مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی

صد و بیست و هفتم

مروری انتقادی بر مقررات عمومی حفاظت از داده اتحادیه اروپا

A critical review of the EU General Data Protection Regulation

بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۱۲۷

فروردین ۱۴۰۲

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

مروری انتقادی بر مقررات عمومی حفاظت از داده اتحادیه اروپا

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه‌شده در: پژوهشگاه فضای مجازی- گروه مطالعات حقوقی و مقرراتی فضای مجازی

تهیه‌کننده:
امیرعباس رکنی (دانشجوی دکتری امنیت ملی دانشگاه عالی دفاع ملی)

ناظر علمی:
سید امین پیشنماز (دانشجوی دکتری حقوق خصوصی دانشگاه شهید بهشتی)

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰،
کدپستی ۱۵۱۵۶۷۴۳۱۱
شماره تماس: ۸۶۱۲۱۰۶۱
http://www.majazi.ir

فهرست

بخش ششم

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سیدابوالحسن فیروزآبادی

دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

مقـررات عمومـی حفاظـت از داده‌هـای اتحادیـه اروپـا (GDPR) یکـی از سـخت‌گیرانه‌ترین قوانیـن ناظـر بـر حریـم خصوصـی داده و یـک الگـوی بین‌المللـی اسـت. (GDPR) به‌منظـور نظام‌منـد کـردن فراینـد جمـع‌آوری و پـردازش داده توسـط پلتفرم‌هـای آنلایـن، شناسـایی حـق بنیادیـن حفاظـت از داده و حقوق منبعـث از آن، موردحفاظـت از محرمانگی همـه اشـخاص و قانون‌منـد سـاختن شـرایط خـروج داده از اتحادیـه اروپـا و منطقـه اقتصـادی اروپـا و درعین‌حـال، جابه‌جایـی آزاد داده‌هـا، گـردش سـریع و آزادانـه اطلاعـات و مهم‌تـر از همـه، شکسـت انحصـار و تسـلط غول‌هـای فنـاوری بـر داده‌هـای شـخصی کاربـران و سوءاسـتفاده از آن به‌منظـور توسـعه صنعـت تبلیغـات نگاشـته شـد. ایـن شـرکت‌ها ماهیـت و چهـره حریـم خصوصـی را تغییـر داده‌انـد و بسـیاری از کاربـران از میـزان، نـوع و نحـوه جمـع‌آوری داده‌هـای شـخصی توسـط پلتفرم‌هـای آنلایـن خیلـی بـزرگ (VLOP) همچـون گـوگل و فیس‌بـوک بی‌اطـلاع هسـتند و ایـن شـرکت‌ها بـدون ارائـه توضیحـات واضـح و مشـخص، اقـدام بـه سوءاسـتفاده از بی‌اطلاعـی کاربـران و سـاخت مناطـق تاریـک در صنعـت فنـاوری می‌کننـد. (GDPR) به‌منظـور تابانـدن نورافکـن شـفافیت بـر

دستورالعمل‌های جمع‌آوری داده توسط شرکت‌ها و پلتفرم‌ها و به رسمیت شناسی حقوق اساسی دیجیتال کاربران در ۱۴ آوریل ۲۰۱۶ توسط پارلمان اروپا تصویب و از تاریخ ۲۵ مه ۲۰۱۸ به شکل رسمی لازم‌الاجرا شد. باوجوداین، پس از گذشت چهار سال از اجرایی شدن این قانون به نظر می‌رسد که مقررات عمومی حفاظت از داده نتوانسته است به شکلی کامل و درست اهداف خود را محقق سازد. افزایش بروکراسی در شرکت‌ها، پیرابندهای رضایت کاربر خسته‌کننده، تورم قضایی و انباشت پرونده‌ها در هیئت‌های حفاظت از داده‌های شخصی و عدم توازن میان کشورهای عضو در اجرایی ساختن مقررات (GDPR) ازجمله مهم‌ترین معضلات شناخته‌شده در بازه زمانی اجرایی شدن این قانون است. به همین دلیل، اتحادیه اروپا در حال بازنگری در برخی از ساختارها و ایجاد یک بسته خدمات دیجیتال نوین متناسب با نظام حکمرانی سایبری اروپایی است. در نوشتار پیش رو، ضمن انجام مروری بر مقررات عمومی حفاظت از داده، به بررسی چالش‌های ناشی از اجرای آن و مسیر پیش روی اتحادیه اروپا با توجه به تجربیات ناشی از اجرای (GDPR) خواهیم پرداخت.

واژگان کلیدی

مقررات عمومی حفاظت از داده، اتحادیه اروپا، پارلمان اروپا، حریم خصوصی.

مقدمه

مقدمه

مقـررات عمومـی حفاظـت از داده‌هـای اتحادیـه اروپـا (GDPR) در سـال ۲۰۱۶ توسـط پارلمـان اروپـا و شـورای اتحادیـه اروپـا بـه تصویـب رسـید و به‌طـور رسـمی در مـاه مـه ۲۰۱۸ اجرایـی شـد تـا بـر اسـتفاده از داده‌هـای شـخصی شـهروندان توسـط شـرکت‌های اتحادیـه اروپـا و خـارج از آن‌کـه داده‌هـای شـهروندان اتحادیـه اروپـا را جمـع‌آوری، پـردازش و ذخیـره می‌کننـد، نظـارت کنـد. بـرای بسـیاری در اتحادیـه اروپـا، تصویـب مقـررات عمومـی حفاظـت از داده یک‌لحظـه تاریخـی بـود. در زمـان اجـرا، معـاون سـابق کمیسـیون اروپـا، ویویـن ردینـگ[1] ، خاطرنشـان کـرد کـه اصلاحـات امـروز اعتمـاد بـه خدمـات دیجیتـال را احیـا و ماشـین رشـد صنعـت در فـردا را دوبـاره روشـن می‌کنـد.» باوجـود سـتایش ایـن قانـون به‌عنـوان یکـی از بزرگ‌تریـن دسـتاوردهای اتحادیـه اروپـا، ذی‌نفعـان نسـبت بـه اجـرای آن ابـراز تردیـد می‌کننـد. در میـان کسـب‌وکارها، بـا توجـه بـه ابهامـات موجـود در ایـن قانـون و همچنیـن تـرس از هزینه‌هـای مرتبـط، سـردرگمی در مـورد نحـوه اجـرا و التـزام بـه آن وجـود دارد. در سـال ۲۰۱۸، نظرسـنجی[2] PwC نشـان داد کـه شـرکت‌ها بیـش از ۱,۳ میلیـون

1. Viviane Reding

۲. پرایـس واتـر هـاوس کوپـر (PricewaterhouseCoopers) شـرکت چندملیتـی خدمـات حرفـه‌ای بریتانیایـی اسـت کـه در زمینـه ارائـه خدمـات مشـاوره مدیریـت، مشـاوره مالـی و سـرمایه‌گذاری، مشـاوره حقوقـی و مالیاتـی، بیمه‌سـنجی، خدمـات حسـابداری و حسابرسـی فعالیـت می‌کنـد.

یـورو بـرای طرح‌هـای آموزشـی و آمادگـی بـرای اجـرای مقـررات عمومـی حفاظـت از داده پیش‌بینـی کرده‌انـد. حتـی در حـال حاضـر، نگرانی‌هـا در مـورد پیامدهـای منفـی قانـون بـر رشـد و نـوآوری کسـب‌وکارها همچنـان در بسـیاری از شـرکت‌های اروپایـی وجـود دارد. بـرای پیـروی از مقـررات عمومـی حفاظـت از داده، شـرکت‌ها بایـد بـه چندیـن قانـون، ازجملـه الزامـات رضایت‌منـدی، حفـظ حریـم خصوصـی بـر اسـاس طراحـی و اعلان‌هـای نقـض اجبـاری پایبنـد باشـند. ایـن قانـون مجموعـه‌ای از حقوق را بـه کاربـران بـرای دسترسـی و کنتـرل داده‌هایشـان می‌دهـد، ازجملـه حـق قابلیـت انتقـال داده‌هـا و «حـق فراموش‌شـدن». هـر کشـور عضـو باید یـک مرجـع حفاظـت از داده‌هـا[1] (DPA) (چنـد مرجـع حفاظـت از داده‌هـا در مـورد کشـورهای فـدرال، ماننـد آلمـان) منصـوب کنـد کـه مسـئول نظـارت و اجـرای قانـون مقـررات عمومـی حفاظـت از داده اسـت.

سـازمان‌های ناقـض مقـررات عمومـی حفاظـت از داده ممکـن اسـت تـا ۴ درصـد از گـردش مالـی سـالانه یـا تـا ۲۰ میلیـون یـورو جریمـه شـوند. از زمـان لازم‌الاجـرا شـدن، درمجمـوع ۸۳۹ جریمـه صادرشـده اسـت. تنها ۱۶ جریمـه در سـال ۲۰۱۸ صـادر شـد و صرفـاً یکـی از آن‌ها حداقـل ۱۰۰۰۰۰ یـورو بـود. ۳۰۲ جریمـه در سـال ۲۰۲۰ و ۲۶۶ جریمـه در سـال ۲۰۲۱ صادرشـده اسـت. بالاتریـن جریمه‌هـا در سـال ۲۰۲۰ بـرای شـرکت‌های گـوگل (۵۰ میلیـون یـورو)، H&M (۳۵,۳ میلیـون یـورو) و Telecom Italia (۲۷,۸ میلیـون یـورو) در اتحادیـه اروپـا و هتل‌هـای بین‌المللـی ماریـوت[2] (۱۸,۴ میلیـون یـورو) و بریتیـش ایرویـز[3] (۲۰ میلیـون یـورو) در انگلسـتان صـادر شـد. H&M، خرده‌فـروش پوشـاک سـوئدی، اطلاعـات شـخصی کارکنـان خود را بـدون رضایت صریـح زیر نظر داشـته و جمع‌آوری

1. Data Protection Authority
2. Marriott
3. British Airways

می‌کرد و با استفاده از این داده‌ها برای ساخت و تکمیل پرونده‌های کارمندان و سیاست‌گذاری درباره تصمیم‌گیری‌های استخدامی اقدام می‌کرد. علاوه بر پرداخت جریمه، این شرکت مجبور به اقدامات اصلاحی متعددی ازجمله انتصاب یک هماهنگ‌کننده جدید حفاظت از داده‌ها و ارائه طرحی به مرجع حفاظت از داده‌ها در مورد نحوه اجرای مقررات عمومی حفاظت از داده در آینده شد. این شرکت همچنین موظف شده تا به نحو مقتضی به کارکنان آسیب‌دیده غرامت پرداخت کند.

در طول مدت‌زمانی که از اجرایی شدن این مقررات می‌گذرد، نمونه‌های بسیار دیگری وجود دارد که جریمه‌های ناشی از اجرای مقررات عمومی حفاظت از داده منجر به تغییرات مثبت در سیاست‌های شرکت شده است. بر اساس یک آمار، حدود ۱۰۰ جریمه به همراه اقدامات اصلاحی به دلیل «اقدامات فنی و سازمانی ناکافی برای تضمین امنیت اطلاعات» صادر شد. در مقایسه، مجموع جریمه‌ها برای عدم اجرای کافی تعهدات اعلان نقض داده‌ها تنها حدود ۲۰ مورد است که بالاترین جریمه برای سایت Booking.com به مبلغ ۴۷۵۰۰۰ یورو است. بااین‌حال، آمارها حاکی از آن است که تعداد اعلان‌های نقض داده‌ها به شکل روزانه نسبت به قبل از شروع همه‌گیری کرونا افزایش‌یافته است.

به‌طورکلی، چندین کشور عضو در صدور جریمه‌ها فعال‌تر بوده‌اند. اسپانیا با ۲۷۷ جریمه (۲۱۲ مورد از آن در سال ۲۰۲۱ صادرشده است) در صدر است، پس‌ازآن ایتالیا (۸۸)، رومانی (۶۲)، مجارستان (۴۴) و آلمان (۳۲) قرار دارند. درمجموع مبلغ جریمه،

ایتالیا با ۸۴ میلیون یورو پیشتاز است و پس‌ازآن فرانسه (۵۷ میلیون یورو)، آلمان (۴۹ میلیون یورو)، انگلیس (۴۴ میلیون یورو) و اسپانیا (۳۲ میلیون یورو) قرار دارند. لوکزامبورگ اخیراً به این جمع پیوست و بزرگ‌ترین جریمه تا به امروز را برای سایت آمازون (۷۴۶ میلیون یورو) صادر کرد[1] که آمازون قصد درخواست تجدیدنظر در این مورد را دارد (tessian ,۲۰۲۲). این نحوه فعالیت و اعمال جریمه کاملاً در تضاد با عملکرد کمیسیون حفاظت از داده‌های ایرلند[2] (DPC) است که به دلیل کندی کار برای جریمه شرکت‌هایی که تحت صلاحیت خود هستند موردانتقاد قرارگرفته است[3].

مکانیسم سازگاری مقررات عمومی حفاظت از داده (تک‌مرحله‌ای[4]) مستلزم آن است که مقام ناظر در کشور عضوی که شرکتی، تأسیس اصلی خود را در آن اعلام کرده است، در همه موارد مربوط به حریم خصوصی تصمیم‌گیری کند. غول‌های بزرگ فناوری، ازجمله فیس‌بوک، توییتر، گوگل و اپل، ایرلند را مرکز تأسیس اصلی خود اعلام کرده‌اند (به همین دلیل ایرلند، خانه دوم غول‌های فناوری سیلیکون ولی نام‌گرفته است) و کمیسیون حفاظت از داده‌های ایرلند را به‌عنوان مرجع اصلی خود معرفی کرده‌اند. بااین‌حال، کمیسیون حفاظت از داده‌های ایرلند به دلیل منابع و کارکنان ناکافی خود محدودشده و همین امر منجر به تلنبار شدن حجم قابل‌توجهی

1. On July 2021 ,16, the Luxembourg National Commission for Data Protection (CNDP) issued the biggest fine ever for the violation of the GDPR in the amount of 746€ million (888$ million) to Amazon.com Inc.

2. Ireland's Data Protection Commission

۳. کمیسیون حفاظت از داده‌ها (DPC) یک مرجع مستقل ملی در اتحادیه اروپا است که مسئول حمایت از حقوق اساسی افراد به‌منظور حافظت از داده‌های شخصی آن‌ها است. کمیسیون حفاظت از داده‌های ایرلند موظف به نظارت بر انطباق رفتارهای شرکت‌های فناوری مستقر در ایرلند با مقررات عمومی حفاظت از داده‌ها (GDPR) بوده و وظایف و اختیارات مقرر در سایر چارچوب‌های نظارتی مهم ازجمله مقررات حریم خصوصی ایرلند (۲۰۱۱) و دستورالعمل اتحادیه اروپا را نیز بر عهده دارد.

4. one-stop shop

از پرونده‌هـا شـده اسـت(nathantrust,۲۰۲۲). تـا بـه امـروز، تنهـا جریمه‌هـای عمـده آن علیـه توییتـر بـه مبلـغ ۴۵۰۰۰۰ یـورو صادرشـده، بـا توجـه بـه حجـم درآمـد توییتـر، رقـم کمـی اسـت و واتـس‌اپ هـم جریمـه ۲۲۵ میلیـون یورویـی دریافـت کـرده اسـت. کمیسـیون حفاظـت از داده‌هـای ایرلنـد اسـتدلال کـرده اسـت کـه بـا توجـه بـه پیچیدگـی و اندازه جریمه‌هـای احتمالـی، آن‌هـا بایـد زمـان بیشـتری را بـرای شـرکت‌های فنـاوری بـزرگ صـرف کننـد.

بااین‌حـال، ایـن اسـتدلال در میـان سـایر تنظیم‌کننده‌هـای اروپایـی هـم بایـد صـادق باشـد، درحالی‌کـه آن‌هـا بـا سـرعت بسـیار بیشـتری بـه پرونده‌هـای تخلفـات رسـیدگی و اقـدام بـه صـدور رأی می‌کننـد. بـر همیـن اسـاس، نماینـدگان پارلمـان اروپـا در مـاه مـه سـال ۲۰۲۱ بـه قطعنامـه‌ای رأی دادنـد کـه بـه دلیـل عـدم اجـرای مقـررات عمومـی حفاظـت از داده علیـه ایرلنـد اعـلام تخلـف کـرد(euractiv,۲۰۲۱).

دیـوان دادگسـتری اروپـا[1] (CJEU) نیـز اسـتفاده مؤثـر از مکانیسـم تک‌مرحلـه‌ای را پیچیـده کـرده اسـت. به‌طورکلـی، ایـن مکانیسـم همچنـان به‌عنـوان یـک نقطـه اختـلاف در میـان مراجـع حفاظـت از داده‌هـا در نظـر گرفتـه می‌شـود. یوهانـس کاسـپار[2]، کمیسـر حفاظـت از داده هامبـورگ، ادعـا می‌کنـد کـه ایـن امـر منجـر بـه تأخیرهـای طولانـی و اختـلال در ارتباطـات شـده اسـت. باوجوداین انتقـادات، هیئـت حفاظـت از داده‌هـای اروپـا کـه همـکاری بیـن مراجـع حفاظـت از داده‌هـا را ترویـج و بـه آن نظـارت می‌کنـد، در مـورد ایـن مکانیسـم اعـلام کـرده اسـت کـه ۲۵۴ رأی نهایـی وجـود دارد کـه در آن‌هـا بـا موفقیـت از ایـن مکانیسـم استفاده‌شـده اسـت.

1. European Court of Justice
2. Johannes Caspar

یکی دیگر از موانع برای تنظیم‌کننده‌ها، تفاوت و اختلاف بین منابع مالی و امکانات آن‌ها و شرکت‌ها است. درحالی‌که تنظیم‌کننده‌ها منابع محدودی دارند، شرکت‌ها، به‌ویژه شرکت‌های بزرگ، درآمد و نیروی انسانی بسیار بیشتری در اختیاردارند. به‌این‌ترتیب، شرکت‌ها یاد می‌گیرند که می‌توانند از منابع خود برای شناسایی نقاط ضعف در رویه‌های قانونی استفاده کنند و برای کاهش جریمه‌های خود درخواست تجدیدنظر کنند. در ماه مارس، وال‌استریت ژورنال گزارش داد که ۱۵ درخواست تجدیدنظر برای کاهش جریمه در شش ماه گذشته ارائه‌شده است. در یکی از این موارد، دادگاه برلین جریمه صادرشده برای Deutsche Wohnen را رد کرد، زیرا آن‌ها کارمند خاصی را که مسئول این تخلف بود شناسایی نکردند(wsj,۲۰۲۱). از سوی دیگر، مواردی نیز وجود دارد که درخواست‌های تجدیدنظر لغو شده است، مانند پرونده کمیسیون ملی انفورماتیک و آزادی فرانسه[1] علیه شرکت گوگل که در آن هزاران شاکی خصوصی، گوگل را متهم به پردازش اطلاعات خصوصی کاربران جهت شخصی‌سازی تبلیغات کردند(edpb.europa,۲۰۱۹).

باوجود بسیاری از انتقادات، مقررات عمومی حفاظت از داده هنوز در مرحله اولیه خود است و بسیاری از کشورها به نظارت بر پیشرفت آن ادامه خواهند داد، زیرا در مورد چگونگی ایجاد نظام حفاظت از داده خود و اجرای مؤثر قوانین دغدغه‌مند هستند. استرالیا، ژاپن، کره جنوبی، برزیل و چین قبلاً قوانین حفظ از حریم خصوصی داده خود را با الهام از مقررات عمومی حفاظت از داده تنظیم نموده‌اند و البته با اعمال تغییراتی مبتنی بر اصول حاکم بر نظام حکمرانی داده

1. National Commission on Informatics and Liberty

خـود آن را از جهـات مختلـف بومی‌سـازی کرده‌انـد. چهـار سـال بـرای اظهارنظـر در خصـوص چنیـن قانونـی ناکافـی و کوتـاه اسـت، چیزهـای زیـادی بـرای آمـوزش بـه تنظیم‌کننده‌هـا و سیاسـت‌گذاران در مـورد مزیـت ایـن نـوع قوانیـن و همچنیـن موانـع بالقـوه و زمینه‌هـای بهبـود وجـود دارد. اجـرای مقـررات عمومـی حفاظـت از داده به‌تدریـج رویه‌هـای امنیتـی شـرکت‌ها را بهبـود می‌بخشـد و از حریـم خصوصـی کاربـران محافظـت می‌کنـد. احتمـالاً چندیـن سـال طـول خواهـد کشـید تـا هماهنگـی و یـک وحـدت رویـه ایجـاد شـود. بااین‌وجـود، بـه نظـر می‌رسـد کـه اتحادیـه اروپـا در راسـتای عـزم جـدی خـود بـرای تبدیل‌شـدن بـه الگـوی جهانـی تنظیم‌گـری در حـوزه داده، بـه همیـن مقـدار نیـز اکتفـا ننمـوده و بـر اسـاس بررسـی تجربیـات آموختـه از اجرایـی کـردن مقـررات عمومـی حفاظـت از داده، سـعی بـر بهبـود عملکـرد قوانیـن خـود دارد. بـه همیـن منظـور، قانـون جدیـدی بـا عنـوان خدمـات دیجیتـال را آمـاده نمـوده کـه در حـال طـی تشـریفات نهایـی خـود بـرای لازم‌الاجـرا شـدن اسـت.

بـر اسـاس آنچـه گفتـه شـد، در گـزارش پیـش رو پـس از مـروری بـر مقـررات عمومـی حفاظـت از داده‌هـا و بررسـی جدی‌تریـن اشـکالات کارکـردی آن، بـا توجـه بـه اینکـه قانـون خدمـات دیجیتـال به‌شـدت موردتوجـه کارشناسـان قرارگرفتـه و به‌نوعـی آن را برطرف‌کننـده نقض‌هـای مقـررات عمومـی حفاظـت از داده معرفـی می‌کننـد، نسـبت میـان ایـن دو سـند اروپایـی ناظـر بـر حـوزه تنظیم‌گـری داده را بررسـی خواهیـم کـرد.

بخش اول

ضرورت حفاظت از داده‌های شخصی کاربران

بسیاری از کارشناسان بر این باور هستند که اینترنت به مرحله‌ای از توسعه رسیده است که دولت‌ها منابع یا سرعت لازم و کافی برای واکنش به جرائم سایبری را ندارند. از سوی دیگر، کسب‌وکارها نیز انگیزه لازم برای تمرکز بر این موضوع را ندارند. در شرایطی که کاربران نیز دانش کافی برای محافظت از خود و داده‌های شخصی ندارند، چه کسی موظف بر حفاظت از کاربران است؟ نیمی از جمعیت جهان آنلاین هستند و هرروز ردپای دیجیتال بیشتری از خود به‌جای می‌گذارند. حدود ۸۹ درصد از آمریکایی‌ها و ۷۰ درصد از اروپایی‌ها روزانه از اینترنت استفاده می‌کنند و نرخ نفوذ جهانی اینترنت به‌سرعت در حال افزایش است. آمارها نشان می‌دهد که ۱۶ میلیون از خانه‌های آمریکایی‌ها در حال حاضر دارای ۸۳ میلیون دستگاه مجهز به فناوری اینترنت اشیا هستند و انتظار می‌رود این تعداد در سال‌های آینده افزایش یابد. تحقیقات پارکس اسوسیتز[1] نشان می‌دهد که ۳۲ درصد از خانواده‌های آمریکایی حداقل یک دستگاه متصل دارند و ۵۰ درصد نیز قصد خرید یک دستگاه خانه هوشمند را در سال آینده دارند. جان رمزی[2]، مدیر ارشد فناوری

1. Parks Associates
2. John Ramsey

در شرکت امنیت سایبری سکیور وُرک[1] ، استدلال می‌کند که در واقع امروز ما بیش‌ازحد به هم متصل هستیم: «امروزه یک نفر چندین حسگر همراه خود دارد. یک خودروی امروزی دارای ۵۰۰ حس‌گر است، ۶۰۰ حس‌گر در خانه مدرن و ۶۰۰۰ حس‌گر در یک هواپیمای مدرن وجود دارد. همه این چیزها در حال تولید داده هستند.» درحالی‌که استفاده از اینترنت اشیا در چند سال گذشته به‌طور تصاعدی در حال رشد بوده است، مقیاس پذیرش اینترنت اشیا و قابلیت همکاری دستگاه‌ها، محیطی ناامن ایجاد کرده است و کاربران را بیش از هر زمان دیگر در برابر نشت داده‌های شخصی آسیب‌پذیرتر است. با افزایش تعداد کاربران و حجم داده‌ها نقض و نشت داده‌ها هم امری رایج‌تر و شدیدتر شده است. گزارش جهانی ریسک‌های مجمع جهانی اقتصاد در سال ۲۰۱۸ به این نتیجه رسید که حملات سایبری که قبلاً در مقیاس بزرگ و خطرناک در نظر گرفته می‌شدند، امروزه عادی تلقی می‌شوند. هکرها چابک‌تر شده‌اند و تهدیدها پیچیده‌تر می‌شوند. هکرها به‌طور فزاینده‌ای از فناوری پیشرفته مانند یادگیری ماشینی برای انجام حملات برق‌آسا استفاده می‌کنند.

در سال‌های اخیر، مسائل متعددی پیرامون نحوه برخورد شرکت‌ها (در اینجا منظور از شرکت‌ها به معنای عام هر شخص حقوقی است که به مناسبت ارائه یک خدمت اطلاعات کاربران را ذخیره می‌کند) با اطلاعات کاربرانشان به وجود آمده است. داده‌های شخصی به دلایل سیاسی و اقتصادی بدون رضایت کاربران پردازش می‌شوند. IBM تخمین می‌زند که هزینه نقض

1. Secure works

داده‌ها در مقیاس ۵۰ میلیون موضوع حمله سایبری، بیش از ۳۵۰ میلیون دلار در سال است(gizmodo,۲۰۱۸). به گفته مجمع جهانی اقتصاد، حملات سایبری و کلاه‌برداری از داده‌ها محتمل‌ترین خطرات جهانی هستند. یورو بارومتر[1] این نتیجه را تائید می‌کند؛ بیش از نیمی از کاربران اروپایی جرائم سایبری را یک چالش مهم می‌دانند(learngerman.dw,۲۰۲۲). این آمار اگرچه در نقاط مختلف جهان متفاوت است، اما همچنان جزء دغدغه‌های اصلی ملی و بین‌المللی است.

تحقیقات نشان می‌دهد که نگرش کاربران نسبت به امنیت سایبری و ضرورت حفاظت از داده‌های شخصی رشد قابل‌توجهی داشته و امروزه در مقایسه با سال‌های گذشته کاربران بیشتری نگران داده‌های خود هستند. گزارش‌های اخیر حاکی از آن است که عمده‌ترین مسائلی که کاربران را نگران می‌کند، مربوط به ایمنی داده‌های شخصی آن‌هاست. بر اساس گزارش واحد اطلاعات اکونومیست، ۹۳ درصد از کاربران از حفظ حریم خصوصی و امنیت به‌عنوان یکی از دغدغه‌های اصلی خود نام می‌برند(forgerock,۲۰۲۲). یورو بارومتر که به نمایندگی از کمیسیون اروپا نظرسنجی‌های افکار عمومی را انجام می‌دهد، دریافت که ۸۶ درصد از مردم معتقدند که در معرض خطر فزاینده قربانی شدن جرائم سایبری هستند (ec.europa,۲۰۱۹).

مصرف‌کنندگان نیز به دستگاه‌های که داده‌های بیشتری از آن‌ها جمع‌آوری می‌کنند مانند دستگاه‌های مجهز به اینترنت اشیا صرفاً به‌عنوان یک دارایی ارزشمند نگاه نمی‌کنند و با شکل‌گیری یک وضعیت تناقض‌آمیز آن‌ها را به‌عنوان تهدیدی

1. Euro barometer

برای حریم خصوصی خود تلقی می‌کنند. تأمین امنیت دستگاه به چالشی جدی تبدیل‌شده است که فقدان آن ممکن است منجر به نقض حریم خصوصی شود و مصرف‌کنندگان به‌طور فزاینده‌ای از این تهدیدات آگاه می‌شوند. گزارشی از اکونومیست[1] نشان می‌دهد که ۷۵ درصد از دارندگان دستگاه‌های مجهز به اینترنت اشیا ویژگی‌های حریم خصوصی دستگاه را «بسیار مهم» ارزیابی می‌کنند(forgerock,۲۰۲۲). بر اساس نظرسنجی دیگری از بیش از ۲۶۰۰ مشتری، ۷۷,۵ درصد نگران دسترسی غیرمجاز به دستگاه‌های خود هستند(telecompaper,۲۰۲۲). در همین حال، گیگیا گزارش می‌دهد که ۷۳ درصد از مصرف‌کنندگان در مورد امنیت دستگاه مجهز به اینترنت اشیا «بسیار نگران» یا «نگران» هستند(internetofbusiness,۲۰۱۷).

با توجه به این توضیحات و قرار گرفتن موضوع امنیت داده در کانون توجه کاربران، کارشناسان و دولت‌مردان، سؤال مهمی که مطرح می‌شود آن است که چه کسی مسئول تأمین امنیت داده‌ها است؟ در بخش بعدی به این پرسش پرداخته خواهد شد.

1. The Economist

بخش دوم

چه کسی مسئول امنیت داده‌هاست؟

امروزه هیچ اتفاق‌نظری در مورد اینکه چه کسی مسئول حفظ حریم خصوصی داده‌ها است وجود ندارد. برخی از کاربران بر این باور هستند که خودشان مسئولیت تأمین امنیت داده‌ها را بر عهده دارند، اما برخی دیگر فکر می‌کنند دولت‌ها یا مشاغلی که به مناسبت‌های گوناگون اقدام به جمع‌آوری داده می‌کنند برای مدیریت این موضوع پیچیده مجهزتر هستند.

بر اساس یافته‌های پی. دابلیو. سی[1]، مصرف‌کنندگان از شرکت‌ها انتظار دارند که از داده‌های آن‌ها به‌طور فعال محافظت کنند. ۹۲ درصد از مصرف‌کنندگان می‌گویند که شرکت‌ها باید در موردحفاظت از داده‌ها فعال باشند، ۸۲ درصد موافق هستند که دولت باید نحوه استفاده شرکت‌ها از داده‌های خصوصی را تنظیم کند و ۷۲ درصد فکر می‌کنند که کسب‌وکارها بهترین تجهیزات را برای محافظت از آن‌ها دارند. طبق گزارش گیگیا، در همین حال، ۶۳ درصد از مردم معتقدند که خود افراد مسئول داده‌های خود هستند و در این خصوص نباید به دولت‌ها و یا شرکت‌ها تکیه کنند، درحالی‌که ۱۹ درصد فکر می‌کنند که مسئولیت بر عهده شرکت‌ها است و

1. PwC

۱۸ درصد معتقدند که دولت‌ها باید در حفاظت از کاربران پیش‌قدم شوند(globenewswire,۲۰۲۲). تحقیقات جی. دی. ام. اِی نتایج متفاوتی را نشان می‌دهد، به‌طوری‌که ۳۸ درصد از پاسخ‌دهندگان می‌گویند مصرف‌کنندگان مسئول داده‌هایشان هستند و ۱۵ درصد از آن‌ها انتظار دارند که دولت‌ها اقدامات لازم را انجام دهند. تنها ۵ درصد معتقدند که کسب‌وکارها و سازمان‌ها باید پاسخگو باشند(dma.org,۲۰۲۲).

اما گزارش جی. دی. ام. اِی نتیجه‌گیری می‌کند که ۳۵ درصد از مردم معتقدند این موضوع نیازمند تلاش مشترک مصرف‌کنندگان، دولت‌ها و شرکت‌ها است[1]. گزارش واحد اطلاعات اکونومیست[2] نشان می‌دهد که ۳۱ درصد از افراد موردبررسی انتظار دارند سازندگان دستگاه و ارائه‌دهندگان خدمات با دولت‌ها همکاری کنند و استانداردهای حفظ حریم خصوصی را رعایت کنند(forgerock,۲۰۲۲).

بررسی آمارهای موجود نشان می‌دهد که بسیاری از کاربران بر این نظر هستند که مسئولیت نهایی امنیت داده‌های خود را بر عهده دارند. بااین‌حال، طبق یک مطالعه، کمتر از نیمی از مردم حتی اقدامات احتیاطی اولیه را به‌صورت آنلاین انجام می‌دهند. حدود ۴۵ درصد نرم‌افزار آنتی‌ویروس را نصب می‌کنند یا بسته موجود خود را ارتقا می‌دهند. ۳۹ درصد کوکی‌ها را که در وب‌سایت‌ها محدود می‌کنند و ۳۵ درصد ایمیل‌ها را تنها در صورتی باز می‌کنند که منبع را بشناسند(europa,۲۰۲۲). وقتی صحبت از امنیت رمز عبور می‌شود، وضعیت فقط اندکی بهبودیافته است. آمار نشان می‌دهد که ۷۰ درصد از افراد از هفت کاراکتر یا کمتر برای ساخت رمز عبور

1. Ibid.
2. Economist

در حساب‌های آنلاین خود استفاده می‌کنند. یورو بارومتر به این نتیجه رسید که ۶۲ درصد از مردم رمز عبور خود را برای حداقل یک سرویس آنلاین در طول ۱۲ ماه گذشته تغییر داده‌اند. بااین‌حال، کاربران با افزایش آگاهی از مخاطراتی که متوجه داده‌های آن‌ها هست شروع به انجام اقدامات احتیاطی بیشتری می‌کنند. برخی از کاربران شروع به اجتناب از به اشتراک‌گذاری اطلاعات خودکرده‌اند از دریافت برخی از خدمات آنلاین به دلیل نگرانی از حریم خصوصی، اجتناب می‌کنند یا قبل از خرید یک دستگاه اینترنت اشیا میزان داده‌ای که توسط دستگاه جمع‌آوری می‌شود را بررسی می‌کنند. یورو بارومتر نشان می‌دهد که ۸۷ درصد از کاربران از افشای اطلاعات شخصی خود به‌صورت آنلاین اجتناب می‌کنند و ۳۹ درصد اطلاعات شخصی خود را در وب‌سایت‌ها کاهش می‌دهند. از هر ۱۰ پاسخ‌دهنده، یک نفر به‌طورکلی از بانکداری آنلاین انصراف داده است. کاربران آنلاین ارزش حریم خصوصی و امنیت داده‌ها را به‌مراتب بیش‌ازپیش درک می‌کنند و همین امر سبب شده است تا در پاسخ به این نگرانی، یک تلاش مشترک در قالب همکاری دولت‌ها، پلتفرم‌ها و کاربران شکل بگیرد.

بخش سوم

مقررات عمومی حفاظت از داده

مقررات عمومی حفاظت از داده‌ها مصوب پارلمان اتحادیه اروپا به تنظیم مقررات، توضیح شرایط و فرآیندهای مربوط به داده‌های شخصی اشخاص حقیقی و حقوقی و همچنین پردازش آن‌ها، برقراری سازوکار حفاظت و تضمین حفاظت از داده‌های شخصی و درعین‌حال حفاظت از جریان آزاد اطلاعات، حقوق مبنا و آزادی‌های کاربران درون اتحادیه اروپا می‌پردازد. بر اساس این قانون، هر شخص حقیقی یا حقوقی که به پردازش داده‌های اشخاص به‌منظور ارائه کالا یا خدمات به شهروندان اتحادیه اروپا می‌پردازد، موظف است تا این مقررات را رعایت کرده و مطابق با آن عمل کند.

حق حفاظت از حریم خصوصی بخشی از کنوانسیون اروپایی حقوق بشر[1] مصوب ۱۹۵۰ است. مطابق ماده هشت این کنوانسیون: «هرکسی از حق احترام به زندگی خصوصی و خانوادگی، خانه و مراسلاتش برخوردار است». از زمان مورد شناسایی قرار گرفتن این حق، اتحادیه اروپا به دنبال توسعه دامنه این حق و شناسایی آن در زمینه‌های مختلف و برقراری حمایت قانونی از آن بوده است. اتحادیه اروپا در یکی از اقدامات قابل‌توجه خود، مقارن با اختراع

۱. کنوانسیون اروپایی حقوق بشر (European Convention on Human Rights) یک معاهده بین‌المللی برای حفاظت از حقوق بشر و آزادی‌های اساسی در اروپاست، که در سال ۱۹۵۰، پیش‌نویس آن توسط نهاد نوبنیاد شورای اروپا تهیه، و در سوم سپتامبر ۱۹۵۳ لازم‌الاجرا شد.

اینترنت و آغاز انقلاب تکنولوژیک شروع به ایجاد تأسیس‌های قانونی جهت حفاظت از داده‌های کاربران نمود. در سال ۱۹۹۵ (راهنما) دستورالعمل حفاظت از داده‌های اروپا[1] را به تصویب رساند که یک نظام حداقلی استاندارد برای حفاظت از حریم خصوصی و امنیت داده‌ها بود و کشورهای عضو اتحادیه نیز این دستورالعمل را مبنای قانون‌گذاری داخلی قرار داده و همچنین سازوکارهای منطبق با آن را اجرایی کردند. این دستورالعمل به شکل اختصاصی ناظر بر پردازش داده‌های شخصی شهروندان کشورهای عضو اتحادیه اروپا است. این دستورالعمل، سه اصل کلی را برای قانون‌گذاری به کشورهای عضو اتحادیه اروپا پیشنهاد کرده است:

۱-شفافیت، ۲- هدف مشروع، ۳-تناسب. طبق اصول پیشنهادی، پردازش داده‌های شخصی نباید اصلاً انجام بگیرد، مگر آنکه شرایط مشخص‌شده در اصول احراز گردد.

با این تفاسیر، این اقدام اتحادیه کافی به نظر نمی‌رسید. نرخ نفوذ اینترنت و تعداد کاربران روزبه‌روز در حال افزایش بود و اینترنت همانند یک مکنده دیتاهای کاربران را جمع‌آوری می‌کرد. از آغاز قرن بیست و یکم، ارائه خدمات مختلف و متعدد بر بستر اینترنت آغاز شد. اکثر مؤسسات مالی بانکداری آنلاین را ارائه کردند. از سال ۲۰۰۶ فیس‌بوک شروع به کارکرد و ناگهان غول‌های فناوری ظاهرشده و کنترل اینترنت را بر عهده گرفتند. از آغاز دهه دوم قرن، کم‌کم اختلافات کاربران و پلتفرم‌ها آغاز شد و روزبه‌روز نیز برشدت و دامنه آن افزوده شد.

در سال ۲۰۱۱ یکی از کاربران از شرکت گوگل به خاطر اسکن

1. the European Data Protection Directive

صندوق پیام‌های الکترونیکی‌اش شکایت کرد(cnet,۲۰۱۱) و بعدازاین رویداد بود که مرجع حفاظت از داده‌های اتحادیه اروپا اعلام نمود که اتحادیه نیازمند «یک رویکرد جامع در موردحفاظت از اطلاعات شخصی»[1] و بر همین اساس بازنگری در دستورالعمل-۱۹۹۵ آغاز شد. این اولین گام در مسیر ایجاد مقررات عمومی حفاظت از داده‌ها است و یک سال بعد، در سال ژوئن ۲۰۱۲ نخستین پیش‌نویس این مقررات تهیه شد. این مقررات در سال ۲۰۱۶ به تصویب پارلمان اروپا رسید و از سال ۲۰۱۸، برای کلیه سازمان‌ها لازم‌الاجرا شد.

باگذشت بعد از ۱۰ سال از تنظیم متن اولیه مقررات عمومی حفاظت از داده، امروز بسیاری از کارشناسان معتقدند که اروپا اقدام به جدی‌ترین نظام حفاظت از داده‌های کاربران در جهان نموده و این مقررات الگوی بسیاری از نظام‌های ملی بوده و قوانین داخلی متعددی منبعث از آن تهیه‌شده است؛ اما در مقابل نیز برخی از صاحب‌نظران حریم خصوصی معتقد هستند که این مقررات عملکرد مطلوبی نداشته و آن‌چنان‌که انتظار می‌رفت ظاهرنشده‌اند. در ادامه مروری بر نقاط قوت و ضعف مقررات عمومی حفاظت از داده‌ها انجام خواهد شد.

1. “a comprehensive approach on personal data protection”

بخش چهارم

آیا مقررات عمومی حفاظت از داده برای تمامی کشورها مناسب است؟

انقلاب صنعتی چهارم در حال حاضر سوار بر یک موج متلاطم از وقایع است که به‌احتمال‌زیاد آینده صنعت فناوری در پایان آن مشخص خواهد شد. شرکت متا و پلتفرم‌های متعلق به آن، گوگل و بسیاری از پلتفرم‌های بزرگ جهان اکنون در مقابل پرسش‌های سخت مربوط به حریم خصوصی قرارگرفته‌اند و با شیوه‌های تأمین امنیت داده‌های کاربران دست‌وپنجه نرم می‌کنند. اعتماد به پلتفرم‌های بزرگ و غول‌های فناوری در حال کاهش است و علاوه بر کاربران، امروزه سیاست‌مداران نیز به آن‌ها بدبین شده‌اند. کارشناسان در حال تلاش هستند تا بفهمند چگونه می‌توانند قوانین حفاظت از حریم خصوصی را منقح کنند، از داده‌های کاربران محافظت کنند و درعین‌حال با بهره‌گیری از مدل‌های تجاری و تبلیغات هدفمند خود، تداوم جریان مالی و خلق پول را نیز تأمین کنند. این موقعیت پارادوکسیکال، هر روز بیش‌تر جدی و حیاتی شده و منازعات بر سر آن جدی‌تر می‌شود. با تصویب و لازم‌الاجرا شدن مقررات عمومی، موج جدیدی به راه افتاد که اروپا راه‌حل نهایی پایان دادن به این چالش‌ها و منازعات را یافته است. اروپا با تصویب سخت‌گیرانه‌ترین

قانـون حمایـت از حریـم خصوصـی در جهـان، بـه شـکل قاطعانـه‌ای عـزم خـود بـرای پایـان دادن بـه عـدم تعهـد پلتفرم‌هـا بـه حریـم خصوصـی کاربـران را نشـان داد. بـا توجـه بـه اثـر بروکسـل[1] کـه بیانگـر فراینـد جهانی‌سـازی قوانیـن اتحادیـه اروپـا و تبعیـت شـرکت‌ها از قوانیـن حاکـم بـر ایـن منطقـه اسـت، همـه انتظـار شـکل‌گیری یـک نظـم جهانـی در خصـوص حفاظـت از داده‌هـای شـخصی کاربـران را داشـتند. حتـی خـود اروپایی‌هـا نیـز، در پـس بسـیاری از تصمیمـات حقوقـی و قضایـی خـود، چنیـن انگیـزه‌ای را بـه شـکل نهانـی دارنـد و در خصـوص موضوعـی بـا این سـطح از اهمیـت نیـز، ایـن انگیـزه دوچنـدان بـود. چراکـه تقریبـاً تمامـی پلتفرم‌هـای مطـرح جهـان بـه کاربـران اتحادیـه اروپـا خدمـات ارائـه می‌دهنـد و انطبـاق شـرکت‌ها بـا مقـررات عمومـی، به‌راحتـی در سرتاسـر جهـان تبدیـل بـه یـک الگـوی قانونـی می‌شـود. در همـان ایـام آغازیـن اجرایـی شـدن مقـررات نیـز بسـیاری از پلتفرم‌هـا در تبلیغـات خـود اعـلام می‌کردنـد کـه قصـد جهانی‌سـازی اصـول منـدرج در مقـررات عمومـی را دارنـد و وقتـی آن را در یکـی از بزرگ‌تریـن بازارهـای هـدف خـود اجـرا می‌کننـد، بهتـر اسـت کـه در همه‌جـا ایـن کار را انجـام بدهنـد.

امـا در عمـل ایـن اتفـاق هرگـز بـا آن حالـت ایـده آلـی کـه مدنظـر اتحادیـه اروپـا بـود، رخ نـداد. دلیـل واضـح و سـاده‌ای بـرای ایـن ناکامـی وجـود دارد و آن عبـارت از ایـن اسـت کـه ایالات‌متحـده آمریـکا، در مواجهـه بـا غول‌هـای فنـاوری نمی‌توانسـت سیاسـتی مشـابه بـا اتحادیـه اروپـا اتخـاذ کنـد. از سـوی دیگـر، نحـوه و میـزان پذیـرش قوانیـن در میـان جوامـع مختلـف متفـاوت اسـت. افـکار عمومـی در بسـیاری از کشـورهای اروپایـی، بسـیار سـختگیرتر و منضبط‌تـر از جامعـه آمریکایـی هسـتند و

1. The Brussels Effect

از قوانین سخت‌گیرانه حمایت می‌کنند. در یک نظرسنجی در خصوص سختگیری نسبت به قوانین ناظر به حریم خصوصی، ۸۵ درصد از آلمانی‌ها از استانداردهای سخت‌گیرانه حمایت کردند، درحالی‌که تنها ۲۹ درصد از پاسخ‌دهندگان آمریکایی این احساس را داشتند(dotmagazine, ۲۰۲۲). در ایالات‌متحده آمریکا، رویکردها نسبت به حریم خصوصی به‌مراتب متعادل‌تر است. در رویکرد آمریکایی، بنابر این است که به‌منظور حمایت از نوآوری شرکت‌های فناوری، توانایی آن‌ها در جمع‌آوری، تجزیه‌وتحلیل و کسب درآمد از داده‌ها با حداقل محدودیت مواجه شود. چراکه کاربران برای دریافت خدمات رایگان جذب پلتفرم‌ها می‌شوند و آن‌ها نیز برای کسب درآمد از داده‌های تولیدشده توسط آن‌ها استفاده می‌کنند. در مقابل، حفاظت از رقابت‌پذیری و مبارزه با انحصارگرایی و نقش آن در توسعه فناوری در راستای مبارزه با لابی‌گرانی که برای منافع خود قوانین فدرال را حتی تغییر می‌دهند، بسیار حیاتی است.

از سوی دیگر، در کشوری مثل آمریکا اکثر قوانین تنظیم‌کننده حریم خصوصی توسط ایالت‌ها تنظیم می‌شوند و با همدیگر دارای تفاوت‌های زیادی هستند. تنها در ایالت کالیفرنیا که تحت حاکمیت قانون حریم خصوصی مصرف‌کننده کالیفرنیا[1] است شاهد یک نظام سخت‌گیرانه هستیم و در دیگر ایالت‌ها این رویکرد را نمی‌بینیم.

به‌طورکلی رویکرد جوامع نسبت به دادوستد با پلتفرم‌ها در ازای حریم خصوصی کمتر با همدیگر متفاوت است. از همین رو به نظر می‌رسد که هم شرکت‌ها و هم مصرف‌کنندگان نیازمند قوانین متناسب با نظام ارزشی خاص خود هستند.

1. California Consumer Privacy Act

مسئله دیگر آن است که گفتمان غالب بر تنظیم‌گری حریم خصوصی داده، اغلب شرکت‌های فناوری و بازارهای نوظهور فناوری را نادیده می‌گیرد و همین امر منجر می‌شود تا مسائل مختلفی با تصویب قوانین به وجود بیاید. شرکت‌های بزرگ نیز مزید بر علت هستند. به‌عنوان‌مثال برخی از بزرگ‌ترین بازارهای هدف فیس‌بوک، رشد فوق‌العاده سریعی را در کشورهای آسیایی و آفریقایی را تجربه می‌کنند. از ۱۰ کشور جهان که بیشترین کاربر فیس‌بوک را دارند، تنها دو کشور ایالات‌متحده آمریکا با مجموع ۲۴۰ میلیون کاربر و ژاپن با نزدیک به ۵۶ میلیون کاربر توسعه‌یافته هستند. هشت کشور باقی‌مانده همگی جز کشورهای توسعه‌نیافته یا درحال‌توسعه هستند و هند با ۴۱۶ میلیون بیشترین کاربر فیس‌بوک در جهان را دارد(worldpopulationreview,۲۰۲۲). در این لیست نام کشورهای مثل فیلیپین، ویتنام، مکزیک، اندونزی، برزیل و پاکستان به چشم می‌خورد.

تحقیقات نشان می‌دهد که کاربران در کشورهای توسعه‌نیافته یا درحال‌توسعه اعتماد بیشتری به محتوای آنلاین و ارائه‌دهندگان خدمات دارند(hbr,۲۰۱۸). دسترسی محدود به اطلاعات و مطبوعات آزاد، سواد پایین رسانه‌ای و دانش محدود کاربر ازجمله عوامل مؤثری است که سبب می‌شود تا کاربران حساسیت کمتری نسبت به حریم خصوصی داده‌های خود داشته باشند. همین دلایل آسیب‌پذیری آن‌ها را در مقابل برخی از عارضه‌های شایع شبکه‌های اجتماعی همچون اخبار جعلی و گمراه‌کننده نیز افزایش می‌دهد. به‌عنوان‌مثال، فیس‌بوک در بسیاری از کشورهای فقیر جهان مترادف

با اینترنت است. فیس‌بوک این جایگاه را مدیون سرویس «Free Basics» خود است، پروژه‌ای که در آن امکان استفاده رایگان از سرویس‌ها و سایت‌های مشخصی را به کاربران می‌دهد. این سرویس تا سال ۲۰۱۶ در بیش از ۳۰ کشور در دسترس بوده و تعداد کشورها در سال ۲۰۱۹ به ۶۵ کشور افزایش پیدا می‌کند که نیمی از آن‌ها آفریقایی هستند. کاربران این سرویس اکنون بیش از ۱۰۰ میلیون نفر هستند(globalmedia,۲۰۲۲). میانمار یک مثال قابل‌توجه در این خصوص است، این کشور در سال ۲۰۱۴ و قبل از ارائه اینترنت رایگان فیس‌بوک، ۲ میلیون کاربران فیس‌بوک داشت، درحالی‌که پس ورود Free Basics در سال ۲۰۱۶، این تعداد به ۳۰ میلیون کاربر رسید. کاربران میانماری متحمل زیان‌های قابل‌توجهی از فیس‌بوک شدند و کمپین اخبار جعلی و سخنان نفرت‌آمیز علیه اقلیت قومی روهینگیا، یک خشونت سامان‌مند سازمان‌یافته در فیس‌بوک بود، بااین‌وجود، فیس‌بوک همچنان در این کشور محبوب و مقبول است، زیرا کاربران میانماری به آن وابسته هستند. هندوستان نیز به‌عنوان بزرگ‌ترین جامعه کاربری فیس‌بوک همین وضع را دارد و گروه‌های واتس‌اپی در هند یک چالش اساسی هستند. پخش اخبار جعلی، نفرت پراکنی و درگیری‌های قومیتی ازجمله اصلی‌ترین موضوعات واتس‌اپ هندوستان است، بااین‌وجود کاربران هندی به‌شدت به این پلتفرم وابسته هستند.

بدیهی است در چنین شرایطی، اولویت‌های بسیار متفاوتی برای یک کشور و کاربران آن ایجاد می‌شود که برای تأمین آن‌ها مجبور به انتخاب هستند و قدرت چانه‌زنی آن‌ها به همین میزان کاهش پیدا

می‌کند. شرکتی همچون متا، این خدمات رایگان را در ازای جمع‌آوری و پردازش بی‌قیدوشرط داده‌های کاربران در اختیار این‌گونه کشورها قرار می‌دهد و مسلماً کاربران در این خصوص حساسیت به‌مراتب کمتری نسبت به کاربران اروپایی دارند.

مسئله دیگر، لزوم احتیاط کشورهای درحال‌توسعه به‌ضرورت حمایت از شرکت‌های کوچک و نو پا است. مقرراتی همچون مقررات عمومی حفاظت از داده‌های اروپا هزینه‌های هنگفتی بر این‌گونه شرکت‌ها تحمیل می‌کنند و تحمیل وظایف و هزینه‌های سنگین بر مشاغل کوچک که به نحوی با داده‌های کاربران در ارتباط هستند، رشد آن‌ها را با چالش مواجه خواهد کرد.

تأسیس رژیم‌های فوق استاندارد، عوارض دیگری نیز دارد و آن تقویت انگیزه قانون‌گریزی است؛ مثلاً شرکت متا، به نحوی برنامه‌ریزی کرده است تا جامعه کاربری میلیاردی خود که عمدتاً در کشورهای درحال‌توسعه ساکن هستند، نتوانند با استناد بر مقررات عمومی حفاظت از داده شکایتی ثبت کنند و در عوض آن‌ها را ذیل قانون حریم خصوصی مصرف‌کننده کالیفرنیا برده است. درمجموع، این عوامل درنهایت منجر به بالکانیزه شدن جهان دیجیتال خواهد شد؛ این تمایزات باعث تصور منطقه امن دیجیتال در کشورهای پیشرفته و منطقه قرمز دیجیتال در کشورهای درحال‌توسعه می‌شوند. جدای از فشار و تأثیرات منفی که برای شمولیت و فراگیری وجود دارد، نابرابری ضریب نفوذ تکنولوژی دیجیتال و تفاوت در درجه حفاظت از داده‌ها خود می‌تواند به‌نوعی نابرابری جدید تبدیل شود.

پرسشی که باقی می‌ماند عبارت از این است که چنانچه بنا

بـر دلایـل پیش‌گفتـه، مقـررات عمومـی حفاظـت از داده‌هـا، نمی‌توانـد نسـخه مناسـبی بـرای تمـام کشـورها باشـد و گویـای مثـال نقـض اثـر بروکسـل اسـت، آیـا می‌توانـد الگـوی مناسـبی بـرای خودتنظیمـی و برداشـتن گام‌هـای مثبـت از سـوی شـرکت‌ها بـرای محافظـت بهتـر از داده‌هـای شـخصی کاربـران باشـد؟ غول‌هـای فنـاوری در طـول سـالیان گذشـته رویـه‌ای را بنیـان گذاشـته‌اند کـه بسـیاری از فعالیـن حـوزه حریـم خصوصـی را نگـران کـرده اسـت. بی‌مسـئولیتی و بی‌مبالاتـی مدیرانـی همچـون مـارک زاکربـرگ کـه در مـوارد متعـددی از داده‌هـای شـخصی کاربـران پلتفرم‌هـای متعلـق بـه متـا سوءاسـتفاده کـرده اسـت و یـا الگـوی «اقتصـاد توجـه» گـوگل و پایـش مـداوم داده‌هـای کاربـران به‌منظـور شخصی‌سـازی تبلیغـات تجـاری می‌توانـد تبدیـل بـه رویـه ثابـت شـرکت‌های فنـاوری شـده و ضـرورت حمایـت از داده‌هـای شـخصی کاربـران، به‌عنـوان یـک ارزش رنـگ ببـازد و منافـع اقتصـادی کلان ناشـی از پـردازش و فـروش داده به‌جـای آن بنشـیند. بااین‌وجـود، مقـررات عمومـی تلاشـی بـود تـا سـرعت ایـن فراینـد را کـم کنـد، همان‌طـور کـه گلدمـن سـاکس[1] تخمیـن می‌زنـد، ایـن مقـررات در یـک بـازه زمانـی یک‌سـاله تـا ۷ درصـد تأثیـر منفـی بالقـوه بـر کسـب‌وکار فیس‌بـوک از تجـارت بـا داده‌هـا بگـذارد(investors,۲۰۱۸). آمـار و ارقـام گویـای آن اسـت کـه خودتنظیمـی به‌عنـوان ابـزار مناسـبی جهـت تحصیـل اطمینـان از تمامیـت داده‌هـای شـخصی عمل‌نکـرده و صرفـاً تأثیـر کمـی بـر گـردش مالـی فیس‌بـوک در حـوزه تجـارت داده گذاشـته اسـت. نکتـه قابل‌توجـه آن اسـت کـه در مدیریـت وضعیـت تناقض‌آمیـز داده‌هـای

1. Goldman Sachs

گلدمـن سـاکس یـک بانـک سـرمایه‌گذاری چندملیتـی آمریکایـی و شـرکت خدمـات مالـی اسـت کـه دفتـر مرکـزی آن در شـهر نیویـورک اسـت.

خصوصی کاربران و الگوی اقتصادی شرکت‌ها، مسائل اساسی‌تری نیز وجود دارد که باید به آن توجه نمود. در کسب‌وکارهای فناورانه عصر حاضر، داده در حکم واحد پولی است و به‌نوعی هسته اقتصادی شرکت را شکل می‌دهد و برای بسیاری از ارائه‌دهندگان خدمات رایگان یا ارزان‌قیمت، هیچ شیوه جایگزینی وجود ندارد. به همین دلیل، برخی از واقع‌گرایان بر این باور هستند که باید به توسعه دامنه اختیارات شرکت‌ها در پردازش داده‌های کاربران پرداخت و از این طریق اجازه داد تا صنعت زنده بماند؛ اما این تفکر می‌تواند خطرناک باشد، چراکه مدیریت آن امری نزدیک به غیرممکن است و هرلحظه ممکن است که شرایط از کنترل خارج شود؛ اما می‌توان از راه‌کارهای بازدارنده‌ای برای استانداردسازی این فرایند استفاده نمود. در شرایطی که قوانینی همچون مقررات عمومی حفاظت از داده اروپا قابلیت عملیاتی شدن در بسیاری از کشورهای جهان را ندارد، باید توجه بیشتری به مفهوم «مسئولیت اجتماعی دیجیتال[1]» داشت. از شرکت‌ها انتظار می‌رود تا به شکل داوطلبانه خود را مقید به رعایت اصولی بدانند که حریم خصوصی کاربران را به بهترین شکل تضمین می‌کند و این اقدام در راستای مسئولیت اجتماعی آن‌ها باید صورت پذیرد. در غیر این صورت، دولت‌ها مجبور خواهند بود با ارجحیت دادن امنیت داده‌های شخصی شهروندان خود بر منافع ناشی از فعالیت شرکت‌های فناوری، اقدام سخت‌گیرانه‌تری اتخاذ کنند و به این بار به شکل جدی اقتصاد غول‌های فناوری را تحت تأثیر قرار بدهند. چین مثال خوبی از این فرایند است؛ غول‌های فناوری آمریکایی تمام تلاش خود را انجام می‌دهند تا در جامعه عظیم

1. digital social responsibility

کاربـران چینـی سـهمی ثابـت و سـودی تضمین‌شـده بـه دسـت آورنـد، امـا قوانیـن سـخت‌گیرانه دولـت چیـن در حـوزه داده آن‌هـا را مجبـور بـه تجدیدنظرهـای اساسـی در شـرایط کاری خـود کـرده اسـت.

بخش پنجم

مروری بر چالش‌های کارکردی مقررات عمومی اروپا

مقـررات عمومـی حفاظـت از داده، یـک تـلاش جاه‌طلبانـه از سـوی اتحادیـه اروپـا بـرای ایجـاد نظـام اسـتاندارد و یکپارچـه جهـت تنظیم‌گـری حریـم خصوصـی کاربـران و داده‌هـای متعلـق بـه آن‌هـا اسـت. تنظیم‌گـری داده در چنیـن وسـعت و مقیاسـی، یـک اقـدام پیچیـده و چالش‌برانگیـز اسـت و عملیاتـی سـازی یـک مکانیسـم اجرایـی کارآمـد، نیازمنـد گـذر زمـان و تحقـق کامـل بلـوغ نظـام حکمرانـی برداده‌هاسـت. بااین‌وجـود، بایـد توجـه داشـت کـه مقـررات عمومـی حفاظـت از داده بـا تمـام مزیت‌هـا و نوآوری‌هایـی کـه بـه همـراه داشـته، جهـان فنـاوری را بـا برخـی عـوارض ناخواسـته مواجـه کـرده و ایـن شـرایط، در پارادایـم تلقـی داده‌هـا به‌عنـوان کالا و نـه به‌عنـوان یـک دارایـی جمعـی، از بسـیاری جهـات قابل‌انتظـار بـود. مقـررات عمومـی بـه معنـی واقعـی کلمـه نتوانسـته اسـت انحصـار غول‌هـای فنـاوری در جمـع‌آوری و پـردازش داده‌هـای شـخصی کاربـران را کاهـش دهـد و ایـن دقیقـاً همـان هدفـی بـود کـه ایـن مقـررات بـرای انجـام آن پایه‌ریـزی شـد و اگـر درگـذر ایـن ایـام نتوانسـته اسـت کـه حتـی بـه آن اندکـی نزدیـک شـود، شـاید مقـررات بیشـتر و اختصاصی‌تـری موردنیـاز اسـت.

در ایـن بخـش، مـروری بـر چنـد مـورد از مشـهودترین چالش‌هـای کارکـردی و عـوارض ناشـی از اجرایـی شـدن آن خواهیـم داشـت.

۵-۱- عدم توازن میان کشورهای عضو در اجرایی ساختن مقررات

اقتصـاد داده از بـدو پیدایـش درون یـک حجـاب دیجیتـال شـکل‌گرفته بـود تـا شـیوه‌های ایـن تجـارت سـودآور از قانون‌گـذاران و کاربـران پنهـان بمانـد. داده‌هـا جـزء دارایی‌هـای شـرکت و یـک راز اختصاصـی تلقـی می‌شـدند، حتـی اگـر به‌طورکلـی از رفتـار و تعامـلات کاربـران استخراج‌شـده بودنـد. دنیـای فنـاوری در پوسـت‌اندازی‌های اخیـر خـود رفته‌رفتـه بـه دنبـال پایـان دادن بـه تفکـر تعلـق داده بـه پلتفـرم اسـت و هم‌گرایـی نیروهـای کاربـران، دولـت و بـازار اکنـون بـه کاربـران توانایـی بیشـتری بـرای محافظـت از داده‌هـای شـخصی می‌دهـد؛ امـا مسـئله قابل‌توجـه آن اسـت کـه کشـورهای مختلـف توانایـی یکسـانی در عملیاتی‌سـازی تمامـی اسـتانداردها نداشـته و از همیـن رو، بـرای اجـرا دچـار مشـکل می‌شـوند. ایـن امـر ناشـی از حداکثـری سـاختن اسـتانداردها در تنظیـم مقـررات عمومـی حفاظـت از داده اسـت. شـرکت‌ها نیـز دقیقـاً با چنیـن وضعیتـی مواجـه هسـتند.

ایرلنـد نمونـه خوبـی از کشـورهایی اسـت کـه پـس از اجرایـی شـدن مقـررات عمومـی حفاظـت از داده دچـار مشـکلات فراوانـی شـد. همان‌طـور کـه در بخش‌هـای قبـل اشـاره شـد، بسـیاری از غول‌هـای فنـاوری بـه دلیلـی معافیت‌هـای مالیاتـی مقـر اروپایـی خـود را در ایرلنـد قـرار داده‌انـد. درنتیجـه بزرگ‌تریـن پرونده‌هـای ناشـی از مقـررات عمومـی حفاظـت از داده، بـر عهـده کمیسـیون حفاظـت از داده‌هـای ایرلنـد[1] اسـت، امـا

1. The Irish Data Protection Commission (DPC)

ایرلنـد توانایـی کافـی بـرای رسـیدگی بـه پرونده‌هـای مربـوط بـه تخلـف شـرکت‌های مسـتقر در کشـور خـود برخـوردار نیسـت(techzine,۲۰۲۱). رسـیدگی بـه هرکـدام از پرونده‌هـای مطروحـه سـال‌ها زمـان می‌بـرد و ایـن کشـور بـه همیـن دلیـل موردانتقـاد جـدی اتحادیـه اروپـا قرارگرفتـه اسـت، ایـن در حالـی اسـت کـه به گفتـه ناظـر اتحادیـه، یکـی از اصلی‌ترین دلایـل عـدم توانایـی ایرلنـد در انجـام وظایـف محولـه، نبـود زیرسـاخت کافـی و سـامانه‌های موردنیـاز بـرای رسـیدگی مؤثـر بـه پرونده‌هـای محولـه اسـت. بـر همیـن اسـاس، قوانیـن ناظـر بـر حـوزه حریـم خصوصـی داده، بـرای شـرکت‌ها نیـز محدودیت‌هـای مختلفـی ایجـاد می‌کنـد. اکثـر شـرکت‌های بـزرگ درحال‌توسـعه حاضـر، بـر سـر موضـوع داده دچـار چالـش شـده‌اند. اکثـر آن‌هـا موظـف هسـتند یـک افسـر حفاظـت از داده منصـوب کننـد[1]. افسـر حفاظـت از داده‌هـا ثبـت کلیـه پـردازش داده‌هـای شـخصی توسـط دیـوان حسابرسـی اروپـا را نگـه‌داری می‌کنـد. افسـر حفاظـت از داده‌هـا ممکـن اسـت توصیه‌هایـی عملـی بـرای بهبـود حفاظت از داده‌هـا ارائـه کنـد و بـه دادگاه و کنترل‌کننده‌هـا و پردازشـگرهای داده در موردحفاظـت از داده‌هـا مشـاوره دهـد.

هم‌چنیـن بایـد از اینکـه حقـوق و آزادی‌هـای افـرادی کـه داده‌هـای شـخصی آن‌هـا پـردازش می‌شـود، تحـت تأثیـر عملیـات پـردازش قـرار نمی‌گیـرد اطمینـان حاصـل نمایـد.

کمیتـه کارکنـان، کنترل‌کننـدگان داده‌هـا و پردازشـگرها، یـا هـر فـرد دیگـری، می‌تواننـد در مـورد هـر موضوعـی کـه مربـوط بـه تفسـیر یـا اجـرای مقـررات باشـد، بـدون نیـاز بـه مجـاری رسـمی و قانونـی، بـا مأمـور حفاظـت از داده‌هـا مشـورت کننـد. هم‌چنیـن هیچ‌کـس نبایـد

1. Data protection officer

برای تماس با مأمور حفاظت از داده‌ها در مورد نقض ادعایی مقررات متضرر شود.

بر اساس بند ۶ از ماده ۳۷ مقررات عمومی حفاظت از داده:

«افسر حفاظت داده باید یکی از کارمندان کنترل‌گر یا پردازشگر باشد، یا بر اساس قرارداد خدمت، وظایف محوله را انجام دهد».

ماده ۳۹ قانون مذکور در خصوص وظیفه افسر حفاظت از داده مقرر می‌دارد:

افسر حفاظت داده باید حداقل دارای وظایف زیر باشد: اطلاع‌رسانی و توصیه به کنترل‌گر یا پردازشگر و کارکنانی که تعهدات پردازشی را مطابق این مقررات و دیگر مقررات حفاظت داده اتحادیه و کشورهای عضو انجام می‌دهند. نظارت بر سازگاری با این مقررات و همچنین دیگر مقررات حفاظت داده در اتحادیه و کشورهای عضو و همچنین سیاست‌های کنترل‌گر و پردازشگر در ارتباط با حفاظت داده‌های فردی، شامل تخصیص مسئولیت‌ها، افزایش آگاهی و آموزش کارکنان درگیر در امور پردازش و حسابرسی‌های مربوطه. انجام مشاوره برحسب درخواست، برای انجام ارزیابی اثر حفاظت داده و نظارت بر کارایی، پیرو ماده‌ی ۳۵. همکاری با نهاد نظارتی. فعالیت به‌عنوان نقطه‌ی تماس برای نهاد نظارتی در تمامی مسائل مرتبط با پردازش، مشتمل بر مشاوره پیشین، مندرج در ماده‌ی ۳۶ و مشاوره در تمامی موضوعات مدنظر. افسر حفاظت داده باید در انجام وظایف خود به ریسک‌های مربوط به عملیات پردازش و ماهیت، قلمرو و اهداف پردازش توجه داشته باشد.

۵-۲- خستگی از اعلام رضایت[1]

ایـن ابتـکار در بـادی امـر به‌عنـوان یکـی از موفقیت‌هـای مقـررات عمومـی حفاظـت از داده معرفـی شـد، بااین‌حـال کارشناسـان حریـم خصوصـی بـر ایـن بـاور هسـتند کـه نبایـد تـا ایـن حـد خوش‌بیـن بـود. از زمـان اجرایـی شـدن مقـررات عمومـی، کاربـران بـه شـکل بیشـتری، بـدون مطالعـه و توجـه بـه جزئیـات، در هنـگام ورود بـه یـک سـایت بـا مقـررات آن موافقـت کـرده و بـر روی گزینـه «پذیـرش» کلیـک می‌کننـد.

درواقـع، نقطـه تعامـل واقعـی بسـیاری از کاربـران بـا مقـررات عمومـی صرفـاً خلاصـه بـه همیـن موافقت‌کـردن بـا درخواسـت‌های پی‌درپـی سـایت‌های مختلـف در طـول اسـتفاده از اینترنـت می‌شـود. ارائـه هشـدار حفاظـت از حریـم خصوصـی و جلـب رضایـت کاربـر، تبدیـل بـه رویکـرد غالـب اکثـر سـازمان‌ها بـرای انطبـاق بـا مقـررات عمومـی شـده اسـت؛ امـا از منظـر حقـوق قراردادهـا، یـک موافقـت ناآگاهانـه و بـدون توجـه بـه مفاد قـرارداد بامعنـی رضایـت صریـح و آگاهانـه ناسـازگار اسـت. تبلیغـات بالاپـر[2] بـه شـکل بی‌پایـان، مبهـم و ناخوانـا در تمـام سـایت‌ها بـه هنـگام ورود بـر روی صفحه‌هـای نمایـش کاربـران ظاهرشـده و آن‌هـا بـدون درک از معنـی جمـلات، صرفـاً تائیـد کـرده و عبـور می‌کننـد. ایـن فراینـد منجـر بـه شـکل‌گیری پدیـده‌ای بـه نـام خسـتگی از اعـلام رضایـت شـده اسـت. آمارهـا نشـان می‌دهـد کـه ۴۶ درصـد از کاربـران در یـک نظرسـنجی، اعـلام کرده‌انـد کـه ایـن شـرایط جدیـد هیـچ تغییـری نسـبت بـه قبـل ایجـاد نکـرده و صرفـاً منجـر بـه کلافگـی و خسـتگی کاربـران شـده اسـت(marketoonist,۲۰۱۹).

مقـررات عمومـی در ایـن خصـوص به‌وضـوح ضعـف عملکـردی خـود

1. consent fatigue
2. pop up

را نشـان داده اسـت. حتـی ایـن وضعیـت منجـر بـه طـرح شـکایت‌های حقوقـی متعـددی شـده اسـت و دادگاه عالـی اتحادیـه اروپـا در همیـن خصـوص اعـلام کـرد کـه ارائه‌دهنـدگان خدمـات حـق ندارنـد کـه کوکی‌هـای خـود را در قالـب یـک موافقت‌نامـه بـه کاربـران تحمیـل نماینـد(pinsentmasons,۲۰۲۲).

۵-۳- ابهام قانونی در قبال فناوری تصمیم‌گیری خودکار[1]

تصمیم‌گیـری خـودکار (ADM) شـامل اسـتفاده از داده‌هـا، ماشـین‌ها و الگوریتم‌هـا بـرای تصمیم‌گیـری در زمینه‌هـای مختلفـی، ازجملـه مدیریـت عمومـی، تجـارت، بهداشـت، آمـوزش، قانـون، اشـتغال، حمل‌ونقـل، رسـانه و سـرگرمی همـراه بـا مقادیـر متفـاوت از مداخلـه انسـانی اسـت. نظـارت یـا مداخلـه ADM شـامل داده‌هـای منبـع بـا مقیـاس بزرگـی اسـت؛ کـه از پایگاه‌هـای داده، متـن، رسـانه‌های اجتماعـی، حسـگرها، تصاویـر یـا گفتـار بـه دسـت می‌آینـد. همچنیـن، بـا اسـتفاده از طیـف وسـیعی از فناوری‌هـا، ازجملـه نرم‌افـزار رایانـه‌ای، الگوریتم‌هـا، یادگیـری ماشـینی، پـردازش زبـان طبیعـی، هـوش مصنوعـی، هـوش افـزوده و روباتیـک پـردازش می‌شـوند. اسـتفاده روزافـزون از سـامانه‌های تصمیم‌گیـری خـودکار (ADMS) در طیـف وسـیعی از زمینه‌هـا، مزایـا و چالش‌هـای زیـادی را بـرای جامعـه انسـانی ایجـاد می‌کنـد کـه نیازمنـد در نظـر گرفتـن پیامدهـای فنـی، قانونـی، اخلاقـی، اجتماعـی، آموزشـی و اقتصـادی اسـت. پلتفرم‌هـای اطلاعـات دیجیتـال و سـرگرمی به‌طـور فزاینـده‌ای توصیه‌هـای خـودکار (سـامانه‌های توصیه‌گـر) را بـر اسـاس اطلاعـات جمعیتـی، انتخاب‌هـای قبلـی، فیلتـر مشـارکتی یـا فیلتـر مبتنـی بـر محتـوا بـه کاربـران ارائـه

1. Automated Decision-Making

می‌دهند که شامل پلتفرم‌های موسیقی و ویدئو، انتشارات دانشگاهی، توصیه‌های بهداشتی، پایگاه داده محصولات و موتورهای جستجو می‌شود. بسیاری از سامانه‌های توصیه‌گر اختیار را برای کاربران در پذیرش توصیه‌ها فراهم می‌کنند و حلقه‌های بازخورد الگوریتمی مبتنی بر داده‌ها را بر اساس اقدامات کاربر سیستم ترکیب می‌کنند(Araujo et al,۲۰۲۰).

فناوری تصمیم‌گیری خودکار، ازآنجایی‌که همچنان موضوعی جدید در حوزه داده تلقی می‌شود و ابعاد جدیدی از کاربری آن درحال‌توسعه است، به شکل متقن سازوکارهای حقوقی برای تنظیم‌گری آن پیش‌بینی‌نشده است. مقررات عمومی حفاظت از داده، اگرچه در خصوص استفاده‌های موردی از داده‌ها تعیین تکلیف نموده است، اما در خصوص عملکرد الگوریتم‌ها تصمیم خاصی نگرفته است. این موضوع می‌تواند دامنه‌های خیلی وسیعی داشته باشد. به‌عنوان‌مثال، یکی از کاربردهای تصمیم‌گیری خودکار، مربوط به فرایندهای رسیدگی قضایی می‌شود. در نظام‌های حقوقی برخی از کشورهای جهان، ابزارهای الگوریتمی برای تکمیل یا جایگزینی قضاوت، کارمندان دولت و افسران پلیس در بسیاری از زمینه‌ها استفاده می‌شود. در ایالات‌متحده، از آن برای ایجاد امتیاز جهت پیش‌بینی خطر تکرار جرم در مراحل دستگیری پیش از محاکمه و صدور احکام، ارزیابی آزادی مشروط برای زندانیان و پیش‌بینی «نقاط حساس» برای جنایات آینده استفاده می‌شود. این امتیازات ممکن است منجر به اثرات خودکار شود یا ممکن است برای اطلاع‌رسانی تصمیمات اتخاذشده توسط مقامات در سیستم قضایی

استفاده شود. تحقیقاتی که در این زمینه انجام‌گرفته نشان می‌دهد که الگوریتم‌های ارزیابی ریسک مورداستفاده در سیستم قضایی ایالات‌متحده عمیقاً تحت تأثیر سوگیری قرار داشته و به شکل افراطی، نژادپرستانه عمل می‌کنند، درحالی‌که خروجی آن‌ها به‌عنوان یک مبنای معتبر برای صدور احکام قطعی در نظر گرفته می‌شود(propublica,۲۰۲۲).

مشکل اصلی مقررات عمومی حفاظت از داده آن است که در خصوص تصمیم‌گیری خودکار تجویز می‌کند که در صورت رضایت کاربر یا ضروری بودن نمایه‌سازی، نمایه‌سازی مجاز است. این موضوع را می‌توان به‌عنوان مبنای عملکرد تمام پلتفرم‌های الگوریتمی در نظر گرفت؛ زیرا تمامی آن‌ها، به منظور سفارشی‌سازی تبلیغات، کاربر را نمایه کرده و این نمایه‌سازی برای عملکرد الگوریتم «ضروری» است. در نمایه‌سازی کاربران، شکست مفهوم رضایت بر پردازش به‌خوبی آشکار می‌شود؛ زیرا نمایه‌های مبتنی بر داده‌های انباشته یا پردازش‌شده می‌توانند بدون اطلاع و رضایت کاربر ایجاد شوند.

۵-۴- افزایش بروکراسی‌های شرکتی

الزامات ناشی از مقررات عمومی حفاظت از داده منجر به آن شده است تا بسیاری از شرکت‌های اروپایی به‌ویژه استارتاپ‌ها مجبور به کاهش سرمایه‌گذاری در حوزه زیرساخت‌های امنیت سایبری و بودجه‌های تبلیغاتی شده‌اند و در عوض لایه‌ای از بروکراسی را به شرکت‌های خود اضافه کرده‌اند. مقررات عمومی حفاظت از داده مبتنی بر شیوه خود سیاست‌گذاری و خود گزارش‌دهی[1] تنظیم‌شده

1. self-policing, self-reporting model

است و شرکت‌ها به‌جای اینکه عملاً به تغییر فرایندهای پیشین و بهبود عملکرد بپردازند، بر اضافه کردن کارکنان و پیچیده کردن مقررات داخلی به‌منظور انطباق ظاهری با مقررات عمومی حفاظت از داده می‌پردازند. به‌عنوان‌مثال، فیس‌بوک مدل کسب‌وکار خود را بعد از لازم‌الاجرا شدن مقررات عمومی تغییر نداد، به‌جای آن اقدام به استخدام وکلای بیشتر و تقویت معاونت حقوقی شرکت برای دفاع از عملکرد کاری خود کرد. این وکلا موظف به پاسخ‌دهی به تخلفات شرکت فیس‌بوک در کمیسیون‌های حفاظت از داده اتحادیه اروپا هستند و این شرایط هیچ تغییری در عملکرد این شرکت ایجاد نکرده است. واقعیت این است که اکثر کاربران فیس‌بوک در صورت تمایل به برقراری ارتباط با دوستان، خانواده و اطرافیان خود مجبور به اعلام رضایت به شرایط فیس‌بوک هستند و محدودیت در انتخاب چاره دیگری برای آن‌ها باقی نگذاشته است. گوگل نیز رویه مشابهی را در پیش‌گرفته است. در خصوص پلتفرم یوتیوب که متعلق به این شرکت است، گوگل مدل اقتصاد الگوریتمی و تبلیغاتی یوتیوب را تغییر نداده است و صرفاً با تغییر در ادبیات و ارائه برخی توضیحات به کاربران می‌گوید که چرا تبلیغات سفارشی‌سازی شده را دریافت می‌کنند و اگر این اتفاق نیافتد، متعاقباً کیفیت خدمات دریافتی از سوی کاربران کاهش پیدا خواهد کرد.

هنگامی‌که این مسائل را در کنار پیچیدگی‌های حقوقی مقررات عمومی حفاظت از داده و اطلاعات کم مدیران شرکت‌ها از یک‌سو و تلاش‌های ظاهری و سطحی آن‌ها برای انطباق می‌گذاریم، جای تعجبی باقی نمی‌ماند که چرا مقررات عمومی حفاظت از داده باعث

ایجـاد بروکراسـی بیشـتر و نـه تغییـر فرهنـگ تعامـل بـا داده‌های شـخصی می‌شـود.

بـر اسـاس آنچـه گفتـه شـد، بـه نظـر قابـل‌درک می‌رسـد کـه چـرا بدنـه کارشناسـی اتحادیـه اروپـا و کمیته‌هـای فرعـی پارلمـان اروپـا، خصوصاً کمیتـه آزادی‌هـای مدنـی، عدالـت و امـور داخلـی[1] بـر اصـلاح و تقویـت پروتکل‌هـای مقـررات عمومـی حفاظـت از داده تأکیددارنـد. قانـون خدمـات دیجیتـال، تـا حـدی به‌منظـور تکمیـل مقـررات عمومـی تهیـه و تنظیم‌شـده اسـت. امـا بایـد توجـه داشـت کـه نقطه‌ضعف‌هـای اصلـی مقـررات عمومـی حفاظـت از داده بیشـتر از آن‌کـه ماهـوی باشـد، ناشـی از عـدم قابلیـت اجرایـی اسـت. (GDPR) نتوانسـت غول‌هـای فنـاوری و ابـر ذخیـره کننـدگان داده را متوقـف کنـد، بـه همیـن دلیـل اروپـا بـه سـمت تقویـت نظـام حقـوق محافظـت از داده شـهروندان خـود و تهیـه یـک بسـته خدمـات دیجیتـال نویـن بـرای کنتـرل و مهـار (Very Large Online Platform) در حـال حرکـت اسـت. در ادامـه نگاهـی بـر مسـیر پیـش روی نظـام حکمرانـی بـر داده اتحادیـه اروپـا، بـر اسـاس تجربیـات آموخته‌شـده از(GDPR) خواهیـم داشـت.

1. the Committee on Civil Liberties, Justice and Home Affairs (LIBE)

۲. کمیتـه آزادی‌هـای مدنـی، عدالـت و امـور داخلـی پارلمـان اروپـا، کمیتـه‌ای اسـت کـه مسـئولیت حمایـت از آزادی‌هـای مدنـی و حقـوق بشـر را کـه در منشـور حقـوق اساسـی اتحادیـه اروپـا ذکـر شده‌اسـت برعهـده دارد.

بخش ششم

مسیر پیش روی نظام حکمرانی بر داده اتحادیه اروپا بر اساس تجربیات آموخته شده از GDPR

از سال ۲۰۱۲، کمیسیون اروپا اقدامات متعددی را جهت شکل دادن به آینده نظام حکمرانی بر داده اتحادیه اروپا انجام داده است. یکی از اصلی‌ترین گام‌های برداشته‌شده، تصویب مقررات عمومی حفاظت از داده‌ها یا همان (GDPR) بود که در ماه مه ۲۰۱۸ لازم‌الاجرا شد. هدف مقررات عمومی حفاظت از داده‌ها، حفاظت از حقوق داده‌های شخصی متعلق به افراد حقیقی است. در پایان سال ۲۰۲۰، کمیسیون اروپا یک گام فراتر رفت و پیشنهاد خود را برای تصویب قانون خدمات دیجیتال منتشر کرد که به‌عنوان بخشی از استراتژی دیجیتال اتحادیه اروپا، شامل مقرراتی برای به‌روزرسانی چارچوب قانونی تجارت الکترونیک است. پارلمان اروپا در ۵ ژوئیه ۲۰۲۲ موفق به تصویب «بسته خدمات دیجیتال» یا به عبارت دقیق‌تر دو قانون خدمات دیجیتال (DSA) و بازارهای دیجیتال (DMA) شد. اقدامی که از مدت‌ها با کمپین‌های طولانی و سخت شرکت‌های فناوری برای کم کردن این پیشنهادها مواجه بود و «نقطه عطف تنظیم غول‌های اینترنتی» و ایجاد امنیت شدید برای کاربران و اولین مجموعه «قوانین جامع» برای سکوهای آنلاین خوانده می‌شود. قانون خدمات

دیجیتال عنوان چارچوب قانونی جدید بود که اولین بار کمیسیون اروپا در دسامبر ۲۰۲۰، برای مقابله با چالش‌هایی مانند فروش محصولات جعلی، گسترش سخنان نفرت‌انگیز، تهدیدات سایبری، محدود کردن رقابت و تسلط بر بازار پیشنهاد کرد. ایده اصلی پشت این پیشنهاد این بود: آنچه در دنیای واقعی غیرقانونی است، باید در دنیای آنلاین نیز غیرقانونی باشد. و تأکید شد که هدف از تصویب این قانون ایجاد یک دنیای آنلاین امن‌تر است(bino,۲۰۲۲).

صلاحیت محلی مقررات عمومی حفاظت از داده و قانون خدمات دیجیتال در مرزهای کشورهای عضو متوقف نمی‌شود. برای مثال، یک حادثه در توییتر منجر به وضعیتی شد که کاربران توییتر توییت‌های خود را که مربوط به سال ۲۰۱۴ بود، بدون اطلاع خود در دسترس عموم قراردادند. این نقض (GDPR) حداقل ۸۸,۷۲۶ کاربر توییتر اتحادیه اروپا و منطقه اقتصادی اروپا را در سراسر قاره تحت تأثیر قرار داد. به همین دلیل، ضروری است که مقامات ملی کشورهای مختلف عضو برای اجرای کافی این قانون همکاری کنند. همکاری در اینجا یک عنصر اساسی است چراکه ظرفیت و کیفیت اجرایی را افزایش می‌دهد. صلاحیت حفاظت از ضمانت اجرایی این مقررات عمدتاً بر عهده مقامات ملی است، کمیسیون اروپا هم به تمایل کشورهای عضو برای حفظ این صلاحیت‌ها در سطح ملی احترام می‌گذارد و مزایای عملکردی ارائه می‌دهد زیرا مقامات ملی اغلب به اطلاعات در سطح ملی دسترسی بهتری دارند؛ بنابراین، هم مقررات عمومی حفاظت از داده و هم قانون خدمات دیجیتال مقرر می‌دارند که مقامات ملی کشورهای مختلف عضو، تحت هماهنگی

یک‌نهاد در اتحادیه اروپا همکاری کنند. بااین‌وجود، تجربه مقررات عمومی حفاظت از داده ثابت کرد که برخورد با تخلفات فرامرزی کار چندان ساده‌ای نیست و پیچیدگی چنین ساختارهایی حتی می‌تواند منجر به اجرای ناقص این مقررات شود.

مقررات عمومی حفاظت از داده مکانیسم یک مرحله‌ای را پیشنهاد می‌دهد، به این معنی که اجرای فرامرزی مقررات عمومی حفاظت از داده توسط مقام نظارتی اصلی سازمان‌دهی می‌شود، یعنی مرجعیت با کشور عضوی است که شرکت کنترل‌کننده یا پردازشگر داده، آن را مقر اصلی خود معرفی کرده است. بااین‌حال، همان‌طور که پیش‌تر مورداشاره قرار گرفت، این مکانیسم بار بزرگی را بر دوش برخی از کشورهای عضو همانند، ایرلند و لوکزامبورگ گذاشته است، به دلیل آنکه غول‌های فناوری مقر اروپایی خود را در این دو کشور بنانهاده‌اند. این اتفاق ممکن است منجر به وضعیتی شود که برخی از مقامات نظارتی با عقب‌ماندگی‌های بزرگ و تورم قضایی شدید روبرو شوند زیرا ظرفیت رسیدگی به حجم عظیم پرونده‌های مطروحه علیه تخلفات پلتفرم‌ها را ندارند. مرجع اصلی باید با مقامات سایر کشورهای عضو همکاری کند زیرا اشخاص موضوع داده در کشورهای عضو دیگر نیز تحت تأثیر نقض مقررات قرار می‌گیرند. برای این منظور، مقامات اصلی و ذی‌ربط باید در طول مرحله تحقیق و تصمیم‌گیری به اجماع دست یابند. اگرچه این اجماع نظر امیدوارکننده به نظر می‌رسد، اما ممکن است روند اجرایی را به‌شدت کند نماید. علاوه بر این، مقامات باید اطلاعات را مبادله نموده، کمک متقابل ارائه کنند یا تحقیقات مشترکی را

انجـام دهنـد. بااین‌حـال، مقامـات نظارتـی ملـی حاضـر بـه اسـتفاده از ایـن ابـزار نیسـتند و بنابرایـن تـا پایـان سـال ۲۰۲۰ تنهـا یـک عملیـات مشـترک انجام‌شـده اسـت. بایـد دیـد کـه آیـا گـروه پشـتیبانی کارشناسـان هیئـت حفاظـت از داده اتحادیـه اروپـا جایگزیـن مفیـدی بـرای ایـن مسـئله خواهنـد بـود یـا خیـر. تحـت سیسـتم قانـون خدمـات دیجیتـال، اجـرای فرامـرزی توسـط هماهنگ‌کننـده سـازمان خدمـات دیجیتالـی[1] سـامان‌دهی می‌شـود؛ هماهنگ‌کننـده خدمـات دیجیتـال کشـورهای عضـو کـه شـرکت ارائه‌دهنـده خدمـات دیجیتـال، آن را مرکـز اصلـی یـا نماینـده خـود معرفـی کـرده اسـت.

ایـن مرجـع به‌عنـوان یـک نقطـه تمـاس واحـد بـرای مقامـات ملـی و اتحادیـه اروپـا عمـل می‌کنـد. بااین‌حـال، ممکـن اسـت وظایفـی را بـه مرجـع دیگـری در کشـور عضـو خـود محـول کنـد، بـه ایـن معنـی کـه در یـک کشـور عضـو مقامـات متعـددی می‌تواننـد مسـئول سـازمان‌دهی اجـرای مقـررات فرامـرزی باشـند.

ماده ۳۸ قانون خدمت دیجیتال در این خصوص مقرر می‌دارد:

«هماهنگ‌کننـده خدمـات دیجیتـال موظـف هسـتند تـا بـا یکدیگـر و سـایر مقامـات ذی‌صـلاح ملـی و کمیسـیون همکاری‌هـای لازم را بـه عمل‌آورنـد».

البتـه موضـوع همـکاری به‌انـدازه مقـررات عمومـی حفاظـت از داده «رویـه‌ای سـازی شـده[2] » نیسـت. مـاده ۷۶ قانـون خدمـات دیجیتـال مقـرر مـی‌دارد کـه هماهنگ‌کننـده خدمـات دیجیتالـی کـه شـکایت را دریافـت می‌کنـد، در صـورت نیـاز بـه همـکاری فرامـرزی کـه می‌توانـد شـامل تبـادل اطلاعـات و سـازمان‌دهی تحقیقـات مشـترک (به‌صـورت

1. Digital Services Coordinator
2. proceduralized

دائـم یـا موقـت) باشـد، بایـد مقامـات ذی‌صـلاح و هماهنگ‌کننـدگان خدمـات دیجیتـال سـایر کشـورهای عضـو را درگیـر کنـد و ایـن کار ممکن اسـت از سـازمان‌دهی عملیـات جمع‌آوری داده‌هـا تـا بازرسـی از اماکـن را شـامل شـود. قانـون خدمـات دیجیتـال صراحتـاً در بنـد اول مـاده ۴۵ مقرر مـی‌دارد کـه شـروع درخواسـت اقدامـات اجرایـی فرامـرزی ازاین‌دسـت، ممکـن اسـت توسـط هماهنگ‌کننـده خدمـات دیجیتـال از یـک کشـور عضـو دیگـر یـا هیئـت خدمـات دیجیتـال[1] نیـز باشـد و ایـن ابـزار مهمـی بـرای هماهنگ‌کننـدگان خدمـات دیجیتـال و هیئت‌مدیـره اسـت تـا اقدامـات اجرایـی را انجـام دهنـد.

اجـرای قوانیـن اتحادیـه در مـوارد نقـض مقـررات برون‌مـرزی کـه مقامات کشـورهای مختلـف عضـو را درگیـر می‌کنـد بـه دلایـل متعـددی پیچیـده اسـت؛ بنابرایـن، رویکـرد اروپایـی عمیقـاً نیازمنـد شـیوه‌های اجـرای ترکیبـی اسـت کـه هـم مقامـات و نهادهـای سـطح منطقـه‌ای اتحادیـه اروپا و هـم نهادهـای ملـی را درگیـر می‌کنـد. یـک مـدل از اقدامـات شـبکه‌ای بـا عناصـر متمرکـز فضـای کافـی را در سـطح ملـی بـرای اجـرای اهـداف اتحادیـه اروپـا فراهـم نمـوده، نهادهـای متمرکـز ایـن شـیوه‌های اجرایـی را هماهنـگ کـرده و می‌تواننـد مقامـات ملـی را وادار کننـد تـا به‌گونـه‌ای عمـل کننـد کـه بـه شـیوه‌های اجرایـی مناسـب کمـک کنـد.

هماهنگـی رویه‌هـای عملیاتـی سـازی در سـطح ملـی هـر دو سـند قانـون خدمـات دیجیتـال و مقـررات عمومـی حفاظـت از داده بـه عهـده هیئـت اتحادیـه اروپـا اسـت. در مـورد مقـررات عمومـی حفاظـت از داده، هیئـت حفاظـت از داده اتحادیـه اروپـا (متشـکل از روسـای مقامـات نظارتـی ملـی) و بـرای قانـون خدمـات دیجیتـال، هیئـت خدمـات دیجیتـال اتحادیـه اروپـا

1. the Board for Digital Services

(متشکل از مقامات سطح بالای هماهنگ‌کنندگان خدمات دیجیتال) است. رئیس کمیسیون اروپا در هیئت دوم به‌عنوان رئیس و مسئول ارائه پشتیبانی تحلیلی و اداری نقش بزرگی دارد. علیرغم وجود یک بیانیه امیدوارکننده در قانون خدمات دیجیتال، مبنی بر اینکه هدف اتحادیه اروپا برای خدمات دیجیتال، دستیابی به یک دیدگاه مشترک در اتحادیه برای کاربرد منسجم قانون خدمات دیجیتال است (قانون خدمات دیجیتال، ماده ۸۹)، این هیئت در حقیقت صرفاً یک نقش مشاوره‌ای دارد زیرا باید از هماهنگی مشترک حمایت کرده و تحقیقات و نظرات، درخواست‌ها و توصیه‌هایی را خطاب به مقامات ملی و هماهنگ‌کنندگان خدمات دیجیتال صادر نماید؛ به‌عنوان‌مثال، مستند بر بند اول ماده ۴۹ قانون خدمات دیجیتال؛ نقشه‌های راه یا جداول زمانی برای فعالیت‌های مشترک ارائه کند. بااین‌حال، این راهنمایی ازنظر قانونی الزام‌آور نیست.

هیئت حفاظت از داده‌های اتحادیه اروپا هم ممکن است نظرات، دستورالعمل‌ها و توصیه‌هایی را اتخاذ کند که خطاب به مقامات ملی ارائه می‌شود که در صورت عدم پیروی مقامات ناظر ملی از آن‌ها، بر اساس ماده ۶۵ مقررات عمومی حفاظت از داده، نظرات می‌تواند درنهایت به تصمیمات الزام‌آور تبدیل شوند؛ بنابراین، نفوذ هیئت حفاظت از داده اتحادیه اروپا می‌تواند در عمل بسیار زیاد باشد؛ زیرا هیئت حفاظت از داده‌های اروپا می‌تواند تصمیمات نهایی الزام‌آوری را برای مقامات نظارتی ملی اتخاذ کند - به‌عنوان‌مثال، زمانی که اختلافاتی بین مقامات نظارتی ملی ایجاد می‌شود، بر اساس ماده ۶۵ مقررات عمومی حفاظت از داده. این هیئت اختیار

فیصلـه دادن بـه اختلافـات را دارد[1].

بااین‌حـال، ایـن مکانیسـم بـا اشـکالات جـدی مواجـه اسـت زیـرا هیئـت حفاظـت از داده‌هـا به‌شـدت بـه سـلیقه‌های شـخصی مقامـات نظارتـی ملـی بـرای بـه اشـتراک گذاشـتن اطلاعـات موردنیـاز، وابسـته اسـت و اگـر یـک مرجـع نظارتـی اصلـی نتوانـد موضـوع را به‌انـدازه کافـی بررسـی کنـد، ایـن هیئـت تمـام عناصـر موردنیـاز بـرای تصمیم‌گیـری صحیـح را نخواهـد داشـت. تصمیمـات هیئـت حفاظـت از داده‌هـا به‌طورکلـی چارچـوب منـد و محدودشـده اسـت و در هنـگام اجـرای تصمیـم هیئـت، فضـای زیـادی بـرای مقامـات نظارتـی ملـی باقـی می‌گـذارد.

تحـت قانـون خدمـات دیجیتـال، هیئـت خدمـات دیجیتـال اتحادیـه اروپـا دارای صلاحیت‌هـای اجرایـی قـوی نیسـت، بلکـه خـود کمیسـیون اروپـا ایـن صلاحیـت را دارد؛ به‌عنوان‌مثـال، کمیسـیون اروپـا ممکـن اسـت اختلافـات بیـن هماهنگ‌کننـدگان خدمـات دیجیتـال در مـورد اقدامـات اجرایـی انجام‌شـده را حـل کنـد (اگرچـه قانـون خدمـات دیجیتـال الزامـی نـدارد کـه آن‌هـا بایـد بـه اجمـاع نظـر برسـند.) و در صـورت نیـاز، ممکـن اسـت از هماهنگ‌کننـده خدمـات دیجیتـال درخواسـت کنـد تـا اقدامـات مختلفـی را بـرای اطمینـان از انطبـاق بـا قانـون خدمـات دیجیتـال انجـام دهـد (قانـون خدمـات دیجیتـال، مـاده ۴۵). مشـخص نیسـت اگـر پیگیری‌هـای هماهنگ‌کننـده خدمـات دیجیتـال کافـی نباشـد چـه اتفاقـی می‌افتـد. فقـط در صـورت اقدامـات اجرایـی مرتبـط

به‌منظـور تضمیـن کاربـرد درسـت و سـازگار ایـن مقـررات در مـوارد مختلـف، هیئت‌مدیـره بایـد یـک تصمیـم الـزام‌آور را در مـوارد زیـر اتخـاذ کنـد:
الـف- زمانـی کـه در حالـت اشاره‌شـده در مـاده‌ی ۶۰(۴)نهـاد نظارتـی موردنظـر مخالفـت منطقـی بـا تصمیـم پیش‌نویـس نهـاد پیشـرو داشـته باشـد یـا نهـاد پیـش رو بـه دلیـل منطقـی و وارد نبـودن اختـلاف، آن را رد کنـد. تصمیـم الـزام‌آور بایـد تمامـی موضوعاتـی کـه در مخالفـت منطقـی و مسـتدل، موردبحـث هسـتند، به‌ویـژه مـوارد ناقـض ایـن مقـررات را لحـاظ کـرده باشـد؛ ب- زمانـی کـه دیدگاه‌هـای متضـادی نسـبت بـه شایسـتگی کسـب عنـوان شـعبه‌ی اصلـی بـرای نهادهـای نظارتـی وجـود داشـته باشـد؛ ج- زمانـی کـه نهـاد نظارتـی دارای صلاحیـت در مـوارد منـدرج در مـاده‌ی ۶۴(۱)نظـر هیئت‌مدیـره را جویـا نمی‌شـود یـا ازنظـر هیئت‌مدیـره کـه طبـق مـاده‌ی ۶۴ صادرشـده، پیـروی نکنـد. در ایـن حالـت هـر نهـاد نظارتـی مربوطـه، یـا کمیسـیون می‌توانـد موضـوع را بـه اطـلاع هیئت‌مدیـره برسـاند.

بـا پلتفرم‌هـای آنلایـن بسـیار بـزرگ، کمیسـیون می‌توانـد از طریـق تصمیمـات الـزام‌آور مطابـق بـا «سیسـتم نظـارت پیشـرفته» مداخلـه و بـر اسـاس مـاده ۵۰ قانـون خدمـات دیجیتـال عمـل کنـد. به‌طـور خلاصـه، ایـن قانـون مسـتلزم آن اسـت کـه کمیسـیون اروپـا دارای اختیـارات بسـیار گسـترده‌ای در زمینـه تحقیـق یـا تصمیم‌گیـری بـرای اجـرای برخـی مـواد قانـون خدمـات دیجیتـال در رابطـه بـا غول‌هـای فنـاوری باشـد. در ایـن مـوارد، هماهنگ‌کننـده خدمـات دیجیتـال از قـدرت مداخلـه خـود سـلب می‌شـود.

یکـی از ابتـکارات قابل‌توجـه در قانـون خدمـات دیجیتـال کـه بـر اسـاس تجربـه مکانیسـم یـک مرحلـه‌ای در مقـررات عمومـی حفاظـت از داده انجام‌گرفتـه اسـت، پیشـنهاد کمیسـیون اروپـا بـرای عملیاتـی سـازی یـک مـدل اجرایـی ترکیبـی بـا همـکاری افقـی بیـن مقامـات ملـی تحـت هماهنگـی نهادهـای متمرکـز بـه روشـی متفـاوت از سیسـتم مقـررات عمومـی حفاظـت از داده اسـت. اینکـه آیـا ایـن سیسـتم پاسـخ مناسـبی بـه چالش‌هـای اجرایـی فرامـرزی اتحادیـه اروپـا اسـت یـا خیـر، در آینـده معلـوم می‌شـود. اگرچـه ایـن قانـون تـا حـدی مبتنـی بـر رویـه قضایـی اسـت، امـا نشـان داد کـه همـکاری تحـت مقـررات عمومـی حفاظـت از داده پیچیـده و دسـت‌وپا گیـر اسـت و نقـش هیئـت حفاظـت از داده‌هـا در عمـل بسـیار سسـت و مسـامحه گرانـه اسـت.

اینکـه آیـا اشـکال همـکاری پیشنهادشـده در قانـون خدمـات دیجیتـال - بـدون امـکان درخواسـت کمـک متقابـل یـا تصمیم‌گیـری مشـترک - منجر بـه شـیوه‌های اجرایـی منسـجم و مناسـب می‌شـود یـا خیـر، جـای سـؤال دارد. اگرچـه قانـون خدمـات دیجیتـال، بـرای مثـال، تحقیقـات مشـترک را

پیش‌بینی می‌کند، فرض بر این است که بسیاری از همکاری‌ها از طریق راه‌های غیررسمی سازمان‌دهی می‌شود. ازیک‌طرف، اشکال غیررسمی و غیر سلسله مراتبی همکاری منجر به تعامل بیشتر بین مقامات شده و یادگیری را افزایش می‌دهد و اعتماد را در بین اعضای این شبکه ایجاد می‌کند که برای مؤثر بودن همکاری ضروری است(Polak,۲۰۱۶).

از سوی دیگر، رویه‌های غیررسمی هم پاسخ سریع به نقض قانون خدمات دیجیتال را تقریباً غیرممکن می‌سازد، زیرا عوامل بسیاری درگیر کار می‌شوند (مانند هماهنگ‌کنندگان خدمات دیجیتال، سایر مقامات ذی‌صلاح، هیئت خدمات دیجیتال اتحادیه اروپا و کمیسیون اروپا). در این مورد، اهمیت رسمی‌سازی این فرایند توسط ناظر حفاظت از داده‌های اروپا احساس می‌شود، چراکه با ارجاعات صریح‌تر به مقامات ذی‌صلاح و مورد شناسایی قرار دادن شرایط و چارچوبی که در آن همکاری باید انجام شود، از عملیاتی سازی دقیق قانون حمایت کند.

جمع‌بندی

جمع‌بندی

داده‌ها یکی از ارزشمندترین دارایی‌های عصر دیجیتال هستند. آن‌ها چه در کنار همدیگر و به‌صورت تجمیع شده و چه به شکل مجزا، معنادار، ذی‌قیمت و راهبردی هستند. داده‌ها منجر به ایجاد تحولی عظیم در صنایعی همچون تبلیغات و خلق تجارت‌های غول‌آسایی همچون پردازش داده شده‌اند. طبقه‌بندی آن‌ها می‌تواند منجر به شکل‌گیری اطلاعات فوق‌العاده استراتژیک شده و شناخت عمیقی از شخص یا اشخاص موضوع داده به دست دهد. این موارد، صرفاً بخش کوچکی از اهمیت داده‌ها بود و بر همین اساس، از نخستین روزهای تجاری‌سازی اینترنت و تولید داده توسط کاربران، برخی از مجموعه‌ها به شکل متمرکز و تخصصی اقدام به جمع‌آوری و پردازش داده‌های کاربران نمودند. تجمیع داده‌ها در دست شرکت‌ها فناوری، منجر به بر هم خوردن توازن قدرت در صنعت فناوری و قدرت خلق ارزش‌افزوده شد و غول‌های فناوری رفته‌رفته با روشن شدن زوایای پنهان ارزش داده‌ها به سمت شکل دادن یک انحصار تمام‌عیار برای در اختیار داشتن داده‌ها رفتند؛ به‌عبارت‌دیگر، درک ارزشمندی و خطیر بودن داده‌ها میان شرکت‌های فناوری و دولت‌مردان به‌موازات

همدیگر پیش نرفت و دولت‌ها خیلی دیر به فکر ساماندهی داده‌های شخصی کاربران و حفاظت از آن‌ها افتادند. بااین‌وجود، در هر مرحله‌ای این اقدام یک نیاز حیاتی برای هر کشوری بوده و بی‌توجهی نسبت به آن منجر به شکل‌گیری زیان‌های جبران‌ناپذیری خواهد شد.

تنظیم‌گری حقوق داده‌ها به شکل مستقیم تحت تأثیر سیاست‌های حکمرانی بر فضای مجازی هر کشوری قرار دارد. ابرقدرت‌ها و بازیگران مؤثر فضای مجازی، بر اساس نوع نگاه و نظام ارزشی خود، نظام حکمرانی برداده مخصوص به خود را تشکیل می‌دهند و نوع مواجهه هر دولت با داده، به‌خوبی بیانگر اندیشه‌ها و سیاست‌های آن دولت نسبت به فضای مجازی، حقوق و آزادی‌های شهروندی است. اتحادیه اروپا به‌عنوان یک نظم منطقه‌ای، دارای ارزش‌های مخصوص به خود است که سعی نموده در طول دهه‌های گذشته آن‌ها را میان ملت‌های اروپایی به‌عنوان ارزش جمعی نهادینه کند. این ارزش‌ها به‌خوبی خود را در مقررات عمومی حفاظت از داده نمایان ساخته است. حریم خصوصی، به رسمیت شناسی حقوق نوپدیدی همچون حق بر فراموشی، حق قابلیت نقل‌وانتقال داده و از همه مهم‌تر تلقی داده به‌عنوان یک کالا، بیانگر ارزش‌های اروپایی است. سخت‌گیری‌هایی که در محافظت از داده‌های شخصی کاربران نیز در قالب تکالیف مختلف بر شرکت‌ها تحمیل می‌شود، در همین راستا است.

اتحادیه اروپا با مقررات عمومی حفاظت از داده به دنبال آن بود که تبدیل به یک الگوی مسلط در حکمرانی بر داده شده و با بهره‌مندی از اثر بروکسل، رویکرد خود نسبت به داده را

جهانی‌سازی کند. با توجه به آنچه در این نوشتار موردبررسی قرار گرفت، مشخص شد که اروپا در تحقق اهداف خود آن‌چنان‌که توقع می‌رفت، موفق نبوده و بر همین اساس، باگذشت ده سال از تهیه و تنظیم پیش‌نویس مقررات عمومی، به دنبال ایجاد یک تحول عمیق و برداشتن گام‌های جدیدتر است. در این میان، نکته مهم و قابل‌توجه آن است که علی‌رغم آنکه گفته می‌شود فضای مجازی سبب شکل‌گیری الگوها، رفتارها، چالش و مشکلات مشابه و واحد و از سوی دیگر، راه‌کارها، راه حل‌ها و روش‌های حل مسئله مشابه و واحد می‌شود، تجربه مقررات عمومی به‌خوبی ثابت کرد که هنگام سیاست‌گذاری، قانون‌گذاری و تنظیم‌گری، نمی‌توان برای تمامی کشورها نسخه‌ای واحد پیچید و تفاوت‌ها، تمایزات و پتانسیل‌ها و زیرساخت‌های هر کشور را باید در نظر داشت و متناسب یا همان سطح برای آن تصمیم‌گیری نمود.

منابع

منابع

1. https://dma.org.uk/uploads/misc/5b0522b113a-23 global-data-privacy-report---final5_2-b0522b11396e.pdf
2. https://www.pinsentmasons.com/out-law/news/pre-ticked-cookie-consent-boxes-prohibited
3. (www.dw.com), D. (2022). Cyber-crime is Europe›s ‹big challenge› | DW Learn German. Retrieved 14 August 2022, from https://learngerman.dw.com/en/cyber-crime-is-europes-big-challenge/a15988087-
4. “Massachusetts Woman Sues over Gmail Snooping - CNET.” CNET, www.cnet.com, 10 Aug. 2011,https://www.cnet.com/tech/services-and-software/massachusetts-woman-sues-over-gmail-snooping/.
5. Analyst Report: What Iot Means for Consumer Privacy | Forge Rock. (2022). Retrieved 14 August 2022, from https://www.forgerock.com/resources/view/68775648/analyst-report/what-iot-means-for-consumer-privacy.pdf
6. Analyst Report: What Iot Means for Consumer Privacy | Forge Rock. (2022). Retrieved 14 August

2022, from https://www.forgerock.com/resources/view/68775648/analyst-report/what-iot-means-for-consumer-privacy.pdf
7. Analyst Report: What Iot Means for Consumer Privacy | Forge Rock. (2022). Retrieved 15 August 2022, from https://www.forgerock.com/resources/view/68775648/analyst-report/what-iot-means-for-consumer-privacy.pdf
8. Araujo, T., Helberger, N., Kruikemeier, S. et al. In AI we trust? Perceptions about automated decision-making by artificial intelligence. AI & Soc 2020) 623–611 ,35). https://doi.org/10.1007/s-00931-019-00146w
9. Civil Society and the Challenge of Resistance to Corporate Connectivity Projects. – Global Media Technologies and Cultures Lab. (2022). Retrieved 16 August 2022, from https://globalmedia.mit.edu/21/04/2020/the-rise-and-fall-and-rise-again-of-facebooks-free-basics-civil-and-the-challenge-of-resistance-to-corporate-connectivity-projects/#:~:text=In20%early2%202016%C20%Free20%Basics,up20%to20%20100%million20%people.
10. Commission, E. (2022). Euro barometer. Retrieved 15 August 2022, from https://europa.eu/eurobarometer/surveys/detail/2249
11. Data privacy, consent fatigue, and GDPR - Marketoonist | Tom Fishburne. Marketoonist | Tom Fishburne -

Marketoonist Is the Thought Bubble of Tom Fishburne. Marketing Cartoons, Content Marketing with a Sense of Humor, Keynote Speaking. https://marketoonist.com/05/2019/data-privacy-consent-fatigue-and-gdpr.html

12. Facebook Risk From Europe›s Data Privacy Law Bigger Than Google›s, Retrieved 16 August 2022, from https://www.investors.com/news/technology/facebook-risk-bigger-than-googles-from-europes-consumer-privacy-law/

13. Facebook Users by Country 2022) .2022). Retrieved 16 August 2022, from https://worldpopulationreview.com/country-rankings/facebook-users-by-country

14. Germany: Land of Data Protection and Security – But Why? (2022). Retrieved 16 August 2022, from https://www.dotmagazine.online/issues/security/germany-land-of-data-protection-and-security-but-why

15. https://wayback.archive-it.org/3/12090/https://ec.europa.eu/digital-single-market/en/news/special-eurobarometer-europeans-attitudes-towards-cyber-security

16. Machine Bias.). Retrieved 21 August 2022, from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

17. ‹Mega› Data Breaches Cost Companies a Staggering Fortune. (2018). Retrieved 14 August 2022, from https://

gizmodo.com/mega-data-breaches-cost-companies-a-staggering-fortune1827510737-
18. MEPs call for infringement procedure against Ireland. (2021). Retrieved 13 August 2022, from https://www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/
19. Polak, J. The virtues of interdependence and informality: an analysis of the role of transnational networks in the implementation of EU directives. New Directions in the Effective Enforcement of EU Law and Policy, 129-105. doi: 9781784718695.00015/10.4337
20. Rosenthal, M. (30 .(2022 Biggest GDPR Fines To-Date | Latest GDPR Fines | Updated 2022 | Tessian. Retrieved 13 August 2022, from https://www.tessian.com/blog/biggest-gdpr-fines- Also see: Masha Komnenic CIPP/E, F. (36 .(2022 Biggest GDPR Fines & Penalties So Far [2022 Update]. Retrieved 13 August 2022, from https://termly.io/resources/articles/biggest-gdpr-fines/
21. Shah, S., & Shah, S. (2017). More than two-thirds of consumers are concerned about IoT device security. Retrieved 14 August 2022, from https://internetofbusiness.com/consumers-iot-device-security/
22. Survey: 68 Percent of U.S. Consumers Fear Brands Put Their Personal Data at Risk. Retrieved 15 August 2022, from https://www.globenewswire.com/news-release

23. Telecom paper. (2022). Retrieved 14 August 2022, from https://www.telecompaper.com/partner-content/the-next-generation-of-connected-experience-precision-protection-and-personalization1261782--
24. The 4 Dimensions of Digital Trust, Charted Across 42 Countries. (2018). Retrieved 16 August 2022, from https://hbr.org/02/2018/the-4-dimensions-of-digital-trust-charted-across-42-countries
25. The CNIL›s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC(2019), Retrieved 13 August 2022, from: https://edpb.europa.eu/news/national-news
26. The Irish Data Protection Commission (DPC)
27. Wave of Legal Appeals Challenges How European Regulators Enforce Privacy Rules(2021), Retrieved 13 August 2022, from: https://www.wsj.com/articles/wave-of-legal-appeals-challenges-how-european-regulators-enforce-privacy-rules11615800602-?reflink=desktopwebshare_permalink
28. Why are High Growth Companies choosing Ireland as a location? (2022). Retrieved 13 August 2022, from https://www.nathantrust.com/insights/why-are-high-growth-companies-choosing-ireland-as-a-location
29. Witteman, E. (2021). Criticism of Irish privacy authority for slow GDPR action. Retrieved 21 August 2022, from https://www.techzine.eu/news/privacy-

compliance/57666/criticism-of-irish-privacy-authority-for-slow-gdpr-action/

۳۰. بسته خدمات دیجیتال اتحادیه اروپا تصویب شد؛ سایه قوانین جدید تنظیم‌گری بر سر غول‌های تکنولوژی – بینو. (۱۴۰۱).
from https://bino.ir/ ,2022 August 27 Retrieved /6495/6495/content

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب خروشان است که می‌آید و دائما هم بر آب آن افزوده و خروشان تر می‌شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

csri.ac.ir