حفظ حریم خصوصی بیماران، پیش‌نیاز توسعه‌ی سلامت الکترونیک

مهدی فقیهی[1]

غلامرضا معمارزاده طهران[2]

حسین رفوگر آستانه[3]

چکیده

رشد، گسترش و افزایش سرعت و همه‌گیری شبکه‌های مقیاس وسیع در سال‌های اخیر موجب تحولی عظیم در جنبه‌های مختلف زندگی بشری شده است و تأثیر این فناوری بر علوم، فنون و کسب‌وکار، موجب ظهور حیطه‌های جدیدی همچون دولت الکترونیک، آموزش الکترونیک و سلامت الکترونیک شده است. سلامت الکترونیک با ایجاد پرونده‌ی الکترونیک سلامت، اطلاعات بهداشت و درمان را تجمیع و یکپارچه می‌کند که تجمیع این اطلاعات برای ذی‌نفعان گوناگون، مشروط بر حفظ حریم خصوصی بیماران و رعایت محرمانگی، بسیار سودمند است. در کشورهای پیشرفته، دولت‌ها با اتخاذ سیاست‌ها و انجام اقدامات مناسب، ملزومات توسعه سلامت الکترونیکی را فراهم آورده‌اند. در این مقاله سعی شده است که با مروری بر چگونگی تأمین حفظ حریم خصوصی در کشورهای منتخب جهان و بررسی وضعیت فعلی کشور به راهکاری برای تأمین حفظ حریم خصوصی داده‌های الکترونیک حوزه سلامت کشور دست یافت.

واژگان کلیدی

سلامت الکترونیک؛ حریم خصوصی؛ حفاظت از داده؛ ایران؛ پرونده الکترونیکی سلامت

---

۱. دانشجوی دکتری مدیریت دانشکده‌ی مدیریت و اقتصاد دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، مدیر گروه مطالعات ارتباطات و فناوری اطلاعات مرکز پژوهش‌های مجلس شورای اسلامی(نویسنده مسؤول).

۲. استادیار دانشکده‌ی مدیریت و اقتصاد دانشگاه آزاد، واحد علوم و تحقیقات

۳. کارشناس ارشد مدیریت صنعتی دانشگاه آزاد اسلامی، واحد تهران مرکزی، پژوهشگر گروه مطالعات ارتباطات و فناوری اطلاعات مرکز پژوهش‌های مجلس شورای اسلامی

حفظ حریم خصوصی بیماران، پیش‌نیاز توسعه‌ی سلامت الکترونیک

موضوع حفظ حریم خصوصی بیمار به‌عنوان یکی از اصول پذیرفته شده در بین بیماران و ارائه‌دهندگان خدمات سلامت و پزشکی بوده است و به همین دلیل بیماران مسایل و موضوعاتی را که حتی از نزدیک‌ترین کسان خود مخفی می‌کنند برای پزشکان بازگو می‌کنند. (پارسا، ۱۳۸۸هـ‌ش.، ص۱۲) فناوری‌های نوین با وجود منافع بسیاری که برای بشر به ارمغان می‌آورد، مسایلی را نیز متوجه بشر می‌سازد که در صورت عدم چاره‌اندیشی، این مسایل به تهدید بدل می‌شوند. با پیشرفت فناوری و جایگزینی ابررایانه‌ها به رایانه‌های شخصی کوچک، داده‌های متمرکز به داده‌های غیرمتمرکز و پراکنده تبدیل شدند و افراد برای ذخیره‌سازی و پردازش اطلاعات به مراکز ابررایانه‌ها مراجعه نمی‌کردند و در محل کار یا منازل خود در مقیاسی محدودتر ولی تقریباً با همان میزان کارایی امور اطلاعاتی خود را سامان می‌بخشیدند. بدیهی است این وضعیت منجر به پراکنده شدن بخشی از اطلاعات خصوصی افراد شده است اما آنچه خود این تمرکززدایی را با تحول اساسی مواجه ساخته و به واقع وارد عرصه‌ی جدیدی کرده است. (جلالی، ۱۳۸۵هـ‌ش.، ص۱۶) رشد، گسترش و افزایش سرعت و همه‌گیری شبکه‌های مقیاس وسیع مانند اینترنت است و تشدید رقابت و تغییرات، ظهور نیازهای جدیدی همچون نیاز به ارتباطات روزافزون، تحرک‌پذیری و انعطاف و غیره را به‌وجود آورده است. تلاش در برآورده کردن نیازهای جدید منجر به بازگشت و بلوغ مدل قدیمی رایانش شبکه‌ای در قالب یک مدل جدید عرضه‌ی خدمات فناوری اطلاعات، شده است. تقریباً از بدو اختراع رایانه‌ها دو راه برای استفاده از رایانش مطرح بود. یکی استفاده از توان رایانه‌ای که از آن به‌طور مستقیم استفاده می‌شد و دیگری رایانش با کمک شبکه بود. رایانش ابری[1] به‌معنای ارائه‌ی خدمات رایانشی (ذخیره‌سازی،

ایجاد نرم‌افزار، استفاده از نرم‌افزارها) از طریق اینترنت یا ابر است. (هزاوه، ۱۳۸۸هـ‌ش.، ص۱۷)

در تعریف بالا در عبارت «خدمات رایانشی»، «خدمات» نقش مهمی دارد. استفاده از این کلمه ریشه در نگاه خدمت‌گرا دارد. نگاه خدمت‌گرا نقش مهمی در این حیطه ایفا می‌کند. در نگاه سنتی قبلی، رایانش به‌عنوان یک محصول درنظر گرفته می‌شد؛ بدین معنی که با خرید و تملک نرم‌افزار و سخت‌افزار توسط اشخاص حقیقی و حقوقی و با کمک و مشاوره کادر فناوری اطلاعات، اشخاص قادر هستند از امکانات رایانشی (به‌طور نمونه نرم‌افزارهای پردازش اطلاعات سلامت) استفاده کنند؛ در صورتی که شرکتی تنها بهای استفاده از خدمت رایانشی مورد نیازش را بپردازد با اجاره خدمات رایانشی شرکت ثالث، هزینه‌ی بسیار کمتری پرداخت خواهد کرد. (کشاورز، ۱۳۸۹هـ‌ش.، ص۲۲) امروزه تقریباً در هر کشوری که استفاده از خدمات رایانشی مورد نیاز باشد شبکه‌های وسیع مانند اینترنت در همه‌ی زمان‌ها و مکان‌ها با سرعت بسیار بالا در دسترس هستند و هزینه‌ی اندکی نیز بابت استفاده از آن پرداخت می‌شود. با افزایش سرعت نقل و انتقال داده در شبکه جهانی وب، مدت‌زمانی که صرف رفت و برگشت داده به مرکزی که رایانش در آنجا انجام می‌شود آنقدر ناچیز است که انتقال داده دیگر حس نمی شود. همچنین هزینه انتقال داده و ترافیک در بیشتر کشورهای پیشرفته روندی کاهشی دارد و در محاسبات مالی، رقم ناچیزی درنظر گرفته می‌شود. (رجبی، ۱۳۹۰هـ‌ش.، ص۵) با وجود چنین پیشرفت‌ها و راهکارهای جدید، استفاده از فناوری اطلاعات در سلامت و مراقبت‌های بهداشتی در بسیاری از کشورها تبدیل به ضرورت مهمی شده است. الکترونیکی نمودن پرونده‌ی سلامت، حسابداری و صدور صورت‌حساب‌های درمانی به‌صورت الکترونیکی، از مصداق‌های کاربرد

فناوری اطلاعات و ارتباطات در سلامت با ابزار شبکه‌های رایانه‌ای است. سیستم‌های الکترونیکی سلامت به‌ویژه پرونده‌ی سلامت الکترونیکی علاوه بر مدیریت بهتر سلامت شخصی، موجب کاهش هزینه‌ها در مراقبت‌های بهداشتی با اجتناب از تشخیص‌های دوگانه و یا تجویز داروی تکراری می‌شود. از الزامات سیستم‌های سلامت الکترونیک، امنیت و حفظ حریم خصوصی است. بدیهی است که تجمیع سیستم‌های سلامت الکترونیکی فرایند بسیار حساسی است زیرا افشای اطلاعات بیماران صدمات زیادی به بیمار وارد می‌کند و تبعات اجتماعی جبران‌ناپذیری دارد. (پوراسماعیل، ۱۳۸۷هـ‌ش.، ص۷) به‌عنوان مثال بانک‌ها با دسترسی به این اطلاعات می‌توانند با درخواست وام برخی از افراد مخالفت کنند و یا دسترسی کارفرما به اطلاعات شخصی سلامت کارمند می‌تواند منجر به از دست دادن کار کارمند شود. حال این سؤال مطرح می‌شود که چگونه می‌توان بر چالش حفظ حریم خصوصی داده‌های سلامت کشور در فضای مجازی فایق آمد؟ با توجه به اهمیت حفظ حریم خصوصی داده‌های سلامت افراد در این مقاله سعی کرده‌ایم با مروری بر تجربیات برخی کشورها و همچنین شناخت وضعیت فعلی کشور به راهکارهایی برای حفظ حریم خصوصی داده‌های سلامت الکترونیک برای توسعه‌ی بیشتر استفاده از منافع سلامت الکترونیک دست بیابیم.

روش بررسی

با توجه به این‌که در این مقاله پژوهشگر باید ادبیات و سوابق مسأله و موضوع تحقیق را مطالعه کند، روش، مطالعه‌ی کتابخانه‌ای است که از طریق بررسی اسناد و مدارک مربوط و مطالعه‌ی قوانین انجام شده است.

حریم خصوصی[۲] و حمایت از داده‌ها[۳]

تعریف حریم خصوصی بستگی کامل به فرهنگ و زمینه‌های اجتماعی و محیطی دارد. در بسیاری از کشورها، این مفهوم با مقوله‌ی حفظ اطلاعات که حریم خصوصی را در معنای مدیریت اطلاعات شخصی تفسیر می‌کند پیوند خورده و در هم ادغام شده است. در عین حال محافظت از حریم خصوصی معمولاً به‌عنوان ابزاری برای ترسیم محدوده خطوطی که جامعه می‌تواند در امور افراد دخالت کند تلقی می‌شود. نبود یک تعریف خاص، نشان از کم‌اهمیتی این مفهوم نیست؛ به یک معنا، تمامی موارد حقوق بشر، جنبه‌ها و ابعادی از حق حریم خصوصی هستند. در دهه‌ی ۱۸۹۰ میلادی، دوتن از قضات دادگاه عالی ایالات متحده‌ی آمریکا به‌نام‌های ساموئل وارن و لوئیس براندیس در مقاله‌ای با عنوان «حق حریم خصوصی»، برای اولین بار این مسأله را به‌عنوان یک بحث جدی و صریح حقوقی مطرح و حریم خصوصی را حق افراد برای تنها بودن تعریف کردند. (فولادی، ۱۳۸۶هـ‌ش.، ص۲۵)

به گمان ایشان، حریم خصوصی از جمله‌ی ارجمندترین حقوق در یک دموکراسی است و حمایت از آن باید در قانون اساسی بازتاب یابد. رابرت الیس اسمیت، سردبیر مجله‌ی «حریم خصوصی»، آن را چنین تعریف کرده است: تمایل هر یک از ما برای فضای فیزیکی که می‌توانیم از مداخله، مزاحمت، اضطراب و آشفتگی یا پاسخ‌گویی رها باشیم و برای کنترل زمان و جلوگیری از افشای اطلاعات شخصی درباره‌ی خود تلاش کنیم. ادوارد بلوشتاین، رییس پیشین دانشگاه نیوجرسی، حریم خصوصی را علاقه به شخصیت انسانی می‌داند. به اعتقاد او حریم خصوصی از شخصیت محترم شمرده شده، استقلال فردی، منزلت و استحکام شخصیت، حمایت می‌کند. براساس یک تعریف دیگر، حریم خصوصی،

حق افراد برای برخورداری از حمایت شدن در برابر مداخله‌ی بی‌اجازه دیگران در امور و زندگی خود و خانواده‌شان است؛ خواه این عمل با ابراز مستقیم فیزیکی صورت پذیرد یا به‌وسیله‌ی نشر اطلاعات. (پورناجی، ۱۳۸۷هـ‌ش.، ص۲) اشتراک اغلب تعاریف حریم خصوصی، رازداری است. این عنصر مستقیماً بر آنچه مورد تأکید این نوشتار است یعنی حریم اطلاعات خصوصی، اشاره دارد. به‌عبارت دیگر، آنچه افراد در این‌جا دنبال می‌کنند این است که بر اطلاعات معرفشان کنترل و نظارت داشته باشند که به این ترتیب، تنها بحث افشای آن‌ها مطرح نیست و استفاده‌های آتی یا مکرر را نیز دربر می‌گیرد.

بر این اساس، شایان ذکر است این عنصر تا حدی در قلمرو حریم خصوصی جدی تلقی می‌شود که عده‌ای کل این قلمرو را در حریم اطلاعات خصوصی خلاصه کرده‌اند و حتی در بعضی کشورها، برای حمایت از حریم خصوصی افراد، قوانینی تحت عنوان حمایت از داده‌ها به تصویب رسیده است؛ لذا با توجه به این‌که اولاً اسنادی قانونی تحت عنوان حمایت از داده‌ها برای حمایت از حریم خصوصی افراد وجود دارد.

حمایت از داده‌ها ماهیتی فنی و کاربردی دارد و با حریم خصوصی که یک مفهوم حقوق بشری است تفاوت دارد اما این نکته را هم نمی‌توان انکار کرد که مباحث این دو حوزه در برخی ابعاد، تلاقی‌هایی با یکدیگر دارند. بعضی از ابعاد حریم خصوصی هیچ ارتباط نزدیکی با سامان‌دهی داده‌های شخصی در سیستم‌های اطلاعات ندارند، مانند ورود غیرمجاز به منزل، اختیار ورود و تفتیش و نیز لطمه به اعتبار شخصی در رسانه‌ها. همچنین ابعادی از حمایت داده‌ها هستند که هیچ‌گونه ارتباط نزدیکی با حریم خصوصی ندارند. برای مثال، استفاده از اطلاعات نادرست یا ناقص برای تصمیم‌گیری راجع به اشخاص، در واقع تحت شمول حمایت از

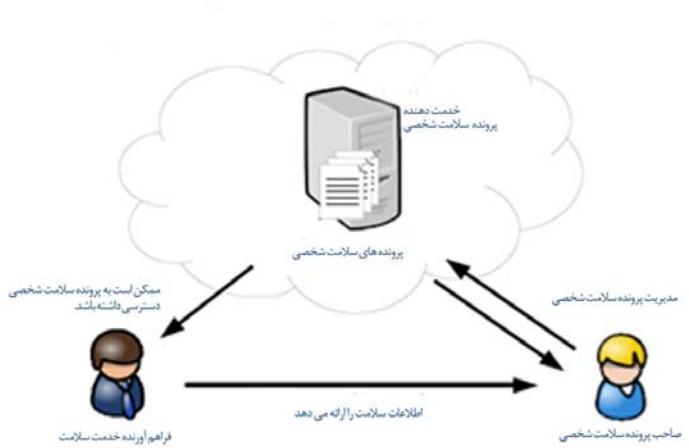
داده‌ها قرار می‌گیرد ولی هیچ دغدغه‌ای را راجع به حریم خصوصی برنمی‌انگیزد. در حقیقت این دو حوزه با یکدیگر همپوشانی دارند و آن حوزه‌ای که تحت شمول هر دو قرار می‌گیرد را می‌توان حریم اطلاعات یا بهتر از آن حریم داده‌ها نامید اما در این‌که چه داده‌هایی «خصوصی» تلقی شود دیدگاه‌های بسیار متنوعی وجود دارد. این تنوع از یک فرد به فرد دیگر، از جامعه‌ای به جامعه‌ی دیگر، از کشوری به کشور دیگر و حتی در دوره‌های زمانی مختلف نیز ملاحظه می‌شود. بعضی اشخاص مایلند دیگران راجع به آن‌ها بیشتر بدانند. در این‌جا سن، شخصیت، خلق‌وخو، دیدگاه‌ها و عقاید تمامی نقش‌آفرینان تعیین کننده است. تنوع‌های اجتماعی و فرهنگی در میان بخش‌های مختلف یک جامعه نیز تأثیرگذار است. (رابینز، ۱۳۸۹هـ‌ش.، ص۱۷۳) تنوع نهادها، فرهنگ‌ها، آداب و رسوم، شیوه و ویژگی‌های سیاسی حکومت در میان جوامع مختلف از عوامل تمایز هستند. تغییراتی که در دیدگاه‌های یک جامعه رخ می‌دهد نیز با عوامل بسیاری ارتباط دارد که از آن میان می‌توان به این موارد اشاره کرد: توسعه‌ی اقتصادی، تغییر استانداردهای آموزشی، مشارکت اجتماعی و فرصت‌های بالفعل برای خودتعیینی. (جلالی، ۱۳۸۵هـ‌ش.، ص۳۰)

با توجه به مباحث فوق یکی از جلوه‌های اصلی حریم خصوصی افراد، اطلاعات خصوصی آن‌هاست. به همین ترتیب یکی از راه‌های مؤثر و نتیجه‌بخش، مصون نگهداشتن حریم خصوصی، دور نگهداشتن اطلاعات خصوصی از هرگونه تعدی و تعرض است. در ادامه به‌طور ویژه به بحث در مورد حفاظت داده‌های شخصی سلامت الکترونیک پرداخته می‌شود.

چالش حفاظت از داده‌های شخصی در سلامت الکترونیک

برای شرح اهمیت و ضرورت مسأله‌ی حفاظت از داده‌های سلامت الکترونیک، گردش جریان اطلاعات سلامت الکترونیک در پرونده‌ی سلامت الکترونیک اشخاص به‌صورت شماتیک در شکل ۱ نشان داده شده است. براساس شکل، زمانی که شخص، قصد استفاده از پرونده‌ی الکترونیکی سلامت خود را دارد با رایانه خدمت دهنده‌ای[۴] که وظیفه خدمت‌دهی پرونده‌ی سلامت الکترونیک[۵] را دارد از طریق کشیدن کارت هوشمند، وارد کردن کد، اثر انگشت و... ارتباط برقرار می‌کند و هویت بیمار از طرف این خدمت دهنده مورد تأیید قرار می‌گیرد؛ رایانه‌ی خدمت دهنده ممکن است متعلق به فراهم کننده داده‌ها نباشد و به شخص ثالثی تعلق داشته باشد. این رایانه کار ذخیره‌سازی و پردازش اطلاعات را انجام دهد. رایانه‌ی خدمت دهنده، دسترسی فراهم آورنده خدمت سلامت[۶] (دکتر، بیمارستان، داروخانه، آزمایشگاه و...) را به اطلاعات پرونده‌ی سلامت الکترونیک فراهم می‌آورد. بر این اساس وظیفه حفاظت از داده‌ها در این مدل برعهده‌ی رایانه‌ی خدمت دهنده شخص ثالث است؛ البته سطح دسترسی فراهم آورندگان خدمات دسترسی به اطلاعات بیمار را خود بیمار می‌تواند تعریف کند؛ به‌عنوان نمونه بیمار می‌تواند دسترسی دکتر خانوادگی خود را به کلیه‌ی اطلاعات پزشکی خود بدهد و دسترسی متصدیان داروخانه را به برخی اطلاعات محدود کند. از مزیت‌های این سیستم متمرکز، دسترسی اطلاعات بدون محدودیت مکانی است؛ به‌طوری یک پزشک به راحتی به داده‌ها و نتایج آزمایش‌های پزشک دیگر بیمار دسترسی پیدا می‌کند و هزینه‌های تشخیص بیماری و تجویز داروها مضاعف نمی‌شود.

شکل ۱. گردش جریان اطلاعات سلامت الکترونیک در پرونده‌ی سلامت الکترونیک



در سیستم‌های سنتی، ارائه دهندگان خدمات بهداشتی، سوابق پزشکی بیماران خود را بر روی کاغذ، ذخیره و در یک محل مشخص مثلاً یک فایل قفل شده، نگهداری می‌کردند؛ نگهداری این اطلاعات در یک محیط کنترل شده موجب اطمینان خاطر از امنیت و محرمانگی اطلاعات و رعایت حریم خصوصی افراد می‌شد. افزایش استفاده از رایانه‌های شخصی، فناوری‌های نوین و بانک‌های اطلاعاتی در موسسأت پزشکی به صورت غیرمتمرکز دسترسی به اطلاعات پزشکی بیماران را از گذشته آسان‌تر کرد لیکن با راه‌اندازی بانک‌های اطلاعاتی متمرکز دسترسی آسان به اطلاعات شخصی بیماران به‌عنوان چالشی جدی در حوزه‌ی سلامت الکترونیک مطرح شد. این چالش با بحث برون‌سپاری فناوری اطلاعات و استفاده از خدمات رایانش ابری اهمیت بیشتری می‌یابد و احتمال نقض حریم خصوصی افراد بیشتر می‌شود زیرا در برون‌سپاری، داده می‌تواند از طریق

اینترنت قابل دسترسی باشد. در مدل ارائه شده، دسترسی به اطلاعات، سلامت بیماران را برای فراهم کنندگان خدمات سلامت اعم از پزشکان و پرستاران، مسؤولان داروخانه‌ها و متصدیان آزمایشگاه‌ها از طریق یک شبکه عمومی مانند اینترنت فراهم می‌آورد که خطرات زیادی را برای نقض حریم خصوصی و امنیت اطلاعات بیماران ایجاد می‌کرد. برای رفع این چالش رعایت ۷ شرط «تأیید، احراز هویت، کنترل دسترسی، دنباله‌ی ممیزی، محرمانه بودن، صداقت، در دسترس بودن و عدم انکار» لازم است. اگر این ۷ شرط رعایت شود، امنیت سیستم تضمین می‌شود؛ امنیت، به این معنی یعنی تضمین یکپارچگی داده‌ها، در دسترس بودن، صحت و محرمانه بودن و حفظ حریم خصوصی، برای دستیابی به اعتماد و پذیرش کاربران از سیستم‌های الکترونیکی سلامت. محرمانگی به این معناست که در اجرای هر سیستم سلامت الکترونیک باید اطمینان داشت که داده‌ها به‌صورت محرمانه و امن نگهداری می‌شوند. در سیستمی که نشان داده است، هر سیستم یا نرم‌افزار آن که با اطلاعات شخصی سروکار دارد امن بوده و صرفاً قابل دسترس برای افراد مجاز باشد. حصول این اطمینان در سیستم‌های سلامت الکترونیکی که از شبکه‌های عمومی نظیر اینترنت استفاده می‌کنند، آسان نیست. با توجه به این‌که حریم خصوصی و امنیت در این شبکه‌ها به خوبی رعایت نشده است، می‌تواند تهدیدی برای توسعه‌ی سلامت الکترونیک به‌شمار رود. تهدید به تمامیت داده‌ها به این معناست که داده‌ها نمی‌توانند توسط افراد غیرمجاز ساخته، تغییر یا حذف شوند. تمامیت، همچنین یکپارچگی داده‌ها که در بخش‌های مختلف پایگاه داده ذخیره شده‌اند را تحت‌الشعاع قرار می‌دهد. اعتبار و سندیت دلالت بر موثق بودن داده‌ها و نیز اصل بودن آن‌ها دارد؛ به طریقی که اطمینان حاصل شود که داده‌ها کپی یا جعلی نیستند. (لوهر، ۲۰۱۰م.، ص۸)

حفاظت از داده‌های سلامت شخصی در کشورهای منتخب

اصل رازداری و حفظ حریم خصوصی بیماران از مهم‌ترین وظایف اخلاق در حیطه‌ی پزشکی است که دارای سابقه‌ی دیرینه در دنیای پزشکی است. (پارسا، ۱۳۸۸هـ‌ش.، ص۲) در بسیاری از کشورها، درز اطلاعات به‌صورت عمدی و سهوی به خارج از سیستم براساس قوانین حریم خصوصی این کشورها، مسؤولان سامانه‌های اطلاعات پزشکی و ارائه دهندگان خدمات فناوری اطلاعات، مشمول مجازات‌های سختی می‌شود. مقررات‌گذاری حریم خصوصی در سلامت الکترونیک از جنبه‌ی فنی تنها شامل اطلاعات پزشکی بیماران نمی‌شود بلکه باید به موارد دیگری همچون حسابداری و صدور صورت‌حساب درمان و دارو را نیز دربر می‌گیرد؛ علاوه بر این برای راه حل‌های مبتنی بر کارت هوشمند، باید اطمینان باید حاصل شود که راه‌های مختلفی برای دسترسی به داده‌های پزشکی وجود داشته باشد. به‌عنوان نمونه ممکن است در صورتی که صاحب کارت در اثر سانحه‌ای بی‌هوش شده باشد و فرد همراه بیمار بستری شده برای تهیه‌ی دارو به داروخانه مراجعه می‌کند، کارت هوشمند قادر به تأیید هویت فرد در حالات ذکر شده نیست. این چالش عمده‌ای است که در حوزه‌ی حریم خصوصی داده‌های سلامت الکترونیک وجود دارد. براساس استاندارد اساس بین‌المللی ایزو (کمیته‌ی فنیو، مصوبات کنسرسیوم سطح ۷ سلامت)، استانداردهای مربوط به زیرساخت‌های سلامت الکترونیک را تعریف کرده‌اند که شامل مشخصاتی برای جنبه‌های امنیتی و محرمانگی اطلاعات است. تمرکز اصلی بر قابلیت کاربری متقابل اطلاعات و تعریف قالب‌های مبادله‌ی اسناد و نام‌گذاری اشیای پزشکی است (می یری، ۲۰۰۹م.، ص ۲۳). فقدان زیرساخت‌های حقوقی سلامت الکترونیک به‌ویژه قانون حفاظت از

داده‌ها، یکی از موانع توسعه‌ی دولت الکترونیک است. در این راستا کشورهای مختلف دست به اقداماتی زده‌اند که در ادامه به برخی از آنها اشاره می‌شود.

الف) ایالات متحده‌ی آمریکا

در حوزه‌ی سلامت الکترونیک قوانین متعددی در ایالات متحده‌ی آمریکا به تصویب رسیده است. یکی از این قوانین، قانون پاسخ‌گویی و قابلیت انتقال بیمه‌های بهداشتی است که در سال ۱۹۹۶م. توسط کنگره‌ی آمریکا به تصویب رسید. موضوع اول قانون پاسخ‌گویی و قابلیت پوشش بیمه‌ی سلامت کارگران و خانواده‌های آنان، هنگامی که کارگران شغلشان را از دست می‌دهند و یا تغییر شغل می‌دهند است و موضوع دوم قانون، تعیین و الزام استانداردهای ملی برای تراکنش‌های سلامت الکترونیکی و شناسه‌های ملی برای عرضه کنندگان، برنامه‌های بیمه سلامت با تأکید بر امنیت و حریم داده‌های سلامت است. استانداردها برای آن تدوین شده‌اند که با استفاده‌ی گسترده از مبادلات داده‌ی الکترونیکی، کارامدی و اثربخشی سیستم بهداشت ایالات متحده را افزایش دهند. (مویله، ۲۰۱۱م.، ص۴۲) به دلیل وجود نظام قانون‌گذاری فدرال در ایالات متحده برای حفاظت از داده‌های شخصی افراد، قوانین متعدد دیگری تصویب شده است که به‌عنوان نمونه، قانون حریم خصوصی ماساچوست یکی از این قوانین است. در این قانون برای اشخاصی که در ارتباط با شهروندان ایالت ماساچوست داده‌هایی را در اختیار دارند یا اجازه دارند در اختیار داشته باشند، استانداردهایی تدوین می‌شود. این قانون حداقل استانداردهایی را که در ارتباط با حفاظت از اطلاعات شخصی در متون کاغذی و الکترونیکی باید لحاظ شود مشخص می‌کند. هدف قانون این است که از امنیت و حریم اطلاعات افراد مطابق با استانداردها حفاظت شود و از

دسترسی غیرمجاز یا استفاده از اطلاعات در راستای حفظ مشتری از صدمات یا مشکلات جدی ممانعت شود. ضمن این‌که تصویب قانون مبارزه با سرقت هویت آمریکا در سال ۲۰۰۳م.، یکی دیگر از زیرساخت‌های تأمین کننده‌ی حقوق سلامت الکترونیک است. این قوانین شرکت‌ها را ملزم می‌کند که تمهیداتی بیندیشند که از سرقت هویت کاربران به‌ویژه کاربران سلامت الکترونیک جلوگیری شود. (رجبی، ۱۳۹۰هـ.ش.، ص۴۳)

ب) آلمان

سامانه‌ی مراقبت‌های پزشکی در آلمان بر محور طرحی موسوم به بیمه‌ی سلامت استوار است که ۷۰ میلیون نفر از جمعیت ۸۰ میلیون نفری آلمان را تحت پوشش خود قرار داده است. این طرح خدماتی همچون ویزیت‌های مقدماتی، ویزیت‌های اورژانسی، داروهای تجویزی، خدمات دندان‌پزشکی، درمان‌های بیمارستانی و نیز خدمات توان‌بخشی را شامل می‌شود. شبکه‌های محلی و منطقه‌ای که مطب پزشکان عمومی نیز به‌صورت مجازی عضو آن‌ها هستند به ازای هر بیماری که با اشتراک‌گذاری پرونده‌ی پزشکی خود در این شبکه‌ها موافقت نموده، سالیانه بودجه‌ای در حدود ۵۰۰ یورو بیشتر دریافت می‌کنند. بیمارستان‌ها نیز با عضویت در این شبکه‌ها، نامه‌های الکترونیکی را دریافت می‌کنند. پهنای باند دسترسی به اینترنت در آلمان بین ۱ تا ۶ مگابایت در ثانیه برآورد می‌شود. همچنین قراردادهایی میان سازمان‌های بیمه‌گر در آلمان و سازمان‌های بیمه‌گر خارج از آلمان منعقد شده که امکان تبادل داده‌های بیمه‌ای در خارج از مرزها را فراهم کرده است. فرمت‌های تبادل داده‌ها نیز اغلب انحصاری و از سوی ارائه‌دهندگان خدمات فناوری اطلاعات برای هر شبکه‌ی خاص طراحی شده‌اند. در آلمان حریم

خصوصی بیمار بر دیگر ابعاد پرونده‌ی الکترونیکی سلامت یا پوشه‌ی الکترونیکی بیمار برتری دارد. در این راستا افراد بیمه شده، نخست باید رضایت مقدماتی خود را برای تشکیل پرونده‌ی الکترونیکی سلامت ابراز کنند. بدین ترتیب افراد مختار خواهند بود حتی بخش‌هایی از این پرونده را پنهان یا مسدود کنند. (رای، ۲۰۰۶م.، ص۴۲) امنیت سلامت الکترونیک در سطح فدرال از سوی آژانس ملی امنیت در عرصه‌ی فناوری اطلاعات و نیز مقام حفاظت از داده‌های فدرال مورد بررسی قرار گرفته است. در سطح ایالاتی نیز این مسأله از جانب مقامات امنیتی و ایالات بازبینی شده است. در قانون فدرال، حفاظت از داده‌های شخصی آلمان به‌صورت باز تعریف شده است. همه‌ی داده‌هایی که با یک فرد شناسایی شده است یا فردی که ممکن است توسط عرضه‌کنندگان، کاربران یا اشخاص ثالث شناسایی شوند، از سوی قانون‌گذار داده‌ی شخصی تعریف شده است. (اکهاردت، ۲۰۱۱م.، ص۷۸)

ج) هلند

سامانه‌ی مراقبت‌های پزشکی در هلند سالیانه هزینه‌ای بالغ بر ۵۵ میلیارد یورو مصرف می‌کند. بیش از ۹۰ درصد مؤسسات فعال در عرصه مراقبت‌های پزشکی در این کشور خصوصی هستند و ۱۰ درصد باقی بیمارستان‌های عمومی وابسته به دانشگاه و کلینیک‌های کوچک دولتی هستند. ضریب نفوذ اینترنت در هلند ۷۳/۳ درصد است و جایگاه پنجم جهان را به خود اختصاص داده است. بهره‌مندی هلند از چنین زیرساخت ارتباطی‌ای، به راهبرد ملی فناوری اطلاعات در این کشور استحکام ویژه‌ای بخشیده است. دولت هلند در جستجوی پایه‌ریزی سامانه‌ای متمرکز در عرصه‌ی پرونده‌ی الکترونیکی سلامت نیست بلکه درصدد آن است که داده‌های پزشکی را در مراکز داده‌ی محلی مختلف ذخیره‌سازی کند. از این

رهگذر امکان ادغام داده‌های پزشکی مرتبط از مراکز داده‌ی محلی با سامانه‌ی ملی مجازی فراهم می‌شود. تقریباً تمامی پزشکان عمومی و اغلب پزشکان بالینی متخصص در مراقبت‌های مقدماتی از پرونده‌ی الکترونیکی سلامت استفاده می‌کنند و تمامی بیمارستان‌ها نیز به سیستم‌های اطلاعاتی الکترونیکی مجهزند. این سامانه براساس نگرش اداری و مالی پایه‌ریزی شده است و برعکس سامانه‌های مورد استفاده‌ی انگلستان و دیگر کشورهای اروپایی بیمارمحور و فرایندبنیاد نیستند که این امر یکی از چالش‌های پرونده‌ی الکترونیکی سلامت هلند شمار می‌رود. همگام با ارائه‌ی خدمات پرونده‌ی الکترونیکی سلامت، قوانین مربوط به حفاظت از داده‌های پزشکی نیز در هلند به تصویب رسیده است. این قوانین، ذخیره‌سازی متمرکز اطلاعات پزشکی بیماران را مجاز نمی‌داند. براساس قانون پرونده سلامت الکترونیک، متخصصان بخش سلامت ملزم به حفاظت از پرونده‌های مربوط به وضعیت پزشکی و درمانی هر بیمار خواهند بود. برمبنای قوانین مربوط به حریم خصوصی، بازیابی داده‌های پرونده‌ی الکترونیکی توسط پزشکان صرفاً با هدف ارائه‌ی مراقبت‌های پزشکی مجاز خواهند بود. (می یری، ۲۰۰۹م.، ص۷۳)

ت) انگلستان

نظام خدمات درمانی همگانی در انگلستان پس از جنگ جهانی دوم با هدف دسترسی تمامی شهروندان به مراقبت‌های پزشکی پایه‌ریزی شد. این نظام، سامانه‌ی نوینی از مراقبت‌های پزشکی مبتنی بر بیمه‌ی اجتماعی است که بالغ بر ۵۱ میلیون شهروند انگلیسی را تحت پوشش قرار می‌دهد. در نظام مراقبت‌های پزشکی انگلستان، پایگاه داده‌ای در سطح ملی موسوم به اسپاین[۷] پایه‌ریزی شده است که خلاصه‌ای از پرونده‌های بیماران در آن‌جا ذخیره‌سازی شده است. در پایگاه داده‌ی

مذکور، انباری از پرونده‌های پزشکی، فرایندهای نظارت بر روند دسترسی، مرکز ارسال پیام و درگاه‌هایی برای کاربران بالینی درنظر گرفته شده است. (پوراسماعیل، ۱۳۸۷هـ‌ش.، ص۲۰) در خلاصه پرونده‌ی پزشکی هر فرد، اطلاعات مربوط به مراقبت‌های پزشکی که از سوی سامانه‌های پرونده‌ی سلامت الکترونیک جهت بازیابی اطلاعات بیماران مورد استفاده قرار می‌گیرد موجود است. وزارت سلامت انگلستان، مرجع صالح و قانون‌گذار[۸] اصلی عرصه‌ی پرونده‌ی سلامت الکترونیک است و مراجع ذی‌صلاح دیگری همچون توسعه‌ی پرونده‌های درمانی با بهره‌گیری از مکانیزم‌های نظارت گوناگون در این عرصه فعالیت دارند. حریم خصوصی و چالش امنیت نیز در قوانین پایه‌ریزی شده است که از سوی اداره‌ی سلامت راهبری می‌شود. براساس قوانین موجود در انگلستان، اطلاعات باید زمانی فاش شود که رضایت بیمار وجود داشته باشد یا این‌که قانون آن را درخواست نماید. آرای صادر شده از سوی دادگاه‌ها نشان می‌دهد که رازداری فقط وقتی ممکن است نقض شود که منفعت عمومی مهم‌تر از حریم خصوصی باشد. (پارسا، ۱۳۸۸هـ‌ش.، ص۷) حقوق بیمارانی که اطلاعات آن‌ها در پرونده‌ی سلامت الکترونیک ذخیره شده است از طریق خط مشی نظام خدمات درمانی همگانی انگلستان و قوانین مربوط به حفاظت از داده‌ها تضمین می‌شود؛ بر این اساس هر یک از بیماران می‌توانند از نگهداری داده‌های خود در پایگاه داده‌ی پرونده‌ی سلامت الکترونیک متمرکز جلوگیری کنند. در این راستا هر یک از پزشکان موظف خواهند بود که در جهت انعقاد قراردادهای تجاری با نظام خدمات درمانی همگانی انگلستان به‌عنوان ارائه‌دهنده‌ی خدمات ملی، اقدام کنند. پایگاه داده‌ی اسپاین به‌عنوان خلاصه پرونده‌ی مرکزی، تنها درصد کوچکی از اطلاعات

نگهداری شده در سامانه‌های درمانی اولیه و ثانویه را در خود جای داده است. (کریستودولو، ۲۰۰۸م.، ص۵۲)

ث) کانادا

سامانه‌ی مراقبت‌های پزشکی در کانادا که از سوی دولت تأمین می‌شود، ۱۳ طرح بیمه‌ی سلامت ایالتی و ولایتی را در خود جای داده است. هدف این سامانه تضمین دسترسی همگانی به خدمات پزشکی و بیمارستانی ضروری صرف‌نظر از سن، درآمد و بدون پرداخت هزینه‌ی مستقیم در قبال خدمات، طراحی شده است. در این راستا در قانون سلامت که در سال ۱۹۸۴م. به تصویب رسید به اصول ملی و ارزش‌های بنیادین در عرصه‌ی مساوات و یکپارچگی اشاره شده است که سامانه‌ی مراقبت‌های پزشکی را راهبری می‌کند. این اصول عبارتند از: قابلیت دسترسی، قابلیت انتقال، همگانی بودن و جامعیت. تأمین امنیت و نیز حریم خصوصی، عناصر ضروری در عرصه‌ی پرونده‌ی سلامت الکترونیک به‌شمار می‌روند که در سند زیرساخت مفهومی امنیت و حریم خصوصی پرونده‌ی سلامت الکترونیک نسخه‌ی ۱۰۱ در ژوئن ۲۰۰۵م. و نسخه‌ی دوم از طرح انتشار یافته در سال ۲۰۰۶م. مورد بررسی قرار گرفته‌اند. (بلاک، ۲۰۰۸م.، ص۵۰) در این راستا در کانادا به موضوع حریم خصوصی در بسیاری از قوانین مربوط به حریم خصوصی خاص در عرصه‌ی مراقبت‌های پزشکی و حریم خصوصی عام در سطح محلی، ایالتی و فدرال پرداخته شده است. از این گذشته از نظر دولت کانادا، موضوع حریم خصوصی باید در ارزیابی‌های تمامی پروژه‌های دریافت کننده‌ی بودجه و برخوردار از اطلاعات پزشکی سلامت لحاظ شود. این امر تضمین کننده‌ی توجه به موضوع حریم خصوصی و امنیت در کلیه‌ی مراحل پروژه است. (بلاک، ۲۰۰۸م.، ص۴۲)

ج) ترکیه

جمعیت سالمند، تغییر انتظارات بیماران و نیاز مردم و دولت به کاهش هزینه‌های سلامت از اسباب توجه و توسعه‌ی سلامت الکترونیک در ترکیه بوده است. پروژه‌ی سلامت الکترونیکی در ترکیه، پروژه‌ی بزرگ و بلندمدتی است به‌دست وزارت سلامت ترکیه هدایت می‌شود. (یورت، ۲۰۰۸م.، ص۹) پروژه‌ی سلامت الکترونیک مشتمل بر چند طرح سلامت الکترونیک است که از مهم‌ترین نگرانی‌های اجرای این طرح‌ها فقدان استانداردهای اطلاعات سلامت در سطح ملی و فقدان زیرساخت‌های حقوقی از جمله حفظ حریم خصوصی در سلامت الکترونیک است. در ترکیه شورای عالی ارتباطات نهاد اصلی حفظ حریم خصوصی و حمایت از داده‌ها در ارتباطات الکترونیکی است. در ماده‌ی ۲۰ مقررات مربوط به وظایف این شورا بر منع دسترسی به اطلاعات در ارتباطات الکترونیکی نظیر تلفن، موبایل و پست الکترونیکی بدون رضایت افراد اشاره شده است. با وجود این تأکید قانونی در ترکیه قانون مشخصی در مورد حفاظت از داده‌های پزشکی وجود ندارد و حتی تعریف مشخصی نیز از اطلاعات شخصی سلامت وجود ندارد. (برک، ۲۰۱۰م.، ص۷)

حریم خصوصی و حفاظت از داده‌ها در ایران

در قانون اساسی جمهوری اسلامی ایران به حفظ حریم خصوصی افراد تأکید شده است و در اصول ۳۳، ۳۲، ۲۸، ۲۵، ۲۳، ۲۲، ۲ و ۳۹ قانون اساسی تأکید بر حفظ حریم خصوصی افراد مشاهده می‌شود. اصل ۲۲ قانون اساسی حیثیت و جان و مال و حقوق و مسکن و شغل اشخاص را مصون از تعرض دانسته است؛ اصل ۲۳ هرگونه تفتیش عقاید را ممنوع اعلام کرده است و در اصل ۲۵ نیز بازرسی و

نرساندن نامه و ضبط و فاش نمودن مکالمات و افشای محتوای آن از هرگونه تجسس مگر به حکم قانون ممنوع دانسته است؛ بنابراین در مهم‌ترین ارکان حکومتی و عهدنامه‌ی مردم و حکومت که در قانون اساسی متجلی شده است حریم خصوصی، اساساً از موضوعات بسیار مهم تلقی شده است. ردپای دیگر اهمیت حفظ حریم خصوصی را می‌توان در فرمان هشت ماده‌ای امام خمینی (ره) به قوه‌ی قضاییه و تمام نهادهای اجرایی در مورد اسلامی شدن قوانین در تاریخ ۱۳۶۱/۹/۲۴هــ‌ش. است که در این فرمان ورود بدون اذن به منازل و محل کار افراد و شنود تلفن و گوش دادن به نوار و ضبط صوت دیگران به‌نام کشف جرم و تجسس در اسرار دیگران و افشای آن، ممنوع و جرم اعلام شده است.

برخلاف اهمیت حفظ حریم خصوصی در اسناد بالادستیِ جمهوری اسلامی ایران به‌ویژه قانون اساسی، مقررات و قوانین حاکم ایران حافظ حریم خصوصی نیست. صرفاً در قانون جزای ایران، حمایت‌ها راجع به اموال و اشخاص و تا حدودی حیثیت آن‌ها برقرار شده، اما به‌طور مستقیم نقض حریم خصوصی آنان را متذکر نشده و تنها حمایتی که بخشی از محدوده‌ی حریم خصوصی را محترم می‌شمارد ماده‌ی ۶۹۴ از فصل ۲۶ قانون مجازات اسلامی راجع به هتک حرمت منازل و املاک موضوع مواد ۶۹۰ الی ۶۹۶ است که هیچ‌کدام ناظر به فضای مجازی نیست؛ البته قانون تجارت الکترونیک ایران مصوب ۸۲/۱۰/۱۷ هــ‌ش. مجلس شورای اسلامی در مواد ۵۸ تا ۶۱ به موضوع حمایت داده‌ها پرداخته است؛ نیز براساس بند (ه) ماده ۱۰۳ قانون برنامه‌ی چهارم که در آن قوه‌ی قضاییه موظف است به تهیه‌ی لایحه‌ی «حفظ و ارتقای حقوق شهروندی و حمایت از حریم خصوصی افراد، در راستای اجرای اصل بیستم (۲۰) قانون اساسی جمهوری اسلامی ایران» شده بود در سال ۸۵ هــ‌ش. این لایحه تقدیم مجلس شورای اسلامی شد که پس از مدتی بنا به

درخواست دولت از دستور کار مجلس شورای اسلامی خارج گردید. در این طرح به حریم خصوصی جسمانی، منازل، محل کار، حریم خصوصی اطلاعات، اطلاعات شخصی در فعالیت‌های رسانه‌ها، حریم خصوصی ارتباطات و مسؤولیت‌های ناشی از نقض حریم خصوصی توجه شد و در آن به موضوع حریم خصوصی و ارتباطات اینترنتی در هفت ماده پرداخته شد. براساس مندرجات لایحه، شنود، ضبط، ذخیره یا انواع دیگر رهگیری ارتباطات خصوصی اینترنتی اشخاص بدون رضایت آن‌ها مجاز نیست. ارائه‌دهندگان خدمات عمومی ارتباطات اینترنتی باید کلیه‌ی تدابیر فنی و اداری را برای تأمین امنیت و خدمات خود فراهم کنند. با این وصف، کشور از لحاظ وجود قوانین حفظ حریم خصوصی و حفاظت از داده‌های شخصی دارای خلاء جدی است.

حفاظت از داده‌های سلامت در ایران

در کشور ما از سال ۱۳۸۰هــ‌ش. موضوع سلامت الکترونیک و پرونده‌ی الکترونیک سلامت مورد توجه بوده است و کوشش‌های آن اغلب در بدنه‌ی دولت انجام گرفته است. این کوشش‌ها بیشتر به‌دست وزارت بهداشت و سازمان تأمین اجتماعی انجام شده است که هنوز با سطح مورد انتظار فاصله‌ی زیادی دارد؛ البته به‌دلیل مشخص نشدن نهاد ناظر و سیاست‌گذار به‌عنوان متولی سلامت الکترونیک و پرونده‌ی الکترونیک سلامت در کشور، تضمینی برای تحقق اهداف این بخش در آینده وجود ندارد. فقدان قوانین تسهیل کننده‌ی توسعه‌ی سلامت الکترونیک کشور و قوانینی که سلامت الکترونیک را جزء اولویت‌های اساسی کشور قرار دهد از خلاءهای حقوقی موجود کشور است. (فقیهی، ۱۳۹۰هــ‌ش.، ص۲۱) البته ماده‌ی ۶۴۸ قانون مجازات اسلامی، افشای اطلاعات بیماران را در

محیط فیزیکی جرم‌انگاری کرده است؛ برطبق این ماده، پزشکان، جراحان، ماماها، داروفروشان و کلیه‌ی کسانی که به مناسبت شغل یا حرفه‌ی 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. وجود چنین زیرساخت حقوقی‌ای لازم است ولی کافی نیست و لزوم قانون حفاظت از داده‌های شخصی در فضای مجازی، می‌تواند امنیت و محرمانگی جمع‌آوری داده، کنترل و به اشتراک‌گذاری اطلاعات را فراهم نماید.

نتیجه

براساس مطالعات انجام شده و کارهای پژوهشی پیشین نظیر گزارش پژوهشی مرکز پژوهش‌های مجلس شورای اسلامی یکی از موانع اساسی توسعه‌ی سلامت الکترونیک در کشور فقدان قانون مشخصی در موضوع حفظ حریم خصوصی و حمایت از داده‌های سلامت است. برطبق مطالعات انجام شده کشورهایی نظیر آلمان، انگلیس و کانادا برای مقابله با این چالش اقداماتی را انجام داده‌اند؛ در این کشورها حریم خصوصی بیمار بر دیگر ابعاد پرونده‌ی الکترونیکی سلامت یا پوشه‌ی الکترونیکی بیمار برتری دارد. در این راستا افراد بیمه شده، نخست باید رضایت مقدماتی خود را برای تشکیل پرونده‌ی الکترونیکی سلامت ابراز کنند. بدین ترتیب افراد مختار خواهند بود حتی بخش‌هایی از این پرونده را پنهان یا مسدود کنند و هر یک از بیماران می‌توانند از نگهداری داده‌هایشان در پایگاه داده پرونده‌ی سلامت الکترونیک متمرکز جلوگیری کنند. قانون حفاظت از داده‌ها علاوه بر درنظر داشتن شروط فوق باید متضمن جمع‌آوری و پردازش داده‌های شخصی به‌طور قانونی و منصفانه و صرفاً برای اهداف سلامت باشد. داده‌ها باید متناسب و مرتبط با اهداف و واضح و روزآمد باشند و نباید بیش از زمان لازم نگهداری شوند و ضمانت اجرایی مناسب علیه پردازش غیرمجاز و غیرقانونی داده‌ها لحاظ شود، همچنین انتقال داده‌ها به خارج از پرونده باید سطح مقتضی حمایت از حقوق و آزادی‌های افراد را از حیث پردازش داده‌های شخصی تأمین کند. علاوه بر لزوم تصویب قانون حریم خصوصی یا حفاظت از داده‌ها، همانند دولت کانادا، موضوع حریم خصوصی باید در ارزیابی‌های تمامی پروژه‌های دریافت کننده‌ی بودجه و برخوردار از اطلاعات پزشکی سلامت لحاظ شود؛ ضمن این‌که تصویب قوانینی در زمینه‌هایی همچون سرقت هویت نیز راهگشای توسعه‌ی

سلامت الکترونیک کشور است. در حال حاضر همان‌گونه که در کار پژوهشی امیرحسین جلالی با عنوان «حریم خصوصی در فضای سایبر» به آن اشاره شد به دلیل نبودِ قانون حفاظت از داده‌ها در ایران، امکان سوءاستفاده از اطلاعات شخصی سلامت افراد وجود دارد و حریم خصوصی افراد می‌تواند بعضاً از سوی مجریان قانون، ارائه‌دهندگان خدمات شبکه‌ای و سایر افراد مورد تعرض قرار گیرد.

مجریان قانون طبق قوانین و مقررات ممکن است به اطلاعات و داده‌های خصوصی افراد جهت پیشگیری از وقوع جرم یا تعقیب مجرمان دسترسی داشته باشند. اگر ضابطه‌ی خاصی برای استفاده از این اطلاعات وجود نداشته باشد این اختیار منجر به وارد شدن لطمه به حریم خصوصی افراد می‌شود.

ارائه‌دهندگان خدمات شبکه‌ای به راحتی می‌توانند انواع بسیاری از داده‌های الکترونیکی خصوصی افراد را در مقیاس وسیع در اختیار داشته باشند. این تهدید دو جنبه دارد: اولین جنبه سوءاستفاده‌ی خود فراهم کننده خدمات شبکه‌ای از اطلاعات شخصی است و جنبه‌ی دوم همان‌گونه که در پایان‌نامه‌ی کارشناسی ارشد اسماء موسوی خراسانی به آن اشاره شده است سوءاستفاده افراد دیگر در بستر ارتباطی است. صاحبان و متصدیان خدمات شبکه‌ای فراهم کننده‌ی ارتباطات، بین زیان‌دیدگان و سوءاستفاده کنندگان در دنیای مجازی هستند. این تهدید در فضای سایبر با وجود افرادی که جمع‌آوری، ذخیره‌سازی و بهینه‌سازی داده‌های خصوصی کاربران را به قصد اقدامات تعرض‌آمیز یا فروش به مجرمان سایبری، حرفه‌ی خود قرار داده‌اند بیشتر می‌شود. به‌دلیل وجود تهدید نقض حریم خصوصی داده‌های سلامت، وجود قانون حفاظت از داده‌ها از سوءاستفاده‌ی داده‌های شخصی سلامت افراد تا حد زیادی جلوگیری می‌کند.

باید توجه داشت که وجود قانون حریم خصوصی، شرط لازم برای توسعه‌ی سلامت الکترونیک است ولی شرط کافی نیست و جهت حفظ حریم خصوصی کاربران، ارائه‌دهندگان خدمات شبکه‌ای ملزم به استفاده از سامانه‌های اعتبارسنجی مشتریان، سامانه‌های رمزنگاری اطلاعات، دیوارهای آتشین، سامانه‌های تشخیص تجاوز، نرم‌افزارهای ضد جاسوسی و ضد هرزنامه می‌باشند. قانون‌گذاران نیز باید تعهدات و همچنین سطح دسترسی ارائه‌دهنده‌ی خدمات شبکه‌ای به اطلاعات شخصی افراد را ضابطه‌مند نمایند. همچنین قانون گذاران باید دسترسی به اطلاعات شخصی افراد برای مجریان را در چارچوب قوانین حفظ حریم خصوصی و حفاظت از داده‌ها ضابطه‌مند نمایند. هر چند اجرای سلامت الکترونیک به‌ویژه ایجاد پرونده‌ی سلامت الکترونیک منافع زیادی برای افراد و کشور ایجاد می‌کند به‌دلیل احتمال افشای داده‌های خصوصی، باعث نگرانی‌هایی می‌شود که این نگرانی‌ها با تصویب قوانینی در موضوع حریم خصوصی، امن‌سازی ارتباطات الکترونیکی و ضابطه‌مند کردن نحوه‌ی دسترسی مجریان و ارائه‌دهندگان خدمات شبکه‌ای کاهش می‌یابد.

پی‌نوشت‌ها

1- Cloud computing
2- Privacy
3- Data protection
4- Server Computer
5- Personal Health Record (PHR)
6- Health care provider
7- Spine
8- Regulator

فهرست منابع

جلالی، امیرحسین ـ (۱۳۸۵هـ.ش.)، حریم خصوصی در فضای سایبر (حریم داده‌های الکترونیکی)، تهران، مرکز پژوهش‌های مجلس شورای اسلامی

رجبی، ابوالقاسم ـ (۱۳۹۰هـ.ش.)، رایانش ابری، تهران، مرکز پژوهش‌های مجلس شورای اسلامی

ریاضی، حسین ـ (۱۳۸۷هـ.ش.)، پرونده الکترونیکی سلامت در ایران، تهران، انتشارات وزارت بهداشت

پورناجی، بنفشه ـ (۱۳۸۷هـ.ش.)، نگاهی به پدیده حریم خصوصی، تهران، اعتماد

رابینز، استیفن پی ـ (۱۳۸۹هـ.ش.)، (مترجمان: سید محمد اعرابی و علی پارساییان)، (۱۳۸۹هـ.ش.)، دفتر پژوهش‌های فرهنگی، چاپ چهارم

هزاوه، بابک ـ (۱۳۸۸هـ.ش.)، رایانش ابری پدیده‌ای نوین، تحلیلگران عصر اطلاعات، سال سوم، شماره‌ی ۲۷ و ۲۸، آبان و آذر ۸۸

کشاورز، حمیدرضا ـ (۱۳۸۹هـ.ش.)، مروری بر محاسبات ابری، ماهنامه‌ی رایانه خبر، سال هفتم، شماره‌ی ۶۱

پوراسماعیل، حسن و فقیهی، مهدی ـ (۱۳۸۷هـ.ش.)، بررسی وضعیت سلامت الکترونیک در ایران، مرکز پژوهش‌های مجلس شورای اسلامی

فقیهی، مهدی و معمارزاده، غلامرضا ـ (۱۳۹۰هـ.ش.)، شناسایی اولویت‌های خط‌مشی‌گذاری توسعه‌ی سلامت الکترونیک در ایران، مدیریت سلامت، شماره‌ی ۴۳

فولادی، محمد ـ (۱۳۸۶هـ.ش.)، اخلاق روزنامه‌نگاری، آسیب‌ها و چالش‌ها، ماهنامه‌ی معرفت، شماره‌ی ۱۲۳

پارسا، مجتبی ـ (۱۳۸۸هـ.ش.)، حریم خصوصی و رازداری در پزشکی و جنبه‌های مختلف آن، مجله‌ی اخلاق و تاریخ پزشکی، شماره‌ی ۴

موسوی خراسانی، اسماء ـ (۱۳۸۸هـ.ش.)، مسؤولیت مدنی ارائه‌دهندگان خدمات اینترنتی، پایان‌نامه‌ی کارشناسی ارشد، دانشکده‌ی حقوق دانشگاه تهران

Löhr, h(2010), Securing the E-Health Cloud, Proceedings of the 1st ACM International Health Informatics Symposium.

Steven L, Walter W, Heidenreich G, Yantis G, Bakker H, Stegwee ,R. Electronic Health Records , a Global Perspective. New York: Himss Enterprise System Steering Committee; 2008.

Ray P, Androuchko L, Androuchko V. A comparative overview of e-health development in developing and developed countries. Luxamburg: Information Society & Media; 2006

Meyeri, Hüsing T, Didero M, Korte W. Ehealth Benchmarking. Bonn: Gesellschaft für Kommunikations- und Technologieforschung mbH; 2009

Christodoulou E, Dunbar A, Gaspar P, Jaksa R., Krapez K. The Development of eHealth in an Enlarged EU. Seville (Spain), Institute for Prospective Technological Studies; 2008.

Black A, Anandan C, Cresswell K, Pagliari C, McKinstry B, Procter R, Majeed A, Sheikh A. The Impact of eHealth on the Quality & Safety of Health Care. London: Imperial college of London; 2008.

Eckhardt, Jens; Hilber LL.M, Marc; Giebichenstein ,Rüdiger; Niemann, Fabian; Helbing, Thomas;Weiss, Andreas. Guidelines Cloud Computing German Law, Data Protection & Compliance. Euro Cloud. 2011

http://en.eurocloud.de/2011/03/04/eurocloud-guidelines-cloud-computing-german-law-data-protection-and-compliance./

Berk, Emer(2010), A General overview data protection and privacy law in Turkey, ADLAW international

Yurt, Nihat(2008), Turkey`s E-Health activities, National Health department

Moyle, Ed``(2011), Why cloud computing change the game for HIPPA security , Technews world.

یاداشت شناسه‌ی مؤلف

غلامرضا معمارزاده طهران: استادیار دانشکده‌ی مدیریت و اقتصاد دانشگاه آزاد، واحد علوم تحقیقات

حسین رفوگر آستانه: کارشناس ارشد مدیریت صنعتی، دانشگاه آزاد اسلامی واحد تهران مرکزی، پژوهشگر گروه مطالعات ارتباطات و فناوری اطلاعات مرکز پژوهش‌های مجلس شورای اسلامی

مهدی فقیهی: دانشجوی دکتری مدیریت دانشکده‌ی مدیریت و اقتصاد دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، مدیر گروه مطالعات ارتباطات و فناوری اطلاعات مرکز پژوهش‌های مجلس شورای اسلامی

نشانی الکترونیکی: mail@mfaghihi.ir

تاریخ دریافت مقاله: ۱۳۸۸/۸/۲۴

تاریخ پذیرش مقاله: ۱۳۸۹/۳/۳