Privacy in Cyberspace

Atefeh Abbasi[1]

Abstract

Information technology provides better medical services and so appropriate conditions for misuse of personal information. Medical information is an important part of sensitive computer data. For the growing of information technology. Protection of patient`s privacy in cyberspace has become one of the main matters of medical law. To this end. The rules are set out in international documents including the right to choose beneficiaries at the information gathering stage. Observance of data security. transparency and access to data and accuracy in data retention. The necessity of related processing and the prohibition of disclosure of data at the stage of information use and finally. the need to eliminate or prohibit transboundary data transfer at the end of the patient status process, however the constitution and some of laws emphasize to privacy and non-disclosure of patients but E-commerce law and cybercrime law generally refer to the protection of such information and without regard to the above sequence and order. Merely refer to the principles of subject satisfaction. Legal collection. as well as data dilatation. The principle of data accuracy and their elimination. Punishments were not sufficient to ensure compliance with the above principles. It is necessary to comply with the precise criteria mentioned above together with appropriate them.

Keywords

Privacy, Sensitive Computer Data, Patient, Cyberspace, Medical Information

Please cite this article as: Abbasi A. Privacy in Cyberspace. Iran J Med Law 2020; 14(54): 115-130.

---

1. Assistant Professor, Faculty of Law, Imam Sadegh University, Sisters Campus Unit, Tehran, Iran. Email: atefehabbasi@isu.ac.ir

Original Article Received: 14 December 2019 Accepted: 6 June 2020

گستره حریم خصوصی بیمار در فضای مجازی

عاطفه عباسی[۱]

چکیده

با وجود آنکه فناوری اطلاعات، ارائه بهتر خدمات پزشکی را ممکن ساخته، لکن شرایط مناسبی را جهت دسترسی به اطلاعات شخصی افراد و سوءاستفاده احتمالی از آن‌ها نیز فراهم می‌آورد. اطلاعات پزشکی بخش مهمی از داده‌های رایانه‌ای حساس را تشکیل می‌دهند که حمایت از محرمانگی آن‌ها با توجه به پیشرفت روزافزون فناوری اطلاعات، یکی از مهم‌ترین دغدغه‌های متولیان این حوزه است. جهت رفع این مشکل در اسناد بین‌المللی، قواعدی در زمینه لزوم تحصیل قانونی، مضیق و مرتبط داده‌ها و نیز توجه به حق انتخاب ذی‌نفع در مرحله گردآوری اطلاعات، رعایت ضوابط مربوط به امنیت، شفافیت و دسترسی به داده‌ها و دقت در صحت آن‌ها در مرحله نگهداری اطلاعات، ضرورت پردازش مرتبط با هدف و نیز ممنوعیت افشای داده‌ها در مرحله به کارگیری اطلاعات و در نهایت لزوم امحای داده‌ها و ممنوعیت انتقال فرامرزی آن‌ها در انتهای فرایند رسیدگی به وضعیت بیمار، پیش‌بینی شده است، هرچند قانون اساسی و دیگر قوانین کشورمان بر لزوم حفظ حریم خصوصی و منع افشای اسرار افراد، از جمله بیماران تأکید دارد، لکن در حوزه اطلاعات رایانه‌ای صرفاً برخی مواد قانون تجارت الکترونیکی و قانون جرائم رایانه‌ای به صورت کلی به حفاظت از اطلاعات مزبور اشاره نموده‌اند. از میان اصول صدرالذکر نیز بدون رعایت توالی و ترتیب فوق، اصول رضایت سوژه، تحصیل قانونی و نیز گردآوری مضیق داده‌ها، اصل صحت داده‌ها و امحای آن‌ها در قوانین داخلی ذکر شده‌اند. ضمانت اجراهای کیفری موجود نیز در تضمین رعایت اصول فوق کافی نبوده و ضروری است نسبت به تصویب قانونی جامع با ضمانت اجراهای متناسب، اقدام گردد.

واژگان کلیدی

حریم خصوصی، داده رایانه‌ای حساس، بیمار، فضای مجازی، اطلاعات پزشکی

---

۱. استادیار گروه حقوق پردیس خواهران دانشگاه امام صادق (ع)، تهران، ایران.

Email: atefehabbasi@isu.ac.ir

نوع مقاله: پژوهشی **تاریخ دریافت مقاله:** ۱۳۹۸/۹/۲۳ **تاریخ پذیرش مقاله:** ۱۳۹۹/۳/۱۷

مقدمه

حریم خصوصی (Privacy) به معنی دورماندن از دید جامعه، زندگی خصوصی، خلوت، آرامش و آسایش بوده (۲-۱) و ناظر بر حق هر انسان برای رهایی از دخالت‌های بی‌مورد سایرین اعم از دولتی و غیر آن، در اموری است که مداخله ایشان توجیهی ندارد و تعرض به این حریم به مفهوم تلاش برای به دست‌آوردن اطلاعات شخصی است، لذا حریم خصوصی را می‌توان محدوده‌ای از زندگی افراد دانست که به عموم مردم ارتباطی ندارد (۳). به عبارت بهتر حریم خصوصی، حق پنهان‌کردن حقایق زندگی شخصی از دیگران بوده و شامل مواردی از زندگی انسان است که از سوی دیگران غیر قابل تسخیر می‌باشد (۴).

با عنایت به آنکه عدم رعایت حریم خصوصی بیمار، موجب افزایش سطح تنش و اضطراب وی و مشکلاتی نظیر احساسات منفی، کاهش همکاری او با کادر درمان، تغییر در الگوی خواب و... می‌گردد (۵)، سازمان بهداشت جهانی از سال ۱۹۹۴، این مفهوم را که مشتمل بر ابعاد فیزیکی، روانی، اجتماعی و اطلاعاتی می‌باشد، به عنوان یکی از اصول اخلاق پزشکی در بیانیه حقوق بیماران قید نمود (۶). منظور از بعد فیزیکی حریم خصوصی بیماران، مکان قابل دیدی است که بدن انسان را احاطه کرده و منطقه‌ای حفاظت‌شده برای فرد، تلقی گردیده و مواردی چون حفظ فاصله شخصی، پوشیدگی بیمار و لمس بدن وی را شامل می‌شود. در معاینات فیزیکی بر حفظ حریم فیزیکی بیمار از طریق ارائه پوشش مناسب و جلوگیری از در معرض دید قرارگرفتن غیر ضروری بدن وی تأکید شده است. حریم خصوصی روحی ـ روانی، به توانایی انسان برای شکل‌دادن به ارزش‌ها و نیز روابط وی با دیگران و تقسیم افکار و اطلاعات خصوصی خود با سایرین اشاره دارد (۷). بعد اجتماعی حریم خصوصی نیز شامل تلاش افراد برای کنترل تماس‌های اجتماعی آن‌هاست (۸)، تلاش برای گمنامی، خلوت و گوشه‌گیری در جامعه با هدف حفظ حریم مزبور انجام می‌پذیرد (۹).

وجه اطلاعاتی حریم خصوصی که ارتباط زیادی با محرمانه‌ماندن اطلاعات شخصی بیمار دارد، حق افراد در تعیین چگونگی، زمان و مکان ارائه اطلاعات خود به دیگران اعم از اشخاص، سازمان‌ها و تشکیلات درمانی را دربر می‌گیرد (۱۰) و بر حفظ حق بیماران به عدم انتشار اطلاعات خصوصی ایشان، تأکید نموده و چالش مهم افشای اطلاعات خصوصی بیمار توسط پزشک و سایر افراد تیم پزشکی را در طول دوران بیماری و پس از آن، مطرح می‌نماید.

هرچند برخی معتقد به تهدید حریم افراد بر اثر پیشرفت تکنولوژی اطلاعاتی نیستند (۱۱)، ولی با توجه به تأثیر پیشرفت ابزارهای اطلاعاتی در ذخیره و پردازش اطلاعات و ناشناختگی آن برای ذی‌نفعان فضای مجازی (۱۲)، امکان تهیه نسخه دقیق اطلاعات رایانه‌ای و تکثیر آن‌ها بدون اطلاع ذی‌نفع، انتشار بر خط اطلاعات (۱۳)، عدم امکان تمییز اطلاعات اصلی از غیر آن و امکان کسب درآمد از اطلاعات دیگران و حتی نقض حریم خصوصی از سوی دولت‌ها، ضروری است تدابیر لازم در جهت حمایت از داده‌های مزبور اتخاذ گردد. بر این اساس توسعه تکنولوژی اطلاعاتی و روند رو به رشد استفاده از رایانه در کلیه مقاطع زندگی، نیاز فزاینده به حفاظت اطلاعات را ایجاب نموده است (۱۴). به دیگر سخن تا پیش از اختراع رایانه و افزایش امکان ذخیره‌سازی و پردازش داده‌ها به صورت بر خط، قوانین سنتی وافی به مقصود بود، لکن در اثر پیشرفت تکنولوژی از دهه ۱۹۷۰ و رشد فزاینده روش‌های جمع‌آوری، ذخیره، دستیابی، مقایسه، انتخاب و انتقال داده‌ها، مخاطرات علیه حقوق خصوصی و فردی بیماران افزایش یافته است.

این مقاله بر آن است که با توجه به نقش انکارناپذیر فناوری اطلاعات در درمان و پردازش اطلاعات پزشکی، ضمن تشریح اطلاعات رایانه‌ای پزشکی و بررسی اسناد بین‌المللی و نیز تحلیل اصول مستنبط از این اسناد که ناظر بر حمایت از اطلاعات رایانه‌ای است، نظام حقوقی ایران را در حمایت کیفری از اطلاعات مزبور مورد آسیب‌شناسی قرار دهد. سنجش میزان مطلوبیت نظام کیفری ایران در حمایت از حریم خصوصی بیماران، پرسشی است که این مقاله به دنبال پاسخ آن است.

حریم خصوصی اطلاعات در پرتو اسناد فراملی و حقوق برخی کشورها

اسناد بین‌المللی به دنبال همسان‌سازی مقررات اداری، مدنی و کیفری در رابطه با حفظ حریم خصوصی می‌باشند، هرچند تصریح به حریم خصوصی در این اسناد به قطع‌نامه کنگره استکهلم بازمی‌گردد که زندگی خصوصی و خانوادگی فرد، نام، هویت، اقامتگاه و مکاتبات وی را مصون از مداخله‌های خودسرانه دانست، اما در واقع حریم خصوصی بخشی از امنیت و آزادی افراد است که به صراحت در ماده ۱۲ اعلامیه جهانی حقوق بشر، ماده ۱۷ میثاق بین‌المللی

حقوق مدنی و سیاسی و ماده ۸ کنوانسیون اروپایی صیانت از حقوق بشر و آزادی‌های بنیادین نیز ذکر شده‌اند (۱۵).

همچنین شورای همکاری‌های اقتصادی و اجتماعی سازمان ملل متحد در سال ۱۹۸۰ توصیه‌نامه‌ای متضمن برخی رهنمودها پیرامون اصول محدودیت جمع‌آوری داده‌ها، کیفیت گردآوری آن‌ها، بیان هدف صریح از ذخیره اطلاعات مزبور، محدودیت استفاده از آن‌ها، برقراری تدابیر ایمنی و میزان مسؤولیت افراد مرتبط، منتشر ساخت (۱۶).

در ۱۹۸۸ کمیسیون فرعی مربوط به جلوگیری از تبعیض نژادی و حمایت از حقوق اقلیت‌ها متعلق به کمیسیون حقوق بشر سازمان ملل متحد، طرحی را برای قانونمندکردن فایل‌های کامپیوتری داده‌های شخصی تهیه کرد که در مجمع عمومی سازمان طی قطع‌نامه ۹۵/۴۵ به تصویب رسید.

گروه کاری حمایت از داده‌های شورای اروپا با تأکید بر حمایت از محرمانگی در عصر حاضر، تاکنون بیش از ۶۰ سند، چندین متن آموزشی، توصیه نامه و رهنمود ارائه داده و کمیته وزرای آن در سال ۱۹۸۰ پس از سال‌ها بحث و بررسی در باب مسائل حقوق خصوصی و فردی، «کنوانسیون حمایت از حقوق افراد در زمینه پردازش خودکار داده‌های شخصی» (۱۷) را مورد تصویب قرار داد که با بیان ۱۰ اصل اساسی، مبین حداقل استانداردهایی است که باید در قوانین داخلی منظور گردند.

هدف این کنوانسیون، حمایت از داده‌ها و حفظ حریم خصوصی افراد و حقوق و آزادی‌های بنیادین ایشان به هنگام پردازش خودکار داده‌های شخصی است (۱۷). بر اساس این سند، داده‌های شخصی، حتی اگر میان اطلاعات مربوط به گروه‌های اجتماعی، مؤسسات و شرکت‌ها باشند، جزئی از این معاهده بوده و باید به طور قانونی و شفاف تهیه، پردازش و برای اهداف مشروع و خاص ذخیره شده و به صورت روزآمد و بدون مغایرت با اهداف معاهده نگهداری شوند. پردازش داده‌های شخصی مربوط به خصوصیات نژادی، عقاید سیاسی یا مذهبی و نیز داده‌های شخصی مربوط به زندگی جنسی، وضعیت بهداشتی و محکومیت‌های کیفری افراد جز در موارد مصرح قانونی ممنوع می‌باشد (۱۷). پیش‌بینی تدابیر امنیتی برای حمایت از داده‌های مزبور با هدف جلوگیری از تخریب اتفاقی یا غیر مجاز آن‌ها از دیگر موارد مندرج در این کنوانسیون است، البته این سند دارای برخی محدودیت‌ها در خصوص داده‌های مربوط به

امنیت و آسایش عمومی، منافع مالی کشور و مبارزه با جرائم می‌باشد و نیز استفاده بی‌ضرر از داده‌ها را در زمینه تحقیقات علمی و آماری مجاز می‌داند (۱۷).

کمیته کارشناسان حفاظت از داده‌ها نیز همزمان با تصویب کنوانسیون فوق به بررسی و تکمیل رهنمودهایی پرداخت که به صورت توصیه نامه‌های غیر الزام‌آور تصویب گردید. در تکمیل این معاهده رهنمودهای ۹۵/۴۶ و ۹۷/۶۶ در باب حمایت از اشخاص در خصوص پردازش داده‌های شخصی و گردش آزاد داده‌های حساس، از جمله داده‌های پزشکی به تصویب رسیده است.

شایان ذکر است قانون حمایت از داده ایتالیا (۱۸)، قانون حمایت از داده بریتانیا (۱۹) و قانون فدرال آمریکا (۲۰) متضمن مباحثی در خصوص حریم خصوصی درمانی است که قواعد مربوط به اعلام رویه مورد عمل در حمایت از حریم خصوصی بیمار، حق دسترسی بیمار به فایل حاوی داده‌های او، حق اصلاح داده‌های نادرست توسط وی، اعلام موارد افشای مجاز داده‌ها به بیمار، وظایف بیمارستان و نهادهای مشابه در جهت آموزش کارکنان در زمینه نحوه به کارگیری رویه‌های فنی و اداری متناسب، منع افشای داده‌های مربوط به سلامت روانی، حق منع بیمارستان از درج نام بیمار در لیست بیماران، موارد استثنایی قانون و نیز نحوه رسیدگی به شکایات را همراه با واکنش کیفری مناسب نسبت به نقض قواعد مزبور پیش‌بینی نموده‌اند.

حایگاه اطلاعات پزشکی در میان داده‌های رایانه‌ای و مخاطرات این حوزه

مقصود از اطلاعات رایانه‌ای که از آن به داده تعبیر می‌شود، کلیه عملیات و برنامه‌های رایانه‌ای و نتایج عملیات مزبور است که با دستورهای مشخصی هدایت شده (۲۱) و شامل ترکیبی از چندین شماره است که اطلاعاتی اعم از متن، تصویر، صوت و فیلم ویدیویی را در زمینه‌های مختلف ارائه می‌دهد. برخی داده‌های مزبور، مربوط به شخص معینی بوده و موجب تمایز وی از سایرین می‌گردد، به داده‌های مزبور داده‌پیام شخصی اطلاق می‌شود. از میان داده‌های مزبور برخی مربوط به جنبه‌های کاملاً فردی زندگی فرد از قبیل مشخصات نژادی، عقاید سیاسی و فلسفی، اطلاعات مربوط به سلامت جسمی و روانی، روابط جنسی، اطلاعات اقتصادی و... می‌باشند که نمایانگر شخصیت و هویت وی بوده و تحت عنوان داده‌های شخصی حساس از آن‌ها یاد می‌شود. با توجه به ارتباط تنگاتنگ داده‌پیام‌های شخصی حساس با حریم

خصوصی افراد خصوصاً در حوزه اطلاعات پزشکی (اعم از جسمی و روحی)، حمایت از داده‌های مزبور از طریق وضع و به کارگیری ضمانت اجراهای متناسب اجتناب‌ناپذیر است.

بر این اساس هرگونه پردازش، جمع‌آوری، انتقال، ارائه و افشای داده‌ها بدون رضایت ذی‌نفع مانند استفاده یا انتقال غیر قانونی آن‌ها با هدف کسب منفعت یا هر قسم سوءاستفاده احتمالی دیگر، عدم تمهید تدابیر فنی و پرسنلی ضروری جهت حفاظت از آن‌ها اعم از کوتاهی در انتصاب افراد موثق یا قصور در انتخاب تدابیر امنیتی برای نگهداری و پردازش داده‌های شخصی حساس، عدم ارائه داده‌های مذکور در موارد معین قانونی یا ارائه آن‌ها با تغییر در شکل اولیه و نیز انتقال غیر قانونی آن‌ها به کشورهای دیگر در زمره موارد تعرض به حریم خصوصی می‌باشند و در جهت حمایت از داده‌های مذکور می‌توان از ضمانت اجرای مناسب از جمله مجازات، جبران خسارت برابر با ضرر وارده و اعاده حیثیت از متضرر، متناسب با نوع جرم و آثار آن بهره جست.

ضوابط حمایت از اطلاعات پزشکی در فضای مجازی

حمایت از داده‌های شخصی حساس مرتبط با بیماران از زمان تحصیل داده‌ها، آغاز و مراحل نگهداری، پردازش و امحای داده‌های مزبور را نیز پوشش می‌دهد (۲۲).

هنگام جمع‌آوری اطلاعات مربوط به بیماری، ذی‌نفع باید از طرق متعارفی نسبت به هدف مؤسسه درمانی از جمع‌آوری اطلاعات، هویت اشخاصی که اطلاعات برای آن‌ها افشا خواهد شد و در نهایت ضمانت اجرای عدم ارائه کامل اطلاعات آگاه شود. گردآوری داده‌های متعلق به بیماران، باید با توسل به روش‌های قانونی صورت گیرد. به واقع مشروعیت ابزار تحصیل داده ناشی از رضایت ذی‌نفع (بیمار) و در برخی موارد استثنایی، حکم صریح قانون است، لذا اصل بر آن است که این اطلاعات از فرد و با اطلاع وی، از سایرین دریافت شود. از این امر تحت عنوان اصل تحصیل قانونی و منصفانه داده‌ها یاد می‌شود (۲۳). علاوه بر این تحصیل داده‌ها برای اهداف قانونی و مشروع، مجاز است و باید منطبق با هدف اولیه و به میزان مورد نیاز برای تحقق آن هدف صورت گیرد. این امر مبین لزوم تحصیل مضیق و مرتبط داده‌هاست.

ذی‌نفع در تصمیم‌گیری و ابراز نظر صریح خود مبنی بر رضایت یا عدم رضایت نسبت به گردآوری داده‌های مزبور، مختار بوده و این حق انتخاب باید به موقع و به درستی از سوی

مؤسسه درمانی به بیمار اعلام شود. به دیگر سخن باید پیش از هرگونه گردآوری داده، حق انتخاب بیمار به اطلاع وی برسد. آگاهی دقیق بیمار از موضوع به همراه اختیار وی در اعلام یا عدم اعلام رضایت پیش از عملیات پزشکی به وی اعلام می‌شود و موارد استثنایی خلاف آن، محدود به حکم قانون یا دستور قاضی دادگاه است. در موارد اضطراری نظیر اقدامات فوری درمانی یا در مقام تحقیق، تألیف یا تحلیل آماری و آموزشی، همچنین موارد مرتبط با امور امنیتی و نیز حفظ مصالح حیاتی جامعه اصولاً استثنائاتی بر این اصل وارد می‌شود.

پس از گردآوری و دریافت اطلاعات، نوبت به نگهداری آن‌ها می‌رسد. نگهداری داده‌های بیماران بر عهده پرسنل درمانی به عنوان پردازشگر داده بوده و مسؤول پردازش مکلف است برای جلوگیری از دسترسی یا پردازش غیر مجاز داده‌هایی که تحصیل نموده یا در اختیار دارد، تدابیر امنیتی لازم را به کار بندد و عدم به کارگیری چنین تدابیری موجب مسؤولیت اوست (۲۴).

شفاف‌سازی فعالیت‌های فضای مجازی و عرضه اطلاعات مربوط به آن‌ها تا حدودی منجر به کاهش تخلفات می‌شود، لذا ضمن رعایت محرمانگی داده‌ها، اعمال شفافیت نیز ضروری است و مؤسسات گردآورنده یا پردازش‌کننده داده باید در صورت تقاضای ذی‌نفع، امکان دسترسی وی به محتوا، هدف گردآوری و سایر اطلاعات مربوط را فراهم آورده و با اتخاذ تدابیر مناسب به نحو شفافی آن‌ها را در دسترس کاربر قرار دهند.

یکی از آثار اقدام شفاف، سهولت دسترسی ذی‌نفع به داده‌های خود است. بر این اساس، مؤسسه درمانی مکلف است در صورت درخواست ذی‌نفع امکان دستیابی او به اطلاعات مربوط به نوع، ماهیت و روش گردآوری داده‌ها و کیفیت آن‌ها و همچنین کپی‌برداری از داده‌ها و اطلاع از هویت مؤسسات و اشخاصی که داده‌ها در اختیار ایشان قرار گرفته را با هزینه‌ای معقول فراهم آورد (۲۵). وجود خطر برای سلامتی، حیات یا حریم خصوصی سایرین، فقدان توجیه منطقی درخواست دسترسی با توجه به اوضاع و احوال حاکم بر موضوع، وجود منع قانونی و قضایی یا امنیتی دسترسی به داده‌های مورد بحث یا ایجاد اخلال در تعقیب و کشف یک جنایت، از جمله استثنائات وارد بر این اصل است.

علاوه بر لزوم رعایت موارد فوق، یکی از خطرات بالقوه علیه حریم خصوصی اشخاص، عدم صحت داده‌هاست که ریشه در اشتباه یا قصور در مرحله گردآوری، ذخیره یا پردازش داده‌ها و

یا کامل‌نبودن داده‌های گردآوری‌شده دارد، لذا توجه به کیفیت و محتوای داده‌ها ضروری بوده و در صورت اختلاف بیمار و سازمان درمانی نسبت به صحت داده‌ها، فرد می‌تواند تصحیح اطلاعات ناصحیح خود را از سازمان، تقاضا کرده و سازمان نیز در صورت مخالفت باید دلایل انکار یا امتناع خود را حداکثر تا ۴۵ روز از زمان دریافت درخواست تشریح کند (۲۳). در این مورد، مسؤولیت سازمان درمانی، نافی مسؤولیت دارندگان مؤسسات خدمات اینترنتی و نیز شخصی که به صورت غیر مجاز اقدام به پردازش یا انتشار داده‌ها نموده، نخواهد بود.

به هر رو داده‌ها به منظور خاصی، جمع‌آوری و نگهداری می‌شوند و به کارگیری آن‌ها برای تحقق هدف مزبور انجام می‌گیرد. وفق بند «ب» ماده ۲ دستورالعمل اروپایی حمایت از داده شخصی، هر نوع عملیات نسبت به داده‌های شخصی نظیر جمع‌آوری، ثبت، سازماندهی، ذخیره، تطبیق، تغییر، بازیافت، مشاهده، استفاده، ارسال، تنظیم، ترکیب و یا به گردش‌انداختن داده‌های شخصی از طریق وسایل خودکار یا بدون آن انجام می‌پذیرد. این امر باید به نحوی صورت گیرد که تشخیص هویت ذی‌نفع آن‌ها، برای مدتی بیش از زمان لازم برای جمع‌آوری یا پردازش آن‌ها امکان‌پذیر نباشد.

برای تضمین حفظ داده‌ها در این مرحله، اصل پردازش مرتبط داده‌ها و ممنوعیت افشا صرفاً به پردازشگر اجازه می‌دهد پردازش داده‌ها بر اساس توافق صورت‌گرفته با ذی‌نفع یا حکم قانونگذار انجام شود و در موارد شک، اصل بر عدم امکان پردازش قرار گیرد، لذا گردآوری و پردازش، محدود به یک هدف است و تفسیر موسع آن به موارد مشابه و افشای داده‌ها نزد اشخاص ثالث جز در موارد قانونی که برای جلوگیری از وقوع یک جرم مهم یا برای صیانت از امنیت و سلامت عمومی و نیز تحقیقات پزشکی ضروری باشد، تجاوز به حریم خصوصی اطلاعاتی محسوب می‌شود، البته اگر هدف ثانویه از متفرعات منطقی و غیر قابل اجتناب هدف اولیه بوده یا ذی‌نفع قبلا انتظار چنین پردازشی را داشته، پردازش مزبور نیز مجاز تلقی می‌شود (۲۶).

پس از استفاده از داده‌ها نوبت به امحای آن‌ها می‌رسد. اتخاذ تدابیر امنیتی از جانب دارنده داده‌ها، مستلزم آن است که به محض برطرف‌شدن نیاز وی به داده‌ها نسبت به از بین‌بردن آن‌ها اقدام نماید. این وظیفه به ویژه بر عهده مؤسسات خدمات اینترنتی است که داده‌های مربوط به کاربران همه روزه در حافظه رایانه‌های آن‌ها ذخیره می‌شود.

با توجه به آنکه امکان انتقال فرامرزی داده‌ها منجر به کاهش اعتماد به دولت و در نتیجه تحریم اطلاعاتی کشور می‌گردد، باید اصل را بر عدم امکان انتقال داده‌ها نهاد. اصل ممنوعیت انتقال داده‌ها، دال بر آن است که انتقال بعدی داده‌ها به ثالث اعم از آنکه به صورت درون مرزی یا فرامرزی باشد، ممنوع است. رعایت اصل ممنوعیت انتقال فرامرزی داده خصوصاً در کشورهای فاقد سطح کافی حمایت از حریم خصوصی ضروری است (۲۶). شایان ذکر است در صورت لزوم انتقال داده‌های مربوط به امنیت ملی، امور بهداشتی افراد جامعه و جرائم مهم نیازی به کسب رضایت ذی‌نفع نمی‌باشد (۲۳).

در نهایت آنکه بر اساس اصل مسؤولیت؛ گردآورنده و پردازشگر داده‌های پزشکی اعم از تیم پزشکی و کارکنان محل درمان در صورت تحقق شرایط عمومی و اختصاصی مندرج در قانون، نسبت به تخلف از احکام قانونی و تجاوز به حریم خصوصی شهروندان، مسؤولیت داشته و شهروندان در هرحال حق دادخواهی و بهره‌مندی از روش‌های جبران خسارت را خواهند داشت (۳۲- ۲۷).

آسیب‌شناسی نظام حقوقی ایران

هرچند از واژه حریم خصوصی در قانون اساسی جمهوری اسلامی ایران ذکری به میان نیامده، لکن در حقوق ایران از بدو قانونگذاری، احترام به مصادیق این حق مورد توجه بوده و در اصول متعدد قانون مزبور، مصادیقی از حریم خصوصی مانند حرمت مسکن (اصل ۲۲)، منع تفتیش عقاید (اصل ۲۳) و حریم خصوصی مکاتبات و مخابرات (اصل ۲۵) مورد حکم قرار گرفته است. از میان قوانین عادی نیز برخی مواد قانون مجازات اسلامی، ماده واحده احترام به آزادی‌های مشروع و حفظ حقوق شهروندی مصوب ۱۳۸۳، آیین دادرسی کیفری مصوب ۱۳۹۲، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و قانون تجارت الکترونیکی به حمایت از مصادیقی از حریم خصوصی پرداخته‌اند.

ضمانت اجرای کیفری عدم حفظ حریم خصوصی بیماران در ماده (۶۴۸) وضع گردیده، ماده مزبور مقرر می‌دارد: «اطبا و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند هرگاه در غیر از 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.» شاید بتوان با توجه به اطلاق واژه «اسرار» و تفسیر تحت‌اللفظی آن، افشای اطلاعات رایانه‌ای را نیز مشمول مجازات این ماده قانونی دانست، لکن با توجه به زمان تصویب این ماده (۱۳۷۵ ش.) و لزوم تفسیر منطقی قوانین و مراجعه به مشروح مذاکرات مجلس شورای اسلامی در زمان تصویب آن، به نظر می‌رسد مقنن در زمان نگارش قانون، توجهی به سیستم‌های رایانه‌ای و پردازش خودکار داده‌ها نداشته است.

در فضای مجازی دو قانون تجارت الکترونیکی در سال ۱۳۸۲ و قانون جرائم رایانه‌ای در سال ۱۳۸۸ به تعیین برخی ضوابط جرم‌انگاری اعمال ناقض حریم خصوصی رایانه‌ای پرداخت. نقض امنیت داده‌ها در فضای سایبر در قالب تعرض به تمامیت و صحت داده‌ها و نقض محرمانگی آن‌ها قابل تصور است و از جمله مصادیق آن می‌توان به نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌ها، دسترسی غیر مجاز به داده‌های رایانه‌ای یا مخابراتی، شنود غیر مجاز محتوای در حال انتقال، مختل یا غیر قابل پردازش‌کردن داده‌های متعلق به غیر، سابوتاژ سیستم‌های رایانه‌ای یا مخابراتی، سرقت یا جعل داده‌های متعلق به دیگری، هتک حیثیت از طریق انتشاریافتن صوت و فیلم تحریف‌شده دیگری، فروش یا انتشار یا در دسترس قراردادن گذرواژه، نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی و... به عنوان مصادیق جرم‌انگاری آن اشاره نمود (۳۳).

ماده ۵۸ فصل سوم قانون تجارت الکترونیکی نیز با عنوان حمایت از داده‌پیام‌های شخصی، شرایط قانونی ذخیره، پردازش و توزیع داده‌پیام‌های شخصی را بیان نموده، اما مصادیق مزبور، تنها ناظر به داده‌های شخصی حساس می‌باشد که نشان از توجه مقنن به اهمیت حفظ این داده‌ها دارد، هرچند مناسب‌تر بود که از اصطلاح «حساس» نیز پس از عبارت «داده‌پیام‌های شخصی» استفاده می‌نمود، لذا با استناد به این قانون می‌توان ذخیره، پردازش و توزیع داده‌پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص را بدون رضایت صریح ایشان غیر قانونی دانست.

قانون مزبور در صورت فرض رضایت شخص موضوع داده‌پیام (بیمار)، امکان ذخیره، پردازش و توزیع داده‌های مزبور را منوط به آن دانسته که محتوای داده‌پیام وفق قوانین مصوب مجلس شورای اسلامی گردآوری گردد. بدین‌معنا که داده‌های مزبور خلاف قانون نبوده و به عبارت بهتر

با نظم عمومی، اخلاق حسنه و قوانین شرعی موافق باشد؛ هدف ذخیره، پردازش و توزیع داده‌های مزبور باید به روشنی تشریح شود؛ داده‌پیام باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع آن، شرح داده شده، جمع‌آوری گردد و تنها برای اهداف تعیین‌شده مورد استفاده قرار گیرد؛ داده‌پیام باید صحیح و روزآمد باشد؛ شخص موضوع داده‌پیام باید به پرونده‌های رایانه‌ای حاوی آن دسترسی داشته و بتواند داده‌پیام‌های ناقص و نادرست را اصلاح یا محو کند؛ ضروری است شخص موضوع داده‌پیام قادر باشد در هر زمان با رعایت ضوابط مربوط، درخواست محو کامل داده‌پیام‌های شخصی مربوط به پرونده رایانه‌ای خود را بنماید و در نهایت ذخیره، پردازش یا توزیع داده‌پیام‌های مربوط به سوابق پزشکی و بهداشتی تابع آیین‌نامه‌ای است که در ماده ۷۹ این قانون پیش‌بینی شده است.

به موجب این ماده ذخیره، پردازش و توزیع داده‌پیام‌های مربوط به سوابق بهداشتی و پزشکی، تابع آیین‌نامه‌ای است که برابر ضوابط مندرج در این قانون باید با پیشنهاد وزارت بهداشت، درمان و آموزش پزشکی به تصویب هیأت وزیران برسد، لکن علی‌رغم تفویض اختیار هیأت مزبور به موجب بند ۵ مصوبه مورخ ۱۳۸۵/۹/۱۲ هیات وزیران به کارگروهی متشکل از وزرای صنعت، معدن و تجارت (به عنوان رییس)، ارتباطات و فناوری اطلاعات، راه و شهرسازی، صنایع و معادن، امور اقتصادی و دارایی و رییس کل بانک مرکزی جمهوری اسلامی ایران، تاکنون به درستی مراحل چهارگانه تحصیل، نگهداری، پردازش و امحای داده‌ها و اصل مسؤولیت پردازش‌کننده اطلاعات لحاظ نشده‌اند.

توضیح نخست آنکه مفاد این قانون علاوه بر عدم رعایت توالی و ترتیب مراحل تحصیل، پردازش و توزیع داده‌پیام‌های شخصی حساس صرفاً ناظر به برخی اصول حمایت از داده‌های رایانه‌ای، از جمله اصول تحصیل قانونی و منصفانه، تفسیر مضیق و مرتبط، صحت داده‌ها و امحای آنان می‌باشد و در بحث مسؤولیت گردآورنده اطلاعات نیز جز ماده ۷۸ این قانون که صرفاً جبران خسارت را پیش‌بینی نموده، نمی‌توان حکمی بیش از آنچه در قوانین مسؤولیت مدنی و آیین دادرسی کیفری در خصوص نحوه جبران خسارات ناشی از جرم وضع شده، یافت. گفتنی است قوانین اخیرالذکر به دلیل برخی کاستی‌ها حتی در حوزه فضای غیر مجازی (سنتی) نیز قادر به ارائه نتیجه مطلوب نمی‌باشند؛ ثانیاً اصول انتخاب در مرحله اول، امنیت، شفافیت و دسترسی؛ در مرحله دوم، پردازش مرتبط و ممنوعیت افشا؛ در مرحله سوم و منع

انتقال داده‌ها در فراسوی مرزها؛ در مرحله چهارم از دید مقنن مغفول مانده، لذا مواد ۵۸ به بعد قانون مذکور در حمایت از داده‌های حساس پزشکی ناکارآمد هستند؛ ثالثاً با توجه به ارتباط تنگاتنگ حفظ حریم خصوصی افراد با حقوق و آزادی‌های فردی، اخلاق حسنه و نظم عمومی، ضمانت اجرای نقض مقررات این قانون نیز وافی به مقصود نمی‌باشد. ضمانت اجرای مورد نظر در باب چهارم این قانون و آیین‌نامه مربوطه وضع شده و بر اساس احکام مزبور، ماده ۷۱ این قانون به مجازات نقض شرایط مقرر در مواد ۵۸ و ۵۹، ماده ۷۲ به تشدید مجازت ارتکاب این جرم توسط دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسؤول و در نهایت ماده ۷۳ به مجازات بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی اختصاص دارند.

هرچند در قانون جرائم رایانه‌ای به مصادیق متعددی از جرائم رایانه‌ای اشاره شده و دسترسی غیر مجاز به داده‌ها یا سامانه‌های مذکور که به وسیله تدابیر امنیتی حفاظت شده و همچنین شنود غیر مجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های فوق‌الذکر وفق مواد ۱ و ۲ جرم‌انگاری گردیده‌اند، لکن در این قانون نیز صرفاً بارقه‌هایی از اصول حاکم بر حمایت از داده، از جمله اصل رضایت سوژه و عدم امکان انتقال داده‌ها را می‌توان مشاهده نمود.

نتیجه‌گیری

حریم خصوصی محدوده معقولی است که انتظار می‌رود از دسترس دیگران اعم از دولتی و سایر اشخاص حقیقی و حقوقی مصون بماند، ولی پیشرفت عصر ارتباطات آن را با چالش‌های جدی مواجه می‌سازد.

با افزایش موارد سوءاستفاده از اطلاعات رایانه‌ای خصوصاً در حوزه سلامت جسمی و روانی افراد، جامعه جهانی به تبیین اصول و قواعد ناظر بر حمایت از حریم خصوصی پرداخت و اسناد الزام‌آور و نیز توصیه‌نامه‌های مصوب سازمان‌های بین‌المللی و منطقه‌ای، الگوی مناسبی را جهت تنظیم قواعد داخلی دولت‌ها ارائه نمودند. با دقت در اسناد مورد بحث می‌توان لزوم تحصیل قانونی، مضیق و مرتبط و نیز توجه به حق انتخاب ذی‌نفع را بر مرحله گردآوری اطلاعات بیمار، رعایت امنیت، شفافیت و دسترسی به داده‌ها و دقت در صحت آن‌ها را بر مرحله نگهداری اطلاعات، ضرورت پردازش مرتبط و ممنوعیت افشای داده‌ها را بر مرحله به کارگیری اطلاعات و در نهایت لزوم امحا و ممنوعیت انتقال فرامرزی داده‌ها را بر مرحله پایانی حاکم دانست. رعایت

اصول رضایت و مسؤولیت گردآورنده و پردازشگر داده‌های پزشکی نیز در کلیه مراحل چهارگانه فوق ضروری است.

قانون اساسی جمهوری اسلامی ایران بر لزوم حفظ حریم خصوصی تأکید نموده، لکن تنها ماده ۶۴۸ قانون مجازات اسلامی، صاحبان حرف، از جمله افراد مرتبط با امور پزشکی را مکلف به حفظ اسرار حرفه‌ای خود نموده است. قانون تجارت الکترونیکی و قانون جرائم رایانه‌ای به طور کلی به حفاظت از اطلاعات مزبور اشاره نموده و قانون تجارت الکترونیکی، از میان اصول صدرالذکر بدون رعایت توالی و ترتیب فوق، صرفاً به اصول رضایت سوژه، تحصیل قانونی و مضیق داده‌ها، اصل صحت داده‌ها و امحای آن‌ها اشاره نموده است. در حوزه تضمین رعایت اصول فوق نیز ضمانت اجرای کیفری مندرج در مواد ۷۱ تا ۷۳ قانون تجارت الکترونیکی و مواد ۱ و ۲ قانون جرائم رایانه‌ای در باب جرم‌انگاری دسترسی و شنود اطلاعات شخصی وافی به مقصود نمی‌باشد.

لذا با عنایت به عدم ذکر کلیه ضوابط ناظر بر حمایت از داده، خصوصاً عدم تبیین دقیق اصل مسؤولیت پردازش‌کننده داده، نمی‌توان به ضمانت اجرایی مناسب در این حوزه دست یافت و به جهت ارتباط حفظ داده‌های مزبور و رعایت حقوق فردی، ضروری است تدوین قانونی جامع در راستای حمایت از این حریم در دستور کار قرار گیرد. بدیهی است این قانون باید ضمن شمول بر تمامی فعالیت‌های این حوزه، قادر به جلوگیری از تعرض به آن در عرصه بین‌المللی نیز باشد.

References

1. Wild SE. Webster's New World Dictionary, Law dictionary. New York: Wiley Publishing; 2006. p.207.

2. Moien M. Persian dictionary. Tehran: Amir Kabir Publication; 1984. Vol.2 p.22. [Persian]

3. Ansari B. Privacy law. Tehran: Samt Publication; 1394. p.11. [Persian]

4. Smartt U. Media & Entertainment Law. London: Routledge; 2014. p.35.

5. Sawada NO, Correia FA, Mendes IA, Coleta JA. Personal and territorial space of the patients: A nursing ethics question. Med Law 1996; 4(15): 267-270.

6. A declaration on the promotion of patients' rights in Europe. WHO. Regional Office for Europe. Kluwer Law International. The Hague; 1994.

7. Burgoon J. Privacy and communication. Communication Yearbook. Mishigan: International Communication Association; 1982. p.249.

8. Barkay A, Tabak N. Elderly residents' participation and autonomy within a geriatric ward in a public institution. Int J Nurs Pract 2002; 8(4): 198-209.

9. Schwartz B. The social psychology of privacy. AJS 1968; 73(6): 741-52.

10. Collette J. Role demands, privacy and psychological well-being. Int J Soc Psychiatry 1984; 30(3): 222-230.

11. Gardner R, Lundsgaarde H. Evaluating of user acceptance of a clinical expert systems. J Am Med Inform Assoc 1994; 1(6): 428-438.

12. Mohseni F. Privacy. Tehran: Imamsadegh Publication; 1390. p.33. [Persian]

13. Fathi Y, Shahmoradi KH. The Scope and the Territory of Privacy in Virtual Space. The Judiciary Law Journal 2017; 81(99): 229-252. [Persian]

14. Moehr JR. Informatics in the service of health. a look to the future. Methods INF Med 1998; 37(2): 165-170.

15. Goodwin G, Guy S. Basic documents on Human Rights. Edited by Ian B. 5th ed. New York: Oxford University Press; 2006. p.225.

16. Cyber Crime... and Punishment? 2000. Available at: http://www.mcconnellinternational.com.

17. Convention for the protection of individuals with regard to automatic processing of personal data. Strasbourg. 1981. Available at: htpp://www.conventions.coe.int/treaty/.

18. Available at: http://www.Elj.warwick.ac.uk/jilt/dp/material/1675_eng.htm.

19. Available at: http://www.hmso.gov.uk/acts/acts1998/80029_a.htm#1.

20. Health insurance portability and accountability act 1996.

21. Lewis W. Data warehousing and ecommerce. New Jersey: Princeton Hall; 2001. p.5.

22. An outline study of the implementation of data protection principles. Pccy. Cdpc. CE. 1997. Available at: http://www.Coe.int/treaty.

23. Information privacy principles common wealth. 1988. Available at: http://www.latvobe.edu.au/records/downloads/information-privacy-principles-cwealth.pdf.

24. Available at: http://www.austlii.edu.au/itlaw/articles/IPPs.html.

25. Available at: http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.html.

26. Available at: http://www.privacy.gov.au/publications/npps01.

27. Malakotti R, Savarayi P. Tort in the cyberspace. Private Law Research 1395; 4(15): 129-149. [Persian]

28. Berman J, Bruening P. Is Privacy Still Possible in the Twenty-first Century. Social Research 2001; 68(1): 306-318.

29. Simmons R. Why 2007 is not like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence. Journal of Criminal Law and Criminology 2007; 97(2): 531-568.

30. McGovern TM. Is Privacy Now Possible? Social Research 2002; 68(1): 412-422.

31. Weiming SH. Applications of agent-based systems in intelligent manufacturing. Advanced Engineering Informatics 2006; 7(20): 33-51.

32. Pollman E. A Corporate Right to Privacy: A Critical Analysis. Minnesota Law Review 2014; 99(1): 2014-2027.

33. Abbasi A, Akbari A. Cyber crime. Tehran: Majd; 1394. p.35-36. [Persian]