

## جرایم پزشکی از راه دور ناشی از سلامت الکترونیکی

عباس کریمی<sup>۱</sup>

ایمان رحیمی پور<sup>۲</sup>

مهدی حسنی<sup>۳</sup>

### چکیده

پزشکی از راه دور (تله مدیسین) چهره نوینی از طبابت است که در زمینه‌های گوناگون می‌تواند یاری‌رسان طبقات مختلف جامعه بشری باشد. هدف اولیه از اختراع این تکنولوژی، حمایت از بیماران در معرض خطری بود که به دلایل مختلف دسترسی سریع و به موقع به امکانات خاص پزشکی برای آنها مقدور نیست. سیطره‌ی این فناوری از مشاوره‌ها و ویزیت‌های از راه دور تا انواع عمل‌های جراحی از طریق سیستم‌های الکترونیکی را دربر می‌گیرد. این فناوری همان‌طور که فرزند دو رشته پزشکی و IT است، جرایم پزشکی و IT را نیز در هم ادغام کرده و تأثیر جرائم پزشکی را به وسعت اینترنت درآورده است. اهم خطراتی که بیماران را در استفاده از تله مدیسین تهدید می‌کند، کنجکاوی افراد، سوءاستفاده هکرها و گروه‌های تروریستی در این زمینه است. این افراد به طرق مختلف از قبیل دسترسی و افشای اطلاعات سلامت اشخاص، جعل عناوین خاص پزشکی، خرابکاری در سیستم‌های الکترونیکی، انتقال ویروس به شبکه‌های اینترنتی و استماع غیرمجاز ارتباطات، در پی اجرای مقاصد نامشروع ذهنی، اقتصادی یا سیاسی خویش هستند. این پژوهش ابتدا به بیان خطرات و جرائم بالقوه پزشکی از راه دور پرداخته و سپس با مطالعه‌ی قوانین جزایی ایران (اعم از قانون مجازات اسلامی، قانون تجارت الکترونیک، قانون جرائم رایانه‌ای) پاسخ جزایی این نظام حقوقی را در برخورد با این جرائم مورد بررسی قرار خواهد داد.

### واژگان کلیدی

تله مدیسین؛ جرم؛ پرونده الکترونیکی سلامت؛ محرمانگی داده‌ها.

۱. عباس کریمی: استاد گروه حقوق خصوصی دانشکده‌ی حقوق و علوم سیاسی دانشگاه تهران

۲. ایمان رحیمی پور: دانشجوی دکترای حقوق کیفری و جرم‌شناسی دانشگاه تربیت مدرس

۳. مهدی حسنی: دانشجوی کارشناسی ارشد حقوق خصوصی دانشگاه مفید قم

## جرایم پزشکی از راه دور ناشی از سلامت الکترونیکی

قوانین و مقررات مربوط به اجرای مشاغل پزشکی، بر اقدامات موافق موازین علمی و فنی پزشکان در انجام وظایفشان صحنه گذاشته و تنها آنان را در موارد خاص مسئول دانسته است. با این حال، ورود چهره‌های نوین طبابت همانند تله‌مدیسین، حقوق بیماران، مسئولیت پزشک و اشخاص ثالث را در کشورهای پیشرفته دستخوش تغییراتی نموده است که قوانین سنتی پاسخگوی آن نیست. بنابراین اگرچه این علم در نظام پزشکی ایران طفلی نوپا است، قانونگذاری در این زمینه مستلزم یک نظام قضایی پویا است. زیرا عدم قانونگذاری در این گونه مسائل عواقب جبران‌ناپذیری به همراه دارد. شاهد مثال این مورد مرد سوئسی مبتلا به ایدز بود که پس از ورود به خاک مالزی و علم به بیماری خویش با هفده زن رابطه جنسی برقرار نمود. متعاقب این عمل، دادگاه تنها به اخراج وی از مالزی حکم داد و تنها دلیل این حکم ناعادلانه ضعف قانونگذاری این کشور بود.<sup>۱</sup>

با این وصف بررسی جنبه‌های کیفری سوء استفاده‌های احتمالی از تله‌مدیسین ضروری است. این پژوهش درصدد است پس از تعریف واژه‌های کلیدی در مبحث اول، به مصادیق مجرمانه‌ای که در این زمینه قابلیت تحقق دارد، (مبحث دوم) بپردازد.

### مبحث اول: مفهوم جرایم دور درمانی

در بند اول ابتدا به بیان مفهوم تله‌مدیسین پرداخته و سپس با تبیین جرم (بند دوم)، رابطه تله‌مدیسین و جرم مورد بررسی قرار می‌گیرد.

## بند اول: مفهوم تله مدیسین

Tele که از لغت یونانی telos نشأت گرفته به معنی «فاصله، مسافت، دور» و Medicine که ریشه آن به واژه‌ی لاتین «mederi» برمی‌گردد به معنای «معالجه، درمان» است. حاصل ترکیب این دو لغت، که نخستین بار در دهه ۷۰ میلادی توسط توماس برد<sup>۲</sup> صورت گرفت، واژه telemedicine است.

ساده‌ترین تعریف ممکن که ترکیب و ترجمه تحت‌اللفظی تله مدیسین است می‌تواند «پزشکی از راه دور» باشد. ولی به واقع این تعریف ساده، گویای تمام زوایای telemedicine نیست. از طرف دیگر تعریف رسمی و واحد برای تله‌مدیسین ارائه نشده است. در توضیح این عنوان، از تعریف ساده در یک خط تا گزارش کاملی که دپارتمان تجاری، بهداشتی و خدمات انسانی آمریکا<sup>۳</sup> در ژانویه ۱۹۹۷ به کنگره داده می‌توان یافت. در ذیل نمونه‌هایی از تعاریف ارائه شده‌ی سازمان‌های دست‌اندرکار بیان می‌شود:

تعریف کمیسیون اروپا: دسترسی سریع به مهارت‌های پزشکی به‌وسیله فناوری اطلاعات و ارتباطات بدون توجه به جایی که بیمار یا اطلاعات بیمار قرار دارد. تعریف سازمان بهداشت جهانی: اعمال مراقبت‌های بهداشتی شامل تشخیص، مشاوره، معالجه و آموزش با استفاده از محاورات صوتی - تصویری و ارتباط داده‌ها.

علاوه بر تعاریف سازمان‌های مذکور، تعاریف ذیل نیز در تشریح عبارت تله‌مدیسین بیان شده است.

۱. ارائه از راه دور خدمات پزشکی با زیرساخت‌های ارتباط از راه دور. ۲. انتقال داده‌های پزشکی الکترونیکی (تصویر، صدا و پرونده بیمار) از محلی به محل دیگر
۳. استفاده از تکنولوژی ارتباط از راه دور برای ارائه، تسهیل و تسریع خدمات

پزشکی با دسترسی به پایگاه‌های داده یا لینک کلینیک یا مطب پزشکان به بیمارستان‌های مرکزی یا انتقال تصاویر برای آزمایش در جای دیگر.

اما «استفاده از فناوری اطلاعات و ارتباطات برای انتقال اطلاعات پزشکی جهت تشخیص، درمان و آموزش پزشکی» می‌تواند تعریفی جامع از پزشکی از راه دور باشد، که در تشریح آن باید گفت:

– فناوری مورد بحث می‌تواند شامل تمام وسایل الکترونیکی ارتباطی نظیر تلفن، فکس و... باشد، هر چند که اغلب IT و کامپیوتر به ذهن متبادر می‌شود.

– انتقال، ممکن است از طریق ارتباط بین پزشک و بیمار یا بین شاغلان حرفه پزشکی و بدون بیمار باشد.

– اطلاعات پزشکی شامل پخش زنده صدا و یا تصویر، فایل‌های صوتی تصویری، محاورات طرفینی، پرونده پزشکی و... است.

با وجود تفاوت، در ادبیات تعاریف مختلف، آنچه به چشم می‌خورد این نکته است که در هیچ کدام از تعاریف، تعریفی از واژه «پزشکی»<sup>۴</sup> به دست داده نشده است. علت این امر نیز در این نکته است که «پزشکی از راه دور» علم جدیدی نیست، بلکه شیوه و فناوری نوینی در علم پزشکی است که با ورود و گسترش کاربرد فناوری اطلاعات و ارتباطات به وجود آمده است و این امکان را فراهم آورده است که همان خدمات پزشکی که در شکل سنتی بر بالین بیمار انجام می‌گرفت در این زمان با هزاران کیلومتر فاصله صورت پذیرد.

به‌طور خلاصه و ساده، چنانچه وسایل الکترونیکی واسطه عرضه خدمات پزشکی باشند، به آن شیوه درمانی «پزشکی از راه دور» گفته می‌شود. مشاوره‌ی ساده‌ی تلفنی بین پزشک و بیمار، مشاوره‌ی پزشکی بین صاحبان حرف پزشکی، ویزیت‌های اینترنتی، نظارت بر عمل جراحی از طریق ویدئو کنفرانس، عمل جراحی پزشک

از راه دور به‌طور مستقیم توسط بازوهای مکانیکی (روبات) و حتی عمل جراحی توسط روبات با برنامه طراحی شده قبلی پزشک، همگی نمونه‌هایی از پزشکی از راه دور هستند.

تاریخچه و سیر تکامل «پزشکی از راه دور» را باید در روند تکاملی وسایل ارتباط از راه دور دید. پنج مرحله اختراع تلفن و تلگراف، رادیو، ساخت تلویزیون و امکان ارتباطات تصویری، آغاز به کار تکنولوژی‌های فضایی و ماهواره‌ای و در آخر ورود تکنولوژی دیجیتال کامپیوتر و اینترنت که انقلابی عظیم در هر زمینه‌ای را فراهم ساخت، مراحل تکامل پزشکی از راه دور است؛ زیرا با اختراع هر وسیله‌ای صاحبان حرف پزشکی از آن برای بهبود خدمات خود استفاده کردند. دسترسی بهتر و سریع‌تر به مراقبت‌های پزشکی، دسترسی به مراقبت‌های پزشکی بهتر، کاهش هزینه و آموزش بهینه بیماران و صاحبان حرف پزشکی از جمله مزایای استفاده از پزشکی از راه دور است. موانع فنی و پشتیبانی (زیرساخت‌های سخت‌افزاری و نرم‌افزاری)، مخالفت‌های سازمانی، موانع روانی و مباحث اخلاقی و حقوقی نیز در زمره محدودیت‌های رواج این تکنولوژی است.

#### بند دوم: مفهوم جرم

علمای حقوق کیفری هر یک جرم را به‌گونه‌ای تعریف کرده‌اند. هر یک از این تعاریف با تمام ژرفکاری، اغلب از گرایش‌های نظری مکتب‌های خاصی ملهم بوده است. برای نمونه مکتب عدالت مطلق، جرم را هر فعل مغایر اخلاق و عدالت تعریف کرده، یا بنا به تعریف گاروفالو، جرم عبارت است از تعرض به احساس اخلاقی بشر، یعنی جریحه‌دار کردن آن بخش از حس اخلاقی که احساسات

بنیادی، نوع خواهانه یعنی شفقت و درستکاری را شامل می‌شود (اردبیلی، ۱۳۸۲، ص ۱۱۹).

از یک دید کلی، جرم شامل رفتاری است مخالف نظم اجتماعی که مرتکب آن را در معرض مجازات یا اقدامات تأمینی، تربیتی و درمانی قرار می‌دهد. در واقع جرم رفتار مخالف نظم اجتماعی یک انسان علیه جامعه است. به جهت اینکه جامعه نمی‌تواند در قبال هر فردی که دارای حالات خطرناک است خودسرانه عکس‌العمل نشان دهد، بنابراین قانونگذار برای تعیین اعمالی که مستلزم اعمال کیفر است مداخله می‌کند. از نظر حقوقی و قضایی پدیده جزائی یا جرم مبتنی بر رفتاری است مخالف نظم اجتماعی که قانون آن را پیش‌بینی و مستوجب کیفر دانسته و اعمال یک مجازات یا اقدام تأمینی را نسبت به مرتکب آن تجویز نموده است (گلدوزیان، ۱۳۸۱، ص ۶۵).

از دیدگاه اسلام، افعالی جرم تلقی می‌شود که مغایر با احکام یا اوامر و نواهی باری تعالی باشد. این افعال در قرآن کریم به نام‌های مختلف از قبیل سوء، سیئه، اثم، جناح و... مذکور است. جناح که موضوع حدود و تعزیرات اسلامی است شامل هر فعلی ولو آنکه تنها جنبه شخصی داشته باشد یعنی مفسده آن عاید خصوص مرتکب گردد نیز می‌شود. بنابراین از این دیدگاه جرم عبارت است از رفتار خلاف مصالح و منافع فردی و اجتماعی که به منظور پیشگیری از آن مراجع قضایی ناشی از قدرت و حاکمیت، احکام الهی و کیفری تعیین کنند (گرگی، ۱۳۵۸، ص ۹۲).

در نظام حقوقی، با توجه به تعریف فوق، اگر جرم تعدی به اصول اخلاقی و شرعی تلقی شود، مفهوم عامی به دست می‌آید که آزادی اشخاص را مورد تهدید قرار می‌دهد و تعدی قضات را به همراه دارد. لیکن بنابر آیاتی همانند «و ما کتا

معدبین حتی نبعث رسولا» (سوره مبارکه اسراء، آیه شریفه ۱۵) و اصولی همچون «قبح عقاب بلا بیان» تنها فعلی، جرم است که توسط قانونگذار، جرم قلمداد و برای آن مجازات تعیین شود.

عبارت «با استناد به منابع معتبر اسلامی یا فتاوی معتبر حکم قضیه را صادر نماید» در اصل ۱۶۷ قانون اساسی<sup>۵</sup> نیز در صدد بیان آن نیست که هر عملی که در آراء فقها نامشروع تلقی شده، جرم است، بلکه قاضی تنها حق دارد با توجه به این اصل در تعیین مصادیق و مفاهیم به منابع رجوع نماید، نه آنکه آنها را به عنوان قانون مورد استفاده قرار دهد و صرفاً این منابع در تفسیر قانون کمک می‌نماید.

#### بند سوم: رابطه تله مدیسین و جرم

جرم، از منظر اخلاقی و شرعی با جرایم قابل تصور در تله مدیسین همپوشانی دارد؛ لیکن همان‌طور که بیان شد در نظام‌های حقوقی بنابر اصل قانونی بودن جرم و مجازات، (همان‌گونه که در ماده ۲ قانون مجازات اسلامی نیز به آن اشاره شده است) تنها هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد جرم محسوب می‌شود. رابطه تله مدیسین با جرم با توجه به تعریف اخیر عموم و خصوص من وجه است به این معنی که مصادیقی از سوءاستفاده‌های اشخاص از تله مدیسین با توجه به قانون فعلی جرم خواهد بود همانند شخصی که بنابر دشمنی که با بیماری دارد به وسیله تبحر خویش در وسایل جراحی الکترونیکی خللی وارد نموده، به نحوی که چنین خللی منجر به فوت بیمار شود. با توجه به ماده ۲۰۶ قانون مجازات اسلامی، وی مجرم به قتل عمدی عدوانی است و خصوصیتی در این مصداق وجود ندارد تا بتوان آن را از مصادیق قتل عمد خارج نمود.

ولی برخی دیگر از تضييع حقوق احتمالی بیماران در تله‌مدیسین، گرچه قبح آن واضح است، لیکن به دلیل فقدان قانونگذاری جامع، شخص قابل مجازات نیست همانند عدم اتخاذ تدابیر امنیتی مناسب جهت حفظ امنیت داده‌های مربوط به سلامت بیماران و یا عدم پوشش قانون در خصوص مسؤولیت کیفری پزشکانی که به وسیله‌ی سیستم‌های الکترونیکی و مخابراتی از در خطر بودن بیماران اطلاع کسب نمایند.<sup>۶</sup>

بنابراین در مبحث دوم، ضمن ذکر مصادیق سوء استفاده‌های اشخاص از تله‌مدیسین، این مقاله در پی آن است که با بیان و تفسیر قوانین موجود، برخورد نظام کیفری در مقابل این اعمال را مورد بررسی قرار دهد و متعاقب آن چنانچه قوانین فعلی مصادیقی را پاسخگو نباشند، متذکر خواهد شد.

#### مبحث دوم: مصادیق جرایم دور درمانی

تله‌مدیسین قابلیت ارتکاب جرایم علیه اشخاص، اموال و امنیت و آسایش عمومی را دارا است، که در این مبحث به بررسی ارتکاب جرایم گوناگون در فضای تله‌مدیسین پرداخته خواهد شد.

#### بند اول: سوء استفاده از پرونده‌های الکترونیکی

ماده ۸۸ قانون برنامه چهارم توسعه وزارت بهداشت را ملزم به طراحی و استقرار نظام جامع اطلاعات سلامت شهروندان ایرانی نموده و به دنبال آن ماده‌ی ۳۹ برنامه‌ی پنجم توسعه، ادامه دهنده‌ی آن گردیده است، امری که می‌تواند یکی از زیرمجموعه‌های پزشکی از راه دور باشد.



لازمه ایجاد سیستم فوق، ایجاد پرونده الکترونیک سلامت (EHR) و پرونده الکترونیک پزشکی (EMR) است. لذا ابتدا به تعاریف پرونده‌های الکترونیک پزشکی و سلامت پرداخته و سپس جرایم قابل تحقق در این زمینه بیان خواهد شد.

### الف: تعاریف پرونده‌های الکترونیک

#### ۱. پرونده‌ی الکترونیک پزشکی

در یک بیان ساده، همان پرونده‌های پزشکی کاغذی است که به روش الکترونیکی و با استفاده از زیرساخت فناوری اطلاعات ثبت و نگهداری می‌شوند. در تعریفی دیگر پرونده‌ی الکترونیک پزشکی را می‌توان داده‌های مربوط به بیماران دانست که توسط اشخاص یا مراکز ارائه دهنده خدمات پزشکی (مطب، کلینیک، بیمارستان و...) ثبت و نگهداری می‌شوند.

#### ۲. پرونده‌ی الکترونیک سلامت

چنانچه تحت یک سیستم جامع، پرونده‌های پزشکی الکترونیک که توسط مراکز مختلف درمانی جمع‌آوری شده به انضمام سایر اطلاعات مربوط به سلامت شخص از دوران جنینی تا مرگ، به صورت مرکزی و کامپیوتری جمع‌آوری شود به آن پرونده‌ی الکترونیک سلامت گفته می‌شود. اتحادیه‌ی ملی فناوری اطلاعات سلامت<sup>۷</sup>، پرونده‌ی الکترونیک سلامت را این‌گونه تعریف نموده است: «اطلاعات ثبت شده‌ی مربوط به سلامت اشخاص که توسط بیش از یک شخص یا سازمان که درگیر بهداشت و مراقبت اشخاص هستند، جمع‌آوری می‌شوند.»<sup>۸</sup>

در نتیجه، پرونده‌ی الکترونیک سلامت یک پرونده‌ی با فرمت دیجیتال است که قابلیت اشتراک داشته و تنها برای افراد و نهادهای خاصی امکان دسترسی وجود دارد. بنابر آنچه بیان شد پرونده‌ی پزشکی الکترونیک بخشی از منابع تشکیل دهنده‌ی پرونده‌ی سلامت الکترونیک است.

### ب: جرایم قابل تحقق

به رغم مزایایی نظیر کاهش هزینه‌های درمانی، بهبود کیفیت مراقبت، ارتقای دانش پزشکی و قابلیت نگهداری و انتقال پرونده‌ها و سرعت ارائه خدمات، محرمانگی و امنیت اطلاعات سلامت شهروندان از مهمترین چالش‌های حقوقی فراروی توسعه آن است. اهمیت این دغدغه‌ها به حدی است که مانع توفیق دولت انگلیس در متقاعد کردن گروهی از فعالان بخش خصوصی ارائه‌دهنده خدمات بهداشتی برای پیوستن و همکاری به لحاظ استقرار نظام جامع سلامت شده و در امریکا و آلمان نیز دیتابیس‌های سلامت مورد انتقاد قرار گرفته است.

مزایایی که برای استفاده از کامپیوتر و اینترنت نظیر امکان ذخیره‌ی انبوه اطلاعات و طبقه‌بندی آنها در حجم کم و حتی مجازی، امکان دسترسی به اطلاعات بدون توجه به بُعد مسافت از منبع آنها و... بیان می‌شود، می‌تواند از طرف دیگر، تهدیدی جدی به‌شمار آید. هرچند نقض محرمانگی و امنیت در پرونده‌های کاغذی نیز ممکن است، لیکن به دو دلیل حساسیت در مورد پرونده‌های الکترونیک بیشتر خواهد بود؛

نخست اینکه همواره در دوران گذر از انتقال یک سیستم به سیستم جدید به جهت مخالفت‌های سازمانی و روانی<sup>۱</sup> نقاط ضعف سیستم جدید بیشتر مدنظر قرار می‌گیرد و دوم اینکه گستره پرونده‌های الکترونیک از لحاظ حجم و دسترسی،

بیشتر از پرونده‌های کاغذی است بنابراین نقض محرمانگی و امنیت آن نیز در حجم گسترده‌تری صورت می‌گیرد و تهدیدی جدی‌تر به شمار می‌رود. محرمانگی، مالکیت، کنترل و دسترسی به پرونده‌های پزشکی از مهم‌ترین مباحث این حوزه است. هر چند در حقوق ایران وضعیت این مسائل به وضوح مشخص نشده است ولی در کشورهای پیشرو، این موارد به بحث و بررسی و قانونگذاری منجر شده است.<sup>۱۰</sup>

با نگاه کلی به مقررات تصویب شده درباره‌ی این مسائل می‌توان بیان داشت؛ دیدگاه اتخاذ شده‌ی غالب قوانین خارجی، مسؤلیت دارنده این داده‌ها نسبت به محرمانگی و مالکیت تهیه کننده داده‌ها بر پرونده‌های الکترونیک پزشکی را دربر دارد، لیکن بیمار حق بر محرمانه نگهداشتن این داده‌ها و دسترسی به آنها را دارد. منظور از کنترل بر این داده‌ها نیز اصلاح و تغییر داده‌های پزشکی اشخاص است که از حقوق هر دو طرف است.

امروزه اطلاعات مربوط به بیماری و سلامت اشخاص به عنوان یکی از جنبه‌های خصوصی زندگی افراد مورد پذیرش و حمایت جوامع بشری قرار گرفته و مبدل به جزئی از حریم خصوصی افراد گشته است (که نقض آن جرایم علیه اشخاص محسوب می‌شود). مجموعه‌ی پرونده‌ی پزشکی الکترونیک، مراجعان یک پزشک یا مراکز پزشکی و درمانی دیتابیس‌هایی را تشکیل می‌دهند که برای صاحبان آن داده‌ها دارای ارزش اقتصادی و تجاری است (جرایم علیه اموال). همچنین اطلاعات مربوط به سلامت افراد جامعه می‌تواند از جمله داده‌های حساس یک کشور محسوب شود که دولت‌ها تمایلی به ارائه آمار دقیق در این زمینه نداشته و تنها میل به استفاده از آنها برای سیاستگذاری در امر بهداشت کشور وجود دارد؛ زیرا

ممکن است ارائه آمار دقیق در برخی زمینه‌ها آرامش روانی کشور را تحت الشعاع قرار دهد (جرائم علیه امنیت و آسایش عمومی). بنابراین جرایم قابل تحقق مصادیق فوق، تحت سه عنوان افشای اطلاعات سلامت شخصی (جرائم علیه اشخاص)، ربایش اطلاعات پزشکی (جرائم علیه اموال) و انتشار داده‌های سرّی (جرائم علیه امنیت و آسایش عمومی) مورد بررسی قرار خواهد گرفت.

#### ۱. افشای اطلاعات سلامت اشخاص

منظور از نقض محرمانگی دستیابی افراد غیرمجاز به داده‌ها، در اختیار قرار دادن این اطلاعات برای دیگران و نهایتاً افشای داده‌های مذکور است. به دلیل عدم تصویب آیین‌نامه‌ی ذکر شده در ماده‌ی ۶۰ قانون تجارت الکترونیک<sup>۱۱</sup>، هر چند افراد واجد صلاحیت برای دسترسی به اطلاعات پزشکی و بهداشتی نامشخص است؛ لیکن بدون توجه به مصادیق افراد صالح، ضمانت اجرای کیفری دسترسی غیرمجاز و نقض محرمانگی داده‌ها مورد بررسی قرار می‌گیرد. هر چند در قانون مجازات اسلامی درباره‌ی حمایت از حریم خصوصی اطلاعاتی، بحثی به میان نیامده، اما در قانون تجارت الکترونیک و قانون جرم رایانه‌ای مقرراتی در این باب بیان شده است. قانون تجارت الکترونیک در فصل سوم و تحت عنوان حمایت از داده‌ها، ذخیره، پردازش و توزیع داده‌های سلامت را مشروط به رضایت صریح شخص و رعایت اصولی نموده و در ماده‌ی ۷۱ همین قانون ضمانت اجرای نقض آن را بیان نموده است.

علاوه بر این قانون جرایم رایانه‌ای نیز به‌طور کلی انتشار یا در دسترس غیر قرار دادن اسرار دیگران به‌وسیله سیستم‌های رایانه‌ای و مخابراتی را (بدون کسب

رضایت) که منجر به ضرر یا عرفاً باعث هتک حیثیت وی گردد، جرم و مستحق مجازات دانسته است. (ماده ۱۷) و به‌طور یقین اطلاعات مربوط به سلامت و بیماری افراد از جمله اطلاعاتی است که افشای آن موجب ضرر وی گردیده و در مورد بیماری‌های خاص هتک حیثیت را به دنبال خواهد داشت، این نقض ممکن است توسط افراد مجاز و غیرمجاز به دسترسی اتفاق بیفتد. علاوه بر انتشار، نفس دسترسی و یا شنود این داده‌ها برای افراد غیرمجاز به علت غیرعمومی بودن این اطلاعات و ارتباطات مشمول جرمی جداگانه خواهد بود (مواد ۱ و ۲ قانون جرایم رایانه‌ای).

جمع‌آوری پرونده‌های الکترونیکی پزشکی بیماران یک حق و یک تکلیف را برای صاحبان حرف پزشکی به دنبال دارد. قبل از بیان حقوق مالکانه‌ی صاحبان پرونده‌ی پزشکی<sup>۱۲</sup> به بررسی تکلیفی که برعهده آنان وجود دارد پرداخته می‌شود. هر چند داده‌های پزشکی جزء اموال تهیه‌کنندگان آن است، ولی این حقوق مالکانه مطلق نبوده، بنابراین صاحبان آن حق کامل تصرف و انتفاع و یا به قول حقوق‌دانان رومی «حق استعمال»، «حق استئمار» و «حق اخراج از ملکیت» را به‌طور مطلق ندارند. قانونگذار نیز برای انتقال و افشای این داده‌ها توسط صاحبان حرف پزشکی مجازات مقرر نموده است (ماده ۶۴۸ قانون مجازات اسلامی).

علاوه بر آن به علت حساسیت بالای این اطلاعات این تکلیف برای تهیه‌کننده وجود دارد که برای حفظ و امنیت این داده‌ها تدابیر معقولانه‌ای را به کار برد تا امکان دسترسی و تهدیدات ناشی از اعمال خاطیان کاهش یابد. با وجود اهمیت بحث در این زمینه و تکلیف مهم به‌طور خاص قوانین جزایی بدان نظر نداشته و بدلیل مالکیت تهیه‌کنندگان پرونده‌ی پزشکی حتی بیمارانی متضرر، نمی‌توانند به

ماده‌ی ۶۷۴ قانون مجازات نیز تمسک جویند (زیرا ماده فوق ناظر به خیانت در امانت است) و تنها باید چشم به قوانین مسؤولیت مدنی داشته باشند. در برخی کشورها همانند استرالیا نه تنها قانونگذار عدم رعایت موارد امنیتی توسط پزشک در ذخیره، پردازش و انتقال داده را جرم‌انگاری نموده بلکه رعایت نکردن تناسب اهمیت اطلاعات و شیوه‌های امنیتی را مستوجب مجازات دانسته است، توضیح آنکه در مواردی همچون حفظ اطلاعات پرونده‌ی اشخاص مبتلا به ایدز، صرف استفاده از شیوه‌های ابتدایی امنیتی (که متناسب برای حفظ نتایج مشاوره‌های پزشکی محسوب می‌شود)، پزشک را از مسؤولیت کیفری مبرا نمی‌نماید، بلکه وی ملزم به استفاده از شیوه‌هایی با امنیت بالا، نظیر رمزنگاری (متقارن و نامتقارن) است (اسمیت، ۱۹۹۷، ص ۶).

## ۲. ربایش اطلاعات پزشکی

همان‌طور که سابق اشاره شد مالک پرونده‌های پزشکی تهیه‌کنندگان آنند و حق مالکیت نسبت به آن دارند. بنابراین پرونده‌ی پزشکی جزء اموال وی محسوب گردیده و باید تحت احترام و حمایت قرار گیرد. امروزه با توجه به تعریف و دیدگاه جدیدی که نسبت به مال وجود دارد، دیگر تردیدی در شناسایی اطلاعات (اگر دارای ارزش اقتصادی باشد) به عنوان مال وجود ندارد. بنابراین دیتابیس‌های مربوط به اطلاعات بیماران و بیماری‌های آنان جزء اموال پزشک یا مراکز درمانی است که آنها را جمع‌آوری نموده است. این اطلاعات علاوه بر اینکه برای صاحبان آن جزء اسرار تجاری محسوب می‌گردد دستیابی به آنها برای سایر رقبا و برخی از مراکز، دارای ارزش اقتصادی است. برای مثال تولیدکنندگان محصولات و ارائه‌دهندگان خدمات پزشکی با کمک این

دیتابیس‌ها جامعه هدف خود را به راحتی شناسایی نموده و مستقیم با آنان در ارتباط قرار می‌گیرند.

امری که امروزه در فضای مجازی برخی با استفاده از برنامه‌های کوکی و ویروس‌های ساکر<sup>۱۳</sup> به دنبال آن هستند (وارنی، ۱۹۹۶، ص ۲۴).

با توجه به مطالب فوق، ناقضان حقوق فوق تحت عناوین ذیل قابل مجازاتند.

قانون مجازات اسلامی در ماده ۱۹۷ سرقت را «ربودن مال دیگری به‌طور پنهانی» تعریف نموده است. تعریفی که می‌تواند مصداق فوق را نیز دربر گیرد. تنها تفاوت ربایش دیتا با سایر اموال مادی در این است که در ربایش اموال مادی، ربودن باعث خروج تسلط و دسترسی صاحب مال به آن است، ولی در ربایش اطلاعات این امکان وجود دارد که اطلاعات بدون خروج از دسترسی صاحب آن در اختیار غیر قرار گیرد. لیکن مطابق آنچه در قانون مجازات اسلامی بیان شده به‌طور عام ربایش اطلاعات در فضای مجازی نیز مشمول سرقت اعم از حدی و غیرحدی قرار می‌گیرد. در فصل دوم قانون تجارت الکترونیکی با عنوان حمایت از اسرار تجاری، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی را جرم دانسته و در تعریف اسرار تجاری الکترونیکی آن را شامل داده‌هایی می‌داند که به‌طور مستقل دارای ارزش اقتصادی بوده و در دسترس عموم قرار ندارد و تلاش‌های معقولانه‌ای برای حفظ و حراست از آنها انجام گرفته است. (مواد ۶۴ و ۶۵) و متعاقب آن در ماده ۷۵ به بیان ضمانت اجرای کیفری ناقضان پرداخته است. بالاخره قانون جرایم رایانه‌ای به‌طور خاص پس از تعریف یک نوع از سرقت رایانه‌ای در ماده ۱۲ مجازات آن را ذکر نموده است.<sup>۱۴</sup>

## ۳. انتشار داده‌های سری

تشکیل پرونده‌ی الکترونیک سلامت شهروندان و تمرکز اطلاعات سلامت آنان تشکیل دهنده‌ی مجموعه‌ای است که حفظ و محرمانگی اطلاعات آن برای دولتمردان از اهمیت بسزایی برخوردار است؛ زیرا از یک سو افشای برخی آمار اثرات سوئی را برای جامعه در پی دارد و از سوئی دیگر دستیابی به این منبع اطلاعاتی می‌تواند یک رانت اطلاعاتی برای فعالان عرصه سلامت در داخل و خارج از کشور باشد. قانون مجازات اسلامی در فصل اول کتاب پنجم خود به جرایم ضد امنیت داخلی و خارجی کشور پرداخته است. امنیت مفهوم عامی است که شامل امنیت سیاسی، نظامی، اقتصادی، بهداشتی، روانی و... می‌باشد.

در مورد پرونده سلامت شهروندان، دسترسی اشخاص غیرمجاز و انتشار اطلاعات موجود در آن تهدیدی برای امنیت روانی کشور محسوب می‌شود. امری که علاوه بر قانون مجازات اسلامی در قانون جرایم رایانه‌ای نیز مورد اشاره قرار گرفته است. تبصره ۱ ماده ۳ قانون جرایم رایانه‌ای داده‌های سری را داده‌هایی می‌داند که افشای آن به امنیت کشور یا منافع ملی لطمه می‌زند. بنابراین پرونده الکترونیک سلامت جزء این گروه است که خاطیان و متجاوزان این حوزه را تحت شمول مواد ۳ و ۴ قانون قرار می‌دهد.

علاوه بر مسائل جاسوسی و امنیتی پرونده الکترونیک سلامت، رانت اطلاعاتی ناشی از این پرونده‌ها که ممکن است توسط افراد مجاز به دسترسی داده‌ها مورد سوء استفاده قرار گیرد نیز مسأله‌ای قابل تأمل است. امری که با وجود نیاز مبرم جامعه به‌طور واضح مقنن به وضع مقررات راجع به استفاده کنندگان رانت اطلاعاتی به‌طور کلی و در این حوزه خاص نپرداخته است.<sup>۱۵</sup> هر چند هیأت وزیران در قسمت «ز» بند ۲ «برنامه ارتقاء سلامت نظام اداری و مقابله با فساد»



در سال ۱۳۸۲ وزارت اطلاعات و وزارت دادگستری را ملزم به تهیه لایحه تشدید مجازات سوء استفاده‌کنندگان از اطلاعات منتشر نشده و نیز افشای غیرقانونی اطلاعات اشخاص نزد دستگاه‌های مختلف نموده بود. امری که در غالب کشورهای پیشرفته دنیا جرم‌انگاری شده است؛ مثلاً آلمان بر مبنای قانون مصوب سال ۱۹۹۴ مجازات زندان پنج‌ساله و پرداخت جریمه نقدی معادل ۳ میلیون مارک را در نظر گرفته. آفریقای جنوبی بر مبنای قانون مستقیم مصوب سال ۱۹۹۸ پرداخت حداکثر ۲ میلیون راند و ۱۰ سال زندان را در نظر گرفته. در آمریکا در سال ۱۹۸۴ به پرداخت مبلغی معادل سه برابر سود کسب شده یا زیان متحمل نشده (زیانی که در صورت عدم دسترسی به اطلاعات متحمل می‌شد) ناشی از این‌گونه معاملات محکوم می‌شوند.<sup>۱۶</sup>

#### بند دوم: مسائل ناشی از جعل عناوین پزشکی

بنا به حساسیت موجود در حِرَف پزشکی کشورها مقررات خاصی را برای اشتغال به این مشاغل وضع و نظارت ویژه‌ای بر آن دارند. در فضای مجازی که ترکیبی از اطلاعات قابل اعتماد و غیرقابل اطمینان است ادعای داشتن مهارت و حرفه خاص، امر دشواری به نظر نمی‌رسد. جدای از بحث علم بزه‌دیده‌شناسی که یکی از علل جرم را قصور بزه‌دیده می‌داند، در این مقاله تنها به بیان مسؤولیت جاعل عنوان پرداخته خواهد شد.

بنابر ماده‌ی ۵۲۳ قانون مجازات اسلامی «جعل و تعزیر عبارتند از: ساختن نوشته یا سند یا ساختن مهر یا امضای اشخاص رسمی یا غیررسمی خراشیدن یا تراشیدن یا... به کار بردن مهر دیگری بدون اجازه‌ی صاحب آن و نظایر اینها به قصد تقلب»

در زمینه‌ی جعل عنوان پزشکی باید دو مصداق را از یکدیگر تفکیک کرد. مورد اول در مواردی است که شخصی با نشان دادن مدارک تقلبی و جعلی به وسیله‌ی وسایل الکترونیکی خود را پزشک معرفی می‌نماید. در این فرض بنابر ماده‌ی فوق و همچنین ماده‌ی ۶ قانون جرایم رایانه‌ای<sup>۱۷</sup> شخص بنابر قوانین کلی درباره‌ی به جعل قابل مجازات است و جعل الکترونیکی در این مصداق خصوصیتی ندارد تا فاعل آن قابل مجازات نباشد. لیکن در خصوص مورد دو یعنی هنگامی که شخص بدون ارائه مدرکی خود را پزشک معرفی و اقدام به فعالیت‌های پزشکی نماید، ضمانت اجرایی وضع نشده است. این در حالی است که در برخی از کشورها نه تنها برای این دسته از افراد مجازات وضع شده، برای آن دسته از پزشکانی که خارج از حوزه خود به عنوان پزشک صلاحیت دار اقدام به مشاوره، معاینه، عمل جراحی و... نیز می‌نمایند مسؤولیت کیفری در نظر گرفته شده است (اسمیت، ۱۹۹۴، ص ۵۸).

ولی در نظام حقوقی ایران از قوانین جزایی برای جعل عناوین غیردولتی جرمی لحاظ نشده، مگر آنکه جاعل مرتکب جرم دیگری شود که تحت همان عنوان جزایی مجازات می‌گردد.

برای مثال شخصی که عنوان پزشکی را جعل نماید، اگر چه از جهت جرم جعل قابل پیگرد نیست، اگر بدین وسیله مالی را از بیماران اخذ نماید، می‌تواند در قالب جرم کلاهبرداری تحت تعقیب کیفری قرار گیرد.

#### بند سوم: مسائل ناشی از اقدامات هکر، مخربان و تروریسم

هکرها کسانی هستند که غیرمجاز به اطلاعات کامپیوتری دسترسی پیدا می‌کنند و براساس قوانین ایران قابل مجازات هستند. (ماده‌ی ۱ و ۲ قانون جرایم رایانه‌ای)

اگر بعد از دسترسی به داده‌ها خساراتی به اطلاعات وارد نمایند، عنوان مخرب به آنها اطلاق خواهد شد و همچنین اگر در پی مقاصد سیاسی خویش باشند تروریست محسوب می‌شوند.

اقدامات اشخاص فوق می‌تواند دربر گیرنده‌ی جرایم متنوعی باشد. اولین مورد از بین بردن اطلاعات جمع‌آوری شده‌ی مربوط به سلامت مراکز درمانی است که خود به چند شیوه صورت می‌گیرد. خرابکاران یا با استفاده از توانایی‌های خویش داده‌ها را از بین می‌برند یا آنکه در ماهیت آن تغییر ایجاد می‌نمایند (اختلال در تمامیت و صحت داده‌ها) (ماده‌ی ۸ قانون جرایم رایانه‌ای).

برای مثال درباره‌ی تخریب داده‌ها می‌توان به از بین بردن تحقیقات ده ساله‌ی کشور ایتالیا در خصوص اطلاعات جمع‌آوری شده‌ی ایدز توسط مخربان اشاره کرد (کلاگ، ۱۹۹۲، ص ۱۴۱).

دومین مورد اختلال در سیستم‌های الکترونیکی و رایانه‌ای است. امروزه پزشکی از راه دور این امکان را فراهم نموده است که اعمال جراحی از طریق ویدئو کنفرانس، بازوهای مکانیکی هدایت شونده توسط پزشک معالج از فواصل دور و یا به کمک ربات‌های هوشمند با برنامه‌ی تنظیمی در حافظه‌ی آن صورت گیرد. در این میان مخربان با ایجاد اختلال در سیستم‌های الکترونیکی می‌توانند مانع انجام عمل جراحی شوند. برای مثال در استرالیا شخصی، عمل جراحی را به دلیل اخذی از مسئولان بیمارستان به تأخیر انداخت (چیانگ، ۱۹۹۷، ص ۴۴). در قانون جرایم رایانه‌ای نیز این امر مورد اشاره قرار گرفته است (ماده‌ی ۹).

و سومین خطری که ممکن است فعالان پزشکی از راه دور با آن مواجه گردند، هنگامی است که مخربان با انجام دادن اقداماتی مانع دسترسی آنان به داده‌های پزشکی و سلامت در جریان روند سلامت بیمار گردند. (ماده‌ی ۱۰) برای نمونه

می‌توان به شخصی اشاره نمود که با دستیابی به سیستم کامپیوتر بیمارستانی و ممانعت از دسترسی پزشکان معالج به اطلاعات طبقه‌بندی شده‌ی بیمار، عمل جراحی را شش روز به تأخیر انداخت (دای، ۱۹۹۶، ص ۲۷).

### نتیجه

نتایج به دست آمده از این مطالعه نشان می‌دهد، هر چند در بسیاری از موارد، جرایم جدید ناشی از دور درمانی، چهره‌ی نوینی از جرایم قدیمی با همان ماهیت است، ولی به نظر می‌رسد برای حمایت از حقوق بیماران راهی به جز وضع قوانین و مقررات جدید متناسب با طبیعت این جرایم که در محیط مجازی صورت می‌گیرد وجود ندارد.

علت اصلی عدم تکافوی مقررات نظام حقوقی ایران در پزشکی از راه دور، عدم غنای قانونی در دو زمینه تشکیل‌دهنده تله‌مدیسین، یعنی پزشکی و فناوری اطلاعات و ارتباطات است. بنابراین لازم است برای رفع نقایص قانونی در این زمینه به جهت اهمیت موضوع، قوانین خاصی وضع گردد، بدین ترتیب که ابتدا قانونگذار با پیش‌بینی مصادیق مجرمانه‌ی این رشته (همانند جعل عنوان پزشکی) به وضع قوانینی جامع بپردازد و سپس در آیین‌نامه‌ای، نحوه‌ی ذخیره، پردازش و انتقال داده‌های سلامت اشخاص تعیین شده و مسائلی نظیر مجرمانگی، دسترسی، مالکیت و... تبیین گردد.

## پی‌نوشت‌ها

1- <http://www.healthcareitnews.com>

2- Thomas Bird

۳- تله‌مدیسین این پتانسیل را دارد که زندگی هر آمریکایی را تغییر دهد. در مناطق روستایی دورافتاده جای که یک بیمار و نزدیک‌ترین صاحبان حرف پزشکی با حدود صدها مایل فاصله از هم می‌توانند ارتباط برقرار کنند، تله‌مدیسین می‌تواند به معنی دسترسی به مراقبت‌های بهداشتی در جاهایی باشد که قبلاً کمتر در دسترس بوده است.

4- Medicine

۵- «قاضی موظف است کوشش کند حکم هر دعوا را در قوانین مدونه بیابد و اگر نیابد با استناد به منابع معتبر اسلامی یا فتاوی معتبر، حکم قضیه را صادر نماید و نمی‌تواند به بهانه‌ی سکوت یا نقص یا اجمال یا تعارض قوانین مدونه، از رسیدگی به دعوا و صدور حکم امتناع ورزد.»

۶- با توجه به عبارت «اگر مرتکب از کسانی باشد که به اقتضای حرفه خود می‌توانسته کمک مؤثری بنماید به حبس ... محکوم خواهد شد» قانون مجازات خودداری از کمک به مصدومان و رفع مخاطرات جانی مصوب ۱۳۵۴ تنها پزشکانی مسؤول کمک به مصدومان و مجروحان هستند که اشخاص در معرض خطر را مشاهده نمایند نه آنکه از وقوع چنین خطری اطلاع پیدا نمایند.

7- NAHIT.

8- <http://www.ehealth-hoda.ir>

9- Techno phobia.

10- E.g. USA: Health Insurance Portability and Accountability Act (HIPAA); Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

۱۱- ماده ۶۰: «ذخیره، پردازش و یا توزیع داده پیام‌های مربوط به سوابق پزشکی و بهداشتی تابع آیین‌نامه‌ای است که در ماده‌ی (۷۹) این قانون خواهد آمد.» و ماده ۷۹ بیان داشته: «وزارت بازرگانی موظف است زمینه‌های مرتبط با تجارت الکترونیکی را که در اجرای این قانون مؤثر می‌باشند شناسایی کرده و با ارائه پیشنهاد و تأیید شورای عالی فناوری اطلاعات، خواستار تدوین مقررات مربوطه و آیین‌نامه‌های این قانون توسط نهادهای ذی‌ربط شود. این آیین‌نامه‌ها و مقررات پس از تصویب هیأت وزیران به مرحله اجرا درخواهند آمد. سایر آیین‌نامه‌های مورد اشاره در این قانون به ترتیب ذیل تهیه خواهند شد: ...»

ج - آیین‌نامه‌ی مربوط به ماده‌ی (۶۰) این قانون به پیشنهاد وزارت بهداشت، درمان و آموزش پزشکی و سازمان مدیریت و برنامه‌ریزی کشور تهیه و به تصویب هیأت وزیران خواهد رسید.

۱۲- به جهت آنکه بحث از حقوق مالکانه‌ی پزشک، مرتبط با جرایم علیه اموال است در قسمت بعدی به آن پرداخته خواهد شد.

13- Sucker Lists

۱۴- این ماده اشعار می‌دارد: «هر کس به‌طور غیرمجاز داده‌های متعلق به دیگری را بریاید، چنان‌چه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۱۵- البته می‌توان ارائه‌دهندگان این رانت‌ها را تحت عناوینی تحت تعقیب قرار داد (برای مثال با تفسیری از ماده ۶۰۴ قانون مجازات اسلامی و بند ب ماده ۳ قانون جرایم رایانه‌ای)

16\_ www.acclearn.com

۱۷- ماده‌ی ۶: «... الف) تغییر داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه‌ی داده‌ها»

#### فهرست منابع

##### الف: کتب فارسی

- اردبیلی، محمد علی - (۱۳۸۲). حقوق جزای عمومی، ج اول، چ ۴، تهران، نشر میزان  
کاتوزیان، ناصر - (۱۳۸۲). حقوق مدنی اموال و مالکیت، چ ۷، تهران، نشر میزان  
گرچی، ابوالقاسم - (۱۳۵۸). حقوق جزای عمومی اسلام، نشریه‌ی موسسه‌ی حقوق تطبیقی، ش ۶  
گلدوزیان، ایرج - (۱۳۸۱). بایسته‌های حقوق جزای عمومی، چ ۶، تهران، نشر میزان

##### ب: قوانین

- قانون تجارت الکترونیک  
قانون جرایم رایانه‌ای  
قانون مجازات اسلامی

##### ج: منابع انگلیسی

- Cheong, I.R.& Kidd, M.R, 1997, Safe practices in cyberspace: A medical perspective on computer viruses, Medical Journal of Australia, vol. 166.  
Clough, B & Mungo, P (1992), Approaching Zero: Data Crime and the Computer Underworld, Faber and Faber, London.  
Day, K. (1996), Defending yourself and your organization from information warfare, paper presented to the information warfare and competitive intelligence conference.  
Smith, R.G.(1994), Medical Discipline: The professional Conduct Jurisdiction of the General Medical Council, 1858-1990, Clarendon Press, Oxford.

- Smith, Russell G. (1997), telemedicine and crime, Australian Institute of Criminology.
- Varney, C. (1996), Regulating cyberspace: An off the record interview with Federal Trade Commissioner Christine Varney, Computer Underground Digest.

د: منابع اینترنتی

<http://www.acclearn.com/forum/index.php?topic>

<http://www.healthcareitnews.com>

<http://www.ehealth-hoda.ir>

<http://www.orthosupersite.com>

<http://www.itiran.com>

#### یادداشت شناسه‌ی مؤلف

عباس کریمی، استاد گروه حقوق خصوصی دانشکده‌ی حقوق و علوم سیاسی دانشگاه تهران

ایمان رحیمی پور، دانشجوی دکترای حقوق کیفری و جرم‌شناسی دانشگاه تربیت مدرس

نشانی الکترونیکی: [iman.rahimipoor@gmail.com](mailto:iman.rahimipoor@gmail.com)

مهدی حسینی، دانشجوی کارشناسی ارشد حقوق خصوصی دانشگاه مفید قم

تاریخ وصول مقاله: ۱۳۸۸/۱۲/۲۰

تاریخ پذیرش مقاله: ۱۳۸۹/۳/۱۳