بررسی تعارض رهیافت‌های تدابیر موقعیت‌مدار نظارت سایبری، با حریم خصوصی کاربران

زهرا فرهادی آلاشتی* و عبدالرضا جوان جعفری بجنوردی**

تاریخ دریافت ۱۳۹۴/۹/۱۷	تاریخ پذیرش ۱۳۹۵/۳/۱۸

پیشرفت فناوری‌های ارتباطی و اطلاعاتی، شناسایی موقعیت‌های پیش‌جنایی و پیشگیری از بزهکاری احتمالی سایبری را تسهیل کرده است، تا جایی که با کاربست گسترده ابزارهای فاوا، می‌توان امنیت حداکثری این فضا را تأمین کرد. اما، هرچه گستره کاربست روش‌های نظارتی، به‌ویژه نظارت الکترونیکی، افزایش می‌یابد، صیانت از امنیت داده‌های کاربران نیز دشوارتر می‌شود، به‌طوری‌که، همواره چالشی دوگانه فراروی نهادهای مسئول پیشگیری از جرم وجود دارد. آنان ازیک‌سو، مکلف‌اند در چارچوب اسناد و مقررات بین‌المللی و منطقه‌ای حامی حریم خصوصی حرکت کنند و ازسوی دیگر، موظف به تأمین فضایی عاری از فرصت‌های مجرمانه و پیشگیری از بزهکاری هستند. هرگونه پیشگیری از بزه‌دیدگی برخط، مستلزم تناسب تدابیر اتخاذی با بزه احتمالی و احراز ضرورت کاربست آنها ازسوی مقام صالح قضایی خواهد بود. ازاین‌رو، نمی‌توان در راستای تأمین فضایی امن قیود فوق را نادیده گرفت و با نظارت فراگیر از آماج احتمالی بزه صیانت کرد. استفاده از تدابیر هوش مصنوعی، دوربین‌های مداربسته و سایر روش‌های نظارتی تا جایی مورد پذیرش است که کرامت انسانی آماج بزه مخدوش نگردد و دسترسی غیرقانونی به اطلاعات شخصی آنها برای پیشگیری از خطر احتمالی، مجاز دانسته نشود. در مقاله پیش‌رو، همسویی و یا عدم همسویی رایج‌ترین تدابیر رسمی نظارتی با چارچوب‌های حقوق بشری صیانت از حریم خصوصی ارزیابی و همچنین جنبه‌های گوناگون تداخل آنها را با حریم خصوصی بررسی خواهیم کرد و سپس راه‌حل مناسب با هر یک را ارائه خواهیم داد.

کلیدواژه‌ها: نظارت؛ جرائم سایبری؛ پیشگیری موقعیت‌مدار؛ حریم خصوصی؛ امنیت داده؛ حقوق بشر

---

* کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشکده علوم اداری و اقتصادی، دانشگاه فردوسی مشهد؛
Email: z.farhadialashti@gmail.com

** دانشیار دانشکده علوم اداری و اقتصادی، دانشگاه فردوسی مشهد (نویسنده مسئول)؛
Email: javan-j@um.ac.ir

مقدمه

با ورود فضای سایبر به زندگی بشر، دریچه‌ای از دنیای نوین گشوده شد و فرصت‌های بیشماری را برای زندگی آسان‌تر فراهم کرده است. به‌موازات نفوذ بی‌حد و حصر این فضا به بسیاری از جنبه‌های زندگی روزمره، تأمین امنیت آن نیز حائز اهمیت بوده و توجه خاصی را می‌طلبد. چراکه، به همان میزانی که این فضا ارمغان‌آور رفاه بیشتری است، فرصت‌های مجرمانه بسیاری را نیز برای بزهکاران بالقوه فراهم کرده و از دشواری‌های مرسوم ارتکاب بزه در فضای مادی نیز کاسته است. ازاین‌رو، در سال‌های گذشته، دغدغه‌های بسیاری برای تأمین امنیت این فضا و پیشگیری از بزه‌دیدگی ایجاد شده است، تاجایی‌که امروزه با صنعت امنیت سایبری[1] مواجه هستیم.

صیانت از آماج احتمالی بزه همواره حائز اهمیت بوده و بشر درصدد کاهش موقعیت‌های احتمالی ارتکاب بزه بوده است. ازاین‌رو، از دیرباز تدابیر پیشگیرانه موقعیت‌مدار، با مداخله در فرصت‌های پیش‌جنایی سعی در کاهش یا حذف موقعیت‌های ارتکاب بزه داشته‌اند. این نوع پیشگیری که در زمره تدابیر پیشگیرانه کنشی قرار دارد، درصدد ایجاد تغییرات بنیادین در جامعه مورد نظر نیست، بلکه برعکس، درصدد کاهش فرصت‌های جنایی از طریق روش‌های خاصی است.[2]

کلارک بر این عقیده است که «پیشگیری وضعی درصدد کاهش تمایلات ارتکاب بزه از طریق تعالی جامعه و نهادهای آن نمی‌باشد، بلکه تمرکز آن بر کاهش فرصت‌ها و موقعیت‌های ارتکاب بزه از طریق کاهش جذابیت آنهاست» (Clarke, 1997: 2). تقسیم‌بندی‌های متعددی از روش‌های پیشگیرانه موقعیت‌مدار ارائه شده[3] که در یک دسته‌بندی کلی می‌توان آنها را در دو گروه گنجانید. گروه نخست، تدابیری که به دنبال سلب و یا دشوار کردن ارتکاب رفتار مجرمانه‌اند و گروه دوم، درصدد کاستن از جاذبه‌ها و محرک‌های موقعیت‌های جنایی هستند (میرخلیلی، ۱۳۸۸: ۳۶).

---

1. Cyber Security Industry

۲. کوهن از این حالت با اصطلاح وضعیت‌های پیش‌جنایی نام می‌برد.

۳. به‌عنوان نمونه کلارک و هومل در سال ۱۹۹۲ تکنیک‌های ۱۲ گانه‌ای و در سال ۱۹۹۷ آن را به ۱۶ تکنیک افزایش دادند و در سال ۲۰۰۳ کورنیش و کلارک آن را به ۲۵ تکنیک ارتقا دادند.

یکی از روش‌های پیشگیری موقعیت‌مدار که به افزایش خطر ارتکاب بزه[1] منجر می‌شود، کاربست تدابیر نظارتی است. از دیرباز، نظارت[2] جایگاه ویژه‌ای در سیاست‌های پیشگیری از بزهکاری داشته و با توجه به نقش بازدارنده آن از ارتکاب بزه، همچنان در اشکال مختلف مورد استفاده قرار می‌گیرد.[3] زمانی افزایش نور محیط، تعبیه نیروهای پلیس در اماکن پرخطر و مواردی از این دست در زمره روش‌های رایج نظارتی برای کاهش بزهکاری به‌شمار می‌آمدند. امروزه، تغییر شکل برخی جرائم و ظهور جرائم نوین، سبب شده است کاربست این روش‌ها به تنهایی کفایت نکند و حتی در برخی موارد قابل اعمال بر برخی از آماج و موقعیت‌های احتمالی نیز نباشد. با ورود ابزارهای فناوری‌های ارتباطات و اطلاعات (فاوا)،[4] این مشکل به‌طور چشمگیری کاهش یافته است و برنامه‌های پیشگیرانه با موفقیت بیشتری همراه شده‌اند.

دسته‌بندی‌های مختلفی از تدابیر نظارتی ارائه می‌شود. به‌عنوان نمونه، کلارک و هومل (۱۹۹۷)، نظارت را به سه دسته نظارت رسمی،[5] غیررسمی[6] و نظارت از طریق کارکنان[7] تقسیم کرده‌اند. کرنیش و کلارک در سال ۲۰۰۳، دسته‌بندی تقریباً مشابهی را ارائه داده‌اند که براساس آن، نظارت به سه دسته نظارت رسمی، طبیعی[8] و مدیریت مکانی[9] تقسیم می‌شود. از طرف دیگر، تدابیر نظارتی را می‌توان با توجه به ماهیت ابزار آنها به نظارت مادی[10] و الکترونیکی[11] تقسیم کرد که هر دو گونه قابلیت اعمال در فضای مادی و سایبری را خواهند داشت. آنچه در این نوشتار شالوده اصلی بحث ما را تشکیل می‌دهد، کاربست تدابیر نظارت الکترونیکی رسمی است که ازسوی مقامات مسئول پیشگیری از

---

1. Increasing the Risk of Crime
2. Surveillance

۳. در ابتدای این مبحث لازم به ذکر است زمانی که از نظارت به‌صورت کلی سخن به میان می‌آید، منظور در مرحله ماقبل بزهکاری و به عنوان یکی از تکنیک‌های پیشگیری موقعیت‌مدار است و در مراتب بعدی، تهیه ادله ارتکاب بزه و شواهد و مدارک مورد نظر است.

4. Information and Communications Technology (ICT)
5. Formal Surveillance
6. Informal Surveillance
7. Surveillance by Employee
8. Natural Surveillance
9. Place Manager
10. Physical Surveillance
11. Electronic Surveillance

جرم، در راستای پیشگیری موقعیت‌مدار از جرائم سایبری صورت می‌گیرند.[۱]

امروزه، نظارت به یکی از مفاهیم میان‌رشته‌ای چالش‌برانگیز تبدیل شده است. چراکه تدابیر نظارتی ازیک‌سو، با استفاده از قدرت حکومت، می‌توانند ارمغان‌آور امنیت باشند و ازسوی‌دیگر، قابلیت نقض حریم خصوصی و تجاوز به آن را دارند. «به جهت طبیعت باز شبکه راه برای نیروهای پلیس آنچنان هموار است که بدون داشتن حکم بازرسی می‌توانند افراد را تحت کنترل قرار دهند» (احمدی، ۱۳۸۷: ۱۰۱). ازاین‌رو، به‌موازات کاربست تدابیر پیشگیرانه نظارتی، دغدغه‌های فراوانی درباره صیانت از حریم خصوصی به‌وجود آمده است، چراکه؛ این ابزارها به‌مثابه تیغ دولبه‌ای عمل می‌کنند که در صورت استفاده غیراصولی از آنها «به قیمت نقصان یافتن حریم خصوصی، اقدام به مقابله با رفتارهای خطرناک یا ضداجتماعی» خواهند کرد (محسنی، ۱۳۹۴: ۲۱۵).

با مراجعه به اسناد بین‌المللی و منطقه‌ای حقوق بشری که در صدر آنها کنوانسیون بین‌المللی حقوق مدنی و سیاسی قرار دارد، می‌توان دریافت که اصل بر رعایت و صیانت از حق حریم خصوصی است و صرفاً در صورت وجود حکم قانونی و با رعایت ضرورت و تناسب اقدامات مربوطه با خطر احتمالی و نظارت مقام قضایی صالح، می‌توان حریم خصوصی را نقض کرد.[۲] از طرف دیگر، ماهیت برخی تدابیر نظارت الکترونیکی سایبری به‌گونه‌ای است که در صورت استفاده وسیع آنها امکان تجاوز به حریم خصوصی

---

۱. علت انتخاب تدابیر نظارتی رسمی سایبری این است که به‌علت دامنه شمول وسیع کاربست این تدابیر، در مقام عمل عمل منجر به پیشگیری از قسم عمده‌ای از جرائم سایبری می‌شوند و ازسوی‌دیگر، به علت ماهیت این فضا ابزارهای نظارت الکترونیکی کارایی دارند.

۲. ماده (۱۷) میثاق بین‌المللی حقوق مدنی و سیاسی: «۱. هیچ‌کس نباید در زندگی خصوصی و خانوادگی و اقامتگاه یا مکاتبات خود، مورد مداخلات خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد و همچنین شرافت و حیثیت او نباید مورد تعرض غیرقانونی واقع شود. ۲. هرکس حق دارد در مقابل این‌گونه مداخلات یا تعرضات از حمایت قانون برخوردار شود».

ـ ماده (۸) کنوانسیون اروپایی حقوق بشر: «۱. هرکس حق دارد که حرمت زندگی خصوصی، خانوادگی، منزل و مکاتباتش محفوظ بماند. ۲. هیچ مداخله‌ای از طرف مرجع عمومی نسبت به اعمال این حق نباید صورت گیرد، مگر اینکه براساس قانون بوده و در جامعه‌ای دمکراتیک در راستای تأمین امنیت ملی، سلامت عمومی یا رفاه اقتصادی کشور برای جلوگیری از بی‌قانونی یا جرم، حمایت از بهداشت یا اخلاقیات، یا برای حمایت از حقوق و آزادی‌های دیگران لازم باشد».

ارتباطاتی[1] و اطلاعاتی[2] وجود خواهد داشت و رکن محرمانگی[3] نقض خواهد شد.

ازاین‌رو، کشورهای پیشرو، صیانت از داده‌های شخصی را در دستور کار خود قرار داده و ضمانت اجراهای حقوقی و کیفری متعددی را وضع کرده‌اند. سرآمد و پیشتاز قوانین حمایت از داده را می‌توان در اتحادیه اروپا مشاهده کرد. نخستین دستورالعمل شورای اروپا درباره حمایت از داده در سال ۱۹۹۵، با عنوان «حمایت از اشخاص در جریان پردازش داده‌های شخصی و جریان آزاد اطلاعات»[4] به تصویب رسید. پیرو گسترش ابزارهای ارتباطی و پردازش داده‌های شخصی برای اهداف گوناگون، نیاز به روزآمد کردن این دستورالعمل احساس شد. ازاین‌رو، دستورالعمل «پردازش داده‌های شخصی و حمایت از حریم خصوصی ارتباطات الکترونیکی»[5] در سال ۲۰۰۲ به تصویب رسید و دستورالعمل اخیر را ملغی کرد. علاوه‌بر اسناد الزام‌آور یاد شده، دسته‌ای دیگر از اسناد ارشادی وجود دارند که همانند اسناد پیشین سعی در صیانت از حریم خصوصی و قانونمند کردن مداخلات را در آن دارند که مهم‌ترین آنها «رهنمودهای سازمان همکاری‌های اقتصادی و توسعه به‌منظور صیانت از حریم خصوصی و جریان فرامرزی داده‌های شخصی» (OECD, 1980) است که اصول هشت‌گانه‌ای را به‌منظور حمایت از داده‌ها به رسمیت شناخته و از کشورهای عضو درخواست کرده است تا این اصول را در قوانین داخلی خود وارد کنند.

با بررسی قوانین حمایت از داده، می‌توان دریافت که آن‌دسته از تدابیر نظارت الکترونیکی که به اطلاعات شخصی[6] افراد تجاوز می‌کنند، منجر به نقض حریم خصوصی برخط خواهند شد. برای تشخیص معیار اطلاعات شخصی باید به قوانین کشور مورد مطالعه مراجعه کرد، چراکه در سیستم حقوقی هر کشوری مصادیق و مبانی تشخیص این اطلاعات متفاوت است. در کشور ما قانونی مختص به حمایت از حریم خصوصی و بالاخص داده‌های

---

1. Informational Privacy
2. Communicational Privacy
3. Confidentiality
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
5. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).
6. Personal Information

شخصی وجود ندارد و در قوانین گوناگون بنا به موضوع مورد حمایت به این حیطه اشاره شده است که مهم‌ترین آنها فصل سوم قانون تجارت الکترونیکی و قانون انتشار و دسترسی آزاد به اطلاعات است. در حال حاضر، تنها مستند قانونی برای تمییز اطلاعات شخصی از غیرشخصی در نظام حقوقی کشورمان، ماده (۱) قانون انتشار و دسترسی آزاد به اطلاعات است که اطلاعات را به دو دسته شخصی و عمومی تقسیم کرده است. براساس این ماده، «اطلاعات فردی، نظیر نام و نام‌خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است». بنابراین، زمانی که سخن از نقض محرمانگی اطلاعات و به‌عبارت‌دیگر، تجاوز به حریم خصوصی سخن به میان می‌آید، منظور دسترسی غیرقانونی به اطلاعات شخصی است.

در این نوشتار بر آن هستیم که به بررسی تطابق یا عدم تطابق رایج‌ترین و مؤثرترین روش‌های نظارتی حاکمیتی، با حریم خصوصی کاربران بپردازیم و به این سؤال پاسخ دهیم که آیا به همان میزانی که این ابزار قادر به تأمین امنیت حداکثری شبکه هستند، قادرند امنیت صاحبان داده‌ها را نیز حفظ کنند و بدون تخطی به آنها، فضایی با کمترین فرصت ارتکاب جرم فراهم آورند؟ چراکه حریم خصوصی در فضای مادی و در فضای غیرمادی محترم است و تغییر فضا، تغییری در حقوق صاحبان داده و تکالیف نهادهای مسئول پیشگیری از جرم ایجاد نمی‌کند. بنابراین، همان‌گونه که در قطعنامه مجمع عمومی سازمان ملل متحد اشاره شده است «حقوقی که مردم در فضای غیر برخط دارند، در فضای برخط نیز وجود دارد و محترم می‌باشد» (Resolution Adopted by the General Assembly, 2014: 2).

۱. داده‌کاوی[1] حداکثری و نقض محرمانگی داده‌های کاربران

با پیشرفت فناوری‌های هوش مصنوعی،[2] امروزه داده‌کاوی به‌عنوان یکی از قدرتمندترین و مؤثرترین ابزارهای مورد نیاز مجریان قانون برای شناخت فرصت‌های بزهکارانه احتمالی تبدیل شده است، به‌گونه‌ای که بعد از حملات تروریستی ۱۱ سپتامبر، به‌عنوان یکی از روش‌های شاخص پیشگیری از تروریسم سایبری استفاده می‌شوند. روش‌های داده‌کاوی

1. Data Mining
2. Artificial Intelligence

زمانی مورد استفاده قرار می‌گیرند که شمار فراوانی از داده‌های خام[1] وجود دارند و کشف هدف مورد نظر از میان این گستره عظیم، غیرممکن و یا دشوار باشد. ازاین‌رو، این روش‌ها را «شیوه‌ای مؤثر برای استخراج اطلاعات و داده‌های مهم از میان انبوه داده‌ها» تعریف کرده‌اند (Taniar, 2008: 119).

پیشینه استفاده از روش‌های داده‌کاوی، به علم مدیریت بازمی‌گردد و «برای پیش‌بینی عادات رفتاری مشتریان استفاده می‌شده است» (Mena, 2003: 293). امروزه نیز از این روش برای افزایش بهره‌وری و شناخت سلایق مشتریان استفاده می‌شود،[2] اما صرفاً منحصر به این حیطه نبوده و در بسیاری از حوزه‌های دیگر به‌ویژه در حیطه تحلیل پدیده‌های مجرمانه کاربرد دارد که علت آن را می‌توان در «ماهیت پیچیده داده‌های مرتبط با جرم و بزهکاری و روابط نامحسوس میان این داده‌ها» دانست (اسکندری، علیزاده و کاظمی، ۱۳۹۰: ۴۰).[3]

---

1. Raw Data

۲. به‌عنوان نمونه، اگر بخواهیم از اولین کاربست این روش‌ها که امروزه نیز رایج است، مثال بزنیم، می‌توان به خرید برخط کتاب اشاره کرد. عموماً مشاهده می‌شود که هنگام خرید کتاب، عناوینی در راستای موارد جست‌وجو شده کاربر به وی پیشنهاد می‌شود. در حقیقت وب‌سایت‌های مذکور از نرم‌افزارهای داده‌کاوی پیش‌بینی‌کننده استفاده می‌کنند. به این صورت که، موارد جست‌وجو شده کاربر را به‌عنوان الگوی کتب مورد علاقه وی در نظر می‌گیرند و سپس پیش‌بینی می‌کنند که کتبی در این حیطه و یا حیطه‌های مشابه آن را مطالعه می‌نماید.

۳. برای درک تأثیر چشمگیر روش‌های داده‌کاوی در فرایند پیشگیری از جرم و احتمال نقض امنیت داده‌های کاربران در این فرایند، نیازمند آشنایی نسبی با مراحل آن هستیم. ازاین‌رو، به‌طور اجمالی به ذکر مراحل مختلف و درعین‌حال مرتبط آن می‌پردازیم. مرحله نخست فرایند داده‌کاوی، تشکیل پایگاه داده‌هاست. هرچه داده‌های خام موجود در پایگاه داده‌ها بیشتر باشد، احتمال حصول نتیجه‌ای معتبرتر و نزدیک‌تر به واقعیت بیشتر خواهد بود. پس از این مرحله، داده‌های هدف یا همان داده‌های مورد نظر از میان حجم انبوه داده‌ها جدا می‌شوند. به‌عبارت‌دیگر، در این مرحله داده‌های مورد نیاز و کارآمد از داده‌های ناکارآمد تفکیک و منبعی تقریباً یک‌دست ایجاد می‌شود. در مرحله سوم، نرم‌افزار، داده‌های هدف را مورد تجزیه و تحلیل قرار می‌دهد. در گام چهارم، داده‌ها تبدیل شده و هریک از آنها در دسته‌بندی‌های خاص خود، که برای حصول نتیجه‌ای مناسب از داده‌کاوی نیاز است، قرار خواهند گرفت. مرحله پنجم، یکی از مراحل مهم داده‌کاوی است؛ زیرا در این مرحله، با توجه به هدفی که برای داده‌کاوی در نظر گرفته شده و الگوریتم‌هایی که برای آن تعیین شده است، الگوهای مورد نظر از میان داده‌ها، استخراج خواهند شد. در مرحله ششم، داده‌ها مطابق با الگوهای تعریف شده پردازش خواهند شد و الگوهای ناکارآمد حذف می‌شوند. در مرحله هفتم، الگوی نهایی مورد نظر از میان داده‌های ارائه شده استخراج خواهد شد و به صورت نمودار، تصویر، جدول، ساختاره و ... پردازش می‌شوند و در آخرین مرحله، هدف و یا همان دانش مورد نظر ارائه خواهد شد.

روش‌های مختلف داده‌کاوی درصدد توصیف[1] داده‌ها و یا پیش‌بینی[2] پدیده‌های پیش‌رو هستند. برای دستیابی به هدف نخست، «با استفاده از داده‌های موجود، توصیفی از آنها ارائه می‌شود» (Fogelman-Soulie, Perrotta and Piskorski, 2008: 288). به‌عنوان نمونه، در برخی موارد به‌منظور درک موقعیت‌های جنایی و تدوین برنامه‌های راهبردی جامع برای مبارزه با آنها، نیاز به شناخت جامع وضعیت بزهکاری و سپس برنامه‌ریزی متناسب با هدف است. در این حالت، روش‌های داده‌کاوی توصیفی بهترین ابزار هوش مصنوعی تجزیه و تحلیل موقعیت جنایی به‌شمار می‌آیند.[3]

یکی دیگر از موارد پرکاربرد استفاده از روش‌های داده‌کاوی در برنامه‌های پیشگیری از جرم، داده‌کاوی پیش‌بینی‌کننده است. قبل از ورود به این قسمت که موضوع مورد بحث این گفتار را نیز تشکیل می‌دهد، گفتنی است تا قبل از ابداع روش‌های داده‌کاوی، برای پیشگیری بسیاری از جرائم احتمالی از روش‌های سنتی تحلیل داده‌ها که توسط انسان صورت می‌گرفت، استفاده می‌شده است که معایبی همچون زمان‌بر بودن و کارایی اندک داشت. اما به علت حجم بالای داده‌های موجود در فضای سایبر، امکان استفاده از این روش‌ها برای پیشگیری از جرائم احتمالی وجود نخواهد داشت و روش‌های داده‌کاوی که سعی در پیش‌بینی موقعیات پیش‌جنایی می‌کنند، کاربرد فراوانی برای نهادهای متصدی پیشگیری از جرم دارد.[4] به‌علت شمار فراوان داده‌های در حال جریان در فضای سایبر، کشف بسیاری از موقعیت‌های تهدیدآمیز بدون استفاده از روش‌های داده‌کاوی پیش‌بینی‌کننده، تقریباً غیرممکن خواهد بود. نهادهای پیشگیری‌کننده از وقوع جرم، در صورتی می‌توانند طیف گسترده‌ای از فرصت‌های مجرمانه را شناسایی و قبل از گذار از

---

1. Descriptive
2. Predictive

۳. به‌عنوان نمونه نیروهای پلیس منطقه‌ای درصدد بررسی جرائم حوزه استحفاظی خود هستند و می‌خواهند دریابند که چه جرائمی بیشتر در حوزه مأموریت آنها رخ می‌دهند و همچنین کدام دسته از جرائم خسارات بیشتری وارد می‌کنند و سپس به‌ترتیب اولویت و اهمیت جرائم، نیروهای خود را برای پیشگیری و کنترل و مبارزه با آنها اختصاص دهند.

۴. امروزه، عموماً در ادبیات جرم‌شناسی سایبری، از این‌گونه داده‌کاوی با عنوان «داده‌کاوی مبتنی‌بر الگو» (Data Mining Pattern Based) یاد می‌شود، همان‌گونه که در شرح مراحل داده‌کاوی بیان کرده‌ایم، در صورت تعیین الگوی تخمین ارتکاب بزه مورد نظر، نرم‌افزار قادر به پیش‌بینی موقعیت‌های احتمالی بزهکاری خواهد بود.

مرحله اندیشه به عمل آنها را خنثی کنند که از نرم‌افزارهای قوی داده‌کاوی با الگوهای پیش‌بینی‌کننده بهره ببرند. ازاین‌رو، امروزه غالب نیروهای پلیس از این روش به‌منظور شناخت موقعیات احتمالی ارتکاب جرم استفاده می‌کنند. آنان داده‌های خام بسیاری درباره مشخصات بزهکاران سابقه‌دار و جرائم آنها، اماکن جرم‌خیز، شیوه‌های ارتکاب بزه و اطلاعاتی از این دست را در اختیار دارند و روزانه به این اطلاعات نیز افزوده می‌شود. حال، چنانچه به‌عنوان نمونه؛ پرونده‌ای مربوط به قتل زنجیره‌ای در حوزه استحفاظی آنها مطرح شود و بخواهند از بزه‌دیدگی‌های احتمالی آتی پیشگیری کنند، با توجه به سابقه محکومان و متهمان به قتل، شیوه ارتکاب جرم و شواهد و مدارک موجود و ارائه آن به نرم‌افزار مورد نظر، احتمال شناسایی قاتل و یا قاتلان احتمالی وجود خواهد داشت. درحالی‌که، در صورت فقدان چنین ابزارهایی، می‌بایست تمام پرونده‌های قتل‌های زنجیره‌ای را در بازه زمانی طولانی مطالعه کنند و حتی در صورت موفقیت آنها در پیش‌بینی بزهکار، زمان از دست خواهد رفت و چه‌بسا افراد بسیاری نیز به قتل برسند. بنابراین، «سرعت و بررسی جامع هزاران نمونه و اطلاعات بی‌شمار دیگری که هر روزه به اطلاعات سابق اضافه می‌شوند، برای مبارزه با جرم ضروری است. با توجه به حجم انبوه اطلاعات موجود نزد نیروهای پلیس، آنها نیازمند شیوه‌های گوناگونی برای تجزیه و تحلیل داده‌ها هستند. ازاین‌رو؛ نرم‌افزارهای داده‌کاوی پیش‌بینی‌کننده، ابزارهایی قوی و درعین‌حال بسیار مفید و ضروری برای نیروهای پلیس هستند» (Bennett and Hess, 2007: 21).

اما، سؤال مهمی که در این خصوص وجود دارد این است که آیا کاربست همه روش‌های نظارتی داده‌کاوی، به نقض امنیت داده‌های کاربران منجر خواهد شد و رهگیری غیرقانونی ارتباطات محسوب می‌شود؟ پاسخ این سؤال منفی است. صرف استفاده از روش‌های داده‌کاوی، منجر به نقض حریم خصوصی کاربران و جرم رهگیری غیرقانونی ارتباطات نخواهد بود؛ زیرا درصورتی‌که جمع‌آوری و استفاده از داده‌ها، مطابق موازین مندرج در اسناد حقوق بشری باشد، مغایرتی وجود نخواهد داشت. ازاین‌رو، به علت انعکاس این موازین در اصول حمایت از داده، تطابق و یا عدم تطابق مراحل داده‌کاوی را با این اصول بررسی خواهیم کرد.

الف) گردآوری قانونی و منصفانه داده‌ها:[1] اصل گردآوری قانونی و منصفانه داده‌ها که یکی از اصول محدودیت گردآوری داده‌هاست، به این نکته مهم اشاره دارد که «باید محدودیت‌های قانونی برای جمع‌آوری داده‌ها وجود داشته باشد و داده‌ها با استفاده از ابزار قانونی و به‌طور منصفانه جمع‌آوری شوند» (OECD, 1980: 7). براساس این اصل هر شیوه یا ابزاری که براساس قانون برای جمع‌آوری داده‌ها[2] ممنوع باشد، نباید مورد استفاده قرار گیرد. همچنین، رضایت صاحب داده‌ها نیز از لوازم این اصل است، مگر اینکه؛ در موارد استثنایی و به دلایل امنیتی و مصالح عمومی به صاحب داده‌ها اطلاع داده نشود و رضایت وی اخذ نشود، که حتی در این صورت نیز باید تضمینات قانونی برای حفظ حقوق وی رعایت شده و صرفاً در محدوده مجوز قانونی اقدام شود.

اولین چالشی که همواره فراروی نهادهای مسئول پیشگیری از جرائم سایبری وجود دارد این است که برای نظارت بر رفتار کاربران از کدام دسته از داده‌های موجود در شبکه استفاده کنند؟ به‌عبارت‌دیگر، جمع‌آوری داده‌ها[3] و تشکیل پایگاه‌های داده با استفاده از کدام داده‌ها و اطلاعات انجام گیرد؟ چراکه جمع‌آوری داده‌ها در هر حالتی غیرقانونی نیست، بلکه؛ چنانچه داده‌های موجود بدون رعایت شرایط و تضمینات قانونی جمع‌آوری شوند یا در غیر موارد تعیین شده مورد استفاده قرار گیرند، اقدام غیرقانونی بوده و حریم خصوصی اطلاعاتی صاحبان داده نقض می‌شود. آنچه در تشکیل پایگاه‌های داده حائز اهمیت است و می‌تواند منجر به نقض حریم خصوصی کاربران شود، این است که پایگاه‌ها با توجه به موقعیت‌ها یا آماج احتمالی بزه، تشکیل می‌شوند. بنابراین، نهادهای مسئول برای پیشگیری از بزه احتمالی مورد نظر و یا شناسایی موقعیت‌های ارتکاب بزه، باید آماج را تحت نظارت قرار دهند و این امر در گام اول نیازمند درج داده‌های آنان در پایگاه‌های داده است. حال، چنانچه هدف از داده‌کاوی نظارت فراگیر[4] بر رفتارهای کاربران باشد، در این حالت، نیاز به تشکیل پایگاه‌هایی جامع از اطلاعات آنان است. چراکه در این حالت، به‌منظور تأمین امنیت حداکثری «تنها بر اطلاعات شخص معینی نظارت نمی‌شود، بلکه

1. Fair and Lawful Collection
2. Data Gathering
3. Data Aggregation
4. Mass Surveillance

اطلاعات افراد بسیاری برای آینده احتمالی مورد نظارت قرار خواهد گرفت» (Stalla-Bourdillon, Joshua and Mark, 2014: 14).

در این‌گونه از داده‌کاوی احتمال بسیار بیشتری برای نقض حریم خصوصی کاربران وجود دارد، چراکه به‌ازای پیشگیری از بزهکاری هریک از مجرمان احتمالی، نیاز به حکم مقام قضایی است، و طی نمودن این روند فرصت کافی را برای مجرمان فراهم می‌آورد. ازسوی‌دیگر، امروزه دستیابی به داده‌های شهروندان برای نهادهای مسئول پیشگیری از جرم، به دشواری گذشته نیست. چراکه، افراد اطلاعات و داده‌های بسیاری را نزد نهادها و صاحبان مشاغل و خدمات گوناگون دارند و «تقریباً همه افراد به نوعی پرونده‌دار شده‌اند، بدون آنکه از محتویات پرونده خود با خبر باشند» (نوری و نخجوانی، ۱۳۸۳: ۲۹). بنابراین، با وجود پرونده‌های الکترونیکی حاوی مشخصات افراد در سازمان‌ها و نهادها، دستیابی به این اطلاعات آسان شده است و «روش‌های جدید داده‌کاوی این امکان را به دولت‌ها می‌دهند که داده‌ها و اطلاعات مربوط به افراد را بدون توجه به اینکه در کجا قرار دارند، مورد پردازش قرار دهند» (TAPAC, 2004: 36) و پایگاه‌های داده خود را به‌آسانی تجهیز کنند.

نمونه واضح گردآوری غیرقانونی داده‌های کاربران را می‌توان در نیروهای امنیتی ایالات متحده آمریکا، در ماه اوت سال ۲۰۱۳ مشاهده کرد. پیرو جست‌وجو واژگان «کوله‌پشتی»،[1] «زودپز»[2] و «حادثه بمب‌گذاری آوریل سال ۲۰۱۳ بوستون»[3] توسط پدر، مادر و فرزند پسر خانواده در موتور جست‌وجوگر شرکت گوگل، نیروهای ضد تروریستی مظنون به طراحی عملیات تروریستی مانند حادثه بمب‌گذاری سال ۲۰۱۳ بوستون شدند. آنها، صبح روز بعد منزل این خانواده را محاصره کردند و پس از دستگیری اعضای خانواده سؤالاتی درباره قصد آنها برای تهیه بمب ساعتی خانگی پرسیدند. نیروهای ضد تروریستی بر این عقیده بودند که عبارت جست‌وجو شده موجب ظن آنها به تهیه بمب خانگی و تعبیه آن در زودپز و ایجاد حادثه‌ای همانند بمب‌گذاری بوستون شده است.

با دقت در این مثال، می‌توان به‌وجود نرم‌افزارهای داده‌کاوی پیش‌بینی‌کننده پیشرفته

1. Back Pack
2. Pressure Cooker
3. April 2013 Boston Bombing

پی برد. نرم‌افزارهایی که پایگاه‌های داده آنها، به صورت ۲۴ ساعته حداقل از میزبان‌های شرکت گوگل تأمین می‌شوند[۱] و در خوشبینانه‌ترین حالت، داده‌های گردآوری شده، متعلق به کاربران آمریکایی هستند. حال، سؤال اساسی که مطرح می‌شود این است که کدام سند بین‌المللی یا منطقه‌ای حقوق بشری اجازه چنین نقض فراگیر حریم خصوصی کاربران را حتی به قیمت پیشگیری از بزه احتمالی می‌دهد؟[۲]

سؤالاتی از این قبیل، اذهان بسیاری از نهادها و اشخاص حامی حریم خصوصی را درگیر کرده و منجر به طرح شکایات بسیاری در دادگاه‌های داخلی و بین‌المللی شده است. یکی از مهم‌ترین موارد، شکایتی با نام «دیده‌بان برادر بزرگ و دیگران علیه دولت انگلستان»[۳] است که در تاریخ سوم اکتبر ۲۰۱۳، در دادگاه اروپایی حقوق بشر اقامه شد.[۴] شاکیان این پرونده براساس ماده (۳۴) کنوانسیون اروپایی حقوق بشر ادعا کردند که اقدامات دولت انگلیس در راستای نظارت بر اطلاعات کاربران و جمع‌آوری آنها، مطابق با مقررات کنوانسیون اروپایی حقوق بشر نبوده و حق حریم خصوصی مندرج در ماده (۸) این کنوانسیون را نقض کرده است. مستند دولت انگلیس برای قانونی بودن اعمال خود، ماده (۸) قانون قدرت تحقیقات[۵] مصوب سال ۲۰۰۰ است. این ماده، دو نوع اخطار متفاوت برای نظارت بر ارتباطات داخلی و بین‌المللی را به رسمیت شناخته است. براساس ماده (۲۰) این قانون، ارتباط خارجی[۶] «آن دسته از ارتباطاتی هستند که به خارج از جزیره انگلستان فرستاده شده یا از خارج جزیره به داخل ارسال می‌شوند». ازطرف‌دیگر، برای مداخله در ارتباطات داخلی، فرد یا محل معین باید شناسایی شود و نمی‌توان همه افراد کشور را تحت نظارت قرار داد. درحالی‌که برای نظارت بر ارتباطات خارجی نیاز به شناسایی نخواهد بود و طبق قانون «نظارت فراگیر» می‌تواند اعمال شود.

---

۱. چرا که احتمال دارد علاوه‌بر اطلاعات موارد کاربران موتور جست‌وجوگر شرکت گوگل از اطلاعات کاربران شرکت‌های اینترنتی دیگر نیز استفاده کنند.

۲. برای مطالعه بیشتر در مورد تأثیر قانون میهن‌پرستی بر حریم خصوصی کاربران آمریکایی رک.: آقابابایی، ۱۳۸۹: ۱۷-۱.

3. Big Brothers Watch and Others against the United Kingdom

۴. گفتنی است این پرونده پس از افشاگری‌های ادوارد اسنودن از ابزارهای داده‌کاوی حاکمیت‌ها برای شنود اطلاعات کاربران، اقامه شده است.

5. Regulation of Investigatory Powers Act (RIPA)

6. External Communications

اما، نکته بسیار مهم اینجاست که اقدامات کاربران انگلیسی که از خدمات میزبان‌های خارج از خاک انگلیس استفاده می‌کنند، شامل ارتباطات خارجی می‌شود و دولت انگلیس با استفاده از این ماده تمام فعالیت‌های سایبری آنها را تحت نظارت قرار می‌دهد. دولت انگلستان با استناد به این ماده از برنامه‌های پریسم[۱] آمریکا و همچنین تمپورا[۲] استفاده می‌کند و اطلاعات کاربران را براساس بند «۴» قسمت ۸ این قانون جمع‌آوری می‌نماید. دادگاه اروپایی این سؤال را از نماینده دولت انگلیس پرسید که آیا نظارتی چنین فراگیر برای پیشگیری از بزهکاری احتمالی و تأمین امنیت کاربران انگلیسی ضرورت دارد؟ همچنین، براساس نظر دادگاه حتی در صورت احراز شرط ضرورت، تدابیر نظارتی نباید مداخله‌آمیز باشند و حریم خصوصی کاربران را تحت‌الشعاع قرار دهند. همان‌گونه که مشاهده می‌کنید دادگاه به شروط مندرج در ماده (۸) کنوانسیون اروپایی حقوق بشر استناد کرده است و هرگونه کاربست تدابیر پیشگیرانه احتمالی را منوط به تجمیع شرایط این ماده می‌داند.

ب) گردآوری مضیق و مرتبط:[۳] مشکل عمده‌ای که در فرایند جمع‌آوری داده‌های برخط برای پایگاه‌های داده وجود دارد این است که در اغلب موارد، علاوه‌بر داده‌های هدف، داده‌های غیر مرتبط نیز جمع‌آوری می‌شوند. در این حالت اصل گردآوری مضیق و مرتبط نقض می‌شود. به موجب این اصل، «گردآوری داده‌ها باید تنها به میزان مورد نیاز برای هدف اولیه و اعلام شده صورت گیرد و گردآوری داده‌های اضافی ممنوع است» (اصلانی، ۱۳۸۹: ۱۳۴).

پایبندی به این اصل، در مورد داده‌ها و اطلاعاتی که مرتبط با دنیای صفر و یک نیستند، امکان‌پذیر است. اما، در مورد داده‌های موجود فضای سایبر بسیار دشوار است. چراکه، تا

---

۱. نام اصلی این برنامه US-984XN است و به پریسم (PRISM) معروف شده است. پریسم برنامه‌ای نظارتی است که آژانس امنیت ملی آمریکا آن را طراحی کرده است و دادگاه نظارت بر اطلاعات خارجی آمریکا بر نحوه عملکرد آن نظارت می‌کند. این برنامه از اطلاعات میزبان شرکت‌های گوگل، یاهو، یوتیوب، اپل، مایکروسافت، فیسبوک و اسکایپ به‌منظور نظارت بر فعالیت‌های کاربران استفاده می‌کند و ارتباطات الکترونیکی کاربران را مورد بررسی قرار می‌دهد.

۲. تمپورا (TEMPORA) برنامه‌ای است که سازمان اطلاعات انگلستان (GCHQ) هدایت می‌کند این برنامه روی کابل‌های فیبر نوری در اروپا نصب شده است و ترافیک داده‌های کاربران و مکالمات تلفنی آنها را مورد نظارت و بررسی قرار می‌دهد.

3. Collection for a Proper Purpose

زمانی که داده‌ها پردازش و خوانده نشوند امکان آگاهی از ماهیت آنها وجود نخواهد داشت. ازاین‌رو، چنانچه صرفاً مجوز نظارت برای پیشگیری از جرمی خاص وجود داشته باشد، نباید از سایر داده‌های کاربر استفاده کرد و صرفاً آن قسمت از ترافیک داده‌های وی را که احتمال مجرمانه بودن آنهاست، بررسی کرد، امری که دستیابی به آن چندان آسان نیست. همچنین، این مشکل در مورد سابقه داده‌هایی که طبق قانون ذخیره شده‌اند نیز وجود دارد، مگر اینکه مقام ناظر بداند کاربر مورد نظر در آن بازه زمانی صرفاً رفتار مجرمانه احتمالی را انجام می‌داده است. به‌عنوان نمونه، چنانچه براساس قرائن و گزارش‌های واصله مشخص شود که کاربری از گروهی مجرمانه است که قصد نفوذ به سامانه بانکی را دارند و برای خنثی کردن حمله ارتکابی آنان، نیاز به رهگیری فعالیت‌های سابق آنان است، قانوناً باید داده‌های مربوط به همین عمل از ارائه‌دهندگان خدمات دسترسی درخواست شوند، درحالی‌که، تفکیک داده‌های مذکور از سایر داده‌های کاربر در آن بازه زمانی بسیار دشوار خواهد بود.

۲. نظارت ویدئویی در مراکز عمومی ارائه‌دهنده خدمات دسترسی

پیرو استفاده از دوربین‌های مداربسته[1] در اماکن عمومی نظیر خیابان‌ها، پارکینگ‌ها، مراکز خرید و اماکنی از این قبیل و پژوهش‌های بی‌شماری که درباره کارکرد مثبت آنها در کاهش ارتکاب جرائم صورت پذیرفت، استفاده از این دوربین‌ها به‌منظور کاهش جرائم سایبری در اماکن عمومی ارائه‌دهنده خدمات دسترسی نیز رایج شده و در سال‌های اخیر، فزونی یافته است.[2] منظور اماکن عمومی ارائه‌دهنده خدمات دسترسی، آن دسته از اماکنی است که پس از دریافت مجوزهای لازم از مقامات صلاحیتدار، اجازه فراهم کردن دسترسی به اینترنت برای کاربران عمومی را خواهند داشت. کافی‌نت‌ها و هتل‌ها نمونه‌هایی از این اماکن هستند. علت اصلی کاربست این دوربین‌ها، استفاده فراوان بزهکاران از خدمات موجود در این اماکن به‌منظور ناشناس ماندن در حین ارتکاب جرم است، چراکه؛

---

1. Closed Circuit Television (CCTV)

۲. به‌عنوان نمونه، پلیس فتای جمهوری اسلامی ایران در بند «۱۷» بخشنامه پلیس فضای تولید و تبادل اطلاعات به صاحبان کافی‌نت‌ها، آنها را ملزم به نصب دوربین مداربسته کرده است. براساس این بند: «نصب دوربین مداربسته داخلی با قابلیت ضبط تمام‌وقت، نگهداری تصاویر و امکان بازبینی تا شش ماه الزامی است» (www.cyberpolice.ir/page/11631).

به‌علت گمنامی کاربران و عدم ردیابی فعالیت‌های آنان، اماکنی از این دست، فرصت مناسبی را برای ارتکاب جرم فراهم می‌آورند. به‌عنوان نمونه، در بسیاری از موارد انتقال بدافزارها،[1] جاسوسی از گذرواژه‌های موجود در مرورگرها[2] در محیط امن و ناشناس اماکن ارائه‌دهنده خدمات دسترسی اتفاق می‌افتد.

مقامات ناظر از طریق نصب این دوربین‌ها به صورت آشکار یا پنهان، قادر خواهند بود فعالیت‌های مراجعان را زیرنظر بگیرند و از ارتکاب بسیاری از رفتارهای مجرمانه احتمالی پیشگیری کنند. درواقع، آنچه عمدتاً منجر به کاهش بزهکاری می‌شود، آگاهی بزهکاران احتمالی از مکانیزم نظارت است، چراکه استفاده از این دوربین‌ها در مقابل دیدگان کاربران، «منجر به ایجاد هراس و ارعاب در بزهکاران بالقوه می‌شود» (Miller, Hess and Orthman, 2014: 281). به‌عبارت‌دیگر، به‌علت رصد فعالیت‌های بزهکار احتمالی با دوربین، وی به‌طور محاسبه‌گرایانه به این نتیجه می‌رسد که هزینه ارتکاب جرم، بسیار بیشتر از منافع آن است.

با وجود تأثیر مثبت این دوربین‌ها در کاهش بزهکاری، تعبیه آنها در اماکن فوق در برخی موارد می‌تواند منجر به نقض حریم خصوصی اطلاعاتی و ارتباطاتی کاربران می‌شود. علت تشکیک در مورد نقض حریم خصوصی این است که نمی‌توان به‌صورت مطلق حکم به نقض داد و با توجه به اینکه این دوربین‌ها در چه اماکنی و چه زاویه‌ای نصب شده‌اند و چه مواردی را نظارت می‌کنند، نتیجه متفاوت است. چراکه، ممنوعیت مطلقی برای استفاده از دوربین‌های مداربسته وجود ندارد، و فناوری‌های نوین نیز در بسیاری از موارد همان کاری را انجام می‌دهند که نیروهای انسانی با صرف زمان و وقت بیشتری می‌بایست انجام دهند. بنابراین، این فناوری‌ها نیز تابع شرایط و ضوابط الزام‌آور صیانت از حریم خصوصی می‌باشند و همانند سایر حوزه‌های نظارت، «دوربین‌های مراقبت از همان محدودیت‌های پلیس برخوردار است» (ابراهیمی، ۱۳۹۱: ۱۰۸) و اصولاً تناقضی با حریم خصوصی کاربران نخواهند داشت.

برای بررسی امکان نقض حریم خصوصی کاربران با دوربین‌های مداربسته باید توجه کرد که اماکن ارائه‌دهنده خدمات اینترنتی اماکنی کاملاً خصوصی نیستند و همگان اجازه ورود و استفاده از خدمات این اماکن را دارند. اما، با این وجود برای هر کاربری در این

1. Malwares
2. Browsers

مکان نیز، حدی از حریم خصوصی مفروض است. ازاین‌رو، امروزه دیگر نمی‌توان این عقیده را پذیرفت که در اماکن عمومی هیچ حدی از حریم خصوصی وجود ندارد، بلکه افراد در این اماکن نیز می‌توانند انتظار معقولی از حریم خصوصی[1] داشته باشند. نویسندگان مختلف، تعاریف گوناگونی از این اصطلاح ارائه داده‌اند. برخی از آنان از وجه تمایز اطلاعات خصوصی از اطلاعات عمومی برای تبیین این مفهوم سود جسته‌اند. به‌نظر آنان اطلاعاتِ «آن دسته از رفتارهایی که فرد منطقاً انتظار دارد که مورد نظارت قرار نگرفته یا ذخیره نشوند» (Atkinson and Delamont, 2011: 231)، در حیطه اطلاعات خصوصی جای دارند. در مقابل، برخی دیگر بر این عقیده‌اند که «زمانی که فرد انتظار واقعی از حریم خصوصی دارد و جامعه آن انتظار را به‌عنوان انتظاری منطقی بپذیرد، انتظار معقول از حریم خصوصی وجود خواهد داشت» (V. del Carmen, 2014: 194). این‌گونه به‌نظر می‌رسد که انتظار معقول از حریم خصوصی زمانی وجود خواهد داشت که عرف جامعه دمکراتیک، تجاوز به آن را مجاز نمی‌شمارد. علت برشمردن قید دمکراتیک این است که به علت شرایط حاکم بر شهروندان جوامع غیردمکرات، انتظار آنها از حقوقشان نسبت به جوامع دمکرات کمتر بوده و همچنین به علت «عادت کردن آنها به تدابیر نظارتی، انتظار متعارف از حریم خصوصی نیز کاهش خواهد یافت» (Klitou, 2014: 98).

بنابراین، باید به بررسی این موضوع پرداخت که انتظار افراد از حریم خصوصی در این اماکن تا چه حدی منطقی است. به قول یکی از نویسندگان، «اشخاصی که در اماکن عمومی به سر می‌برند، باید قبول کنند که تابع و تسلیم حوادث و اتفاقات عادی و طبیعی در زندگی اجتماعی روزمره هستند» (انصاری، ۱۳۹۰: ۲۵). بنابراین، هر آنچه که لازمه زندگی اجتماعی است، در فضای بیرون جزء حریم خصوصی نخواهد بود. مانند اینکه فرد انتظار داشته باشد، چهره وی رؤیت نشود. اما، «تا زمانی که افراد در محیط عمومی حرکت غیرعادی انجام ندهند، می‌توانند انتظار حریم خصوصی داشته باشند» (Hudson, 2010: 32). بنابراین، با توجه به محیطی که فرد در آن قرار دارد و رفتاری که در آنجا انجام می‌دهد، حد خاصی از حریم خصوصی برای وی مفروض است.

1. Reasonable Expectation of Privacy

اما، مشکل از آنجا آغاز می‌شود که تکنولوژی‌های نوین هرروزه امکانات بیشتری را برای نفوذ به حریم خصوصی کاربران فراهم می‌آورند و آنها را به چشم‌ها و گوش‌هایی برای نقض حریم خصوصی کاربران تبدیل می‌کنند. امروزه، با استفاده از خاصیت بزرگ‌نمایی[1] این دوربین‌ها، می‌توان کوچک‌ترین حرکات مراجعان را زیر نظر داشت و حتی از صفحات مورد مشاهده آنان فیلمبرداری کرد. با کنار هم قرار دادن صفحات مشاهده شده و حالات و بازخوردهای چهره کاربران، می‌توان عادی یا مشکوک بودن فعالیت‌های آنان را احراز کرد. بنابراین، مقام ناظر می‌تواند دریابد که کاربران چه مطالبی را مطالعه، از چه رمزهای عبوری استفاده و با چه کسانی صحبت می‌کنند و ... . این فرایند به معنی ورود به جزیی‌ترین و شخصی‌ترین حوزه زندگی ارتباطاتی کاربران است.[2] همچنین، نوعی دیگر از این دوربین‌ها علاوه‌بر ضبط تصویر، قابلیت ضبط صدا را نیز دارند و می‌توانند مکالمات را شنود کنند. بنابراین، مراجعی که از فناوری انتقال صدا در بستر شبکه[3] استفاده می‌کند یا گفت‌وگوی ویدئویی[4] انجام می‌دهد، تمام مکالمات وی ضبط خواهد شد.

با توجه به مباحث فوق، می‌توان دریافت چنانچه از دوربین‌های مداربسته صرفاً جهت مشاهده رفتارهای عادی کاربران که شامل ورود و خروج آنها می‌باشد، استفاده شود، مشکلی از جهت حریم خصوصی وجود نخواهد داشت و نصب اختیاری دوربین‌ها در این اماکن، باید صرفاً تا حدی باشد که موجبات خدمات‌دهی بهتر را فراهم کند و درعین‌حال به فعالیت‌های خصوصی کاربران نیز خللی وارد نسازد.

---

1. Zoom

۲. در کنار این دوربین‌ها، امروزه دسته‌ای از دوربین‌های مداربسته وجود دارد، که به صورت هوشمند بزهکاران احتمالی را شناسایی می‌کنند، به این معنا که چنانچه متصدی مکان، به کاربری خاص شک داشته باشد و حدس زده باشد که از امکانات موجود در مرکز وی به‌منظور ارتکاب جرم استفاده می‌کند، می‌تواند تصویر کاربر مورد نظر را که در نتیجه مراجعات سابق در اختیار داشته است را برای دوربین تعریف کند و چنانچه فرد مورد نظر وارد مکان مورد نظر شود، تمام فعالیت‌های وی روی صفحه رایانه مقام ناظر قابل مشاهده باشد. همچنین، در صورتی که مقام ناظر همواره در محل حضور نداشته باشد و یا خواهان نظارت بر کاربران از راه دور باشد می‌تواند از فناوری‌هایی همچون «سامانه اعلام خطر» استفاده کند یا حتی با استفاده از «دوربین‌های مداربسته متصل به آی پی» تمام فعالیت‌ها را از راه دور کنترل کند. برای مطالعه بیشتر ر.ک.: خانعلی‌پور واجارگاه، ۹۴:۱۳۹۰.

3. Voice Over Internet Protocol (VOIP)

4. Video Chat

۳. شناسنامه‌دار کردن کاربران رویاروی محرمانگی اطلاعات شخصی

همان‌گونه که در مبحث نظارت ویدئویی نیز گفته شد برخی بزهکاران با ارتکاب جرم در اماکن عمومی ارائه‌دهنده خدمات دسترسی حضوری، امنیت نسبی خود را تأمین می‌کنند. بنابراین، هرگونه اقدامی به‌منظور آگاهی از هویت و فعالیت کاربران و به حداقل رسانیدن ناشناختگی آنان، می‌تواند به‌عنوان ابزاری مؤثر برای کاهش بزهکاری به‌شمار آید. دسته‌ای از کشورها، هرگونه استفاده از خدمات این اماکن را منوط به شناسایی مراجعان می‌کند و در صورت عدم احراز هویت، از فعالیت آنان جلوگیری خواهند کرد. شناسایی کاربران این کشورها از طریق ارائه اطلاعات هویتی، شماره تماس و همچنین نشانی محل سکونت صورت گرفته و پس از اختصاص شماره شناسایی، دسترسی به شبکه میسر می‌شود. همچنین، ازآنجاکه دسترسی بعدی به فعالیت‌های کاربر دشوار است، غالباً در همان زمان استفاده از شبکه، فعالیت‌های آنان ذخیره می‌شود.

به‌عنوان نمونه، در سال ۲۰۰۸ تدابیر نظارتی سختگیرانه‌ای برای کافی‌نت‌ها در مصر وضع شد. کاربران مصری ملزم بودند «مشخصات هویتی، شماره تماس و نشانی پست الکترونیک خود را در اختیار متصدیان قرار دهند و سپس، با استفاده از شماره کاربری که از طریق تلفن همراه خود دریافت می‌کردند، قادر به دسترسی به اینترنت بودند» (Deibert and et al., 2010: 529). پلیس فتای جمهوری اسلامی ایران نیز در بندهای ۸ تا ۱۰ بخشنامه صادره به کافی‌نت‌ها،[۱] متصدیان این اماکن را ملزم به ثبت اطلاعات هویتی و سایر اطلاعات کاربری شامل روز و ساعت استفاده، نشانی پروتکل اینترنت[۲] اختصاص‌یافته

---

۱. «... ۸. دفاتر خدمات اینترنت موظف‌اند اطلاعات هویتی کاربران را با دریافت مدارک شناسایی معتبر (ترجیحاً کارت ملی) ثبت و از ارائه خدمات به مراجعه‌کنندگانی که مدارک شناسایی ارائه نمی‌کنند، خودداری کنند.

۹. اطلاعات هویتی که بایستی مورد ثبت دقیق قرار گیرند عبارت‌اند از: نام و نام خانوادگی، نام پدر، کد ملی، کد پستی و شماره تلفن تماس.

۱۰. دفاتر خدمات اینترنت موظف‌اند علاوه‌بر اطلاعات هویتی کاربران، سایر اطلاعات کاربری شامل روز و ساعت استفاده، IP اختصاص یافته و فایل لاگ وب‌سایت‌ها و صفحات رؤیت شده را ثبت و حداقل تا ۶ ماه نگهداری کنند».

۲. نشانی پروتکل اینترنت (Internet Protocol Address) معرف دستگاه متصل به شبکه است. «هنگامی که دستگاه رایانه و یا هر وسیله دیگری که به شبکه اینترنت متصل می‌شود، نشانی پروتکل اینترنت مختص به خود را دریافت می‌نماید» (Harwood, Rusen and Ballew, 2015: 445).

به کاربر و مهم‌تر از آن پوشه لاگ[1] وب‌سایت‌ها و صفحات رؤیت شده، نموده است.

تشخیص هویت کاربران با استفاده از اطلاعات شخصی آنها ممنوع است، بنابراین به‌طور مطلق نمی‌توان حکم به نقض حریم خصوصی آنان به‌دلیل درخواست اطلاعات داد. چنانچه براساس حقوق داخلی کشور، اطلاعات درخواست شده در زمره اطلاعات شخصی باشند، مطالبه آنها بدون دستور مقام قضایی صالح، ممنوع است. با مطالعه قوانین کشورهای گوناگون محرز می‌شود که ترافیک داده‌های برخط، حافظه نهان اطلاعات و مواردی از این قبیل جز حریم خصوصی اطلاعاتی کاربران است. بنابراین، ذخیره مواردی همچون پوشه لاگ وب‌سایت تمام کاربران مطلقاً ممنوع است، چراکه این پوشه‌ها «تمام فعالیت‌های کاربر در وب‌سایت‌هایی که از آنها بازدید کرده است را ذخیره می‌کنند» (Jansen, Spink and Taksa, 2008: 125) و با استفاده از نرم‌افزارهای لاگ‌خوان می‌توان آنها را بازخوانی کرد و از فعالیت‌های کاربر آگاه شد.

برای پیشگیری از بزه احتمالی نباید همه کاربران را شناسنامه‌دار کرد و با رهگیری فعالیت‌های آنها، از اندیشه‌ها و سلایق آنها آگاه شد. تعمیم ارتکاب جرم احتمالی به همگان مخالف اصل برائت بوده و نباید به بهانه برخورد با اقلیتی کوچک امنیت و آسایش را از کل جامعه سلب کرد. ازاین‌رو، اگرچه دولت مسئول تأمین امنیت فعالیت کاربران و پیشگیری از بزه‌دیدگی احتمالی است، اما؛ این مهم را نباید فراموش کرد که «حریم خصوصی ایشان نیز چهره‌ای از همان امنیتی است که دولت متکفل تأمین آن است» (زندی، ۱۳۹۳: ۲۱۵).

مجمع عمومی سازمان ملل متحد در قطعنامه صادره سال ۲۰۱۳، هرگونه اجبار شرکت‌های تلفنی و ارائه‌دهندگان خدمات اینترنتی[2] به ذخیره اطلاعات کاربران به‌منظور نظارت دولت بر فعالیت‌های آنان را غیرضروری و غیرمتناسب خوانده است. با مقایسه اشخاص مورد حمایت این قطعنامه با کاربران اماکن ارائه‌دهنده خدمات عمومی می‌توان دریافت هنگامی‌که اشخاص حقوقی با دامنه فعالیت ملی و بین‌المللی حق در اختیار گذاشتن اطلاعات شخصی کاربرانشان را ندارند، به طریق اولی، کاربران اماکن ارائه‌دهنده خدمات دسترسی نیز از چنین حمایتی برخوردار خواهند بود.

---

1. Log File
2. Internet Service Provider

با توجه به مباحث مطرح شده در گفتارهای پیشین می‌توان دریافت که نهادهای مسئول پیشگیری از جرم اجازه نظارت فراگیر بر رفتارهای کاربران را نخواهند داشت. شاید با توجه به دامنه وسیع خسارات اغلب جرائم سایبری، پذیرش چنین راه‌حلی دشوار باشد، اما، با مقایسه آن با نقض حریم خصوصی مادی، می‌توان به‌خوبی اهمیت حفظ حریم خصوصی در مقابل کاربست روش‌های نظارت الکترونیکی را درک کرد. به‌عنوان نمونه، تصور کنید مقامات امنیتی شهری متوجه شوند که در یکی از نامه‌های پست شده در ماه اخیر، طرح ترور یکی از مقامات عالی سیاسی یا نخبگان علمی کشور تشریح شده است. یکی از تدابیر پیشگیری از این عملیات تروریستی این است که همه نامه‌های دریافتی این شهر در فاصله زمانی سی روز گذشته توقیف شده و محتویات همه نامه‌ها دقیقاً بررسی شوند. ازیک‌سو، نامه‌های شهروندان از حریم خصوصی ارتباطاتی آنها به‌حساب آمده و قانوناً باید محترم شمرده شوند و ازسوی‌دیگر، شاید بتوان نامه‌ای که اذعان شده است به این شهر ارسال شده است را از میان انبوه نامه‌های ارسالی پیدا کند. یکی از اقداماتی که برای پیشگیری از جرم احتمالی می‌توان انجام داد، بازرسی تمام نامه‌ها و یافتن نامه مورد نظر است. تفاوت این روش با نرم‌افزارهای داده‌کاوی، دوربین‌های مداربسته، بررسی پوشه‌های لاگ وب‌سایت‌ها و مواردی از این دست این است که عامل انسانی مبادرت به تجزیه و تحلیل و پیش‌بینی می‌کند. اما، آنچه واضح است اینکه با این اقدام حریم خصوصی ارتباطاتی همه دریافت‌کنندگان نامه‌ها را باید نقض کنند. حال، آیا برای پیشگیری از این خطر می‌توان حریم خصوصی کاربران را نقض کرد؟[1]

---

۱. برای تقریب به ذهن این ایده، از مثال مشهور «شکنجه و بمب ساعتی» کمک می‌گیریم. ابتدا به‌طور خلاصه بیان می‌شود که به موجب این سناریو، «پلیس، تروریست احتمالی را که مکان بمب مهیبی را می‌داند و ممکن است تعداد بسیاری از افراد را به کشتن دهد، را دستگیر می‌کند. حال، آیا برای جلوگیری از این اتفاق و با هدف یافتن مکان بمب، می‌تواند وی را شکنجه کند؟ یا نباید وی را شکنجه کرد و با انفجار بمب احتمالی، سبب مرگ افراد بی‌گناه شد؟» (S. Jeffreys, 2009: 3). پاسخ به این سؤال فرضی منفی است؛ زیرا این فرد تحت اصل برائت بوده و مجرم بودن وی ثابت نشده است. همچنین، چنانچه شکنجه را برای موارد استثنایی مجاز دانستیم، باید تشکیلات و سازمانی را برای این کار سازماندهی کرده و افرادی را به این منظور آموزش دهیم تا همیشه منتظر چنین اتفاقی باشند و پس ازگذر زمان شکنجه برای حالت اضطراری ـ با این توجیه که منافع عمومی در خطر است ـ امری عادی خواهد شد.

آنچه که سبب جذابیت و درعین‌حال گردش آزادانه اطلاعات[1] در فضای سایبر می‌شود، ناشناختگی کاربران در این فضاست. سلب حق ناشناختگی اکثریت کاربران و آگاهی از عادات و سلایق آنان به نوعی شناسنامه‌دار کردن آنهاست که حتی به‌منظور تأمین امنیت حداکثری نیز پذیرفتنی نیست. چراکه، «چنانچه کاربران شبکه‌ای احساس کنند فعالیت‌های آنها تحت نظارت مستمر زنده یا غیرزنده قرار دارد، بی‌تردید در نحوه فعالیت خود تجدیدنظر خواهند کرد که این خود به معنای ناکام ماندن اهدافی است که از ظهور این فضا دنبال می‌شد» (جلالی فراهانی، ۱۳۸۴: ۱۵۴). از طرفی، به علت پیشگیری از بزهکاری گروهی اندکی، اکثریت کاربران بهنجار به نوعی مجرم پنداشته می‌شوند که این امر، مغایر اصل برائت است. باید به خاطر داشت که صیانت از حریم خصوصی اصل است و «استثنائات آن باید به صورت مضیق تفسیر شده» (Rengel, 2013: 88) و از تعمیم موارد استثنایی به تهدیدهای احتمالی پیش‌رو، اجتناب شود؛ چراکه با نهادینه شدن این روش و کسب اطلاعات گسترده، تضمینی برای جلوگیری از سوءاستفاده‌های احتمالی و تداوم نقض حریم خصوصی برخط با تمسک به اهمیت پیشگیری از جرم و امکان ردیابی موقعیت‌های مجرمانه وجود ندارد.

بنابراین، نهادهای مسئول باید درصدد پیشگیری موقعیت‌مدار عادلانه از جرائم احتمالی برآیند. آن دسته از تدابیر پیشگیرانه، عادلانه هستند که از چارچوب‌های تعیین شده قانونی تجاوز نکنند. ماده (۱۲) قطعنامه شماره ۲۰۰۲/۱۳ شورای اقتصادی و اجتماعی سازمان ملل متحد با عنوان «برنامه توسعه پیشگیری مؤثر از جرم»[2] نیز بر اهمیت قانونمدار بودن تدابیر پیشگیرانه تأکید کرده است. این قطعنامه که مختص تدابیر پیشگیرانه غیرقهرآمیز است، کاربست هرگونه سیاست‌های پیشگیرانه را منوط به صیانت از آن دسته از حقوق بنیادین بشری که در اسناد بین‌المللی به رسمیت شناخته شده‌اند، دانسته و دولت‌ها را تشویق به ترویج فرهنگ قانونمداری برای سیاست‌های پیشگیرانه کرده است. ازاین‌رو، نهادهای مسئول نمی‌توانند از هر نوع تدابیر پیشگیرانه‌ای، بدون پایبندی به حقوق مدنی و سیاسی استفاده کنند، بلکه برای کاربست هر نوع تدابیر پیشگیرانه، ملزم به رعایت قیود برشمرده شده در اسناد یادشده برای صیانت از این حقوق هستند و ازآنجاکه تفاوتی میان تدابیر پیشگیرانه

1. Free Flow of Information
2. Action to Promote Effective Crime Prevention

کنشی و یا واکنشی در این اسناد وجود ندارد، می‌توان قائل به آن بود که پیشگیری موقعیت‌مدار نیز، «به‌منظور عادلانه شدن مستلزم همان حقوق و آزادی‌های فردی‌ای است که باید به هنگام پیشگیری کیفری رعایت شوند» (نجفی ابرندآبادی، ۱۳۸۳: ۵۸۴).

با توجه به مطالب برشمرده شده می‌توان دریافت که با کاربست تدابیر نظارتی در سطح وسیع، احتمال نقض حریم خصوصی کاربران وجود دارد و به قیمت نقض این حق، می‌توان از بسیاری فرصت‌های احتمالی بزهکارانه پیشگیری کرد. بنابراین، برای جلوگیری از این نتایج سوء، کاربست تدابیر نظارتی همه‌جانبه در سطح کلان توصیه نمی‌شود. کم‌رنگ کردن نقش حاکمیت‌ها، به معنی نفی نقش مؤثر آنان در راهبری پیشگیری موقعیت‌مدار از بزه سایبری نخواهد بود. ازاین‌رو، نخستین وظیفه آنان تصویب قوانین حمایت از حریم خصوصی برخط، در مقابل شقوق متفاوت تدابیر پیشگیرانه نظارتی است. چراکه قوانین دقیق، راه هرگونه سوءاستفاده احتمالی را مسدود و حیطه وظایف مسئولان پیشگیری از جرم را مشخص می‌کند. در کنار قوانین فوق، آنان می‌توانند به‌منظور تکمیل تدابیر نظارتی خود، کاربران را تشویق به استفاده از خدمات پیشگیرانه شرکت‌های امنیت خصوصیِ تحت نظارت خود کنند. در این صورت هریک از کاربران (مانند: شرکت‌ها، مراکز صنعتی، مراکز علمی، کاربران خانگی و ...) با توجه به نیازی که به امنیت دارند و رضایت ناشی از آن، از بخشی از حق حریم خصوصی خود چشمپوشی خواهند کرد. در این حالت، دولت نقش حمایتی خود را حفظ می‌کند و با تصویب قوانین موجد مسئولیت مدنی و مسئولیت کیفری و همچنین نظارت مداوم، از متقاضیان این خدمات حمایت می‌کند.

۴. جمع‌بندی و نتیجه‌گیری

به‌موازات تأثیر چشمگیر فناوری‌های اطلاعات و ارتباطات بر کاهش مخاطرات فضای سایبر، امروزه بسیاری از اعضای جامعه جهانی به امنیتی شدن این فضا و پیشگیری حداکثری از بزهکاری تمایل نشان می‌دهندکه یکی از نتایج آن، نقض گسترده حق حریم خصوصی کاربران است. غالب روش‌های نظارت الکترونیکی اعم از روش‌های هوش مصنوعی داده‌کاوی، دوربین‌های مداربسته، ذخیره فعالیت برخط کاربران و مواردی از این دست، زمانی تأثیرگذارند که در سطح وسیع به‌کار روند و طیف گسترده‌ای را مورد

نظارت قرار دهند. اما، هرچه بر گستره کاربست این تدابیر افزوده شود، حریم خصوصی جامعه تحت نظارت بیشتر در معرض نقض قرار خواهد گرفت و رعایت تناسب تدابیر اتخاذی با پیشگیری از بزه احتمالی بسیار دشوارتر خواهد بود. همچنین، باید خاطر نشان ساخت که در بسیاری از موارد نظارت همیشگی بوده و به‌منظور پیشگیری از هرگونه نقض احتمالی امنیت به‌کار گرفته می‌شود و به دنبال پیشگیری از جرمی خاص نخواهند بود و به‌عبارت‌دیگر، ضرورتی برای پیشگیری از بزه وجود ندارد.

به‌منظور اجتناب از آثار سوءتدابیر نظارتی، باید در نظر داشت که دولت‌ها تنها تا جایی موظف به تأمین امنیت سایبری و پیشگیری از بزهکاری برخط هستند که قیود برشمرده شده در اسناد مرجع حقوق بشری، اجازه مداخله در حریم خصوصی کاربران را می‌دهد و فراتر از آن حق تحدید و یا تعلیق آن را نخواهند داشت. بنابراین، هرگونه نقض حریم خصوصی کاربران به‌منظور تأمین امنیت سایبری و پیشگیری از بزه، استثنا بوده و در صورت تحقق شرایط مورد نیاز، می‌بایست به حداقل مداخله در حریم خصوصی اکتفا کرد و صرفاً آن را به حال تحدید و نه تعلیق درآورد. چراکه، تأمین امنیت سایبری زمانی ارزشمند است که شأن و کرامت کاربران پایمال نشود و امکان استیفای آنها از این حق بنیادینشان وجود داشته باشد. در غیر این صورت، به‌منظور پیشگیری از بزه‌دیدگی احتمالی، آنان، بزه‌دیده بالفعل اقدامات مداخله‌جویانه متصدیان پیشگیری از جرم خواهند شد.

کاستن از تدابیر نظارتی فراگیر از جانب حاکمیت‌ها، به معنی انکار نقش مهم آنها در مدیریت پیشگیری موقعیت‌مدار از بزه سایبری نیست. غالب مشکلات کاربست تدابیر پیشگیرانه نظارتی از آنجا آغاز می‌شود که نهادهای مسئول از اختیارات خود پای را فراتر می‌نهند. ازاین‌رو، به‌نظر می‌رسد که یکی از مهم‌ترین وظایف حاکمیت‌ها تدوین قوانین به روز برای صیانت از حریم خصوصی برخط کاربران و در نظر گرفتن ضمانت اجراهای قانونی کارآمد در مقابل هرگونه سوءاستفاده احتمالی است. همچنین، آگاهی‌بخشی افراد از مخاطرات فضای سایبر و واگذار کردن تأمین امنیت به بخش‌های امنیت خصوصی می‌تواند بسیار کارآمد باشد. چراکه در این حالت، با توجه به نیازهای کاربران به‌منظور پیشگیری از بزه‌دیدگی احتمالی، از بخشی از حق خود چشمپوشی می‌کنند.

منابع و مآخذ

۱. آقابابایی، حسین (۱۳۸۹). «لیبرالیسم، حریم خصوصی و قانون پاتریوت»، فصلنامه *سیاست* (مجله دانشکده حقوق و علوم سیاسی)، دوره ۴۰، ش ۲.

۲. ابراهیمی، شهرام (۱۳۹۱). *جرم‌شناسی پیشگیری*، ج ۱، چاپ دوم، تهران، میزان.

۳. احمدی، احمدرضا (۱۳۸۷). «نقص حریم خصوصی، چالشی فراروی پیشگیری وضعی از وقوع جرم»، فصلنامه *مطالعات پیشگیری از جرم*، (۳)۶.

۴. اسکندری، حمیدرضا، سمیه علیزاده و پروانه کاظمی (۱۳۹۰). «کاربرد داده‌کاوی در شناسایی و کشف الگوهای پنهان جرم سرقت»، فصلنامه *نظم و امنیت انتظامی*، (۴)۴.

۵. اصلانی، حمیدرضا (۱۳۸۹). *حقوق فناوری اطلاعات*، چاپ دوم، تهران، میزان.

۶. انصاری، باقر (۱۳۹۰). *حقوق حریم خصوصی*، چاپ دوم، تهران، سمت.

۷. بخشنامه صادره پلیس فتا به کافی‌نت‌ها www.cyberpolice.ir/page/11631.

۸. جلالی فراهانی، امیرحسین (۱۳۸۴). «پیشگیری وضعی از جرائم سایبری در پرتو موازین حقوق بشر»، *فقه و حقوق*، ۲.

۹. خانعلی‌پور واجارگاه، سکینه (۱۳۹۰). *پیشگیری فنی از جرم*، تهران، میزان.

۱۰. زندی، محمدرضا (۱۳۹۳). *تحقیقات مقدماتی در جرائم سایبری*، تهران، جنگل.

۱۱. قانون تجارت الکترونیکی، مصوب مجلس شورای اسلامی، ۱۳۸۲/۱۰/۱۷.

۱۲. قانون جرائم رایانه‌ای، مصوب مجلس شورای اسلامی،۱۳۸۸/۱۱/۱۱.

۱۳. قانون دسترسی انتشار و دسترسی آزاد به اطلاعات، مصوب مجلس شورای اسلامی، ۱۳۸۸/۱۱/۴.

۱۴. محسنی، فرید (۱۳۹۴). *حریم خصوصی اطلاعات: مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه*، چاپ دوم، تهران، انتشارات دانشگاه امام صادق.

۱۵. میرخلیلی، سیدمحمود (۱۳۸۸). *پیشگیری وضعی از بزهکاری با نگاهی به سیاست جنایی ایران*، تهران، سازمان انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.

۱۶. نجفی ابرندآبادی، علی‌حسین (۱۳۸۳). «پیشگیری عادلانه از جرم»، *مجموعه مقالات در تجلیل از استاد دکتر محمد آشوری*، تهران، سمت.

۱۷. نوری، محمدعلی و رضا نخجوانی (۱۳۸۳). *حقوق حمایت داده‌ها*، تهران، کتابخانه گنج دانش.

18. Atkinson, Paul and Sara Delamont (2011). *SAGE Qualitative Research Methods* (Vol. 4), Great Britain, SAGE Publications Ltd.

19. Bennett, Wayne and Kären Hess (2007). *Criminal Investigation*, Canada, Wadsworth Publishing.

20. *Big Brother Watch and Others Against the United Kingdom*, Fourth Section, Application No. 58170/13, Lodged on 4 September 2013.
21. Clarke, R. V. and R. Homel (1997). A Revised Classification of Situational Crime Prevention Techniques, In S. P. Lab (Ed.), *Crime Prevention at a Crossroads*, Cincinnati, OH: Anderson.
22. Clarke, Ronald V. (1997). *Situational Crime Prevention: Successful Case Studies*,2nd ed, United States of America, Harrow and Heston.
23. Deibert, Ronald and John Palfrey, Rafal Rohozinski and Jonathan Zittrain (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, United States of America: The MIT Press.
24. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).
25. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
26. F. Fogelman-Soulie, D. Perrotta and J. Piskorski (2008). *R. Steinberger, Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and their Applications to Security*, IOS Press, Netherlands.
27. Harwood, Michael, Adrian Ciprian Rusen and Joli Ballew (2015). *IC3: Internet and Computing Core Certification Global Standard 4 Study Guide*, Canada, Sybex.
28. Hudson, David (2010). *The Right to Privacy* (Point/ Counterpoint), United States of America, Chelsea House Publishers.
29. Jansen, Bernard J., Amanda Spink and Isak Taksa (2008). *Handbook of Research on Web Log Analysis*, New York, IGI Global.
30. Klitou, Demetrius (2014). *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*, Netherlands, T. M. C. Asser.
31. Mena, Jesús (2003). *Investigative Data Mining for Security and Criminal Detection*, United States of America, Butterworth-Heinemann.
32. Miller, Linda, Kären Hess and Christine Orthmann (2014). *Community Policing: Partnerships for Problem Solving* (Seventh Edition), United States of America, Delmar Cengage Learning.
33. Organization for Economic Cooperation and Development (OECD) (1980). *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*.
34. Rengel, Alexandr (2013). *Privacy in the 21st Century*, Boston, Martinus Nijhoff Publishers.
35. S. Jeffreys, Derek (2009). *Spirituality and the Ethics of Torture* (13th Edition), United States of America: Palgrave Macmillan.
36. Stalla-Bourdillon, Sophie, Phillips Joshua and D. Ryan Mark (2014). *Privacy vs. Security*, UK, Springer.

37. Taniar, David (2008). *Data Mining and Knowledge Discovery Technologies*, UK and USA, IGI Publishing.
38. The Parliament of the United Kingdom, *Regulation of Investigatory Powers Act 2000*. (RIP or RIPA).
39. The Right to Privacy in the Digital Age, Resolution Adopted by the General Assembly (21 January 2014), A/RES/68/167.
40. UN General Assembly, Universal Deceleration of Human Rights, 10 December, 1948.
41. United States Dept of Defense, Technology and Privacy Advisory Committee (TAPAC) (2004). *Safeguarding Privacy in the Fight against Terrorism: Report of the Technology and Privacy Advisory Committee: The Report of the Technology and Privacy Advisory Committee* , Washington, D.C: DOD Technological Innovations in Crime Prevention and Policing: A Review of the Research on Implementation and Impact.
42. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot).
43. V. del Carmen, Rolando (2014). *Criminal Procedure: Law and Practice*, United States of America, Cengage Learning.