Examining the Role of Forensic Nurses in Cybersecurity and Preventing Crimes in Cyberspace

Mitra sedghi Sabet[1], Amirreza Mahmoudi[2], Atefeh Lorkojuri[3], Shadi Dehghanzadeh[4]

Abstract

Cybercrimes have become a growing concern for human society. Healthcare systems have experienced increased types, impacts, and frequency of cybercrime in recent years. These attacks have negatively impacted patients' privacy, healthcare providers' ability to deliver care, and the overall security of healthcare organizations. Nurses are uniquely positioned to help protect against cybercrimes and report them, as they are among the largest workforces in the healthcare system. Nurses are on the frontline of patient care and the use of healthcare technology. Considering this issue, the present study aims to explain the role of forensic nurses in cybersecurity and preventing crimes in cyberspace within the healthcare system. It employs a descriptive-analytical research method and through the documentary methodology by using library and internet data. The findings indicate that forensic nurses can act highly successfully in detecting misconducts resulting from cybercrimes against individuals, as with their command of legal concepts they can construct a framework for strengthening evidence. Additionally, with appropriate interventions, they will provide necessary care for these victims. Conversely, as frontline users and liaisons between the clinical world and information technology, they can significantly help prevent crimes and maintain cybersecurity in the healthcare system by being aware of cyber threats, early identification and reporting of unusual activities as well as documenting the details.

Keywords: Forensic Nursing, Cybersecurity, Crime Prevention, Cyberspace, Cybercrimes

[1] . PhD. of Student in Criminal Law and Criminology, Faculty of Humanities, Lahijan Branch, Islamic Azad University, Lahijan, Iran.
[2]. Assistant Prof. at Law Department, Faculty of Humanities, Lahijan Branch, Islamic Azad University, Lahijan, Iran. (Corresponding Author).
Email: Amirreza.mahmodi@gmail.com
[3]. Assistant Prof. at Law Department, Faculty of Humanities,, Lahijan Branch, Islamic Azad University, Lahijan, Iran.
[4]. Assistant Prof. at Nursing, Department Rasht Branch, Islamic Azad University, Rasht, Iran.

بررسی نقش پرستاران قانونی در امنیت سایبری و پیشگیری از جرائم در فضای مجازی

میترا صدقی ثابت[۱]، امیررضا محمودی[۲]، عاطفه لرکجوری[۳]، شادی دهقان‌زاده[٤]

چکیده

جرائم سایبری به نگرانی فزاینده‌ای برای جامعه بشری تبدیل‌شده است. در سال‌های اخیر، جرائم سایبری در نظام سلامت ازنظر نوع، تأثیر و فراوانی به‌شدت افزایش‌یافته است. این حملات بر حریم خصوصی بیمار، توانایی ارائه‌دهندگان مراقبت در ارائه مراقبت و امنیت سازمان‌های مراقبت‌های بهداشتی تأثیر منفی گذاشته است. پرستاران به‌طور منحصربه‌فردی برای کمک به محافظت در برابر جرائم سایبری و گزارش آن‌ها قرار دارند، زیرا آن‌ها یکی از بزرگ‌ترین جمعیت شاغل در نظام سلامت هستند و در خط مقدم مراقبت از بیمار و استفاده از فناوری مراقبت‌های بهداشتی قرار دارند. با توجه به این مسئله پژوهش حاضر باهدف تبیین نقش پرستاران قانونی در امنیت سایبری و پیشگیری از جرائم در فضای مجازی در نظام سلامت، با رویکرد توصیفی و تحلیلی و با روش اسنادی از طریق گردآوری داده‌های کتابخانه‌ای انجام شد. یافته‌ها حاکی از این بود که در این عرصه پرستاران قانونی از یک‌سو می‌توانند در تشخیص سوء رفتارهای حاصل از جرائم سایبری علیه اشخاص بسیار موفق عمل کنند زیرا آنان با تسلط بر مفاهیم قانونی قادر به ساخت چارچوبی برای تقویت شواهد بوده و با مداخلات مناسب خود مراقبت لازم را از این قربانیان به عمل خواهند آورد و از سویی دیگر نیز قادر خواهند بود به‌عنوان کاربران خط مقدم و رابطین بین دنیای بالینی و فناوری اطلاعات، با آگاهی از تهدیدهای سایبری با شناسایی و اطلاع‌رسانی زودهنگام فعالیت‌های غیرعادی و مستند نمودن جزئیات در پیشگیری از جرائم و برقراری امنیت سایبری در حوزه نظام سلامت کمک شایانی نمایند.

واژگان کلیدی: پرستاری قانونی، امنیت سایبری، پیشگیری از جرم، فضای مجازی، جرائم سایبری

---

۱. دانشجوی دکتری رشته حقوق جزا و جرم شناسی، گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران

۲. استادیار، گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران (نویسنده مسئول).

پست الکترونیک: Amirreza.mahmodi@gmail.com

۳. استادیار، گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران

٤. استادیار، گروه پرستاری، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران

مقدمه

فناوری، جامعه امروزی را از دولت‌ها گرفته تا اقتصاد و ارتباطات تحت تأثیر قرار داده است و از زمان ظهور اینترنت و شبکه جهانی وب، جامعه کارآمدتر و پیشرفته‌تر شده است (Nurse, 2018: 2). در بسیاری از موارد مردم ناگزیر به استفاده از فضای سایبر هستند به‌نحوی‌که این فضا بخشی از زندگی واقعی مردم و مراودات اجتماعی آنان شده است (صبوری و ثقفی، ۱۳۹۸: ۱۲٦). به‌واسطه فناوری‌های جدید، زندگی بشر در معرض تغییرات بسیاری قرارگرفته است. گسترش استفاده از رایانه، موبایل و وسایل الکترونیکی در کنار افزایش ضریب نفوذ اینترنت سبب شده که انقلاب وسیعی در نحوه ارتباط افراد با یکدیگر رخ دهد (دهقان فر، پاک نهاد و ایروانیان ، ۱٤۰۲: ۱٦).

اینترنت به‌عنوان مهم‌ترین رسانه عصر جدید در کنار محاسن و مزایای بی‌شمار خود که منشأ آثار مثبت و بالنده‌ای برای تعالی انسان می‌باشد، نقش تخریب‌کننده‌ای نیز می‌تواند برای جامعه بشری ایفا کند. هرچند هدف از اختراع رایانه، تسریع و تسهیل پردازش اطلاعات بوده و مخابرات نیز به‌عنوان مهم‌ترین ابزار ارتباطی، در نشر اطلاعات پردازش‌شده، نقش به سزایی داشته است اما طی نیم‌قرن اخیر، به‌تدریج با کشف قابلیت‌های شگرف ناشی از تلفیق این دو فناوری، عرصه فناوری اطلاعات و ارتباطات دگرگون‌شده است. اوج این انقلاب را می‌توان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که از دهه نود میلادی به بعد، تحولی بنیادین را در این حوزه رقم‌زده است. این شبکه‌ها که از بسیاری سامانه‌های رایانه‌ای متصل به یکدیگر تشکیل‌شده‌اند، فضایی با ویژگی‌های کاملاً جدا از دنیای فیزیکی به وجود آورده‌اند که با عنوان «فضای سایبر» شناخته می‌شود (حسین زاده، عطازاده و قیوم‌زاده، ۱۳۹۹: ٦۰۵).

اینترنت علاوه بر گسترش ارتباطات و عرضه طیف گسترده‌ای از دانش و فرصت‌ها برای کاربران خود؛ به دلیل ویژگی‌های خاص فضای مجازی موجبات انجام رفتارهای مجرمانه را فراهم کرده و افرادی را نیز در معرض خطر قربانی شدن قرار می‌دهد (Hammer et al, 2013: 306). ویژگی‌های فضای مجازی از قبیل عدم وابستگی به زمان و مکان خاص، امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام، به همراه ماهیت جرائم سایبری؛ عواملی هستند که شیوه‌های ارتکاب این نوع جرائم را متنوع‌تر، کشف جرائم و به دام انداختن مجرمان را دشوارتر کرده است (امیریان فارسانی، ۱٤۰۲:۳).

تمایز جرائم سایبری در مقایسه با جرائم سنتی در ویژگی‌های انحصاری آن است. در این نوع بزه، مرتکبان ناشناس در فضایی ناشناخته با برخورداری از فناوری نوین و وسایل پیشرفته دست به اعمال مجرمانه زده و به اهداف شوم خود می‌رسند بدون آن‌که اثری همانند جرم سنتی از خود برجای گذارند. ویژگی دیگر این دسته از جرائم عدم‌تشخیص درست طیف بزه دیدگان است؛ زیرا افراد و سازمان‌های متعددی می‌توانند هدف این مجرمان قرار گیرند. این موضوع نشان می‌دهد مجرمان سایبر فارغ از زمان و مکان بوده و این نوع از جرائم، جنبه فراملی و فرا سرزمینی به خود گرفته است (کرمی، ۱۳۹۷: ۳۳٦).

جرائم سایبری به روش‌های مختلفی تعریف‌شده، اما اساساً می‌توان آن را به‌عنوان هر جرمی (سنتی یا جدید) در نظر گرفت که می‌تواند از طریق یا با استفاده از فناوری‌های دیجیتال انجام یا فعال شود. چنین فناوری‌هایی شامل رایانه‌های شخصی، لپ‌تاپ، تلفن‌های همراه و دستگاه‌های هوشمند هستند، اما دامنه آن برای دربرگرفتن دستگاه‌ها و زیرساخت‌های هوشمند و هدایت آن توسط اینترنت اشیاء[1]، به‌سرعت در حال گسترش است (Nurse, 2018: 3).

امروزه، خدمات سلامت نیز با طوفان سایبری مواجه است که از افزایش داده‌های بیماران، سرمایه‌گذاری ناکافی در امنیت داده‌ها و سیاست‌های ناسازگار مربوط به حریم خصوصی داده‌ها منشأ گرفته است. باوجوداینکه قوانینی مانند قانون انتقال و پاسخگویی بیمه سلامت[2] جهت محافظت از محرمانگی و یکپارچگی داده‌ها وضع‌شده، اما حملات سایبری به داده‌های سلامت شدت گرفته است (Luh & Yen, 2020: 1).

در مواردی که ذینفعان نظام سلامت آماج حملات مجرمان سایبری قرار می‌گیرند، این پرستاران هستند که در مواجهه اولیه با قربانیان بوده و باید برای شناسایی و مقابله با انواع آسیب‌پذیری‌های سایبری اقدام نمایند (Lee, 2020: 64). برخی موارد، بزه دیدگان از قربانیان جرائم سایبری علیه اشخاص مانند برخوردهای جنسی غیرقانونی[3]، قلدری سایبری[4]، هرزه‌نگاری کودکان[5] و کلاه‌برداری مراقبت‌های بهداشتی[6] هستند، در چنین موقعیت‌هایی پرستاران قانونی به دلیل ارتباط نزدیک با قربانیان فرصت آموزش

---

[1]. Internet of Things (IOT)
[2]. Health insurance portability and accountability act (HIPPA)
[3]. Illegal Sexual Encounters
[4]. Cyberbullying
[5]. Child Pornography
[6]. Healthcare Fraud

به آنان داشته و از این طریق جهت پیشگیری و مقابله با این نوع جرائم مساعدت می‌نمایند (Hammer et al, 2013: 306). برخی موارد نیز اطلاعات مربوط به پرونده‌های الکترونیک سلامت، داده‌های تحقیقات ژنومی، دستگاه‌های پزشکی و فناوری‌های پوشیدنی در دسترسی غیرمجاز مجرمان سایبری قرارگرفته و از این طریق امنیت سایبری در حوزه سلامت تهدید می‌شود. در این مواقع پرستاران با گزارش به‌موقع حوادث مشکوک نقش مهم خود را در برقراری امنیت سایبری در این حوزه ایفا می‌نمایند (Lee, 2020: 64).

جرائم سایبری همانند سایر جرائم علیه اشخاص، می‌تواند با استفاده از شکاف موجود بین نظام‌های عدالت و سلامت منجر به نادیده گرفتن حقوق قربانیانی شود که هم‌زمان نیازمند بهره‌مندی از خدمات دو نظام فوق می‌باشند. این خلأ از دانش محدود کارکنان دو نظام مذکور از مبانی حرفه‌ای یکدیگر و تداخل روندهای عدالت و سلامت ناشی می‌شود که رفع آن تشریک‌مساعی کارگزاران این دو نظام را می‌طلبد.

برخی کشورها جهت رفع این معضل مبادرت به طرح راه‌حلی در مراکز درمانی به‌صورت جلب همکاری پرستاران متخصص در علوم قانونی نمودند و هم‌اینک آنان به‌منزله واسطه‌ای بین دو نظام سلامت و عدالت با موفقیت عمل می‌کنند. پیشگیری از نقض حقوق قربانیان، افزایش دقت و سرعت در رسیدگی پرونده‌های پزشکی قانونی، شناسایی و گردآوری مناسب شواهد، مدیریت خطر و آمادگی برای ادای شهادت تخصصی در دادگاه ازجمله تأثیرات مطلوبی هستند که می‌توان از حضور پرستاران قانونی در نظام عدالت کیفری برشمرد (صدقی ثابت و همکاران، ۱٤۰۱: ۵).

با توجه به رواج روزافزون جرائم سایبری به‌ویژه آن دسته که نظام سلامت و ذینفعان آن را تحت تأثیر قرار داده و پیامدهای گسترده‌ای را برای جامعه در پی دارد از یک‌سو و لزوم بهره‌مندی از کلیه ظرفیت‌های موجود در جامعه به‌منظور پیشگیری و مقابله با این دسته جرائم از سویی دیگر و همچنین با عنایت به دستاوردهای ارزنده پیشگیری و مقابله با این دسته از جرائم، لازم است به نقش مؤثر پرستاران قانونی در این حوزه توجه ویژه‌ای مبذول گردد زیرا باملاحظه یافته‌ها و نتایج سوابق پژوهش، می‌توان انتظار داشت که استقرار و جلب همکاری پرستاران قانونی راهکار مناسبی جهت امنیت سایبری و پیشگیری از جرائم در فضای مجازی در حوزه نظام سلامت باشد.

هدف از پژوهش حاضر تبیین نقش پرستاران قانونی در امنیت سایبری و پیشگیری از جرائم در فضای مجازی در نظام سلامت است تا از این طریق به این پرسش پاسخ داده شود که نقش پرستاران قانونی در امنیت سایبری و پیشگیری از جرائم در فضای مجازی در نظام سلامت چیست؟ فرضیه‌ای که در پاسخ به این پرسش مورد تحلیل قرار می‌گیرد این است که پرستاران قانونی در امنیت سایبری و پیشگیری از جرائم در فضای مجازی در حوزه نظام سلامت نقش مؤثری دارند؛ بنابراین، در پژوهش حاضر بامطالعه اسناد و منابع کتابخانه‌ای و استفاده از روش توصیفی و تحلیلی فرضیه مورد کنکاش قرار گرفت. در این روش منابعی نظیر کتب، مقالات و مستندات حقوقی و پرستاری موردبررسی قرارگرفته است. از مهم‌ترین اقدامات صورت گرفته در این پژوهش شناسایی نقش پرستاران قانونی در پیشگیری از جرائم سایبری علیه اشخاص مانند قلدری سایبری، هرزه‌نگاری علیه کودکان و تقلب در مراقبت‌های بهداشتی، پیشگیری از جرائم علیه امنیت سایبری در حوزه نظام سلامت و شناخت ضرورت پیش‌بینی جایگاهی برای پرستاران قانونی جهت پر کردن شکاف موجود بین نظام‌های عدالت و سلامت در ممانعت از تضییع حقوق قربانیانی است که هم‌زمان نیازمند بهره‌مندی از خدمات دو نظام فوق هستند.

۱. پیشینه پژوهش

پرستاری قانونی از تخصص‌های نوین در کشور محسوب می شود و تحقیقات اندکی در مورد نقش و جایگاه این رشته در ایران صورت گرفته است. این رشته در برخی از کشورها جایگاه خود را در هر دو نظام سلامت و عدالت یافته است. ازجمله، برن و همکاران (۲۰۱۷) در مطالعه‌ای به بررسی اطلاعات و مداخلات پرستاران در مواجهه با قربانیان زورگویی سایبری و رسانه‌های اجتماعی و خانواده آن‌ها پرداخته و اظهار داشتند که رسانه‌های اجتماعی به پلت فرم اصلی برای آزار و اذیت سایبری تبدیل‌شده و قربانیان اغلب پیامدهای سلامتی منفی را تجربه می‌کنند که مستقیماً با آزار و اذیت سایبری مرتبط است. به همین دلیل، بسیار مهم است که پرستاران از رسانه‌های اجتماعی و علائم هشداردهنده قربانیان آزار و اذیت سایبری و نحوه پیشگیری از این نوع خشونت مطلع باشند (Byrne et al, 2017: 1).

مک درموت (۲۰۲۰) نیز در مطالعه‌ای تحت عنوان «امنیت سایبری: پرستاران در خط مقدم پیشگیری و آموزش» با اشاره به این‌که در سال‌های اخیر، جرائم سایبری در مراقبت‌های بهداشتی ازنظر نوع، تأثیر و فراوانی به‌شدت افزایش‌یافته است، اظهار داشتند این حملات بر حریم خصوصی بیمار، توانایی ارائه‌دهندگان مراقبت در ارائه خدمات و امنیت سازمان‌های مراقبت‌های بهدا شتی تأثیر منفی گذا شته

است و پرستاران به‌طور منحصربه‌فردی برای کمک به محافظت در برابر جرائم سایبری و گزارش آن‌ها قرار دارند، زیرا آن‌ها یکی از بزرگ‌ترین گروه‌های نظام سلامت بوده و در خط مقدم مراقبت از بیمار و استفاده از فناوری در مراقبت‌های بهداشتی قرار دارند (Kamerer & McDermott, 2020: 48).

وجه تمایز این مطالعه علاوه بر بدیع بودن موضوع در خصوص تبیین نقش پرستاران قانونی در نظام سلامت کشور در راستای شناسایی قربانیان و بازماندگان جرائم سایبری در حوزه نظام سلامت؛ رویکردی است که نویسندگان به نقش پیشگیرانه این متخصصان در حوزه فوق داشته‌اند. بر این اساس در مطالعه حاضر با تأکید بر شناسایی قربانیان و پیامدهای جرائم سایبری در نظام سلامت توسط پرستاران قانونی، به بیان نقش این پرستاران در پیشگیری از این جرائم و برقراری امنیت سایبری پرداخته‌شده است.

۲. مفاهیم نظری

در این بخش فضای مجازی[1]، امنیت سایبری[2] جرائم سایبری[3]، پیشگیری از جرم[4] و پرستاری قانونی[5] به‌عنوان مفاهیم اصلی پژوهش مورد تحلیل و بررسی قرارگرفته است.

۲,۱. فضای مجازی

امروزه محیط مجازی بخش مهمی از زندگی بشر را در برگرفته به‌گونه‌ای که مراودات انسان‌ها در این محیط بر مراودات فیزیکی و سنتی غالب گردیده و با سرعتی وصف‌ناپذیر توسعه‌یافته تا آنجا که بدون آن، زندگی اجتماعی امکان‌پذیر نخواهد بود. اینترنت، تلفن همراه و سایر رسانه‌های مختلف دنیای جدیدی را فراهم نموده‌اند که هریک از آن‌ها به لحاظ وسعت مطالب، وجوه مشترک همه آن‌ها از دیدگاه جرم‌شناسی تحت عنوان «فضای مجازی» بیان می‌گردد (محسنی، ۱۳۹٤: ۳۳۷).

فضای مجازی، مفهومی برای توصیف فناوری دیجیتال به‌هم‌پیوسته گسترده‌ای است که با افزایش استفاده از اینترنت، شبکه و مخابرات دیجیتال به‌سرعت در حال رشد می‌باشد (نوروزیان و همکاران، ۱٤۰۲:۳٤) و همانند دنیای واقعی در کیفیت زندگی افراد جامعه تأثیرگذار است. فضای مجازی در این معنا «به

---

[1]. Cyberspace
[2].Cyber security
[3]. Cybercrimes
[4]. Crime Prevention
[5]. Forensic Nursing

مجموعه‌هایی از ارتباط درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. در این فضا مرز بین دنیای درون و بیرون تقریباً ناپدید می‌شود و دیگر زمان معنایی ندارد. درواقع می‌توان گفت فضای مجازی گستره‌ای از ذهن است که می‌تواند تمامی اشکال زندگی واقعی را بسط و معنا دهد» (نوروزی و افراخته، ۱٤۰۰: ۲٦٥).

برخلاف فضای فیزیکی که دارای محدودیت‌های زیادی چون محصور بودن شخص در زمان و مکان است، فضای مجازی به‌گونه‌ای است که اشخاص قادر هستند در یک‌زمان در قلمروهای مجازی مختلفی حضورداشته و فعالیت کنند. علاوه بر این، گمنام ماندن در فضای مجازی و اتخاذ نام‌های جعلی نسبت به فضای فیزیکی بسیار ساده‌تر است. ازاین‌روست که گفته می‌شود سرعت، کثرت، سهولت ارتکاب جرم، کم‌هزینگی، عدم محدودیت به مرزهای جغرافیایی، ناشناختگی باعث بروز جرائمی شده است که از سایر جرائم متمایز است (بهره‌مند، ۱۳۹٦:٥٥).

۲,۲. امنیت سایبری

فضای مجازی محیطی جذاب برای کاربران خود به وجود آورده که سبب فریب کاربران و ایجاد اعوجاج در نگرش‌های آنان شده است، بنابراین لزوم رعایت امنیت در این فضا که امنیت سایبری نامیده می‌شود، احساس می‌گردد. امنیت، بنیادی‌ترین نیاز هر جامعه و مهم‌ترین عامل برای دوام زندگی اجتماعی به شمار می‌رود. مفهوم امنیت تحت تأثیر تحولات سطح کلان بین‌الملل دستخوش تغییر شده و با شروع روند جهانی‌شدن و تحت تأثیر فناوری اطلاعات و ارتباطات مفهومی چندبعدی یافته است (حیدری، ۱٤۰۱: ٤۹).

امنیت سایبری شامل حفاظت از اطلاعات با پیشگیری، شناسایی و پاسخ به حملات سایبری است. باوجود تدابیر بسیار پیشرفته فناوری مانند ممیزی، احراز هویت، مجوز و اقدامات حفظ حریم خصوصی داده‌ها مانند رمزگذاری، خطای انسانی می‌تواند باعث نقص در امنیت شود؛ بنابراین، امنیت سایبری از اولویت بالایی برخوردار است (Kamerer & McDermott, 2020: 48).

فناوری همگام ایجاد تحول در پزشکی، حوزه سلامت را با چالش‌هایی مواجه ساخته و حریم خصوصی بیماران را در معرض تهدید قرار داده است. با افزایش مقیاس داده‌های بیمار؛ ایمنی و یکپارچگی اطلاعات

پزشکی به‌طور فزاینده‌ای درخطر است. به‌طوری‌که امروزه مسائل امنیت سایبری و حریم خصوصی در تحقیقات ژنومی، تجهیزات پزشکی مانند ضربان‌سازها و فناوری‌های پوشیدنی که به‌طور مداوم داده‌های بیومتریک را از طریق حس‌گرهای الکترونیکی هوشمند ضبط و داده‌ها را از طریق اینترنت مبادله می‌کنند در برابر حملات سایبری آسیب‌پذیر و باید موردتوجه قرار گیرند (Luh & Yen, 2020: 3).

متأسفانه، جامعه شاهد نرخ هشداردهنده‌ای از حملات سایبری و نقض حریم خصوصی بیماران است. نرخ نقض امنیت اطلاعات بهداشتی ۲۱ درصد از کل نقض امنیت سایبری در سراسر جهان را تشکیل می‌دهد (Heald, 2017: 270). به‌عنوان‌مثال با توسعه فناوری اطلاعات الکترونیک، استفاده از پرونده سلامت الکترونیک[1] رویکردی رایج برای ثبت اطلاعات پزشکی بیماران محسوب می‌شود. این اطلاعات در پایگاه‌های اطلاعاتی بیمارستان‌ها و نهادهای پزشکی ثبت و ذخیره می‌شود و بیماران هیچ‌گونه کنترلی نسبت به اطلاعات پزشکی خود ندارند، بنابراین، نگرانی‌هایی جدی در خصوص امنیت و حفظ حریم خصوصی داده‌های پزشکی و چگونگی دسترسی به این اطلاعات وجود دارد، زیرا داده‌های پزشکی می‌تواند به‌راحتی سرقت، دست‌کاری و یا حتی به‌طور کامل حذف شوند که این امر موجب تأخیر در فرآیند درمان و یا حتی به خطر انداختن زندگی بیمار خواهد شد (پور نقی، بیات و فرجامی، ۱۳۹۹: ۱۰۲).

۲,۳. جرائم سایبری

ظهور فناوری‌های جدید و ایجاد فرصت‌های مجرمانه سبب شده است که ارتکاب رفتارهای مجرمانه از طریق این بستر با رشد خیره‌کننده‌ای روبه‌رو شود. به همین دلیل بررسی جرائم سایبری و شناخت زوایای گوناگون آن از اهمیت ویژه‌ای برخوردار است (دهقان‌فر، پاک نهاد و ایروانیان، ۱٤۰۲: ۱۸).

۲,۳,۱. تعریف جرائم سایبری

جرائم سایبری، طیف گسترده‌ای از افعال مجرمانه را شامل می‌شود و ماهیت متغیر آن ناشی از پیشرفت لحظه‌به‌لحظه فناوری اطلاعات و شیوه‌های سوءاستفاده از آن است. در تعریف جرائم سایبری دو معنی و مفهوم وجود دارد. در تعریف مضیق، جرم سایبری عبارت از جرائمی است که فقط در فضای سایبر

[1]. Electronic Medical Record (EMR)

رخ می‌دهد، مانند هرزه‌نگاری، افترا، آزار و اذیت و سوءاستفاده از پست الکترونیکی. جرائمی که در آن‌ها کامپیوتر به‌عنوان ابزار و وسیله ارتکاب جرم به کار گرفته می‌شود، در زمره جرائم سایبری قرار نمی‌گیرد. در تعریف موسع، جرم سایبری هر فعل و ترک فعلی است که «در» یا «از طریق» یا «به کمک» از طریق اتصال به اینترنتت، چه به‌طور مستقیم یا غیرمستقیم رخ می‌دهد و توسط قانون ممنوع و برای آن مجازات در نظر گرفته‌شده است. بر این اساس جرائم سایبری را می‌توان به سه دسته تقسیم کرد: دسته اول، جرائمی هستند که در آن‌ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند مانند سرقت و تخریب. دسته دوم، جرائمی هستند که در آن‌ها رایانه به‌عنوان ابزاری برای مجرم در ارتکاب جرم به کار گرفته می‌شود. دسته سوم، جرائمی هستند که می‌توان آن‌ها را جرائم سایبری محض نامید. این نوع از جرائم کاملاً با جرائم کلاسیک تفاوت دارند و تنها در دنیای مجازی به وقوع می‌پیوندند اما آثار آن‌ها در دنیای واقعی ظاهر می‌شود؛ مانند دسترسی غیرمجاز به دستگاه‌های رایانه‌ای (کرمی، ۱۳۹۷: ۳۳۷-۳۳۸).

هیچ تعریف واحدی از جرائم سایبری وجود ندارد و این امر احتمالاً به این دلیل است که این پدیده به‌طور مداوم در حال تکامل و گسترش است. توماس و لودر[1] جرائم سایبری را به‌عنوان «فعالیت‌های رایانه‌ای که غیرقانونی بوده یا توسط طرف‌های خاص غیرقانونی در نظر گرفته می‌شوند و می‌توانند از طریق شبکه‌های الکترونیکی جهانی انجام شوند» تعریف می‌کنند، درحالی‌که گوردون و فورد[2] «هر جنایتی که با استفاده از رایانه، شبکه یا دستگاه سخت‌افزاری تسهیل یا ارتکاب می‌یابد» را جرائم سایبری می‌نامند (Phillips et al, 2022: 382).

به نظر می‌رسد صرف‌نظر از اختلاف‌نظرها در این مقوله کامل‌ترین تعریفی که با توجه به رویکرد قانون جرائم رایانه‌ای مصوب ۱۳۸۸، بتوان ارائه کرد بدین‌صورت باشد: «هر جرمی که قانون‌گذار به‌صراحت رایانه را به‌منزله موضوع یا وسیله جرم جزء رکن مادی آن اعلام کرده باشد، یا عمل رایانه به‌منزله موضوع یا وسیله ارتکاب یا وسیله ذخیره یا پردازش یا انتقال دلایل جرم در آن نقش داشته باشد»، جرم رایانه‌ای تلقی می‌شود (کرمی، ۱۳۹۷: ۳۳۸).

۲،۳،۲. انواع جرائم سایبری

---

[1]. Thomas and Loader
[2]. Gordon and Ford

جرائم سایبری را ازلحاظ فلسفه قانون‌گذاری و قوانین حاکم بر آن‌ها می‌توان به دو گروه تقسیم کرد. گروه اول شامل طیفی از جرائم رایانه‌ای است که با قوانین مربوط به جرائم کلاسیک قابل‌تعقیب و مجازات هستند و نیاز به قانون‌گذاری جدید ندارند و می‌توان آن‌ها را به جرائم علیه اشخاص، اموال، امنیت و آسایش عمومی، اخلاق، عفت عمومی و خانواده دسته‌بندی نمود. گروه دوم شامل طیفی از جرائم رایانه‌ای است که دسته‌ای از آن، جرائم جدیدی هستند که ارتکاب آن‌ها قبل از پیدایش فناوری اطلاعات به‌هیچ‌وجه امکان‌پذیر نبوده است، مانند دستیابی غیرمجاز، شنود غیرمجاز، اخلال درداده و اخلال در سیستم (پور ابراهیم، ۱٤۰۰: ۱۵۸).

جرائم سایبری را به سیستم‌های دوگانه[1] و سه‌گانه[2] نیز طبقه‌بندی می‌کنند. در طبقه‌بندی دوگانه، جرائم سایبری را بر اساس نقشی که فناوری در ارتکاب جرم یا عمل ایفا می‌کند، تفکیک و بین جرائم «مبتنی بر سایبری» و «وابسته به سایبری» تمایز قائل می‌گردند. جرائم وابسته به سایبری جرائمی هستند که با ظهور فناوری به وجود آمده و نمی‌توانند خارج از دنیای دیجیتال واقع گردند مانند هک کردن. در مقابل، جرائم مبتنی بر سایبری، جرائم سنتی هستند که پیش از ظهور این فناوری بوده و اکنون توسط فناوری سایبری تسهیل شده‌اند و از جرائم یقه‌سفیدها تا قاچاق مواد مخدر، آزار و اذیت آنلاین، تروریسم و فراتر از آن را شامل می‌شود (Phillips et al, 2022: 383).

در طبقه‌بندی‌های سه‌گانه؛ دو رویکرد متفاوت ارائه شده ا ست. در رویکرد اول، طبقه‌بندی سه عاملی جدید از جرائم سایبری بر اساس نقش فناوری در عمل مجرمانه به‌صورت جرائم در دستگاه، جرائم با استفاده از دستگاه و جرائم علیه دستگاه مطرح شد. در رویکرد دومی تلاشی برای گسترش طبقه‌بندی دوگانه فوق با یک دسته اضافی (جرائم مبتنی بر سایبری، جرائم وابسته به سایبری و جرائم به کمک سایبری) صورت پذیرفت (Nurse, 2018: 3).

۲,٤. پیشگیری از جرم

جرم از بزرگ‌ترین معضلاتی است که در طول تاریخ، امنیت جوامع انسانی را با چالش‌های جدی مواجه ساخته و پیشگیری از آن همواره ذهن بشر را به خود مشغول داشته است. پیشگیری از جرم، موضوعی

---

[1]. Dichotomies of Cybercrime
[2]. Trichotomies of Cybercrime

میان‌رشته‌ای است که به دلیل ارتباط تنگاتنگی که با انسان و جامعه انسانی دارد، نهادی زنده و پویا، با عناصر متغیر در جوامع مختلف و نیازمند روزآمد شدن مداوم است (محسنی، ۱۳۹٤: ٥٦).

پیشگیری در معنای عام، گستره وسیعی از اقدامات کیفری و غیر کیفری را در برمی‌گیرد و در معنای مضیق، فقط تدابیر غیر کیفری را شامل می‌شود. ریموند گسن[1]، پیشگیری از بزه‌کاری را مهم‌ترین سازوکار سیاست جنایی دانسته که با توسل به اقدام‌های غیر قهرآمیز درصدد کاهش یا از بین بردن عوامل فردی، محیطی و وضعی جرم‌زا و گرایش به بزه‌کاری است (نیاز پور، ۱۳۹۵: ۹۲). طبق متن ماده ۱ قانون پیشگیری از وقوع جرم (۱۳۹٤)، پیشگیری از وقوع جرم عبارت است از پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدامات لازم برای از میان بردن یا کاهش آن. در الگوهای علمی پیشگیری از جرم مراحل شناسایی مسئله جرم و هدف‌گذاری، آسیب‌شناسی علل جرم، ارائه راه‌حل‌های کاربردی، اجرای راه‌کارهای پیشگیرانه و ارزیابی نتایج دیده می‌شود.

۲,٤,۱. پیشگیری از جرم در فضای مجازی

مزایای استفاده از اینترنت و فناوری‌های دیجیتال بر کسی پوشیده نیست، اما چالش‌ها و نگرانی‌های زیادی را فراروی جامعه بشری قرار داده است. نکته مهم این است که مجرمان سایبری آمادگی و تمایل فراوانی به بهره‌برداری از نیازها و ضعف‌های روانی انسان مانند تمایل ذاتی آنان به اعتماد و کمک به یکدیگر، نیاز به عشق و محبت دارند و این در حالی است که متأسفانه این ویژگی‌ها بر تصمیم‌گیری انسان در مورد امنیت بسیار تأثیرگذار هستند.

به دلیل سابقه مجرمان سایبری در سوءاستفاده از نیازها و ضعف‌های روانی قربانیان که بر پیچیدگی و توانمندی آن‌ها افزوده، رویکردهای پیشگیری، شناسایی و بازدارندگی از رفتارهای مجرمانه آن‌ها نیز باید توسعه یابد. حوزه امنیت سایبری دارای طیف وسیعی از مدل‌ها، دستگاه‌ها و ابزارهای جدید است که هدف آن‌ها جلوگیری و شناسایی حملات علیه افراد است. جرم‌شناسی نیز یک حوزه کلیدی است و در حال حاضر قوانین متعددی در سراسر جهان وجود دارد که به دنبال جلوگیری از جرائم آنلاین و محاکمه مرتکبان آن هستند. در اتخاذ رویکردهای پیشگیری از جرائم در فضای مجازی، تدوین برنامه‌های هماهنگ

[1]. Raymond Gassin

و میان‌رشته‌ای الزامی است زیرا تنها از این طریق است که می‌توان بینش هر حوزه را به‌درستی تجزیه‌وتحلیل کرد تا به موضوع جرائم سایبری به‌طور کامل و جامع پرداخت (Nurse, 2018: 24).

۲,٤,۲. نقش نظام سلامت در پیشگیری از جرم

جامعه ما دچار بیماری مزمن کثرت جرائم و تخلفات شده است که حاصل آن فشار بیش‌ازحد به قوه قضائیه است. برای برون‌رفت از این چالش باید با رویکرد بهداشت قضایی، سلامت حقوقی و اصلاح مبادی ورودی جرائم، از وقوع جرم جلوگیری و از اصلاح ساختارها و فن‌های پیشرفته روز دنیا استفاده کرد. از همان ابتدای تدوین قانون اساسی، عده‌ای معتقد بوده‌اند که قوه قضاییه بدون همکاری قوه‌ی مجریه نمی‌تواند در امر پیشگیری از وقوع جرم حرکت قابل‌توجهی انجام دهد (صبح دل، ۱۳۹٦: ۹۳).

سازمان‌ها، وزارتخانه‌ها و تشکیلات دولتی می‌توانند به‌طور مستقیم یا غیرمستقیم نقش پیشگیرانه خویش را در قالب پیشگیری اجتماعی یا وضعی ایفاء می‌کنند. ازجمله می‌توان به نقش وزارت بهداشت، درمان و آموزش پزشکی در این رابطه اشاره کرد. نقش این وزارتخانه در سیاست‌گذاری حوزه سلامت و همچنین ارائه خدمات سلامت به قربانیان و در برخی موارد به مجرمان که به دلیل ابتلای به برخی بیماری‌ها مرتکب جرم می‌گردند، موقعیت حساسی و مؤثری را برای این وزارتخانه در پیشگیری و کاهش جرائم رقم می‌زند.

پرستاران متخصصانی هستند که به دلیل ارتباط نزدیک با قربانیان جرائم می‌توانند در پیشگیری و مقابله با جرم نقش مؤثری ایفا نمایند و در رابطه با مراقبت از قربانیان جرائم سایبری علیه اشخاص مانند کلاه‌برداری در مراقبت‌های بهداشتی، برخوردهای جنسی غیرقانونی، زورگویی سایبری، هرزه‌نگاری کودکان می‌توان از تخصص پرستاری قانونی بهره جست (Hammer et al, 2013: 306).

۲,۵. پرستاری قانونی

تحول در علوم بهداشتی انگیزه مطالعات متعددی را در زمینه عملکرد و نقش پرستاران برانگیخته است. پرستاری قانونی یکی از رشته‌های تخصصی است که علوم پرستاری را با فرآیندهای قانونی تلفیق و به بررسی مرتکبان یا قربانیان خشونت، رویدادهای آسیب‌زا یا سایر وقایع جنایی می‌پردازد (Özdena et al, 2019: 86). پرستاران قانونی با شناسایی و مراقبت از قربانیان و حمایت از بازماندگانشان قادر به

ارائه تصویری علمی و بشردوستانه از این فراموش‌شدگان هرج‌ومرج دنیای بحران‌زده کنونی ازجمله زنان و کودکان آسیب‌پذیر هستند (Scannell, 2018: 12).

پرستاران قبل از ارزیابی و مراقبت این فرض را در نظر دارند که مددجوی تحت مراقبت آن‌ها می‌تواند یک بیمار قانونی باشد. بیمارانی که علاوه بر دریافت خدمات بهداشتی و درمانی نیازمند خدمات سیستم قضایی هم‌زمان هستند را بیمار قانونی می‌نامند (Erkan et al, 2017: 1). آنان باهدف قرار دادن افراد در معرض خطر و مشارکت در مداخلات کلیدی همچون اطلاع‌رسانی و آموزش، فعالیت‌های پیشگیرانه خود را گسترش دهند.

۲,۵,۱. تعریف و پیشینه پرستاری قانونی

پرستاری قانونی تلفیقی از پرستاری و فرآیندهای قانونی است؛ به‌عبارتی‌دیگر استفاده از جنبه‌های قانونی مراقبت‌های سلامتی همراه با آموزش‌های زیستی، روانی و اجتماعی پرستاری در روند تحقیقات علمی، درمان تروما و یا مرگ‌ومیر قربانیان و مرتکبان سوء رفتار، خشونت، حوادث و فعالیت‌های جنایی است (Hammer et al, 2013: 3).

از دیرباز، پرستاران وظیفه مراقبت از قربانیان خشونت را بر عهده داشته و واسطه‌ای بین دو نظام سلامت و عدالت کیفری بودند. مشکلات موجود در شناسایی قربانیان و افزایش مراجعه آنان به بیمارستان‌ها، ضرورت پرستاری قانونی را در دهه ۱۹۷۰ آشکار کرد. پرستاری قانونی برای اولین بار از امریکا منشأ گرفت و سپس به سایر کشورها گسترش یافت. در برخی کشورها همچون ایالات‌متحده و کانادا، پرستاران قانونی مرزهای عملیاتی خود را به سمت تشکیل نقش‌های مستقل حرفه‌ای نظیر مشاغل کارآگاهی، تحقیقات پلیسی، وکالت، حوادث و بیمه گسترش داده است.

۲,۵,۲. نقش‌های پرستاری قانونی

وجود پرستاران قانونی در برهه‌ای که سیر جرم و خشونت روند فزاینده‌ای را دنبال می‌کند، بسیار حیاتی است. رفع نیازهای بهداشتی و قانونی قربانیان، مظنونان و عاملان خشونت ضرورت معرفی و به‌کارگیری پرستارانی را ایجاب نمود که آموزش‌های لازم را در هر دو حوزه پرستاری و قانونی دریافت داشته و قادر به مراقبت‌های جامع و قانونی باشند (Berishaj et al, 2020: 286). پرستاران قانونی برای حمایت از حقوق قانونی مددجویان در قالب نقش‌های متنوعی مانند پرستار قانونی بالینی[1]، پرستار قانونی محقق

[1]. Forensic Clinical Nurse

مرگ[1]، بازرس پرستار قانونی[2]، پرستار قانونی معاینه گر تجاوز جنسی[3]، مدیران خطر[4]، روان پرستار قانونی[5]، پرستار قانونی اصلاحی[6]، وکیل پرستار[7]، پرستار مشاور حقوقی[8] و پرستار پزشکی قانونی[9] در بسیاری از کشورها فعالیت می‌کنند (صدقی ثابت و همکاران، ۱۴۰۱:۱۱-۷).

پرستاران قانونی ضمن مراقبت از قربانیان و بازماندگان خشونت‌ها، با جمع‌آوری و مستندسازی شواهد، از حقوق قانونی مددجویان خود دفاع نموده و بنا به‌ضرورت شهادت تخصصی می‌دهند (Amar and Sekula, 2015: 8). نقش پرستاران قانونی را نباید با نقش پزشکان قانونی و یا مجریان قانون اشتباه گرفت. آن‌ها بیش از هر چیز پرستارانی هستند که برای مراقبت از بیماران آموزش‌دیده‌اند ولی ازآنجایی‌که پزشکان قانونی تمام‌وقت نزد قربانیان خشونت در مراکز درمانی حضور ندارند، نیاز به وجود متخصصینی که علاوه بر انجام اقدامات لازم قانونی، به‌طور دائم در مراکز درمانی مستقر باشند، بیش‌ازپیش احساس می‌گردد (Aravani, 2020: 17). ضرورت وجود پرستاران متخصص در علوم قانونی برای پیشگیری از خشونت مورد تأکید سازمان بهداشت جهانی قرارگرفته و توصیه‌شده که برای حل مشکل خشونت، خدمات و مراقبت‌های باکیفیت، مؤثر و مبتنی بر نیازهای قربانیان و امنیت آنان توسط متخصصان آموزش‌دیده نظام سلامت ارائه شود (Donaldson, 2020: 2). پرواضح است که خدمات این دسته از پرستاران شامل حال قربانیان خشونت سایبری نیز خواهد بود.

۲،۵،۳. جنبه‌های عملی پرستاری قانونی

پرستاران بخش‌های اورژانس نخستین افرادی هستند که با پرونده‌های پزشکی قانونی ارجاع شده مواجه شده، وسایل و بدن قربانی را در حین معاینه بررسی نموده و با بستگان وی ارتباط برقرار می‌کنند. مهارت تفکر انتقادی، توجه به جزئیات، اندیشیدن به مسائل حقوقی پیرامون مددجویان و برخورداری از دانش پزشکی قانونی آنان را قادر به ارائه رویکردی فعال در پیشگیری از جرم با شناسایی قربانیان، جلوگیری

---

1. Forensic Nurse Death Investigator (FENDI)
2. Forensic Nurse Examiner
3. Sexual Assault Nurse Examiner (SANE)
4. Risk Manager
5. Psychiatric Forensic Nurse
6. Forensic Correctional, Institutional, or Custodial Nursing
7. Nurse Attorney
8. Legal Nurse Consultant
9. Nurse Coroner

از آسیب بیشتر یا مرگ ناشی از خشونت دوره‌ای، تشخیص زودهنگام موقعیت‌های بالقوه عاملان سوء رفتار و مستندسازی شواهد می‌نماید.

توانایی پرستاران در کشف و جمع‌آوری شواهد جرم بر نتیجه تصمیمات قانونی تأثیر بسزایی دارد زیرا همواره این احتمال وجود دارد که نتایج حاصل از رسیدگی پرونده‌های جنایی تحت‌الشعاع جمع‌آوری نادرست یا ناقص شواهد قانونی در موقعیت‌های پیچیده قرار گیرد. پرستاران مسئول هدایت تحقیقات قانونی نیستند اما موقعیت آنان در شناسایی، جمع‌آوری و حفظ شواهدی که می‌تواند برای تحقیقات قانونی ضروری باشد را نمی‌توان نادیده گرفت.

۳. نقش پرستاران قانونی در پیشگیری از جرائم سایبری

به‌منظور بررسی نقش پرستاران قانونی در پیشگیری از جرائم سایبری و کمک در برقراری امنیت سایبری به تفکیک به بیان نقش آنان در دو مقوله پیشگیری از جرائم سایبری علیه اشخاص و جرائم علیه امنیت سایبری در حوزه نظام سلامت پرداخته می‌شود.

۳,۱. نقش پرستاران قانونی در پیشگیری از جرائم سایبری علیه اشخاص

در جرائم سایبری علیه اشخاص، رایانه وسیله ارتکاب جرم است. مهم‌ترین مصداق‌های جرائم علیه اشخاص یعنی قتل و ایراد آسیب بدنی عمدی و غیرعمدی را می‌توان از رهگذر دستیابی به دستگاه‌های رایانه‌ای بیمارستان‌ها و تغییر دادن علامت‌ها و نسخه‌های یک بیمار مرتکب شد. همچنین جرائم قذف، توهین، افترا و نشر اکاذیب که از جرائم علیه شخصیت معنوی افراد است و سایر جرائم غیر جسمی علیه اشخاص را می‌توان در مقیاسی بسیار گسترده‌تر از گذشته با رایانه مرتکب شد (رحیق اغصان، ۱۳۹۹: ۱۰۳). از انواع جرائم سایبری که علیه اشخاص صورت می‌گیرد می‌توان به مواردی مانند برخوردهای جنسی غیرقانونی، زورگویی سایبری، هرزه‌نگاری کودکان و کلاه‌برداری در مراقبت‌های بهداشتی اشاره کرد.

۳,۱,۱. برخوردهای جنسی غیرقانونی و اینترنت

کودکان و نوجوانان همچنان قربانیان جنسی ناخواسته در فضای مجازی هستند. تمایل نوجوانان به ریسک‌پذیری همراه با مهارت‌های فنی در رایانه، آنان را به جمعیت آسیب‌پذیر تبدیل نموده که گاه عواقب غم‌انگیزی را تجربه خواهند کرد. آن‌ها در فضای مجازی ضمن بحث راجع به فعالیت‌های روزمره خود، به تبادل اطلاعات و ابراز احساسات خود می‌پردازند و در برخی از این موارد چیزهایی را که نباید در معرض دید عموم قرار گیرد، مانند عکس‌های نامناسب یا اطلاعات شخصی خود را به اشتراک می‌گذارند که می‌تواند منجر به بهره‌کشی و اخاذی از آنان گردد. نگرانی اصلی این است که نوجوانان هیچ مشکلی در این اقدام نمی‌بینند.

در این موارد پرستاران قانونی می‌توانند برای ارتقای ایمنی کودکان و نوجوانان جهت استفاده از اینترنت از طریق آموزش و کمک به والدین، کارکنان مدارس و متخصصان مراقبت‌های بهداشتی در مواردی همچون نظارت بر استفاده صحیح از فضاهای مجازی و توجه به تغییرات رفتاری که ممکن است نشانه یک رابطه اینترنتی نامناسب باشد نقش مؤثری را در پیشگیری از جرائم سایبری ایفا نمایند. این پرستاران می‌دانند که بین نظارت بر فعالیت یک نوجوان و تجاوز به حریم خصوصی او مرز باریکی وجود دارد و در اتخاذ استراتژی‌هایی جهت ایمنی این گروه آسیب‌پذیر باید به نیاز آن‌ها به حفظ حریم خصوصی توجه و استقلال متناسب با سن آنان را مدنظر قرار دهند. هرگونه اقدام نامناسب می‌تواند منجر به تلاش نوجوان برای پنهان کردن فعالیت‌هایش از بقیه اعضای خانواده شود (Hammer et al, 2013: 315).

یادآوری این نکته مهم است که بزرگ‌سالان نیز ممکن است قربانی این جرائم شوند، لذا باید در حین استفاده از اینترنت نکات ایمنی را رعایت کنند. ازآنجاکه بزرگ‌سالان به‌طور فزاینده‌ای از اینترنت برای برقراری ارتباط استفاده می‌کنند، متجاوزان نیز به همان اندازه اینترنت را برای یافتن قربانیان احتمالی به‌کار می‌گیرند. اینترنت با دسترسی مجرمان به قربانیان در یک دوره زمانی طولانی به مجرمان این امکان را می‌دهد تا با جلب اعتماد، کنترل آنان را به دست آورده و احتمالاً ملاقاتی را در دنیای فیزیکی با آنان ترتیب دهند.

۳،۱،۲. قلدری سایبری

قلدری، شکل خاصی از رفتار پرخاشگرانه و سوء رفتار مکرر و هدفمند است که توسط فرد یا گروهی علیه قربانی اعمال می‌شود که اغلب نمی‌تواند به‌راحتی از خود دفاع کند. قلدری سایبری نوعی آزار و

اذیت آنلاین است که از طریق ابزارهای فنّاورانه مدرن مانند اینترنت یا تلفن‌های هوشمند رخ می‌دهد (Nurse, 2018: 9). حمله آنلاین ممکن است به‌صورت تهدید، تحقیر، اتهامات صریح جنسی و به‌طورکلی نظرات وحشتناکی باشد که متوجه قربانی شده و برای دیدن عموم به اشتراک گذاشته می‌شود. قلدری سایبری پیامدهایی مانند خودکشی، مشکلات روانی، احساس خشم و خصومت نوجوانان را به همراه دارد که در برخی موارد سبب می‌گردد همین قربانیان خود به مرتکبان بعدی آزار و اذیت سایبری تبدیل گردند (Simsek et al, 2019: 202).

حضور در رسانه‌های اجتماعی در زندگی جوانان رایج شده، به‌طوری‌که بیش از ۹۰ درصد نوجوانان کاربران فضای مجازی هستند و متأسفانه در برخی موارد رسانه‌های اجتماعی به یک پلت فرم اصلی برای آزار و اذیت سایبری تبدیل‌شده است؛ بنابراین، لازم است که مسئولین سلامت و ایمنی جوانان، ازجمله پرستاران، بیشتر به این مشکل فراگیر بپردازند. ازآنجایی‌که پرستاران در مواجهه با قربانیان، با آن‌ها ارتباط برقرار می‌کنند، در موقعیت خوبی قرار دارند تا علائم و پیامدهای اولیه آزار اینترنتی مانند مشکلات جسمی، روانی، اجتماعی و عاطفی را شناسایی و در فرآیندهای پیشگیری شرکت جویند (Byrne et al, 2017: 1).

درحالی‌که اجماع جهانی در مورد مداخلات قانونی متناسب وجود ندارد، اما همه موافق آموزش شیوه‌های رفتاری صحیح هنگام حضور در شبکه‌های اجتماعی جهت مقابله با پدیده قلدری سایبری هستند. پرستار قانونی می‌تواند نقش کلیدی در توسعه چنین برنامه‌هایی ایفا کند (Hammer et al, 2013: 316). آنان اولین شاهدان عواقب آزار و اذیت اینترنتی در زندگی روزمره قربانیان هستند، زیرا قربانیان اغلب با ناراحتی‌های جسمی و روانی ثانویه به قلدری به مراکز درمانی مراجعه می‌کنند. آنان ضمن ارائه خدمات بهداشتی به قربانیان از موقعیت خوبی نیز برای آموزش و ترویج فرهنگ مثبت به قربانیان و همراهان آنان برخوردارند.

۳،۱،۳. هرزه‌نگاری کودکان

هرزه‌نگاری، یکی از مهم‌ترین جرائم علیه اخلاق و عفت عمومی است که طی آن نمایش آشکار رفتار جنسی باهدف هیجان، تحریک یا ارضای جنسی در شکل‌های مختلف ازجمله کتاب، عکس، پویانمایی، مجسمه، متن، نقّاشی، فیلم، بازی و مجله ارائه می‌شود. با گسترش فنّاوری‌های نو، هرزه‌نگاری سنّتی که

در اشیاء فیزیکی خود را نشان می‌داد به فضای مجازی راه یافت و با سرعت چشم‌گیری گسترش پیدا کرد (جواهری، اسماعیلی و حاجی‌تبار فیروزجائی، ۱۳۹۹: ۱۷۳).

در بند پ ماده ۲ قانون الحاق دولت جمهوری اسلامی ایران به پروتکل اختیاری کنوانسیون حقوق کودک در خصوص فروش، فحشاء و هرزه‌نگاری کودکان آمده است: هرزه‌نگاری کودک به هرگونه نمایش کودکِ درگیر در فعّالیّت‌های واقعی یا مشابه‌سازی‌شده آشکار جنسی با هر وسیله یا هرگونه نمایش اندام جنسی کودک برای اهداف عمدتاً جنسی اطلاق می‌شود.

متأسفانه تصاویر دیجیتال به دلیل افزایش توانایی ایجاد، ذخیره و تردد هرزه‌نگاری کودکان در قالب دیجیتال، بسیاری از موانع سنتی اجرای قانون و تدارکات را برای تولید و توزیع انبوه آن مطالب از بین برده و تجارت هرزه‌نگاری کودکان را متحول کرده است. سوءاستفاده از کودک برای هرزه‌نگاری یکی از جدیدترین اشکال سوءاستفاده از کودکان در فعّالیّت‌های مجرمانه جنسی است که ازجمله آثار مخرّب آن، به وجود آمدن اختلالات جنسی و روانی می‌باشد که در برخی موارد می‌تواند به مقدمه‌ای برای جرائم جنسی تبدیل گردد (جواهری، اسماعیلی و حاجی‌تبار فیروزجائی، ۱۳۹۹: ۱۸۲).

به‌منظور پیشگیری از این جرم در فضای مجازی، هوشیاری و نظارت والدین از اهمیت ویژه‌ای برخوردار است و این امر نیازمند آگاهی‌بخشی و آموزش است؛ که پرستاران قانونی در کنار سایر مسئولان و مراجع ذی‌ربط، ضمن تسهیل گزارش هرزه‌نگاری؛ با انجام ارزیابی، مشاوره و آموزش والدین و جامعه، مدافع حمایت از کودکان در برابر این نوع از جرائم خواهند بود.

۳,۱,٤. تقلب در مراقبت‌های بهداشتی

نوجوانان و سالمندان بیش از همه در معرض خطر تقلب در مراقبت‌های بهداشتی هستند. نوجوانان مدام به دنبال راه‌حل یا مشاوره در مورد موضوعاتی مانند وزن، آکنه، افسردگی، جراحی پلاستیک و ورزش هستند و سالمندان نیز که بخش بزرگی از مبتلایان به بیماری‌های مزمن را تشکیل می‌دهند، اغلب به دنبال اطلاعات و محصولاتی برای درمان بیماری‌های خود در اینترنت هستند. برخی وب‌سایت‌ها داروها و محصولاتی را تبلیغ می‌کنند که فاقد ارزش درمانی بوده و در برخی موارد می‌توانند برای جمعیت‌های آسیب‌پذیر فاجعه‌بار نیز باشند (Hammer et al, 2013: 322).

بنابراین می‌توان گفت پرستاران قانونی در ایفای نقش مدافعه‌گری خود نسبت به چنین موقعیت‌های مشکوک هوشیار بوده و با مشاهده و ارزیابی مددجویان از طریق لنز پزشکی قانونی قادر به شناسایی قربانیان این نوع کلاه‌برداری نیز هستند. ازاین‌رو، با برگزاری کارگاه‌ها و سمینارهای آموزشی قادر خواهند بود جمعیت‌های آسیب‌پذیر را در زمینه خطرات ناشی از فعالیت‌های مرتبط با سلامت شخصی در اینترنت آگاه سازند. هم‌چنین آنان با اطلاع از وب‌سایت‌های بالقوه خطرناک می‌توانند در سیاست‌گذاری برای محدود کردن تقلب در مراقبت‌های بهداشتی شرکت فعال داشته باشند.

۳,۲. جرائم علیه امنیت سایبری در حوزه نظام سلامت

جرائم علیه امنیت سایبری در حوزه نظام سلامت به نگرانی فزاینده‌ای برای جامعه بشری تبدیل‌شده است. حمله سایبری یک تهدید بین‌المللی برای مراقبت و ایمنی بیمار است و از تمام عرصه‌های مراقبت‌های بهداشتی عبور می‌کند. استفاده گسترده از پرونده الکترونیک سلامت، شبکه‌های سیستم اطلاعات مراقبت‌های بهداشتی، تراکنش‌های اطلاعاتی و تجهیزات مبتنی بر فناوری، چالش‌هایی را برای پرستارانی که فناوری را در کارکردهای شغلی روزانه خود مدیریت می‌کنند، ایجاد می‌کند. به‌عنوان کاربران خط مقدم، پرستاران همچنین نقشی حیاتی در حفظ اطلاعات بهداشتی و مدیریت امنیت سایبری ایفا می‌کنند (Kamerer & McDermott, 2020: 48).

امنیت پرونده الکترونیک سلامت و حفظ حریم خصوصی اطلاعات سلامت از اولویت‌های حیاتی همه مراکز بهداشتی درمانی است. تهدیدات سایبری داخلی ممکن است از سوی کارمندان ناراضی، کارمندانی که آموزش امنیت سایبری مناسبی ندارند یا مهاجمان خارجی که به‌عنوان هکر شناخته می‌شوند، رخ دهد. جرائم سایبری تهدیدی جدی و نگران‌کننده علیه نظام سلامت است. عواقب این حملات می‌تواند به یک کابوس مالی و شخصی برای بیماران و خانواده‌ها تبدیل شود. در سال ۲۰۱۳، تخمین زده شد که آمریکایی‌ها ۱۲ میلیارد دلار برای مقابله با عواقب پرونده‌های پزشکی به خطر افتاده خود هزینه کردند برخی از پیامدهای به خطر افتادن اطلاعات سلامتی بیمار شامل سرقت، کلاهبرداری و سوءاستفاده است (Luna et al, 2016: 2).

مجرمان سایبری می‌توانند یک سازمان مراقبت‌های بهداشتی را از طریق هک کردن، استقرار بدافزارها و باج افزارها و سرقت داده‌ها فلج کنند. پرونده الکترونیک سلامت در معرض خطر ممکن است با قطع

درمان، آسیب جدی به بیماران وارد کند که به‌طور بالقوه می‌تواند منجر به آسیب یا مرگ شود. سرقت هویت و دست‌کاری داده‌ها نیز می‌تواند منجر به هزینه‌های شخصی نجومی برای بیماران و کارکنان نظام سلامت در قالب تقلب اعتباری، هزینه‌های قانونی و هزینه‌های اضافه برداشت و همچنین عوارض روحی و استرس ناشی از برخورد با این پیامدها شود (Kamerer & McDermott, 2020: 48-49).

تهدیدات فزاینده امنیت سایبری در نظام سلامت ایجاب می‌کند که حفظ امنیت اطلاعات در نظام سلامت یک موضوع ضروری در پرستاری باشد. در دنیای دیجیتال امروزی، پرستاران باید از خطر دست‌کاری عمدی داده‌ها و سیستم‌های بیمار آگاه باشند تا بتوانند تهدیدات و مشکلات بالقوه مرتبط با یکپارچگی و امنیت داده‌ها و سیستم‌ها را شناسایی کنند، زیرا آنان رابط بین دنیای بالینی و فناوری اطلاعات هستند و نقش مهمی در کاهش تهدیدات داخلی دارند. اگر پرستار از تهدید داخلی مشکوک یا سایر فعالیت‌های غیرعادی آگاه شود، باید فوراً به مسئولین مربوطه در سازمان اطلاع داده و جزئیات را مستند کند (Lee, 2020: 63).

با گسترش استفاده از پرونده الکترونیک سلامت در کشور، پرستاران قانونی می‌توانند از حملات سایبری در مراکز بهداشتی درمانی جلوگیری کرده و به‌طور مناسب به آن‌ها پاسخ دهند. نکات حفاظتی مانند عدم به اشتراک‌گذاری رمزهای عبور، عدم کلیک روی لینک‌های ناامن یا ناشناس در ایستگاه‌های پرستاری، گزارش فوری ایمیل‌های مشکوک به مراجع ذی‌صلاح به‌منظور پیشگیری و گزارش تهدیدات سایبری و حفظ امنیت سایبری توصیه‌شده است زیرا کمک آنان در توقف تهدیدات سایبری و نقض امنیت حیاتی است (Kamerer & McDermott, 2020: 50).

ازآنجاکه حملات سایبری می‌تواند بر مراقبت از بیمار تأثیرگذار باشد، بنابراین پرستاران آگاه به مدد هوشیاری خود می‌توانند با اقداماتی مانند شناسایی و گزارش به‌موقع تهدیدها و اقدامات صحیح به جلوگیری از مخاطرات و پیامدهای ناگوار ناشی از تهدیدات سایبری کمک نمایند.

نتیجه‌گیری

عصر اینترنت مزایا و همچنین چالش‌های بزرگی را به همراه داشته است. صاحب‌نظران در سال‌های اخیر در وضعیت آشفته‌ای قرار داشته و همه در تلاش هستند تا پیامدهای چالش جرائم سایبری و نقض امنیت سایبری را شناسایی و ضمن واکنش‌های مناسب، روش‌هایی را برای مقابله با آن اتخاذ کنند. تلاش‌های

زیادی برای بهبود وضعیت موجود صورت می‌پذیرد، ولی به دلیل ماهیت خاص جرائم سایبری و ارتکاب آن در فضای مجازی و نیز پیچیدگی‌های مسیر کشف جرم؛ قانون‌گریزی همچنان در فضای سایبری حاکم است. در این میان، حوزه نظام سلامت و ذینفعان آن نیز از این آشفتگی‌ها مصون نبوده و متحمل آسیب‌های فراوانی می‌شوند.

با افزایش چشمگیر جرائم سایبری علیه اشخاص و آمار فزاینده قربانیان به‌ویژه قربانیان خشونت سایبری که نیازمند خدمات درمانی و مراقبتی هستند، مسئولیت خطیری بر عهده نظام سلامت نهاده شده است. پرستاران که ستون فقرات نظام سلامت را تشکیل می‌دهند، نقشی مهم در کمک به این قربانیان دارند. به استناد قانون پیشگیری از وقوع جرم (۱۳۹٤) و به مدد اختیارات برگرفته از آن در وضعیت کنونی می‌توان با استمداد از نهادهای مختلف اجتماعی تا حدی از قربانیان خشونت حمایت و از بروز مجدد بزه دیدگی آنان پیشگیری نمود. بهره‌مندی از ظرفیت‌های نظام سلامت یکی از این راهکارها محسوب می‌گردد و از تأثیرگذارترین متخصصان در این نظام، پرستاران هستند که در خط مقدم مواجهه با قربانیان قرار دارند.
در سمت دیگر این طیف، وضعیت امنیت سایبری در نظام سلامت قرار دارد که نگرانی‌های بی‌سابقه‌ای را ایجاد می‌کند. مددجویان، سازمان‌ها و کارکنان نظام سلامت از تهدیدات و نقض امنیت سایبری رنج می‌برند. ازآنجایی‌که پرستاران نقش مهمی در حفاظت از اطلاعات بیمار دارند، فناوری مراقبت‌های بهداشتی بخشی جدایی‌ناپذیر از نقش حرفه‌ای آن‌ها است. اولین گام در مقابله با تهدیدات سایبری، درک موضوع رویکرد کنونی ما برای امنیت داده‌ها در حوزه نظام سلامت است. تضمین امنیت سایبری در نظام سلامت، به‌ویژه در مواجهه با افزایش دیجیتالی شدن و به اشتراک‌گذاری داده‌ها، نیازمند مشارکت هماهنگ متخصصان، ارائه‌دهندگان خدمات سلامت، اخلاق مداران، نهادهای نظارتی، بیماران و به‌طورکلی جامعه است.

در پاسخ به پرسش پژوهش حاضر مبنی بر این‌که نقش پرستاران قانونی در امنیت سایبری و پیشگیری از جرائم در فضای مجازی چیست؟ یافته‌ها حاکی از این بودند که قربانیان خشونت‌های سایبری اغلب با طیف گوناگونی از شکایات جسمی و روانی و در برخی موارد حتی با قصد و اقدام به خودکشی و سوءمصرف مواد به بخش‌های اورژانس مراجعه می‌کنند. در آنجا پرستاران با رویکردی کل‌نگر و ابراز همدلی و درک پیچیدگی‌های این نوع خشونت؛ به ارزیابی و رفع نیازهای جسمی، عاطفی و روانی این قربانیان می‌پردازند. در برخی کشورها جهت رفع این معضل مبادرت به جلب همکاری پرستاران قانونی

در مراکز درمانی کردند. پرستاران قانونی هنگام ارائه مراقبت‌ها با اندیشیدن به مسائل حقوقی پیرامون مددجویان و برخورداری از دانش پزشکی قانونی قادر به ارائه رویکردی فعال در پیشگیری از جرم از طریق شناسایی قربانیان، جلوگیری از آسیب بیشتر یا خودکشی ناشی از خشونت، تشخیص زودهنگام موقعیت‌های بالقوه عاملان سوء رفتارها و مستندسازی شواهد بوده و مسئولیت همکاری با مجریان قانون برای حفاظت از حقوق قربانیان تحت مراقبت را نیز می‌پذیرند.

از سویی دیگر، به دلیل استفاده گسترده از پرونده الکترونیک سلامت، شبکه‌های سیستم اطلاعات مراقبت‌های بهداشتی، تراکنش‌های اطلاعاتی و تجهیزات مبتنی بر فناوری در نظام سلامت، پرستاران به‌عنوان کاربران خط مقدم، نقشی حیاتی در حفظ اطلاعات بهداشتی و مدیریت امنیت سایبری ایفا می‌کنند؛ بنابراین فرضیه پژوهش مبنی بر این‌که پرستاران قانونی در امنیت سایبری و پیشگیری از جرائم در فضای مجازی نقش مؤثری دارند، مورد تائید قرار گرفت. امید آن می‌رود که نتایج حاصل از پژوهش از یک‌سو توجه مسئولین و صاحب‌نظران را به نقش پرستاران قانونی که فراتر از نقش سنتی پرستاران و سازگار با چالش‌های زمانه ما است، جلب نماید و از سویی دیگر آشکارساز این واقعیت باشد که با افزایش ارتباط مستقیم بین ارائه خدمات بهداشتی و قضایی، نقش پرستاران قانونی در شناسایی و پیشگیری از فعالیت‌های مجرمانه در حال گسترش است. علاوه بر این پرستار قانونی می‌تواند به‌عنوان یک مربی، یک مدافع قربانیان جرائم اینترنتی و یک فعال برای قانون‌گذاری مناسب و مؤثر کمک کند.

پیشنهادها

به‌منظور پر شدن خلأ موجود بین دو نظام عدالت و سلامت و کمک به پیشگیری از جرائم در فضای مجازی پیشنهاد می‌شود مسئولین امر مبادرت به آموزش و جلب همکاری پرستاران متخصص در علوم قانونی نموده و با بهره‌مندی از توانمندی این متخصصان حرفه‌ای در جهت تشریک‌مساعی دو نظام از طریق شناسایی قربانیان و پیامدهای جرائم سایبری به برقراری هر چه بیشتر امنیت سایبری کمک نمایند.

منابع

۱. امیریان فارسانی، امین. (۱۴۰۲). «تدابیر پیشگیری وضعی از جرائم سایبری در بوته آسیب‌شناسی حاکم بر آن»، فصلنامه مطالعات حقوقی فضای مجازی، دوره ۲، شماره ۳.

۲. بهره‌مند، حمید. (۱۳۹٦). «چالش‌های مقررات تعدد جرم در جرائم سایبری»، مجله حقوقی دادگستری، سال ۸۱، شماره ۱۰۰.

۳. پور ابراهیم، احمد. (۱٤۰۰). «مروری بر جرائم رایانه‌ای و تبیین ماهیت تاریخی و تقنینی آن»، فصلنامه قضاوت، شماره ۱۰۷.

٤. پور نقی، سید مرتضی. بیات، مجید و فرجامی، یعقوب. (۱۳۹۹). «یک طرح جدید و امن برای اشتراک‌گذاری داده‌های پزشکی مبتنی بر فناوری زنجیره بلوکی و رمزنگاری مبتنی بر ویژگی»، پدافند الکترونیکی و سایبری، سال ۸، شماره ۱.

۵. جواهری، غلامرضا. اسماعیلی، مهدی و حاجی تبار فیروزجائی، حسن. (۱۳۹۹). «هرزه‌نگاری سایبری : از مبانی نظری تا الگوهای واکنش کیفری»، پژوهش حقوق کیفری، دوره ۸، شماره ۳۰.

٦. حسین زاده، روزبه. عطازاده، سعید و قیوم‌زاده، محمود. (۱۳۹۹). «بررسی جرم شناختی جرم هرزه نگاری در فضای سایبر و نقش جامعه در مقابله و پیشگیری از آن»، جامعه‌شناسی سیاسی ایران، سال ۳، شماره ۲.

۷. حیدری، صدیقه. (۱٤۰۱). «عوامل روانشناختی موثر بر فرهنگ و آگاهی امنیت سایبری در دوره شیوع کووید- ۱۹»، فصلنامه رویش روان‌شناسی، سال ۱۱، شماره ۷۵.

۸. دهقان فر، آزاده. پاک نهاد، امیر و ایروانیان، امیر. (۱٤۰۲). «بررسی نقش ویژگیهای محیطی در ارتکاب جرائم بین کاربران فضای مجازی: مطالعه موردی جوانان شیراز»، فصلنامه مطالعات حقوقی فضای مجازی، دوره ۲، شماره ۲.

۹. رحیق اغصان، حسن. (۱۳۹۹). «جرائم ارتکابی علیه اشخاص در فضای مجازی و سایبری»، فصلنامه فقه و حقوق معاصر، سال ٦، شماره ۱۱.

۱۰. صبح دل، محمد (۱۳۹٦). «جایگاه حقوقی قوه قضاییه در پیشگیری اجتماعی»، فصلنامه علمی حقوقی قانون یار، دوره ٤.

۱۱. صبوری، رضا و ثقفی، کامیار. (۱۳۹۸). «بررسی جرائم سایبری حوزه اجتماعی و راهبردهای پیشگیری و مقابله با آن در جمهوری اسلامی ایران»، نشریه امنیت ملی، سال ۹، شماره ۳٤.

۱۲. صدقی ثابت، میترا. محمودی، امیررضا. لرکجوری، عاطفه و دهقان‌زاده، شادی (۱٤۰۱)، «نگاهی به پرستاری قانونی و نقش آن در نظام سلامت و نظام عدالت کیفری»، مجله حقوق پزشکی، دوره ۱٦، شماره ۵۷.

۱۳. کرمی، داوود. (۱۳۹۷). «سیاست کیفری افتراقی در قلمرو ارکان متشکله جرائم سایبری»، فصلنامه مجلس و راهبرد، سال ۲۵، شماره ۹۳.

۱٤. محسنی، فرید. (۱۳۹٤)، جرم‌شناسی، چاپ اول، تهران، انتشارات دانشگاه امام جعفر صادق (ع).

۱۵. نوروزی، زهرا و افراخته، عبدالحمید. (۱٤۰۰). «واکاوی خشونت سایبری زنان و چتر حمایت قانون‌گذاری ملی و بین‌المللی»، پژوهش‌نامه زنان، سال ۱۲، شماره ۲.

۱٦. نوروزیان، حمیدرضا. ملکی، مصطفی و موسوی فرد، سید محمدرضا، (۱٤۰۲). «جستاری بر رویکردهای پیشگیرانه مدیریت فرهنگ محور فضای مجازی و تأثیر آن بر وقوع تخلفات و جرائم انتخاباتی، انتخاب‌های حاکم بر نظام سیاسی ایران، فصلنامه مطالعات حقوقی فضای مجازی، دوره ۲، شماره ۳.

۱۷. نیاز پور، امیرحسین (۱۳۹۵)، «اساسی سازی حقوق پیشگیری از جرم در ایران»، فصلنامه پژوهش حقوق کیفری، شماره ٦.

18. Amar, Angela. F. Sekula, L. Kathleen. (2015). *A practical guide to forensic nursing*. USA: Sigma Theta Tau International.
19. Aravani, Aikaterini. (2020). "The Need for Training in Forensic Nursing", *Nosileftiki*, 59 (1), 17-23.
20. Berishaj, Kelly. et al. (2020). "Forensic Nurse Hospitalist: The Comprehensive Role of The Forensic Nurse in A Hospital Setting", *Journal of Emergency Nursing*, 46(3), 286-293. DOI: 10.1016/j.jen.2020.03.002.
21. Byrne Elizabeth. Vessey, Judith. A. & Pfeifer, Lauren. (2017). 'Cyberbullying and Social Media: Information and Interventions for School Nurses Working With Victims, Students, and Families', *Journal of School Nursing*, 1-13. DOI: 10.1177/1059840517740191.
22. Donaldson, Andrea.E. (2020). "New Zealand emergency nurses knowledge about forensic science and its application to practice", *International Emergency Nursing Journal*, 1-6. Doi: 10.1016/j.ienj.2020.100854.
23. Erkan, Iitir. Yesilyurt, Abdulgani. Kayserili, Aydan. (2017). "Analysis of Awareness for Healthcare Professionals in Forensic Nursing", *Forensic Research & Criminology International Journal*, 5(3), 1-5. DOI:10.15406/ frcij.2017. 05.00153.
24. Hammer, Rita. M. et al. (2013). *Forensic Nursing: A Handbook for Practice*. Second Edition. USA: Kevin Sullivan.
25. Heald, Kristen. (2017). "Why the insurance industry cannot protect against health care data breaches". *Journal of Health Care Law and Policy*, *19*(2), 270–292.
26. Kamerer, Jessica. L. & McDermott, Donna. (2020). "Cybersecurity: Nurses on the Front Line of Prevention and Education", *Journal of Nursing Regulation*, 10 (4), 48-53.
27. *Lee, Kim. (2020).* Cybercrime, ransomware, and the role of the informatics nurse, *Nursing2020*, 50(3), 63-65. DOI-10.1097/01.NURSE.0000654064.67531.c5
28. Luh, Frank. & Yen, Yen. (2020). "Cybersecurity in Science and Medicine: Threats and Challenges', *Trends in Biotechnology*, 1-4.

29. Luna, Raul. et al. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care, 24*(1), 1–9. https://doi.org/10.3233/ THC-151102
30. Nurse, Jason R.C. (2018). "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit", *Printed from The Oxford Handbook of Cyberpsychology*,1-33. DOI: 10.1093/oxfordhb/9780198812746.013.35
31. Özdena, Dilek. et al. (2019). "The impact of forensic nursing course on students" knowledge level on forensic evidence", *Journal of Forensic and Legal Medicine*, 66, 86–90. DOI: 10.1016/j.jflm.2019.06.012.
32. Phillips, Kirsty.et al. (2022). "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies", *Journal of forensic sciences*, 2, 379–398. DOI: org/10.3390/forensicsci2020028.
33. Scannell, Meredith; et al (2018). "Human Trafficking: How Nurses Can Make a Difference". *Journal of Forensic Nursing*, vol 14, No 2, DOI: 10.1097/JFN.0000000000000203.
34. Simsek, Nuray. Sahin, Derya. & Evli, Mahmut. (2019). "Internet Addiction, Cyberbullying, and Victimization Relationship in Adolescents ", *Journal of Addictions Nursing*. 30 (3), 201–210. DOI: 10.1097/JAN.0000000000000296.

۳۵. قانون جرائم رایانه‌ای (۱۳۸۸)

۳۶. قانون پیشگیری از وقوع جرم (۱۳۹٤)

۳۷. قانون الحاق دولت جمهوری اسلامی ایران به پروتکل اختیاری کنوانسیون حقوق کودک در خصوص فروش، فحشاء و هرزه‌نگاری (۱۳۷۹)