معارف اسلامی و حقوق، سال هشتم، شماره اول ـ بهار و تابستان ۱۳۸٦، صص ۱۷۳ - ۱۹٦

# حریم خصوصی ارتباطات اینترنتی(مطالعه در حقوق ایران و اتحادیه اروپا)

**ستار زرکلام***

تاریخ دریافت: ۱۳۸۶/۲/۲۸
تاریخ پذیرش: ۱۳۸۶/۵/۸

**چکیده:**

*حریم زندگی خصوصی، امروزه به دلیل ظهور فن‌آوری‌های اطلاعاتی و ارتباطی نوین مورد تهدید قرار گرفته است. از یک سو، اینترنت دسترسی به داده‌های شخصی، هم چنین تحریف و تخریب آن‌ها ونیز بهره برداری از هویت اشخاص و انتشار این اطلاعات را برای اهداف غیر مجاز تسهیل می‌کند و از سوی دیگر، امکان ردیابی اطلاعات مرتبط با هویت فرد و محتوای پیام‌های ارسالی را فراهم می‌سازد.*

*اما در قواعد ناظر بر حمایت از زندگی خصوصی، این فناوری جدید کمتر مورد توجه قرار گرفته است. هر نوع اطلاعات که جنبه شخصی دارند، نظیر اطلاعات جسمانی، تصویر، صدا، روابط جنسی، عقاید فلسفی، مذهبی، سیاسی، ریشه‌های نژادی و قومی و حتی نوع علائق و سلیقه‌ها به محض آن که از طریق داده‌های الکترونیکی مورد پردازش قرار می‌گیرند باید مورد حمایت قانون‌گذار قرار گیرند.*

*این مقاله با هدف بررسی مفاهیم اساسی مرتبط با حریم خصوصی داده‌های شخصی و سیر تحول قانون‌گذاری در این زمینه و مطالعه مقررات حقوق ایران و اتحادیه اروپا در زمینه داده‌های شخصی و تنگناهای حقوقی حمایت از داده‌های شخصی تدوین شده است.*

**واژگان کلیدی**

*حریم خصوصی، داده‌های شخصی، اصول حاکم بر داده‌های شخصی، گردش آزاد داده‌ها، تعارض مکانی قوانین کیفری*

---

* عضو هیات علمی گروه حقوق دانشگاه شاهد

**مقدمه**

بهره‌گیری از ابزارهای فنی موجود بـه منظـور حمایـت از داده‌هـا نظیـر فیلتـر کـردن و رمزنگاری[1] ضروری و مفید هستند ولی به هیچ وجه کافی نیستند. برای حمایت کافی و مؤثر از حریم خصوصی داده‌های شخصی در ارتباطات الکترونیکـی از جملـه اینترنـت وجود قواعد حقوقی متناسب با چنین حمایتی اجتناب ناپذیر هستند.

این قواعد از مدت‌ها پیش در قالب مقررات قانونی در حقوق برخـی از کـشورهـا وارد شده است. اولین قانون ملی حمایت از داده‌ها در سـال ۱۹۷۳ در سـوئد تـصویب شد(رک. قاجار، ۱۳۷۹، ص ۷۵ ). همچنین می‌تـوان بـه قـانون حمایـت از داده[2] سـال ۱۹۸٤ انگلستان که در سال ۱۹۹۸ با قانونی به همـین نـام جـایگزین شـد( Bainbridge, 2000, P. 35 ) و نیز قـانون شـماره ۱۷–۷۸ مـورخ ٦ ژانویـه ۱۹۷۸ فرانـسه «راجـع بـه انفورماتیک، فایل‌ها و آزادی‌ها» که به ویژه با قانون مورخ ۱۸ ژوئه ۲۰۰۱ تحت عنـوان «حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخـصی» مـورد اصـلاح واقـع شده است اشاره کرد.( Loi n. 78-17 du 6 janvier 1978 relative à l'informatiques, aux fichiers et aux liberté, p. 354. ).

غیر از کشورهایی که حمایـت از داده‌هـای شخـصی را در قالـب قواعـد حقـوقی درآورده‌اند، برخی از سازمان‌های بین‌المللی از مدت‌ها پیش گام‌های مهمی در این زمینه برداشته‌اند. از آن جمله می‌توان سازمان همکاری و توسعه اقتصادی سازمان ملل متحـد OECD را نام برد که در سال ۱۹۷۷ اصولی را به منظور حمایـت از داده‌هـا ارائـه کـرده است هرچند که این اصول بیشتر توسعه تجارت و اقتصاد را در نظر داشته‌اند. به علاوه، سازمان ملل‌متحد با توجه به پیشرفت‌های فنـاوری واطلاعـاتی بـه موضـوع از دیـدگاه حقوق بشر نگریسته و در سال ۱۹۹۰ رهنمودهایی برای قانون‌گذاری فایل‌های داده‌های شخصی رایانه‌ای ارائه کرده است. ازهمه مهم‌تر باید به پارلمان و شـورای اروپـا اشـاره کرد که از سال ۱۹۷٦ فعالیت خود را برای تدوین دستورالعمل‌هایی بـرای کـشورهـای عضو در خصوص حمایت از داده‌های شخصی آغـاز کـرده اسـت( قاجـار، ۱۳۷۹، ص ۷۳) که ازآن جمله دستورالعمل‌های تصویب‌شده در سال‌هـای ۱۹۹۵، ۲۰۰۲ و ۲۰۰٦ را می‌توان نام برد.

در حقوق ایران، تاکنون مقررات خاصی برای حمایت ازحـریم خـصوصی وجـود ندارد و لایحه‌ای که در سال‌های اخیر در این زمینـه تـدوین شـده هنـوز بـه تـصویب

نرسیده است. با این حال، حمایت از داده‌های شخصی برای اولین بار در قانون تجارت الکترونیکی مصوب سال ۱۳۸۲مورد توجه قرار گرفته است. هر چند چنین حمایتی را باید به فال نیک گرفت، ولی این مقررات در مقایسه با مقررات سایر کشورها و مقررات سازمان‌های بین‌المللی در این خصوص دارای ایرادات جدی است.

برای بررسی ابعاد مختلف حریم خصوصی ارتباطات در شاه‌راه‌های اطلاعاتی یا اینترنت ابتدا به بررسی مفهوم اطلاعات شخصی و مفاهیم مرتبط وسیر تحول قانون‌گذاری در زمینه حمایت از حریم خصوصی داده‌های شخصی(مبحث اول) می‌پردازیم. سپس نحوه حمایت از حریم خصوصی داده‌های شخصی در حقوق ایران و اتحادیه اروپا مورد بررسی قرار می‌گیرد( مبحث دوم) پس از آن مسایل مهم حقوقی مرتبط با حریم خصوصی داده‌های شخصی مورد تحلیل قرار گفته و سرانجام به نقد مقررات ایران در خصوص داده‌های شخصی می‌پردازیم(مبحث چهارم).

### ۱. مفاهیم مرتبط با گردآوری و پردازش داده‌های شخصی وسیرتحول قانون‌گذاری در این زمینه

#### ۱-۱. مفاهیم مرتبط با گردآوری و پردازش داده‌های شخصی

در زمینه گردآوری و پردازش داده‌های شخصی، اصطلاحات و مفاهیمی مورد استفاده قانون‌گذار ایرانی و کشورهای مختلف قرار گرفته که آشنایی با آن‌ها برای درک بهتر قواعد حقوقی حاکم دراین خصوص که در این مقاله مورد بحث قرار گرفته اند مفید به نظر می‌رسد.

**داده‌های شخصی**، داده‌ها و اطلاعات زمانی با نام یا شخصی تلقی می‌شوند که، به طور مستقیم شناسایی افراد حقیقی را ممکن سازد. داده‌هایی که مستقیماً شخصی تلقی می‌شوند عبارتند از: نام و نام خانوادگی اشخاص، و داده‌هایی که به طور غیرمستقیم شخصی تلقی می‌شوند عبارتند از: آدرس جغرافیایی یا پستی، شماره ملی، شماره گواهینامه رانندگی، شماره حساب بانکی. شماره کارت بانکی، شماره اشتراک آب و برق و تلفن و گاز، هم چنین عکس یا تصویری که شناسایی شخص را ممکن سازد .(Vivant et autres,. 2002, n. 4902, p. 854. )

**پردازش الکترونیکی اطلاعات شخصی**، که در بحث از حریم خصوصی ارتباطات الکترونیکی ممنوعیت‌ها و محدودیت‌هایی برای آن وضع شده، عبارت است از: مجموعه عملیاتی که با استفاده از وسایل اتوماتیک، جمع‌آوری، ثبت، تدوین، تغییر، حفظ و انهدام اطلاعات شخصی را ممکن می‌سازد و هم چنین مجموعه عملیاتی با

همان ماهیت که امکان بهره‌برداری از فایل‌ها یا پایگاه داده و به ویژه، ارتباطات همزمان یا تماس‌ها، مشاوره‌ها یا تبادل اطلاعات شخصی را فراهم می‌سازد.( Cf. Loi n. 78-17 (du 6 janvier 1978)

**داده‌های غیرقابل جمع‌آوری یا حساس**، به آن دسته از اطلاعات گفته می‌شود که به طور مستقیم یا غیرمستقیم، ریشه‌های نژادی، عقاید سیاسی، فلسفی یا مذهبی یا تعلق آن‌ها به سندیکا یا کانون صنفی خاص و نیز گرایشات جنسی آنان را تعیین می‌کند( .(Directive n. 95/46/ce 2002, n. 559, p. 375.

**داده‌های قابل جمع‌آوری**، منظور اطلاعات راجع به کیفیت، کمیت و غیرشخصی نظیر داده‌های مرتبط با تولیدات، مدیریت انبارها و داده‌هایی که مستقیم یا غیرمستقیم حاوی اطلاعات با نام یا شخصی نیستند.

**فایل‌های دورنما**، منظور مجموعه اطلاعاتی است که شرکت‌های تجاری در خصوص دورنمای فعالیت‌های خود، مستقل یا همراه با اطلاعات مشتریان خود نگهداری می‌کنند. اگر این فایل‌ها حاوی مشخصات و نشانی اشخاص حقیقی یا اشخاصی باشد که در داخل یک شخص حقوقی(شرکت یا ادارات دولتی) قرار دارند، پردازش داده‌های مرتبط با آنان داده‌های شخصی تلقی خواهد شد.

**فایل‌های شخصی مرتبط با داده‌های آموزشی**، مجموعه داده‌هایی است که شرکت‌ها یا دفاتر مشاوره در زمینه دوره‌های آموزشی در اختیار دارند و متضمن پردازش اطلاعات با نام برای اقدام جهت آموزش کارکنان است. این پردازش‌ها حاوی اطلاعات در خصوص دوره آموزشی، تجربه حرفه‌ای و مشخصات شناسنامه‌ای، داوطلبان استخدام هستند. فایل‌های مرتبط با دوره‌های آموزشی ممکن است به علاوه متضمن اطلاعات حساس راجع به سلامتی، تعلق صنفی، موضع سیاسی، نتایج تست شخصیتی یا تحلیل مبتنی بر خط شناسی و نظایر آن باشد(Cf. Directive n. 95/46/ce).

**فایل‌های داده‌های شخصی**، مجموعه سازمان داده شده داده‌های شخصی است که مطابق معیارهای مشخص شده قابل دسترسی است. خواه این مجموعه متمرکز، غیرمتمرکز یا تقسیم شده به روش عملکردی یا جغرافیایی باشد(Cf. Directive – Art2 c. (n. 95/46/ce.

**مسئول پردازش**، عبارت از شخص حقیقی یا حقوقی، مقامات عمومی، بخش خدمات یا سایر سازمان‌هایی است که به تنهایی یا مشترکاً، اهداف و ابزارهای پردازش داده‌های شخصی را تعیین می‌کنند(Cf. Directive n. 95/46/ce – .Art 2 d).

**مسئول فرعی پردازش**، شخص حقیقی یا حقوقی، مقامات عمومی، بخش خدمات یا سایر سازمان‌هایی که به حساب مسئول پردازش، داده‌های شخصی را پردازش می‌کنند(Cf. Directive n. 95/46/ce – .Art2 e).

**دریافت‌کننده**، شخصی حقیقی یا حقوقی، مقامات عمومی، بخش خدمات یا سایر سازمان‌هایی که داده‌ها را دریافت می‌کنند، اعم از این که شخص ثالث باشد یا خیر. با این حال مقاماتی که ممکن است داده‌ها را در چارچوب مأموریت تحقیق خاص دریافت کنند، دریافت‌کننده محسوب نیستند(Cf. Directive n. 95/46/ce – .Art2 g).

**رضایت شخص ذیربط**، هرگونه اعلام اراده آزاد، مشخص و بیان شده که توسط آن شخص ذیربط، می‌پذیرد که داده‌های شخصی مرتبط با وی پردازش شود(Cf. –Art. d2 Directive n. 95/46/ce).

**کاربر**، هر شخص حقیقی که از خدمات ارتباطات الکترونیکی قابل دسترسی توسط عموم، با هدف استفاده شخصی و حرفه‌ای استفاده می‌کند بدون آن‌که ضرورتاً از مشترکان این خدمات باشد(Directive"europeénne"du 12 juillet 2002, Art. 2d).

**داده‌های عبوری**، کلیه داده‌های پردازش شده است که هدف از آن راهیابی به ارتباطات توسط یک شبکه ارتباطات الکترونیکی یا ارائه فهرست آن باشد (Cf. Directive europeénne du 12 juillet 2002,Art. 2b)

**داده‌های ثابت**، کلیه داده‌های پردازش شده در یک شبکه ارتباطات الکترونیکی است که شامل موقعیت جغرافیایی دستگاه پایانی یک کاربر خدمات ارتباطات الکترونیکی قابل دسترسی توسط عموم باشد( Cf. Directive europeénne du 12 juillet 2002,Art. 2b).

**محموله الکترونیکی**، هرگونه پیام به شکل نوشته، حالت، صدا یا تصویر فرستاده شده توسط یک شبکه عمومی اطلاع‌رسانی که ممکن است در شبکه یا دستگاه پایانی دریافت‌کننده انبار شود تا زمانی که شخص اخیر آن را وصول کند.( Cf. Directive europeénne du 12 juillet 2002,Art. 2h)

### ۱-۲. سیر تحول قانون‌گذاری در زمینه حمایت از داده‌های شخصی

از زمانی که کشورها برای اولین بار به قانون‌مند کردن تحصیل و پردازش داده‌های شخصی پرداختند تا به امروزکه تعداد کشورهای دارای مقررات قانونی در این زمینه به میزان قابل توجهی افزایش یافته، قانون‌گذاری در زمینه حریم خصوصی داده‌های شخصی سیری تکوینی طی کرده که ازهر دوره ای از آن به «نسل» یاد می‌شود. در این گفتار به طور خلاصه به بررسی نسل‌های مختلف قانون‌گذاری در این زمینه می‌پردازیم:

**قواعد نسل اول**: اولین قواعد در زمینه داده‌های شخصی در پاسخ به ضرورت‌های پردازش داده‌های شخصی در ارتباط با حکومت وموسسات بزرگ تدوین شد. هدف از تدوین چنین قوانینی این بود که داده‌های شخصی را در بانک‌های اطلاعاتی ملی متمرکز کنند. بسیاری از مقررات قانونی نسل اول بر حمایت مستقیم از حریم خصوصی توجه نداشتند. بالعکس، این قواعد به عملکرد داده‌های شخصی در جامعه معطوف بودند و اساساً نگاه کارکردی به امر پردازش داده‌ها داشتند، به گونه ای که قواعد متعلق به این نسل از به کارگیری کلماتی نظیر«محرمانگی»، «حمایت از حریم خصوصی» که امروزه کاربرد فراوان دارند اجتناب می‌کردند و به جای آن‌ها بیشتر از اصطلاحات فنی همانند «داده»، «بانک‌های داده»، «ثبت داده» و« فایل‌های داده» استفاده می‌کردند.

**قواعد نسل دوم**: حمایت از داده‌های شخصی در نسل دوم به حق محرمانگی زندگی خصوصی شهروندان معطوف شد و مبانی شناخته شده محرمانگی، نظیر «حق خلوت» و «حق حریم خصوصی شخصی» مورد توجه قرار گرفت. در نتیجه حمایت از داده‌های شخصی صراحتاً به حق محرمانگی پیوند خورد و به عنوان حق فرد در زمینه موضوعات شخصی در قبال جامعه شناخته شد. به علاوه، تمامی قواعد مرتبط با حمایت از داده‌های شخصی بر حق فرد به دسترسی و اصلاح داده‌های مربوط به خود تأکید کردند.

**قواعد نسل‌سوم**: در قواعد نسل سوم از پردازش داده‌های شخصی، آزای‌های فردی و حق افراد نسبت به اطلاعات شخصی و خصوصی خویش، با حق مداخله بیشتر در تعیین داده‌های قابل پردازش تکمیل شد. شخص نه تنها همانند قواعد نسل دوم می‌توانند در خصوص ارائه یا عدم ارائه داده‌های خصوصی خود تصمیم بگیرد بلکه می‌تواند به طور مستمر در امر پردازش داده‌ها مداخله کند. قواعد نسل سوم از داده‌های

شخصی بر حق شخص به تعیین اطلاعات قابل پردازش و اعتقاد به این‌که شهروندان می‌توانند این حق را اعمال کنند استوار است.

**قواعد نسل چهارم** : قانون‌گذاران دریافتند که به طور کلی اشخاص در اعمال حقوق خود در موضع ضعف قراردارند. از این روقواعد نسل چهارم داده‌های شخصی تلاش نمودند تا این ضعف را به دو طریق مختلف برطرف کنند.

از یک سو، قانون‌گذاران سعی کردند تا موضع افراد در مقابل نهادهای قدرتمند اطلاعاتی را با بهره‌گیری از سازو کارهای قانونی تقویت کنند. از سوی دیگر، قانون‌گذاران نسل چهارم، حمایت از طریق نمایندگی قانونی را جایگزین آزادی مشارکت افراد درارائه و تعیین داده‌های قابل پردازش کردند. چنین رویکردی از این ایده نشات می‌گیرد که برخی از زمینه‌های اطلاعاتی شخصی باید به طور مطلق مورد حمایت قرار گیرد به نحوی که سنگینی آن بر افراد تحمیل نشود( Rowland and Macdonald, 2005, pp. 316-318).

در چارچوب اتحادیه اروپا، تصویب دستورالعمل ۱۵ مارس ۲۰۰۶ راجع به«*نگهداری داده‌های شخصی تولید یا پردازش شده در چارچوب تأمین خدمات ارتباطی الکترونیکی قابل دسترسی برای عموم یا شبکه‌های عمومی ارتباطی و اصلاح دستورالعمل ۲۰۰۲ اتحادیه اروپا*»(Directive 2006/24/ce, 13/4/2006, L 105/54) خبر از نسل جدید از قواعد مرتبط با داده‌های شخصی می‌دهد. بر خلاف نسل‌های دوم تا چهارم قواعد مرتبط با داده‌های شخصی که بر حمایت از حقوق فردی معطوف هستند، هدف از تدوین این دستورالعمل تأمین امنیت ملی، آرامش و نظم عمومی کشورهای عضو و پیشگیری از اعمال مجرمانه و حمایت از حقوق وآزادی‌های دیگران است( Cf. Directive 2006/24/ce, Paragraph 9)

## ۲. چگونگی حمایت از حریم خصوصی داده‌های شخصی در حقوق ایران و اتحادیه اروپا

برای بررسی نحوه حمایت ازحریم خصوصی داده‌های شخصی، مطالعه در حقوق ایران و اتحادیه اروپا که مقررات واحدی را در این زمینه برای کشورهای عضو آن اتحادیه تدوین کرده مفید به نظر می‌رسد.

### ۲-۱. حقوق ایران

در محیط واقعی و غیر مجازی، مقررات منسجمی در خصوص حمایت از حریم خصوصی وجود ندارد ولایحه‌ای که در سال‌های اخیر در این خصوص تهیه شده، هنوز به تصویب نرسیده است. بنابراین، قواعد پراکنده ناظر بر حمایت از حریم خصوصی اشخاص را باید در قانون اساسی جمهوری اسلامی ایران و برخی مقررات کیفری و حقوقی از جمله، قانون مجازات اسلامی، قانون آیین دادرسی کیفری و قانون آیین دادرسی مدنی جستجو کرد.

با این همه، با تصویب قانون تجارت الکترونیکی در سال ۱۳۸۲، قواعدی در خصوص حمایت از حریم خصوصی اطلاعات شخصی در فضای مجازی و محیط اینترنتی پیش‌بینی شده است و قانون‌گذار فصل سوم از باب سوم این قانون(مواد ۵۸ تا ٦۱) را به «حمایت از داده پیام‌های شخصی» اختصاص داده است. به این ترتیب، در حالی که در محیط واقعی قواعد منسجمی برای حمایت از حریم زندگی خصوصی وجود ندارد، داده‌های شخصی مورد حمایت قانون‌گذار قرار گرفته است.

بر اساس ماده ۵۸ این قانون:

*«ذخیره، پردازش و یا توزیع داده پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیر قانونی است».*

ماده ۵۹ قانون مورد بحث ذخیره، پردازش و توزیع داده پیام‌های شخصی را در بستر مبادلات الکترونیکی تابع شرایط زیر قرارداده است:

«الف. اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند.

ب. داده پیام باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع آوری برای شخص موضوع داده پیام شرح داده شده جمع آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرارگیرد.

ج. داده پیام باید صحیح و روز آمد باشد.

د. شخص موضوع داده پیام باید به پرونده‌های رایانه ای حاوی داده پیام‌های شخصی مربوط به خود دسترسی داشته و بتواند داده پیام‌های ناقص و یا نادرست را محو یا اصلاح کند.

هـ شخص موضوع داده پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده‌های رایانه‌ای داده پیام‌های شخصی مربوط به خود را بنماید. »

مواد ٦٠ و ٦١ قانون تجارت الکترونیکی، ذخیره، پردازش و توزیع داده پیام‌های مربوط به سوابق پزشکی و بهداشتی و سایر موارد راجع به دسترسی موضوع داده پیام، از قبیل مستثنیات، افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسئول دیده بانی و کنترل جریان داده پیام‌های شخصی را موکول به تدوین آیین‌نامه کرده است.

مواد ۷۱ تا ۷۳ این قانون نیز برای اشخاصی که مواد ۵۸ و ۵۹ پیش گفته را نقض کنند مجازات تعیین کرده است. در صورتی که این جرم توسط دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسؤول ارتکاب یابد، مرتکب به حداکثر مجازات مقرر(سه سال حبس) محکوم خواهد شد. سرانجام، چنان‌چه جرم به دلیل بی مبالاتی و بی احتیاطی دفاتر خدمات صدور گواهی الکترونیکی رخ دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی محکوم خواهد شد.

### ۲-۲. حقوق اتحادیه اروپا

در محدوده اتحادیه اروپا سه دستورالعمل در سال‌های ۱۹۹۵ و ۲۰۰۲ و ۲۰۰٦در زمینه حمایت از حریم خصوصی داده‌های شخصی به تصویب شورا و پارلمان اتحادیه اروپا رسیده است. در این گفتار به طور خلاصه به بررسی محتوای این سه دستورالعمل- که در واقع مکمل هم هستند- می‌پردازیم.

#### ۲-۲-۱. دستورالعمل اروپایی مورخ ٢٤ اکتبر۱۹۹۵ (Cf. Directive n. 95/46/ce)

دستورالعمل اروپایی مورخ ۹۵/٤٦ اکتبر ۱۹۹۵ شورا و پارلمان اروپا تحت عنوان «*حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده‌ها*» دارای شش بخش است، که به ترتیب دارای عناوین زیر هستند:

مقررات کلی، شرایط کلی قانونی بودن پردازش داده‌های شخصی، اعتراضات قضایی و مسئولیت و ضمانت اجراها، انتقال داده‌های شخصی به کشورهای ثالث، کدهای رفتاری، مقامات کنترل کننده و گروه حمایت از اشخاص در مقابل پردازش

داده‌های شخصی. این مقررات را به طور خلاصه در سه قسمت قلمرو اعمال و اصول کلی و مستثنیات بررسی می‌کنیم.

**الف. اصول کلی حمایت از داده‌های شخصی**

- داده‌ها باید به صورت صحیح و قانونی پردازش شوند(بند الف ماده ۱-٦).
- داده‌ها با هدف مشخص، صریح و مشروع گردآوری شوند و پس از آن به صورت غیر مرتبط با هدف گردآوری مورد استفاده قرار نگیرد(بند ب ماده ۱-٦).
- پردازش باید متناسب و مرتبط با اهداف مورد نظر باشد و از افراط در استفاده از آن‌ها خودداری شود(بند پ ماده ۱-٦).
- داده باید به صورت صحیح و- اگر ضرورت داشته باشد - بروز گردآوری و پردازش شوند و ترتیبی اتخاذ شود که داده‌های نادرست و غیر مرتبط با اهداف تعیین شده، حذف یا اصلاح شوند(بند ت ماده ۱-٦).
- داده‌ها به شکلی نگهداری شوند که امکان شناسایی اشخاص ذینفع را - در مدتی که بیشتر از مدت زمان لازم برای اجرای هدف پردازش نباشد - فراهم سازد(بند ث ماده ۱-٦)
- پردازش داده‌هایی که متضمن ریشه‌های نژادی، قومی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی یا تعلقات صنفی باشد و نیز پردازش داده‌های مرتبط با سلامتی و زندگی جنسی ممنوع است(ماده ۱-۸) مگر با رضایت صریح ذینفع در این پردازش(بند الف ماده ۲-۸).
- اشخاصی که داده‌ها نزد آنان سپرده شده است مکلف به اطلاع رسانی به اشخاص ذینفع هستند(ماد ۱۰ و ۱۱).
- افراد ذینفع باید ازحق دسترسی به داده‌های پردازش شده برخوردار باشند (ماده ۱۲).
- اشخاص ذینفع حق دارند با با پردازش داده‌های مرتبط با آنان مخالفت کنند (ماده ١٤).
- اشخاص که به نام مؤسسه پردازش عمل می‌کنند مکلف به رازداری درباره داده‌های شخصی هستند(ماده ١٦).

– اشخاص پردازش کننده داده‌ها باید از داده‌های شخصی در مقابل تخریب تصادفی یا غیر قانونی آن‌ها مراقبت کنند(ماده ۱۷).

**ب. مستثنیات حمایت از داده‌های شخصی**

برابر بند ۱ماده ۱۳ دستورالعمل ٢٤ اکتبر ۱۹۹۵ کشورهای عضو می‌توانند مقرراتی مبنی بر محدود کردن تکالیف و حقوق پیش‌بینی شده درماده ۱-٦، ماده ۱۰ و ۱-۱۱ و مواد ۱۲ و ۲۱ وضع کنند به شرط این‌که این محدودیت‌ها برای ملاحظات زیر ضرورت داشته باشد:

– امنیت کشور؛

– دفاع ملی؛

– امنیت عمومی؛

– پیشگیری، جستجو، کشف و تعقیب اعمال مجرمانه یا تخلفات انتظامی درباره حرفه‌های تابع مقررات خاص؛

– منفعت اقتصادی یا مالی مهم یک کشور عضو یا اتحادیه اروپا از جمله در زمینه‌های پولی، بودجه‌ای و مالی؛

– مأموریت برای کنترل، انجام تحقیقات یا تدوین مقررات ناشی ازاعمال حاکمیت در موارد پیش‌بینی شده در بندهای پ، ت و ث، هر چند به صورت مقطعی.

– حمایت از شخص ذینفع یا حقوق و آزادی‌های دیگران.

به موجب بند ۲ ماده ۱۳ دستورالعمل، کشورهای عضو می‌توانند در مواردی که هیچ‌گونه خطرآشکاری به زندگی خصوصی اشخاص ذینفع وجود نداشته باشد، با وضع مقررات قانونی، حقوق مقرر در ماده ۱۲(حق دسترسی اشخاص ذینفع به داده‌ها) را محدود کنند به شرط این‌که داده‌ها صرفا با هدف پژوهش‌های علمی پردازش شوند یا به صورت داده‌های شخصی و برای مدتی که نباید از مدت زمان لازم برای هدف صرف مطالعات آماری بیشتر باشد ذخیره شوند.

### ۲-۲-۲. دستور العمل اروپایی مورخ ۱۲ ژوئیه ۲۰۰۲

(Cf. Directive europeénne du 12 juillet 2002).

دستورالعمل شماره CE /۲۰۰۲/۵۸ مورخ ۱۲ ژوئیه ۲۰۰۲ تحت عنوان «زندگی خصوصی و ارتباطات الکترونیکی» از یک سو جانشین دستورالعمل شماره ۹۷/٦٦/CE پارلمان و شورای اروپا در خصوص «پردازش داده‌های شخصی و حمایت از حریم خصوصی در بخش ارتباطات از راه دور» و از سوی دیگر مکمل دستورالعمل اروپایی مورخ ٢٤ اکتبر ۱۹۹۵ است.

ویژگی‌های این دستورالعمل در مقایسه با دستورالعمل مورخ ٢٤ اکتبر ۱۹۹۵ عبارتند از:

– تضمین امنیت خدمات ارتباطات الکترونیکی توسط ارائه دهندگان خدمات اینترنتی به لحاظ فنی(بند ۱ ماده ٤)؛

– تکلیف اطلاع‌رسانی ارائه‌دهندگان خدمات اینترنتی از خطرات مرتبط با نقض امنیت شبکه(بند ۲ ماده ٤)؛

– تضمین محرمانگی ارتباطات در خصوص داده‌های عبوری(ماده ۵)؛

– لزوم بی نام بودن داده‌های عبوری و مستثنیات آن(بندهای ۱و ۲ ماده ٦)؛

– تکلیف اطلاع رسانی ارائه دهندگان خدمات اینترنتی از اشکال داده‌های عبوری آنها(بند ٤ ماده ٦)؛

– لزوم ارائه صورت‌حساب کامل از سوی ارائه‌دهندگان خدمات اینترنتی و تکلیف دولت‌های عضو به آشتی میان صورت‌حساب کابل به مشترکان و اصل احترام به زندگی خصوصی آنان(ماده ۷)؛

– تکالیف ارائه دهندگان خدمات اینترنتی در خصوص معرفی مورد نظر و خطوط وصل‌شده و محدودیت‌های آن(ماده ۸ب)؛

– لزوم کسب رضایت برای پردازش داده‌های ثابت کاربران یا مشترکان(ماده ۹)؛

– لزوم رضایت کاربر یا مشترک در خصوص ارتباطات ناخواسته و یا رایگان (ماده ۱۳)؛

– شرایط و ضوابط تهیه سال‌نامهٔ الکترونیکی یا کاغذی مشترکان و حقوق مشترکان در خصوص اطلاعات مندرج در این سالنامه‌ها(ماده ۱۲).

### ۲-۲-۳. دستورالعمل اروپایی ۱۵ مارس ۲۰۰۶

این دستورالعمل که «نگهداری داده‌های شخصی تولید یا پردازش شده در چارچوب تأمین خدمات ارتباطی الکترونیکی قابل دسترسی برای عموم یا شبکه‌های عمومی ارتباطی و اصلاح دستورالعمل ۲۰۰۲ اتحادیه اروپا» نام دارد (Cf. Directive 2006/24/ce) همان‌طور که گفته شد با هدف کنترل و نگهداری داده‌هایی تدوین شده که می‌تواند برای تأمین امنیت ملی، آرامش و نظم عمومی و پیشگیری از اعمال مجرمانه ویا حمایت از حقوق و آزادی‌های دیگران اهمیت داشته باشد( Cf. Directive 2006/24/ce,Paragraph 9 de l'introduction).

مطابق ماده ۵ دستورالعمل، انواع داده‌هایی که کشورهای عضو مکلف به نگهداری آن‌ها هستند عبارتند از داده‌هایی که یافتن و شناسایی مبدا ارتباط(شماره تلفن تماس گیرنده و نام و آدرس مشترک یا کاربر) را ممکن سازد، داده‌هایی که برای شناسایی مقصد ارتباط(شماره تلفن طرف مکالمه) ضروری هستند، داده‌هایی که امکان تعیین تاریخ و ساعت و مدت ارتباط را فراهم سازد و بالاخره، داده‌هایی که برای شناسایی نوع ارتباط و هویت ملی طرفین ارتباط ضروری هستند. (Cf. Directive Art. 5 2006/24/ce,)

مدت نگهداری از داده‌ها با توجه به ماده ٦ دستورالعمل حداقل ٦ ماه و حداکثر ۲ سال است.

با دقت در سایر مواد دستورالعمل مشخص می‌شود که به طور مشخص هدف تدوین کنندگان این دستورالعمل، مبارزه با جرایم سازمان یافته و تروریسم است.

احتمالاً برای جلوگیری از سوء استفاده و نقض حریم خصوصی افراد در بند ۲ ماده ۱ دستورالعمل پیش‌بینی شده است که تکلیف دولت‌های عضو به نگهداری ازداده‌ها ناظر به محتوای ارتباطات الکترونیکی نیست.

با توجه به مجموعه مقررات اروپایی و بین‌المللی در زمینه حمایت از حریم خصوصی داده‌های شخصی، اصولی استخراج شده اند که «اصول حاکم بر داده‌های شخصی» نام گرفته اند.

منظور از این اصول «قواعد کلی حاکم بر موضوع حمایت از داده است که می‌توان با یاری از آن‌ها حتی در مواردی که قانون‌گذار حکم صریح و خاصی ندارد، در

تبیین و تعیین فروع بحث و یافتن راه حل مسایل و قضایای جزیی به راه حل قضیه دست یافت».(اصلانی، ۱۳۸٤، صفحه ۳۳۵).

این اصول را به‌طور عمده به چهار دسته تقسیم بندی کرده‌اند. **اصول مرتبط با تحصیل داده‌ها** که شامل اصل تحصیل قانونی و منصفانه، اصل تحصیل مضیق و مرتبط، اصل انتخاب و اصل اطلاع است. **اصول مرتبط با نگهداری داده‌ها** که اصل امنیت، اصل شفافیت، اصل دسترسی و اصل درستی را در بر می‌گیرد. **اصول مرتبط با به کارگیری داده‌ها** که در برگیرنده اصل پردازش مرتبط و اصل ممنوعیت افشا هستند و بالاخره **اصول مرتبط با امحا و انتقال داده‌ها** که شامل اصل امحا و اصل عدم انتقال است(اصلانی، ۱۳۸٤، صص ۱۳٤ تا۲٦۰).

### ۳. مسایل حقوقی مرتبط با حمایت از داده‌های شخصی

قواعد حقوقی مرتبط با حمایت از حریم خصوصی داده‌های شخصی چه در حقوق ایران و چه در حقوق اتحادیه اروپا، گاه ابعاد تازه‌ای به برخی قواعد حقوقی می‌دهد که نیاز به مطالعه دقیق‌تر را ایجاب می‌کند و گاه اعمال آن‌ها تعارض قوانین کشورهای مرتبط با موضوع را موجب می‌شود که بررسی نحوه حل این تعارضات راضروری می‌سازد.

#### ۳-۱. حمایت از داده‌های شخصی و جریان آزاد داده‌ها و اطلاعات

دستورالعمل‌های اتحادیه اروپا به شرحی که گذشت تلاش کرده‌اند بین منافع متعارض تعادل برقرار کنند. این دو منفعت که در تعارض با هم هستند همانند که در عنوان دستورالعمل مورخ ۲٤ اکتبر ۱۹۹۵ آمده است؛ حمایت از اشخاص حقیقی در مقابل پردازش داده‌های خصوصی از یک سو و جریان آزاد داده‌ها از سوی دیگر.

سیاست تقنینی ملی تلاش دارد تا از مردم در مقابل پردازش داده‌های شخصی حمایت کند. با این همه، ماهیت فرا ملی وغیر محلی داده‌های شخصی که محیط سایبر زمینه ساز آن است ضرورت وضع قواعد مشترک از سوی دولت‌ها را بیش از پیش آشکار می‌سازد. سازمان‌های بین‌المللی و منطقه‌ای و به ویژه اتحادیه اروپا تلاش می‌کنند بین ارزش‌های بنیادی و در عین حال متضاد یعنی احترام به زندگی خصوصی و جریان آزاد اطلاعات آشتی بر قرار کنند( Cf. Directive n. 95/46/ce. Considérations n. 2 et 3 à 11). در حقیقت، از یک سو باید حق احترام به حریم خصوصی اشخاص که در

زمره حقوق بشر به شمار می‌آید تأمین شود و از سوی دیگر، گردش آزاد داده‌ها و اطلاعات که لازمه توسعه اقتصادی و اجتماعی است تضمین گردد.

از این رو، ابزارهای قانونی اعم از ملی، اروپایی و بین‌المللی باید تعارض بین آزادی‌های مختلف نظیر آزادی جریان اطلاعات، آزادی تجارت و معاملات و آزادی زندگی خصوصی در ابعاد مختلف آن نظیر داده‌های مرتبط با شخص ذینفع، تاریخ زندگی، فعالیت‌ها، دیدگاه‌ها، مذهب، زندگی خانوادگی وبیماری‌های وی را حل و فصل کنند( Rigaux, 2000, pp. 27-40. ).

### ۳-۲. حمایت از داده‌های شخصی و مفهوم رضایت

همان‌طور که گفته شد بر اساس ماده ۵۸ قانون تجارت الکترونیکی سال ۱۳۸۲ « ذخیره، پردازش و یا توزیع داده پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دید گاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیر قانونی است.» ضرورت رضایت صریح شخص ذینفع برای گردآوری و پردازش داده‌های مذکور در ماده ۵۸ فوق –که به داده‌های حساس معروفند**(رک. گفتار اول از مبحث اول)** در ماده ۸ دستورالعمل اروپایی ٢٤ اکتبر سال ۱۹۹۵(همان‌طور که دیدیم) تکرار شده است. با این حال بند(الف) ماده ۷ دستورالعمل سال ۱۹۹۵ غیر قابل تردید بودن رضایت را هم ضروری دانسته است. افزودن چنین وصفی به مفهوم رضایت در حقوق اروپایی این سوال را مطرح کرده است که آیا رضایت ضمنی هم می‌تواند غیرقابل تردید باشد یا خیر؟ برخی از حقوقدانان فرانسوی به این پرسش پاسخ مثبت داده اند و به این منظورمواد ۷ و ۸ دستورالعمل سال ۱۹۹۵ را با بند ۱ ماده ۳ کنوانسیون رم مورخ ۱۹ ژوئن سال ۱۹۸۰ در باره «قانون حاکم بر تعهدات قراردادی» مقایسه کرده‌اند. بر اساس جمله دوم از این بند از ماده ۳، انتخاب قانون حاکم توسط طرفین «باید صریح باشد یا به صورت قابل اطمینان از مقررات قراردادی یا از اوضاع و احوال حاکم استنباط شود. » به علاوه مقررات دیگری وجود دارند که امکان رضایت ضمنی را تقویت می‌کنند. از آن جمله می‌توان به بند(ب) ماده ۷ دستورالعمل سال ۱۹۹۵ اشاره کرد که شرط رضایت را – چنان‌چه پردازش داده‌ها *برای اجرای قراردادی که شخص ذینفع طرف آن است یا برای اجرای تدابیر* پیش قراردادی که به تقاضای وی انجام شده ضروری باشد–

منتفی می‌داند. حکم این ماده علاوه بر قرارداد کار قراردادهای متعدد دیگری را که از جمله در زمینه بانک، بیمه، حمل و نقل، خرید اعتباری و قرض انعقاد می‌یابد شامل می‌شود.

در حقوق ا یران، با توجه به عبارت«رضایت صریح» که در ماده ۵۸ قانون تجارت الکترونیکی به کار رفته تردیدی وجود ندارد که در زمینه داده‌های حساس که ماده ۵۸ ناظر به آن است رضایت باید صریح باشد و نمی‌توان آن را از رفتارو کردار یا سکوت شخص ذینفع استنباط کرد. با این همه، این تحلیل باید به داده‌های حساس محدود شود. در خصوص سایر داده‌ها از جمله داده‌های شخصی مرتبط با قراردادها و تعهدات هر چند این قبیل داده‌ها نیز مطابق ساز و کاری مبادله می‌شوند که در مواد ۱۷ تا ۲۵ قانون تجارت الکترونیکی پیش‌بینی شده است ولی در آن‌چه به محتوای داده پیام مربوط می‌شود فضای سایبریا محیط الکترونیکی تغییری درماهیت قواعد حقوقی موجود در این زمینه نمی‌دهد. با توجه به مواد ۱۹۱ تا ۱۹۳ قانون مدنی رضایت اعم است از صریح یا ضمنی و ایجاب و قبول می‌تواند به هر دو شکل تحقق پذیرد(کاتوزیان، ۱۳۷٦، صص ۲۵۹ تا۲٦۱، شماره ۱۳۸). و اگر این موضوع در قانون تجارت الکترونیکی سال ۱۳۸۲مغفول مانده به این دلیل است که ازیک سو ماده ٦۱ این قانون متأسفانه بسیاری از جنبه‌های حمایت از داده‌های شخصی را به آیین‌نامه موکول کرده و از سوی دیگر همان‌طور که خواهیم دید مقررات حقوق ایران در این زمینه دارای نقایص و ایرادات جدی هستند. به آن‌چه گفته شد باید اضافه شود چنان‌چه گردآوری و پردازش داده‌ها از جمله برای منافع عمومی، امنیت ملی، دفاع ملی، مبارزه با جرایم سازمان یافته یا تروریسم اجتناب ناپذیر باشد، اساساً رضایت شخص ذینفع ضرورت نخواهد داشت.

### ۳-۳. حمایت از داده‌های شخصی و تعارض قوانین

از آن‌جا که اینترنت امکان دسترسی عموم را به داده‌ها و اطلاعات در سراسر جهان فراهم می‌آورد چه به لحاظ مدنی و چه به لحاظ کیفری قوانین کشورهای مختلف را رو در روی هم قرار می‌دهد به گونه‌ای که گاه رفع و حل تعارض بین قوانین کشورهای مرتبط با موضوع را ایجاب می‌کند.

### ۳-۳-۱. تعارض قوانین در زمینه مسئولیت مدنی

همان‌طور که در چکیده مقاله گفته شد، اینترنت امکان نقض حریم خصوصی داده‌های شخصی را نه فقط در محدوده یک کشور خاص بلکه در سطح بین‌المللی فراهم می‌سازد. در محیط اینترنتی حریم خصوصی ممکن است توسط اشخاص حقیقی و حقوقی که در کشورهای مختلف مستقر هستند و به گردآوری و پردازش داده‌های شخصی می‌پردازند مورد تعرض قرار گیرد. در نتیجه، با توجه به دخالت عناصر خارجی(از قبیل محل ورود ضرر، محل اقامت زیاندیده) در شکل گیری این تجاوز، این سوال مطرح می‌شود که مسئولیت‌های مدنی ناشی از آن با اعمال کدام‌یک از قوانین مرتبط باید حل و فصل شود؟

ماده ۲۳ دستورالعمل سال ۱۹۹۵ اتحادیه اروپا کشورهای عضو را مکلف می‌کند خسارات ناشی از پردازش غیر قانونی داده‌های شخصی را جبران کنند. ولی این ماده قانونی را که باید چنین مسئولیتی را تشخیص دهد معین نمی‌کند. در واقع معلوم نیست رابطه علیت، محدوده جبران خسارت، ماهیت ضرر، پذیرش یا عدم پذیرش خسارات معنوی، خسارات غیر مستقیم وعدم النفع براساس قانون چه کشوری به عمل می‌آید. در این‌باره، بسیاری قانون محل ورود **خسارات**[۳] را پیشنهاد کرده‌اند، هر چند که علاوه بر مشکلات ناشی از تشخیص محل ورود ضرر، قاعده داری مستثنیاتی است وبه علاوه می‌تواند به بهانه مغایرت به نظم عمومی کنار گذاشته شود. برای تعیین قانون حاکم، برخی عنصر ارتباط«محلی را که حقوق مورد ادعا نقض شده اند» به اقامت‌گاه(یا محل سکونت دایمی) ترجیح داده اند(Cf. Rigaux; p. 39.)

در حقوق ایران به طور کلی در زمینه مسئولیت مدنی و به‌طور خاص درباره مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌های شخصی هیچ‌گونه قاعده‌ای برای حل تعارض قوانین وجود ندارد. به علاوه ادبیات حقوقی در این زمینه بسیار اندک هستند. قوانینی که با توجه به عناصر ارتباط موجود در این زمینه، قابل اعمال هستند عبارتند از: قانون متبوع دادگاه، قانون محل ورود ضرر، قانون محل اقامت زیاندیده، قانون محل حمایت و قانون مرتبط با احوال شخصیه چنان‌چه نقض حریم خصوصی را از موضوعات مربوط به احوال شخصیه بدانیم. هر یک از این راه حل‌ها مزایا و معایبی دارد که در این مقاله مجال پرداختن به آن‌ها وجود ندارد و اهمیت موضوع، مطالعه دقیق‌تر در این زمینه را طلب می‌کند.

### ۳-۳-۲. تعارض مکانی قوانین کیفری

برابر ماده ۷۱ قانون تجارت الکترونیکی سال ۱۳۸۲:

«هرکس در بستر مبادلات الکترونیکی شرایط مقرر در مواد ۵۸ و ۵۹ این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود. »

هم‌چنین مطابق ماده ۷۲ همان قانون اگر مرتکب دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسئول باشند به حدأکثر مجازات مقرردر ماده ۷۱ محکوم خواهند شد. بالاخره، بر اساس ماده ۷۳ قانون پیش گفته اگر جرایم مذکور در ماده ۷۱ درنتیجه بی مبالاتی و بی احتیاطی دفاتر خدمات صدور گواهی الکترونیکی رخ دهد مرتکب به سه ماه تا یک سال حبس محکوم خواهد شد.

ویژگی فراملی و بین‌المللی ارتباطات اینترنتی، این امکان را فراهم می‌سازد که جرایم موضوع مواد فوق بیش از جرایمی که در محیط مادی اتفاق می‌افتند به دلیل وجود یک عنصر خارجی نظیر تابعیت مجرم، محل وقوع جرم، محل کشف جرم و محل دستگیری مجرم صلاحیت جزایی کشورهای مختلف را برای رسیدگی به موضوع و مجازات مجرم موجب شود. باید دید تعارض بین قوانین کشورهای مختلف در این زمینه چگونه باید حل و فصل شود.

در چار چوب اتحادیه اروپا، ماده ٢٤ دستورالعمل سال ۱۹۹۵ به صورت کلی کشورهای عضو را مکلف کرده است ضمانت اجراهای کیفری مناسب در قبال نقض مقررات آن کنوانسیون اتخاذ کنند. با توجه به ماده ٤ این دستورالعمل که «قانون ملی حاکم» نام دارد، مشخص می‌شود که اصل صلاحیت سرزمینی در چارچوب اتحادیه برسمیت شناخته شده است. بر اساس این ماده:

«هریک از کشورهای عضو مقررات ملی خود را در باره داده‌های شخصی موضوع این کنوانسیون در موارد زیر اعمال می‌کند :

– هرگونه پردازش اتوماتیک که در چارچوب فعالیت مسئول پردازش(رک. گفتار اول از مبحث اول) مستقر در سرزمین یکی از کشورهای عضو صورت گیرد. . .(بند الف ماده ۱– ٤).

– در صورتی که مسئول پردازش در خارج از سرزمین یک کشور عضو ولی در محلی که قانون ملی او به موجب حقوق بین الملل عمومی حاکم است تشکیل شود(بند ب ماده ۱–٤).

– چنان‌چه مسئول پردازش در سرزمین اتحادیه اروپا تشکیل نشده ولی با وسایلی اعم از خودکار یا غیر خود کار در سرزمین یکی از کشورهای عضو مستقر است. . . »(بند پ ماده ۱–٤).

در آن‌چه به مسایل کیفری مربوط است، اصل صلاحیت سرزمینی به این معنا است که از یک سو، مراجع کیفری صلاحیت خود را بر اساس معیارهای مرتبط با قانون محل وقوع دادگاه[٤] تعیین می‌نمایند و از سوی دیگر، جرایم و مجازات‌ها را نیز بر اساس همین قانون اعمال می‌کنند.

در حقیقت، صلاحیت کیفری از آن کشوری است که محل پردازش داده‌ها در آن قرار دارد. این اصل دارای یک عنصر ارتباط جایگزین است: در صورتی که مسئول پردازش در سرزمین اتحادیه اروپا تشکیل نشده باشد، کشور عضوی که «ابزارهای خودکار یا غیرخودکار» برای پردازش داده‌ها درآن مستقر است صلاحیت خواهد داشت. اتحادیه اروپا از این طریق در صدد است تا مانع از آن شود که داده‌های گردآوری شده در یکی از کشورهای عضو در خارج از چارچوب اتحادیه پردازش شوند. به همین دلیل، معیار اعمال قوانین کیفری یکی از کشورهای عضو، گاه محل تشکیل مسئول پردازش و گاه محل وقوع ابزارهای گردآوری و پردازش داده‌ها است( Cf. Rigaux. p. 38).

با این همه، سرزمینی بودن تنها معیار تعیین صلاحیت کیفری نیست و یک مرجع کیفری ممکن است بر اساس تابعیت مرتکب یا مجنی علیه نیز صلاحیت پیدا کند. در نتیجه حتی اگر جرم در خارج روی داده باشد، جرایم و مجازات‌ها بر اساس قانون محل وقوع دادگاه تعیین خواهد شد به شرط این‌که عمل در کشور محل ارتکاب جرم تلقی شود.

قانون تجارت الکترونیکی ایران حکمی در زمینه نحوه حل تعارض مکانی قوانین جزایی قابل اعمال نسبت به حریم داده‌های شخصی– که از موضوعات حقوق کیفری بین‌المللی است– ندارد و در این خصوص باید به مقررات کیفری از جمله مواد ۳ تا ۸ قانون مجازات اسلامی مراجعه شود. ماده ۳ این قانون اصل صلاحیت سرزمینی را مورد

پذیرش قرار داده است. بنابراین اگر پردازش داده غیر قانونی داده‌ها در سرزمین ایران رخ داده باشد قوانین جزایی ایران(یعنی مواد ۷۱ تا ۷۳ قانون تجارت الکترونیک) بدون تردید اعمال خواهند شد. چنان‌چه گردآوری و پردازش غیر قانونی داده‌های شخصی قسمتی در ایران و نتیجه آن در خارج یا قسمتی در خارج از ایران و نتیجه آن در ایران حاصل شده باشد و یا به طور کلی گرد آوری و پردازش در خارج ولی نتیجه آن در ایران حاصل شود با توجه به ماده ٤ قانون مجازات اسلامی در حکم جرم واقع شده در ایران محسوب و برابر مقررات کیفری ایران قابل مجازات خواهد بود. در این صورت حتی اگر عمل گرد آوری و پردازش داده‌های در کشور محل وقوع، جرم تلقی نشود، صرف حصول نتیجه در ایران، عمل مطابق قوانین ایران قابل مجازات خواهد بود هر چند که این امر برخلاف اصول شناخته شده حقوق کیفری بین‌المللی است.

هم‌چنین، براساس ماده ٦ قانون مجازات مجازات اسلامی چنان‌چه جرایم موضوع مواد ۷۱ تا ۷۳ قانون تجارت الکترونیک توسط بیگانگان در خدمت جمهوری اسلامی ایران، مستخدمان دولت به مناسبت شغل و وظیفه خود در خارج از ایران ویا توسط مأموران سیاسی و کنسولی و فرهنگی دولت ایران که از مصونیت استفاده می‌کنند ارتکاب یابد برابر مقررات مواد فوق قابل مجازات خواهند بود.

سرانجام، چنان‌چه در آینده ایران عضو کنوانسیون‌های بین‌المللی مرتبط با جرایم سایبری شود با عنایت به ماده ۸ قانون مجازات اسلامی می‌تواند صلاحیت کیفری خود را در صورت دستگیری مجرم در ایران اعمال کند.

### ٤. نقد حقوق ایران در زمینه حمایت از حریم خصوصی داده‌های‌شخصی

مقایسه بین مقررات اتحادیه اروپا با مقررات قانون تجارت الکترونیکی ایران مصوب سال ۱۳۸۲ در زمینه داده‌های شخصی نشان می‌دهد که حقوق ایران از این حیث دارای نقایص جدی است که باید از سوی مقنن مورد بازنگری قرار گیرد. این نقایص را به دو دسته عمده می‌توان تقسیم بندی کرد: نقایص مرتبط با داده‌های شخصی از یک‌سو(گفتار اول)، وفقدان مقررات در خصوص اشخاص و مؤسسه‌های گردآوری و پردازش کننده داده‌های شخصی از سوی دیگر(گفتار دوم)

### ٤-١. نقایص مرتبط با اصول حاکم بر داده‌های شخصی

این نقایص به نوبه خود در دو گروه قابل مطالعه هستند: فقدان برخی از اصول حاکم بر داده‌های شخصی، کامل نبودن اصول پیش‌بینی شده و ارجاع برخی دیگر به آیین‌نامه.

#### ٤-١-١. فقدان برخی مقررات حاکم بر داده‌های شخصی

مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی در زمینه داده‌های شخصی، برخی از اصول ناظر بر حمایت از حریم خصوصی داده‌ها و اطلاعات شخصی در محیط الکترونیکی را مورد توجه قرارد اده است. از آن جمله می‌توان به اصل تحصیل قانونی و مبتنی بر رضایت سوژه یا شخص موضوع گردآوری و پردازش(ماده ۵۸)، اصل تحصیل مضیق و مرتبط(بندهای الف و ب ماده ۵۹)، اصل درستی یا صحت داده‌های گردآوری شده(بند ج ماده ۵۹)، اصل دسترسی(بند د ماده ۵۹) و اصل امحا(بند ه ماده ۵۹) اشاره کرد.

با این حال، برخی از اصول دیگر که از جمله در حقوق اروپایی و مقررات برخی کشورها به آن‌ها تصریح شده، در حقوق ایران مورد توجه قانون‌گذار قرارنگرفته است. از آن جمله می‌توان به اصل انتخاب، اصل امنیت، اصل شفاف سازی، اصل ممنوعیت افشا، اصل پردازش مرتبط و اصل عدم انتقال را نام برد. به علاوه همان‌طور که گفته شد قانون تجارت الکترونیکی در زمینه مفهوم رضایت، قواعد حل تعارض مرتبط با مسئولیت مدنی اشخاصی که به گرد آوری و پردازش داده‌های شخصی می‌پردازند و نیز رابطه حریم داده‌های شخصی و جریان آزاد اطلاعات سکوت اختیار کرده است.

#### ٤-١-٢. کامل نبودن اصول پیش‌بینی شده

هر چند همان‌طور که گفته شد، قانون‌گذار ایرانی برخی از اصول حاکم بر داده‌های شخصی را مورد تصریح قرارداده است، با این حال گاه همه مقتضیات آن اصل در مقررات موضوع مواد ۵۸ تا ٦١ قانون تجارت الکترونیکی پیش‌بینی‌نشده هست.

به عنوان مثال، در خصوص اصل قانونی بودن و لزوم تحصیل رضایت سوژه، هر چند ضرورت آن در ماده ۵۸ به صراحت ذکر شده است ولی مستثنیات آن پیش‌بینی نشده و با توجه به ماده ٦١ آن قانون به آیین‌نامه واگذار شده است. ارجاع مستثنیات حمایت از داده‌های شخصی به آیین‌نامه جای تأسف دارد، زیرا این مستثنیات هم به

اندازه خود اصل از اهمیت برخوردار هستند و باید در قالب قانون پیش‌بینی شود تا از هرگونه سوءاستفاده احتمالی جلوگیری شود. دراین خصوص همان‌طور که دیدیم، حقوق فرانسه و اتحادیه اروپا این مستثنیات را در چارچوب قوانین آورده‌اند.

به علاوه، اصل دسترسی به داده‌های گردآوری و پردازش شده نیز همانند اصل رضایت دارای مستثنیاتی است که قانون‌گذار ایرانی در مورد آن‌ها سکوت اختیار کرده است(اصلانی، ۱۳۸٤. صفحه ۳٤۳).

### ٤-۲. نقایص مرتبط با اشخاص و مؤسسه‌های گردآوری و پردازش کننده داده‌ها و ارائه دهندگان خدمات اینترنتی

حقوق کشورهای مورد مطالعه، هم‌چنین دستورالعمل‌های اتحادیه اروپا مقررات صریح و روشنی را درقالب قانون در خصوص نحوهٔ تشکیل، فعالیت، وظایف و اختیارات و نیز مسئولیت‌های اشخاصی که به گردآوری و پردازش داده‌های شخصی می‌پردازند و نیز تکالیف و مسئولیت‌های ارائه دهندگان خدمات اینترنتی وضع کرده‌اند و به این ترتیب روابط حقوقی تمامی اشخاص دست‌اندرکار و ذینفع را مشخص کرده‌اند. حقوق ایران متأسفانه از این حیث نیز دارای ایراد است، زیرا بر اساس مادهٔ ٦۱ قانون تجارت الکترونیک در این زمینه هم به آیین‌نامه ارجاع شده است. بدیهی است امکان پیش‌بینی مقررات آمره و ضمانت اجراها اعم از حقوقی و کیفری در چارچوب آیین‌نامه وجود ندارد.

لایحهٔ «حریم خصوصی» که برای ارائه به مجلس شورای اسلامی تدوین شده، این ایراد را از حیث تکالیف و مسئولیت‌های کیفری ارائه دهندگان خدمات اینترنتی تاحدودی حل کرده است. ولی این لایحه نیز در خصوص نحوهٔ تشکیل، فعالیت، وظایف و اختیارات و نیز مسئولیت‌های اشخاصی که به گردآوری و پردازش داده‌های شخصی می‌پردازند سکوت اختیار کرده است.

علاوه بر آن‌چه گفته شد، مقررات حقوق ایران ناظر بر حمایت از داده‌های شخصی از حیث مصادیق داده‌های مورد حمایت و ضمانت اجراهای کیفری نیز دارای ایراداتی است که نیاز به بررسی جداگانه دارد.

## جمع‌بندی

پیش‌بینی مقررات راجع به حمایت از داده‌ها و اطلاعات شخصی در بستر مبادلات الکترونیکی در حقوق ایران و در قالب تجارت الکترونیکی را باید به فال نیک گرفت. با این حال، در مقایسه با اتحادیه اروپا این مقررات دارای ایرات جدی است که باید مرتفع شوند. از سوی دیگر، فقدان مقررات جامع در زمینه حمایت از حریم خصوصی به‌طور کلی و در محیط واقعی مانع از آن خواهد بود که حمایت از داده‌های شخصی در دادگاه‌ها و مراجع اداری به درستی فهمیده و اجرا شود. زیرا در اکثر کشورهایی که مقررات حمایت از داده‌های شخصی وضع شده است، مقررات ناظر به حمایت از حریم خصوصی سال‌ها است که وجود دارند و دادگاه‌ها و سایر مراجع رسیدگی با مفاهیم مرتبط با آن و نیز ماهیت قواعد ناظر بر آن آشنایی کامل دارند. امیدواریم لایحهٔ حریم خصوصی که در بردارنده مقررات جامع در زمینه حمایت از حریم خصوصی، چه در محیط واقعی و چه در فضای مجازی است با رفع ایرادات آن هر چه زودتر به تصویب برسد تا کم‌بود حقوقی موجود در این زمینه برطرف شود.

## یادداشت‌ها

۱.(برای ملاحظه تفصیل عملکرد این ابزارها و سایر ابزارهای فنی رک. Cadoux, pp.41-50)

2. Data protection
3. Lex loci delicti
4. Lex fori



## کتاب‌نامه

### فارسی

۱. اصلانی، حمید(۱۳۸٤). *اصول حاکم بر حمایت از داد*، مندرج در مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات. تهران: معاونت حقوقی و توسعه قضایی قوه قضاییه. مرکز مطالعات توسعه قضایی. چاپ اول.
۲. اصلانی، حمید(۱۳۸٤) *حقوق فناوری اطلاعات*، تهران: نشر میزان. چاپ اول.
۳. قاجار، سیامک(اردیبهشت ۱۳۷۹). *ابعاد حقوقی کاربرد کامپیوتر، حریم خصوصی، حمایت از داده*، خبرنامه انفورماتیک. سال پانزدهم.

٤. کاتوزیان، ناصر(۱۳۷٦). *حقوق مدنی، قواعد عمومی قراردادها*، جلد اول(مفهوم عقد- انعقاد و اعتبار قرارداد. تراضی). تهران: شرکت سهامی انتشار. چاپ چهارم.

**لاتین**

1. Bainbridge David(2000). *Introduction to computer law*. Longman. Fourth Edition.
2. Cadoux, Louise(2000). "*Les solutions techniques de protection de la vie privée*". in La protection de la vie privée dans la société d'information.(sous la direction de Pierre Tabatoni. Tome 2. Presse universitaire de france(Puf). première édition. pp. 41- 50.
3. Debbasch Charles, Isar Hervé, Agostinelli Xavier(2002) *Droit de la communication*(Audiovisuel- Presse- Internet). Dalloz 1er éd.
4. *Directive n. 95/46/ce du Parlement européenne* et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces donneés(2002). *in Lamy droit de l'informatique et des réseaux*,(sous la directionde Michel Vivant et autres). éd. Lamy. n. 559, p. 375.
4. *Directive vie privée et communications éléctroniques du 12 juillet 2002*, in File://A\:DIRECTIVE%20VIE%20PRIVEE%20ET%20COMMUNICATION%20E. . .
5. *Directive 2006/24/ce du parlement européenne et du conseil*, in Journal officiel de l'union européenne,13/4/2006, L 105/54
6. Guinchard, Serge, Harichaux, Michèle et Tourdonnet Renaud(1999). *"Internet pour le droit*. Paris. Monchrestien. pp. 228-232.
7. *Loi n. 78-17 du 6 janvier 1978 relative à l'informatiques, aux fichiers* et aux libertés, Journal officiel du 7 janvier 1978 in Lamy droit de l'informatique et des réseaux(sous la direction de Michel Vivant et autres), n. 555, p. 354.
8. Rigaux, François(2000). *"Libre circulation des données et protection de la vie privée*". in La protection de la vie privée dans la société d'information(sous la direction de Pierre Tabatoni). Tome 2. Presse universitaire de france(Puf). première édition, pp. 25- 40.
9. Rowland, Diane and Macdonald, Elizabeth(2005). *Information technology law*. Cavendish publishing. third edition.
10. Vivant, Michel et autres,(2002*). Lamy droit de l'informatique et des réseaux. guide, solutions et application pratique contractuelle*. Lamy.