فصلنامهٔ علمی پژوهشی رفاه اجتماعی، سال ششم، شماره ۲۵

درآمدی بر حقوق حاکم بر حمایت از داده‌های شخصی در حوزه بهداشت و سلامت

حمیدرضا اصلانی*

طرح مسأله: *فناوری اطلاعات و ارتباطات همهٔ حوزه‌های زندگی بشر، از جمله حوزهٔ بهداشت و سلامت را تحت تاثیر قرار داده است. پزشکی از راه دور و همچنین فراگیر شدن نظام‌های تامین اجتماعی، مستلزم برخورداری از پایگاه‌های دادهٔ پیشرفته و روزآمد از شهروندان می‌باشد. میزان اهمیت داده‌های شخصی با توجه به نوع و ماهیت آن‌ها متفاوت است. داده‌های شخصی مربوط به سلامتی و خصوصیات وراثتی در زمرهٔ داده‌های شخصی حساس می‌باشند که باید با بالاترین استانداردهای امنیت اطلاعات نگهداری شوند و هرگونه تعدی به آن‌ها در اغلب نظام‌های حقوقی ممنوع و قابل عقاب است. بررسی و تحلیل نظام حقوقی متناسب با این قسم داده‌ها امروزه در عصر فناوری اطلاعات، ضرورت ویژه دارد و در تشکیل پروندهٔ الکترونیکی سلامت نقش تعیین‌کننده ایفا می‌کند.*

روش: *این تحقیق از نوع توصیفی ـ تحلیلی است که در آن سعی می‌شود با مراجعه به منابع حقوقی و قوانین نظام‌های مختلف حقوقی و مقایسهٔ آن با قوانین و مقررات ایران کاستی‌های حقوق ایران نمایش داده شود.*

یافته‌ها و نتایج: *در کشورهای مختلف دنیا سعی شده تا با وضع مقررات حمایتی ویژه، امنیت داده‌های مربوط به سلامتی و خصوصیات وراثتی را تامین کنند. برخلاف نظام‌های حقوقی پیشرو در زمینهٔ حقوق فناوری اطلاعات، نظام حقوقی ایران حمایت مطلوبی از این قسم داده‌ها به‌عمل نیاورده است و برای روزآمد شدن و انطباق با استانداردهای جهانی نیازمند اصلاح است.*

کلید واژه‌ها: اصول حمایت از داده، داده‌های شخصی، داده‌های وراثتی، پروندهٔ الکترونیک سلامت، حریم خصوصی

تاریخ دریافت: ۸۴/۴/۲۸ تاریخ پذیرش: ۸۶/۵/۱۸

* دانشجوی دورهٔ دکترای حقوق خصوصی دانشگاه شهیدبهشتی <hamidreza.aslani@gmail.com>

مقدمه

فناوری اطلاعات و ارتباطات، بسیاری از عرصه‌های حیات بشری را تحت تاثیر قرار داده است. آموزش، تفریح، تجارت و اقتصاد، امنیت، اداره و سلامت جامعه جملگی در پرتو به‌کارگیری این فناوری‌ها دستخوش تغییر شده‌اند. امروزه به‌کارگیری این فناوری‌ها امکان گردآوری پایگاه‌های عظیم داده که متضمن اطلاعات مربوط به سوابق و وضعیت سلامت جسمی و روحی میلیون‌ها شهروند می‌باشد و از همه مهمتر، دسترسی به محتوای این پایگاه‌ها بدون حضور فیزیکی را فراهم آورده است. همچنین گردآوری اطلاعات مربوط به بیماری‌ها و تعداد و اقشار بیماران، امکان پردازش داده‌ها در سطح وسیع و مقابله با اپیدمی‌ها و انتقال تجارب درمانی را فراهم آورده است. در چنین فضایی مشکل زمان و مکان که به‌عنوان دو مانع پیش روی توسعه و گسترش دانش پزشکی و عرضهٔ خدمات درمانی وجود داشت روزبه‌روز کم‌رنگ‌تر می‌گردد (National Research Council,1997). از سوی دیگر، به‌کارگیری این فناوری‌ها امکان انجام برخی فعالیت‌های *پزشکی از راه دور*[1] را فراهم نموده است. به‌عنوان مثال پزشک معالج می تواند در مواردی، بدون حضور فیزیکی در بیمارستان شرح حال بیمار را از طریق دستیاران خود به‌صورت *برخط*[2] دریافت نموده و داروهای مورد نیاز وی را تجویز نماید.

به‌کارگیری فناوری اطلاعات در عرصهٔ تامین بهداشت و سلامت شهروندان، همچون سایر مواردی که این قبیل فناوری‌ها در زندگی بشر به‌کار گرفته شده‌اند طیف وسیعی از مباحث و مسائل حقوقی را به میان آورده است که تبیین آن‌ها می‌تواند به قاعده‌مند نمودن این قبیل فعالیت‌ها کمک شایانی کند. به‌عنوان مثال، امکان استناد به نسخه و تجویز دارو به‌صورت غیرحضوری و از راه دور، مسوولیت پزشک و کلینیک در خصوص امکان

1. Telemedicine

برای دیدن مفهوم و دامنه شمول این اصطلاح ر.ک به:

Dept. of Research & Development,1997؛ Nancy Brown,1996

2. Online

دستیابی کاربران غیرمجاز به داده‌ها، خرابکاری و هک شدن داده‌ها و آثار آن بر سلامت بیماران، تغییر شکل یافتن داده‌ها و تجویزهای الکترونیکی در زمان انتقال داده‌ها، مسالهٔ تائید هویت بیمار و پزشک و.... تنها نمونه‌ای از صدها مسالهٔ حقوقی قابل طرح در حوزهٔ بهداشت و سلامت الکترونیکی است. آن‌چه در این مقاله مورد بررسی قرار خواهد گرفت مسألهٔ حمایت از داده‌های شخصی در عرصهٔ بهداشت و سلامت خواهد بود که در پرتو به‌کارگیری فناوری اطلاعات و ارتباطات گردآوری، پردازش و دسترسی بدان به‌نحو قابل ملاحظه‌ای تسهیل شده است. سعی خواهد شد که مبانی حقوقی حمایت از این داده‌ها و مسوولیت‌های متصدیان این حوزه و جایگاه این داده‌ها از حیث سطح حمایت در نظام‌های مختلف حقوقی بررسی و با نظام حقوقی ایران مقایسه شود.

۱) جایگاه بحث

حقوق فناوری اطلاعات، شاخه‌ای جدید از دانش حقوق است که به تبیین مسائل حقوقی ناشی از به‌کارگیری و گسترش فناوری اطلاعات و ارتباطات می‌پردازد. این شاخه از دانش در یکی از مهمترین زیرشاخه‌های خود به مسالهٔ حریم خصوصی شهروندان که در فضای مجازی دستخوش چالش و تهدیدات جدی است پرداخته و به‌ویژه، مسالهٔ *حریم خصوصی اطلاعاتی*[1] ایشان را قاعده‌مند می‌سازد. مراد از حریم خصوصی اطلاعاتی، *مجموعه اطلاعات و داده‌های مربوط به زندگی شخصی شهروندان می‌باشد که نوع انسان تمایل به حفظ محرمانگی و مصونیت آن از هرگونه دخل و تصرف غیرمجاز دارد*. این داده‌ها را در یک تقسیم‌بندی کلی می‌توان به شش دسته ذیل تقسیم نمود (اصلانی،۱۳۸۴):

- داده‌های شخصی مربوط به سلامتی و خصوصیات وراثتی؛
- داده‌های شخصی تجاری و اقتصادی؛
- داده‌های شخصی اعتقادی؛
- داده‌های شخصی جنسی؛

1. Information Privacy

- داده‌های شخصی مربوط به محکومیت‌های کیفری؛
- داده‌های شخصی عمومی؛

آن‌چه در این نوشتار مورد بررسی قرار خواهد گرفت، وضعیت حقوقی حمایت از داده‌های دسته نخست می‌باشد.

۲) تعریف

در یک تعریف ساده می‌توان گفت که مراد از داده‌های شخصی مربوط به سلامتی و خصوصیات وراثتی، *مجموعه اطلاعاتی است که مبین وضعیت سلامت یا عدم سلامت فیزیکی یا روانی شخص و همچنین مختصات و داشته‌های ژنتیکی و ذاتی انسان‌هاست*. توضیح این نکته ضروری است که هرچند داده‌های مربوط به سلامتی و داده‌های مربوط به خصوصیات وراثتی ماهیتاً از یکدیگر متفاوتند، لیکن در اینجا نظر به قرابت و مشابهت فراوان میان مباحث مربوط به این دو دسته از داده‌ها و همچنین ارتباط نزدیک میان این‌دو (از این حیث که خصوصیات وراثتی غالباً بر سلامتی افراد نیز موثر می‌باشد)، هر دو دسته را ذیل یک عنوان بررسی می‌نمائیم.

۳) اهمیت بحث

اطلاعات مربوط به پاره‌ای از بیماری‌ها و اختلالات جسمی یا روانی آن‌چنان برای اشخاص مهم تلقی می‌شوند که افشاء و سوء استفاده از آن‌ها ممکن است برخلاف تمایل شخص بوده و موجب سرافکندگی یا عوارض اجتماعی دیگر برای او شود[۱]. به‌عنوان مثال ابتلای شخص به بیماری ایدز که مثلاً ممکن است ناشی از عدم رعایت اصول بهداشتی در یک آرایشگاه عمومی باشد (یا حتی مواردی که این بیماری ناشی از ارتکاب سایر

۱. به‌عنوان مثال، اخیراً دیدیم که در جریان اخذ رای اعتماد کابینهٔ دولت نهم از مجلس شورای اسلامی، اطلاعات مربوط به ابتلای یکی از وزرای پیشنهادی رئیس جمهور به بیماری سرطان (صرف‌نظر از صحت و سقم آن) موانعی را برای وزیر پیشنهادی ایجاد کرده بود.

رفتارهای خطرناک غیر اخلاقی است) علی الاصول در زمرهٔ چنین داده‌هایی است.

همچنین خصوصیات وراثتی اشخاص که ممکن است آثار روانی یا جسمی در ایشان به دنبال داشته باشد در زمرهٔ اطلاعاتی هستند که علی‌الاصول انسان‌ها تمایلی به افشاء آن ندارند. در صورتی که این گونه داده‌ها در اختیار سودجویان و سوء استفاده گران بیافتد، ممکن است از یک‌سو موجب ایجاد تنش‌های عمیق و مخرب در زندگی شخصی و خانوادگی شخص شده و از سوی دیگر فضای اخلاقی جامعه را به سمت چیرگی نمودها و رفتارهای غیراخلاقی سوق داده و آرامش اجتماع را دستخوش تزلزل کند[1]. همواره محتمل است که اطلاعات مربوط به سوابق پزشکی و یا خصوصیات ژنتیکی شخص از طریق شبکه مورد دستبرد و یا سوء استفاده‌های دیگر قرار گیرد. در چنین وضعیتی حمایت حقوقی از داده‌هایی از این قبیل، راه‌حل نهایی برای مقابله با سودجویان و سوءاستفاده‌گران است. این گونه داده‌ها که در زمرهٔ *داده‌های شخصی حساس*[2] قرار می‌گیرند در نظام‌های مختلف حقوقی کم و بیش مورد حمایت می‌باشند. هدف از چنین حمایتی، از یک‌سو تامین آرامش خاطر شهروندان و حمایت از قواعد اخلاقی منع‌کنندهٔ افشای اسرار (که تقریباً در تمامی مکاتب اخلاقی و به‌خصوص مذاهب توحیدی نیز مورد تاکید قرار گرفته است)[3] و از سوی دیگر، انتفاع از مزایای بی‌شمار به‌کارگیری فناوری اطلاعات و ارتباطات در عرصهٔ بهداشت و سلامت جامعه است؛ زیرا بدون تامین امنیت چنین داده‌هایی امر گردآوری داده‌ها و در نتیجه، پردازش و به‌کارگیری آن‌ها در عرصهٔ سلامت و بهداشت جامعه مختل خواهد شد.

---

۱. برای دیدن نمونه‌هایی از اخبار مربوط به این قبیل سوء استفاده‌ها، ر.ک به: Janlori Goldman, 1996.

2. Sensitive Personal Data

۳. در حقوق اسلامی مفاهیمی چون منع تجسس (سورهٔ حجرات، آیهٔ ۱۲) و حرمت غیبت (سورهٔ حجرات، آیهٔ ۱۲) و لزوم استیذان قبل از دخول در منازل غیر (سورهٔ نور، آیات ۲۷و۲۸) و برشمرده شدن صفت ستاربودن خداوند در زمرهٔ صفات ثبوتیه و حمیده، درکنار توصیه به خداگونه شدن و موارد مشابه، مبین اهمیت و محترم بودن حریم خصوصی واطلاعات مربوط به زندگی خصوصی افراد می‌باشد.

۴) اصول حاکم بر حمایت از داده

بر اساس آن‌چه در بالا بدان اشاره شد، تردیدی در لزوم حمایت ویژه از محرمانگی و امنیت *داده‌های شخصی مربوط به سلامتی و خصوصیات وراثتی* شهروندان به‌ویژه در فضای مجازی باقی نخواهد ماند. لیکن سوال اساس‌تر این است که ماهیت این حمایت چیست؟ و قواعد حقوقی مربوط دقیقاً چه الزاماتی را به همراه دارند؟ برای پاسخ به این سوال باید گفت که مجموعه الزامات و ضوابط حاکم بر مسالهٔ حمایت از داده‌ها (به‌ویژه در فضای مجازی) که صرف‌نظر از قوانین موجود در یک نظام حقوقی خاص قابل اعمال می‌باشند را *اصول حاکم بر حمایت از داده* می‌نامیم که ذیلا اشاره‌ای گذرا و شرح‌الاسم گونه، به هریک خواهیم افکند (اصلانی، ۱۳۸۵: ۱۳۳) این اصول مبین الزامات لازم الرعایه در عرصهٔ حمایت از داده به‌ویژه *داده‌های شخصیِ مربوط به سلامتی و خصوصیات وراثتی* می‌باشند و به شرح ذیل‌اند:

۱-۴) اصول مربوط به تحصیل داده‌ها

۱-۱-۴) اصل تحصیل قانونی و منصفانه[1]

مطابق این اصل، تحصیل داده‌های شخصی مربوط به دیگری می‌باید از طریق روش و ابزار قانونی و مشروع صورت گیرد.

۲-۱-۴) اصل تحصیل مضیق و مرتبط[2]

به‌موجب این اصل، اولاً تحصیل داده‌ها تنها برای هدف قانونی و مشروع مجاز است (یا

1. Fair Means of Collection
2. Collection for a Proper Purpose

در برخی منابع از این اصل با عنوان اصل هدف مضیق Purpose Limitation Principle یاد شده است. به‌عنوان نمونه ر.ک به: Graham Greenleaf,1996

لااقل می‌توان گفت تحصیل داده‌ها برای هدف غیرقانونی یا نامشروع ممنوع است)؛ ثانیاً نوع داده‌های گردآوری شده باید با هدف اولیهٔ تحصیل داده‌ها منطبق باشد؛ ثالثاً گردآوری داده‌ها باید تنها به میزان مورد نیاز برای هدف اولیه و اعلام شده صورت گیرد و گردآوری داده‌های اضافی ممنوع است.

۳-۱-۴) اصل انتخاب[1]

اصل انتخاب بدان معناست که موسسه یا شخصی که قصد گردآوری داده‌ها در خصوص شخص سوژه را دارد پیش از هرچیز می‌باید این امکان را برای کاربر فراهم آورد که صریحاً نظر خود را مبنی بر این‌که آیا با گردآوری داده‌های شخصی خود موافقت دارد یا خیر اعلام نماید.

۴-۱-۴) اصل اطلاع[2]

مفهوم اصل اطلاع آن است که گردآوری و پردازش داده‌های شخصی (حداقل در خصوص پردازش‌های تغییردهنده داده) منوط به اعلام مراتب به شخص سوژه می‌باشد مگر در مواردی که قانون بنا به پاره‌ای مصالح استثنایی و مصرح (همچون مسائل امنیتی) خلاف آن را مقرر دارد.

1. Opt Principle
2. Notice Principle

اصطلاح معادل دیگری که در این خصوص مورد استفاده قرار می‌گیرد و رواج دارد "آگاه کردن کاربر از دلیل گردآوری داده‌ها" می‌باشد که البتّه تنها ناظر بر مرحلهٔ گردآوری داده‌هاست و نسبت به مرحلهٔ پردازش داده‌ها شمولی ندارد. ر.ک به: Graham Greenleaf, op.cit

۲-۴) اصول مربوط به نگهداری داده‌ها[۱]

۱-۲-۴) اصل امنیت[۲]

اصل امنیت بدان معناست که کسی که داده‌ها را تحصیل نموده یا در اختیار دارد می‌باید تدابیر امنیتی لازم برای جلوگیری از دسترسی یا پردازش غیرمجاز داده‌ها توسط دیگران را به‌کار گیرد و عدم به‌کارگیری چنین تدابیری موجب مسئولیت اوست.

۲-۲-۴) اصل شفافیت[۳]

بر اساس این اصل، موسسهٔ مورد بحث باید اولاً در صورت تقاضا، امکان دسترسی اشخاص به محتوا، نوع، هدف گردآوری و سایر اطلاعات مربوط به داده‌های شخصی ایشان را فراهم آورده و ثانیاً باید رویهٔ خاصی برای حمایت از حریم خصوصی اطلاعاتی اشخاص داشته باشد و آن را به‌نحو شفاف در دسترس کاربران قرار دهد.

۳-۲-۴) اصل دسترسی[۴]

به‌موجب این اصل، موسسهٔ دارندهٔ داده‌ها می‌باید در صورت درخواست کاربری که داده‌های او تحصیل یا پردازش می‌شود (سوژه)، امکان دستیابی او را به اطلاعات مربوط به نوع، ماهیت و روش گردآوری و احیاناً کیفیت داده‌های مزبور فراهم آورد.

---

۱. لازم به یادآوری است که مفهوم اصل امنیت، اصل صحت و اصل دسترسی در مانحن فیه با مفهوم این اصول در مباحث مربوط به امنیت که از ابعاد فنی مورد بررسی قرار می‌گیرد تفاوت‌هایی دارد که ذیل هر یک از عناوین به اختصار تبیین شده‌اند.

2. Security Principle

3. Transparency Principle

در برخی متون اصطلاح اصل گشوده بودن (Openness Principle) به همین مفهوم به‌کار رفته است. ر.ک به: Nigel Waters, 2001

4. Access Principle

۴-۲-۴) اصل صحت[1]

این اصل که اصلی کیفی بوده و ناظر بر محتوای داده‌ها است اقتضای آن دارد که موسسه یا شخصی که به گردآوری و پردازش داده‌ها می‌پردازد در تمام مراحل، نه تنها داده‌های صحیح گردآوری پردازش و منتقل نماید، بلکه ترتیبات و تدابیر مقتضی برای حصول اطمینان از صحیح بودن، کامل بودن و روزآمد بودن داده‌ها نیز به‌کار گیرد.

۴-۳) اصول مربوط به به‌کارگیری داده‌ها

۴-۳-۱) اصل پردازش مرتبط[2]

بر اساس این اصل، گردآورنده و پردازشگر داده‌ها تنها اجازهٔ پردازش داده‌ها را در حدود مورد توافق داشته یا اجازهٔ قانون‌گذار را دارد و باید از پردازش آن‌ها برای اهداف غیرمرتبط و ثانوی خودداری کند.

۴-۳-۲) اصل ممنوعیت افشاء[3]

بر اساس این اصل، افشاء داده‌ها به اشخاص ثالث و به‌منظور نیل به یک هدف ثانوی، امری است که علی الاصول در چارچوب اجازهٔ اولیهٔ صادره از سوی سوژه یا قانون‌گذار نمی‌گنجد و لذا ممنوع است و این اصل در تمامی مراحل تحصیل پردازش و انتقال داده‌ها لازم الرعایه می‌باشد.

---

1. Accuracy of Information

از این اصل با عنوان کیفیت داده (Data Quality) یا کیفیت اطّلاعات (Information Quality) نیز یاد شده است .ر.ک

(The Office of the Privacy Commissioner of Australia,2000), (Nigel Waters,op.cit)

2. Proper Purpose Proccess

3. Disclosure Restriction Principle

۴-۴) اصول مربوط به امحاء و انتقال داده‌ها

۴-۴-۱) اصل امحاء[1]

این اصل که از آثار اصل امنیت است، اقتضا دارد که به محض برطرف شدن نیاز پردازش‌گر یا دارندهٔ داده‌ها به آن‌ها، نسبت به زائل نمودن و امحاء داده‌های مزبور اقدام نماید.

۴-۴-۲) اصل عدم انتقال

بر این اساس، در بحث از حریم خصوصی اطلاعاتی یکی از اصول حاکم و بنیادین که در تمام مراحل، باید از سوی دارنده و پردازش‌گر داده‌ها رعایت شود، اصل ممنوعیت داده‌های شخصی به‌ویژه انتقال فرامرزی آن است.

۴-۵) سایر اصول

۴-۵-۱) اصل رضایت[2]

بر اساس این اصل، از آن‌جا که هدف از تدوین مقررات حمایت از داده‌های شخصی در درجهٔ اول صیانت از حقوق شهروندان است، لذا علی الاصول در اغلب موارد، اخذ رضایت سوژه می‌تواند وصف ممنوعیت و تخلف را از اعمال ناقض حریم خصوصی (در هریک از مراحل تحصیل، پردازش و انتقال و امحاء داده‌ها) سلب نماید.

۴-۵-۲) اصل مسئولیت[3]

بر اساس این اصل می‌توان گفت که گردآورنده و پردازش‌گر داده‌ها نسبت به تخلف از احکام قانونی و تجاوز به حریم خصوصی شهروندان علی الاصول و مشروط به تحقق

1. Erase Principle
2. Consent Principle
3. Redress Principle

شرایط عمومی و اختصاصی مسوولیت دارد و شهروندان در هرحال حق دادخواهی و تقاضای بهره مندی از روش‌های جبران را دارند (اصلان،۱۳۸۴).

در پایان یادآوری این نکته ضروری است که همچون همهٔ اصولی که در دانش حقوق مورد استناد واقع می شوند، این اصول نیز مطلق و بلااستثنا نبوده و در مواردی اعمال آن‌ها با پاره‌ای تحدیدها و تضییقات مواجه می‌باشد که بررسی آن‌ها از حوصلهٔ این مقال بیرون است.

۵) وضعیت بحث از منظر حقوق تطبیقی

در حقوق برخی کشورها که به بحث حاضر پرداخته‌اند، اصولاً *داده‌های شخصی مربوط به سلامتی و خصوصیات وراثتی* در زمرهٔ داده‌های شخصی حساس جای گرفته و نظر به حساسیت و اهمیتی که ممکن است پردازش آن‌ها یا ارتکاب سایر اعمال ممنوعهٔ فوق‌الاشاره نسبت بدان‌ها در پی داشته باشد، مقررات ویژه‌ای برای حمایت از آن‌ها در نظر گرفته شده است. ذیلا اشاره‌ای گذرا به چگونگی حمایت از این داده‌ها و اعمال اصول فوق در چند نظام حقوقی پیشرو می‌افکنیم.

۱-۵) اتحادیه اروپایی

بند ۱ مادهٔ ۸ دستورالعمل شمارهٔ 95/46/EC اتحادیه اروپایی مقرر می‌دارد که «*کشورهای عضو پردازش داده‌های شخصی مربوط به ریشه‌های قومی و نژادی، اعتقادات سیاسی، عقاید دینی و فلسفی، عضویت در اتحادیه‌های تجاری و پردازش داده‌های مربوط به سلامتی و زندگی جنسی را ممنوع خواهند نمود*».

داده‌های موضوع این ماده که به داده‌های شخصی حساس معروفند، تقریباً در اغلب قوانین و متون قانونی مشابه مشمول حمایت‌هایی بیش از سایر داده‌ها قرار گرفته‌اند. همان‌گونه که ملاحظه می‌شود، مطابق این ماده، از دستورالعمل که در واقع راهنمای کشورهای عضو در امر قانون‌نویسی در عرصهٔ حمایت از داده‌های شخصی می‌باشد،

داده‌های مربوط به سلامتی اشخاص در زمرهٔ داده‌های مورد حمایت بوده و پردازش آن‌ها جز در موارد مصرح مجاز نمی‌باشد. همچنین مادهٔ ۵ این سند تکلیف کشورهای عضو دائر بر لزوم تعیین دقیق موارد استثنا از حکم مزبور را پیش‌بینی نموده است. نکته‌ای که در اینجا ذکر آن ضروری است، تعریف واژهٔ *پردازش* که در ماده ۸ فوق ممنوع شده است می‌باشد. مطابق بند b مادهٔ ۲ این سند، *پردازش داده‌های شخصی یعنی عملیات یا مجموعه عملیاتی که بر روی داده‌های شخصی، خواه از طریق ابزارهای خودکار خواه غیرخودکار* انجام می‌شود، از قبیل تحصیل، ضبط کردن، سازماندهی، ذخیره نمودن، هماهنگ نمودن یا جایگزین نمودن، بازیابی، استفاده، افشاء از طریق انتقال، انتشار یا در دسترس قرار دادن از طرق دیگر، دسته‌بندی یا ترکیب، انسداد، امحاء یا تخریب داده‌ها. بر این اساس، ملاحظه می‌شود که مجموعه اعمال ممنوعی که مطابق این تعریف با ملحوظ داشتن حکم مادهٔ ۸ پیش گفته می‌باشد، در خصوص داده‌های شخصی مربوط به سلامتی مورد رعایت قرار گیرد، طیف وسیعی از اعمال را دربرمی‌گیرد.

همچنین در دستورالعمل فوق، مطابق بند ۲ همان ماده، پردازش این قبیل داده‌ها در پنج مورد مجاز شمرده شده است که در واقع استثناهای اصل فوق می‌باشند. لازم به توضیح است که هرچند در این دستورالعمل و برخی متون قانونی مشابه، عبارت داده‌های مربوط به ریشه‌های قومی و نژادی مستقل از داده‌های مربوط به سلامتی و خصوصیات وراثتی به‌کار رفته است، لیکن به اعتقاد ما، با کمی مسامحه می‌توان این گونه داده‌ها را در زمرهٔ داده‌های وراثتی مورد بررسی قرار داد و لذا از ذکر جداگانهٔ آن خودداری می‌نمائیم.

۲-۵) انگلستان و ایتالیا

قانون حمایت از دادهٔ انگلستان مصوب ۱۹۹۸ نیز در مادهٔ ۲ داده‌های شخصی حساس را در ۸ بند برشمرده که بند پنجم آن به *داده‌های مربوط به سلامتی و شرایط جسمانی یا روانی*[1] شخص سوژه اختصاص دارد و در جدول شمارهٔ ۳ ضمیمه، مقررات نسبتاً مفصل

1. Physical or mental health or condition

مربوط به پردازش داده‌ها از جمله داده‌های شخصی حساس را مقرر نموده است. این مقررات که نوعاً تحت تاثیر دستورالعمل فوق الاشاره تنظیم شده است، تا حدود زیادی از حیث محتوا با احکام دستورالعمل مزبور انطباق دارد.

همچنین مادهٔ ۲۲ قانون حمایت از دادهٔ ایتالیا نیز همچون قانون انگلستان، ضمن احصاء مصادیق داده‌های حساس (از جمله داده‌های مربوط به سلامتی) پردازش این گونه داده‌ها را مشروط به شرایطی از جمله اخذ رضایت کتبی قبلی سوژه و اخذ اجازه از مقام ناظر نموده است. البته به‌موجب مادهٔ ۲۳ همان قانون، پردازش این گونه داده‌ها توسط برخی اشخاص و نهادهای متولی امر سلامت در جامعه از حکم فوق مستثنی می‌باشد.

۳-۵) ایالات متحدهٔ امریکا

در امریکا قانونِ "Health Insurance Portability and Accountability Act" مصوب ۱۹۹۶ که اختصارا *HIPAA* نامیده می‌شود و یک قانون فدرال می‌باشد و همچنین سازمانی با همین نام، متکفل قاعده‌مند نمودن نحوهٔ تحصیل و پردازش داده‌های مربوط به سلامتی اشخاص می‌باشند. اهم مفاد و اصول مندرج در این قانون عبارتند از:

- حداقل استانداردهای ملی لازم‌الرعایه؛
- اعلام رویهٔ مورد عمل در حمایت از حریم خصوصی بیمار، به او؛
- حق دسترسی بیمار به فایل‌های حاوی داده‌های او؛
- حق اصلاح داده‌های نادرست؛
- اعلام موارد افشاء داده‌های بیمار در موارد مجاز افشاء، به او؛
- وظایف بیمارستان‌ها و نهادهای مشابه در جهت آموزش به‌کارگیری رویه‌های فنی و اداری متناسب، کارکنان و انتصاب مرجع پاسخگویی؛
- منع افشاء داده‌ها به کارفرمایان؛
- منع افشاء داده‌های مربوط به سلامت روانی؛
- حق منع بیمارستان از درج نام بیمار در سیاههٔ بیماران بیمارستان؛

- موارد استثناء قانونی؛
- رسیدگی به شکایات.

لازم به ذکر است که با توجه به امکان دسترسی و پردازش این گونه داده‌ها توسط پزشکان و داروسازان، نهادهای متکفل بیمه‌های درمانی و سایر دست‌اندرکاران بخش درمان امروزه در اغلب نظام‌های حقوقی مدرن مقررات ویژه‌ای نسبت به این قشر در جهت صیانت از حریم *خصوصی بیماران*[1] یا حریم *خصوصی درمانی*[2] اعمال می‌شود و اصولاً مبحث حریم خصوصی بیماران خود، حوزهٔ مستقلی از مباحث حریم خصوصی محسوب می‌شود.

۴-۵) کنوانسیون جرایم محیط سایبر (کنوانسیون بوداپست)[3]

کنوانسیون بوداپست یک کنوانسیون اروپایی است. این کنوانسیون با هدف "جلوگیری از اعمالی که علیه محرمانگی[4]، تمامیت[5] و در دسترس بودن[6] سیستم‌های رایانه‌ای، شبکه‌ها و داده‌های رایانه‌ای به‌وقوع می‌پیوندد" تدوین و تصویب شد. این کنوانسیون سعی دارد اسناد معتبر بین‌المللی و به‌ویژه اسناد اروپایی از جمله "کنوانسیون اروپایی ۱۹۵۰ حقوق بشر"، "میثاق بین‌المللی حقوق سیاسی و مدنی" ۱۹۶۶ سازمان ملل متحد، کنوانسیون۱۹۸۱ شورای اروپا ناظر به" حمایت از افراد در برابر پردازش خودکار داده‌های شخصی" و.... را ملحوظ دارد.

1. Patient Privacy Rights
2. Medical Privacy

۳. این کنوانسیون در تاریخ ۲۳ سپتامبر۲۰۰۱ در شهر بوداپست به امضای کشورهای اروپایی عضو اتحادیهٔ اروپایی و چند کشور اروپایی غیر عضو اتحادیهٔ مزبور رسید و هدف آن، حمایت از جامعه در برابر جرائم محیط سایبر است.

4. Confidentiality
5. Integrity
6. Availability(Accessibility)

در خصوص وضعیت و چگونگی حمایت از داده‌های شخصی عرصهٔ بهداشت و سلامت در کنوانسیون بوداپست باید خاطر نشان نمود که علی‌رغم آن‌که مطابق مفاد مقدمه کنوانسیون، یکی از اهداف مهم این سند، حمایت از محرمانگی و تمامیت و در دسترس بودن داده‌های شخصی است و در همین راستا نیز مواد مختلف آن از جمله مواد ۲،۳،۴،۵ و ۷ به نحوی از انحاء به حمایت از محرمانگی، تمامیت و در دسترس بودن داده‌ها، به‌ویژه داده‌های شخصی پرداخته است و مقررات حمایتی برای آن پیش‌بینی نموده است (جلالی، ۱۳۸۳)، مع‌الوصف اولاً هیچ تقسیم‌بندی از اقسام داده‌های شخصی عرضه ننموده است و ثانیا و بالتبع هیچ حمایت ویژه و خاصی را در خصوص داده‌های شخصی حساس و در میان آن‌ها، داده‌های شخصی مربوط به وضعیت سلامت و بهداشت افراد پیش بینی ننموده است.

بر این اساس می‌توان به‌طور خلاصه نتیجه گرفت که کنوانسیون یاد شده حمایت ویژه و خاص نظیر آن‌چه در اسناد پیشین بدان‌ها اشاره شد، مد نظر نداشته و لذا از این منظر سطح حمایت مطلوبی از داده‌های شخصی مربوط به وضعیت بهداشت و سلامت و همچنین داده‌های شخصی ناظر بر خصوصیات وراثتی شخص به‌دست نمی‌دهد.

۵-۵) وضعیت حقوق ایران

در باب وضعیت بحث در حقوق ایران باید گفت که حمایت قانون‌گذار ایرانی از داده‌های مربوط به سلامتی (و خصوصیات ژنتیکی) افراد پیش از تصویب قانون تجارت الکترونیکی تنها در گستره‌ای بسیار محدود مسبوق به سابقه می‌باشد و هرگز قانون‌گذار ایرانی به فکر حمایت همه جانبه از این داده‌ها نبوده است. به‌عنوان نمونه در قوانین پیشین (قبل از تصویب قانون تجارت الکترونیکی) مادهٔ ۶۴۸ قانون مجازات اسلامی مقرر می‌دارد *اطباء و جراحان و ماماها و داروفروشان و کلیهٔ کسانی که به مناسبت شغل یا حرفهٔ خود محرم اسرار می‌شوند، هرگاه در غیراز موارد قانونی، اسرار مردم را افشا کنند به سه ماه و یک روز تا یک سال حبس و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی*

محکوم می‌شوند. توجه به مفاد این ماده مبین آن است که علی‌رغم این‌که حکم این ماده نسبت به مانحن فیه خاص بوده[1] و تنها شامل کسانی می‌شود که به مناسبت شغل خود محرم اسرار مردم می‌شوند و مطلق دارندگان داده‌های مربوط به سلامتی را تحت پوشش قرار نمی‌دهد، لیکن پذیرش این حکم از جانب قانون‌گذار به‌ویژه با لحاظ تحولات ناشی از پیدایش و گسترش فناوری اطلاعات و ارتباطات، مبین آن است که قانون‌گذار ایران آمادگی و زمینهٔ مناسب برای تهیهٔ قوانین حمایت‌کننده از داده‌های مورد بحث را داراست.

در باب وضعیت بحث در پرتو فناوری اطلاعات و ارتباطات در حقوق داخلی نیز باید خاطر نشان نمود که قانون‌گذار ایران در مادهٔ ۵۸ قانون اخیر التصویب تجارت الکترونیکی سال ۱۳۸۲ که تنها قانونی است که به این امر پرداخته است مقرر می‌دارد *ذخیره، پردازش و یا توزیع «داده پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هرعنوان غیرقانونی است. همچنین مطابق مادهٔ ۶۰ همان قانون، ذخیره، پردازش و یا توزیع «داده پیام»های مربوط به سوابق پزشکی و بهداشتی تابع آیین نامه‌ای است که در مادهٔ ۷۹ این قانون خواهد آمد*. البته این آئین نامه تاکنون به تصویب نرسیده است و لذا خلاء قانونی در این خصوص مشهود است. همچنین به‌موجب مادهٔ ۷۱ قانون فوق‌الذکر، *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*.

گذشته از ایرادات عدیدهٔ نگارشی و قانون‌نویسی موجود در متن مواد مذکور، باید گفت که مطابق این نصوص قانونی، اولاً قانون‌گذار علی‌الاصول مطلق داده‌های شخصی را مورد حمایت قرار نداده است، بلکه مصادیق داده‌های مورد حمایت احصاء شده در مادهٔ ۵۸ فوق مبین آن است که تنها داده‌های شخصی حساس (از جمله داده‌های مربوط به

۱. البته می‌توان گفت که این ماده از جهتی نسبت به مانحن فیه عام می‌باشد، زیرا علاوه بر داده‌های مربوط به سلامتی می‌توان آن را به سایر داده‌های شخصی نیز تسری داد.

سوابق پزشکی و بهداشتی) مورد حمایت قانون‌گذار می‌باشد.

ثانیاً مطابق مادهٔ ۵۹ همان قانون که مقرر می‌دارد *درصورت رضایت شخص موضوع «داده پیام» نیز به شرط آنکه محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع «داده پیام»های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:*

الف) اهداف آن مشخص بوده و به طور واضح شرح داده شده باشد.

ب) «داده پیام» باید تنها به اندازهٔ ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع «داده پیام» شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.

ج) «داده پیام» باید صحیح و روزآمد باشد.

د) شخص موضوع «داده پیام» باید به پرونده‌های رایانه‌ای حاوی «داده پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده پیام»های 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 پروندهٔ رایانه‌ای «داده پیام»های شخصی مربوط به خود را بنماید؛ و همچنین قید مذکور در ذیل مادهٔ ۵۸ (بدون رضایت صریح آن‌ها) تنها موردی که در نظر قانون‌گذار ایرانی به‌عنوان استثنایی بر اصل ممنوعیت پردازش این گونه داده‌ها مقرر گردیده است اخذ رضایت سوژه البته با رعایت شرایط مقرر در این مواد می‌باشد و قانونگذار با آن‌که در مقام بیان بوده است از موارد خاص و استثنایی که بنا به دلایل امنیتی، و مصالح عمومی و امثال ذلک بتوان دست به پردازش این داده‌ها زد سخنی به میان نیاورده که این سکوت در مقام بیان موید این نتیجهٔ نه چندان معقول و منطقی است که حتی در چنین شرایط خاصی نیز حاکمیت نباید اقدام به پردازش داده‌ها بزند؛ که این امر البته با رویکرد مبتنی بر حداقل حمایت و محدودنگر حاکم بر قانون مزبور چندان انطباقی نیز ندارد. علی‌ای‌حال مطابق نتیجهٔ نه چندان منطقی و مناسبی که از این قواعد برمی‌آید، حتی در

مواردی که پردازش داده‌های شخصی مربوط به سلامت و وضعیت وراثتی اشخاص برای مقابله با یک اپیدمی ضروری است، این امر باید با اخذ رضایت از تک تک افراد صورت گیرد!

ثالثاً با آن‌که قانون‌گذار می‌توانسته در همین بخش از قانون از داده‌های شخصی حساس، به‌ویژه داده‌های مربوط به سلامتی و خصوصیات ژنتیکی و نژادی که موضوع بحث حاضر می‌باشد، با پیش‌بینی یک متن جامع قانونی حمایت کلی به‌عمل آورد، مع‌الوصف از این کار خودداری نموده است. لذا در شرایط فعلی پردازش داده‌های مورد بحث و انتشار آن‌ها تنها در صورتی ممنوع است که در فضای مجازی و در قالب داده پیام[1] که مطابق تعریف قانونی مندرج در بند الف مادهٔ ۲ قانون مزبور (که عبارت است از هر نمادی از واقعه، اطلاعات یا مفهوم که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود) صورت گیرد و سایر اشکال تجاوز به این حق، مورد حکم قرار نگرفته است.

رابعاً با وجود آن‌که داده‌های احصاء شده در ماده ۵۸ فوق الذکر ماهیتا اختصاص به اشخاص حقیقی دارد، مع‌الوصف قانون‌گذار در این ماده از واژهٔ اشخاص که جمع واژهٔ شخص می‌باشد به‌نحو مطلق استفاده کرده است که با لحاظ بند م مادهٔ ۲ قانون که مقرر می‌دارد «شخص»[2] اعم است از شخص حقیقی و حقوقی و یا سیستم‌های رایانه‌ای تحت کنترل آنان، گونه‌ای عدم تطابق میان مفاد ماده مذکور و تعریف اخیرالذکر (که نوعی حقیقت شرعیه محسوب می‌شود[3]) به چشم می‌خورد. هرچند می‌توان گفت که مراد از داده پیام‌های شخصی»[4] مطابق بند ر مادهٔ ۲ موصوف «داده پیام»های مربوط به یک شخص

1. Data Message

2. Person

۳. مراد از حقیقت شرعیه در اینجا مفهوم این عبارت در دانش اصول استنباط می‌باشد که به معنی آن است که از آن‌جا که خود شارع (قانون‌گذار) اقدام به تعریف مراد خود از واژهٔ مورد بحث نموده است، لذا رجوع به متفاهم عرفی از این واژه و استمساک به تبادر ممنوع است. ر.ک به: محمدی، ۱۳۷۶.

4. Private Data

حقیقی (موضوع «داده»[1]) مشخص و معین می‌باشد.

همچنین در پایان خاطر نشان می‌سازد، که اخیراً لایحه‌ای تحت عنوان "لایحهٔ مجازات جرائم رایانه‌ای" توسط جمعی از متخصصان به هماهنگی و به سفارش قوهٔ قضائیه تدوین شده و مراحل تصویب در قوهٔ قضائیه و دولت را نیز پشت سر گذاشته است که هم اکنون در مجلس شورای اسلامی تحت بررسی است (توحیدی نافع، ۱۳۸۴). در لایحهٔ مورد اشاره نیز به دلیل تاسّی فراوان مدونین آن، از کنوانسیون بوداپست، روح حاکم بر کنوانسیون مورد بحث حاکم است و مآلا حمایت ویژه و خاصی از داده‌های شخصی حساس و در میان آن‌ها، داده‌های مرتبط با وضعیت سلامتی و خصوصیات وراثتی شهروندان پیش‌بینی نشده است.

۶) نتایج و یافته‌ها

راهیابی فناوری اطلاعات به عرصهٔ سلامت و پزشکی امری محتوم و البته مفید است. در این رهگذر مسائل حقوقی عدیده‌ای قابلیت بروز دارند که از جمله مهم‌ترین آن‌ها نحوهٔ صیانت از اطلاعات و داده‌های مرتبط با وضعیت سلامتی و خصوصیات وراثتی شهروندان می‌باشد که دلیل عمدهٔ آن تسهیل گردآوری، دسترسی و پردازش این داده‌ها در سطحی گسترده و وسیع می‌باشد که به مدد به‌کارگیری فناوری اطلاعات میسور شده است. نظری به حقوق کشورهای پیشرو مبین اتخاذ رویکرد منطقی و متوازن این نظام‌های حقوقی در حمایت از داده‌ها است که مبتنی بر اصل اولیه حمایت و امکان ترتب استثناهای قانونی بر این اصل اولیه می‌باشد. در این میان داده‌های موضوع این مقاله به دلیل اهمیت و خصوصیات ویژهٔ خود مورد حمایت بیشتری قرار گرفته است. قانون‌گذار ایران برخلاف نظام‌های حقوقی مزبور با اتخاذ رویکردی دوگانه از یک‌سو مطلق این‌گونه داده را مورد حمایت قرار نداده است و تنها صور خاصی از آن را آن‌هم در صورتی که در قالب داده پیام باشد، مورد حمایت تلقی می‌کند و از سوی دیگر هیچ‌گونه استثنایی جز اخذ رضایت

1. Data Subject

شخص سوژه در این مسیر به رسمیت نشناخته است و روشن نیست که در برخورد با مواردی که گردآوری و پردازش این داده‌ها برای تامین سلامت عمومی یا امنیت و مصالح عمومی ضروری باشد، همچنین در خصوص مواردی که استفاده تنها جنبهٔ آماری یا علمی تحقیقاتی داشته باشد چه رویکردی را اتخاذ نموده است. لایحهٔ جرائم رایانه‌ای نیز از این منظر خاص، هیچ‌گونه نوآوری نداشته و بر ابهام موضوع افزوده است.

منابع

References

- اصلانی، حمیدرضا. (۱۳۸۵)، **اصول حاکم بر حمایت از داده**، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه با همکاری شورای عالی اطلاع رسانی، قم، سلسبیل، چاپ اول.
- اصلانی، حمیدرضا. (۱۳۸۴)، **حقوق فناوری اطلاعات، حریم خصوصی در جامعه اطلاعاتی**، نشر میزان، تهران، چاپ اول.
- توحیدی نافع، جلال و دیگران. (۱۳۸۴)، **اظهار نظر کارشناسی درباره لایحه جرائم رایانه‌ای**، دفتر ارتباطات و فناوری‌های نوین، مرکز پژوهش‌های مجلس، شمارهٔ مسلسل ۷۵۵۲.
- جلالی، امیر حسین. (۱۳۸۳)، **کنوانسیون جرائم سایبر (کنوانسیون بوداپست)**، تهران، مرکز مطبوعات و انتشارات قوه قضائیه.
- محمدی، ابوالحسن. (۱۳۷۶)، **مبانی استنباط حقوق اسلامی یا اصول فقه**، انتشارات تهران، دانشگاه تهران، چاپ هشتم.

- Brown, Nancy. (2005), **Telemedicine Coming of Age**, September 28, 1996,* Updated on January 13, 2005, available at: <http://tie.telemed.org/articles/article.asp?path=articles&article=tmcoming_nb_tie96.xml>, (April 2006).
- Convention on Cybercrime, Budapest, 23. XI. 2001, available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, (June 2005).
- Data Protection Act 1998 of UK, available at: <http://www.hmso.gov.uk/acts/acts1998/80029--a.htm#1>, (May 2005).
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ,available at: <http://www.cdt.org/privacy/eudirective/EU_Directive_.html>, (April 2005).
- Goldman, Janlori. (1996), **Statement of Janlori Goldman**, Deputy Director,Center for Democracy and Technology, Before the House Committee on Government Reform and Oversight Subcommittee on Government Management, Information and Technology on Medical Records Confidentiality, June 14, 1996, available at: <http://www.cdt.org/testimony/960614goldman.html>, (September 2006).

References منابع

- Greeanleadf, Graham (1996), **Privacy Principles - irrelevant to cyberspace?**, Privacy Law & Policy Reporter (Prospect Publishing), 3 PLPR 114, September 1996, available at: <http://www2.austlii.edu.au/itlaw/articles/IPPs.html>, (April 2005).
- Italian Personal Data Protection Code. (2003), **Legislative Decree**, No. 196 of 30 June 2003, available at: <http://www.privacy.it/privacycode-en.html>, (May 2005).
- National Research Council. (1997), **Protecting Electronic Health Information, Computer Science and Telecommunications Board**, Commission on Physical Sciences, Mathematics, and Applications, National Academy Press, Washington, D.C., 1997, available at: <http://www.nap.edu/catalog.php?record_id=5595#toc>, (April 2005).
- Pacific Privacy Pty Ltd & Convenor. (2005), **Adequacy of Australian Privacy Laws in Relation to the European Union Directive**, Australian Privacy Charter Council available at: <http://www.workplaceinfo.com.au/nocookie/alert/2001/01329.htm>, (April 2005).
- Telermedicine Report. (1997), The Medical Information System Development Center, Japan, available at: <http://square.umin.ac.jp/enkaku/96/Enkaku-RepSoukatu-nof-eng.html>, (April 2005).
- The Health Insurance Portability & Accountability Act (HIPAA). (1996), enacted by the U.S. Congress in 1996, available at: <http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act>, (June 2005).
- The Office of the Privacy Commissioner of Australia. (2000), **National Privacy Principles** (Extracted from the Privacy Amendment (Private Sector) Act 2000), available at: <http://www.privacy.gov.au/publications/npps01.html#c>, (September 2006).