**Original Article**

# Ethical Dimensions of General Data Protection regulations and its Impact on Iran's Regulations and Citizenship Rights in Cyberspace

**Ali Arman[1], Akbar Varvaee[2*], Mohammed Javad Jafari[3]**

1. PhD Candidate, Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.
2. Professor, Faculty Member of Amin University of Police, Tehran, Iran. (Corresponding Author)
Email: Akbar.varvaee@yahoo.com
3. Assistant Professor, Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.

Received: 26 Jul 2018 Accepted: 2 Dec 2018

**Abstract**

**Background and Aim:** Digital world as well as cyberspace are undergoing a rapid change and evolution. Emerging new technologies like artificial intelligence, machine learning and robotics have raised fundamental ethical challenges related to the privacy and data protection in virtual space by the controllers. This study explains general data protection regulations (GDPR) and then analyzes its impact on Iran's regulations and citizenship rights in cyberspace.

**Materials and Methods:** In this analytical study, using library method, the ethical dimensions of privacy and protection of cyber data are discussed and analyzed.

**Findings:** The study of the GDPR and the compilation of country-specific laws based on religious principles showed that combining these two perspectives could reduce abusing and doing crime in cyberspace. Therefore, these ethical and legal considerations should be included in the laws of the majority of countries, and in particular the Islamic Republic of Iran, based on the GDPR.

**Conclusion:** These ethical concerns and responsibilities should be included in the laws of most countries, in particular the Islamic Republic of Iran, in the near future by the authorities, based on the provisions of the GDPR. Also, training staff on cyber security, the use of relevant security software and the provision of free educational resources can be effective in preventing crime and utilizing cyber-space, especially in financial matters.

**Keywords:** Ethics; Privacy; Cyber Space; General Data Protection Regulations (GDPR)

**Please cite this article as:** Arman A, Vervayi A, Jafari MJ. Ethical Dimensions of General Data Protection regulations and its Impact on Iran's Regulations and Citizenship Rights in Cyberspace. *Bioethics Journal* 2018; 8(30): 119-136.

**مقاله پژوهشی**

# ابعاد اخلاقی مقررات حفاظت اطلاعات عمومی و تأثیر آن بر قوانین ایران و حقوق شهروندی در فضای سایبر

**علی آرمان[۱]، اکبر وروایی[۲*]، محمدجواد جعفری[۳]**

۱. دانشجوی دکتری حقوق کیفری و جرم‌شناسی، دانشگاه آزاد اسلامی واحد کرمانشاه، کرمانشاه، ایران.

۲. استاد، دانشگاه پلیس، تهران، ایران. (نویسنده مسؤول) Email: Akbar.varvaee@yahoo.com

۳. استادیار، دانشگاه آزاد اسلامی واحد کرمانشاه، کرمانشاه، ایران.

دریافت: ۱۳۹۷/۵/۷ پذیرش: ۱۳۹۷/۹/۱۱

**چکیده**

**زمینه و هدف:** دنیای دیجیتال و فضای سایبری به سرعت در حال تغییر و تحول می‌باشد. ظهور فناوری‌های جدید مانند هوش مصنوعی، یادگیری ماشین و رباتیک، چالش‌های اخلاقی جدیدی را در ارتباط با حفظ حریم خصوصی و حفاظت از داده‌ها به فضای سایبر توسط کنترل‌کننده‌ها ایجاد نموده است. در این مطالعه ابتدا مقررات حفاظت اطلاعات عمومی (GDPR) توضیح داده شده و سپس ابعاد اخلاقی حفظ حریم خصوصی و حفاظت از داده‌ها و تأثیر آن بر حقوق شهروندی و مقررات ایران در فضای سایبری تحلیل می‌گردد.

**مواد و روش‌ها:** در این مطالعه تحلیلی، با استفاده از روش کتابخانه‌ای به جمع‌آوری و مطالعه پژوهش‌ها و کتب انتشاریافته، ابعاد اخلاقی حفظ حریم خصوصی و حفاظت داده‌های سایبری مورد بحث و تحلیل قرار گرفت.

**یافته‌ها:** مطالعه مقررات حفاظت اطلاعات عمومی و تدوین قوانین موضوعه کشور بر اساس اصول شرعی نشان داد که با ترکیب این دو دیدگاه می‌توان راه را برای جلوگیری از سوءاستفاده و به حداقل‌رسانی ارتکاب جرم در فضای سایبری کاهش داد. بنابراین این ملاحظات اخلاقی و حقوقی می‌بایست در قوانین موضوعه اکثر کشورها و خصوصاً جمهوری اسلامی ایران، مبتنی بر مقررات حفاظت اطلاعات عمومی (GDPR) گنجانده شود.

**نتیجه‌گیری:** این دغدغه‌ها و مسؤولیت‌های اخلاقی بایستی در آینده نه‌چندان دور در قوانین اکثر کشورها، خصوصاً جمهوری اسلامی ایران، توسط مقامات مذکور و مبتنی بر مقررات حفاظت اطلاعات عمومی (GDPR)، در قوانین موضوعه آن‌ها گنجانده شود. همچنین آموزش کارکنان درباره امنیت فضای سایبری، استفاده از نرم‌افزارهای فعال امنیتی مرتبط و ارائه منابع آموزشی رایگان می‌تواند در جلوگیری از جرم و سوءاستفاده فضای سایبر خصوصاً در مسائل مالی تأثیرگذار باشد.

**واژگان کلیدی:** اخلاق؛ حریم خصوصی؛ فضای سایبری؛ مقررات حفاظت اطلاعات عمومی (GDPR)

**مقدمه**

داده‌ها به سرعت در حال تبدیل‌شدن به شاهرگ حیاتی اقتصاد جهانی هستند. در عصر کلان داده‌ها و هوش مصنوعی، داده می‌تواند هم به عنوان فرصت و هم به عنوان تهدید مطرح گردد (۱). با توجه به این‌که ارائه‌دهنده داده نوع جدیدی از دارایی اقتصادی است، می‌توان با مدیریت صحیح، منسجم، هدفمند، یکپارچه و به کارگیری یک تفکر راهبردی، آن را به یک مزیت رقابتی تبدیل کرد. عدم مدیریت مناسب داده‌ها، خصوصاً در مواردی نظیر حفظ حریم خصوصی و حفاظت از داده‌های محرمانه و حساس مشتریان، می‌تواند به شهرت و اعتبار یک سازمان آسیب برساند و استمرار کسب و کار یک بنگاه اقتصادی را با چالش جدی مواجه نماید.

جامعه دیجیتالی با ظهور تکنولوژی‌های جدید همچون هوش مصنوعی و یادگیری ماشین، رباتیک و اینترنت اشیا به سرعت در حال تغییر است. این تغییرات، سؤالات اخلاقی اساسی جدیدی را که مرتبط با حریم خصوصی و حفاظت اطلاعات است، برمی‌انگیزد (۲).

«مقررات حفاظت اطلاعات عمومی» در اصل بر حفاظت داده‌ها تأثیر می‌گذارد. این مقررات همچنین به طور کلی قوانینی را، به منظور حفاظت از داده‌ها و حقوق اساسی افراد، ایجاد می‌کند که باعث جلوگیری از سوء استفاده از حریم خصوصی آن‌ها می‌شود که ممکن است توسط کنترل‌کننده‌ها در فضای سایبر انجام شود. علاوه بر این، مسائل اخلاقی به طور فزاینده‌ای در جامعه حفاظت داده‌ها شناسایی می‌شوند (۳). ابتکار عمل ( EDPS: European Data Protection Supervisor) با شروع از یک ایده برای مسائل اخلاقی دیجیتالی و ایجاد یک گروه مشورتی اخلاقی، فقط یکی از نمونه‌های مربوط به یک گرایش گسترده‌تر است (۴). نمونه‌های اخلاقی بیشتر، بعداً و با الگوبرداری از قانون عمومی حفاظت از داده اتحادیه اروپا ارائه خواهند شد.

این مقاله، ابعاد اخلاقی حریم خصوصی و حفاظت داده‌ها و حوزه‌ای که «مقررات حفاظت اطلاعات عمومی»، اصول اخلاقی را در ارتباط با این توسعه‌ها در نظر می‌گیرد، بررسی می‌کند و به مشاهداتی خلاصه می‌شود که به طور صریح به دنبال مسؤولیت‌پذیری و پاسخگویی افرادی می‌باشد که به گونه‌ای با حریم خصوصی افراد سر و کار دارند و باید بر اساس آن‌ها، قضاوت‌های اخلاقی را انجام دهند، مانند دولت‌ها، مسؤولین حفاظت داده‌ها (Data Protection Acts) و کمیته‌های اخلاقی. کنترل‌کننده‌ها دلایل مختلفی را برای پردازش داده‌های مشتریان (کنترل‌شونده‌ها) دارند، اما در برخی موارد کنترل‌کننده داده برخلاف اخلاق اقدام به سوء استفاده از داده‌های کاربران کرده و به امنیت این فضا خدشه وارد می‌نمایند. در مقابل، هم اتحادیه اروپا در قوانین جدید خود مجازات‌های شدیدی برای آن‌ها در نظر گرفته است. ما ابتدا از مقررات حفاظت اطلاعات عمومی اتحادیه اروپا بحث می‌کنیم و در نهایت هم راه‌کارهای استنباط‌شده را برای کاربرد در قوانین کشور خودمان مورد بحث قرار می‌دهیم تا راه گشایشی برای اینده در این موضع اساسی و حیاتی باشد.

**مواد و روش‌ها**

در این پژوهش تحلیلی سعی شده تا با استفاده از شیوه کتابخانه‌ای و جمع‌آوری و مطالعه مقالات و کتب، ابعاد اخلاقی حفظ حریم خصوصی و حفاظت داده‌های سایبری و میزان تأیید و تعهد اخلاق در رابطه با این تحولات و مصادیق آن، مورد بحث و تحلیل قرار گیرد.

**تعاریف**

فضای سایبر یا «سایبراسپیس (Cyber Space)» از لحاظ لغوی در فرهنگ‌های مختلف «Cyber» به معنی مجازی و غیر ملموس و مترادف لغت انگلیسی Virtual است.

به چند نمونه از تعاریف سایبراسپیس در سطح بین‌المللی توجه کنید:

ـ «سایبراسپیس» مجموعه به هم پیوسته موجودات زنده از طریق کامپیوتر و ارتباطات راه دور است، بدون در نظرگرفتن جغرافیای عینی (۵).

ـ «سایبراسپیس» اثر فضا و اجتماعی است که توسط کامپیوتر، شبکه‌های کامپیوتری و کاربران شکل گرفته است.

به عبارت دیگر یک دنیای مجازی است که کاربران اینترنت وقتی (Online) هستند، موجودیت پیدا می‌کنند (۶).

با توجه به توضیحات فوق و تعاریفی که از متخصصان بیان شد، می‌توان سایبراسپیس را چنین تعریف نمود: «محیطی مجازی و غیر ملموس، موجود در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و... به صورت فیزیکی و ملموس وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) که به شکل دیجیتالی در دسترس استفاده‌کنندگان و کاربران است.

جنبه‌های منفی و مثبت آن بسیار است، اما جنبه نگران‌کننده سایبر انتشار فوق‌العاده سریع اطلاعات در آن است، مثلاً در لحظه کوتاهی قسمتی از اطلاعاتی که می‌تواند به طور بالقوه مورد سوء استفاده قرار گیرد، در این فضا گسترش پیدا می‌کند (۷).

**۱ـ جرائم در سایبراسپیس (Cyber Crime)**

در محیط سایبر افراد با هویت‌های غیر واقعی و تنها بر اساس تخیلات شخصی در محیط رسانه‌ای اینترنت حاضر می‌شوند و خود را در هر قالب و با هر عنوانی معرفی کرده و با دیگران ارتباط برقرار می‌کنند. امروزه در هر نقطه‌ای از دنیا با هر عنوان، شغل و سلیقه‌ای می‌توان در قالب یک شخص موجه ظاهر شد و دوست‌یابی و تبادل افکار کرد و یا حتی به معاملات تجاری کلان دست زد. حضور پررنگ و بی‌شمار افراد مختلف و از قشرهای گوناگون جامعه، در شبکه‌های بین‌المللی (اینترنت) باعث شده است انواع جدیدی از جرائم کامپیوتری وارد فرهنگ حقوق جزا شود.

برای مثال می‌توان به: ۱ـ جرائم سنتی در محیط دیجیتال شامل جاسوسی، سابوتاژ، جعل، کلاه‌برداری، تخریب، افترا، تطهیر نامشروع پول کامپیوتری (Cyber Laundering) و قاچاق، پورنوگرافی کودکان؛ ۲ـ جرائم مدرن شامل جرائم علیه حمایت از داده‌ها، جرائم در تجارت الکترونیک، جرائم مخابراتی و ماهواره‌ای و... اشاره کرد.

**۲ـ داده**

به اعداد، حروف و علائم که جهت درک و فهم مشترک از انسان‌ها با رایانه سرچشمه می‌گیرند، داده می‌گویند. به طور کلی داده‌ها مجموعه‌ای از نمادها (برای انسان حروف، اعداد، علائم و برای رایانه رمزهای صفر و یک) هستند که حقایق را نشان می‌دهند و برای انسان از طریق رسانه‌های وی (بینایی، شنوایی، چشایی، بویایی، بساوایی) و برای رایانه از طریق لوازم ویژه (صفحه کلید موس و...) به دست می‌آیند (۸).

**۳ـ GDPR**

مقررات حفاظت اطلاعات عمومی یا GDPR ( General Data Protection Regulations)، قانون حفاظت داده در سطح اتحادیه اروپاست که جایگزین دستورالعمل «حفاظت از اطلاعات اتحادیه اروپا»، تدوین‌شده در سال ۱۹۹۵ شده است. قانون فوق، برای هماهنگی قوانین حفظ حریم خصوصی در سراسر اروپا و با هدف محافظت و توانمندسازی حریم خصوصی داده‌های شهروندان و تحول در شیوه برخورد سازمان‌ها، با رویکرد حریم خصوصی داده‌ها، در سراسر اتحادیه اروپا ایجاد شده است. این مقررات ماحصل چندین سال مذاکره است. اولین پیشنهاد در سال ۲۰۱۲ ارائه گردید و نسخه نهایی آن در ۱۴ آوریل ۲۰۱۶ توسط پارلمان اتحادیه اروپا تصویب شد. تمامی اعضای اتحادیه اروپا و بنگاه‌های اقتصادی، مرتبط با هر یک از کشورهای اتحادیه، ملزم شدند که تا ۲۸ می ۲۰۱۸ خود را با قوانین و دستورالعمل‌های آن تطبیق نمایند.

**دستورالعمل مقامات قضایی کیفری و پلیس (دستورالعمل حفاظت از اطلاعات)**

دستورالعمل جدید مقامات قضایی کیفری و پلیس، تبادل اطلاعات روان‌تری را میان پلیس کشورهای عضو و مقامات قضایی اجازه می‌دهد. مقامات مجری قانون کیفری، دیگر مجموعه‌های مختلف قوانین حفاظت از اطلاعات را، با توجه به منشأ اطلاعات شخصی، اعمال نخواهند کرد. این امرباعث ذخیره‌سازی زمان و پول ذخیره خواهد شد و بهره‌وری در مبارزه با جرم را افزایش خواهد داد. داشتن قوانین هماهنگ

در تمامی کشورهای عضو اتحادیه اروپا، کار را برای نیروهای پلیس در همکاری با یکدیگر آسان‌تر می‌سازد.

**ابعاد اخلاقی حریم خصوصی و حفاظت داده‌ها**

قوانین مشخص می‌کنند که چه چیزی باید یا نباید انجام شود. می‌تواند انجام شود یا نمی‌تواند انجام شود. مفاهیم اخلاقی درباره رفتار خوب و بد، پشت این قیدها قرار می‌گیرند. قوانین حفاظت داده‌ها از این نظر با هم تفاوتی ندارند، چون آن‌ها بر اساس مفاهیم اخلاقی هستند که حقوق اساسی حریم خصوصی و حفاظت داده‌ها را پشتیبانی می‌کنند.

ـ چیزی که «مقررات حفاظت اطلاعات عمومی» و نسل‌های قبلی قوانین حفاظت داده‌ها در قانونگذاری ایجاد می‌کند، به کارگیری اصول اخلاقی می‌باشد، هرچند برجسته بودن، روشن‌بودن و وضوح آن‌ها در میان مقررات مدون و مقالات مختلف ارائه‌شده متناوب و قطعی است، اما علاوه بر این، طیف وسیعی از اصول اخلاقی که «مقررات حفاظت اطلاعات عمومی» می‌توانست به آن دست یابد، خیلی وسیع و درخور توجه نیست.

ـ منشور حقوق اساسی اتحادیه اروپا (Charter) «کرامت و هویت انسان» را تصدیق می‌کند. همانطور که در ماده ۱ آمده است. " کرامت انسانی غیر قابل انکار است و باید مورد احترام و محافظت قرار گیرد. کرامت انسانی نه‌تنها یک اصل اخلاقی و بنیادین منشور است، بلکه یک ارزش اساسی تحت حریم خصوصی و حفاظت داده‌ها نیز هست. برابر مقررات حفاظت از داده‌های اروپاییان EDPS ( European Data Protection Supervisor)، کرامت انسانی، محرک اصلی برای پرداختن به اصول اخلاقی به طور صریح بود که در این مقاله، این ادعای اخلاقی را باید به عنوان «اکوسیستم» حفاظت از داده‌ها در نظر گرفت (۹).

ـ «عزت و کرامت» در «مقررات حفاظت اطلاعات عمومی» تنها یک بار آن هم در ماده ۸۸ در مورد «پردازش» در زمینه مفهوم اشتغال ذکر شده است. ماده ۴ شامل یک ارجاع اخلاقی خیلی کلی است که می‌گوید: «پردازش‌کردن داده‌های شخصی باید برای خدمت‌کردن به بشر طراحی شود.» از سوی دیگر، تأکید «مقررات حفاظت اطلاعات عمومی» برای احترام به حقوق و آزادی‌های اساسی افراد طبیعی، یک موضوع جهانی است و این مقررات حق بنیادین حفاظت داده‌ها را در تعدادی از حقوق جزئی از مبحث داده‌ها مشخص می‌کند ( Chapter III of the GDPR).

ـ مفهوم عدالت، در این زمینه، یک نقش کلیدی دارد. عدالت یک بُعد اخلاقی دارد که برای نیازمندی‌های، قانونی برای حفاظت داده‌ها، در قوانین بین المللی و اتحادیه اروپا و همچنین قوانین ملی اهمیت دارد. منشور ماده ۸ نیازمند پردازش‌کردن عدالت است، در حالی که در ماده ۵(۱)(a) آن را شرح می‌دهد و موضوع را به شفافیت، ارتباط می‌دهد، اگرچه آن موضوع می‌تواند به این شکل مورد بحث باشد که شفافیت یک عنصر از عدالت و یا یک نیازمندی جداگانه است. در هر موردی، عدالت مفهومی خیلی پیچیده و مبهم است و ارتباط آن با اصول دیگر می‌تواند به روش‌های مختلفی دیده شود (ما در مورد عدالت، دوباره بحث می‌کنیم) (۱۰).

ـ یکی دیگر از قواعد کلی، احترام به حاکمیت قانون است که منعکس‌کننده ریشه‌های اخلاقی و قانونی اتحادیه اروپا و کشورهای عضو آن است. با توجه به این‌که پردازش اطلاعات شخصی همیشه باید بر پایه قانون متکی باشد، احترام به حاکمیت قانون در قوانین حفاظت از داده‌ها منعکس می‌شود. ما به ماده ۸ منشور و ماده ۶ «مقررات حفاظت اطلاعات عمومی» اشاره می‌کنیم. این مقررات، اصول حفاظت داده‌های سنتی ایجادشده در اسناد برجسته‌ای را، همچون اصول سازمان همکاری اقتصادی و توسعه، ( OECD: Organization for Economic Co-operation and Development) متعلق به سال ۱۹۸۰ و کنوانسیون ۱۰۸ شورای اروپا متعلق به سال ۱۹۸۱ که بر اساس دستورالعمل ۴۶/۹۵ حفاظت از داده‌ها (Data Protection Directive) (این دستورالعمل) و قوانین ملی است، به کار می‌گیرد.

این اصول نیاز دارند که داده‌های شخصی، به صورت عادلانه و به طور مشروع برای یک هدف معتبر دقیق، مرتبط و آپدیت شده، جمع‌آوری شوند.

ـ «مقررات حفاظت اطلاعات عمومی» بیشتر به حوزه امور اخلاقی وارد می‌شود و به اصولی تأکید دارد که قبلاً، زیاد برجسته نبودند. این‌ها شامل شفافیت (یا بازبودن) و مسؤولیت‌پذیری می‌شوند که هر دوی آن‌ها به رابطه اخلاقی و کاربردی بین کنترل‌کننده‌ها و پردازنده‌های داده‌های شخصی و اشخاص می‌پردازند و اصول OECD را منعکس می‌کنند. از طرف دیگر به نظر می‌رسد که «مقررات حفاظت اطلاعات عمومی» فراتر از مسائل مربوط به حفاظت از حقوق فردی است و به منظور جلب توجه به سمت منافع اجتماعی عمومی، به حفاظت از قوانین شخصی، ظاهر می‌شود. همانطور که به عنوان مثال ماده ۵۷(۱)(b) انجام می‌شود که می‌گوید «یک مسؤول نظارتی باید آگاهی عمومی خود و درک ریسک‌ها، دستورات، حفاظت‌ها و قوانین را در ارتباط با پردازش‌کردن داده‌ها، ارتقا بدهد.» این عمل و رفتار، فعلی را در نظر می‌گیرد که مقامات نظارتی برای سال‌ها، به عنوان مربیان اجتماعی، در ارتقای آگاهی عمومی به عنوان بخشی از وظایف خود مشغول به آن بوده‌اند، اگرچه این نقش در دستورالعمل مشخص نشده است.

دلایل کاربردی زیادی برای بالابردن سطح فهم عمومی درباره پردازش‌کردن اطلاعات وحقوق وجود دارد، اما یک بعُد اخلاقی نیز وجود دارد و آن بالارفتن آگاهی عمومی است که می‌تواند برای شکل‌دادن شرایط اجتماعی و یک اکوسیستم برای حریم خصوصی و حفاظت داده‌ها مشارکت کند که در عصر اطلاعات به عنوان عملی «خوب» در نظر گرفته می‌شود (۱۱).

**نظارت: تأثیر اخلاقی ان بر روی انسان‌ها**

یک موضوع کلیدی، نظارت است که توسط تکنولوژی، تسهیل و امکان‌پذیر می‌شود. نظارت یا مانیتورکردن افراد، از جمله پردازش‌کردن داده‌های شخصی آن‌ها توسط عوامل تجاری، حکومتی و اجتماعی، به دلایل مختلفی به کار گرفته می‌شود که بر روی ارزش‌های اخلاقی و اجتماعی، از جمله حریم خصوصی، تأثیر دارد.

گری تی مارکس در دفاع از یک اصل اخلاقی جدید برای «نظارت جدید» (۱۲) بحث می‌کند، چون دغدغه‌های اخلاقی «فراتر از قوانین رویه‌ای» تمایلی به رشد درمورد جمع آوری اطلاعات یا فعالیت‌های نظارتی ندارند او سه ناحیه گسترده از اهمیت را شناسایی کرد: ۱ـ ابزارهایی که داده‌ها را جمع‌آوری می‌کنند؛ ۲ـ زمینه‌هایی که در آن‌ها این فرایندها انجام می‌شود؛ ۳ـ کاربردها، مقاصد یا اهدافی که برای آن‌ها داده‌ها جمع‌آوری می‌شود یا توسط آن‌ها افراد ردیابی، نظارت، دیده، شنیده یا تشخیص داده می‌شوند.

درون این ناحیه‌ها، مارکس تعدادی سؤال اخلاقی مطرح کرده تا درباره سیستم‌های نظارتی پرسیده شوند. بعضی از سؤالات تحریک‌آمیز ـ و سیاسی ـ که او می‌پرسد، برابری و عدالت را به عنوان دغدغه اصلی در نظر می‌گیرد: آیا این ابزارها به طور گسترده‌ای فقط برای افراد ثروتمند، قدرتمند یا متخصصان تکنولوژی در دسترس هستند یا محدود شده‌اند؟ آیا در یک زمینه خاص وجود دارد؟ آیا تاکتیکی به طور گسترده برای همه مردم اعمال می‌شود یا فقط برای افرادی با قدرت کم‌تر یا افرادی که قادر به مقاومت نیستند، اعمال می‌شود؟ و اگر ابزارهایی از مقاومت‌کردن در مقابل فراهم‌آوری اطلاعات شخصی وجود دارند آیا این ابزارها به طور برابر در دسترس هستند یا برای اکثر افراد دارای امتیاز، محدود شده‌اند؟

همانطوری که مارکس پیشنهاد می‌دهد، توسعه تکنولوژی‌های جدید، امکانات و شکل‌هایی از نظارت، ارتباط میانی بین آن‌ها و روش‌هایی را که در زمینه‌های مختلفی به کار می‌گیرند، توسعه داده است (۱۳). ما به طور خلاصه تعدادی از شکل‌های اصلی نظارت را مشخص می‌کنیم:

ـ نگاه‌کردن با نظارت ـ ویدیویی به عنوان مثال اصلی.

ـ گوش‌دادن به عنوان یک شکل از نظارت توسط استراق سمع یا گوش‌دادن به تماس تلفنی (و گوش‌دادن به تماس تلفنی بدون سیم).

ـ مکان‌یابی‌کردن، از طریق محصولات و سرویس‌هایی که می‌توانند افراد را مکان‌یابی کنند و حرکت آن‌ها را ردیابی نمایند.

ـ تشخیص، از طریق فناوری‌هایی که با شیوه‌های مختلف، به عنوان «محاسبات همه‌گیر»، «اطلاعات محیط» و اینترنت، با استفاده از سنسورهای شبکه و محرک، مورد استفاده قرار می‌گیرند (که گاهی اوقات به عنوان «گرد و غبار هوشمند» شناخته شده) و دستگاه‌های شناسایی فرکانس رادیویی.

ـ نظارت‌کردن داده‌های شخصی (یا نظارت داده)، شامل فعالیت‌هایی است که از مجموعه‌هایی از داده‌های شخصی، در راه‌های گسترده و مفرط، برای مقاصد زیادی استفاده می‌کند. این ویژگی تعریفی از حالت کاغذ بازی مدرن، از تقویت ـ قانون ـ و از حوزه‌های عظیمی از اقتصاد مدرن است.

هنگامی که این اَشکال با هم ترکیب می‌شوند، نظارت برای فرد حتی بسیار مؤثرتر است.

سه دلیل نگرانی که درباره نظارت درمبحث ابعاد اخلاقی و قانونی «مقررات حفاظت اطلاعات عمومی» مهم هستند:

ـ قانونی‌بودن: «مقررات حفاظت اطلاعات عمومی» یک سیستم از قوانین و اصولی را که قانونی‌بودن پردازش داده‌ها را تعریف می‌کند، ایجاد می‌کند. به هر حال، چون این قوانین و اصول، طیف وسیعی از شرایط را پوشش می‌دهند، آن‌ها به وضوح به صورت باز و به طور کلی شکل گرفته‌اند. بنابراین این مقررات همیشه به طور قطعی مشخص نمی‌کند که آیا یک عمل نظارتی خاص، قانونی است یا خیر. برای مثال این قانون، تعهدات و مسؤولیت اپراتورها را در صورتی که نظارت به شکل پنهان (همانطور که ممکن است در بعضی از اعمال نظارت بر اجرای قانون باشد) یا غیر شفاف (همانطوری که ممکن است در زمینه‌های اقتصادی یا خدمات عمومی رخ دهد) انجام شود، مشخص نمی‌کند. علاوه بر این، نظارت در بخش عمومی عمدتاً در اختیار سیستم قضایی ملی، تحت ماده ۲۳ باقی مانده است. در نهایت، عملیات نظارت ممکن است از لحاظ قانونی و اخلاقی، چالش‌برانگیز باشد، چون این نظارت با اصول حفاظت داده‌های این مقررات مطابق ماده ۵، همچون عدالت و شفایت، سازگار نیست.

۶-۲- پیامدهای قدرت: نظارت به ارتباط مبتنی بر قدرت، بین نظارت‌کننده و نظارت‌شونده، دلالت دارد که در آن، عیب و نقص قدرت نظارت‌شونده ممکن است منجر به آسیب شخصی به کنترل‌شونده شود. این عدم تعادل قدرت و نتایج مضر بالقوه آن، ابعاد اخلاقی مهمی دارد. این قانون در شرایط خاصی موردنیاز است که این عدم تعادل‌ها در نظر گرفته می‌شوند (Notably, Article 22 GDPR) و در صورت بروز ممکن است، ضمانت اجرایی شدیدی در پی داشته باشد.

۶-۳- اثرات افتراقی نظارت: نظارت ممکن است اثر مضری را بر روی بعضی از افراد، گروه‌ها یا دسته‌های خاصی از افراد، بیشتر از سایرین داشته باشد. این نظارت ممکن است وابسته به این باشد که چگونه اهداف نظارت انتخاب می‌شوند یا برحسب این‌که چگونه مکان‌یابی تکنولوژی‌های نظارتی، به دلیل روش غیر تصادفی، داده‌های بعضی از افراد را ثبت می‌کند و داده‌های بقیه را ثبت نمی‌کند که در آن، انواع مختلفی از داده‌های افراد ممکن است برای دستگاه‌های خاص، مورد پرسش و یا در معرض نمایش قرار بگیرند. هدف‌گذاری عمدی در تفاوت‌های مورد انتظار، جمع‌آوری داده‌های کلان و تحلیل برای مقاصد سیاسی و مقاصد عمومی، توزیع غلط حریم خصوصی و دیگر حقوق انسانی ایجادشده توسط نظارت، همگی می‌توانند در زمینه‌های اخلاقی، فراتر از چیزی که قانون ممکن است بگوید یا نگوید، مورد سؤال قرار گیرند.

## اصول اخلاقی به عنوان بخشی از قانون حفاظت داده‌ها

بخش دوم این قانون ارتباط نزدیک بین مقررات حفاظت داده‌ها ـ مخصوصاً مقررات حفاظت اطلاعات عمومی ـ و اصول اخلاقی را بیان می‌کند. حق اساسی برای حفاظت داده‌ها یک دید قابل پیش‌بینی می‌دهد که داده‌های او به روشی عادلانه پردازش می‌شوند. مفاهیم ارزشمند ـ اخلاقی ـ دیگر در پشت حفاظت داده‌ها عبارتند: از مقام و هویت انسان و خودمختاری شخصی که همگی مفاهیمی با یک بُعد اخلاقی واضح هستند (۱۴). علاوه بر این، ملاحظات اخلاقی نقش مهمی را در کاربرد قانون حفاظت داده‌ها از جمله «مقررات حفاظت اطلاعات عمومی» بازی می‌کند. در یک جامعه اطلاعاتی که با سرعت تغییر می‌کند و تهدیدهایی که از «نظارت جدید» در آن کاملاً ملموس هستند، برای درک یک حوزه قابل توجه، باید روشی در نظر گرفته شود که در آن ارزش و هویت انسانی، عدالت و

دیگر ارزش‌ها در نظر گرفته شود و بر حسب قضاوت‌هایی درباره سازگاری این شرایط با استدلال جامعه‌ای دموکراتیک و آزادی‌خواه بر اساس دستور قانون و حقوق انسانی، مبنا و اساس باشد.

اینجا نیاز است که سؤالات جدید با بُعدی اخلاقی مورد بررسی قرار گیرند و تحلیل‌های اخلاقی تبدیل به بخشی از کاربرد قانون حفاظت داده‌ها شود که محتوای «اخلاقی» و «معقولیت حقوق انسانی» قانون حفاظت داده‌ها را مشخص کند. بعضی از مواد «مقررات حفاظت اطلاعات عمومی» به اصول اخلاقی اشاره می‌کنند، برای مثال، با در نظرگرفتن تبعیض و معایب اجتماعی، در مواد ۷۱، ۷۵ و ۸۵ و فراهم کردن وسیله‌ای برای تحلیل‌های اینده.

«مقررات حفاظت اطلاعات عمومی» همیشه نیازمند قضاوت است. این قانون نمی‌تواند ـ و نباید بتواند ـ که صرفاً به صورت تکنیکی اعمال شود. بنا به گفته دادگاه عدالت اتحادیه اروپا ((Court of Justice of the EU (CJEU)، این مقررات حتی یک دلیل کلیدی پشت استقلال DPA ( Data Protection Acts) است (۱۵). این صلاحیت‌ها برای حقوق متوازن اشخاص با بهره اقتصادی از جریان آزاد داده‌ها مورد نیاز هستند.

متعادل‌کردن بهره‌برداری‌های مختلف نیز در هسته پردازش‌کردن داده‌های شخصی، برای مقاصد سودجویی قانونی که توسط کنترل‌کننده‌ها و ناظران با یک شخص ثالث دنبال شده مطابق با ماده ۶(۱)(f) این مقررات است. به طور کلی‌تر، پردازش‌کردن برای مقاصد «بهره قانونی» به طور افزایشی، با اهمیت می‌شود که نیازمند ارزیابی‌های زمینه‌ای، از جمله توازن بین حقوق اساسی و ابعاد تجاری است.

متعادل‌نمودن ـ که به هر حال انجام می‌شود ـ باید به مقررات اخلاقی «که حفاظت داده‌ها یک حق انسانی است»، احترام بگذارد و باید به این اصل همیشه احترام گذاشته شود. ما ادعا نمی‌کنیم که متوازن‌نمودن بهره‌های مختلف لزوماً به قضاوت‌های اخلاقی نیاز دارند، ولی به هر حال، متعادل‌کردن، نیازمند بُعدی اخلاقی است، وقتی که شامل وزن‌دادن به ارزش‌های اخلاقی یا حقوق انسانی باشد. بنابراین قضاوت درباره این‌که چه چیزی برای یک فرد و جامعه، خوب یا بد است، نیاز می‌باشد.

علاوه بر این، خود این قانون وقتی که اعمال می‌شود، شامل تعدادی از مؤلفه‌هاست که ممکن است نیازمند قضاوت اخلاقی باشد. ماده ۲۴ این قانون، تدارک کلی بر حسب الزامات کنترل‌کننده، رویکردی مبتنی بر ریسک را معرفی می‌کند. آن الزامات مشخص می‌کند که کنترل‌کننده باید ریسک‌های احتمالی مختلف و سخت‌گیرانه‌ای برای حقوق و استقلال اشخاص عادی را در نظر بگیرد. ماده ۷۵ ریسک‌های خاص و ضررها را برای حقوق و استقلال اشخاص بیان می‌کند که حفاظت داده‌هارا مهم می‌داند (۱۶).

این تعامل و مشارکت بین کنترل‌کننده‌ها (ناظران داده) و کنترل‌شونده‌ها، مشارکت مفیدی را که خود حفاظت حریم خصوصی به جامعه اعمال می‌کند، باید در نظر بگیرد. درک مفاهیم حفاظت از حریم خصوصی برای «بهترشدن» همیشه در قانون حفاظت داده‌ها به طور کافی مورد احترام قرار نمی‌گرفته و مورد قبول نبوده، برای مثال، اگر افراد نسبت به ناظران اعتماد اندکی داشته باشند (که داده‌های آن‌ها به اندازه کافی در مقابل تجاوزها یا افشاسازی بدون مجوز محافظت نشود)، این موضوع می‌تواند کیفیت خدمات عمومی و آمارهای رسمی را به خطر بیاندازد. بنابراین افراد درباره خودشان اطلاعات غلط می‌دهند.

قضاوت اخلاقی که باید انجام شود، این است که: آیا یک شخص می‌تواند فردی دیگر را برای مشارکت در یک مورد «خوب و بهتر» مشارکت دهد یا نه. مخصوصاً زمانی که تحویل دادن داده‌های شخصی او به منظور افزایش‌دادن کیفیت خدمات عمومی باشد. به عنوان مثال، گسترده‌ترین استفاده از داده‌های شخصی با استفاده از تحلیل داده‌های کلان ممکن است به طور برجسته‌ای دقت خدمات را افزایش دهد و برای جامعه مزایایی را به همراه داشته باشد. مثال‌هایی ممکن است در بخش سلامت (چگونه سرطان را درمان کنیم و از آن پیشگیری کنیم)، در بخش آموزش (چگونه با ترک تحصیل مبارزه کنیم) و در بخش حمل و نقل (چگونه نیازهای مسافران را در حمل و نقل عمومی بهتر برطرف کنیم).

**دخالت انسان (ناظران) به عنوان یک مؤلفه اخلاقی خاص از «مقررات حفاظت اطلاعات عمومی»**

ارزش اخلاقی عدالت به طور مستقیم در ماده ۲۲ اشاره شده است که این مسأله را ارائه می‌دهد: «افراد باید این حق را داشته باشند که صرفاً برای یک تصمیم و فقط بر اساس یک پردازش‌کردن ساده اتوماتیک، مورد کنترل قرار نگیرند»" و کنترل و مونیتورینگ فقط باید برای موارد استثنا و توسط پردازشگرهای الگوریتی باشد. همین ماده در ادامه بیان می‌کند که استثنا هم وقتی تبدیل به قاعده شود، فرد یک ادعا و بهانه‌ای برای دست‌داشتن دخالت عامل انسانی پیدا و عنوان می‌کند که همان عامل باعث به وجودآمدن این تغییرات در داده‌ها شده است. ماده ۲۲ دیدگاهی را منعکس می‌کند که تصمیمات مهم برای اشخاص، باید توسط انسان‌ها گرفته شود، نه توسط مدل‌های ریاضیاتی که گاهی اوقات عصر الگوریتم‌ها نیز نامیده می‌شود (۱۷).

تصمیم‌گیری اتوماتیک و مونیتورینگ الگوریتمی ممکن است اشخاص و فرایندهای اجتماعی را نابود نماید. اشخاص باید حقی برای اثرگذاری بر روی فرایندهای تصمیم‌گیری داشته باشند که به طور برجسته‌ای روی آن‌ها تأثیر می‌گذارند، اگر آن‌ها توانایی (یکسان) برای اعمال این تأثیر را داشته باشند، مسائل اخلاقی بیشتری به وجود می‌آید. تحولات موضعی همچون هوش مصنوعی و یادگیری ماشین، با سؤالات اخلاقی درگیر می‌شوند. یادگیری ماشین را می‌توان به صورت «مجموعه‌ای از تکنیک‌ها و ابزارها که به کامپیوترها اجازه می‌دهند تا با ایجادکردن الگوریتم‌های ریاضیاتی بر اساس داده‌های جمع‌آوری‌شده، فکر کنند»، تعریف کرد (۱۸).

اما بحثی که تصمیم‌گیری اتوماتیک را پشتیبانی می‌کند، این است که این تصمیم‌گیری اتوماتیک باید مناسب‌تر یا کاراتر یا مؤثر در نظر گرفته شود. عمل ماشین، مناسب‌تر از عمل انسان است، چون از تعصب انسانی در هنگام تصمیم‌گیری‌ها دوری می‌کند. برای مثال، درباره این‌که آیا به فردی اجازه داده شود تا به کشوری وارد شود یا خیر، می‌تواند مفیدتر نیز باشد. یک الگوریتم که خوب آموزش‌دیده باشد، ریسک‌های مثبت یا منفی غلط را کاهش می‌دهد. به هر حال، الگوریتم‌ها دیدگاه ما را تغییر می‌دهند و به دلیل عدم حضور مقیاس انسانی، شفافیت خیلی سخت‌گیرانه ارائه می‌شود.

برای شخص خیلی سخت است تا نتایج داده‌های تولیدشده از طریق ماشین را، در مورد الگوریتمی که ممکن است صرفاً داده‌های آن دارای پیش‌فرض‌های اشتباه یا ناقص باشد، به چالش بکشد یا چون در مواردی که الگوریتم، فردی را که در دسته‌بندی خاصی قرار دارد، در گروهی قرار دهد که او با آن دسته‌بندی هیچ تطابقی ندارد، تحمل نماید. اگر یک الگوریتم خروجی ناعادلانه یا نادرست را تولید کند ـ به عبارت دیگر: یک مثبت غلط یا منفی غلط داشته باشد ـ سنگینی بار اثبات برای شخص ممکن است شدیداً بالا باشد.

یک راه حل در مواردی خاص، پیدا شد که اصلاح‌کردن مشخصات شخصی را فراهم می‌کرد. دو مثال در اینجا آورده شده است: اولی شامل حقوقی است که فراموش یا حذف می‌شود که مشکل به خطرافتادن شهرت در مورد Google Spain بوده و مورد دیگر شامل Google و French PDA (CNIL) می‌شود. یک الگوریتم، نتایج خاصی را در یک موتور جستجو تولید می‌کند که منجر به افشاسازی انتشارات مرتبط با یک فرد می‌شود. هر فردی نیاز دارد برای خنثی‌کردن این نتایج، اگر اثبات شود که عادلانه نیستند، عمل کند؛ در مورد Google Spain، افشاسازی اطلاعات نامرتبط و مضر مرتبط با یک فرد بر روی اینترنت است. در این مورد، CJEU نیازمند اصلاح فردی با دخالت انسانی است؛ مثال دوم در مورد بتینا ولف همسر سابق رییس‌جمهور سابق آلمان است (۱۹). وقتی که مردم اسم او را در Google Search جستجو می‌کردند، عباراتی همچون «فاحشه» و «گارد حفاظتی» ظاهر می‌شد، چون اطلاعات بر اساس الگوریتم‌ها منتشر می‌شدند. او مجبور شد برای خنثی‌کردن اثرات منفی، علیه Google قانوناً دادخواهی نماید تا این نتایج را خنثی کند (۲۰). ما همچنین یک مسأله اخلاقی که از پردازش‌کردن اتوماتیک به وجود آمده بود، کشف کردیم: آیا یک فراهم‌کننده سرویس‌های اینترنت باید معیارهایی را برای جلوگیری‌کردن از آسیب به حریم خصوصی افراد به کار بگیرد؟ پاسخ اخلاقی ممکن است این باشد که ما نمی‌توانیم به هوش مصنوعی تکیه کنیم. ابعاد

انسانی باید در اولویت و مفهوم «کنترل بامعنای انسان» باید وجود داشته باشد (۲۱).

## ملاحظات اخلاقی در مقررات حفاظت اطلاعات عمومی: پاسخگویی و مسؤولیت‌پذیری اجتماعی مشارکتی

ملاحظات اخلاقی، بخشی از این مقررات‌اند، اما بعضی اوقات در متن مستتر هستند. این مقررات، عناصری از تنظیمات مبتنی بر اصول را دارد و فقط مبتنی بر قانون نیست (۲۲). در این قسمت، ما بررسی می‌کنیم که این مقررات چگونه قضاوت‌های اخلاقی را تشویق می‌کند. همانطور که قبلاً ذکر شد، از این مفهوم شروع می‌کنیم که پردازش‌کردن داده‌های شخصی باید برای خدمت به بشر طراحی شوند. ما نشان می‌دهیم که رفتار اخلاقی، یک عنصر از پاسخگویی و مسؤولیت‌پذیری اجتماعی مشارکتی است.

اصل پاسخگویی مفهومی کلیدی است. همانطوری که در ماده ۲۴ بیان شده است. کنترل‌کننده‌های داده، نیاز دارند تا معیارهای ضروری را برای تضمین پذیرفتن، پیاده کنند و قادر به نشان‌دادن این موضوع باشد که آن‌ها این معیارها را استفاده کرده‌اند. هر دو مؤلفه بخشی از مسؤولیت‌پذیری قانونی کنترل‌کننده هستند، در حالی که مؤلفه دوم شامل یک نیازمندی رویه‌ای برای گزارش‌دادن می‌شود. در نتیجه یک گزارش از کاری را که آن‌ها انجام داده‌اند، نشان می‌دهد (۲۳). مهم است که تأکید شود که پاسخگویی فراتر از مسؤولیت‌پذیری قانونی می‌باشد. مسؤولیت‌پذیری قانونی به این موضوع اهمیت می‌دهد که چه کسی چه کاری را انجام بدهد، مسؤولیت‌پذیری ممکن است شامل مفاهیم قانونی برای اجرا یا عدم اجرای نقش‌ها و وظایف باشد. همچنین ممکن است شامل روابط قدرت درون سلسله مراتب سازمانی باشد و پذیرفتن را برای مقام نظارتی و برای عموم نشان بدهد تا آنجا که به طور واضحی توسط مقررات مذکور مورد نیاز باشد. به هر حال، پاسخگویی نیز بر این موضوع دلالت دارد که یک عامل مسؤولیت‌پذیر برای احترام‌گذاشتن به اصولی تحت حریم خصوصی و حفاظت داده‌ها تلاش می‌کند و پذیرفتن یا تکمیل نقش خود را نشان می‌دهد (۲۴) و حتی وقتی که به طور واضح توسط «مقررات حفاظت اطلاعات عمومی» مورد نیاز نباشد، اجرای وظایف و نقش‌ها و نمایش اجرای آن را دربر می‌گیرد.

مسؤولیت‌پذیری قانونی محدودتر و اصل وسیع‌تر پاسخگویی، شامل رفتار اخلاقی در دو مفهوم هستند: در اجراکردن مطابق با «مقررات حفاظت اطلاعات عمومی» (تا جایی که تدارکات آن توسط مقررات اخلاقی پشتیبانی می‌شوند) ـ از طریق دادن گزارش از کارهایی که فرد انجام داده است ـ و در بیان‌کردن این اجرا برای دیگران (یعنی برای عموم یا نمایندگان آن‌ها): از این طریق معنای اصل شفافیت نشان داده می‌شود.

پاسخگویی شامل رویکردی مبتنی بر ریسک می‌شود که ممکن است کنترل‌کننده‌های داده را تشویق کند تا قضاوت‌های اخلاقی را انجام بدهند. همان‌گونه که آن‌ها ممکن است آن را در ارزیابی اثر حفاظت داده‌ها به عهده بگیرند. بنابراین کنترل‌کننده‌های داده‌ها برای ارزیابی‌کردن ریسک‌ها، برای حقوق افراد، مورد نیاز است. عدالت نیز به عنوان یک عنصر از پاسخگویی شناخته می‌شود، چون در ماده ۵(۱) «عادلانه» به همراه «قانونمندی» و «به یک طریق شفاف» با اشاره به پردازش‌کردن داده‌های شخصی لیست می‌شود (۲۵).

علاوه بر این، پاسخگویی (از جمله ارزیابی ریسک) فراتر از پذیرفتن با قانون می‌باشد. پاسخگویی با مشارکت‌دادن مسؤولیت‌پذیری اجتماعی، مرتبط می‌شود که شرکت‌ها را برای اثرشان بر روی جامعه، مسؤولیت‌پذیر می‌کند و نگرانی‌های اجتماعی را در اعمال تجاری‌شان تجمیع می‌کند (۲۶). یک توازی می‌تواند با مشارکت‌دادن مسؤولیت‌پذیری اجتماعی در حوزه محیطی استخراج شود. دیگران، مفهوم پاسخگویی پیشرفته را توسعه دادند که شامل ابعاد اخلاقی نیز هست.

همچنین یک لینک برای ابداع مسؤولیت‌پذیری وجود دارد (یا تحقیق و ابداع مسؤولیت‌پذیری)، طوری که همان‌گونه که اغلب ادعا می‌شود، قانون نمی‌تواند با تکنولوژی جدید ادامه دهد و ممکن است یک وظیفه برای تجارت باشد تا ابداع مسؤولیت‌پذیری را تضمین کند. برای مسؤولیت‌پذیربودن، نوآوری باید به همراه دغدغه‌های توجیه‌شده، برای حریم

خصوصی همراه شود که استفاده‌های آینده از تکنولوژی‌ها و مفاهیم حریم خصوصی ممکن و پیامدهای آن را برای دیگر حقوق انسانی در نظر بگیرد (۲۷). سازمان‌های اخلاقی علاقه دارند تا کار درست را انجام دهند و این نیات خوب ممکن است به پشتیبانی اخلاقی از فعالیت‌های مرتبط با پردازش داده‌های شخصی بینجامد (۲۸). کانت گفته است: هیچ چیزی در جهان ـ ذاتاً هیچ چیز حتی فراتر ـ نمی‌تواند قابل درک باشد که بدون صلاحیت و بررسی خوب نامیده شود، مگر یک خواسته خوب (۲۹). رفتار اخلاقی نیز یک بُعد وظیفه شناسی اخلاقی دارد. خواسته خوب سازمان‌ها، همانطور که در تلاش‌های جدی توصیف می‌شوند، بخشی از پاسخگویی (یا مسؤولیت‌پذیری اجتماعی مشارکتی) تحت «مقررات حفاظت اطلاعات عمومی» است.

بهتر است بگوییم: این تجهیزات خاص بُعد اخلاقی دارند و باید برای برانگیختن رفتار اخلاقی اعمال شوند، نه این‌که اساساً به عنوان تجهیزاتی برای پذیرفتن قانون. بعضی از نویسندگان، مفهوم «اخلاق توسط طراحی» را توسعه می‌دهند. همچنین امکان‌پذیر است که برای توسعه ارزیابی اثر اخلاقی یا اجتماعی باید، با نگاه‌کردن فراتر از حریم خصوصی به اثرات نظارت بر روی یک طیف وسیع‌تر از حقوق و ارزش‌های انسانی برای هر دو حالت شخصی و جمعی فراتر از یک، ارزیابی داده رفت.

## خلاصه: چه کسی باید رهبری قضاوت‌های اخلاقی را بر عهده بگیرد؟

انجام قضاوت‌های اخلاقی نیازمند مشخص‌کردن معیاری برای قضاوت‌کردن «خوب»، «بد»، «درست»، «غلط» و دیگر دسته‌بندی‌های ارزیابی‌کننده اخلاقی است. فراتر از سؤال پذیرش قانونی، این‌ها قضاوت‌های اخلاقی در حوزه‌هایی هستند که لزوماً توافق عمومی در جامعه وجود ندارد. این نوع از قضاوت نیز فراتر از حوزه حفاظت داده‌ها می‌رود. با وجود این، قضاوت‌های اخلاقی به طور افزایشی تبدیل به بخش جدایی‌ناپذیر، از کاربرد «مقررات حفاظت اطلاعات عمومی» می‌شوند. همانطور که قبلاً دیدیم، این قضاوت‌ها یک بخش از پاسخگویی کنترل‌کننده‌های داده‌ها هستند که می‌خواهند کار درست را انجام بدهند. همچنین«سیستم‌های ارزیابی داده» وقتی که طیف گسترده‌ای از وظایف‌شان را تحت ماده ۵۷ انجام می‌دهند، باید توسط ملاحظات اخلاقی هدایت شوند که به نوبه خود در رژیم قانونی نقش دارند. برای ارائه یک مثال، ماده ۸۳(۲)(b) نشان می‌دهد که تحمیل جریمه‌های اجرایی باید بر اساس ویژگی عمدی یا سهوی یک تجاوز باشد که مرتبط با خواسته خوب کنترل‌کننده است و به قضاوت اخلاقی نیاز دارد.

«مقررات حفاظت اطلاعات عمومی» باید به طریق قانونی، مؤثر و سازگار اعمال شود (۳۰). از این رو قضاوت‌های اخلاقی باید بر اساس استانداردهای اخلاقی انجام شوند، اما مقررات مذکور به طور کافی استانداردهای اخلاقی خاص را دربر نمی‌گیرد. هدف دوگانه حفاظت داده اتحادیه اروپا (حفاظت حقوق اساسی، اما حرکت آزادانه داده‌ها) به هیچ کدام کمک نمی‌کند و ممکن است به سادگی کشمکش‌هایی را بین اصول اخلاقی متضاد به وجود بیاورد. اگر استانداردهای اخلاقی باید فرموله شوند و حداقل مفاهیم عمومی «مقررات حفاظت اطلاعات عمومی» را پالایش کنند، سؤال این است که چه کسی رهبری این فرایند را به عهده می‌گیرد.

نقطه شروع می‌تواند این باشد که حفاظت داده‌ها یک حوزه‌ای است که متخصصان «سیستم‌های ارزیابی داده» به عنوان مسؤولین نظارتی برای حفاظت داده‌ها باید با استقلال کامل از بخش‌های اجرایی و دیگر بخش‌های حکومتی (و رها از هر گونه تأثیر خارجی) را در کاربرد قانون نقشی مهم بازی کنند. آن‌ها برای تقویت و راهنمایی‌دادن به سهامداران، مسؤول هستند. نظارت یک مثال است، به طوری که حفاظت اشخاص نباید وابسته به ترجیحات سیاسی روز باشد (۳۱). این بحث حتی در ارتباط با مسائل اخلاقی، قوی‌تر است و آن را برای در نظر گرفتن سازماندهی مکانیسم‌های استاندارد که در فاصله خاصی با حکومت دارند، ملموس می‌کند. به هر حال، این موضوع، به این معنا نیست که «سیستم‌های ارزیابی داده» در یک موقعیت واضح برای انجام‌دادن این نقش هستند.

«مسؤولین سیستم‌های ارزیابی داده» با تنظیم‌کردن یک گروه مشورتی اخلاقی، ابتکاری مهم را به کار گرفته‌اند.

این یک گام جالب، برای اولین‌بار است که ممکن است به رسمیت شناخته شود ـ احتمالاً ـ یک مقام نظارتی برای حفاظت از داده‌ها به طور کامل برای تنظیم استانداردهای تصمیم‌گیری اخلاقی مجهز نیست. این بخش جایی برای توسعه‌دادن مدلی برای اداره‌کردن اصول اخلاقی در زمینه «مقررات حفاظت اطلاعات عمومی» اتحادیه اروپا نیست. به هر حال، تعدادی ازمشاهدات که می‌توانند انجام شوند، به قرار زیر است:

اولاً با وجود این‌که سازمان‌ها خودشان باید یک نقش برجسته‌ای در انجام‌دادن قضاوت‌های اخلاقی، به عنوان بخشی از مسؤولیت‌پذیری‌شان، بازی کنند ـ فرایندی که نمی‌تواند توسط برنامه کاربردی مکانیکی از استانداردهای اخلاقی که به طور دقیق فرموله شده‌اند، جایگزین شود ـ توسعه استانداردهای اخلاقی قابل کاربرد به طور گسترده ممکن است برای تضمین قانونی‌بودن، مؤثربودن و سازگاربودن، مفید باشند، چون این حوزه‌ای است که توافق عمومی گسترده‌ای بر روی خوب و بد مورد نیاز است. بنابراین مهم است تا اطمینان حاصل شود که صنعت و جامعه مدنی می‌توانند نقش مهمی ایفا نمایند. با توجه به این‌که کسب و کار ممکن است نقش مهمی در پی داشته باشد، باید با سایر ذی‌نفعان (مثلاً جامعه مدنی، دولت‌ها) همکاری کند؛ ثانیاً کمیته اخلاقی در سطح EU (اتحادیه اروپا) یا کمیته‌های اخلاقی در سطح ملی یا خصوصی می‌توانند در توسعه‌دادن یا حتی اتخاذکردن استانداردهای اخلاقی و در قضاوت‌های اخلاقی هدایت‌کننده در موارد خاصی، نقش بازی کنند. از آنجایی که رویکردهای سازگار در یک جامعه اطلاعاتی با جریان‌های داده‌ای ثابت مورد نیاز می‌باشد، ما معتقدیم که سؤالات اخلاقی بزرگ نمی‌توانند برای سطح ملی اختصاص داده شوند. در جایی که امکان دارد، هماهنگی در مسائل اخلاقی نباید محدود به خود اتحادیه اروپا باشد و ادراکات اخلاقی در سایر نقاط جهان باید در روند تفکر گنجانده شود؛ ثالثاً این مورد باید، نه نقش جایگزین «سیستم ارزیابی داده‌ها» در سطح اروپا «اداره حفاظت از داده‌های اروپا (EDPB: European Data Protection Board)» را ایفا کند و نه آن را کاهش بدهد و بتواند دیدگاه‌هایی را توسعه دهد که چگونگی ملاحظات اخلاقی را در کاربرد «مقررات حفاظت اطلاعات عمومی» در نظر بگیرد. یک کمیته اخلاقی (یا چندین کمیته اخلاقی) به «سیستم ارزیابی داده‌ها» یا EDPB مشاوره می‌دهند که می‌توانند را در اینجا نقش بازی کنند.

## تبیین مبانی اخلاق اسلامی و حفاظت داده در فضای سایبر

### ۱ـ اصول اخلاقی حریم خصوصی

ورود شبکه‌های اجتماعی به ایران موجب بروز خطراتی در حریم خصوصی کاربران شده است. یکی از آموزه‌های اخلاقی در اسلام، احترام‌گذاشتن به حریم خصوصی افراد است، لذا لازم است نقض حریم خصوصی کاربران در شبکه‌های اجتماعی با تمسک به آموزه‌های اخلاقی اسلام مورد بررسی قرار گیرد و وظایف اخلاقی کاربران و اجتماع پیرامون آن‌ها مشخص شود. احترام به حریم خصوصی افراد، در بسیاری از منابع اسلامی، به صورت اصول اخلاقی حریم خصوصی، موجود است. در ادامه برخی از اصول اخلاقی حریم خصوصی، مستفاد از آیات و روایات، اشاره می‌شود، البته اصول اخلاقی حریم خصوصی گسترده‌تر از موارد زیر است و برای رعایت اختصار به مهم‌ترین آن‌ها پرداخته می‌شود:

**۱-۱- استیذان**: در آیات و روایات متعدد، بر اجازه‌گرفتن برای ورود به منزل دیگران تأکید شده است. از آن جمله است آیه ۲۷ سوره نور (۳۲). که حفظ حریم خصوصی دیگران، فقط به ورود بدون اجازه به منزل چهاردیواری افراد متوقف نیست. امروزه می‌توان به خیلی از مکان‌ها منزل گفت، مثلاً کسی که در پارکی چادری زده، آن چادر منزل اوست، یعنی مکانی است که او برای خود اختیار کرده و خود را در آن ایمن می داند، در صورتی که زمین آن مکان به ملکیت او نرسیده، ولی همه انسان‌ها آنجا را منزلی برای او می‌دانند، لذا هیچ کس بدون اجازه وارد آن نمی‌شود. در عصر حاضر که عصر پیشرفت تکنولوژی است، کامپیوتر و موبایل شخصی به مثابه منازل

انسان‌هاست که تمام اطلاعات و ارتباطات شخصی و خانوادگی خود را در آن می‌ریزند. کاربران، این دو دستگاه را مانند منزل خود، فضایی امن تلقی کرده‌اند که اطلاعات و ارتباطات مهم خود را در آن ذخیره می‌کنند.

**۲-۱- ستار بودن خداوند:** ستاریت یا پرده‌پوشی صفتی از صفت‌های الهی است، پس زمانی که خداوند، با این‌که عالم به گناه افراد است و قدرت در افشای آن را نیز دارد، ولی به خاطر عنایت خویش، عیوب گناهکاران را می‌پوشاند، چه توجیهی برای انسان‌هاست که به دنبال عیوب دیگران باشند و از آن‌ها سوء استفاده نمایند. اخلاق در اینجا حکم می‌کند که انسان‌ها به تمسک از پروردگار خود، عیب‌هایی را که از دیگران می‌داند (۳۳) ، آشکار نکند و به دنبال عیوب و رازهای دیگران به هر نحوی ـ چه در عالم واقعی و چه در فضای مجازی و شبکه‌های اجتماعی ـ نباشد.

**۳-۱- رازداری:** هر کسی در زندگی خود رازهایی دارد که دوست ندارد افشا شود. اسلام، رازداری را صفت پسندیده‌ای می‌داند. خداوند نیز در آیات قرآن به خوبی رازداری و زشتی افشای اسرار اشاره کرده است، مانند آیه ۱۶ سوره توبه (۳۴). بنابراین دنبال راز دیگران گشتن و بعد افشاکردن آن، پرده‌دری‌ست و کاری ناپسندتر است.

**۴-۱- عدم تجسس:** در اسلام کاوش و جستجوکردن عیب دیگران از صفات ناپسند شمرده شده است، خداوند در سوره حجرات آیه ۱۲ آن را خطاب به مسلمانان ذکر کرده است (۳۵).

بنابراین دوری‌جستن از تجسس، از اصول حفظ حریم خصوصی دیگران است. دنبال‌کردن ارتباط و اطلاعات کاربران دیگر، در شبکه‌های اجتماعی مصداق بارز تجسس‌کردن است. این تجسس‌کردن مخصوصاً توسط پردازشگرها و ناظران، زمینه افشای اسرار دیگران و هر دو از کارهای ناپسند و غیر اخلاقی است.

**۵-۱- پرهیز از ظلم**: تجاوز به حریم خصوصی کاربران، مصداق واضح ظلم در حق کاربر است. در اسلام عدالت، حسن و ظلم، قبیح است. برای مثال، فقها غیبت‌کردن را مصداق ظلم به غیبت‌شونده می‌دانند، چراکه این کار موجب هتک حرمت آن فرد می‌گردد و این باعث حرمت غیبت می‌شود و این حکم حرمت را، مستنبط از حکم عقل می‌دانند که می‌گوید هتک حرمت دیگران ظلم، است و ظلم قبیح و حرام است. «وقد حکم العقل بحرمتها ایضا لکونه ظلما للمغتاب وهتکا له» هر گونه هتک حریم خصوصی ـ چه در مواجهه حقیقی باشد و چه در مواجهه مجازی ـ مصداق هتک حرمت دیگران و ظلم است و ظلم نیز از لحاظ اخلاقی کاملاً قبیح است (۳۶).

**۶-۱- سرقت:** با روی کارآمدن فضای مجازی، سرقت فقط مختص به بالارفتن از دیوار مردم نمی‌شود. امروزه ورود به حریم خصوصی کاربران و استفاده‌کردن از اطلاعات و ارتباطات او، مصداق بارز سرقت است، زیرا علاوه بر این‌که اطلاعات، ارزش مالی دارند و یا می‌توانند به سرمایه مالی تبدیل شوند، ذاتاً ارزشمندتر از سرمایه مالی است.

**۷-۱- آزار و اذیت:** تجاوز به حریم خصوصی دیگران، مصداق اذیت و آزاررساندن به کاربران است. در اسلام، اذیت و آزاررساندن به مسلمان‌ها از گناهان بزرگ است. به طور کلی، آزار و اذیت به معنای ایجاد ناراحتی برای دیگران است، یعنی هر چیزی که موجب ناراحتی دیگران شود، مصداق آزار و اذیت است (۳۷). بنابراین هتک حریم خصوصی کاربران نیز ایجاد آزار و اذیت برای اوست، چراکه این از بین‌بردن حریم خصوصی و کند و کاو فعالیت کاربر، برای هیچ کس خوشایند نیست، لذا بر این مبنا، هتک حریم خصوصی موجب آزار و اذیت شده و به لحاظ اخلاقی کار قبیحی است.

## بازتاب سیاست‌های حریم خصوصی در ایران و اقدامات ایران برای همسویی با اتحادیه اروپا

بازتاب این مقررات قبلاً در چند مورد جزئی و محدود خلاصه می‌شد که عبارت بودند از:

ـ مطابق ماده ۷ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، داده‌های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آیین‌نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکارناپذیری آن‌ها محفوظ بماند.

ـ مطابق ماده ۱ بند «الف» و «ب» قانون انتشار و دسترسی آزاد به اطلاعات، اطلاعات شخصی به طور دقیق تعریف شده‌اند: ۱ـ اطلاعات: هر نوع داده که در اسناد مندرج باشد یا به صورت نرم‌افزاری ذخیره گردیده و یا با هر وسیله دیگری ضبط شده باشد؛ ۲ـ 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.

ـ ماده ۱۴ در راستای حمایت از حریم خصوصی بیان می‌دارد که: چنانچه اطلاعات درخواست‌شده 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.

ـ در بند هشتم منشور حقوق شهروندی با عنوان «حق دسترسی به فضای مجازی» آمده است که: حق شهروندان است که از امنیت سایبری و فناوری‌های ارتباطی و اطلاع‌رسانی، حفاظت از داده‌های شخصی و حریم خصوصی برخوردار باشند. پیش از این هم در قانون تجارت الکترونیکی، درباره حفاظت از داده‌های شخصی مطالبی ذکر شده بود که با توجه به مواد تصویبی این قانون، کسانی که این قوانین را نقض کنند، مجرم محسوب می‌شوند.

در ماه‌های اخیر نیز لایحه حمایت از داده و حریم خصوصی در فضای مجازی که به همت سازمان فناوری اطلاعات ایران و پژوهشگاه قوه قضاییه و دانشگاه علم و فرهنگ تدوین شده است، یکی از مهم‌ترین لوایح در خصوص حفظ حریم خصوصی و صیانت از داده‌ها و اطلاعات کاربران در حوزه فضای سایبر است. هدف اصلی این لایحه، حفظ اخلاق، صیانت از حیثیت و کرامت اشخاص موضوع داده‌هاست که شامل تبیین حقوق اشخاص موضوع داده‌ها، به ویژه در تعامل با سایر حق‌های مشروع،اخلاق مداری، ضابطه‌مندی فرایند پردازش داده‌های شخصی، مسؤولیت‌پذیری پردازش، هم‌افزایی امور تنظیمی و نظارتی پردازش و جبران‌پذیری زیان‌ها و آسیب‌های پردازش است.

پیش از این در فضای مجازی و برای سرویس‌هایی که هر روز با سرعت بیشتری در حال رشد هستند، لایحه‌ای نداشتیم. همچنین اطلاعاتی از شهروندان ایرانی در سرویس‌های بین‌المللی ضبط و ثبت می‌شد که قابلیت پیگیری نداشت. به همین دلیل برای صیانت از داده‌های مردم در حوزه سرویس‌های بین‌الملل تلاش شده که در سطح بین الملل، به ویژه با قوانین GDPR تعاملات فراوان داشته باشد.

می‌توان گفت این لایحه صیانت از داده‌ها، در حقیقت سندی است که اگر مردم نگرانی و دغدغه‌ای درباره داده‌هایشان دارند، با مطالعه این سند و تضامینی که به آن‌ها داده شده، همچون سایر قوانین و مقررات می‌توانند با آن اعتماد کنند. این لایحه در اصل دنباله روی از مقررات اروپا، یا همان GDPR که درباره حفاظت از حریم داده‌هاست، می‌باشد.

علی‌رغم کوشش فراوان در تهیه این لایحه، اشکالات شکلی و ماهوی زیادی، آن هم به صورت بنیادین، دارد که در صورت عدم اصلاح می‌تواند منجر به فاجعه‌ای حقوقی شود. فاجعه‌ای که در عالَم حقوق به آن قوانین جرم‌زا می‌گویند. عدم حفاظت از اطلاعات مخصوصاً اطلاعات مالی می‌تواند از جمله مواردی باشد که موجبات ضرر را برای صاحبان داده ایجاد نماید. جالب آنکه در این لایحه از اطلاعات مالی صیانتی به عمل نیامده است.

## شهروندان و کاربران ایرانی می‌توانند از مزایای این قانون بهرمند شوند: آری یا خیر

تا زمان تصویب لایحه صیانت از حریم خصوصی و دادهای عمومی در مجلس شورای اسلامی، خوب است که اشخاص ایرانی که به هر نحوی از انحا، در ارتباط با اتحادیه می‌باشند (به صورت حضور فیزیکی یا مجازی) و فعالیت‌های با این مقررات آنان مرتبط می‌باشد، مطالب ذیل را در نظر داشته باشند تا در تطبیق شرایط دچار مشکلات عدیده نشوند.

ماهیت این قانون و دید جامع و فراگیر آن در ارتباط با حریم خصوصی افراد و محافظت از داده‌ها، باعث شده است که مطالعه آن، از منظر نیازهای امنیتی، بسیار مهم باشد. نیازهای

موجود در این قانون متناسب با دغدغه‌های شرکت‌ها و ارائه‌دهندگان سرویس‌های شبکه اجتماعی داخلی و سایر فعالان حوزه فناوری اطلاعات است.

در بحث گستره اعمال مقررات، اصطلاحات واقعی ماده ۳ GDPR نسبت به خود موضوع گسترده‌تر است، زیرا در واقع هیچ گونه اشاره‌ای به شهروندی ندارد. این عنوان به هر موضوع داده‌ای در اتحادیه اروپا، یعنی شخصی که در اتحادیه اروپا زندگی می‌کند یا با اتحادیه اروپا در ارتباط باشد، اعمال می‌شود. قابل ذکر است که ماده ۳(۲) به پردازش اطلاعات شخصی هر شخص (در اتحادیه اروپا) اطلاق می‌شود و ملیت یا محل اقامت فردی، اهمیتی ندارد. «مقررات حفاظت اطلاعات عمومی» از اطلاعات شخصی شهروندان، ساکنان، گردشگران و سایر افراد بازدیدکننده از اتحادیه اروپا هم محافظت می‌کند. بنابراین تا زمانی که شخصی در اتحادیه اروپا باشد، هرگونه اطلاعات شخصی او توسط هر کنترل‌کننده یا پردازنده که مطابق با الزامات ماده ۳(۲) جمع‌آوری می‌شود، تحت پوشش «مقررات حفاظت اطلاعات عمومی» قرار دارد. همچنین همه شرکت‌های ارائه‌دهنده خدمات را، به کاربران که با داده‌های شخصی افراد سروکار دارند، ملزم به رعایت آن می‌کند، اگرچه این قانون در اتحادیه اروپا وضع شده است، اما حوزه سرزمینی آن محدود به اعضای اتحادیه اروپا نیست و شرکت‌ها و سازمان‌هایی را که در این اتحادیه مستقر نیستند را نیز دربر گیرد.

در مورد ماده ۳(۲)، کنترل‌کننده‌ها یا پردازنده‌ها باید یک نماینده مبتنی بر اتحادیه اروپا را تعیین نمایند. اساساً «مقررات حفاظت اطلاعات عمومی» قوانین حفظ حریم خصوصی در محدوه مکان موضوع داده‌ها را، عوض کرد، یعنی نه مکان کنترل‌کننده و نه پردازنده داده را مهم تلقی نمی‌نماید. بنابراین اگر کسب و کاری در هر جای دنیا در حال تلاش برای فروش محصولات و خدمات خود در اتحادیه اروپا باشد، در GDPR گرفتار خواهد شد.

## نتیجه‌گیری

مقررات جدید اتحادیه اروپا برای تقویت حفاظت از اطلاعات عمومی شهروندان اتحادیه اروپا ایجاد شده است، هرچند این قانون، کار شرکت‌های بزرگی مانند گوگل و فیس-بوک را از گذشته سخت‌تر می‌کند، اما در حقیقت این شرکت‌های کوچک هستند که برای تبعیت از این قانون با مشکلات بسیار بزرگ‌تری مواجه می‌شوند، زیرا تبعیت از این قوانین هزینه‌های زیادی را بر شرکت‌ها تحمیل می‌کند.

با توجه به این‌که ما در کشوری زندگی می‌کنیم که دارای مردمی با تفکرات مذهبی است و از طرفی قوانین موضوعه ما هبر اساس منبع شرعی تدوین شده، می‌توان با تبیین و تحلیل یک سری از مبانی اولیه اسلامی که داری حسن و قبح ذاتی می‌باشند، راه را برای جلوگیری از سوء استفاده و ارتکاب جرم در فضای سایبر به حداقل‌ها کاهش داد. پرورش مبانی اخلاقی اسلام از قبیل اذن دخول، رازداری، رازپوشی، عدم تجسس، منع اکل مال به باطل، منع آزار و اذیت دیگران و... . می‌توان حتی در برخی از موارد بدون اعمال برخوردهای چکشی تا حد امکان این محیط را به یک محیط نسبتاً امن و سالم تبدیل نمود.

آموزش کارکنان در زمینه امنیت سایبری می‌تواند یکی از بهترین سرمایه‌گذاری‌های انجام‌شده توسط یک شرکت باشد. برای تحقق این امر می‌توان از بسیاری از منابع آموزشی رایگان مانند دوره‌های امنیتی سایبری نیز استفاده کرد.

راه حل مناسب برای کاهش خطرات مربوط به حملات سایبری برای شرکت‌های ایرانی که با اتحادیه اروپا همکاری می‌نمایند، استفاده از نرم‌افزار فعال امنیتی سایبری است. این روش به شرکت‌ها کمک خواهد کرد تا هر لحظه اطلاعات دقیقی را در مورد خطرات دریافت کنند و آن‌ها را به منظور جلوگیری از ایجاد شکاف‌های امنیتی از بین ببرند.

آغاز به کار و اجرای EU GDPR می‌تواند به شرکت‌ها و سازمان‌ها برای صرفه‌جویی در زمان و هزینه کمک کند. تغییر در شیوه جمع‌آوری داده‌ها و مدیریت آن‌ها در یک شرکت می‌تواند، روندی طولانی باشد. بنابراین سریع‌تر شروع به برنامه‌ریزی کنید. تمامی شرکت‌های ایرانی که با اتحادیه اروپا

همکاری می‌نمایند، شامل «مقررات حفاظت اطلاعات عمومی» می‌باشند و کلیه ابعاد اخلاقی و ضمانت اجراهای کیفری نیز شامل آن‌ها می‌باشد.

در نهایت این دغدغه‌ها و مسؤولیت‌های اخلاقی بایستی در آینده نه‌چندان دور در قوانین اکثر کشورها، خصوصاً جمهوری اسلامی ایران، توسط مقامات مذکور و مبتنی بر مقررات حفاظت اطلاعات عمومی (GDPR)، در قوانین موضوعه آن‌ها گنجانده شود. همچنین آموزش کارکنان درباره امنیت فضای سایبری، استفاده از نرم‌افزارهای فعال امنیتی مرتبط و ارائه منابع آموزشی رایگان می‌تواند در جلوگیری از جرم و سوءاستفاده فضای سایبر خصوصاً در مسائل مالی تأثیرگذار باشد.

## References


1. Charles R. The Meaning of ‘Accountability’ in the Information Privacy Context’in Daniel Guagnin. Edited by Hempel L, Ilten C, Kroener I, Neyland D, Postigo H. Managing Privacy through Accountability. London: Palgrave Macmillan; 2012. p.149.

2. Reed J. Mesopotamia (Culture and Civilization of Ancient World). Translated by Basir A. Tehran: Amir Kabir; 2007. p.125.

3. Clarke R. Communications of the ACM. *Information Technology and Data veillance* 1988; 31(5): 498-512.

4. Baqirzadeh MR. Comparative Study of Universality of Human Rights in Islam. *Journal of Marifat* 2010; 2(8): 105-124.

5. Abadi M. Peasant history in Persian literature. *Honar va Mardom* 1997; 13(4): 64-70. [Persian]

6. Ghazvini M. Twenty papers. Tehran: The National Assembly Press; 1934. [Persian]

7. Najafi Sahib al-Jawahir MH. Jawahir al-Kalam. Beirut: Dar Ehya al-Turath al-Arabi; 1984. Vol.41 p.222.

8. Aris H. Shakhsyyah al-Uqubat. Beirut: Dar al-Falah; 1997. p.68.

9. Hassani A. Sharh Qanun al-Uqubat al-Eraqi. Cairo: Al-Ershad Press; 1972. p.119.

10. Clifford D, Ausloos J. Data Protection and the Role of Fairness. London: Oxford University Press; 2017. p.283.

11. Mazeaud H, Leone ET-J. Leeons de Droit Civil T.I. French: Famille et Incapacites; 1967. p.111.

12. Raab C. Regulating Surveillance: The Importance of Principles. Edited by Ball K, Haggerty KD, Lyon D. Routledge Handbook of Surveillance Studies. London: Routledge; 2012. p.377-385.

13. Car M. The structure of the family legal system in Iran. Tehran: Roushangran Va Motaleat Zanan; 2002. p.47-59.

14. Hijmans H. The European Union as Guardian of Internet Privacy Law. New York: Governance and Technology Series 31; 2016. p.22.

15. Ibn Manzour M. Lessan al-Arab. Beirut: Dar al-Fakr; 1414 AH.

16. Julia C. Blixurd and Edmond J. Sawyer, A code of ethics for ASIS: The challenge before us. Germany: ASIS Bulletin; 1984. p.8-10.

17. Priscilla M. Regan. Chapel Hill, the University of North Carolina Press, Legislating Privacy Technology. Carolina: Social Values and Public Policy; 1995. p.310.

18. Charles R. Regulating Surveillance: The Importance of Principles. Edited by in Ball K, Haggerty KD, Lyon D. Routledge Handbook of Surveillance Studies. London: Routledge; 2012. p.377-385.

19. Bonnet C, Garbinti B, Solaz A. The Role of Shared Custody in Women’s employment. London: London School of Economic; 2018. p.209.

20. Makarim Shirazi N. Anwar al-Fiqaha, Kitab al-Hudud va al-Tazirat. 1st ed. Qom: Imam Ali School Press; 1197. p.346.

21. Awdah A. Islamic criminal law. Tehran: Iranian Academic Center for Education, Culture & Research; 1993. Vol.2 p.217.

22. Mousavi Y. Evolution of Citizenship rights towards urban order. *Danesh-e Entezami* 2001; 3(4): 23-36.

23. Charles D. Uta Müller and Thomas Potthast (eds.), Ethik in den Kulturen - Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn. Tübingen: Narr Francke Attempto; 2017. p.335-347.

24. Ramizanpur R, Ranjbar AR. Transnational sources of citizenship rights. *Haq Gostar Journal* 2008; 5(3): 45-54.

25. Tabatabaei M. Public freedoms and human rights. 4th ed. Tehran: Tehran University Press; 2009.

26. Horr-e Ameli MIH. Wasael al-Shia ela Tahsil Masael al-Shariah. Beirut: Dar al-Ehya Turath al-Arabi; 1983. Vol.18 p.301-312, 385.

27. Hijmans H. The European Union as Guardian of Internet Privacy Law. New York: Governance and Technology Series 31, at 6.14. See the remarks of the UK Information Commissioner; 2016. p.114.

28. Horre Ameli M. Wasael al-Shia. Beirut: Dar al-Ehya; 2009. Vol.18 p.258.

29. Carsten Stahl B. Responsible research and innovation, The role of privacy in an emerging framework. Beirut: Science and Public Policy; 2013. p.708-716.

30. Kant I. Groundwork of the Metaphysics of Morals. Translated by White Beck L. First Sentence of it Chapter 1. New York: The Liberal Arts Press; 1959. p.9.

31. Ragheb Esfahani H. Al-Mufradat al-Gharibah al-Quran. Edited by Seyed Gilani M. Beirut: Dar al-Marifah; 1991. p.169.

32. Al-Zubaydi M. Taj al-Arus. 1st ed. Beirut: Dar al-Fikr Press; No Date. p.329; Himavi Y. Mojam al-Buldan. Beirut: Dar Sader; 1957. Vol.4 p.132.

33. Holy Quran. Nor: 26.

34. Gary T. Marx, an Ethics for the New Surveillance. Beirut: The Information Society; 1998. p.171-186.

35. Holy Quran. Tobeh: 16.

36. Immanuel K. Groundwork of the Metaphysics of Morals. Translated by White Beck L. First Sentence of it Chapter 1. New York: The Liberal Arts Press; 1959. p.96-119.

37. Ibn Manzoor J. Lisan al-Arab. Beirut: Dar Sader Publishers; 1997. Vol.4 p.378.

38. Holy Quran. Emran: 152.