امنیت سایبری فضای مجازی با نگرشی بر سامانه های دارویی

بابک پورقهرمانی

دانشیار گروه حقوق کیفری و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران (نویسنده مسئول)

b.pourghahramani@yahoo.com

امیرحسین زیورپور

دانشجوی دکتری تخصصی حقوق کیفری و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

Amirhosein.Zivarpour.iau147@gmail.com

چکیده

زمینه و هدف: امروزه صنعت دارو به عنوان یکی از صنایع کلیدی و راهبرد در جهان مطرح است، دارو به دلیل اثرگذاری بر سلامت انسان ها و جوامع بشری همواره از مهم ترین ارکان چرخه سلامت بوده است. بر همین اساس همواره تدارک و تأمین داروی مورد نیاز جامعه حتی در بحرانی ترین شرایط کشور از اولویت خاص دولت هاست. تحول اطلاعات و گسترش روز افزون استفاده از رایانه و اینترنت در تمامی ابعاد زندگی بشر و نیاز شرکت ها، سازمان ها، گروه ها به آن سبب وقوع جرایم مختلفی در فضای مجازی شده است. فضای مجازی با ویژگی های خود مانند فراملی بودن، تعدد بازیگران، مخفی بودن سبب شده افراد وارد این فضا شوند و بدون اینکه به راحتی مورد شناسایی واقع شوند جرایم مختلفی را مرتکب شوند.

روش تحقیق: مطالعه حاضر از نوع توصیفی-تحلیلی می باشد که به بررسی ادبیات موجود در زمینه امنیت فضای مجازی می پردازد. روش گرداوری اطلاعات در این مطالعه، از نوع کتابخانه ای می باشد.

یافته‌ها: در این فضای مجازی اما واقعی و حقیقی جرایم مختلفی مانند سرقت، کلاهبرداری، جعل، جاسوسی به وقوع می پیوندد. برخی از این جرایم سبب آسیب و صدمه زدن به حریم خصوصی افراد در زمینه های درمانی و به خصوص دارویی شده و به عنوان تهدیدی علیه امنیت داده ها محسوب می گردد. برخی دیگر از این جرایم صدمات مالی و اقتصادی وارد می کند و برخی نیز به عنوان تهدید و آسیبی علیه اشخاص می باشد. امنیت داده های هر کشوری یکی از نگرانی های دولت ها می باشد که در صدد تأمین امنیت داخلی و خارجی گام برمی دارند.

نتیجه‌گیری: در جهت مقابله با دستیابی غیر مجاز داده ها و جرایمی که بوسیله وسایل الکترونیکی و به شیوه پیشرفته به وقوع می پیوست، توسط قانونگذار آیین نامه ها و قوانینی وضع گردید تا بدینوسیله راه را برافرادسودجو ببندد و موجبات امنیت داده ها فراهم گردد.

کلید واژه‌ها: امنیت، فضای مجازی، تهدید امنیت، سامانه های دارویی.

مقدمه

ورود رایانه به زندگی بشری و استفاده روزافزون از این وسیله شگفت انگیز سبب بوجود آمدن دگرگونی وتحولات گسترده در حیطه اطلاعات گردیده است. رایانه با ویژگی های منحصر به فرد خود مانند حجم بالای اطلاعات، دسترسی سریع و آسان به اطلاعات و ویژگی های متنوع و فراوان دیگری توانسته است، امکانات بی شماری را در اختیار افراد قرار دهد. همین امر سبب بوجود آمدن جرایم متنوع و مختلفی شده است که در مقایسه با جرایم کلاسیک می تواند آسیب های جبران ناپذیر وخطرناکی را به همراه داشته باشد. محیط فضای مجازی به مجرمین این امکان را می دهد که در فضایی به دور از دیدگان مردم به راحتی و در محیطی امن دست به ارتکاب جرم بزنند. امروزه با توجه به افزایش روز افزون استفاده کنندگان از اینترنت میزان جرایم سایبری نیز سیر صعودی به خود گرفته است. از آنجا که این گونه جرایم در سطح ملی و حتی فراملی رخ می دهد پس می توان گفت برای اینگونه جرایم حد و مرزی وجود ندارد. کاربران در این محیط به ایجاد تغییراتی در داده ها و اطلاعات زده که همین امر نشانگر وقوع جرمی می باشد. مخفی بودن این محیط امکان تعقیب و شناسایی مجرمین را کاهش داده است. پس هر شخص به راحتی در هر نقطه از جهان می تواند در گوشه ای دیگر از جهان جرمی را مرتکب شود. همین امر موجب گردیده است که جهت تأمین امنیت داده ها وسیستم های رایانه ای قوانین و مقرراتی وضع گردد. به دلیل تنوع و گستردگی اینگونه جرایم کشف و مقابله با آنها لازم و ضروری می باشد. به همین دلیل است که تمام حقوق دانان وجرم شناسان به دنبال شناسایی ماهیت اینگونه جرایم بر آمدند.

توسعه پدیده جهانی فناوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد مختلف حیات اقتصادی، اجتماعی، فرهنگی سیاسی و امنیتی ایجاد نموده است. انقلاب الکترونیک تبدیل به مهمترین پدیده تعیین کننده معاصر شده است. روزانه ده ها هزار رایانه ورود خود را به دنیای جدید اعلام می کنند. ظهور شبکه ها به معنای تهدید بزرگ حریم اطلاعاتی و رابطه افراد در مقایسه با فنون قبلی ارتباطات است که ناشی از دسته بندی و ادغام پروندهها و قابلیت ردگیری کارهای روزانه افراد است. این به معنای بوجود آمدن ارزشی ضد ارزش در دسترس بودن در هر مکان و زمان است که به وسیله آن می توان رد افراد را تا عمیق ترین زوایای جامعه گرفت. یکی از نگرانیهای اساسی در مورد اینترنت حفظ حریم شخصی افراد و امنیت داده ها است اطلاعات گوناگون که درباره داده ها نگهداری می شود از طریق نفوذ به این سیستم ها امکان سوء استفاده و ایجاد خطر را برای شهروندان به دنبال خواهد داشت. به طور خاص اطلاعاتی که می تواند محرمانه یا شخص تلقی شود و امکان افشای آن از طریق اینترنت هست عبارتند از : علائم تجاری، روابط جنسی، امور مذهبی و سیاسی، اطلاعات پزشکی و مالی یا امنیتی. این اطلاعات که به دلایل مختلف و برای سهولت دسترسی به آنها و یا انتقال به دیگران از سوی شبکه های رایانه ای حفظ می شود به راحتی می تواند در اختیار افراد غیرصالح قرار بگیرد و با افشای آن ضررهای هنگفتی به مال یا آبروی افراد واردآید. امروزه علاوه بر نظارت هایی که به مدد فناوری اطلاعات در مورد امور شخصی مردم اعمال می شود، اطلاعات خصوصی گردآوری شدهٔ آنان یا دربارهٔ آنان نیز می تواند دستخوش تهدید و نقل و انتقال های کینه توزانه و زیان بار شود.

در میان صنایعی که تجزیه و تحلیل دادهها در آنها در مقیاس گسترده اجرا می‌شوند، صنعت مراقبت‌های بهداشتی و دارویی دارای موقعیت پیشرو است. داده‌های بهداشتی پیچیده است و بازیکنان زیادی دارد که نیاز به هماهنگی دارند. حفظ حریم شخصی دادهها یک مسئله حیاتی برای مراقبت‌های بهداشتی است و محدویت‌های دسترسی به آن‌ها می‌تواند مانع اصلی پیشرفت در تحقیق برای درمان بیماری و مراقبت از بیمار باشد. ذخیره‌سازی اطلاعات پزشکی بیماران در مراقبت‌های بهداشتی بسیار مهم است. این اطلاعات بسیار حساس هستند و همچنین یک هدف اصلی برای حملات سایبری می‌باشند. مهم است که همه اطلاعات حساس، ایمن نگه داشته شوند. خرابکاری و نقض امنیت داده‌های مبهم و تقسیم شده، ارتباطات با تأخیر و ابزارهای مختلف گردش کار ناشی از عدم قابلیت همکاری رنج می‌برند. با این حال، محققان مراقبت‌های بهداشت و سلامت با داده‌های مبهم و

مختلط، ارتباطات تأخیری و ابزارهای مختلف گردش کار مبارزه می‌کنند. سیستم کارآمد و مؤثر مراقبت‌های بهداشتی نیاز به قابلیت همکاری دارد که به برنامه‌های کاربردی نرم‌افزاری و سیستم عامل‌های فناوری اطلاعات اجازه می‌دهد به طور ایمن و یکپارچه ارتباط برقرار کنند، داده‌ها را مبادله کنند و از اطلاعات مبادله شده بین سازمان‌های بهداشتی و فروشندگان برنامه استفاده کنند. فن‌آوری اطلاعات یک سیستم ایجاد پایگاه داده غیرقابل تغییر، امن و توزیع شده از معاملات است. فناوری اطلاعات در ابتدا برای ایجاد یک فهرست توزیع شده از معاملات مالی که بر بانک مرکزی، شرکت اعتباری و یا سایر مؤسسات مالی متکی نبودند، ایجاد شد و این فناوری از طریق انجام معاملاتی در زمینه‌ی مسائل حقوقی، پرونده پزشکی، صورتحساب بیمه و قراردادهای هوشمند توسعه داده شده است.

یکی از قوانین مهم بخش سلامت قانون مربوط به مقررات امور دارویی است که در سال ۱۳۳۴ به تصویب مجلس رسیده است. این قانون که شامل بیست و پنج ماده است ساز و کار امور پزشکی اعم از ایجاد مؤسسات پزشکی، شرایط و مقررات مربوط به پروانه‌های پزشکی، نحوه اداره امور آزمایشگاه‌ها، داروخانه و مراکز تصویربرداری و تجهیزات و ملزومات پزشکی، شرایط ساخت، ورود و فرآورده‌های زیست‌شناختی (بیولوژیک) و فرآورده‌های آزمایشگاه‌ی و صلاحیت مؤسسات تولیدکننده مواد مزبور و تشکیل کمیسیون‌های قانونی برای صدور پروانه‌ها و نحوه نظارت بر مؤسسات پزشکی را معین می‌سازد. این قانون با توجه به تغییر شرایط امور پزشکی بارها توسط مجلس مورد اصلاح قرار گرفته است گرچه این اصلاحات در جهت تکمیل و به‌روز کردن قانون مزبور بوده است. تدوین قوانین دارویی توسط وزارت بهداشت درمان و آموزش پزشکی انجام می‌گیرد، این سازمان باید با توجه به اینکه دارو پایه و محور اساسی و در بسیاری از موارد نقطه نهایی کل عملیات بهداشتی و درمانی و چرخه نظام سلامت را کامل می‌کند، مقرراتی برای آموزش، تولید، واردات، عرضه و مصرف، حفظ و ارتقاء شاخص‌های سلامت و عدم آسیب‌پذیری جامعه تدوین و فراهم کند. قوانین دارویی باید افرادی را که به نوعی با دارو مرتبط هستند از جمله پزشکان، واردکنندگان، سازندگان، توزیع-کنندگان، داروسازان و مصرف‌کنندگان را نیز معین و شرایط و ضوابط رسیدن به کیفیت مطلوب را تعیین کند. مطالعه حاضر به بررسی امنیت داده ها در فضای مجازی در حوزه سامانه های دارویی می پردازد.

چهارچوب نظری

امروزه فناوری اطلاعات تنها محدود به مرزهای جغرافیایی سرزمین ها و در سطح ملی نمی باشد. بلکه یکپارچگی میان سیستم های اطلاعاتی و مخابراتی امکان ذخیره سازی اطلاعات و ارتباطات را در سطح فراملی و بین المللی امکان پذیر ساخته است و همین امر سبب سوءاستفاده و به وجود آمدن جرایم مختلفی در فضای سایبری شده است. از جمله جرایم علیه محرمانگی، تمامیت، دسترسی پذیری سیستم ها و یا شبکه ها می باشد. پس دیگر نمی‌توان مانند گذشته جرایم را منحصر به جرایم مندرج در قانون مجازات اسلامی دانست که بیشتر به بررسی جرایم کلاسیک و سنتی می پرداختند، بلکه با گذشت زمان و استفاده روز افزون از اینترنت جرایمی به وجود آمدند که مصداق و عنوان مشخصی در قانون برای آن وجود نداشت (اکبری و همکاران، ۱۴۰۱، چگینی، ۱۳۹۹). لذا جهت تأمین امینت داده ها و محافظت از اطلاعات شخصی افراد، قانونگذار با تصویب قوانین خاص در جهت حمایت از امنیت داده ها و حریم خصوصی و ارتباطات اشخاص راه را برای سوء استفاده افراد سودجو ببندد (آزادی، ۱۳۹۷). مجموعه قوانین و مقرراتی که توسط قانون گذار در جهت حمایت از داده ها و سیستم های رایانه ای کاربران وضع گردید تا موجبات امنیت ملی فراهم شود، در این فصل به تجزیه و تحلیل جرایم مندرج در قانون «جرایم رایانه ای » به معنای خاص و به طور کامل که در سال ۱۳۸۸ توسط مجلس شورای اسلامی به تصویب رسید می پردازیم. جرایم سایبری نه تنها به عنوان تهدیدی علیه امنیت و آسایش عمومی محسوب می گردد، بلکه گاهی اینگونه جرایم سبب هتک حیثیت و آبروی اشخاص و یا سبب نقض حقوق مالکیت افراد می گردد و به عنوان جرایم علیه اموال و مالکیت شناخته می شود (جهانگشته و همکاران، ۱۳۹۸، ملکوتی، ۱۴۰۱).

برای پیشگیری از سوءاستفاده افراد سودجو در خصوص هک شدن اطلاعات و ایجاد امنیت اطلاعات کاربران این ضرورت احساس شد، که هماهنگی‌های لازم برای آموزش و فرهنگ‌سازی در فضای مجازی اتخاذ گردد. در این راستا چند رویکرد را می‌توان بیان نمود:

یک رویکرد در رویارویی با تهدیدات فضای سایبر و اقدامات قابل سرزنش که امنیت و سلامت این فضا، با آن روبه‌روست موجود است، که جرم‌انگاری با توسل جستن به قانون که لازمه آن داشتن قانون جرائم رایانه‌ای در بسیاری از قوانین مکمل دیگر است (کاکویی و کوچصفهانی، ۱۴۰۰).

از جمله رویکردهای دیگر ایجاد و اتخاذ تدابیر حفاظتی و کنترلی در قالب پیشگیری وضعی و آموزش کاربران توانمندسازی در مقابل و اجتناب از تهدیدات به همراه پیشگیری اجتماعی است، اما بهترین روش بهره‌گیری هم‌زمان از این رویکردها است. واژه فتا را می‌توان اینگونه تفسیر نمود فضای تولید و تبادل اطلاعات، که ابتدا متولی نداشت، لذا پلیس فتا در ناجا تشکیل شد که اصلی‌ترین وظیفه آن حفاظت از حقوق کاربران و اطلاعات در فضای سایبر و شناسایی حفره‌های در سیستم و مشاغل حساس می‌باشد. از جمله مهم‌ترین جرائم ارتکابی در فضای سایبر، نفوذ به اطلاعات شخصی، تخریب داده‌ها، استفاده از بدافزارها، سرقت و کلاهبرداری اینترنتی، انتشار اخبار سیاسی و ... می‌توان برشمرد (صبح خیز، ۱۳۹۴). پلیس فتا می‌تواند با آموزش صحیح از آمار این جرائم بکاهد. با توجه به آمار بدست آمده استان اصفهان در کشف جرائم سایبری رتبه دوم در کشور با ۷۵٪ درصد را در اختیار دارد. در حالی که کشور کره با سابقه چندین ساله استفاده از اینترنت تنها ۳۰٪ درصد میزان کشف جرائم را در اختیار دارد. بنابراین این آمار نشان از آموزش صحیح و به موقع که توسط پلیس فتا استان اصفهان به کاربران استفاده‌کننده از این فضا داده شده است، می‌باشد. از عواملی که باعث آموزش و فرهنگ‌سازی مناسب در فضای سایبر و ایجاد محیطی برای حفظ اطمینان کاربران در اینترنت است.که البته در این راستا نحوه استفاده کاربران چه از نظر تجاری، دانشگاهی یا خانگی باید مدنظر قرار گیرد و نسبت به هر کدام سیاست‌های لازم اتخاذ گردد (محمدزاده، ۱۴۰۱، کمایی، ۱۳۹۶).

روش تحقیق

روش تحقیق این پژوهش کتابخانه ای و به روش توصیفی تحلیلی می باشد و مشتمل بر مراحل زیر است:

مرحله نخست: گرد آوری مطالب و اطلاعات پایه؛ در یک مطالعه کتابخانه ای و اسنادی، پژوهش ها و منابع موجود داخلی و مرتبط با موضوع جمع آوری و طبقه بندی خواهد شد. در ابتدا اطلاعات خام و متغیرهای مورد نیاز شناسایی و اطلاعات پایه و مستندات موجود از طریق مطالعات کتابخانه‌ای و مستندات قبلی، و مراجعات سازمانی جمع آوری می گردد.

مرحله دوم: بررسی، تجزیه و تحلیل، تعیین کیفیت و طبقه بندی اطلاعات کسب شده؛ در این مرحله به بررسی کیفیت اطلاعات، بررسی صحت اطلاعات و تفکیک و دسته بندی اطلاعات پرداخته می‌شود.

مرحله سوم: تحلیل؛ اطلاعات مورد نیاز در رابطه با بوسیله مراجعه به کتابها، پایان نامه‌ها و مقالات ذیربط با روش تحلیلی و توصیفی.

مرحله چهارم: نتیجه گیری و ارائه نتایج برتر؛ در انتهای پژوهش پس از فیش برداری از منابع موجود و جمع آوری به تجزیه و تحلیل مواد قانونی مرتبط پرداخته می شود. که نتایج حاصل از آن در قالب پیشنهاداتی مطرح، تا مورد استفاده نهادهای مربوطه و سایر دستگاه های مرتبط قرار گیرد.

یافته‌ها

داده‌های مراقبت‌های بهداشتی یک منبع ارزشمند از اطلاعات سلامت است. به اشتراک‌گذاری داده‌های مراقبت‌های بهداشتی یک گام ضروری است تا سیستم مراقبت‌های بهداشتی را دقیق‌تر و کیفیت خدمات بهداشتی را بهبود بخشد. داده‌های مراقبت‌های بهداشتی، یکی از دارایی‌های شخصی بیمار است که باید به جای پراکنده شدن در سیستم‌های مختلف مراقبت‌های بهداشتی، توسط بیمار مورد استفاده قرار گیرد و مانع از اشتراک داده‌ها شود و حریم خصوصی بیمار را حفظ کند. حریم خصوصی داده‌ها یک مسئله حیاتی برای مراقبت‌های بهداشتی و محدودیت دسترسی است که می‌تواند مانع عمده‌ای برای پیشرفت در تحقیق برای درمان بیماری و مراقبت از بیمار باشد. از آنجایی که مؤسسات مراقبت‌های بهداشتی و علوم زیستی بر روی مقادیر بی‌شماری از اطلاعات بیمار کار می‌کنند، آموزش و اطلاع‌رسانی به بیماران در مورد نحوه انجام کاربر روی داده‌های آن‌ها می‌تواند روند نتیجه سلامت را تسهیل کند.

همکاری بهتر، دسترسی سریع‌تر و افزایش شفافیت می‌تواند به طور قابل توجهی در بهبود بیمار و همچنین کاهش هزینه‌های مراقبت وی تأثیرگذار باشد. پیش‌بینی می‌شود که پیاده‌سازی فناوری اطلاعات می‌تواند قابلیت‌های جدیدی را به ارمغان بیاورد و به طور بالقوه موجب اختلال در روند فعلی شود. تحقیق و توسعه موجب بهبود مراقبت و مدیریت می‌شود، بازار را گسترش می‌دهد و در نهایت موجب کاهش هزینه‌ها می‌شود. ایجاد سیستم عامل‌های فناوری اطلاعات می‌تواند به بیمارستان‌ها، پرداخت کنندگان و دیگر اشخاص در زنجیره ارزش‌های مراقبت‌های بهداشتی اجازه دسترسی به اطلاعات بیمار را بدون آسیب رساندن به امنیت داده‌ها و در نهایت صداقت و درستی را بدهد. این سیستم مدیریت قوی سلامت سوابق اطلاعات بیمار را در مقابل حملات سایبری احتمالی محافظت می‌کند.

داده‌های سلامت جمعیت به اطلاعات پزشکی مربوط به جمعیت‌شناسی خاصی اشاره دارد. برای مثال، ممکن است اطلاعات مربوط به خطر سلامتی برای زنان مبتلا به تیروئید در گروه سنی ۲۵-۴۰ سال باشد. برای درک خطرات در یک جمعیت متنوع، معمولاً داده‌ها به صورت ناشناس و بدون اسامی در این موارد نشان داده می‌شوند. وقتی که با مدیریت سلامت جمعیت مواجه می‌شویم، بزرگ‌ترین چالش‌هایی که تا به امروز روی می‌دهد، امنیت داده‌ها، قابلیت اشتراک و قابلیت همکاری است. اگر اطلاعات بیمار پخش و در چندین سیستم ذخیره شود که اجازه انتقال اطلاعات صحیح را ندهد، مجموعه داده‌های سلامت جمعیت در سراسر مجموعه داده‌های مختلف بیمار، کم می‌شود. فناوری اطلاعات یک راه‌حل قابل اعتماد برای این چالش خاص فراهم می‌کند.

هنگامی که به درستی استفاده شود، فناوری اطلاعات به بهبود امنیت، به اشتراک‌گذاری داده‌ها، قابلیت همکاری، یکپارچگی داده‌ها و به‌روزرسانی و دسترسی بلادرنگ اجازه خواهد داد. با استفاده از فناوری فناوری اطلاعات می‌توانید اجازه دهید مردم در مطالعات بهداشتی جمعیت شرکت کنند و علاوه بر این، داده‌های بهتر و به اشتراک‌گذاری داده‌های سلامت جمعیت می‌تواند موجب بهبود مراقبت در میان جمعیت‌های مختلف شود.

سابقه قانون‌گذاری در ایران به حدود ۱۱۳ سال پیش (سال ۱۲۸۵ خورشیدی) بر می‌گردد، ولی در سال ۱۲۹۰ نخستین قانون طبابت تدوین شد و قانون مربوط به مقررات پزشکی و دارویی در سال ۱۳۳۴ تصویب شد که با توجه به شرایط دارویی آن زمان که تا شروع انقلاب اسلامی ایجاب می‌کرد تکیه گاه قانون بیشتر بر نظام تجاری باشد. که پس از انقلاب یک دگرگونی اساسی در مسائل دارویی کشور پیش آمد، که امروزه مجموعه قوانین و مقررات دیگری بر اساس اجزای مختلفی که در نظام سلامت تعریف و ایجاد شده به آن اضافه شده است، یکی از اجزای با اهمیت بخش سلامت، دارو و کالاهای مربوط به آن است.

مجموعه قوانین و مقررات دارویی راه‌هایی را که از آن طریق، دارو می‌تواند بطور صحیح و سالم و مؤثر و به جا به بیمار برسد تعیین می‌نماید. طبق آیین‌نامه ساخت و ورود دارو مصوب سال ۱۳۶۸ سازمان غذا و دارو وضعیت کسانی را که به نوعی با دارو مرتبط‌اند از جمله پزشکان، واردکنندگان، سازندگان، توزیع کنندگان، داروسازان و مصرف‌کنندگان معین کرده است.

این افراد در دسترسی به دارو و نیاز مصرف کننده، نقش‌های مختلفی بر عهده دارند. که هر یک از دست اندرکاران چه کاری باید انجام دهند و چه کاری نباید انجام دهند، حدود وظایف هر یک را معین کرده است.

پس از پیروزی انقلاب اسلامی، سازمان صنایع ملی ایران شرکت‌های دارویی را به دستور قانون ملی شدن صنایع ایران مصوب سال ۱۳۵۸، ملی اعلام کرد و در یک پروسه قابل ملاحظه به نهادها و سازمان‌های متفاوتی واگذار کرد. در حال حاضر عمده سهام شرکت‌های تولید کننده دارو را سازمان تأمین اجتماعی و دومین شرکت بزرگ در زمینه دارو بنیاد پانزدهم خرداد و سومین سهامدار، بانک ملی می‌باشند بر این اساس تعداد شرکت‌های دارویی دولتی در کشور اندک و بیشتر شرکت‌های دارویی، خصوصی می‌باشند.

مجموعه‌ای از اقدامات و سیاستگذاری‌ها از سال ۱۳۵۸ آغاز شد که با شدت تا سال ۱۳۷۳ بر سرنوشت بخش دارو در ایران سایه افکنده بود. در شهریور ۱۳۵۸ طرح ژنریک بر لزوم اصلاحات اساسی در نظام دارویی، سیستم توزیع، نظام آموزشی، ساخت مواد اولیه و تحقیقات تأکید کرد که هدفش جایگزین کردن نام‌های تجارتی با نام‌های ژنریک بود. از آنجا که اجرای «طرح ژنریک» بر صنایع داخلی تکیه داشت. از اواخر سال ۱۳۵۸ برای اعمال مستقیم تصمیم‌های دولت بر مدیریت شرکت‌های تابع سرمایه‌گذاری-های خارجی، ناظران دولتی به کارخانه‌های سازنده دارو اعزام شدند. این مدیران از تیر ماه ۱۳۵۹ در کارخانه‌های دارویی مستقر شدند و این به معنای خلع ید از شرکت‌های دارویی با مالکیت بیگانه بود. نظام دارویی کشور برپایه «طرح ژنریک» بنا شد و داروهای ساخت داخل کشور تنها با نام ژنریک تولید می‌شدند و همین محدودیت در استفاده از نام ژنریک تا سرحد امکان در مورد داروهای ساخته شده وارداتی نیز تحمیل شد.

با پیاده شدن طرح ژنریک این رنگارنگی داروها که ماهیت و فرمول شیمیایی همه داروهای یک گروه یکسان بود و تنها در اسامی تجاری دارای اختلاف بودند محو و سیستمی پیاده شد که به (نظام نوین دارویی ایران) شهرت یافت. روشن است که اعمال، نهادینه ساختن و حمایت از تغییرات ژرف که در کنار سایر سیاست‌ها و روندهای پس از پیروزی انقلاب در پیش گرفته شد و تا حد زیادی هم معلول محدودیت‌های دوران جنگ و تحریم‌های اقتصادی بود، به مجموعه‌ای از سیاست‌گذاری‌ها، مقررات و قوانینی متمرکز و فراگیر از سوی دولت نیاز داشت.

همین نیاز بود که مسئولان دارویی وقت در دوران جنگ و کمیسیون‌های مرتبط در مجلس شورای اسلامی، دارو را به طور رسمی و قانونی کالای اساسی و «استراتژیک» شناختند و نظام اقتصادی سیاسی کشور در مدتی بیش از یک دهه حد اعلای حمایت‌های دولتی را از تولید و واردات دارو در کشور به عمل آوردند. با شمول دارو در شمار کالاهای اساسی و استراتژیک، که نقش اساسی در سلامت جامعه دارد. دولت عملاً خود را متعهد ساخت تا از تولید داخلی حمایت و افزایش ساخت فرمولاسیون‌های جدید را در داخل کشور تشویق کند.

الف- قوانین و مقررات

قانون مربوط به مقررات امور پزشکی و دارویی و مواد خوردنی و آشامیدنی مصوب ۱۳۳۴/۳/۲۹ و اصلاحات بعدی آن و قانون مواد خوردنی و آشامیدنی سال ۱۳۴۶ و اصلاحات سال ۱۳۵۳ نمونه‌های آشکار استفاده از ابزار کیفری در حمایت از امنیت

سلامت مصرف کننده می‌باشد. پس از انقلاب نیز قانون‌گذار با وضع قوانین گوناگون به مسئولیت کیفری تولیدکنندگان در تبصره ماده ۲ قانون حمایت از مصرف کننده توجه کرده است.

مجموعه قوانین و مقررات دارویی راه‌هایی را که از آن طریق، دارو می‌تواند به طور صحیح و سالم و مؤثر و به جا به بیمار برسد تعیین می‌کند. طبق آیین‌نامه ساخت و ورود دارو مصوب سال ۱۳۶۸ سازمان غذا و دارو وضعیت کسانی را که به نوعی با دارو مرتبط هستند از جمله پزشکان، وارد کنندگان، سازندگان، توزیع کنندگان، داروسازان و مصرف کنندگان معین کرده است.

این افراد در دسترسی به دارو و نیاز مصرف کننده، نقش‌های مختلفی بر عهده دارند. که هر یک از دست اندرکاران چه کاری باید انجام دهند و چه کاری نباید انجام دهند، حدود وظایف هر یک را معین کرده است. قوانین دارویی باید وضع کسانی که به نوعی با دارو مرتبط‌اند از جمله پزشکان، وارد کنندگان، سازندگان، توزیع کنندگان، داروسازان و مصرف کنندگان را معین کرده است.

امروزه با توجه به نقش و کارکرد کامپیوتر در زندگی انسان‌ها و ورود آن به زندگی بشر سبب شده است که اطلاعاتی به عنوان اسرار در زمینه های سیاسی، اجتماعی، اقتصادی در آن نگهداری و ذخیره شود که افشای این اسرار لطمات جبران ناپذیری را برای امنیت کشور و افراد داشته باشد. جاسوسی رایانه ای علیرغم جاسوسی سنتی به صراحت در قانون مجازات اسلامی بیان شده است. مواد ۳ تا ۵ قانون جرایم رایانه ای به موضوع جاسوسی اختصاص داده شده است. قانونگذار ایران نیز ماده۳ قانون جرایم رایانه ای را به جرم جاسوسی رایانه ای اختصاص داده است. از نظرماهیت تفاوتی بین جاسوسی سایبری وجاسوسی کلاسیک وجود ندارد و در هر دونوع جاسوسی مرتکب درجهت کسب اطلاعات می باشد وتنها تفاوت بین این دونوع جاسوسی در استفاده از رایانه می باشد وآن هم به دلیل الکترونیکی شدن فعالیت ها درجهت کسب اطلاعات مختلف است. جرم جاسوسی سایبری از لحاظ انجام عملیات نظیر جاسوسی به شیوه سنتی و کلاسیک می باشد. در هر دو نوع از جاسوسی هدف و انگیزه مرتکب یکسان است، تنها طرق و شیوه ی دستیابی به این انگیزه متفاوت است یعنی در جاسوسی سایبری از طریق سامانه های الکترونیکی و رایانه ای به این اهداف دسترسی پیدا می کنند.

عنصر مادی این جرم نیز ارتکاب عمل تجسس به نفع یک طرف و برعلیه طرف دیگر است، پس مرتکب باید با چنین قصد و نیتی این اعمال را انجام دهد و اگر عمل وی بر اثر سهل انگاری و بی توجهی باشد، جرم جاسوسی نمی باشد.

موضوع ماده ۵۰۶ قانون تعزیرات، عدم رعایت اصول حفاظتی و بر اثر مبالاتی خود تخلیه اطلاعاتی توسط دشمنان شود و ماده ۵۱۰مخفی کردن جاسوس می باشد. به دلیل فقدان قانون در زمینه تعریف جاسوسی و مصادیق آن، فضای ابهام آلودی درباره مصادیق این جرم وجود دارد. لیکن از آنجا که تحقق جرایم مذکور، خود موکول به وجود آمدن جرایم جاسوسی می باشد، مصادیق یاد شده را تنها باید به عنوان جرایم مرتبط با جاسوسی در حقوق کیفری ایران قلمداد نمود. جاسوسی سایبری شامل دسترسی غیرقانونی به اطلاعات سری طبقه بندی شده و حفاظت شده به وسیله رایانه یا وسایل الکترونیکی می باشد. جاسوسی سایبری هنر یا تکنیک به دست آوردن اطلاعات سری بدون مجوز گرفتن از نگهدارنده اطلاعات است. استفاده از این طور دسترسی ها را در برابر اطلاعات سری و اطلاعات طبقه بندی شده یا کنترل کامپیوترهای اختصاصی یا کل شبکه ها برای یک مزیت استراتژیک و برای سیاسی، عملیات روانی و فعالیت های بر اندازی فیزیکی و عملیات تخریبی درگیرکرده است. امروزه جاسوسی صنعتی و تجاری به اسرار تجاری، شکل جاسوسی کامپیوتری را به خود گرفته است. هدف جاسوسی کامپیوتری می تواند سخت افزار، نرم افزار یا داده های کامپیوتری باشد. چون مرز جاسوسی و سرقت نرم افزار نیز باید مورد توجه قرار گیرد. از آنجا که بسیاری از اشخاص اطلاعات شخصی خود یا سازمان ها وگروههای مختلف را بر روی شبکه قرار می دهند، جاسوسان سایبری نیز بدنبال بدست آوردن اطلاعات سری و محرمانه اینگونه اشخاص یا به عبارتی بدست آوردن دارایی های معنوی و اطلاعات هویتی آنها هستند تا بدین وسیله و با استفاده از حمله های تروریستی سبب ایجاد خسارت و سرقت هویت و تصاحب اطلاعات آنها شوند.

بنابراین می‌توان جاسوسی سایبری را به مرز صنعت و تجارت کشاند و حتی در فضای سایبری جاسوس با اهداف مختلف مانند سرقت هویت می باشد. سرقت هویت عبارت است از تصاحب یا ادعای هویت شخص دیگراست. اتخاذ عنوان یاهویت دیگری برای کسب مال یا خدمات است یا برای ارتکاب جرم. زمینه های مختلف مبادلات نیز از کامپیوتر به عنوان وسیله ای در جهت کسب اطلاعات و بدست آوردن اسرار تجاری استفاده کرد به عبارت دیگر جاسوس به هر طریقی بدنبال ضربه زدن و کسب اطلاعات محرمانه می باشد. جاسوس سایبری به علل و انگیزه های متفاوتی دست به اینکار می زند، ولی مهمترین دلیل به علل سیاسی بر می گردد و جاسوس بدنبال کسب اطلاعات سری و محرمانه می باشد تا بتواند از این طریق به منافع صنعتی، نظامی، فنی-مهندسی و حتی ضربه زدن به اقتصاد کشور گام بردارد در حالی که انگیزه مجرم سایبری بیشتر بدست آوردن منافع مالی و اقتصادی می باشد.

1- رکن قانونی

بررسی مصادیق جاسوسی در حقوق کیفری هر کشوری می تواند رفتارهایی را که از دیدگاه قانونگذار به عنوان جاسوسی پذیرفته شده است نشان دهد. ممکن است این رفتارهای مجرمانه در برخی از موارد کاملا مشابه با هم مورد جرم انگاری واقع شده باشند. در مقابل، برخی از رفتارهای مجرمانه دیگری نیز وجود دارند که در یک کشور ممکن است به عنوان مصداقی از جاسوسی قابل مجازات اعلام شده باشند، در حالی که در کشور دیگر یا مشمول جرم انگاری واقع شده و یا به عنوان رفتار مجرمانه دیگری از جرایم علیه امنیت مورد توجه قانونگذار قرار گرفته باشند.

قانونگذار ایران در ماده ۳ قانون جرایم رایانه ای چنین مقرر می دارد:«هر کس به طور غیر مجاز نسبت به داده های سری در حال انتقال یا ذخیره شده در سامانه های رایانه ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود، به مجازات های مقرر محکوم خواهد شد:

الف. دسترسی به داده های مذکور یا تحصیل آنها با شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی.

ب. در دسترس قرار دادن داده های مذکور برای دولت،سازمان،شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

برای تحقق عنصر قانونی این جرم عمل شخص باید به صورت دسترسی به داده های مذکور یا تحصیل آنها یا افشای آنها باشد و براساس حکم این ماده صورت بگیرد، پس اگر عمل شخص با عناصر تشکیل دهنده این ماده مغایر باشد مشمول حکم این ماده نمی باشد. ماده ۴ قانون جرایم رایانه ای، نیز با تکرار ماده یک تنها به تغییر موضوع جرم بسنده نموده است و به جرم شروع به ارتکاب جاسوسی اشاره داشته است. ماده ۴:«هر کس به قصد دسترسی به داده های سری موضوع ماده(۳) این قانون، تدابیر امنیتی سامانه های رایانه ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی یا هر دو مجازات محکوم خواهد شد.»

ماده ۵ نیز به بی مبالاتی و بی احتیاطی مأمورین دولتی که مسئول حفظ داده های سری هستند می پردازد. ماده ۵:« چنانچه مأموران دولتی که مسئول حفظ داده های سری مقرر در ماده (۳) این قانون یا سامانه های مربوط هستند و به آنها آموزش لازم داده شده است یا داده ها یا سامانه های مذکور در اختیار آنها قرار گرفته است بر اثر بی احتیاطی، بی مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده ها، حامل های داده یا سامانه های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد».

2- رکن مادی

رکن مادی یکی از عناصر تشکیل دهنده جرم می باشد، چرا که امروزه نمی‌توان کسی را تنها به دلیل فکر و اندیشه مجرمانه مجازات کرد. به عبارت دیگر حالت ذهنی صرف، برای تحقق جرم کافی نیست، بلکه عمل و فعل همراه با سوء نیتی که قانون آن را جرم دانسته است، با نیتی از طرف مرتکب ظهور خارجی پیدا کند.

منظور از «هر کس» در ماده ۳ و ۴ کلیه اشخاص حقیقی اعم از زن، مرد، ایرانی، خارجی، افراد دارای شغل آزاد یا دولتی را شامل می شود. این مواد شامل اشخاص حقوقی نمی باشد، مرتکبین جرم در ماده ۵ مأموران دولتی می باشند که به عنوان مسئول حفظ داده ها و سامانه ها هستند. رفتار مرتکب در ماده ۳ شامل دسترسی به اطلاعات سری و محرمانه یعنی تفحص غیر قانونی اطلاعات و آگاهی یافتن از آنها و افشای اطلاعات برای اشخاص فاقد صلاحیت توسط اشخاص حقیقی می باشد، یعنی هر شخص حقیقی اعم از ایرانی یا خارجی، مرد یا زن با دسترسی غیر مجاز به داده های سری و افشای اطلاعات محرمانه و سری برای اشخاص که نیاز به دانستن اینگونه اطلاعات را ندارند، مشمول این ماده خواهد شد. منظور از داده های سری در تبصره ۱ ماده ۳ ذکر شده است. داده هایی که افشای آنها می تواند سبب لطمه به کشور یا منافع ملی شود. پس موضوع جرم شامل هر گونه فعل یا ترک فعلی خواهد بود که توسط مرتکب انجام خواهد شد، یعنی دسترسی غیر مجاز به داده های محرمانه و سری به وسیله سامانه های رایانه ای که سبب لطمه به امنیت ملی خواهد شد. ماده۴ قانون جرایم رایانه ای ، نیز با تکرار ماده یک تنها به تغییر موضوع جرم بسنده نموده است و به جرم شروع به ارتکاب جاسوسی اشاره داشته است، یعنی قصد دسترسی به داده های سری می باشد، دسترسی به داده های غیرسری حتی اگر با هدف نقض تدابیر امنیتی است جرم نمی باشد پس شخص باید با قصد دسترسی و نقض تدابیر امنیتی بصورت غیر مجاز مرتکب جرم شود. ماده۵ قانون جرایم رایانه ای به بی مبالاتی و بی احتیاطی مأمورین دولتی که مسئول حفظ داده های سری هستند می پردازد و عمل مأمورین دولتی را که به صورت غیر عمدی سبب دسترسی افراد فاقد صلاحیت به اطلاعات خواهند شد را بیان می کند. بی احتیاطی خطای انسانی است که پیامد کار خود را در وضع خاص پیش بینی نمی کند. بی مبالاتی نیز همان بی احتیاطی به صورت ترک فعل می باشد.مقصود از بی مبالاتی ترک تکلیفی است که مقتضای پیشگیری از نتایج ناخواسته مجرمانه است.

پس هرگاه مأمور دولت بر اثر بی احتیاطی و بی مبالاتی خود موجب ورود بیگانگان و دشمنان به سامانه ها یا سیستم های حامل داده شوند و با دست یافتن آن ها به اطلاعات سری و محرمانه سبب افشای اطلاعات و نقض تدابیر امنیتی کشور شوند، مشمول حکم این ماده خواهند شد. در ماده ۳قانون جرایم رایانه ای عبارت از در دسترس قرار دادن داده های مذکور برای اشخاص فاقد صلاحیت افشاء آن برای سازمان، دولت،گروه بیگانگان. پس اگر مرتکب با هدف دیگری غیر از این موارد جرم را انجام دهد مشمول این ماده نخواهد شد. ماده۴ باید با هدف نقض تدابیر امنیتی سامانه های رایانه ای یا مخابراتی باشد و ماده۵ مأموران دولتی هستند که مسئول حفظ داده های سری یا سامانه ها می باشند.

3- رکن روانی

بزه جاسوسی سایبری در زمره جرایم مادی صرف نمی باشد، بلکه احراز رکن روانی آن لازم و ضروری می باشد. ارتکاب جرم یا تظاهر نیت سوء و یا خطای مجرم است. مشروط بر اینکه فاعل چنین فعلی را بخواهد یا دست کم وقوع آن را احتمال دهد و به نقض اوامر و نواهی قانونگذار آگاه باشد. هرگاه فاعل قصد فعل و قصد حصول نتیجه را داشت، عامد محسوب می شود و اگر فاعل قصد فعل داشته باشد بدون آن که نتیجه مجرمانه ای را از آن طلب کند،خاطی محسوب می شود. عنصر معنوی جرم جاسوسی سایبری شامل عمدی بودن و ارادی بودن اقدام مرتکب یعنی آگاهی داشتن از محرمانه و سری بودن داده‌ها است و اطلاع از

دستیابی افراد فاقد صلاحیت به اینگونه اطلاعات می باشد. مرتکب با هدف و نیت لطمه به امنیت ملی و نقض تدابیر امنیتی کشور اینگونه اطلاعات را در اختیار دشمنان و بیگانگان قرار دهد.

ب. راهکار حقوقی تأمین امنیت در فضای سایبر

تناسب، هماهنگی و همسویی، میان مجازات و جرم از لوازم یک نظام کیفری متعادل است. مبنای منطقی برای مجازات از اصول اولیه و بنیادین نظام عدالت کیفری و عامل مشروعیت آن است. در نظام کیفری ایران، تاکنون لااقل مبانی کلی و فراگیر برای تناسب مجازات با جرم ارتکابی مکتوب نشده. است. نبود اصول، بنیادی در تعیین، کیفر، در مرحله تقنین و اجرا از عمده ایرادها، یا شاید عمده‌ترین ایراد نظام کیفری ایران است گاهی، قانونگذار در تعیین مجازات جرمی، فاصله بین حداقل و حداکثر آن را به ۴۰ برابر رسانده است و دادگاه بدون الزام به توجیهی در بین حداقل و حداکثر آن مختار است هر میزان مجازات تعیین کند، که نوعاً تناسبی بین مجازات و جرم دیده نمی‌شود؛ این، امر اصل تناسب مجازات با جرم را مخدوش خواهد کرد. بنابراین بیان معیار کلی و، بنیادین برای رعایت اصل تناسب جرم با مجازات از اصول راهبردی است که باید در نظام کیفری ایران به آن پرداخته شود. همواره در تعیین کیفر، ارزش مجازات باید سنجیده شود. بدین معنا که گاهی فرد بزهکار، دستاورد ارتکاب جرم و میزان مجازات تعیین شده برای آن را بررسی می‌کند که آیا این جرم، با توجه به میزان مجازات تعیین شده برای آن ارزش ارتکاب دارد یا خیر؟ به فرض فرد بزهکار با دسترسی غیر مجاز به سامانه‌های رایانه‌ای بخش دولتی و سرقت داده‌های مربوط به زیر ساخت‌های اساسی دولت به اطلاعاتی دست پیدا می‌کند که می‌تواند سود مالی زیادی را با فروش آن به دول متخاصم، به دست بیاورد. این در حالی است که مجازات دسترسی غیر مجاز (موضوع ماده ۱ قانون جرایم رایانه ای) و سرقت داده (موضوع ماده ۱۲ قانون جرایم رایانه ای) جزای نقدی بسیار اندکی در پی خواهد داشت. بدیهی است که بزهکار، با بررسی میزان مجازات و دستاورد حاصل از ارتکاب جرم به این نتیجه می‌رسد که می‌تواند با ارتکاب جرم چه میزان مال به دست آورد و چه میزان مجازات خواهد شد؛ همین موضوع، انگیزه او را برای ارتکاب به جرم قوی‌تر خواهد کرد قطعاً اگر میزان، مجازات، با توجه به اهمیت جرم تعیین شود فرد بزهکار هرگز خود را در جایگاهی قرار نمی‌دهد که بخواهد با علم به میزان مجازات، اقدام به ارتکاب جرم کند. از ایرادهای دیگری که میتوان در بحث جرایم رایانه‌ای بدان توجه داشت، بحث تحصیل و جمع‌آوری دلایل استنادپذیر است، با توجه به ویژگیهای خاص این فضا، بر خلاف فضای سنتی، قاضی و ضابطان امکان مشاهده و جمع‌آوری ادله را ندارند به معنای واقعی محل وقوع جرمی وجود ندارد که بتوان آثار وقوع جرم را بررسی کرد نوع تحقیقات، توقیف اسباب وقوع جرم و... نیاز به تخصص خاصی دارد در واقع جایگزین شدن موضوع‌های غیر ملموس و سایبر، به جای ادله ملموس و واقعی مسایل حقوقی نوینی را پدید می‌آورد که به یقین، بازخورد مستقیمی نیز در حقوق کیفری خواهد داشت. از این رو لزوم آموزش مجریان قانون، امری است که باید مورد توجه قرار بگیرد(ابراهیم زاده، ۱۳۹۶).

همان طور که دادسرای جرایم رایانه‌ای به عنوان دادسرای تخصصی، در حال حاضر صلاحیت رسیدگی به جرایم ارتکابی را در این بستر دارد میبایست دادگاه‌های کیفری و تجدید نظر نیز، شعب ویژه برای رسیدگی به آرا و قرارهای صادره از دادسرا داشته باشند، زیرا به نظر میرسد رسیدگی در دادگاههای بدوی و تجدید نظر در خصوص منع تعقیب یا کیفرخواست صادره از دادسرای تخصصی جرایم رایانه‌ای نیازمند یک رویکرد و بررسی از جانب متخصصان این امر، است که، متأسفانه در حال، حاضر این گونه دعاوی در شعب عمومی و بیشتر وقتها با قضات غیر متخصص در امر جرایم رایانه‌ای مورد رسیدگی قرار می‌گیرد(ملکوتی و خلیل زاده، ۱۴۰۱).

از دیگر مشکلات فضای سایبر عدم جرم انگاری استفاده از نرم افزارهای عبور از فیلتر (VPN) است. اصول ۳۶ و ۳۷ قانون اساسی که شاخصه و سرلوحهٔ همه قوانین مطروحه در کشور است، حکم به مجازات و اجرای آن را تنها از طریق دادگاه صالح و به موجب قانون مورد شناسایی قرار داده است. حتی قانونگذار اصل را بر برائت میداند و هیچ کس از نظر قانون مجرم شناخته نمی‌شود مگر اینکه جرم او در دادگاه صالح ثابت شود. بر اساس ماده ۲ قانون مجازات اسلامی فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد، جرم محسوب میشود. با توجه به این موارد و از آنجا که در خصوص جرایمی که در فضای مجازی اتفاق می‌افتد قانون خاص آن وجود دارد به نظر میرسد هیچ ماده‌ای از مواد ۵۶ گانه آن وجود ندارد که استفاده از فیلترشکن‌ها یا پروکسی‌ها را عمل مجرمانه معرفی کند؛ مضافاً آنکه در این خصوص نیز، نظریه شماره ۳۶۷/۷ مورخ ۲۵/۲/۱۳۹۹ اداره حقوقی قوه قضاییه می‌گوید:

" نظر به اینکه در قانون جرایم رایانه‌ای مصوب ۸۸ برای صرف استفاده از فیلترشکن یا دانلود رایگان آن مجازاتی پیش بینی نشده لذا با توجه به اصل ۳۶ قانون اساسی و مقررات ماده ۲ قانون مجازات اسلامی اعمال موضوع استعلام قانوناً جرم تلقی نمی‌شوند. "

نتیجه گیری

از آنجا که تکنولوژی های کامپیوتر و اینترنت سبب تغییر ماهیت جرایم از شیوه های کلاسیک به نسل جدیدی از آن با عنوان داده ها و اطلاعات می باشد دیگر قوانین کلاسیک در حقوق کشورها کافی نبود و نیاز به وضع قوانین جدید در این خصوص احساس می گردید. قانونگذار ایران نیز در جهت مقابله با اینگونه جرایم و حفاظت از اطلاعات شخصی اشخاص و امنیت داده ها به وضع قوانینی مرتبط با اینگونه جرایم پرداخته است و این نشانگر این است که حقوق جزا وارد مرحله جدید شده است و با گونه جدیدی از جرایم مواجه است که نیاز به حمایت از اطلاعات و داده ها می باشد.

پتانسیل فناوری اطلاعات برای سامانه های دارویی به منظور ایجاد زیربنای فنی، به شدت به پذیرش فناوری جدید در اکوسیستم مراقبت‌های بهداشتی بستگی دارد. اگرچه نگرانی‌ها و گمانه‌های خاصی در مورد ادغام فناوری اطلاعات با سیستم‌های مراقبت‌های بهداشتی فعلی و پذیرش فرهنگی آن‌ها وجود دارد، این فناوری هنوز در بخش مراقبت‌های بهداشتی محبوب است. این صنعت در سال گذشته از طوفان صنعت سامانه های دارویی گرفته شده است و بسیاری از راه‌حل‌ها برای اتخاذ آن به کار گرفته شده است و ما سعی کردیم این کار را ادامه دهیم. فناوری اطلاعات یک فناوری در حال ظهور است و دارای یک پتانسیل بزرگ است که نه تنها به چند صنایع تأثیر می‌گذارد، بلکه می‌تواند راه کسب و کار را نیز تغییر دهد. امنیت فضای سایبری در سامانه های دارویی آغاز شده است و ما می‌توانیم انتظار داشته باشیم که در آینده نزدیک راه‌حل‌های تجاری فناوری اطلاعات را در جهت ارتقای آن داشته باشیم.

با توجه به این که نه فقط میلیاردها دلار از صنعت داروسازی، بلکه زندگی و سلامتی میلیون‌ها انسان در گروی دارو و صنعت داروسازی است، تمام طرف‌های دخیل باید سعی کنند تا با همکاری یکدیگر مشکل امنیت سامانه های داروهای را حل کنند. اگر مشکلات موجود در زمینه مسئولیت‌پذیری و شناسایی ماهیت اصلی داروها به کمک فناوری های نوین قابل حل باشد، این فناوری بایستی در سطح جهانی پیاده‌سازی شود. در عین حال بحث امنیت سامانه‌های نسخه الکترونیک دارو هم مطرح است که هنوز گواهی امنیتی نسخه الکترونیک صادر نشده است. باید گواهی امنیتی برای حفظ این سیستم به صورت جدی پیگیری شود تا مورد دستبرد و هک قرار نگیرد.

پیشنهادات

۱. با توجه به گستردگی و اهمیت جرایم سایبری و اهمیت امنیت داده ها و حریم خصوصی سامانه های دارویی و از نظر اینکه اینگونه جرایم ماهیتی کاملاً جدید در حوزه حقوق کیفری دارند باید تدوین قوانین و تعقیب مجرمین سایبری اهمیت بسیاری راداشته باشد. قوانین وضع شده توسط قانونگذار در زمینه جرایم سایبری سامانه های دارویی از آنجا که مربوط به سال ۱۳۸۸می باشد بهتر می بود که در مجازات های نقدی که در نظر گرفته شده است تجدیدنظر صورت گرفته و مقدار آن افزایش می یافت.

۲. در زمینه تهدیدات مرتبط با امنیت داده های سامانه های دارویی از آنجا که این تهدیدات در ذیل جرایم سایبری به شمار می آیند این به معنای حذف عنوان آنها نمی باشد و اینگونه تهدیدات در قانون جرایم رایانه ای کم رنگ جلوه داده شده است باید در این مورد نیز توجه بیشتری توسط قانونگذار صورت بگیرد.

۳. در ایران با رواج و استفاده روز افزون از رایانه و اینترنت و افزایش جرایم سایبری سامانه های دارویی نیاز به هماهنگی و همکاری بیشتر پلیس در زمینه کشف و تعقیب مجرمین مشاهده می شود. پس نیاز به آموزش های لازم در این زمینه به نیروی پلیس می باشد، در سطح بین الملل نیاز به همکاری با مجامع بین المللی و شناخت و دستیابی به نوعی اتفاق نظر و ایجاد راه حل‌های بنیادین در مورد شناسایی و تعقیب مجرمین می باشد.

منابع

۱. اسماعیل جهانگشته، سلمان رئیسی، فاطمه دامنی. ۱۳۹۸. بررسی اهمیت امنیت فضای سایبری. هشتمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات.
۲. اکرم محمدزاده. ۱۴۰۱. امنیت سایبری. سومین کنفرانس ملی پدافند سایبری.
۳. اکبری، عباسعلی و نوروزعلی، روح اله، ۱۴۰۱، پیشگیری از جرایم سایبری با نگاهی به طرح صیانت از فضای مجازی، سومین کنفرانس ملی پدافند سایبری، مراغه.
۴. جواد آزادی. ۱۳۹۷. امنیت سایبری یا امنیت فضای مجازی؟ . تاملات رشد. ۱۶۴.
۵. سعید چگینی. ۱۳۹۹. امنیت در فضای مجازی. رشد معلم ۳۳۲. ۳۱-۳۳.
۶. صبح خیز، رضا. (۱۳۹۴). چالش‌های حقوقی جرایم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران، فصلنامه پژوهش‌های اطلاعاتی و جنایی، شماره۳، ص. ۱۲۴.
۷. عیسی کاکویی‌دینکی، حسین مصلحتی‌کوچصفهانی. ۱۴۰۰. فضای مجازی. به‌اندیش
۸. ملکوتی، رسول، & خلیل زاده، مونا. (۱۴۰۱). راهکار حقوقی تامین امنیت سایبری. فصلنامه علمی رسانه، ۳۳(۱)، ۶۹-۹۷. doi: ۱۰. ۲۰۲۱. ۲۷۲۹۲۹./bmsp۲۲۰۳۴.
۹. مریم کمایی، سلامه ابوالحسنی. ۱۳۹۸. مطالعه جامع جرایم سایبری و مجرمین سایبری در فضای مجازی. سومین همایش ملی سبک زندگی و سلامت.

Cyber Security of Virtual Space With an Attitude on Pharmaceutical Systems

Babak pourghahramani

Associate Professor, Department of Criminal Law and Criminology, Islamic Azad University, Maragheh Branch. (Corresponding Author)

b.pourghahramani@yahoo.com

Amirhosein Zivarpour

PhD student in criminal law and criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran

Amirhosein.Zivarpour.iau147@gmail.com

Abstract

Background and purpose: Today, the pharmaceutical industry is considered as one of the key and strategic industries in the world. Medicine has always been one of the most important pillars of the health cycle due to its impact on human health and human societies. On this basis, the procurement and supply of medicine needed by the society, even in the most critical conditions of the country, is always a special priority of the governments. The evolution of information and the increasing use of computers and the Internet in all aspects of human life and the need of companies, organizations, and groups have caused the occurrence of various crimes in cyberspace. The virtual space with its characteristics such as being transnational, multiplicity of actors, secrecy has caused people to enter this space and commit various crimes without being easily identified.

Research method: The present study is descriptive-analytical in nature and examines the available literature in the field of cyberspace security. The method of collecting information in this study is library type.

Findings: Various crimes such as theft, fraud, forgery, espionage take place in this virtual but real space. Some of these crimes cause harm and damage to the privacy of people in the fields of treatment and especially medicine and are considered as a threat to data security. Some of these crimes cause financial and economic damage, and some of them are threats and harm against individuals. The security of the data of any country is one of the concerns of the governments that take steps to ensure internal and external security.

Conclusion: In order to deal with the unauthorized access of data and crimes that occur through electronic means and in an advanced manner, regulations and laws were established by the legislator to close the way for profiteers and ensure data security.

Keywords: Security, Virtual Space, Security Threat, Pharmaceutical Systems.