداماتی درجهت ارائه یک لایحه جامع مرتبط با حریم خصوصی انجام شده است که تاکنون به تدوین یک قانون جامع حفاظت از داده‌ها و حریم خصوصی در ایران منجر نشده است. حق داشتن حریم خصوصی[1] یکی از حقوق بنیادین همه انسانها و به‌ویژه حقوق مخاطبان رسانه‌ها و محصولات فرهنگی و رسانه‌ای است و در کنار حق بر آگاهی که

[1] .right to privacy

اسماعیلی (۱۴۰۱) آنرا به مثابه یکی از حقوق اساسی مخاطبان مورد بحث قرار داده است، از جمله وجوه اساسی حقوق مخاطبان است. بنابراین توانایی و امکان حفاظت از حریم خصوصی اشخاص در فضای مجازی و پلتفرم‌های رسانه‌های اجتماعی به این معنا است که یک بعد محوری از حقوق مخاطبان مورد توجه و تأکید قرار دارد.

بر اساس آنچه گفته شد و به‌ویژه ملاحظه کوشش‌های نافرجام برای ارائه یک قانون جامع حریم خصوصی در ایران، تحولات در اینترنت و پلتفرمی‌شدن آن، رویکردهای کلان به حکمرانی محتواهای پلتفرم‌های اجتماعی و با ملاحظه اینکه حفاظت از حریم خصوصی و ابعاد گوناگون به عنوان یک حق اساسی و پاسداشت کرامت و شأن انسان‌ها است مسئله اصلی این مطالعه این بوده است که «تدوین قانون جامع حکمرانی و تنظیم‌گری حریم خصوصی و داده‌های شخصی در فضای مجازی در ایران چه الزامات و چه ابعادی دارد؟».

روش‌شناسی

این پژوهش از نوع تحلیلی و کیفی است. در انجام این پژوهش از رویکرد چند روشی استفاده خواهد شد. شیوه گردآوری اطلاعات عمدتاً از نوعی کتابخانه‌ای و اسنادی است. برای انجام مطالعه گام‌ها و مراحل مختلفی طی می‌شود. یک بخش از این مطالعه شامل مرور مجموعه مطالعاتی که در ایران درباره حریم خصوصی انجام شده است. علاوه بر بر اساس منابع موجود مفهوم حریم خصوصی در فقه و نیز قوانین و اسناد بالادستی و قوانین مرتبط از قانون اساسی گرفته تا اسناد شورای عالی فضای مجازی و نیز قوانین گوناگون و همینطور پیش‌نویس‌هایی که تاکنون درباره حریم خصوصی ارائه شده است، تحلیل و مضامین آنها استخراج می‌شود تا چه حریم خصوصی در قوانین ایران چه ابعاد دارد و چه ابعادی مورد غفلت واقع شده است. تحلیل رویکرد دینی به حریم خصوصی به ما کمک می‌کند تا یک رویکرد محوری را در تدوین مقررات حریم خصوصی شناسایی کنیم. یک بخش دیگر تحقیق تحلیل قوانین حریم خصوصی (با ملاحظه اینترنت و رسانه های اجتماعی) کشورها و مناطق پیشگام است. علاوه بر این اسناد حریم خصوصی برخی از پلتفرمهای بزرگ همانند گوگل، متا و توئیتر نیز به روش تحلیل محتوای کیفی مورد مطالعه قرار می‌گیرند. مجموع این مطالعات به ما کمک می کند تا تصویر مناسبی از قوانین کنونی مرتبط با حریم خصوصی و حریم داده در سطح جهان کسب کنیم و برای تهیه یک پیش‌نویس جامع قانون اساسی به کار بگیریم. مجموع این مطالعات به ما کمک می کند تا تصویر مناسبی از قوانین کنونی مرتبط با

حریم خصوصی و حریم داده در سطح جهان کسب کنیم و برای تهیه یک پیش‌نویس جامع قانون اساسی به کار بگیریم. این مطالعه دربازه زمانی اسفند ۱۴۰۲ تا مرداد ۱۴۰۳ انجام شده است.

یافته‌ها و نتایج

۱. این تحلیل با هدف کاربرد مبانی نظری اسلامی و دینی در تدوین مقررات حریم خصوصی در ایران انجام شد. مطالعه اسناد بین‌المللی و نیز مقررات فعلی در مورد حریم داده‌ها نشان می‌دهد که مبتنی کردن حق حفاظت از حریم خصوصی بر مبانی متقن و محکم بوده است. ازجمله مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا مبتنی بر منشور حقوق اساسی اتحادیه اروپا است. در این قانون حریم خصوصی به عنوان یک حق اساسی اشخاص حقیقی مدنظر قرار گرفته است. اما ملاحظه اسناد و منابع دینی نشان داد که در زمینه اجتماعی ایران، ملاحظه حق حریم خصوصی را می‌توان فراتر از آن به‌منزله پاسداشت کرامت و منزلت انسان مدنظر قرار دارد.

۲. در اسناد و قوانین گوناگون، امکان تعرض به حریم خصوصی صرفاً با مجوز قانون و حکم قانونی امکان‌پذیر است اما در ادبیات دینی، از مصلحت عمومی یا اجتماعی سخن گفته شده است. از این منظر گرچه مصلحت فرد در احترام به حریم خصوصی وی است اما گاهی برخی مصالح عمومی و اجتماعی همانند حفظ امنیت به ناچار نقض حریم خصوصی را توجیه می‌کند. از این تقدم مصلحت عمومی بر مصلحت فردی می‌توان قوانین و مقررات متناسب را استناط و تدوین کرد.

۳. با ملاحظه گرایش کلی فضای مجازی به پلتفرمی‌شدن و توسعه انواع پلتفرم‌ها ازجمله پلتفرم‌های رسانه‌های اجتماعی، پلتفرم‌های پیام‌رسان و نیز انواع پلتفرم‌های خدمات‌رسان، بحث‌های مرتبط با «حریم خصوصی در فضای مجازی به حریم خصوصی در پلتفرم‌ها تغییرجهت داده است». به‌عبارت دیگر، از آنجا که بخش اعظم تعاملات، ارتباطات و تراکنش‌های افراد پلتفرم–مبنا شده است، حریم خصوصی و حریم داده نیز به‌ناچار تا حد زیادی به حریم خصوصی در پلتفرم‌ها متمرکز شده است. بر این اساس، با ملاحظه حجم گسترده‌تر محتواهای کاربرساخته در انواع پلتفرم‌ها، موضوع صیانت و حفاظت از حریم خصوصی (حریم داده و ارتباط) منوط به و وابسته به مقررات و کردارهای حکمرانی پلتفرم‌ها وابسته شده است. درک، امروزه یکی از حوزه‌های اساسی سازکار تعدیل محتوا یا حکمرانی محتوا در پلتفرم‌ها مربوط به حریم خصوصی است. درهمین راستا سیاست حریم خصوصی یکی از اسناد اصلی پلتفرم‌های بزرگ است که در آن تمام جزئیات مرتبط با نحوه

گردآوری تا اشتراک‌گذاری و فروش اطلاعات و داده‌های شخصی کاربران ذکر شده است. این موضوع شامل قابلیت‌های خاص پلتفرم‌ها و نیز یکی از ویژگی‌های اساسی پلتفرم‌ها که شامل گردآوری داده‌های شخصی به شکل کلان‌داده و انتفاع از این منبع غنی و سودآور نیز می‌شود.

۴. برخلاف اسناد و مقرراتی که از موضوع داده یا شخص یا اشخاص حقیقی برای بحث در مورد نحوه پردازش داده‌ها سخن گفته‌اند، ما از مفهوم کاربر پلتفرم‌ها برای بحث درباره حقوق وی در گردآوری و پردازش داده‌ها استفاده کرده‌ایم. به این علت که وقتی از پلتفرم و رسانه اجتماعی سخن می‌گوییم، ما در اصل عمدتاً با محتوای کاربرساخته مواجه هستیم که محصول کنش کاربران در رسانه‌های اجتماعی است.

۵. ما در این پژوهش از میان انواع حریم خصوصی هم بر حریم داده و هم حریم ارتباط تمرکز کردیم. برخلاف اسنادی که صرفاً حریم داده را مدنظر قرار داده‌اند، ازآنجام که ما می‌خواهیم حفظ حریم خصوصی در پلتفرم‌های گوناگون ازجمله رسانه‌های اجتماعی و پیام‌رسان‌ّها را مدنظر قرار دهیم، تلاش کردیم تا در مورد حریم ارتباط نزدیک مفهوم پردازی کنیم. در مقررات فعلی حق ارتباط صرفاً در شبکه ارتباطات سنتی (همانند ممنوعیت استراق سمع در شبکه مخابرات یا ممنوعیت تفتیش مرسوله‌های پستی) مد نظر قرار گرفته بود اما ما با ملاحظه تحولات فناورانه کنونی آنرا به حفاظت از حق ارتباط در پلتفرم‌ها ازجمله حق حریم خصوصی در ارتباطات میان‌فردی در پیام‌رسان‌ها نیز بسط دادیم. یعنی حق ارتباط را می‌توان به پیام‌رسان‌ها و نیز ارتباط میان‌فردی در رسانه‌های اجتماعی گسترش داد. همچنین ضمن بحث در مورد فضا و مکان لزوم حفظ حرمت حریم مکانی حساب کاربری کاربران در رسانه‌های اجتماعی را دارای حق حریم مکانی تلقی کردیم که در صورت انجام تنظیمات باید محترم شمرده شود.

۶. با وجود بحث‌های گسترده دینی در مورد حریم شخصی و لزوم حفاظت از آن، بخش عمده قوانین و مقررات ایران به این امر بی‌توجه بوده‌اند. حتی در قانون اساسی نیز حق حریم خصوصی به عنوان یک حق اساسی مورد غفلت واقع شده است و برخی اصول آن به شکل تلویحی به آن مرتبط هستند. یکی پیامدهای این موضوع، نبود اصطلاح واحد برای حریم داده و کاربرد اصطلاح مختلف برای آن است. ازجمله حریم داده‌های شخصی در قوانین و مقررات ایران وجود ندارد.

پیشنهادهای سیاستگذارانه

با ملاحظات موارد فوق و مطالعه انجام شده برخی پیشنهادهای سیاستگذارانه درجهت حفاظت از داده‌های شخصی و نیز تدوین مقررات مرتبط به شرح ذیل اعلام می‌شود:

-در تدوین لایحه حفاظت از داده‌های شخصی به مبانی دینی و معرفتی از جمله حریم خصوصی به‌مثابه حرمت به کرامت انسانی توجه شود.

-لازم است با اتکاء به منابع دینی، حریم داده‌های شخصی در فضای مجازی بازتعریف شود و برخی مباحث قابل تعیمم در تدوین قانون لحاظ شود.

-در تدوین لایحه حریم داده‌های شخصی باید حریم ارتباطات نیز مدنظر قرار گیرد. زیرا امروزه حریم داده‌ها و اطلاعات در پلتفرم‌ها و رسانه‌های اجتماعی درهم‌تنیده شده‌اند.

-با مرور قوانین و مقررات و آشفتگی در کاربرد اصطلاح مناسب و تعاریف متفاوت لازم یک اصطلاح عمومی برگزیده و تعریف جامع و فراگیری از آن ارائه شود.

-با ملاحظه پلتفرمی‌شدن فزاینده زندگی روزمره و فعالیت افراد در این فضا، پیشنهاد می‌شود به جای اصطلاحاتی همانند موضوع داده (سوژه داده) و داده اشخاص، از حریم اطلاعات شخصی کاربران استفاده شود.

-در تدوین لایحه حریم اطلاعات شخصی باید حفاظت از حریم اطلاعات در پیام‌رسان‌ها و رسانه‌های اجتماعی مورد توجه قرار گیرد.

-لازم است به مسائل کلان همانند تفاوت پلتفرم‌های رسانه‌های اجتماعی ایرانی و پلتفرم‌های جهانی از منظر دسترسی به داده‌های شخصی کاربران توجه شود.

-در تدوین لایحه حریم داده‌های شخصی رضایت برای پردازش داده‌ها به عنوان یک اصل اساسی باید مورد توجه قرار گیرد.

-لازم است اصل مصلحت عمومی که بر مبنای آن می‌توان مجوز قانونی ورود به حریم خصوصی را صادر کرد مورد تأکید قرار گیرد.

-لازم است پلتفرم‌های داخلی، اصل رمزگذاری سرتاسری تبادیل پیام‌های شخصی را مراعات نمایند.

–در تدوین لایحه مربوط به حفاظت از داده‌ها، دو حوزه حریم خصوصی داده و امنیت داده می‌تواند با هم ترکیب شود. حریم داده‌ها به قوانین، دستورالعمل‌ها و بهترین شیوه‌های حاکم بر جمع‌آوری، استفاده، ذخیره‌سازی و به‌اشتراک‌گذاری داده‌های شخصی اشاره دارد. امنیت داده‌ها به جنبه‌های فنی محافظت از داده‌ها در برابر دسترسی غیرمجاز، سرقت، آسیب یا سایر اشکال فعالیت‌های مخرب مربوط می‌شود. این شامل اجرای اقدامات امنیتی، ابزارها و پروتکل های مختلف برای حفاظت از داده‌ها است.

–هرگونه نظارت و پالایش محتوای شخصی کاربران در پیام‌رسان‌های ایرانی، حتی در فرایند تعدیل محتوا (پالایش محتوا) به‌منزله یکی از سازوکارهای حکمرانی درون‌پلتفرمی یا خودتنظیم‌گری، باید با کسب مجوز از مراجع قانونی صورت گیرد. به‌ویژه در مواردی که موضوع داده‌های شخصی حساس مطرح است.

–لازم است رده‌بندی سنی در حفاظت از داده‌های شخصی مورد توجه قرار گیرد. باید گردآوری داده‌های شخصی کاربران زیر سن قانونی (زیر ۱۳ سال و یا هر سن مقتضی دیگر) به طور کامل ممنوع شود.

–حریم ارتباطی کاربران باید از هر نوع مداخله مصون بماند، مگر به موجب دستور موردی و مشخص قانون.

–لازم است پلتفرم‌ها در برابر حفاظت از داده‌ّای شخصی و حفظ امنیت دارای مسئولیت مطلق باشند. هر نوع نفوذ و افشای اطلاعات شخصی کاربران در این پلتفرم‌ها باید با مجازات‌های شدید و پیشگیری‌کننده همراه باشد.

پیوست ۲

پیش‌نویس لایحه «حفاظت از حریم داده‌های شخصی و حریم ارتباط در پلتفرم(سکو)های رسانه‌های اجتماعی و خدماتی»[۱]

مقدمه

در راستای ضرورت پاسداشت منزلت و کرامت ذاتی انسان که آزادی فردی وی در حریم شخصی‌اش مورد تأکید قرار داده است و مصونیت وی از هرگونه تعرض در قلمروی شخصی وی را اکیداً منع کرده است، درراستای تبعیت از اسناد بین‌المللی که به حریم خصوصی به‌مثابه یک حق بنیادین و اساسی ارج نهاده است، مطابق با برخی اصول قانون اساسی اسلامی که حفظ حرمت و منزلت انسان را مورد تأکید قرار داده است، با ملاحظه فرمان بنیانگذار انقلاب اسلامی مبنی بر وظیفه حکومت برای دفاع از حریم خصوصی، منع ورود به حریم شخصی افراد و ممنوعیت تجسس در احوال شخصی افراد و با ملاحظه تحولات فناورانه و به مخاطره‌افکنده شدن داده‌های شخصی افراد و ضرورت مقررات‌گذاری برای صیانت از داده‌های افراد در فضای جهانی توسعه پلتفرمّ‌های رسانه‌های اجتماعی و خدماتی و نیز ضرورت پاسداشت حریم ارتباطات افراد در رسانه‌های اجتماعی از قبیل پیام‌رسان‌های و مبتنی بر قوانین و مقررات مختلفی که به نحوی از انحاء به حریم داده‌ها و اطلاعات توجه کرده‌اند، این پیش‌نویس به‌منزله تنظیم‌گر گردآوری و پردازش داده‌های شخصی و صیانت از مداخله غیرقانونی در ارتباطات کاربران در رسانه‌های اجتماعی این (پیش‌نویس) لایحه برای بررسی و تصویب ارائه می‌شود.

[۱]. با ملاحظه اینکه اخیراً لایحه جامعی از طرف دولت در مورد حفاظت از داده‌های شخصی به مجلس شورای اسلامی ارائه شده، تمرکز این پیش‌نویس به جهای حفاظت از داده به شکل کلی بر حریم خصوصی در پلتفرم‌های دیجیتال خواهد بود. همچنین با ملاحظه بعد اطلاعاتی حریم خصوصی، بر حریم خصوصی داده‌ها و ارتباطات متمرکز خواهیم شد.

اصول کلی

ماده ۱) این قانون در راستای صیانت از آزادی فردی شهروندان ایران و حفظ کرامت انسانی آنها در حریم خصوصی خود که مورد تأکید مبانی اسلامی، قانون اساسی جمهوری اسلامی ایران و اسناد بین‌المللی مبتنی بر احترام به حریم خصوصی افراد به‌مثابه یک حق اساسی است، تصویب و به اجرا گذاشته می‌شود.

ماده ۳) داده‌های شخصی و حق ارتباط خصوصی اشخاص حقیقی (کاربران) در پلتفرم‌های رسانه‌های اجتماعی تحت حفاظت قانون قرار دارد و هیچ فرد و سازمانی حق نقض آن و تجسس در ارتباطات برخط آنها و پردازش داده‌های شخصی افراد را بدون کسب رضایت افراد یا دستور قانونی ندارد.

ماده ۴) در شرایط خاص که مصالح جمعی بر مصلحت فردی تقدم پیدا می‌کند، از قبیل حفظ امنیت عمومی، با مجوز مشخص و موردی مراجع ذی‌صلاح قانونی، امکان ورود به حریم ارتباطی کاربران وجود دارد اما باید منحصراً در حدود مأموریت تعیین‌شده صورت گیرد و تجسس در امور دیگر برخلاف شرع و غیرقانونی و مستوجب مجازات مقتضی خواهد بود.

ماده ۴) با ملاحظه هدف این قانون که بر فضای مجازی و پلتفرم‌های دیجیتال متمرکز است، منظور از حریم خصوصی که بر بعد اطلاعاتی آن تمرکز دارد، حفاظت از داده‌های شخصی افراد و نیز حریم خصوصی ارتباطات آنها است.

ماده ۵) این قانون پردازش داده‌های شخصی و حریم خصوصی ارتباطات تمام کاربران واقع در قلمرو قضایی جمهوری اسلامی ایران را دربرمی‌گیرد و چنانچه پردازش در خارج از قلمرو قضایی ایران به دلایل گوناگون بر کاربران درون قلمرو قضایی ایران مربوط باشد، نیز قابل تسری و اعمال است.

تعاریف

ماده۶) در راستای اهداف این قانون اصطلاحات اصلی به شرح زیر تعریف می‌شوند:

-«پلتفرم‌های دیجیتال» زیرساخت‌های رایانشی برخطی هستند که تعامل، ارتباطات و تبادل اطلاعات، کالاها یا خدمات بین کاربران را تسهیل می‌کنند. پلتفرم‌های ایجیتال با ایجاد و حفظ ارتباط با دیگران، حس اجتماع و تعامل اجتماعی را تقویت می‌کنند. این پلتفرم‌ها به کاربران اجازه می‌دهند تا اشکال مختلف محتوا مانند متن، تصاویر، ویدیوها و فایل‌های صوتی را با اتصالات خود یا عموم مردم ایجاد، آپلود و به اشتراک بگذارند. ویژگی‌های تعاملی مانند نظرات، لایک‌ها،

اشتراک‌گذاری‌ها و واکنش‌ها باعث ایجاد تعامل و تعامل میان کاربران می‌شود. پلتفرم‌های دیجیتال به دلایل گوناگون اطلاعات شخصی کاربران را پردازش می‌کنند. پلتفرم‌های دیجیتال از الگوریتم‌هایی برای شخصی‌سازی توصیه‌های محتوا بر اساس ترجیحات و رفتار کاربر استفاده می‌کنند و تجربه کلی کاربر را بهبود می‌بخشند. این پلتفرم‌ها داده‌های کاربر را جمع‌آوری می‌کنند تا بینشی در مورد رفتار و ترجیحات کاربر به دست آورند، که به نوبه خود تجربیات شخصی و تبلیغات هدفمند را امکان‌پذیر می‌سازد.

– «حریم خصوصی در پلتفرم‌های دیجیتال» به سطح کنترلی که کاربران بر داده‌های شخصی خود دارند و میزان محافظت از فعالیت‌های برخط آنها در برابر دسترسی غیرمجاز یا نظارت عمومی و یا کاربرد آنها برای تحلیل کلان‌داده‌مبنا یا به قصد استفاده تجاری ازجمله فروش به آگهی‌دهندگان و یا نهادهای امنیتی و یا کاربرد در کارزارهای تبلیغات سیاسی اشاره دارد.

–«کاربران پلتفرم‌های دیجیتال» افراد حقیقی‌ای هستند که از طریق ایجاد حساب کاربری شخصی خود در انواع گوناگون پلتفرم‌ها و خدمات برخط عضو می‌شوند و از آنها برای ارتباط با دیگران، دسترسی به اطلاعات، اشتراک گذاری محتوا و استفاده از خدمات آنلاین مختلف برای مقاصد شخصی، حرفه ای یا تفریحی استفاده می‌کنند. آنها برای دریافت خدمات ملزم به ارائه سطوح مختلفی از اطلاعات شخصی خود هستند.

–«داده‌های شخصی» به معنای هر نوع اطلاعاتی که سبب شناسایی یک شخص حقیقی (کاربران پلتفرم) می‌شود و می‌تواند به‌شکلی مستقیم و غیرمستقیم و به آن شخص مرتبط است. این اطلاعات در دسترس عموم قرار ندارد و می‌تواند به دلایل گوناگون ازجمله عضویت در پلتفرم‌های اجتماعی در دسترس طرف‌های دیگر قرار گیرد. انواع داده‌های شخصی عبارتند از:

–اطلاعات پروفایل کاربر. جزئیاتی مانند نام، سن، جنسیت، موقعیت مکانی، تحصیلات، سابقه کار و سایر اطلاعات بیوگرافی که توسط کاربران ارائه می‌شود.

–داده‌های محتوا و فعالیت. محتوای متنی، عکس‌ها، فیلم‌ها و سایر موارد چندرسانه‌ای که توسط کاربران به اشتراک گذاشته می‌شود، و همچنین اطلاعاتی در مورد فعالیت‌های آنها، مانند لایک‌ها، اشتراک‌گذاری‌ها، نظرات و پست‌ها.

ارتباطات و تعاملات اجتماعی. دوستان، دنبال‌کنندگان و ارتباطاتی که کاربر در پلتفرم‌های رسانه‌های اجتماعی دارد، از جمله پیام‌ها، تعاملات و محتوای مشترک آنها.

داده‌های موقعیت مکانی و دستگاه. اطلاعاتی در مورد موقعیت جغرافیایی کاربران و دستگاه‌هایی که برای دسترسی به پلتفرم‌های رسانه‌های اجتماعی استفاده می‌کنند، از جمله آدرس‌های آی.پی، شناسه‌های دستگاه و جزئیات مرورگر.

داده‌هایی در مورد رفتار و ترجیحات. اطلاعاتی استنتاج‌شده از فعالیت‌های آنلاین کاربران، مانند علایق، سرگرمی‌ها و ترجیحات آنها بر اساس تعامل با محتوا، سابقه مرور و تعامل با تبلیغات.

–اطلاعات تجاری، از جمله سوابق دارایی شخصی، محصولات یا خدماتی که خریداری، اخذ یا مورد توجه قرار گرفته‌اند، یا سایر تاریخچه‌ها یا گرایش‌های خرید یا مصرف.

-اطلاعات بیومتریک.

–اطلاعات فعالیت اینترنتی یا شبکه الکترونیکی دیگر، از جمله اما نه محدود به تاریخچه مرور، تاریخچه جستجو و اطلاعات مربوط به تعامل مصرف‌کننده با یک وب‌سایت، اپلیکیشن یا تبلیغات اینترنتی.

فراداده. داده‌های اضافی تولیدشده از طریق فعالیت کاربر، مانند برچسب‌های زمانی، جزئیات دستگاه و نرم‌افزار و سایر اطلاعات فنی.

اطلاعات شخصی حساس به معنای اطلاعات راجع به وضعیت زندگی جنسی، اعتقادات (اعم از فلسفی ، مذهبی و سیاسی) عضویت در احزاب یا تشکل‌های صنفی و وضعیت نژادی ، قومی قبیله‌ای افراد» تعریف شده است.

«حریم اطلاعاتی» حریم خصوصی ارتباطات در پلتفرم‌های رسانه‌های اجتماعی و برنامه‌های پیام‌رسان به معنای محافظت از مکالمات خصوصی، پیام‌ها و اطلاعات شخصی کاربران در برابر دسترسی، شنود یا نظارت غیرمجاز و ممنوعیت تجسس و استراق سمع و بصر در تعاملات ارتباطی آنها است.

«حریم کلان‌داده‌های رسانه‌های اجتماعی» را می‌توان به‌معنای حق افراد برای کنترل جمع‌آوری، پردازش، ذخیره، استفاده، به اشتراک‌گذاری و افشای داده‌های شخصی کاربران توسط پلتفرم‌های رسانه‌های اجتماعی تعریف کرد.

«حریم خصوصی ارتباطات در پلتفرم‌های شبکه‌های اجتماعی»، توانایی کاربران برای اشتراک‌گذاری ایمن، محرمانه و کنترل‌شده اطلاعات شخصی و پیام‌ها است، با این اطمینان که تعاملات و محتوای آن‌ها در برابر دسترسی، استفاده یا افشاء و پردازش غیرمجاز محافظت می‌شود.

«پردازش» به معنای هرگونه عملیات یا مجموعه عملیاتی است که بر روی اطلاعات شخصی یا مجموعه‌هایی از اطلاعات شخصی انجام می‌شود–شامل گردآوری، ثبت، سازماندهی، ساختاردهی، ذخیره‌سازی، تطبیق یا تغییر، بازیابی، مشورت،

استفاده، افشا از طریق انتقال، انتشار یا در دسترس قرار دادن به هر طریق دیگر، هم‌راستا سازی یا ترکیب، محدودسازی، پاک کردن یا نابودی–صرف نظر از اینکه این عملیات به صورت خودکار انجام شود یا نشود.

«رضایت کاربر» شامل دادن اجازه برای انجام پردازش داده‌های شخصی به شکل خودخواسته و با آگاهی کامل و بدون اجبار از طریق یک اقدام تأییدکننده صریح است.

«نقض داده‌های شخصی» به معنای نقض امنیتی است که منجر به نابودی، فقدان، تغییر، افشای غیرمجاز، یا دسترسی به داده‌های شخصی منتقل‌شده، ذخیره‌شده یا به نحو دیگری پردازش‌شده، به صورت اتفاقی یا غیرقانونی می‌شود.

«نقض حریم اطلاعات» در پلتفرم‌های اجتماعی به معنای دسترسی غیرقانونی و تجسس و استراق سمع و بصر فاقد مجوز و نیز آسیب‌پذیری ایمنی، هک و حملات سایبری در ارتباط شخصی افراد در رسانه‌های اجتماعی و پیام‌رسان‌ها است که به خدشه در محرمانگی ارتباط منجر می‌شود.

اصول پردازش داده‌های شخصی و حریم اطلاعات

ماده ۷) اصول پردازش داده‌های شخصی در پلتفرم‌های دیجیتال به شرح ذیل است:

۱. همه پلتفرم‌های ایرانی موظف هستند تا یک سند جامع حفاظت از داده‌های شخصی به نام سیاست حریم خصوصی را تدوین و به هنگام ثبت نام کاربران، آنها ترغیب کنند تا آنرا مطالعه نمایند و اینکه این سند باید به راحتی در دسترسی عموم قرار گیرد. این سند باید شامل این موارد باشد: انواع داده‌هایی که از کاربران گردآوری می‌شود، نحوه استفاده از داده‌های شخصی، نحوه و مقصود از پردازش داده‌های شخصی که باید مبتنی بر رضایت و عدم دارنده اطلاعات شخصی باشد، و نحوه اشتراک‌گذاری داده‌های ناشناس‌شده و تقلیل‌یافته با طرف‌های سوم باشد.

۲. پلتفرم‌ها به‌هیچ‌وجه مجاز نیستند، اطلاعات شخصی را به طرف‌های ثالث اعم از دولت و سازمانهای دولتی و شرکت‌های تجاری بفروشند.

۳. پلتفرم‌ها باید در مورد اطلاعات گردآوری شده شفاف‌سازی کنند و در مورد اینکه چه داده‌ّایی را و چرا گردآوری می‌کنند به طور شفاف به کاربران خود اطلاع‌رسانی کنند.

۴. پلتفرم‌ها باید کنترل کاربران بر اطلاعات شخصی خود را تسهیل کنند. ازجمله اینکه از طریق تنظیمات حریم خصوصی آنها میزان دسترسی دیگران به اطلاعات شخصی‌شان را کنترل کنند و هرزمان بخواهند بتوانند اطلاعات شخصی خود را محدود و یا حتی آنها را حذف کنند.

۵. پلتفرم‌ها مکلف هستند تا هنگام هر نوع پردازش مبتنی بر کسب رضایت، داده‌های کاربران را تقلیل بدهند تا دارنده اطلاعات شخصی شناسایی‌پذیر نباشد.

۶. پلتفرم‌های رسانه‌های اجتماعی، پیام‌رسان‌های اجتماعی و برنامهّای کاربردی دیگر از جمله پلتفرم‌های خدماتی موظف هستند تا برای هر نوع از دسترسی به اطلاعات شخصی کاربران در رایانه‌های شخصی، رایانک‌ها و تلفن‌های همراه هوشمند، نسبت به امکان دسترسی و سطح دسترسی به فهرست تماس‌ها، فعال‌سازی میکروفن، دوربین تصویربرداری و عکس‌برداری، هر نوع محتوای ذخیره شده ازجمله تصاویر گالری و نیز پیام‌های صوتی ضبط شده از کاربران اجازه بگیرند.

۷. طراحی و توسعه پلتفرم‌ها باید مبتنی بر حفظ حریم خصوصی بر اساس طراحی- که بر ادغام اقدامات حفاظت از داده و حفظ حریم خصوصی در طراحی، توسعه، و استقرار محصولات، خدمات و فرآیندها تأکید دارد-و حفظ حریم خصوصی به شکل پیش‌فرض- که بر اساس آن محصولات، خدمات و فرآیندها باید با بالاترین تنظیمات حریم خصوصی که به‌طور پیش‌فرض فعال شده است، طراحی شوند و به کاربران اجازه دهند تنظیمات برگزیده خود را در صورت نیاز تنظیم کنند- انجام شود.

۸. پلتفرم‌ها باید به شکل دائم تلاش نمایند فناوری‌های حفاظت و ایمنی داده‌های شخصی را ارتقاء دهند.

۹. پلتفرم‌ها باید قوانین و مقررات بالادستی مرتبط با حریم خصوصی، حریم داده و حریم ارتباط را در اسناد و سازوکارهای مواجهه با پردازش داده‌های شخصی رعایت کنند.

۱۰. پلتفرم‌ها به‌هیچ‌وجه مجاز نیستند داده‌های شخصی مربوط به کاربران کودک را پردازش کنند، حتی اگر برخلاف محدودیت عضویت افراد زیر ۱۳ سال کاربر پلتفرم شده باشند.

ماده ۸) اصول حفظ حریم ارتباطات در پلتفرم‌های دیجیتال و پیام‌رسان‌ها به شرح ذیل است:

۱. پیام‌رسانی امن یعنی اجرای رمزنگاری سرتاسری یا سایر اقدامات امنیتی برای اطمینان از اینکه پیام‌های رد و بدل شده بین کاربران قابل دسترسی، رهگیری یا دستکاری توسط طرف‌های غیرمجاز، از جمله خود ارائه‌دهندگان پلتفرم، نباشد یک الزام است.

۲. خصوصی بودن مکالمات در پیام‌رسان‌های اجتماعی یک الزام است و باید گزینه‌هایی برای کاربران برای شرکت در مکالمات خصوصی یا گروه‌های بسته که بدون رضایت صریح یا دعوت، برای سایر کاربران پلتفرم قابل مشاهده نیستند، ایجاد شود.

۳. کاربران باید امکان کنترل محتوا را داشته باشند تا بتوانند انتخاب کنند و کنترل کنند چه کسی یا کسانی می‌توانند محتوای مرتبط با آن‌ها را ببینند، به اشتراک بگذارند یا با آن تعامل داشته باشند.

۴. ناشناسی و استفاده از نام مستعار یک الزام است و پلتفرم‌ها باید امکان این موضوع را فراهم کنند تا کاربران انتخاب کنند از نام واقعی در حین شرکت در گفتگوها یا تعاملات برخط استفاده کنند و یا اینکه ناشناس بمانند و یا از نام استعار استفاده کنند.

۵. به طور کلی ضبط، ذخیره یا انواع دیگر رهگیری ازجمله تجسس در ارتباطات خصوصی افراد در پلتفرم‌ها و پیام‌رسان‌ها بدون رضایت آنها مجاز نیست و صرفاً بر مبنای مصالح عمومی ازجمله موضوع امنیت ملی و با حکم قانونی به شکل موردی، و بدون افشای سایر اطلاعات فردی، تداخل در حریم ارتباطات را امکان‌پذیر می‌کند.

حقوق کاربران

ماده ۸) کاربران پلتفرم‌های رسانه‌های اجتماعی دارای حقوق مختلف مرتبط با حریم خصوصی هستند که مهمترین آنها عبارتند از:

۱. حق اطلاع: کاربران حق دارند از نحوه جمع آوری، ذخیره، استفاده و اشتراک گذاری داده های شخصی آنها توسط پلتفرم مطلع شوند. این اطلاعات باید به شیوه‌ای روشن و شفاف، از طریق سیاست حفظ حریم خصوصی یا شرایط خدمات ارائه شود.

۲. حق دسترسی: کاربران حق دارند به اطلاعات شخصی خود که توسط پلتفرم نگهداری می‌شود دسترسی داشته باشند و در صورت درخواست یک نسخه از این داده‌ها دریافت کنند.

۳. حق تصحیح: کاربران حق دارند اطلاعات شخصی خود را در صورت نادرست یا ناقص بودن، تصحیح، به‌روزرسانی یا اصلاح کنند.

۴. حق پاک کردن (حق فراموش شدن): کاربران این حق را دارند که تحت شرایط خاص، مانند زمانی که داده‌ها دیگر برای هدفی که جمع آوری شده‌اند ضروری نیست، درخواست پاک کردن یا حذف داده‌های شخصی خود را داشته باشند.

۵. حق محدود کردن پردازش: کاربران حق دارند پردازش داده‌های شخصی خود را تحت شرایط خاصی محدود کنند، مانند زمانی که صحت داده‌ها مورد اعتراض قرار می‌گیرد یا زمانی که پردازش غیرقانونی تلقی می‌شود.

۶. حق انتقال داده‌ها: کاربران حق دارند داده‌های شخصی خود را بین پلتفرم‌ها یا خدمات مختلف در قالبی که معمولاً مورد استفاده قرار می‌گیرد و قابل خواندن توسط ماشین است، منتقل کنند.

۷. حق اعتراض: کاربران حق دارند نسبت به پردازش داده‌های شخصی خود برای اهداف بازاریابی مستقیم یا سایر اهداف مبتنی بر منافع مشروع اعتراض کنند.

۸. حق لغو رضایت: کاربران حق دارند رضایت خود را برای جمع‌آوری، استفاده یا به‌اشتراک‌گذاری داده‌های شخصی خود در هر زمان پس بگیرند.

۹. حق طرح شکایت: کاربران حق دارند در صورتی که معتقدند حقوق حریم خصوصی آنها نقض شده است، شکایت خود را به مرجع حفاظت از داده‌ها–مرکز کلی فضای مجازی–ارسال کنند.

نهاد مسئول اجرای قانون

ماده ۹) کمیسیون حفاظت از داده‌های شخصی که در مرکز ملی فضای مجازی تشکیل می‌شود، مسئول برنامه‌ریزی و هماهنگی کلی حفاظت از داده‌های شخصی کاربران خواهد بود. اعضای این کمیسیون و شرح وظایف آن توسط شورای عالی فضای مجازی تعیین و تصویب می‌شود. محافظت از حریم خصوصی کاربران ایرانی در پلتفرم‌های ایرانی و غیرایرانی، افزایش آگاهی کاربران از حریم داده و ارتباطات، آگاهانیدن و ملزم کردن پلتفرم‌ها نسبت به اجرای تعهدات خود درباره حریم

خصوصی کاربران و اعمال قانون علیه پلتفرم‌هایی که مفاد این قانون را نقض می‌کنند و نیز رسیدگی به شکایت‌های کاربران از پلتفرمها وظیفه این کمیسیون است.

ماده ۱۰. این قانون پس از تصویب در مجلس شورای اسلامی و تأیید شورای نگهبان قانونی اساسی لازم‌الاجرا خواهد بود.

منابع

احمدلو، مونا. (۱۴۰۰). حریم خصوصی در فقه و قانون ایران. تهران: مجمع علمی و فرهنگی مجد.

اسماعیلی، محسن. (۱۴۰۰). حقوق آزادی اطلاعات در ایران (جلد اول). شرح و تفسیر کاربردی «قانون دسترسی و انتشار آزاد اطلاعات». تهران: پژوهشگاه فرهنگ، هنر و ارتباطات.

اسماعیلی، مهدیه. (۱۴۰۲). بیانیه سازمان فناوری اطلاعات در خصوص پیام‌رسان بله : حریم خصوصی کاربران نقض نشده است!. ماهنامه پیوست. قابل دسترسی در: https://digiato.com/iran-technology-news/information-technology-organization-statement

امام خمینی (۱۳۶۱ (۱۴۰۳)). حکم انحلال هیأت‌های گزینش در سراسر کشور، و تأسیس هیأت‌های دارای صلاحیت

امام خمینی (۱۳۶۱). فرمان هشت ماده ای امام خمینی (س) درباره حقوق مردم. قابل دسترسی در پرتال امام خمینی: http://www.imam-khomeini.ir/fa/n25179

انصاری، باقر. (۱۳۹۷). حق دسترسی به اطلاعات: آزادی اطلاعات. تهران: دفتر مطالعات و برنامه‌ریزی رسانه‌ها.

آستانه، مجتبی (۱۴۰۲). هک اسنپ‌فود و افشای اطلاعات کاربران؛ اسنپ‌فود بیانیه داد: مسئولیت این اتفاق را می‌پذیریم. وب‌سایت دیجیاتو. قابل دسترسی در: https://digiato.com/iran-technology-news/snapfood-issued-statement-hacking-platform

آقابابایی، حسین. (۱۳۹۷). حریم خصوصی در حقوق کیفری اسلام. تهران: انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.

آقامیری، سیدمحمد امین (۱۴۰۲). میزان پیشرفت شبکه ملی اطلاعات به ۵۹,۱۸ درصد رسید/ ۷ هدف از ۳۰ هدف پیشرفت ضعیفی داشته اند. سایت مرکز ملی فضای مجازی. قابل دسترسی در https://www.majazi.ir/news/100711 :

آیت‌الله خامنه‌ای (۱۴۰۰) سخنرانی نوروزی خطاب به ملت ایران، در تاریخ ۱۴۰۰//۱/۱. قابل دسترسی در : https://farsi.khamenei.ir/newspart-print?tid=2558&npt=12

آیت‌الله خامنه‌ای. (۱۳۹۴). حکم انتصاب اعضای شورای عالی فضای مجازی. قابل دسترسی در:

https://farsi.khamenei.ir/message-content?id=30658

آیت‌الله خامنه‌ای. (۱۴۰۲). حکم تجسس در امور خصوصی دیگران. پایگاه اطلاع‌رسانی دفتر مقام معظم رهبری. قابل دسترسی در:

https://www.leader.ir/fa/content/26514

پایگاه اطلاع رسانی قوانین و مقررات کشور. (۱۴۰۳). قانون برنامه پنج‌ساله هفتم پیشرفت جمهوری اسلامی ایران (۱۴۰۳-۱۴۰۷). پایگاه اطلاع رسانی قوانین و مقررات کشور. قابل دسترسی در:

https://media.dotic.ir/uploads/org/2024/07/06/172026885583043000.pdf

تقی‌پوریان، علی؛ نیک‌بین، جواد و اسماعیلی، مهدی. (۱۴۰۰). ماهیت و آثار رضایت زیان‌دیده در فقه امامیه و حقوق ایران. فصلنامه پژوهش‌های فقه و حقوق اسلامی. سال هفدهم. شماره شصت و چهار. صص. ۴۱-۵۴

حسنی، حسین. (۱۴۰۱). چالش‌های نوظهور دولت‌ها برای حکمرانی فضای سایبر پیامدهای پلتفرمی‌شدن و پیدایش متاورس. علوم سیاسی۲۵،(شماره ۹۸ – تابستان ۱۴۰۱), ۱۶۱-۱۸۴.doi: 10.22081/psq.2022.73424 .

حکم انحلال هیأت‌های گزینش در سراسر کشور و تأسیس هیأت‌های دارای صلاحیت. صحیفه امام. تهران: مؤسسه تنظیم و نشر آثار امام خمینی (س). قابل دسترسی در پرتال امام خمینی: http://www.imam-khomeini.ir/fa/C207_43915

خاکی، مینو، محقق داماد، سید مصطفی و درگاهی، مهدی. (۱۴۰۲). مبانی قرآنی و قواعد مشروعیت نظارت دستگاه‌های دولتی بر حریم خصوصی. فصلنامه مطالعات قرآنی. دوره ۱۴. شماره ۵۴. صص. ۱۸۹-۲۰۱۸.

دانش پور، افتخار. (۱۳۹۵). بررسی حدود مصلحت در حریم خصوصی در تعارض با مصالح اجتماعی با رویکردی بر مبانی فقه اسلامی. دوفصلنامه فقه مقارن، ۴(۸)، ۱۵-۴۵.

دانش‌پور، افتخار (۱۳۹۵). بررسی حدود مصلحت فردی در حریم خصوصی در تعارض با مصالح اجتماعی با رویکردی بر مبانی فقه اسلامی. دوفصلنامه علمی-پژوهشی فقه مقارن. سال چهارم. شماره ۸. صص. ۱۵-۴۵.

دانشنامه ویکی‌فقه. (۱۴۰۳). حریم خصوصی از منظر حقوقی. دانشنامه ویکی‌فقه. قابل دسترسی در: https://fa.wikifeqh.ir

رجایی، غلامعلی، و فکری، محمد. (۱۳۹۰). حریم خصوصی شهروندان در اندیشه امام خمینی(س) با تأکید بر فرمان هشت ماده‌ای. پژوهشنامه متین، ۱۳(۵۲)، ۸۱-۱۰۱.

سروش، محمد. (۱۳۹۸). مبانی حریم خصوصی (براساس منابع اسلامی). تهران. سمت.

فاطمی، مهدی، نوایی، علی اکبر، و عبدالهی نژاد، عبدالکریم. (۱۴۰۱). محدوده ورود حاکم اسلامی در حریم شخصی افراد از نظر فقهی. ماهنامه جامعه شناسی سیاسی ایران، ۵(۱۱)، ۶۳۸۸-۶۴۰۱. doi: 10.30510/psi.2022.345147.3528

فکری، محمد. (۱۳۹۷). حریم خصوصی شهروندان در اندیشه امام خمینی (ره)-بخش نخست. قابل دسترسی در: http://pajoohe.ir

فن دایک، یوزه (۱۴۰۲). فرهنگ اتصال: تاریخ انتقادی رسانه‌های اجتماعی. (مترجم: حسین حسنی). تهران: سوره مهر.

فیروزآبادی، سیدابوالحسن (۱۳۹۹). درآمدی بر حکمرانی فضای مجازی، تهران: دانشگاه امام صادق.

کربلایی، یگانه. (۱۴۰۱). چرا لایحه حفاظت از داده و حریم خصوصی در ایران به نتیجه نرسید؟ + به‌روزرسانی. ماهنامه پیوست. قابل دسترسی در: https://peivast.com/p/150716

کربلایی، یگانه. (۱۴۰۲). بیانیه «بله» درباره انتشار اطلاعات محتوای چت‌های عمومی+به‌روزرسانی. قابل دسترسی در: https://peivast.com/p/170837

کشتگر، امیر و جاور، حسین. (۱۴۰۰). ساحت‌های تأثیر قاعده فقهی «حفظ نظام» بر حق حریم خصوصی. فصلنامه علمی مطالعات حقوق بشر اسلامی. سال دهم. شماره اول (پیاپی ۲۰). بهار ۱۴۰۰.

گودرزی، فرشید. (۱۴۰۰). مسئولیت مدنی ناشی از نقض حریم خصوصی. تهران: انتشارات مجد.

محبی، جلیل. (۱۳۹۷). قانون اساسی و حرمت شرعی حریم خصوصی مردم. https://farsi.khamenei.ir/others-note?id=39368

محسنیان، سیدعلی. (۱۴۰۰). رسانه‌ها در حریم خصوصی. تهران: لوگوس.

مرکز پژوهش‌های مجلس. (۱۴۰۱). قانون مدیریت داده ها و اطلاعات ملی. قابل دسترسی در: https://rc.majlis.ir/fa/law/show/1753599

مرکز ملی فضای مجازی (۱۳۹۲). طرح کلان و معماری شبکه ملی اطلاعات. مرکز ملی فضای مجازی.

مرکز ملی فضای مجازی (۱۳۹۵). تبیین الزامات شبکه ملی اطلاعات. مرکز ملی فضای مجازی.

مرکز ملی فضای مجازی. (۱۴۰۱). سند راهبردی جمهوری اسلامی ایران در فضای مجازی. قابل دسترسی در: https://dotic.ir/news/12841

مرکز ملی فضای مجازی. (۱۴۰۲). دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی. قابل دسترسی در: https://media.dotic.ir/uploads/org/2024/01/20/170576324339587400.pdf

موسی‌زاده، ابراهیم و مصطفی‌زاده، فهیم (۱۳۹۱). نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی. فصلنامه بررسی‌های حقوق عمومی، سال اول، شماره ۲.

مهریزی، مهدی. (۱۳۷۸). دولت دینی و حریم خصوصی (بازخوانی فرمان هشت ماده‌ای امام خمینی (ره)). حکومت اسلامی. ۱۳۷۸. شماره ۱۲.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3), 66-84.

Boyd, D., & Crawford, K. (2012). Critical questions for big data. Information, Communication & Society, 15(5), 662-679.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. New York: Oxford University Press.

Bradford, A. (2023). Digital Empires: The Global Battle to Regulate Technology. Oxford University Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3 (2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Bucher, T., & Helmond, A. (2017). The affordances of social media platforms. In J. Burgess, T. Poell, & A. Marwick (Eds.), The SAGE handbook of social media (pp. 233-253). Sage Publications.

Carah, N. (2021). Media and Society: Power, Platforms, and Participation. Los Angeles & London: Sage Publications.

Cavoukian, A. (2011). Privacy by design The 7 foundational principles. Retrieved from www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Chander, A., & Le, U. P. (2015). Data nationalism. European Journal of International Law, 25(3), 1-4.

Correia, M., & Rodrigues, L. (2023). Security and privacy. In Multidisciplinary Perspectives on Artificial Intelligence and the Law (pp. 81-101). Springer. https//doi.org/10.1007/978-3-031-41264-6_5

Council of Europe. (2018). Modernised Convention 108. Retrieved from https://www.coe.int/en/web/data-protection/modernised-convention108

Crawford, K., & Gillespie, T. (2016). What is a flag for? Social media reporting tools and the vocabulary of complaint. New Media & Society, 18(3), 410-428. https://doi.org/10.1177/1461444814543163

de Gregorio, G. (2021). Moderation. In L. Belli, N. Zingales, & Y. Curzi (Eds.), Glossary of Platform Law and Policy Terms. FGV Direito Rio. https://platformglossary.info/moderation/.

De Souza, R., & Dick, G. N. (2009). Disclosure of information by children in social networking sites: A cause of concern?. CyberPsychology & Behavior, 12(5), 509-512.

Del Giovane, C., Ferencz, J., & López-González, J. (2023). The Nature, Evolution and Potential Implications of Data Localisation Measures. OECD Trade Policy Papers, 278. OECD Publishing. https://doi.org/10.1787/179f718a-en

DeNardis, L. (2014). The global war for internet governance. Yale University Press.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. Telecommunications Policy, 39(9), 761-770. doi:10.1016/j.telpol.2015.05.007

Devane, H. (2023). Data localization: A complete overview. Immuta Blog. https://www.immuta.com/blog/data-localization/

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook friends: Exploring the relationship between college students' use of online social networks and social capital. Journal of Computer-Mediated Communication, 12(4), 1143-1168.

ERR News. (2021, March 2). Estonia, EU countries propose faster 'European digital sovereignty'. ERR News. Retrieved from https://news.err.ee/1608127618/estonia-eu-countries-propose-faster-european-digital-sovereignty

European Centre for International Political Economy. (2017). Data localization and barriers to the free flow of information: A policy perspective. ECIPE Policy Brief, 06/2017.

European Commission. (2024). Data protection in the EU. What is personal data? https.//commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

European Union. (2020). Digital sovereignty for Europe. European Parliamentary Research Service.

https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

European Union. (2024). Article 8: Protection of personal data. EU Charter of Fundamental Rights. Retrieved from https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data#:~:text=1.,basis%20laid%20down%20by%20law.

Fischer, C. (2022, July 25). How Meta's protecting privacy and integrity. Meta. https://about.fb.com/news/2022/07/how-metas-protecting-privacy-and-integrity/

Fleming, S. (2021, March 15). What is digital sovereignty and why is Europe so interested in it? World Economic Forum. Retrieved from https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/

Flew, T. (2024). The Return of the Regulatory State: Nation-States as Policy Actors in Digital Platform Governance. In: Padovani, C., Wavre, V., Hintz, A., Goggin, G., Iosifidis, P. (eds) Global Communication Governance at the Crossroads. Global Transformations in Media and Communication Research - A Palgrave and IAMCR Series. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-29616-1_10

Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

Google. (2024). Google privacy policy. Google. https//policies.google.com/privacy?hl=en-US

Google. (2024). Privacy progress update. Meta. https//about.meta.com/uk/privacy-progress/

Google. (2024). Our principles. Google Safety Center. https//safety.google/principles/?hl=en_US

Gorwa, R. (2019). What is platform governance? Information, Communication & Society, 22(6), 854-871. doi:10.1080/1369118x.2019.1573913

Government of India. (2018). Report of the committee of experts on data protection framework for India. Ministry of Electronics and Information Technology.

Greenleaf, G. (2014). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108. International Data Privacy Law, 4(3), 163–176.

Gutwirth, S., De Hert, P., & Poullet, Y. (2009). The Right to Privacy and Data Protection. In S. Peers, T. Hervey, J. Kenner, & A. Ward (Eds.), The EU Charter of Fundamental Rights: A Commentary (pp. 235–261). Oxford: Hart Publishing.

Haggart, B. (2020). The new protectionism: How national champions and digital nationalism threaten the global economy. Foreign Affairs, 99(5), 57-66.

Hoffman, A. (2020). Splinternet and internet balkanization. Medium. Retrieved from <https://medium.com/@aaronhoffman/splinternet-and-internet-balkanization-47616d09de4b>

Hufbauer, G. C., & Lu, Y. (2021). The digital trade agenda in US–China strategic competition. Journal of International Economic Law, 24(1), 51–72.

Hufbauer, G. C., & Lu, Y. (2021). The digital trade agenda in US–China strategic competition. Journal of International Economic Law, 24(1), 51–72.

Hurel, L. M., & Lobato, L. C. (2018). Data localization, data flows and their impacts on developing countries. JRC Working Papers in Economics and Finance 2018-09, Joint Research Centre (Seville site), European Commission.

ICANN. (n.d.). About ICANN. Retrieved from <https://www.icann.org/about>

Indeed Editorial Team. (2024, January 10). 9 Software Platforms People Use Every Day. https://www.indeed.com/career-advice/career-development/types-of-software-platforms

Internet Governance Forum. (n.d.). About the IGF. Retrieved from <https://www.intgovforum.org/multilingual/aboutigf>

Internet Governance Forum. (n.d.). About the IGF. Retrieved from <https://www.intgovforum.org/multilingual/aboutigf>

Khanna, P. (2019). The new globalism is about connectivity, not geography. World Economic Forum. Retrieved from <https://www.weforum.org/agenda/2019/12/new-globalism-connectivity-geography-business-parag-khanna/>

Kleinwächter, W. (2004). Internet governance: A starting point for a global discussion. Global Internet Governance Academic Network (GIGANET).

Kommerskollegium. (2020). Data Flows, Digital Protectionism, and International Trade. Copenhagen: Danish Business Authority.

Korff, D. (2018). The General Data Protection Regulation: A Practical Guide. Brussels: European Company Lawyers Association.

Kuner, C. (2015). The European Union and the search for a global data protection standard. German Law Journal, 16(5), 1144–1168.

Kurbalija, J. (2016). An introduction to internet governance. DiploFoundation.

Lee, D. (2015). Privacy and social norms. In B. Roessler & D. Mokrosinska (Eds.), Social dimensions of privacy: Interdisciplinary perspectives (pp. 49-62). Cambridge University Press.

Leerssen, P. (2021). Platform governance. In L. Belli, N. Zingales, & Y. Curzi (Eds.), Glossary of Platform Law and Policy Terms. FGV Direito Rio. https://platformglossary.info/platform-governance/

Malcomson, S. (2016). Splinternet: How geopolitics and commerce are fragmenting the world wide web. OR Books.

Marsden, C. (2017). Net neutrality: Towards a co-regulatory solution. Bloomsbury Publishing.

Meta Transparency Center (2023). How Meta enforces its policies. Meta. https://transparency.meta.com/en-gb/enforcement/

Meta. (2023). Privacy at Meta. Meta. Retrieved from https://www.meta.com/company/privacy/

Mik-Meyer, N. (2020). Multimethod qualitative research. In S. Salmons, S. H. McNamee & S. Sharma (Eds.), Qualitative Research (5th ed., pp. 357-374). SAGE.

Montgomery, K. C., & Chester, J. (2009). Interactive food and beverage marketing: Targeting children and youth in the digital age. Journal of Adolescent Health, 45(3), S18-S29.

Mueller, M. (2010). Networks and states: The global politics of internet governance. MIT Press.

Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization, and cyberspace. John Wiley & Sons.

Mueller, M. (2018). Sovereignty and cyberspace: Institutions and Internet governance. Retrieved from https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10410/5th-Ostrom-lecture-DLC.pdf?sequence=1&isAllowed=y (Original work presented as the 5th Annual Vincent and Elinor Ostrom Memorial Lecture at the University of Indiana, October 3rd, 2018).

Mueller, R., Schrittwieser, S., Fruehwirt, P., & Kieseberg, P. (2015, June). Security and privacy of smartphone messaging applications. International Journal of Pervasive Computing and Communications, 11(2), 132-150.

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford Law Books.

OECD. (2013). OECD Privacy Framework. Retrieved from https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-framework.pdf

Oostveen, M. (2016, February 23). Why privacy ≠ data protection (and how they overlap). Alexander von Humboldt Institute for Internet and Society. https://www.hiig.de/en/why-privacy-%E2%89%A0-data-protection-and-how-they-overlap/

Paddy Leerssen (17/12/2021). Governance. In Belli, L.; Zingales, N. & Curzi, Y. (Eds.), Glossary of Platform Law and Policy Terms (online). FGV Direito Rio. https://platformglossary.info/governance/.

Papacharissi, Z. (2009). The virtual sphere: The internet as a public sphere. New Media & Society, 11(1-2), 9-27.

Pichai, S. (2021). We keep your personal online data private, safe, and secure. Google Safety Center. https//safety.google/security-privacy/

Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Protti, M. (2022, May 26). Here's what you need to know about our updated privacy policy and terms of service. Meta. https://about.fb.com/news/2022/05/metas-updated-privacy-policy/

Protti, M. (2024, January 25). Investing in Privacy. Meta. https://about.fb.com/news/2024/01/investing-in-privacy/updated-privacy-policy/

Pujalt, C. (2024, May 2). The imperative of encryption: Ensuring privacy in two-way communications. EMCI Wireless Blog. https://www.emciwireless.com/our-blog/encryption-privacy-in-two-way-communications/

Radu, R. (2019). Negotiating internet governance. Oxford University Press.

Sheldon, R., Loshin, P., & Cobb, M. (2024). Encryption. Retrieved from https//www.techtarget.com/searchsecurity/definition/encryption

Sindhayach, R. (2023, March 27). Data protection in the age of social media: User privacy and regulations. Medium. https://medium.com/@rupasindhayach/data-protection-in-the-age-of-social-media-user-privacy-and-regulations

Smith, M., Szongott, C., Henne, B., & von Voigt, G. (2012). Big data privacy issues in public social media. In 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST) (pp. 1-6). IEEE. https://doi.org/10.1109/DEST.2012.6227909

Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880-1903.

Soltani, A. (2024). California Privacy Protection Agency: 2024-2027 Strategic Plan. California Privacy Protection Agency. www.cppa.ca.gov. Available at: https://cppa.ca.gov/pdf/strategic_plan_2024_2027.pdf

Sujon, Z. (2021). The Social Media Age. Los Angeles and London: Sage.

Sundararajan, A. (2016). The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism. MIT Press.

Treem, J. W., van Zoonen, W., & Sivunen, A. (2023). Social Media Affordances and Privacy. In The Routledge handbook of privacy and social media. Trepte, S., & Masur, P. K. (Eds.). London & New York: Routledge.

Trepte, S. (2021). The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances. Communication Theory, 31(4), 549-570. https://doi.org/10.1093/ct/qtz035

Trepte, S., & Masur, P. K. (2023).Definitions of Privacy. In The Routledge handbook of privacy and social media. Trepte, S., & Masur, P. K. (Eds.). London & New York: Routledge.

United Nations. (1948). Universal Declaration of Human Rights. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (1966). International Covenant on Civil and Political Rights. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Véliz, C. (2022). The Ethics of Privacy and Surveillance. Oxford, UK: Oxford University Press.

Véliz, C. (2024). The ethics of privacy and surveillance. Oxford University Press.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide. Cham: Springer International Publishing.
Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide. Cham: Springer International Publishing.
Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide. Cham: Springer International Publishing.
Weippl, E., & Schrittwieser, S. (2023). Introduction to security and privacy. In Introduction to Digital Humanism (pp. 397-414). Springer. https//doi.org/10.1007/978-3-031-45304-5_26
WSIS. (n.d.). About the Summit. Retrieved from https://www.itu.int/net/wsis/about/summit
Wu, E. (2021). Sovereignty and data localization. The Cyber Project, Belfer Center for Science and International Affairs, Harvard Kennedy School.
X Help Center. (2024). Additional information about data processing. X. https://help.x.com/en/rules-and-policies/data-processing-legal-bases
X. (2023). X Terms of Service. X. https://x.com/en/tos
Yoffie, D. B., & Fisher, D. (2019). Fixing Facebook: Fake news, privacy, and platform governance. Harvard Business School Case 720-400, October 2019. (Revised January 2020).