مقاله مروری

# اصل زرّین اخلاقی و پیشگیری حقوقی استفاده نامشروع از پایگاه داده‌ها

**سهرورد زرشکیان*، دکتر احمد مؤمنی راد**
**گروه حقوق عمومی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران**

(تاریخ دریافت:۹۷/۰۷/۲۱،تاریخ پذیرش۹۷/۰۹/۲۸)

## چکیده

**زمینه:** گردآوری داده‌های افراد در قالب پایگاه داده‌ها یکی از روش‌های نوینی است که همراه با پیشرفت فناوری اطلاعات سیر رو بـه رشـدی داشته است. استفاده از پایگاه داده‌ها در امر مدیریت و سیاست‌گذاری چـالش‌هـایی را درزمینـه‌هـایی چـون نقـض حـریم خصوصـی و رعایـت هنجارهای اخلاقیِ پذیرفته شده ایجاد کرده است. روند روزافزون استفاده از پایگاه داده‌ها در سازمان‌های دولتی و خصوصی ایران ابعاد اخلاقی و حقوقی نوینی را مطرح کرده است که نیازمند بحث و اندیشه است. هدف از انجام این پژوهش در وهله نخست، اثبات غیر اخلاقی بودن استفاده از داده ها بدون اخذ رضایت از صاحب داده در پرتو قاعده زرین اخلاقی است. در گام بعد سعی خواهد شد که با بیان موضع قانونی اتحادیه اروپا و خلأهای قانونی نظام حقوقی ایران، پیشنهادهایی را برای وضع موجود ارائه دهیم.

**نتیجه‌گیری:** برای احتراز از تناقض منطقی باید داده‌های افراد را فقط با لحاظ کردن اصول حاکم بر استفاده از داده‌ها بـه کـار بـرد و عنصـر رضایت را مدنظر قرار داد. به‌منظور تدوین نظام حقوقی جهت تحکیم هنجارهای اخلاقی در این زمینه، با مطالعه رژیم قانونی حاکم بر حمایت از داده‌ها در اتحادیه اروپا برخی از کاستی‌های نظام حقوقی ایران در عرصه قانون‌گذاری مشخص می‌گردد که راهکارهایی برای بهبود آن پیشنهاد شده است.

**کلیدواژگان:** اخلاق، پایگاه داده‌ها، قاعده زرین، حریم خصوصی

## سرآغاز

اخلاق فناوری اطلاعات موضوعی میان‌رشته‌ای است که بحث از آن نیازمند آشنائی و تخصص در دو حوزه اخلاق و فناوری اطلاعات است. اخلاق اطلاعات شاخه‌ای از علم اخلاق است که بر رابطه بین ایجاد، سازمان‌دهی، انتشار و استفاده از اطلاعات، استانداردهای اخلاقی و اصول معنوی حاکم بر ارتباطات انسانی در جامعه تمرکز دارد (۱).

با ظهور فناوری‌های اطلاعاتی و ارتباطی (ICT) از دهه ۶۰ قرن بیستم و نفوذ آن در تمامی شئون جوامع اعم از حقوقی، فرهنگی، اجتماعی و اقتصادی بحث لزوم حمایت از داده‌های افراد در فضای مجازی مطرح گردیده است. افراد برای بهره‌مندی از اغلب مزایای موجود در فضای مجازی در بسیاری موارد ناچار به بارگذاری اطلاعات خود می‌باشند. از سوی دیگر، بحث ایجاد پایگاه داده‌های[1]دولتی که حاوی اطلاعات افراد در ابعاد مختلف است، زمینه را برای در دسترس قرار گرفتن اطلاعات و متعاقب آن نقض بالقوه حریم خصوصی[2] اطلاعاتی افراد فراهم کرده است.

برای اینکه استفاده از داده‌های افراد بدون رضایت آن‌ها با محکی اخلاقی سنجیده شود می‌توان رویکـــردها و نظریات متعدد اخلاقی را بر آن‌ها منطبق ساخت. بدیهی است که هر رویکردی با توجه به مبانی، اصول و شاخصه‌های خود قضاوت خاص خود را از این مسئله داشته باشد. در این مقاله از میان انواع رویکردها و نظریات متفاوت اخلاقی، قاعده زرین را انتخاب شد و آن محمول قضیه منطقی قرار داده شد.

علی‌رغم نوظهور بودن پایگاه داده‌ها و گسترش سریع آن در نظام اجرائی کشور، قوانین و مقررات حامی حریم خصوصی افراد در این زمینه پاسخگو نیست و در رأس آن قانون اساسی کشور ما به‌طور صریح نامی از آن نبرده است و فقط به بیان مصادیق سنتی این حق پرداخته است. با توجه به این امر، لازم است ابتدا نقض حریم خصوصی اطلاعاتی را از منظر اخلاقی بررسی کرده و سپس با استفاده از نظام حمایت قانونی اتحادیه اروپا پیشنهادهایی را برای اصلاح وضع موجود ارائه دهیم. این مسئله با توجه به فقر منابع داخلی در این زمینه اجتناب‌ناپذیر می‌نماید. گفتنی است که دستورالعمل حمایت از داده‌های اتحادیه اروپا از پیشرفته‌ترین و به‌روزترین منابع در این زمینه بوده و برای کلیه اعضای آن الزامی می‌باشد. همچنین بسیاری از کشورها در تدوین قوانین خود از این دستورالعمل استفاده کرده‌اند، از این رو لازم است با بررســـی امکان

نویسندهٔ مسئول: نشانی الکترونیکی: sohrevardz@yahoo.com

سنجی ورود گزاره‌های آن به ادبیات حقوقی خود، گامی در جهت اصلاح وضعیت حاضر برداریم. دستورالعمل اتحادیه اروپا دارای ضمانت اجراهای مناسبی در موارد نقض حریم خصوصی اطلاعاتی و ارتباطی است و حتی کشورهای عضو را ملزم کرده است که قوانینی را با وصف متناسب بودن، مؤثر بودن و بازدارنده بودن برای مجازات وضع کنند. (بند الف ماده ۱۵ دستورالعمل) (۲).

۱- قاعده زرین اخلاقی

فلسفه اخلاق دو شاخه اصلی دارد؛ فرا اخلاق[۳] و اخلاق هنجاری[۴] موضوع فرا اخلاق، ماهیت و روش‌شناسی داوری‌های اخلاقی است. اخلاق هنجاری خود به دودسته است: نظریه هنجاری[۵] که در جستجوی اصول کلی اخلاق است و دسته دیگر اخلاق هنجاری کاربردی که به مطالعه مسائل اخلاقی خاصی می‌پردازد (۳).

از آنجائی که بحث ما مبانی اخلاقی استفاده از پایگاه داده‌ها از منظر قاعده زرین اخلاقی[۶] است از این رو موضوع حاضر در حیطه اخلاق هنجاری کاربردی[۷] قرار می‌گیرد. ذکر این نکته نیز لازم است که انتخاب قاعده زرین اخلاقی از میان سایر نظریات اخلاقی در این مقاله به معنای ترجیح آن بر سایر نظریات نیست و در این زمینه هیچ‌گونه ارزش‌گذاری صورت نپذیرفته است. برای اینکه بتوان قاعده زرین اخلاقی را در بحث استفاده از پایگاه داده‌ها بیان نمود لازم است ابتدا مختصری در باب قاعده زرین اخلاقی گفتگو کرد سپس به بحث حریم خصوصی در پایگاه داده‌ها پرداخت و در آخر استفاده از پایگاه داده‌ها را در پرتو قاعده زرین اخلاقی سنجید.

قاعده زرین اخلاقی دارای سابقه‌ای طولانی است و در بسیاری از کتب دینی به‌نوعی ذکری از آن به میان آمده است. در قوانین حمورابی، چین، مصر، روم و یونان و هند باستان نیز این قاعده به طرق مختلف مورداشاره قرار گرفته است. در ادیان یهودیت، مسیحیت و اسلام نیز این قاعده ذکرشده است (۴). در اسلام جمله مشهور امام علی (ع) دال بر این موضوع است. طبق فرمایش ایشان: «برای مردم آن را بخواه که برای خود می‌خواهی و با دیگران طوری رفتار کن که مایلی درباره‌ات آن‌چنان کنند». می‌توان با رویکردهای مختلفی نظیر روان‌شناسی، فلسفه، جامعه‌شناسی و ... به مفهوم قاعده زرین اخلاقی نگاه کرد که رویکرد ما رویکرد فلسفه اخلاق است. قاعده زرین اخلاقی به‌قدری فراگیر است که در اکثر فرهنگ‌ها اشاراتی به آن شده است و هدف از بیان آن ساختن الگوئی برای رفع تناقضات بوده است (۵).

یکی از فیلسوفان معاصر و طرفداران این قاعده در کتاب مشهور خود، درآمدی جدید به فلسفه اخلاق، پس از واکاوی و تبیین نظریات اخلاقی چون نسبی‌نگری فرهنگی[۸]، شخصی‌انگاری[۹] ، فراطبیعت‌گرائی[۱۰] ، شهودباوری[۱۱] ، عاطفه‌گرائی[۱۲] ، توصیه‌گرایی[۱۳] ، پیامدگرائی[۱۴] و ناپیامدگرائی[۱۵] به انتقادات وارده نسبت به آن‌ها می‌پردازد و در آخر تنها قاعده‌ای را که به مدد آن می‌توان بدون دچار شدن به تناقض منطقی به تکالیف اخلاقی عمل کرد، قاعده زرین می‌داند. فیلسوف دیگری که در این زمینه مباحث فلسفی عمیقی را مطرح کرده است، کانت می‌باشد که بخشی از نظریات گنسلر الهام‌گرفته از وی است (۶).

قضیه قاعده زرین اخلاقی عبارت است از: «با دیگران فقط طوری رفتار کن که رضایت می‌دهی در همان موقعیت با تو رفتار شود». بر اساس این قاعده جمع این دو گزاره ممنوع است: ۱- کاری نسبت به کسی انجام می‌شود؛ ۲- آن فرد توقع ندارد در همان موقعیت کسی نسبت به وی همان کار را انجام دهد. بر اساس این دیدگاه، اگر ما طبق قاعده زرین عمل کنیم، به‌هیچ‌عنوان دچار تناقض منطقی نمی‌شویم؛ البته درصورتی‌که عناصر معرفت، آگاهی، وجدان و بی‌طرفی را به کاربندیم. طبق ضابطه قانون جهانی که گنسلر آن را بیان کرده است: «فقط طوری عمل کن که می‌خواهی هرکسی در آن موقعیت باشد، آن‌طور عمل کند، فارغ از تفاوت‌هایی که در زمان یا شخص می‌توان تصور کرد» (۲). عمل طبق این قاعده، انسان را از افتادن به تناقض در رفتارها و باورهایشان، آن‌گونه که در نظریات نسبی‌نگری فرهنگی، شخصی-انگاری و غیره دچار آن می شوند، بر حذر می‌دارد از این رو می‌تواند الگویی را در استفاده از پایگاه‌های داده تدوین کند که قابلیت تعمیم جهانی دارد.

بر اساس این الگو، ابتدا باید اثبات شود که استفاده از اطلاعات پایگاه داده‌ها بدون رضایت افراد امری غیر مطلوب است که اگر فردی باوجدان، بی‌طرف و معقول در موقعیت آن قرار گیرد احساس رضایت نمی‌کند و می‌توان به این عمل وصف قبیح بودن را اعطا کرد. برای اثبات این امر در قسمت بعد به بیان مهم‌ترین پیامد استفاده از پایگاه داده‌ها یعنی نقض حریم خصوصی افراد پرداخته خواهد شد و در قسمت بعد قاعده زرین بر آن منطبق می شود.

۲- نقض حریم خصوصی اطلاعاتی

ایجاد پایگاه داده‌ها دارای مزایا و معایب بالقوه‌ای می‌باشد؛ بانک اطلاعات یا پایگاه داده‌ها با استفاده از فناوری‌های اطلاعاتی به خصاص فنون آماری، اطلاعاتی را در اختیار دولت (و نهادهای خصوصی) می-گذارد که از یکسو باعث تسریع امور اداری، اجرائی، سیاست‌گذاری و ... می‌گردد و از سوی دیگر مباحثی چون حریم خصوصی را در معرض خطر قرار می‌دهد (۷). مزیت‌های ایجاد پایگاه‌های اطلاعاتی اشتیاق روزافزونی در دولت‌ها پدید آورده که هر چه بیشتر اطلاعات زیادتری را از افراد ذخیره کنند تا هنگام نیاز آن اطلاعات را بازیابی کنند؛ از اثر انگشت گرفته تا نشانی منزل، شغل‌ها و روابط اجتماعی و فعالیت‌های سیاسی و مسائل دیگر (۸).

نگارنده کتاب «حقوق فناوری اطلاعات» در جمع‌بندی خود از مفهوم حریم خصوصی آن را مفهومی می‌داند که عنصر اساسی آن اختیار و آزادی انسان‌ها در تصمیم‌گیری در خصوص میزان وقوف و مداخله سایرین نسبت به زندگی شخصی افراد است. به‌عبارت‌دیگر هر فردی این حق را دارد که خود در خصوص اینکه دیگران تا چه میزان در خصوص زندگی شخصی او بدانند و یا در آن وارد شوند، تصمیم بگیرد و در صورت عدم تمایل ایشان را منع کند (۹). بنابراین در نظر ایشان حریم خصوصی عبارت است از حق اولیه افراد در مصون ماندن حوزه خصوصی ایشان از هرگونه مداخله و تعرض فاقد مجوز قانونی و همچنین منع دیگران از وقوف بر اطلاعات این حوزه.

حق حریم خصوصی که از آن به «حق تنها بودن» نیز یادشده ازجمله حقوقی است که انسان‌ها به دلیل نیازهای شخصی ازیک‌طرف به آن وابسته‌اند و از سوئی دیگر به دلیل ضرورت زندگی جمعی مکلفند این حق را نسبت به دیگران به رسمیت شناخته آن را محترم دارند. به‌عبارت‌دیگر می‌توان گفت که حق بر حریم خصوصی عبارت است از حق مصونیت و حق انسان نسبت به امور شخصی خود. (۱۰)

پژوهشگر دیگری ضمن بررسی تفصیلی تعاریف مختلف در باب حریم خصوصی و نیز دسته‌بندی معیارهای آن در مقام جمع‌بندی، دو ضابطه نوعی و جمعی را در شناخت حریم خصوصی معتبر می‌داند و این مفهوم را این‌گونه تعریف می‌نماید: «حریم خصوصی قلمروی از زندگی هر فرد است که آن فرد به‌طور نوعی یا عرفی یا با اعلان قبلی، انتظار دارد دیگران بدون رضایت وی به اطلاعات راجع به آن قلمرو دسترسی نداشته باشند یا به آن قلمرو وارد نشوند، یا به آن قلمرو نگاه و نظارت نکنند یا به هر صورت دیگری وی را در آن قلمرو مورد تعرض قرار ندهند» (۱۱).

در مورد حریم خصوصی اطلاعاتی که مفهوم خاص‌تری از حریم خصوصی است نیز مراد، مصون بودن داده‌های مربوط به حوزه‌ای از زندگی انسان‌هاست که نوع بشر انتظار دارد سایرین بدون اجازه وی بدان‌ها دسترسی نیافته و آن‌ها را مورد پردازش قرار ندهند؛ بنابراین، در تعریف حریم خصوصی اطلاعاتی می‌توان جنس این تعریف را همان تعاریف پیشین ارائه‌شده در مورد حریم خصوصی به معنی اعم دانست و فصل آن را حیطه موردحمایت یعنی داده‌های شخصی فرد در فضای مجازی تلقی کرد.

همان‌طور که مشخص است، در بحث حریم خصوصی اطلاعاتی از واژه-های «بدون مجوز قانونی»، «بدون رضایت» و «بدون اجازه» یادشده است که همگی بیان‌گر لزوم اجازه پیشین در استفاده از اطلاعات افراد است و دسترسی بدون کسب اجازه افراد به‌نوعی نقض حریم خصوصی محسوب می‌گردد. دسترسی به داده‌های افراد و در اختیار قرار دادن آن به لحاظ قانونی ممنوع است و از مصادیق بارز نقض حریم خصوصی محسوب می‌گردد. برای ساختن چهارچوب اخلاقی جهت منع افراد و دولت‌ها از چنین اعمالی می‌توان متوسل به قاعده زرین اخلاقی شد که در پائین به شرح مفصل آن می‌پردازیم.

۳- استفاده از پایگاه داده‌ها در پرتو قاعده زرین اخلاقی

امروزه استفاده از پایگاه‌های اطلاعاتی، چه در سازمان‌های دولتی و چه در سازمان‌های خصوصی، گسترش زیادی پیداکرده است. گردآوری اطلاعات مختلف افراد در پایگاه داده‌ها در سال‌های اخیر در کشورمان نیز رشد روزافزونی داشته است به‌طوری‌که در قانون برنامه پنجم توسعه و نیز در فصل پنجم قانون مدیریت خدمات کشوری، دستگاه‌های اجرائی به لحاظ قانونی ملزم به راه‌اندازی پایگاه‌های اطلاعاتی شده‌اند. در قانون برنامه پنجم توسعه (فصل چهارم: نظام اداری و مدیریت/ فناوری اطلاعات) به‌ویژه ماده ۴۶، برخی از سازمان‌های دولتی مانند وزارت ارتباطات و فناوری اطلاعات (درزمینهٔ راه‌اندازی شبکه ملی اطلاعات) ملزم به ایجاد پایگاه‌های اطلاعاتی شده‌اند؛ (۱۲) همچنین در بند «ب» ماده مذکور، لزوم پیوستن کلیه دستگاه‌های اجرائی به این پایگاه‌ها ذکر شده است. در ماده ۴۰ قانون مدیریت خدمات کشوری عنوان‌شده است: «به‌منظور ایجاد زیرساخت اطلاعاتی و تمرکز امور مربوط به استفاده از فناوری اطلاعات در خدمات، اداری، دولت موظف است از طریق سازمان ثبت احوال و شرکت پست جمهوری اسلامی ایران و مشارکت کلیه دستگاه‌های اجرائی، پایگاه اطلاعات ایرانیان را طراحی، ساماندهی و اجرا نماید» و در تبصره ۲، شرط استفاده از خدمات را منوط به داشتن کد ملی و کدپستی افراد کرده است.

در سازمان‌های خصوصی نیز شرکت‌ها و مؤسسات با گردآوری اطلاعات مشتریان خود، بانک اطلاعاتی آن‌ها را تشکیل داده و از تکنیک‌های بازاریابی و تبلیغات در ارتباط با آن‌ها سود می‌برند. درنتیجه امروزه پایگاه‌های اطلاعاتی زیادی در کشور بدون اینکه حتی افراد اطلاعی از آن‌ها داشته باشند، وجود دارد. امروزه انباشتگی داده‌ها بسیار ارزشمند گردیده و رغبت در آن زیاد شده است و اگر سامانه‌ای اخلاقی برای آن‌ها لحاظ نگردد، ممکن است آسیب‌هایی جدی به امنیت روانی و آرامش درونی اشخاص وارد آید و جامعه را دچار چالش‌هایی نوین کند (۱۳).

هدف از تشکیل پایگاه‌های اطلاعاتی ساماندهی امور و تسهیل امر برنامه‌ریزی و غیره است اما وقتی بحث از تجاری‌سازی آن‌ها به میان می‌آید، ممکن است نقض حریم خصوصی در آن‌ها اتفاق بیفتد. با مثالی عینی بحث را پیش می‌گیریم. فرض کنید برای ثبت‌نام در دانشگاهی تمامی اطلاعات شخصی و آموزشی، شماره تلفن همراه، کدپستی و سایر اطلاعات در سامانه الکترونیک دانشگاه وارد شده است. دانشگاه بر اساس اطلاعات دانشجویان خود بانک اطلاعاتی آن‌ها را تشکیل می‌دهد. این بانک اطلاعاتی قابلیت تجاری‌سازی دارد. مؤسسات آموزشی زیادی هستند که مشتریان اصلی آن‌ها دانشجویان محسوب می‌شوند مانند مؤسسات کنکوری. حال اگر دانشگاه اطلاعات مربوط به دانشجویان در ازای قراردادی در اختیار این مؤسسات قرار گیرد، شاهد پیامک‌ها و ایمیل‌های ناخواسته تبلیغاتی خواهیم بود که گاهی برای افراد ایجاد مزاحمت می‌کنند به‌ویژه اینکه در بعضی مواقع تعداد پیامک‌ها و ایمیل-های ارسالی زیاد می‌شود و به مزاحمت می‌انجامد.

آیا در مثال فوق دانشگاه حق فروش اطلاعات را به مؤسسات آموزشی بدون اجازه صاحبان داده داشته است؟ استفاده از داده‌های پایگاه‌های اطلاعاتی در این فرض- طبق تعریف قسمت قبل- مشمول نقض حریم خصوصی می‌گردد و به لحاظ قانونی ممنوع است. امروزه تمامی شهروندان با خیل عظیمی ازاین‌گونه پیامک‌ها و ایمیل‌های ناخواسته مواجه می‌شوند. استفاده نامشروع از داده‌های پایگاه‌های اطلاعاتی هم می‌تواند توسط دولت‌ها و هم توسط اشخاص و شرکت‌های خصوصی انجام پذیرد. فرض کنید با ثبت نام در سایتی خصوصی، این سایت بدون رضایت اقدام به ارسال رایانامه‌های ناخواسته به افراد کند. در این صورت عامل این فعل غیرقانونی، اشخاص خصوصی هستند.

اینک سعی می‌کنیم به مدد قاعده زرین اخلاقی این فعل غیرقانونی را تحلیل کنیم. همان‌طور که گفتیم طبق قضیه قاعده زرین، باید با دیگران فقط طوری رفتار کرد که فرد رضایت می‌دهد در همان موقعیت

با او رفتار شود. صورت‌بندی منطقی این قضیه این است که فرد الف اطلاعات خود را با رضایت در اختیار سازمانی قرار می‌دهد؛ رضایت او فقط به استفاده موردنظر وی – به طور مثال، ثبت نام در مثال فوق– که شرطی قانونی است، تعلق می‌گیرد و سازمان موردنظر هیچ رضایتی را از وی برای انتقال اطلاعات به سازمانی دیگر اخذ نکرده است. بنابراین، انتقال اطلاعات افراد بدون اجازه آن‌ها امری غیرقانونی و غیرمنطقی است. برای اینکه این مسئله را در پرتو قاعده زرین تحلیل کنیم باید به مدد قوه تخیل خود را در همان حالت قرار دهیم.

تحلیل مسئله در چارچوب قاعده زرین اخلاقی الزاماتی دارد؛ سازواری، باوجدان بودن و بی‌طرفی. طبق سازواری نباید رفتارهای ما (با دیگران) با خواسته‌هایمان (درباره رفتاری که در موقعیت برعکس یعنی نسبت به خود ما انجام می‌شود) ناهماهنگ باشد. طبق باوجدان بودن، رفتارها و خواسته‌های ما باید با باورهای اخلاقی‌مان هماهنگ باشد و به‌عبارتی بین فکر و عمل ما تناقضی وجود نداشته باشد. بی‌طرفی نیز یعنی درباره کارهای مشابه ارزش‌گذاری‌های مشابه داشته باشیم (۱۴).

اکنون به مدد قوه تخیل قضیه منطقی را صورت‌بندی می‌کنیم. اگر مسئولین پایگاه داده که اقدام به انتقال داده‌های افراد بدون رضایت آن‌ها می‌کنند و در ازای آن به منافع اقتصادی می‌رسند، خودشان در موقعیت صاحبان داده بودند، راضی می‌شدند نسبت به آن‌ها همان رفتار مشابه انجام شود. اگر پاسخ آن‌ها منفی باشد –که در صورت بی‌طرفی، معقول بودن و باوجدان بودن، چنین است– آن‌ها دچار تعارض منطقی شده‌اند. به این معنی که خودشان در مقام عمل، چنین فعلی را انجام می‌دهند ولی اگر در موقعیت مشابه قرار داشتند، انتظار نداشتند کسی چنین رفتاری را با آن‌ها داشته باشد. اگر پاسخ آن‌ها مثبت باشد، نیز از عقلانیت اخلاقی به دور هستند زیرا هیچ انسان معقولی در شرایط مذکور راضی نخواهد بود که بدون رضایت وی اطلاعاتش به دیگران منتقل گردد و مورداستفاده قرار گیرد.

می‌توان به استدلال فوق این ایراد را وارد کرد که شاید مسئولین پایگاه داده با لحاظ کردن کلیه موارد به سؤال فوق پاسخ مثبت بدهند و با استدلالاتی نظیر عصر جهانی شدن و جریان آزاد اطلاعات این عمل را عقلانی بدانند. اینجاست که طرح کننده قاعده زرین اخلاقی ادعا می‌کند، اگر قاعده زرین اخلاقی بدون ترکیب با عوامل دیگر به‌کار رود، ممکن است وافی به مقصود نباشد (۲). به‌طور مثال، اگر عنصر آگاهی را به لوازم این قضیه اضافه کنیم، حتی اگر پاسخ مسئولین پایگاه داده‌ها در انتقال بدون رضایت داده‌ها در شرایط معکوس مثبت باشد، باز هم دچار تناقض شده‌اند و عقلانیت اخلاقی را زیر پا گذاشته‌اند. درنتیجه، همان‌طور که افراد، فارغ از موقعیتشان، راضی نیستند که بدون کسب رضایت و به‌منظور کسب سود اقتصادی، اطلاعات آن‌ها منتقل شود، باید این انتظار را در مورد اعمال خودشان نیز مراعات کنند؛ در غیر این صورت شاهد نقض قاعده زرین اخلاقی خواهیم بود.

این امر در جهان امروز بسیار رایج و شایع می‌باشد. اکثر ما ایرانیان شاهد پیامک‌ها و ایمیل‌های تبلیغاتی ناخواسته در طول روز هستیم و متأسفانه این امر در عمل موردحمایت قانونی قرار نگرفته است .پس از بیان ابعاد اخلاقی این امر در پرتو قاعده زرین اخلاقی نوبت به ارائه راه‌حل می‌رسد. تنظیم نظام حقوقی دقیق و مشخص شدن حقوق و تکالیف شهروندان و دولت‌ها تا حد زیادی می‌تواند باعث پیش‌گیری از این پدیده نامطلوب شود. به‌عبارت‌دیگر، نظام حقوقی با برقراری ضمانت اجراهای کیفری، مدنی و اداری می‌تواند از هنجارهای اخلاقی حمایت مناسبی به‌عمل آورد. در همین راستا مترقی‌ترین اقدامی که در جهان امروز در حمایت از داده‌های افراد صورت پذیرفته است، قوانینی است که اتحادیه اروپا برای حمایت از داده‌ها وضع کرده است. کشورهای دیگر ازجمله کشور ما نیز در امر وضع قوانین در جهات بسیاری از قوانین اتحادیه اروپا، به‌عنوان پیشگام قانون‌گذاری، الهام گرفته و تأثیر پذیرفته‌اند. در قسمت بعد سعی می‌شود چارچوب حقوقی اتحادیه اروپا که حمایتی برای هنجارهای اخلاقی در این زمینه است، تبیین شود و با مقایسه آن با نظام حقوقی ایران، پیشنهادهایی برای بهبود وضعیت موجود ارائه گردد.

۴– اقدامات حقوقی اتحادیه اروپا در حمایت از داده‌ها

اخلاق مقدم بر حقوق است و حقوقدانان یکی از منابع حقوق را اخلاق می‌دانند. در هر جامعه‌ای ابتدا واقعیات از صافی‌های اخلاقی و هنجاری موردقبول اکثر افراد جامعه می‌گذرد و در صورت تأیید، موردحمایت نظام حقوقی قرار می‌گیرد. بنابراین نهادهای حقوقی موردحمایت یک جامعه، اکثرشان دارای پایه‌های اخلاقی می‌باشد. نقض حریم خصوصی همان‌طور که در مبحث قبل بیان شد، امری نامطلوب می‌باشد؛ حال که ابعاد اخلاقی نقض حریم خصوصی مطرح گردید، باید به نظام حقوقی پرداخت و دید چگونه می‌توان نقض حریم خصوصی را در چارچوب آن به حداقل رساند.

ابتدا باید گفت که قوانین و دستورالعمل‌های اتحادیه اروپا یکی از منابع حقوقی کلیه کشورهای عضو آن می‌باشد و دارای اعتباری معادل قوانین داخلی آن‌ها می‌باشد؛ این مسئله بدین معنی است که کشورهای عضو نمی‌توانند قوانینی وضع کنند که در ضدیت با دستورالعمل‌های اتحادیه اروپا باشد و همچنین قوانین و دستورالعمل‌های اتحادیه اروپا در دادگاه-های داخلی کشورهای عضو دارای اعتبار می‌باشند (۱۵).

مهم‌ترین منبع قانونی اتحادیه اروپا در حمایت از داده‌ها دستورالعمل شماره 2002/58/EC است که توسط پارلمان و شورای اروپا[۱۶]تصویب شده است و جانشین دستورالعمل سال ۱۹۹۵ شده است. این دستورالعمل در سال ۲۰۰۶ و ۲۰۰۹ تکمیل شده است و هم‌اکنون ملاک عمل جوامع اروپائی، این دستورالعمل می‌باشد؛ موضوع دستورالعمل، پردازش داده‌های شخصی و حمایت از حریم خصوصی در ارتباطات اینترنتی است. البته لازم به ذکر است که در سال ۲۰۱۲ پیش-نویس لایحه جدید حمایت از داده‌ها تقدیم کمیسیون اروپا شده است که تصویب نهائی آن بنا بر پاره‌ای ملاحظات و درخواست برخی کشورها به سال ۲۰۱۵ موکول شده است. در دستورالعمل اتحادیه اروپا احکامی وجود دارد که برای حمایت از داده‌های افراد در فضای مجازی وضع شده است. تمامی احکام وضع‌شده در این دستورالعمل در راستای ماده ۸ کنوانسیون اروپائی حقوق بشر[۱۷]می‌باشند. در این ماده آمده است: «این حق افراد است که زندگی خصوصی، شخصی، مسکن و مراسلات آن‌ها

مورداحترام قرار بگیرد». از سوی دیگر، دادگاه اروپائی حقوق بشر تفسیر موسعی از حق حریم خصوصی افراد ارائه داده است که بیان‌گر اهمیت این حق بنیادین است؛ از گزاره‌های فوق می‌توان نتیجه گرفت که اتحادیه اروپا حق بر حریم خصوصی را ازجمله حقوق اولیه بشر تلقی می‌نماید.

شایان‌ذکر است که پیشینه دستورالعمل حمایت از داده‌های اتحادیه اروپا به توصیه‌نامه‌های سازمان همکاری‌های اقتصادی و توسعه[۱۸] برمی‌گردد. هرچند توصیه‌نامه‌های این سازمان بیشتر جنبه مشورتی دارد و الزامی نیست لیکن به دلیل انعکاس در دستورالعمل اتحادیه اروپا جنبه الزامی به خود گرفته است. توصیه‌نامه سازمان مذکور بر پایه ۸ مفهوم اصلی در حمایت از داده‌ها بیان شده است؛

۱- اطلاع: وقتی قرار است، داده‌های افراد جمع‌آوری شود، باید این مسئله به اطلاع آن‌ها برسد ۲- هدف: از داده‌ها فقط باید در اهداف از پیش تعیین شده و نه هر هدف دیگری استفاده شود. ۳- مشخص شدن هدف گردآوری داده‌ها: هدف استفاده از داده‌ها باید همزمان با گردآوری آن‌ها ذکر گردد و نه پس‌ازآن. ۴- رضایت: داده‌ها نباید بدون رضایت صاحبان داده، افشاء شوند، مگر اینکه حکم قانونی در این زمینه وجود داشته باشد ۵- امنیت: داده‌های گردآوری شده باید نسبت به هرگونه سوءاستفاده احتمالی مصون باشند. ۶- افشاء: صاحبان داده باید مطلع باشند که چه کسانی داده‌های آن‌ها را جمع‌آوری می‌کنند ۷- دسترسی: باید به صاحبان داده اجازه داد تا به داده‌های خود دسترسی داشته باشند و داده‌های غیردقیق خود را اصلاح کنند ۸- مسئولیت‌پذیری: باید سازوکاری برقرار باشد که طبق آن، صاحبان داده بتوانند، افرادی را که داده‌های آن‌ها را جمع‌آوری می‌کنند نسبت به رعایت موارد فوق مسئول بدانند (۱۶). این هشت اصل در دستورالعمل اروپائی نیز انعکاس یافته و موضوع احکام حقوقی الزام‌آور قرار گرفته است. می‌توان هر یک از موارد ذکرشده را به گزاره‌ای اخلاقی نیز تعبیر کرد؛ به‌طور مثال، در مورد سوم می‌توان گفت اگر مسئولین پایگاه داده، بدون رضایت صاحبان داده، داده‌های مربوط به آن‌ها را افشاء کنند، نه‌تنها عملی غیرقانونی اتفاق افتاده است بلکه حکمی اخلاقی نیز در این باب نقض شده است. اهمیت این اصول هشتگانه تا جائی است که عین این عبارات در نظام حمایت از داده‌های ایالات‌متحده آمریکا نیز آمده است. به‌طور مثال، در قسمت «ب» بند ۱ ماده ۲ قانون «استفاده از امنیت، حمایت و حریم خصوصی» مصوب ۲۰۱۳، قانون‌گذار اپراتورهای تلفن همراه را موظف کرده است که پیش از گردآوری پایگاه داده‌ها از اطلاعات افراد، از آن‌ها کسب رضایت کنند. (۱۷)

داده‌های قابل حمایت در فضای مجازی فراوان‌اند و می‌توان مصادیق زیادی را با مقسم‌های مختلف برای آن در نظر گرفت؛ به‌طور مثال، به اعتبار حساسیت داده‌ها می‌توان آن‌ها را به دودسته داده‌های حساس و غیر حساس تقسیم کرد؛ از سوی دیگر می‌توان با ضابطه «موضوع داده‌ها » آن‌ها را به انواع مختلف مانند پزشکی، جنسی، شخصی و ... تقسیم‌بندی کرد. بحث اساسی در اینجاست که هر نظام حقوقی با توجه به نظام اخلاقی و هنجارهای موردقبول آن جامعه و نیز با توجه به عرف و آداب‌ورسوم ارزش‌های خود نسبت به حمایت از داده‌ها اقدام کرده است؛ در این زمینه نمی‌توان نسخه‌ای یکسان برای تمامی کشورها تجویز کرد بلکه هر کشور فراخور نظام فرهنگی خود باید داده‌پیام‌های موردنظر را مشمول حمایت قرار دهد. دستورالعمل اتحادیه اروپا در بند الف ماده ۲ حیطه شمول حمایت خود را مشخص کرده است. طبق این ماده، داده‌هایی موردحمایت است که مربوط به اشخاص تعیین هویت شده یا ناشناس باشند. افراد شناخته‌شده نیز افرادی هستند که به‌واسطه شاخصه‌هایی چون کد شناسایی، ویژگی‌های جسمی، روان‌شناختی، ذهنی، اقتصادی، فرهنگی یا هویت اجتماعی قابل‌شناسایی هستند.

بند ۲ ماده ۲ نیز فعالیت‌های ناقض حریم خصوصی اطلاعاتی را در مورد داده‌های شخصی برشمرده است و آن را به اقسام پردازش داده‌ها تسری داده است. پردازش داده‌ها اعم از پردازش دستی و یا خودکار داده‌هاست و شامل اموری چون جمع‌آوری، ضبط، ذخیره‌سازی سازمانی، جرح‌وتعدیل، بازیابی، جایگزینی، استفاده، افشاء، انتشار، ادغام یا ترکیب، انسداد، محو یا نابودی داده می‌شود. مصادیق نقض حریم خصوصی اطلاعاتی و تفاسیر موسعی که از حیطه حمایت از آن‌ها به‌عمل‌آمده است، مبین اهمیت مسئله و آسیب‌پذیری بحث حریم خصوصی در فضای مجازی است. احصاء موارد نقض حریم خصوصی این امتیاز را دارد که ضمانت اجرای کیفری را تسهیل می‌کنند و ناقضان نمی‌توانند به بهانه عدم ذکر مصادیق نقض از زیر بار مجازات رها گردند.

هرچند امروزه دولت‌ها با توجه به اقتدار حاکمیتی خود می‌توانند بانک‌های داده گسترده‌ای را از اطلاعات افراد فراهم کنند و توجیه خود را در این زمینه نیاز به سیاست‌گذاری و آینده‌نگری عنوان کنند، لیک هر یک از موارد فوق، تکالیفی را برای دولت و حقوقی را برای شهروندان ایجاد می‌کند که در صورتی تخطی از هرکدام بحث مسئولیت حقوقی و اخلاقی پیش می‌آید (۸). اتحادیه اروپا با توجه به حساسیت امر، صلاحیت حمایتی خود را گسترش داده است؛ به‌طوری‌که حتی اگر داده‌های هر یک از شهروندان اتحادیه اروپا در خارج از حوزه اروپا مشمول نقض قرار بگیرند، آن‌ها را موردحمایت قرار داده است (ماده ۴ دستورالعمل).

نکته قابل انتقادی که در این دستورالعمل مشاهده می‌شود، بند ۳ ماده ۱ آن است که مواردی را از شمول قانون مستثنا کرده است؛ در این ماده فعالیت‌های مربوط به امنیت عمومی و مسائل مربوط به رفاه اقتصادی در مواردی که مربوط به امنیت ملی می‌شوند و فعالیت‌های مربوط به حقوق کیفری دولت‌ها از حیطه حمایت مستثنا شده است؛ یکی از انتقاداتی که به چنین سبک نگارشی وارد است، این است که در مقام استثناء، از مفاهیم کلی با مصادیق مبهم استفاده شود زیرا این مسئله می‌تواند مستمسک دولت‌ها در نقض حریم خصوصی و حقوق مسلم افراد قرار گیرد (۱۸). پیشنهاد این است که وقتی قانون چنین استثنائات وسیعی را معین می‌کند، مصادیق آن را نیز ذکر کند تا باعث سلیقه‌ای عمل کردن نشود. البته دستورالعمل، در ماده ۱۵ خود سعی کرده است این نقیصه را به‌نوعی جبران کند؛ در این ماده محدودیت‌های وضع‌شده را مشروط به ضروری بودن و متناسب بودن دانسته است و بیان کرده است که محدودیت‌ها باید مناسب جامعه‌ای دموکراتیک برای حفاظت از

امنیت ملی باشد. در این ماده همچنین مواردی چون دفاع ملی و پیگیری جرائم کیفری ذکرشده است که البته تعیین مصادیق همین مفاهیم کلی نیز با مشکل مواجه می‌گردد.

ماده ۴ دستورالعمل، دولت را مجاز دانسته است تا بر فعالیت‌های خدمات دهندگان سرویس‌های اینترنت نظارت داشته باشد و آن‌ها را از اقدامات سوء نسبت به داده‌ها منع کند. بند ۳ همین ماده تأمین‌کنندگان خدمات را ملزم کرده است که در صورت مواجهه با نقض اصول مربوط به حمایت از داده‌ها، قضیه را به مقامات ذی‌صلاح اطلاع دهند.

نکته قابل‌تأمل دیگری که وجود دارد، نحوه حمایت از داده‌های ترافیکی است. طبق بند «ب» ماده ۲ دستورالعمل، داده‌های ترافیکی داده‌هایی هستند که برای برقراری ارتباطات الکترونیک و همچنین محاسبه هزینه استفاده از اینترنت لازم هستند؛ نتیجه منطقی این ماده این است که تأمین‌کنندگان خدمات اینترنتی می‌توانند برای محاسبه هزینه استفاده از اینترنت، به داده‌های مذکور دسترسی داشته باشند. حمایت از داده‌های ترافیکی در ماده ۶ دستورالعمل منعکس شده است؛ در این ماده بر این مسئله تأکید شده است که داده‌های ترافیکی به‌محض اینکه دیگر نیازی به استفاده از آن‌ها برای مقاصد فوق نباشد، باید پاک شود؛ مطلوب این بود که ماده ضمانت اجرائی را نیز برای نقض این عمل مقرر می‌کرد. در کنار داده‌های ترافیکی، یکی دیگر از انواع آسیب‌پذیر داده‌ها نیز داده‌های مکانی هستند. به‌طور مثال، اپراتورهای تلفن همراه برای ارائه خدماتی که نیاز به شناسایی محل افراد است، به این‌گونه داده‌ها دسترسی دارند (۱۹). بدیهی است که استفاده از این داده‌ها نیز باید تابع اصول هشتگانه‌ای باشد که پیش از این بیان شد.

یکی دیگر از مسائل قابل‌طرح درزمینه حمایت از داده‌ها به‌ویژه در مورد پایگاه داده‌ها، تعارض گردش آزاد اطلاعات و نقض حریم خصوصی است؛ توضیح اینکه طبق قانون آزادی اطلاعات (موضوع دستورالعمل سال ۲۰۰۳ اتحادیه اروپا) افراد حق دسترسی آزاد به اطلاعات مگر در موارد استثناء را دارند؛ نقض حریم خصوصی استثنای وارده بر آزادی گردش اطلاعات است؛ قانون‌گذار باید مدنظر داشته باشد که حیطه استثنا را به‌قدری گسترش ندهد که به اصطلاح حقوقی دچار تخصیص اکثر شود؛ البته این گزاره به معنای قربانی کردن حق حریم خصوصی افراد نیست؛ حساسیت در موردحمایت از حریم خصوصی افراد در اتحادیه اروپا را می‌توان از ماده ۱۲ دستورالعمل استنتاج کرد؛ در این ماده حتی در دسترس قرار گرفتن داده‌های افراد در سیستم‌های جستجو نیز منوط به رضایت آن‌ها شده است و افراد می‌توانند در صورت عدم تمایل، داده-های خود را از سیستم‌های جستجو نیز محو کنند. برای اتخاذ رویکردی منطقی در این زمینه، روش احصای داده‌های موردحمایت افراد در قوانین، موجه به نظر می‌رسد؛ یعنی همان راهی که در دستورالعمل اتحادیه اروپا آمده است.

۵- تجربه‌های قابل‌اعمال در نظام حقوقی ایران

نظام حقوقی ایران با دریافت اهمیت حمایت از داده‌های شخصی در فضای مجازی در عصر ارتباطات گام‌هایی را در این زمینه برداشته است. یکی از مشکلاتی که درزمینه تدوین قوانین و مقررات در حقوق فناوری اطلاعات وجود دارد، عبارت است از سیال بودن موضوعات مرتبط با فناوری اطلاعات؛ به‌عبارت‌دیگر با توجه به‌سرعت بالای تولید علم در این زمینه، هرروزه با فناوری‌های جدیدی مواجه هستیم که نظام قانون‌گذاری به‌سختی می‌توان همپای آن باشد؛ راه‌حل این مشکل سراسری، به‌روز کردن قوانین درزمینه فناوری اطلاعات است؛ همان‌طور که مشاهده شد، اتحادیه اروپا در طی ۱۹ سال تاکنون، چهار بار اصلاحیه‌ها و مکمل‌هایی را بر قوانین حمایت از داده اعمال کرده است.

در نظام حقوقی ایران، مهم‌ترین قوانینی که در این راستا وضع شده‌اند عبارت‌اند از: قانون تجارت الکترونیک (مصوب ۱۳۸۲) و قانون جرائم رایانه‌ای (مصوب ۱۳۸۸). آیین‌نامه‌هایی نیز در برخی از سازمان‌های دولتی تکالیفی را درزمینه ممنوعیت نقض حریم خصوصی برقرار کرده‌اند که ارزش و اعتبار قانون را ندارند و فقط قابل‌اجرا در همان سازمان هستند. در این مبحث سعی داریم تا کاستی‌های نظام حقوقی ایران درزمینه حمایت از داده‌ها را ذکر کرده و با استفاده از اقدامات اتحادیه اروپا، پیشنهادهایی را برای بهبود آن ذکر کنیم.

نخستین انتقادی که بر نظام حقوقی ایران درزمینه حمایت از داده‌ها وارد است، این است که رژیم حقوقی خاصی را برای حمایت از داده‌ها مشخص نکرده است و در قوانین مختلف، به‌صورت پراکنده به این موضوع اشاره کرده است؛ برای حمایت از حریم خصوصی و سایر نهادهای حقوقی، دو رویکرد کلان وجود دارد؛ نگاه اول این است که الگویی جامع برای حمایت از نهادها برقرار کنیم به این معنی که احکام مفصلی را در یک قانون واحد راجع به موضوعی واحد برقرار سازیم؛ نمونه‌های بارز این رویکرد نظام آمریکا و کانادا است؛ در این کشورها قانون جامعی تحت عنوان حمایت از حریم خصوصی یا حمایت از داده‌ها وجود دارد؛ در رویکرد دوم، مجموعه حمایت‌های نظام حقوقی را باید با استقراء در قوانین یافت (۹)؛ نظام ایران از این مدل پیروی کرده است؛ پیشنهاد این است که برای حمایت فراگیر از حریم خصوصی قانونی جامع در این زمینه وضع شود و اقسام آن را برشمرد؛ البته شایان‌ذکر است که در ایران در سال ۱۳۸۱ تلاش مشابهی صورت گرفته است؛ در این سال پیش‌نویس لایحه حمایت از حریم خصوصی به امضای رئیس‌جمهور وقت رسید که تاکنون در مجلس موردبررسی و تصویب قرار نگرفته است. پیش‌نویس لایحه مذکور تا حد زیادی متأثر از دستورالعمل اتحادیه اروپا است که به علت عدم به‌روزرسانی از یافته‌های جدید اتحادیه اروپا و قوانین مشابه در آن استفاده نشده است. این پیشنویس بخشی را به حریم خصوصی اطلاعات و ارتباطات اختصاص داده است و حاوی احکامی در خصوص حمایت از داده‌ها است؛ البته حمایت‌های صورت گرفته در این پیش‌نویس نیز از حیث حیطه شمول، کامل نبوده و نیاز به اصلاح دارد.

یکی دیگر از کاستی‌های مهمی که در نظام حمایت از داده‌ها در ایران وجود دارد و می‌توان سازوکاری مشابه دستورالعمل اتحادیه اروپا برای آن برقرار کرد، اشاره به نقض اصول هشت‌گانه‌ای است که در مبحث پیشین مطرح شد. در مبحث پیشین به داده‌های ترافیکی اشاره شد؛

دستورالعمل اتحادیه اروپا علاوه بر حمایت از داده‌های ترافیکی، از داده‌های مکانی نیز حمایت به‌عمل‌آمده است. طبق بند «ج» ماده ۲ دستورالعمل، داده‌های مکانی داده‌هایی هستند که وقتی توسط شبکه‌های ارتباطی الکترونیک[۱۹] پردازش می‌شوند، موقعیت جغرافیایی ابزارهای ارتباطی را مشخص کنند؛ به‌عبارت‌دیگر وقتی داده‌های افراد در فضای مجازی پردازش می‌شوند، موقعیت جغرافیایی اتصال آن‌ها به شبکه مشخص می‌گردد. سوءاستفاده‌ای که از داده‌های مکانی می‌تواند به‌طور بالقوه به‌عمل بیاید، بحث بازاریابی الکترونیک است؛ در ایران در عمل شاهد این مورد، چه در ارتباط با پیامک‌های تلفنی ناخواسته و چه ایمیل‌های تجاری، می‌باشیم که سازوکار مناسبی برای آن تهیه نشده است؛ این مورد نقض مسلم حریم خصوصی افراد و ناقض عنصر «رضایت» می‌باشد. به‌طور مثال، وقتی سازمانی تجاری شماره‌های تماس افراد ساکن در یک منطقه را در ازای پرداخت پول به شرکت‌های خدمات ارتباطی به‌دست می‌آورد و به آن‌ها پیامک‌های ناخواسته می‌فرستد، باعث نقض حریم خصوصی افراد می‌گردد؛ دستورالعمل اتحادیه اروپا در ماده نُه، این مسئله را پیش‌بینی کرده است. طبق این ماده، در صورت نیاز به تحلیل داده‌های مکانی، نخست این داده‌ها باید بدون نام تحلیل شوند و اگر قرار باشد داده‌های مکانی با نام تحلیل گردند، باید در مدت‌زمان معین و نیز با رضایت صاحب داده باشند؛ امری که گاهی اوقات در عمل در کشور ما رعایت نمی‌گردد و بسیاری از افراد شاهد ارسال پیامک‌ها و ایمیل‌های ناخواسته از طرف اشخاص و مؤسسات تجاری هستند؛ پیشنهاد می‌گردد سازوکاری حقوقی همراه با ضمانت اجرای مؤثر در این زمینه برقرار گردد تا از سوءاستفاده‌های احتمالی جلوگیری به‌عمل آید. در همین راستا، بحثی نیز در مورد ایمیل‌های اتوماتیک مطرح می‌گردد که به‌نوعی ایمیل ناخواسته محسوب می‌گردد؛ ایمیل‌های اتوماتیک نیز جزو دسته ایمیل‌های ناخواسته محسوب می‌گردند؛ در این دسته از ایمیل‌ها نیز ماده ۱۳ دستورالعمل اتحادیه اروپا، ارسال آن‌ها را مسبوق به رضایت پیشین صاحب ایمیل می‌داند.

مسئله دیگری که در دستورالعمل اتحادیه اروپا پیش‌بینی شده است و در نظام حقوقی ایران علی‌رغم تأثیرپذیری از این دستورالعمل، به‌طور ناقص بدان پرداخته شده است، ممنوعیت پردازش برخی داده‌های شخصی تحت عنوان داده‌های حساس است. در دستورالعمل اتحادیه اروپا شماره 95-46-EC که مکمل دستورالعمل پیشین است و مواد آن همچنان قابل استناد است، مصادیق داده‌های حساس مشخص شده است؛ طبق ماده ۸ این دستورالعمل، اعضای اتحادیه اروپا باید از پردازش داده‌هایی با موضوعات نژادی، قومی، عقاید سیاسی، مذهبی یا اعتقادات فلسفی، عضویت در اتحادیه‌های تجاری و پردازش داده‌های مرتبط با سلامت و زندگی جنسی امتناع کنند. البته دستورالعمل موارد استثناء را نیز مشخص کرده است و آن‌ها را شامل این موارد دانسته است: أخذ رضایت صریح از صاحب داده، مواردی که تحلیل داده به‌منظور دستیابی به اموری درزمینه حقوق استخدامی توسط ممیزان و به‌موجب قوانین داخلی کشورها مجاز باشد، زمانی که پردازش داده برای حمایت از حقوق اساسی صاحب داده لازم باشد و به لحاظ ناتوانی‌های جسمی یا قانونی نتوان رضایت آن‌ها را جلب کرد؛ پردازش داده افراد عضو در مجامع، انجمن‌ها و اتحادیه‌های تجاری به‌گونه‌ای که در راستای اهداف، انجمن، شورا یا اتحادیه باشد و همچنین حفاظت‌های لازم از آن‌ها به عمل آید و بدون رضایت به شخص ثالث منتقل نشود؛ پردازش داده‌هایی که به‌منظور رسیدگی به ادعاهای حقوقی ضروری باشد، پردازش داده‌ها به‌منظور تشخیص بیماری‌های مسری توسط تیم متخصص پزشکی طبق قوانین داخلی هر کشور؛ در ادامه نیز دستورالعمل اجازه برقراری استثنائات بیشتری را به نظام حقوقی هر کشور داده است. قانون‌گذار ایران تقسیم داده‌های شخصی را به داده‌های شخصی حساس و داده‌های شخصی عمومی نپذیرفته است و از آثار حقوقی این تقسیم‌بندی بهره نجسته است. درحالی‌که رویه اکثر نظام‌های حقوقی به سمت پذیرش این تقسیم‌بندی و لحاظ کردن آن در قوانین حمایت از داده است (۹).

در ماده ۵۸ قانون تجارت الکترونیک داده‌های موردحمایت در حقوق ایران احصاء شده است. طبق این ماده: «ذخیره، پردازش و یا توزیع داده‌پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است». قانون‌گذار از انواع داده‌های شخصی حساس، داده‌های تجاری- اقتصادی را موردحمایت قرار نداده است که با توجه به ارزش آن‌ها در اقتصاد امروز و ظهور مفاهیمی چون اسرار تجاری و ... به‌نوعی خلأ محسوب می‌گردد. همچنین قانون‌گذار در مورد ممنوعیت پردازش داده‌های مربوط به محکومیت‌های کیفری افراد سکوت کرده است و آن را مشمول حمایت خود قرار نداده است. عدم‌حمایت از این دودسته داده‌های مهم نقض صریح حریم خصوصی افراد به‌حساب می‌آید. نتیجه عملی این عدم‌حمایت این است که اگر داده‌های مربوط به محکومیت‌های کیفری افراد و نیز داده‌های تجاری وی در فضای مجازی افشاء شود، به لحاظ قانونی هیچ‌گونه اقدامی در حمایت از قربانیان نمی‌توان به‌عمل آورد؛ امید است قانون‌گذار در اصلاحات بعدی این نقایص را اصلاح کند.

## نتیجه‌گیری

استفاده از داده‌های افراد در قالب پایگاه داده‌ها شیوه رایجی است که هم دولت‌ها و هم سازمان‌های خصوصی در دهه اخیر و با رشد فناوری اطلاعات از آن بهره گرفته‌اند. استفاده از اطلاعات موجود در این پایگاه‌ها می‌تواند اهداف مشروع و نامشروعی داشته باشد. اگر هدف استفاده از داده‌ها از ابتدا قید شود و مورد تأیید صاحب داده قرار گیرد یا به‌حکم قانون باشد، استفاده از داده‌ها مجاز است ولیکن اگر عنصر رضایت در استفاده از داده‌ها مدنظر قرار نگیرد، استفاده نامشروع و غیرقانونی تلقی می‌گردد.

مسئله استفاده نامشروع از پایگاه داده‌ها را می‌توان با رویکردها و نظریات مختلف اخلاقی موردبررسی قرارداد لیکن ما در این مقاله محک سنجش را قاعده زرین اخلاقی قرار دادیم. طبق قاعده زرین اخلاقی با

دیگران فقط باید طوری رفتار کرد که فرد رضایت دارد در موقعیت مشابه با او رفتار شود. اگر قاعده زرین اخلاقی را همراه با عناصری چون وجدان، بی‌طرفی، آگاه بودن و معرفت به‌کار بندیم می‌توان آن را به ضابطه‌ای جهانی تأویل کنیم که ما را گرفتار تناقض منطقی در باورها و رفتارهایمان نمی‌کند. در قضیه استفاده از داده‌ها بدون اجازه و رضایت افراد، صورت‌بندی منطقی آن بدین‌صورت شد که اگر مسئولین پایگاه-های داده خود را به‌جای صاحبان داده بگذارند، به‌شرط بی‌طرفی، باوجدان بودن، آگاه بودن و همچنین با پیش‌شرط دانستن نامطلوب بودن نقض حریم خصوصی، هرگز راضی به انجام چنین عملی در حق خود نمی‌شوند از این رو در این زمینه دچار تناقض می‌گردند.

پس از اثبات تناقض درزمینه استفاده از داده‌ها بدون رضایت افراد نوبت به طراحی نظام حقوقی دقیق جهت پیش‌گیری و منع افراد از انجام این عمل غیرقانونی می‌رسد. بدیهی است که هنجارهای اخلاقی اگر با ضمانت اجراهای حقوقی تلفیق شوند، قابلیت اجرای بیشتری دارند. درزمینه نظام حقوقی حاکم بر حمایت از داده‌ها با بیان وضعیت حقوقی ایران، نواقص آن درزمینه فقدان رژیم حقوقی خاص، پراکندگی قوانین، عدم عام‌الشمول بودن آن‌ها و عدم‌حمایت از برخی داده‌پیام‌ها مشخص می‌گردد. قانون‌گذار ایران برای اصلاح این نقیصه می‌تواند از حقوق تطبیقی کمک بگیرد و با استفاده از تجربیات سایر کشورها به غنای نظام حقوقی خود در این زمینه بپردازد. از میان رژیم‌های حقوقی مختلف، رژیم حقوقی اتحادیه اروپا به دلیل به‌روز بودن و پیشگام بودن در این زمینه مبنای مقایسه تطبیقی ما قرار گرفت و با تحلیل مواد آن درزمینه حمایت از داده‌ها، اصول و قواعدی مطرح شد که اگر قانون‌گذار در قوانین بعدی خود بدان‌ها نظر داشته باشد، امکان حمایت از داده را در نظام حقوقی خود گسترش داده است.

## ملاحظه‌های اخلاقی

در این پژوهش مروری با معرفی منابع مورد استفاده، اصل اخلاق امانت داری علمی رعایت و حق معنوی مولفین آثار محترم شمرده شده است.

## واژه نامه

| | |
|---|---|
| 1. Data base | پایگاه داده‌ها |
| 2. Privacy | حریم خصوصی |
| 3. Meta ethics | فرا اخلاق |
| 4. Normative ethics | اخلاق هنجاری |
| 5. Normative theory | نظریه هنجاری |
| 6. Golden rule | قاعده زرین |
| 7. Applied normative ethics | اخلاق هنجاری کاربردی |
| 8. Cultural relativism | نسبی نگری فرهنگی |
| 9. Individualism | شخصی انگاری |
| 10. Super naturalism | فراطبیعت گرایی |
| 11. Intuitionism | شهود باوری |
| 12. Emotionalism | عاطفه گرایی |
| 13. Prescriptivism | توصیه گرایی |
| 14. Consequentialism | پیامدگرایی |
| 15. Non- consequentialism | ناپیامدگرائی |
| 16. European commission | شورای اروپا |
| 17. European Convention on Human Rights (ECHR) | کنوانسیون اروپائی حقوق بشر |
| 18. OECD | سازمان توسعه و همکاری های اقتصادی |
| 19. Electronic communications network | شبکه‌های ارتباطی الکترونیک |

## References


1. Reitz M. (2010). Information ethics. Online dictionary for library and information science. Available at: http://www.abc-clio.com/ODLIS/odlis_i.aspx. Accessed: 12 Feb 2014 .
2. EUR-Lex (2002). E-Privacy directive. Available at: www.privacycommission.be/en/node/3874. Accessed: 8 Feb 2014
3. Harry JG. (2006). Ethics: a contemporary introduction. Translated by: Behreyni H. (2013) Tehran: Asemane Khial Publication. Pp. 31, 193-213. (In Persian).
4. Clayton P, Schloss J. (2004). In evolution and ethics: human morality in biological and religious perspective. New York: Eerdmans. P. 78.
5. Antony F. (1979). Golden rule: a dictionary of philosophy. London: The Macmillan Press. P. 134.
6. Kant I. (1780). The metaphysical elements of ethic. Edited by: Thomas KA. USA: The Pennsylvania State University Publication. P. 25.
7. Johnathan J. (2008). What can information technology do for law? Harvard Journal of Law & Technology; 21 (2): 13-17.
8. Tanni J. (2010). Privacy and confidentiality in data mining. Lisbon: Lisbos Publication. P. 132
9. Aslani H. (2005). IT law. Tehran: Mizan Publication. P. 20. (In Persian).
10. Kadkhodayi A. (2004). Global information networks with emphasis on privacy and human rights violations, [10 pages]. Available at: www.iranwsis.org/default.asp?c=IRAR&R=&1=115#BN115. Accessed: 17 Jan 2014. (In Persian).
11. Ansari B. (2012). Privacy law. Tehran: Samt Publication. P. 38. (In Persian) ..
12. Gov. UK. (2007). Civil service management code. Available at: https://www.gov.uk/government/publications/civil-servants-terms-and-conditions. Accessed: 5 May 2017.
13. Waldo J, Lin S. (2007). Engaging privacy and information technology in a digital age. UK: The National Academies Press. P.18.
14. Gensler H. (1996). Formal ethics. 1st ed. UK: Rutledge Publication. P.52.

15. Treaty on the functioning of the European Union (TFEU). (1965). article 245. Available at: http://www.jus.uio.no/english/services/library/treaties/09/9-01/tfeu_cons.xml. Accessed: 22 Feb 2014.
16. OECD. (2013). the OECD data protection principles. Available at: http://oecdprivacy.org. Accessed: 10 Feb 2013.
17. APPS (2013). Application Privacy Protection, and Security Act. Available at: www.hankjohnson.house.gov/APPS_Act_Key_Provisions.pdf. Accessed: 15 Jan 2014.
18. Machina KF. (1976). Truth, belief and vagueness. Philosophical Logic Journal; 15 (9): 78-83 .
19. Evans G. (1978). Can there be vague objects? Analysis; 38 (4): 208.
20. Kristina I, Giacomo L. (2013). Online personal data processing and eu data protection reform. USA: CEPS Task Force Reports. P. 21.