فصلنامه مطالعات پیشگیری از جرم (علمی- ترویجی)، سال ۱۰، شماره ۳۶، پاییز ۱۳۹۴
از صفحه ۹۱ تا ۱۲۰

مطالعه تقابل حریم خصوصی شهروندی با گونه‌های تمامیت‌خواه پیش‌گیری از جرایم

یحیی مصطفایی[۱]
کارشناس ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی لرستان
تاریخ دریافت: ۹۴/۰۴/۲۷
تاریخ پذیرش: ۹۴/۰۸/۱۱
مریم فرهمندفر
کارشناس ارشد حقوق جزا و جرم‌شناسی دانشگاه آزاد اسلامی کرمانشاه

چکیده

مقوله امنیت ملی و تلاش برای تحقق همه جانبه آن یکی از اصلی‌ترین مباحث در هر نظام سیاسی می-باشد. تحقق این مهم در مواردی با اعمال مجازات نسبت به بزه‌کاران و در مواردی با اتخاذ سیاست‌های پیش‌گیرانه شکل می‌گیرد. اما پیش‌گیری از جرم به منظور تحقق امنیت ملی و توجه به اقدامات پیش‌دستانه در مواردی باعث تقابل گونه‌های تمامیت‌خواه پیش گیری از جرم با حریم خصوصی شده است. سؤال این پژوهش آن است که در تعارض بین پیش‌گیری از جرم به منظور تحقق امنیت ملی و حریم خصوصی کدامیک مقدم است؟ نتیجه این نوشتار آن است که توجه به حوزه عمومی در کنار حفظ حریم خصوصی با محوریت دولت مردسالار می‌تواند پاسخی به این سؤال باشد. روش این تحقیق توصیفی، تحلیلی است.

واژگان کلیدی: امنیت، حریم خصوصی، حوزه عمومی، دولت مردسالار

مقدمه

۱. نویسنده مسئول Email: Asena.mostafaei@chmail.ir

همه تدابیر جامعه در برابر جرم، محدود به پاسخ‌های واکنشی نیست و بخشی از آن جنبه کنشی دارد. جامعه همیشه منتظر وقوع جرم نیست و لذا همواره با توسل به «سیاست کیفری» به چاره اندیشی پیرامون آن نمی‌پردازد، بلکه گاهی با توسل به «سیاست جنایی» با اتخاذ تدابیر پیش‌گیرانه به مقابله با جرم بر می‌خیزد (کن، ۱۳۸۳: ۱۲۳). بنابراین می‌توان گفت از مهم‌ترین اهداف سیاست جنایی مؤثر «پیش‌گیری» از جرم است.

سزار بکاریا نخستین کسی است که پیشنهاد می‌کند برای کاهش میزان جرایم به جای کیفر و مجازات بزه‌کاران با تحول در وضع اقتصادی و اجتماعی جامعه موجبات ارتکاب جرم از میان برداشته شود. در نظر وی یکی از مهم‌ترین اهداف یک سیاست جنایی مؤثر پیش گیری از جرم است (بکاریا، ۱۳۸۹:۱۳۲). پس از او آنریکو فری به کاربردن اصطلاح «جانشین‌های کیفری» را برای دستیابی به این هدف نظر داشت (بکاریا، پیشین: ۱۵).

پیش‌گیری از وقوع جرم در مدل‌های مختلفی تقسیم‌بندی شده است، که تنها به دلیل ضرورت به‌طور مختصر به آن اشاره می‌شود. در یک تقسیم، «پیش‌گیری» به «اولیه»، «ثانویه» و «مرحله سوم» تقسیم‌بندی شده است. این مدل از پیش‌گیری منتسب به برانتینگهام و فاوست و مأخوذ و ملهم از پیش‌گیری و درمان بیماری‌های همه‌گیر در علوم پزشکی است که در آن از یک سیاست سه مرحله‌ای سخن می‌گویند. سطح اول پیشگیری مربوط به جلوگیری از بروز اختلال یا ایجاد موانعی در راه گسترش آن است. سطح دوم به افراد در معرض خطر بیماری اختصاص دارد و شامل اقدام‌هایی است که در مورد یک گروه خاص یا یک گروه در معرض خطر انجام می‌شود. هدف این نوع از پیش‌گیری جلوگیری از وخیم یا مزمن شدن یک اختلال در حال گسترش است (دادستان، ۱۳۸۵: ۲۸۶). سطح سوم به واگیری مجدد بیماران درمان‌شده و مصون‌سازی آن‌ها در مقابل بیماری دوباره مربوط می‌شود (محمد نسل، ۱۳۸۷: ۴۲).

در تقسیم‌بندی کلی پیش‌گیری از جرم به پیش‌گیری «وضعی» و «اجتماعی» تقسیم می شود. پیش‌گیری وضعی به معنای تغییر در محیط پیرامون و آماج جرم به هدف افزایش هزینه

ارتکاب جرم است، که این امر مستلزم استفاده از ابزارهای خاص مدیریتی و تغییرات محیطی برای تقلیل فرصت‌های ارتکاب جرم توسط مجرمین بالقوه می‌باشد. این روش اگرچه منتهی به حذف تمایلات منحرفانه و مجرمانه برای بهبود ساختارها و وضع اجتماع نمی‌شود اما تا حدود زیادی موجب کاهش گرایش مجرمان به ارتکاب اعمال جنایی می‌گردد.

تمرکز و توجه در بکارگیری پیش‌گیری وضعی با نظام عدالت کیفری نیست اما هر روزه طیف وسیعی از سازمان‌های عمومی و خصوصی و نهادها، مدارس، بیمارستان‌ها سیستم های حمل و نقل، فروشگاه‌ها و مراکز خرید، مشاغل تولیدی، شرکت‌ها، پارک‌های محلی، تفریح گاه‌ها، پارکینگ‌ها در معرض برخورد با انواع جرایم قرار دارند که اصولاً آن‌ها را متمایل به استفاده از انواع روش‌های پیش‌گیری وضعی می‌نمایند (کلارک، ۱۹۹۷: ۲).

به طور خلاصه، این شیوه شامل مدیریت، طراحی، کنترل با مهارت و تحت کنترل درآوردن نظام‌مند و پایدار محیط می‌باشد که به واسطه آن ارتکاب جرایم دشوارتر و با خطر بیش‌تری همراه است و منافع حاصله از ارتکاب جرم را آن‌گونه که نزد مرتکبین نمود می‌یابد کاهش می‌دهد (همان: ۴).

مدل اجتماعی پیش‌گیری از جرم بر شخصیت و منش افراد تاکید می‌شود تا تغییر محیط، لذا طرفداران این رویکرد از پیش‌گیری که به «پوزیتیویست یا تحققی» معروف‌اند مدعی خشکاندن ریشه‌های جرم از طریق شناسایی علل وقوع جرم و انجام اصلاحات فردی و اجتماعی می‌باشند (صفاری، ۱۳۸۰: ۲۷۹).

در این میان برای دستیابی به آماج پیش‌گیرانه، حقوق کیفری به صورت میان رشته‌ای با علوم دیگر مانند روان‌شناسی و جامعه‌شناسی مرتبط می‌شود. برای مثال در بُعد اصلاحات فردی، پیش‌گیری اجتماعی از وقوع بزه متأثر از یافته‌های روان‌شناسی است و اصلاحات اجتماعی از وظایف جامعه‌شناسان می‌باشد. بنابراین می‌توان با اصلاح شخصیت مجرم و تغییر در زیرساخت‌های موجود اجتماعی به هدف نهایی یعنی پیش‌گیری از جرم دست یافت. پیش گیری وضعی از جرم ممکن است نقض حریم خصوصی مردم را به دنبال داشته باشند. اما

تغییرات اعمال شده در محیط با استفاده از روش‌های وضعی پیش‌گیری، به دلیل تنوع و گستره کاربرد آن در اماکن گوناگون، به ظاهر ارتباط بیش‌تری با حریم خصوصی دارد؛ از این‌رو این نوشتار تنها نقض حریم خصوصی به واسطه تقابل با سازوکارهای پیش‌گیری وضعی را مورد تحلیل و ارزیابی قرار می‌دهد. ساختار این مقاله به این نحو است که در ابتدا به تبیین مفهوم حریم خصوصی پرداخته و در ادامه ضمن تشریح تقابل رویکرد تمامیت‌خواه دولت در پیش‌گیری از جرم با حریم خصوصی به چالش‌ها و راهبردهای حاصل از تعارض این دو مقوله می‌پردازد.

تأملی در مفهوم حریم خصوصی

از دیدگاه بسیاری از اندیشمندان تعریف حریم خصوصی مقوله‌ای بسیار مشکل و ابهام برانگیز است. اندیشمندانی مانند *ویلیام بی‌نی*، *تام گرتی*، *آرتور میلر*، *دنیل سولو* و دیگران در آثار خود به این مهم اشاره کرده‌اند (انصاری، ۱۳۸۶: ۱۲). *بی‌نی* مشکلات حریم خصوصی را از جهت تعریف به ذات و قلمرو آن مربوط می‌سازد. *میلر* دشواری تعریف را در ابهام و شکنندگی آن می‌داند و از دیدگاه *گرتی* حریم خصوصی مفهومی متغیر است. از نظرگاه *سولو* جامع‌ترین و باارزش‌ترین حق شهروندی، حق بر حریم خصوصی است. در واقع در یک جامعه دموکراتیک باید توانایی لازم برای ایجاد و حفظ اشکال مختلف از روابط اجتماعی بین شهروندان با مردم وجود داشته باشد. ابزار لازم برای این مقوله آن است که مردم زندگی مستقل از یکدیگر داشته باشند و آن‌چه در این میان مهم تلقی می‌گردد آسودگی ذهن و آرامش فیزیکی است.

وی در کتاب خود تحت عنوان «فهم حریم خصوصی» باور دارد که هیچ کس نمی‌تواند معنی حریم خصوصی را به صورت شمرده بیان دارد چرا که مفهومی سیال و در جریان است (سولو، ۲۰۰۸: ۱). «حریم خصوصی» به عنوان یک مفهوم هم‌پوشان، حوزه‌های مختلف مجزایی از مطالعه و موقعیت‌های رویه‌ای را در بر می‌گیرد. حریم خصوصی معنایی فراتر از «خصوصی» دارد و محدود به حفاظت از یک «امر نهان» نمی‌شود. این مقوله مدعی پوشش

دادن به اطلاعات و فعالیت‌هایی است که اشخاص با آن هر روزه درگیرند. برای مثال اعتبار بانکی افراد، تجویز دارو توسط پزشک یا داروساز و غیره. همچنین گفته شده که حریم خصوصی مشمول موقعیت فیزیکی افراد (مانند خانه و محل کار) و اطلاعات (مانند ارزش خانه و میزان دستمزد) نیز می‌شود. اجتماعیون بر حوزه‌های خاصی از مفهوم حریم خصوصی که در طول زمان دچار تغییر شده‌اند تأکید دارند. برای مثال، *رابرت اسمیت* معتقد است که حریم خصوصی فضای فیزیکی ما را به دور از هرگونه گسست، مداخله خودسرانه، حیا یا پاسخگویی خواهان است، و سعی در جلوگیری از فاش شدن اطلاعات شخصی مربوط به افراد دارد (www.biometrics.gov).

با وجود درک و برداشت‌های متفاوت از این مفهوم، وجه اشتراکی همگی در یک چیز یعنی «فرد انسانی» است. در یک مفهوم موسع، حریم خصوصی شامل پنج حوزه می‌گردد:

۱. حوزه تصمیم: این مفهوم از حریم خصوصی، موضوعات مرتبط با صلاحیت شخصی نظیر تصمیم‌گیری در حوزه زندگی شخصی و بدن و همچنین مسائل شخصی مرتبط با خانواده را شامل می‌شود؛
۲. حوزه محیط فیزیکی: مسائلی مانند خانه، اتاق خواب و غیره و به‌طور کلی محیط فیزیکی را در بر می‌گیرد. این‌که چه اشخاصی می‌توانند به این حوزه وارد شوند یا آن را ببینند از جمله مسائلی است که این حوزه بر روی آن تمرکز می‌کند؛
۳. حوزه قصد: در این بخش، حریم خصوصی با فعالیت‌های محرمانه یا منشی و نهادین افراد که به طور عموم قابل رویت نیستند همراه است. تمرکز این حوزه معمولاً به توانایی اشخاص در مانع شدن دیگران برای دسترسی به ارتباطات‌شان در حال یا آینده باز می‌گردد؛
۴. حوزه اطلاعاتی: این حوزه از مفهوم حریم خصوصی در مورد بکارگیری اطلاعات افراد بحث می‌کند. توانایی اشخاص در چگونگی بکارگیری اطلاعات خود (برای چه کسی و چه اهدافی) و پاسخگویی آن‌ها در ارتباط با دیگر اشخاص از

موضوعات مربوط به حوزه اطلاعات حریم خصوصی است؛

۵. حوزه ارتباط: که به «حق اشخاص در امنیت و محرمانه باقی ماندن محتوای کلیه اشکال و صور مراسلات و مخابرات متعلق به ایشان و اطلاعات مربوط به آن» مرتبط است (اصلانی، ۱۳۸۹: ۲۸).

حریم خصوصی نیز از جمله مفاهیمی است که نسبیّت در مورد آن مطرح می‌شود، چرا که با فرهنگ، اقتصاد، نوع رژیم سیاسی حاکم بر آن کشور مرتبط است. لذا می‌توان گفت حریم خصوصی امری نسبی است که مفهوم آن از کشوری به کشور دیگر ممکن است متفاوت باشد (رحمدل، ۱۳۸۴: ۱۲۹). در مجموع برای ارائه یک تعریف جامع از حریم خصوصی باید به مقوله‌های زیر توجه داشت:

۱. نگرانی‌ها و مصلحت‌های حریم خصوصی باید شناسایی شوند؛

۲. اصول اساسی که قلمرو کلی از حمایت از حریم خصوصی را بیان می‌کنند باید مدنظر قرار گیرند؛

۳. نگرانی‌های حریم خصوصی به هنگام توسعه فناوری اطلاعات به سرعت تخمین زده شود؛

۴. فناوری‌های افزایش‌دهنده حریم خصوصی را قبول و یکپارچه نمود.

به لحاظ تاریخی منشاء پیدایش حق بر حریم خصوصی به قرن ۱۹ میلادی باز می‌گردد. در سال ۱۹۸۰ *ساموئل دی وارن* و *لوئیس دی برانـدیز* در اثر خود با نام «حق بر حریم خصوصی» حق مزبور را به عنوان یکی از اسباب مؤثر و ضروری زندگی انسان در حقوق کامن‌لا تلقی کردند.[۱] پیش از انتشار این مقاله هیچکدام از محاکم آمریکا این مقوله را به صورت صریح به عنوان یک حق قانونی مورد شناسایی قرار نداده بودند. اما پس از آن، دادگاه‌ها در سطوح و حوزه‌های گوناگون این حق را مورد پذیرش قرار دادند.[۲] در نیمه نخست قرن بیستم به نظر می‌رسد برای نخستین‌بار محققین آمریکایی «حریم خصوصی

۱. www.estig.ipbeja.pt/~ac_direito/privacy
۲. http://legal-dictionary.thefreedicitionary.com/privacy

فیزیکی» را مطرح کردند. اما در نیمه دوم این قرن، مفهوم دیگری ازحریم خصوصی به نام «حریم خصوصی اطلاعات» توسط آمریکایی‌ها مورد کنکاش واقع شد. حریم خصوصی در سراسر جهان و در رژیم‌ها و فرهنگ‌های گوناگون امری شناخته شده است. از حیث بین-المللی حقوق بشری نیز اسناد جهانی و منطقه‌ای بر این حق مستقل حقوق بشری صحه گذارده‌اند. ماده ۱۲ اعلامیه جهانی حقوق بشر، مواد ۱۰ و ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی، ماده ۸ کنوانسیون اروپایی حقوق بشر، ماده ۷ منشور حقوق بنیادین اتحادیه اروپا و ماده ۱۸ اعلامیه اسلامی حقوق بشر از آن نمونه‌اند (عباسی، ۱۳۹۰: ۱۰۹). اخیراً بسیاری از کشورها این مفهوم را در قوانین اساسی‌شان درج کرده‌اند و در دیگر کشورهایی که این حق در قوانین اساسی رسمیت نیافته، دادگاه‌ها حمایت از آن را به عنوان یک حق پایه‌ای مورد قبول قرار داده‌اند (کمال، ۲۰۰۵: ۲۹)

تقابل گونه‌های تمامیت‌خواه پیش‌گیری از جرم با حریم خصوصی

چنان‌چه در مقدمه بحث اشاره شد گونه‌های مختلف پیش‌گیری از جرم از سوی جرم‌شناسان مطرح شده است. در این بین، استفاده از شیوه پیش‌گیرانه وضعی و اجتماعی بیش از سایر تقسیم‌بندی‌ها، با استقبال مواجه شده، چنان‌که بسیاری از نوشته‌های جرم‌شناسان فرانسوی و آمریکایی راجع به بحث در خصوص این روش‌ها است. در این نوشته تأکید نگارنده بر تبیین روش‌های نوین وضعی پیش‌گیری در تقابل با حریم خصوصی شهروندان است. در صورتی که شیوه‌های جدید پیش‌گیری وضعی بدون توجیه و به صورت افراطی توسط هیأت حاکم به کار گرفته شوند، با حوزه‌های مهمی از حریم خصوصی نظیر حوزه محیط فیزیکی، اطلاعاتی و ارتباطی تداخل پیدا می‌کنند.

دیدگاه‌های تمامیت‌گرا در پیش‌گیری از جرم به شیوه‌های جدید آن نیز تسری یافته است. به لحاظ تاریخی بینش فراگیر یا تمامیت‌خواه از مقوله پیش‌گیری از جرم در اندیشه سیاست جنایی *انریکو فری* مطرح و پس از آن در جنبش دفاع اجتماعی و در نوشته‌های برخی از جرم‌شناسان معاصر دنبال شد. در این زمان «جرم‌مداری» در نظام کیفری جای خود

را به «مجرم‌مداری» داد به گونه‌ای که بسیاری این واقعیت را دریافتند که محدودیت‌های اعمال عدالت کیفری سنتی حکایت از آن دارد که رویکردی فرا واکنشی یعنی توسل به ابزارهای پیش‌گیرانه باید جایگزین روش‌های دیرین گردد (نیازپور، ۱۳۸۳: ۱۲۵). اما به دنبال افزایش «جرایم خُرد» و اعمال سیاست‌های مبتنی بر «تسامح صفر» که ریشه در نظریه جامعه‌شناختی «پنجره‌های شکسته» در آمریکا داشت، مفهوم موسع پیش‌گیری از جرم نیز با استقبال فراوانی روبه‌رو شد. پیش‌گیری در مورد همه چیز، پیش‌گیری برای همه افراد و در نهایت پیش‌گیری توسط همه، از آثار و نتایج اصل «هر اقدامی پیش‌گیری است» خواهد بود.

در این فرض همه اقدامات هیأت حاکمه با توجیه پیش‌گیری از جرم مواجه بوده و تمام اقشار و سطوح جامعه علاوه بر آن‌که آماج تدابیر پیش‌گیرانه واقع می‌شوند خود وظیفه پیش‌گیری از جرم را عهده‌دار می‌شوند (ابراهیمی، ۱۳۸۷: ۵۳). چنین چالشی علاوه بر دولت‌های توتالیتر (جمع‌گرا) و اقتدارگرا به آفت نظام‌های لیبرال دموکراسی نیز بدل شده است. نوع تشکیلات پلیسی دولت‌های توتالیتر که در همه امور مردم به شکل گسترده دخالت می‌کنند و یا دارای قدرت‌های مستقل پلیسی هستند اصولاً گویای حضور حداکثری دولت است، در حالی‌که دولت حداقلی نباید نیازمند نیروی عظیم پلیسی باشد و وجود چنین نیرویی در سطح وسیع حکایت از فاصله بین دولت و مردم دارد (بوزان، ۱۳۸۷: ۵۹ و ۵۷).

کنترل وسیع حوزه‌های مختلف ارتباطی نظیر تلفن همراه، رایانامه، فکس و تلفن، استفاده از روش‌های «بیومتریک» نظیر چهره‌نگاری یا تشخیص صورت، تصویربرداری از عنبیه و رنگ چشم، انگشت‌نگاری، دست‌نگاری، تشخیص صدا، بکارگیری نیروهای امنیتی و پلیسی در سطح شهرها، موازی‌سازی برای تشکیل سازمان‌های اطلاعاتی و امنیتی و غیره بیش از هر چیز زنگ خطری برای تشکیل یک حکومت امنیتی و حرکت به سوی دژواره شدن جامعه محسوب می‌شود.

به تعبیر *فیلیپ ماری* محقق بلژیکی این حالت مرحله گذار دولت اجتماعی به دولت کیفری یا دولت اجتماعی امنیتی است. ظهور دولت اجتماعی به اواخر قرن نوزدهم و زمان

تصویب قوانین حمایت از زنان و کودکان باز می‌گردد. توسعه نظام تأمین اجتماعی و بیمه‌های اجباری و همگانی با انتشار گزارش *بوریج* در ۱۹۴۲ میلادی و پس از آن تصویب اسناد بین‌المللی و انعقاد معاهدات عام و خاص بین‌المللی ادامه یافت. (مجتهدی، ۱۳۸۸: ۶۷). اما تحولات منطقه‌ای و جهانی منجر به تعدیل و کاهش حاکمیت و گسترش فقر و بی‌عدالتی و طرح دولت پدرسالار با هدف پاسخگو نمودن، آگاه‌سازی و آموزش افراد جامعه و بزه‌دیدگان بالقوه در زمینه بزه‌کاری، توسعه فرآیند امنیت خصوصی، نصب دوربین‌های مراقبتی در معابر و اماکن عمومی و خصوصی، هشدار دهنده‌های ضد سرقت، کارت‌های اعتباری و غیره شده است (کاشفی، ۱۳۸۴: ۲۷۲).

کنترل شدید امنیتی ما را با این واقعیت وحشتناک روبه‌رو کرده است که این اندیشه که فناوری همیشه به عنوان یک راهکار باقی می‌ماند و به مشکل تبدیل نمی‌شود اشتباه است. هدایای بزرگ هزینه‌های سنگین به دنبال دارند. معمولاً خطرها زمانی به فاجعه تبدیل می‌شوند که ظرافت زیاد و شکنندگی نهادهای دموکراسی، از جمله عدالت کیفری و اجتماعی را فراموش کنیم. از این روبرخی از نسل چهارم حقوق بشر سخن به میان آورده‌اند که می‌خواهد از کرامت انسانی، زندگی خصوصی و آزادی‌های فردی و اجتماعی در برابر سوءاستفاده‌های علمی حمایت کند. حکومت‌هایی که مایل‌اند خود را در برابر جرم و جنایت قاطع نشان دهند معمولاً از افزایش تعداد و امکانات پلیس برای پیش‌گیری از جرم طرفداری می‌کنند.

دیدگاه عمومی در این باره چنین است که پلیس سنگ بنای حفظ نظم و قانون می‌باشد اما طبق برخی از آمارهای رسمی افزایش تعداد و اختیارات پلیسی نه تنها نظم اجتماعی مطلوب را محقق نکرده بلکه موجب افزایش هراس در بین شهروندان نیز شده است. از این رو یکی از اندیشه‌هایی که در سال‌های اخیر محبوبیت زیادی پیدا کرده آن است که پلیس باید همراه شهروندان برای بهبود کیفیت اجتماع و رفتار مدنی تلاش کند و در این راه به جای زندانی کردن، از آموزش، ترغیب، متقاعدسازی و مشاوره استفاده نماید (گیدنز، ۱۳۹۰:

.(۳۲۲-۳۲۶)

مهم‌ترین ایراد وارده بر مقوله پیش‌گیری وضعی از جرم از حیث حقوق بشری آن است که این مدل از پیش‌گیری در شکل حداقلی خود باعث افزایش محدودیت و به تعبیری مقوله‌ای محدودساز است. تکیه حداکثری بر پیش‌گیری وضعی، منجر به ایجاد یک جامعه فوق امنیتی و دژمانند، تعدی به حریم خصوصی شهروندان و در نتیجه سلب آزادی‌های فردی می‌شود. تأکید بیش از حد بر روش‌های پیش‌گیرانه وضعی، جامعه را تبدیل به یک قلعه نظامی می‌کند که در آن همه چیز توسط همه کس مورد نظارت و کنترل واقع می‌شود. بدین ترتیب چنین راهبردی به‌جای ایجاد احساس امنیت، خود عامل مولد ترس در شهروندان می‌شود (پاک‌نهاد، ۱۳۸۸: ۲۶۵-۲۶۴).

فیلیپ کئو مدیر اسبق جامعه اطلاعاتی یونسکو نکاتی تکان‌دهنده را در حمایت از حریم خصوصی گوشزد کرده است. وی حرمت زندگی خصوصی اشخاص را یکی از مهم‌ترین مسائل حقوق بشر در هزاره سوم می‌داند و یادآور شده است که «برادران بزرگ» هر حرکت انسان‌ها را برای حفظ برتری راهبردی خود زیرنظر دارند. وی می‌گوید ایالات متحده آمریکا با همکاری کانادا، استرالیا، انگلستان و نیوزلند از شبکه‌های اطلاعاتی که در اختیار دارند با شنود، کنترل و پردازش اطلاعات روزانه بیش از ۳ میلیارد پیام تلفنی، دورنگار و رایان‌نامه در سراسر دنیا استفاده می‌کنند و هرگونه حرکت و فعالیت افراد در خانه، محل کار و فراغت و بیمارستان را تحت کنترل دارند (معتمدنژاد، ۱۳۸۹: ۳۳۳-۳۳۲).

امروزه حقوق کیفری نیز صبغه و ماهیتی سخت‌گیرانه و امنیتی یافته است. گسترش دامنه جرم‌انگاری و تشدید ضمانت اجراهای کیفری، توسعه جرم‌انگاری به رفتارهای غیرعمدی، جرم‌انگاری مقدمات جرم، تصویب قوانین برای پیش‌گیری و مقابله با بزه‌های امنیتی و تروریستی در حداقل زمان ممکن بحث حقوق کیفری امنیت‌مدار را در برخی از کشورها نظیر آمریکا و فرانسه مطرح ساخته است (مجیدی، ۱۳۸۶: ۷۷).

حریم جغرافیایی یا مکانی

در این بخش مقاله نقش فناوری برای توسعه «خدمات مبتنی بر تعیین محل» به‌وسیله دولت‌ها، در رابطه با مفهوم حریم خصوصی مورد بررسی قرار می‌گیرد. مسئله اصلی آن است که «انتظار مشروع» از حریم خصوصی مفهوم شایسته و مناسبی برای حمایت از آن در برابر قدرت دولت می‌باشد. استفاده از سازوکارهای جدید فناوری، جمع‌آوری و ثبت اطلاعات مربوط به موقعیت جغرافیایی افراد را آسان کرده است. «اطلاعات جغرافیایی» گونه‌هایی مختلف از اطلاعات می‌باشند که ممکن است مورد پوشش قرار گیرند. در این خصوص تمرکز ما می‌تواند بر روی «داده‌های جغرافیایی»، «داده‌های محلی» و «داده‌های متحرک – پویا» باشد. با در دست داشتن اطلاعات مکانی افراد، دولت‌ها قادر به توسعه سرویس‌های تعیین محل شهروندان می‌شوند، سرویس‌هایی که مجهز به ذخیره‌سازی اطلاعات مربوط به حریم خصوصی افراد است (اس‌جک، ۲۰۰۸: ۳۹۷). استفاده از سامانه‌هایی نظیر «جی.آی.اس» و «جی.پی.اس» از کاربردی‌ترین ابزارها در راستای سطح ایمنی شهروندان بوده و قابلیت‌های فراوان این سامانه باعث شده که در بسیاری از موضوع‌ها از آن مدد بگیرند (واجارگاه، ۱۳۹۰: ۵۵).

در بسیاری از موارد، ثبت اطلاعات مربوط، توسط سرویس‌های تعیین محل را تهدیدی علیه حریم خصوصی خود تلقی کرده‌اند. برای مثال پژوهشی که در بین سال‌های ۲۰۰۲ تا ۲۰۰۷ توسط یکی از سرویس‌های داخلی در کشور آلمان انجام شده نشان می‌دهد که ۳۹ درصد مردم این کشور حریم خصوصی را بنیادی‌ترین حق بشری خود قلمداد کرده‌اند. از میان ۱۱ گزینه پیش رو در این پیمایش ۲ مورد آن‌ها یعنی دوربین های مراقب در مکان عمومی و همچنین تعیین هویت الزامی برای شهروندان ۱۲ سال به بالا به عنوان تهدیدهایی کوچک علیه حریم خصوصی شهروندان اعلام شده است. اما ۹ مورد دیگر که تهدیدهایی جدی و خطرناک در راستای نقض حریم خصوصی اعلام شده‌اند عبارتند از:

۱. انتقال اطلاعات مسافرین توسط سرویس‌های هواپیمایی به کشور مقصد
۲. ردیابی و ثبت موقعیت جغرافیایی افراد به‌وسیله «پویشگرهای خودکار»

۳. انجام عمومی آزمایش DNA
۴. تجسس‌های پیش‌گیرانه توسط دولت
۵. ردیابی و ثبت موقعیت جغرافیایی شهروندان توسط مخابره‌های تلفنی
۶. توقیف احتیاطی در موارد مشکوک
۷. جست‌وجوی منازل به دلیل سوءظن
۸. نظارت دولتی بر «رایانامه‌ها» و ارتباطات اینترنتی
۹. استراق سمع مکالمات تلفنی (اس‌جک، همان: ۳۹۳).

همان‌طور که اشاره شد برخی از این موارد که امکان نقض حریم خصوصی شهروندان را توسط دولت میسر می‌کند به سرویس‌های تعیین محل جغرافیایی مربوط می‌شوند. اگرچه استفاده رایج و مرسوم از این سرویس‌ها تحت لوای حمایت از امنیت شخصی شهروندان معرفی شده است، اما می‌تواند خطری بالقوه برای تهدید حریم خصوصی به حساب آید. بسیاری از این فناوری‌ها ضبط و نظارت، می‌تواند فرصت سوءاستفاده را در اختیار افرادی قرار می‌دهند که به این اطلاعات دسترسی دارند. ابزارهای مجهز به این فناوری تنها زمانی می‌توانند مؤثر و کارا تلقی شوند که در مکان و زمان مناسب و با مداخلات صحیح انسانی صورت گیرند (واجارگاه، ۱۳۹۰: ۱۴۷).

بر اساس آن‌چه گفته شد، با شرایطی می‌توان انتظار مشروع از حریم خصوصی را برای شهروند به وجود آورد. هر شهروندی می‌بایست «انتظار ذهنی و واقعی» از حریم خصوصی را در شرایط مشخص داشته باشد. جامعه نیز باید آماده پذیرش «انتظارات عینی» به عنوان یک امر معقول باشد که در این زمینه نیز آراء مختلفی از دادگاه‌های اروپایی در این زمینه صادر شده است. سؤالی که می‌بایست در این راستا مطرح ساخت چنین است که آیا همه افراد به یک میزان می‌توانند از حریم خصوصی بهره مند شوند؟ اگرچه انتظار مشروع از حریم خصوصی توسط بسیاری از قضات در «دادگاه اروپایی حقوق بشر» به رسمیت شناخته شده است. اما استثنائاتی نیز وجود دارد، برای مثال در دعوای «لویی علیه سوییس» دادگاه چنین

رای داد که شهروندی که درگیر فعالیت‌های مجرمانه (از قبیل حمل و نقل و قاچاق مواد مخدر) است باید انتظار کم تری از حریم خصوصی داشته باشد. در این پرونده دادگاه با استفاده از دستگاه‌های استراق سمع توانسته بود مکالمات منزل *لویی* را تحت پوشش درآورد. دادگاه اعلام داشت که *لویی* باید می‌دانست که مشغول یک عملیات جنایی بوده و همواره خطر پوشش زندگی شخصی او توسط نیروهای مخفی پلیس وجود دارد (www.privacynetwork.info).

امروزه بسیاری از فعالیت‌های مجرمانه سازماندهی شده نظیر پولشویی، تروریسم، قاچاق موادمخدر و غیره تهدیدی علیه امنیت ملی کشورها محسوب می‌شوند. دولت‌ها برای مقابله با این تهدیدات از سرویس‌های پیشرفته تعیین محل اشخاص به‌عنوان یکی از ساده‌ترین و معمول‌ترین روش‌ها استفاده می‌کنند، اگرچه این مهم ممکن است نقض حریم خصوصی برخی را به دنبال داشته باشد. پس انتظار مشروع از حریم خصوصی - نه هرگونه انتظاری - را می‌توان به‌عنوان ابزاری کارا و مؤثر در برابر دخالت‌های دولت به واسطه پیش‌گیری از جرم به رسمیت شناخت. در این بین باید توجه داشت که این اقدامات نباید منجر به نقض حریم خصوصی گسترده افراد شود.

«دوربین‌های مداربسته» نظارت پیش‌گیرانه یا نقض حریم خصوصی؟

در واقع آن‌چه امروزه تلویزیون مداربسته می‌نامیم یکی از شیوه‌های نظارت و مراقبت است که در دهه اخیر به گستردگی در محیط‌های اجتماعی به کار می‌رود. دوربین‌های کنترل‌کننده فروشگاه‌های بزرگ، مراکز تجاری، انبارها، بیمارستان‌ها، ایستگاه‌های قطار، خیابان‌ها و پارک‌ها از این نمونه‌اند (کوسن، ۱۳۸۴: ۳۲۵). اگرچه دوربین‌ها توانایی مراقبت از تمامی حرکات و رفت و آمدهای شهروندان را دارا بوده و در راستای حفظ امنیت شهروندان اتخاذ می‌شود، اما به طور کلی مقوله‌ای خوشایند برای مقامات دولتی است، گرچه نباید حقوق بنیادین را در کارزار امنیت قربانی کرد.

مثال‌های مختلفی از این نحوه رویکرد پیش‌گیرانه وجود دارد که می‌تواند منتهی به

نقض حریم خصوصی شهروندان شود؛ زیرا این مطلب که همه ما می‌توانیم در یک مکان عمومی هم در حالت خصوصی باشیم مورد پذیرش همگانی است. اگرچه ضبط تصاویر در مکان‌های عمومی عادتاً نباید نقض حریم خصوصی تلقی شود اما کاستن از انتظار افراد برای بهره‌مندی از حریم خصوصی در اماکن عمومی به منزله انکار حق برخورداری از حمایت‌های متناسب در قبال سوءاستفاده از نظارت‌های آشکار خیابانی نیست.

زندگی خصوصی ممکن است با آزادی اطلاعات اصطکاک ایجاد نماید، که در این موارد بر اساس عرف رایج، قاضی تشخیص می‌دهد که کدام بخش از زندگی آن‌ها جزء حریم خصوصی و کدام بخش می‌تواند منتشر گردد. موضوع قابل توجه در کشور آمریکا آن است که نشریات زرد با تمسک به جریان آزادی اطلاعات تمایل زیادی به مداخله در زندگی شخصی افراد مشهور دارند. برای مثال در یک مورد عکس برهنه یک هنرپیشه آمریکایی که معلوم شد توسط دوربین‌های مداربسته گرفته شده صفحه اول بسیاری از نشریات آمریکا را به خود اختصاص داده بود. این دوربین‌ها به‌طور قطع به منظور پیش‌گیری از جرم تعبیه شده بودند و نه به منظور ورود به حریم خصوصی اشخاص. به طور کلی در این کشور ورود به حریم خصوصی اشخاص مشهور، بسیار شایع و مورد استقبال توده مردم و نشریات زرد است.

به باور دکترین آمریکایی حریم خصوصی، تمام جنبه‌های حریم خصوصی افراد برای نظارت عموم مجاز و حریم خصوصی، مفهومی جدا و مستقل از سایر حقوق فردی است. «همین که شخصی واجد یک شخصیت عمومی می‌شود کافی است تا تمام جنبه‌های زندگی وی برای رویت و نظارت عموم مجاز گردد. لذا هیچ محدودیتی برای افشاگری در مورد افراد و انتشار اسرار زندگی خصوصی آن‌ها وجود ندارد» (انصاری، پیشین: ۳۱).

مثال دیگر پخش فیلم ویدیوئی از رئیس جمهوری وقت آمریکا *بیل کلینتون* است. فیلم مذکور بیانگر معاشقه با یک زن بود که جنبه عمومی و رسانه‌ای پیدا کرد. دوربین بکارگرفته شده برای ضبط وقایع به لحاظ امنیتی و برای پیش‌گیری از وقوع جرم به کار گرفته شده بود.

در کشور انگلیس نزدیک به چهار میلیون دوربین، مکان‌های عمومی را تحت نظر دارند. هر شهروند انگلیسی، ۳۰۰ بار در روز با حدود ۳۰ شبکه عکس‌برداری می‌شود. ۷۰۰ دوربین نیز پلاک‌های اتومبیل‌هایی که وارد شهر لندن می‌شوند را برای بررسی پرداخت مالیات کنترل می‌کنند. به همین دلیل انگلیس در ترجیح رویکرد امنیتی بر مبنای فناوری مشهور می‌باشد (ابراهیمی، پیشین: ۱۰۳).

با وجود نیاز به احساس امنیت در میان شهروندان در مقابل جرم و نیز وجود چنین فناوری‌های پیش‌گیرانه و نظارتی آیا حریم خصوصی شهروندان ایمن و مصون از تعرض خواهد ماند؟ در کانادا اگرچه نظارت ویدیویی در اماکن عمومی از حدود ۲۰ سال پیش آغاز شده، اما شیوع استفاده از آن به اندازه انگلیسی نیست.

در سال ۱۹۹۵ میلادی ۷۰ درصد کلیه بانک‌های مورد سرقت واقع شده در کانادا مجهز به فناوری نظارت ویدیویی بودند. البته ادعا شده که در ۷۵ درصد مجموع جرایم ارتکابی نظارت ویدیویی در کسب اطلاعات مقدماتی برای کشف جرم نقش مؤثری داشته است. مفسران از همان زمان پیشگویی کردند که نظارت ویدیویی به طور تأسف‌باری به یکی از ابزارهای پیش‌گیری از جرم در آینده تبدیل خواهد شد (نی‌تو، ۱۹۷۷: ۱۰).

تأثیر نظارت ویدیویی در مکان‌ها و موقعیت‌های گوناگون متفاوت است. بسیاری از مطالعات در کانادا نشان می‌دهند که دوربین‌های بدون صفحه نشانگر کم‌ترین تأثیر را در بازدارندگی و پیش‌گیری از وقوع جرم در بانک‌ها و فروشگاه‌ها داشته‌اند. در فرانسه استفاده از ابزارهای شنود، ابزارهای الکترونیکی و نظارت ویدیویی اگر به منظور افشای اطلاعات جنسی یا مالی اشخاص به کار گرفته شوند غیرقانونی است، اما برای کشف عملیات جاسوسی و فعالیت‌های سیاسی مجاز است. اگرچه در حقوق فرانسه تشتت آراء به چشم می‌خورد. به عنوان مثال شعبه جنایی دیوان عالی کشور فرانسه ضبط اعمال و رفتار کارمندان به‌وسیله دوربین مخفی جاسازی شده در دریچه کولر توسط شاکی برای اثبات سرقت و خیانت در امانت کارمندان را نقض حریم خصوصی اشخاص ندانسته است. چرا که این عمل شبیه

به ضبط تصاویر راجع به خلوت و زندگی خصوصی افراد نیست و حتی به بزه‌دیده اجازه داده است تا بدون اطلاع و آگاهی متمم، گفت‌وگوهای تلفنی توهین‌آمیز او را ضبط و به دادگاه ارائه کند، در حالی که شعبه دوم مدنی دیوان عالی کشور ضبط متقلبانه مکالمه تلفنی خصوصی دیگری را غیرقابل پذیرش دانسته است (تدین، ۱۳۸۸: ۱۴۸).

شیوع عملیات تروریستی در سال‌های اخیر جواز استفاده از نرم‌افزارهای الکترونیکی و نظارت ویدیویی در اماکن عمومی را برای دولت فراهم کرده، از این رو امروزه نظارت‌های وسیع دیدبانی الکترونیکی در معابر و مناطق عمومی شهرها وجود دارد. صدها دوربین تلویزیونی حومه شهر پاریس را تحت کنترل دارند. مناطق تجاری و مالی با بیش از ۱۶۰ دوربین که به طور ۲۴ ساعته تحت نظارت پلیس قرار دارند. بیش از ۲۵۰۰ دوربین در اتوبوس‌های شهرداری تعبیه شده‌اند. بیش‌تر فروشگاه‌ها و امنیت ترابری هوایی به‌طور وسیع از چنین نرم‌افزارهایی استفاده می‌کنند. اسپانیا، روسیه، موناکو و دیگر کشورها در سراسر دنیا وضع مشابهی دارند و هر ساله هزینه‌های گزافی را صرف نصب دوربین‌ها و استفاده از نیروی انسانی می‌کنند (نی‌تو، همان: ۱۰).

با وجود واقعیت‌های مشابه پرسش آن است که استفاده از دوربین‌های مداربسته و به طور کلی مراقبت‌های ویدیویی تأثیری در پیش‌گیری و کاهش وقوع جرم داشته و یا آن‌که این نوع اعمال نظارت بر شهروندان با اهداف دیگری طراحی شده‌اند؟ در سال ۲۰۰۶ دادگاه قضایی آمریکا گزارشی راجع به سیستم‌های ویدیویی در مناطق عمومی صادر کرده که توسط جری *راتسفیل* استاد دادگاه جنایی در دانشگاه تمپل تنظیم شده است. این گزارش توضیح کاملی از این فرآیند به دست می‌دهد و مضرات و مزیت‌های وابسته به این تکنولوژی و یافته‌های ارزشمند این سیستم را به طور مختصر بیان می‌کند. این گزارش بیان می‌دارد که مشاهدات کلی در بین سیستم‌های مدیریتی و مناطق عمومی حاکی از کارایی دوربین‌های مراقبت ویدیویی برای پیش‌گیری از جرم می‌باشد اما پیدا کردن مدارک واقعی از کاهش جرم بسیار سخت است. در سال ۲۰۰۲ وزارت کشور انگلستان گزارشی به نام «پیش‌گیری از

جرم بواسطه دوربین‌های مداربسته» منتشر کرد. این گزارش توسط *برانـدون ولِـش* اسـتاد اداره دادگاه جنایی در دانشگاه ماساچوست و *دیوید فارینگتون* استاد جرم‌شناسی در موسسـه جـرم-شناسی دانشگاه کمبریج نوشته شده است. مؤلفان، ۴۶ پژوهش مرتبط از هر دو کشور آمریکـا و انگلیس را طبق معیارهای اسلوب‌شناسی دقیق بررسی کردند و دریافتند که فقط ۲۲ مـورد از مطالعاتشان برای قرار دادن در تجزیه و تحلیل‌ها به اندازه کافی دقیق است.

بر اساس این ۲۲ مطالعه، آن‌ها نتیجه گرفتند که مراقبت ویدیویی به مقـدار کمـی جـرایم را کاهش می‌دهد و بیش‌تر در کاهش جرایم علیه وسـایل نقلیـه در پارکینـگ‌هـا مـؤثر اسـت. مراقبت‌های ویدیویی تأثیر کم و یا هیچ تأثیری روی جرم در حمل‌ونقل عمومی و مرکز شـهر ندارند. *مارتین گیل* استاد جرم‌شناسی در دانشگاه لیسیستر این مقوله را مورد ارزیابی قـرار داده و در نتیجه گزارشی تنظیم نمود. در این گـزارش وی یـک ارزیـابی مـنظم از ۱۳ پـروژه اجـرا شده مراقبت ویدیویی در محل‌های مختلف شامل مرکز شهرها، پارکینگ‌هـا، بیمارسـتان‌هـا و مناطق مسکونی تهیه کرد. نتایج متناقض این پژوهش حاکی از آن است کـه جـرایم در برخـی مناطق کاهش و در مناطق دیگر افزایش یافت. همچنین گزارش متذکر می‌شود کـه سـهم ایـن فناوری‌ها در کمک به پلیس در حفظ نظم عمـومی و کشـف جـرایم بـه صـورت نظـام‌منـد – متشکل از اجزاء کوچک‌تر، با سیاست هدفمند، ناظر، قانونمند و منظم– گسترش یافتـه اسـت. توصیه این گزارش این است که به منظور افزایش قوای زیر بنای این رویکرد پیش‌گیرانه بهتـر است این سیاست توسعه یابد. *وادریسمن* استاد جرم‌شناسـی و رئـیس گـروه امنیتـی و انتظـامی ملی از دانشگاه اوتادا ارزیابی و بررسی تحقیقات را هدایت مـی‌کـرد. مـروری بـر ایـن تحقیـق نشان داد تأثیرات نظارت ویدیویی در مورد جرایم، کاملاً متغیر و نسبتاً غیرقابل پیش‌بینی اسـت و ارزش بازدارنده نظارت ویدیویی، در طول زمان و در مقوله‌های جنایی مختلف می‌باشد.

سیستم‌های نظارت ویدیویی به موقعیت‌های مربوط به گردشگری نیز مربـوط مـی‌شـدند. در مجموع می‌توان گفت در حال حاضر پیدا کردن شواهد واضح که نشـان‌دهنـده ایـن باشـد که نظارت ویدیویی مؤثر در پیش‌گیری از وقوع جرم می‌باشد کار سختی اسـت. بـه هـر حـال

نتیجه گرفتن عکس آن نیز مشکل است. یک نقش خیلی مؤثر و ارزشمند برای نظارت ویدیویی ممکن است مطرح کردن آن به عنوان منبعی از شواهد در کشف و تحقیق جرایم باشد. استفاده از دوربین‌های مداربسته اگرچه با هدف پیش‌گیری از وقوع جرم مورد باشد اما باید علاوه بر روش‌های پیش‌گیری تدابیر لازم به منظور جلوگیری از سوءاستفاده احتمالی را به ترتیب زیر مدنظر داشت:

۱. باید شهروندان را از وجود دوربین‌های مداربسته به‌وسیله تابلوهای اطلاع‌رسانی مطلع نمود تا این وسیله به ابزار سرکوبی مردم تبدیل نشود؛
۲. حق دسترسی افراد به اطلاعات ثبت شده؛
۳. حق بزه‌دیده سوءاستفاده از این سازوکارها جهت مراجعه به دادگاه؛
۴. ممنوعیت نصب دوربین در محل سکونت افراد (ابراهیمی، ۱۳۹۰: ۱۱۱)

توسعه افراط گونه در بکارگیری روش‌های بیومتریک

بیومتریک به‌عنوان روش شناسایی منحصر به فرد انسان‌ها بر مبنای یک یا چند ویژگی یا مشخصه طبیعی است. این روش به عنوان یک شیوه مدیریت دسترسی به هویت و کنترل در گروه‌های تحت نظارت مورد استفاده قرار می‌گیرد. شایع‌ترین روش‌های بیومتریکی به شرح ذیل می‌باشند:

۱. انگشت‌نگاری: فرآیند بیومتریک با انگشت‌نگاری و شست‌نگاری، عملکردی متداول به حساب می‌آید که علت آن می‌تواند به واسطه آشنایی عامه مردم با این رویه و نیز کارایی استاندارد انگشت‌نگاری به‌وسیله جوهر باشد. همچنین امروزه استفاده از دستگاه‌های خواندن اثرانگشت، بیش از حد افزایش پیدا کرده است که در میان آن‌ها می‌توان به قرار دادن این دستگاه در «موشواره» و صفحه کلید یا کارت‌های هوشمند و دستگاه‌های کوچک مرتبط اشاره کرد (سین، ۲۰۰۲: ۱۵).

۲. هندسه و شکل دست: هرچند پیشتازی فرآیند بیومتریک بر اساس شکل دست افراد، بازار خود را از دست داده است اما به هر حال این فناوری همچنان اجرا می‌شود. یکی از دلایل احتمالی کاهش میزان تمایل برای به کارگیری هندسه و شکل دست، چالش برانگیز بودن دقت دستگاه‌های مربوطه است.

۳. اسکن (تصویر) شبکیه چشم: بیومتریک بر اساس تصویربرداری شکل رگ‌های شبکیه چشم افراد هرگز نتوانست علی‌رغم تمایل مردم به فناوری؛ آن‌چنان که انتظار می‌رفت جای مناسبی در میان سایر روش‌ها داشته باشد. دو عاملی که در این زمینه مؤثر بوده‌اند عبارتند از:

الف) فرآیند لازم، برای بازبینی شبکیه چشم افراد، هنگامی که در مقابل و یا حتی در نزدیکی دستگاه قرار می‌گیرند، موجب نگرانی استفاده‌کننده به لحاظ تمیز بودن دستگاه و یا تأثیرات ورود اشعه در چشم، می‌شود.

ب) هزینه تصویربرداری شبکیه به‌ویژه در مقایسه با کاهش هزینه‌های برخی دیگر از تکنولوژی‌های مورد استفاده بیومتریک، هنوز گزاف است. به هر حال این فناوری هنوز جایگاه خود را در مواردی که امنیت مطلوب از برای تسهیلات هسته‌ای و یا نظامی مورد نیاز باشد، حفظ کرده است.

۱. تشخیص عنبیه چشم: فرآیند بیومتریک بر اساس تصویربرداری از فرج عنبیه که رنگ چشم را تشکیل می‌دهند (شکل فیزیکی عنبیه باعث می‌شود که رنگ چشم در اطراف مردمک به رنگ‌های مختلف دیده شود)، به شدت مورد توجه قرار گرفته است و ادعا می‌شود که میزان دقت این تکنولوژی به نسبت سایر فناوری‌های بیومتریک، بیش‌تر است که علت آن قابلیت نصب نرم‌افزاری این تکنولوژی در کامپیوتر و یا دوربین‌های دیجیتال است.

۲. تشخیص صورت: این فناوری متکی بر تصویربرداری ویژگی‌های خاص صورت از قبیل چشم‌ها، بینی و دهان و غیره می‌باشد. فناوری تشخیص صورت احتمالاً شرایط فناوری سایر روش‌های بیومتریکی دیگر را در چند سال گذشته تغییر داده است. تعدادی از تأمین‌کنندگان ادعا نمودند که محصولی دارند که می‌تواند یک صورت را در یک جمعیت انبوه تشخیص دهد که اخیراً این ادعا را در سال ۲۰۰۱ در یک مسابقه فوتبال آمریکایی، عملی گردید. این فناوری پس از حمله یازدهم سپتامبر به طور جدی دنبال شد چرا که به نظر می‌رسید که بتواند تروریست‌ها را در میان جمعیت پیدا کند. در حقیقت، بسیاری از فرودگاه‌ها این فناوری را مورد بررسی قرار دادند. در ایالات متحده آمریکا این دستگاه در فرودگاه‌های بوستون و سایر شهرها یا نصب شده است و یا مورد بررسی قرار گرفته است. ولی تأثیر این فناوری در کاربردهای جهانی مورد اطمینان نبوده است.

۳. تشخیص صدا: این بیومتریک بر اساس این نظریه قرار دارد که صدای هر فرد، واحد و مشخص بوده و با اشخاص دیگر متفاوت است. این امر که قاعدتاً متکی بر تصویر دیجیتالی امواج صوتی ایجاد شده در هنگام گفتن برخی کلمات خاص می‌باشد به گونه‌ای طراحی شده که وقتی فردی بخواهد پس از یک ثبت نام به سیستمی وارد شود وی باید تمام یا بخشی از کلمات را دوباره تکرار کند و سیستم تشابه امواج صوتی را در مقایسه با اجرای اولیه، بررسی خواهد کرد. تشخیص صدا به دقت سایر دستگاه‌های بیومتریک از قبیل انگشت‌نگاری و تشخیص شبکیه نیست ولی می‌تواند تنها فناوری قابل دسترس در برخی کاربردهای خاص (از قبیل فعل و انفعالات تلفنی) باشد.

۴. دینامیک امضا / صفحه کلید: دو مورد که به صورت نمادین و واحد توسط هر فرد

انجام می‌گیرد، امضا کردن و تایپ با صفحه کلید است. بیومتریک دینامیک امضا، جهت، سرعت و فشاری را که در هنگام امضا نام خود داریم بررسی کرده و با امضاهای اخیرمان مقایسه می‌کند. بیومتریک با صفحه کلید، سرعت، ریتم و فشار دست‌ها را هنگام تایپ بررسی می‌کند. لازم به یادآوری است که اخیراً صفحه‌های زیردستی برای امضا الکترونیکی در برخی از فروشگاه‌ها برای خرید با کارت‌های اعتباری به بازار آمده است (رئیسی، ۱۳۹۰: ۱۲۲).

استفاده از روش‌های بیومتریک امروزه اشکال گوناگون و متنوعی یافته است. از سویی قانونی شدن سریع این فرآیند و از جهت دیگر تنوع ابزارهای مورد استفاده منجر به نقض حریم خصوصی افراد شده‌اند. برای نمونه سازمان «ایکائو» که در سال ۱۹۹۴ در شیکاگوی آمریکا تشکیل شد و بیش از ۱۸۹ عضو در سراسر جهان دارد امروزه مسئولیت وضع استانداردهایی را در جهت ارتقای امنیت بر عهده دارد. این سازمان تا سال ۲۰۱۰ همه اعضای خود را ملزم به استفاده از ماشین‌های رمزخوان استاندارد در مرزهای خود نموده است. اجباری شدن استفاده از ماشین رمزخوان در قانون میهن‌پرستی آمریکا برای تقویت سازمان-های آمریکایی در جهت مقابله با عملیات تروریستی از نمونه‌های دیگر توسعه همه‌گیر بیومتریک است. استفاده از بیومتریک به اندازه‌ای شایع شده که فرد در صورت معترض بودن و تن ندادن به انحصار این روش‌ها به صورت اجباری باید از رفت‌وآمد در بسیاری از محیط-های اجتماعی از قبیل فرودگاه‌ها، سالن‌های مترو، هتل‌ها و فروشگاه‌های عظیم خود را محروم ببیند (محسنی، ۱۳۸۹: ۳۳۱ و ۳۳۲).

پیش‌گیری وضعی از جرم در «فضای سایبر»

نقض حریم خصوصی، مقوله‌ای است که می‌تواند باعث رنجش بسیاری از افراد شود. وقوع این موضوع در فضای سایبر نیز امکان‌پذیر است. مطالعه پیش‌نویس لوایح قانونی و خط مشی گذاری‌های دولتی نشان می‌دهد که همواره تقاضای حمایت بیش از حریم خصوصی در فضای سایبر توسط کاربران و مردم وجود دارد. مشکل از آن‌جا ناشی می‌شود که

اینترنت، فضایی آزاد را برای همه کاربران مهیا ساخته و این مسائله حق جمع آوری اطلاعات را برای دیگران به وجود آورده است. در این بین آزادی در جمع‌آوری اطلاعات خصوصی شهروندان برای دولت، بیش از سایرین امکان‌پذیر است. بنابراین همواره این احساس در بین شهروندان می‌تواند وجود داشته باشد که اینترنت به‌عنوان وسیله‌ای در راستای نظارت بر مسائل خصوصی‌شان تلقی گردد (کمال، پیشین: ۲۵).

اگرچه اشخاص تا اندازه‌ای می‌توانند هنگامی که «برخط» هستند مانع از نقض حریم خصوصی خود در فضای سایبر شوند، اما در موارد مختلف مجبور به ارائه اطلاعات مربوط به حریم خصوصی خود به دولت به دلایل گوناگون می‌باشند. آن‌چه مهم است آن‌که با افزایش و پیشرفت در فناوری می‌بایست، راهکارهایی برای جلوگیری از نقض حریم خصوصی پیش‌بینی شوند (ماجستی، ۲۰۱۰: ۲۷).

شواهد زیادی مبنی بر نقض حریم خصوصی مردم در فضای سایبر توسط دولت به دلیل حفظ امنیت ملی وجود دارد. برای مثال پس از حادثه ۱۱ سپتامبر در ایالات متحده آمریکا، دولت به منظور بالا بردن امنیت داخلی، قانونی موسوم به «پاتریوت» به تصویب رسانید که به واسطه آن امکان دسترسی به «رایانامه» شهروندان آمریکایی وجود داشته باشد. اگرچه می‌توان گفت، «در صورتی که منفعت عمومی حاصل از امنیت ملی بیش از منفعت حاصل از اطلاعات محرمانه باشد، اطلاعات مورد حمایت واقع نمی‌شوند» و «به طور کلی دادگاه‌ها به امنیت ملی چنان اهمیتی می‌دهند که بر اساس آن حکم به افشای اطلاعات محرمانه می‌نمایند» (استنلی، ۱۳۹۱: ۹۶).

به طور کلی ایجاد تعادل بین تضمین حریم خصوصی شهروند و امنیت ملی دولت و تشخیص این‌که کدام یک بر دیگری تقدم دارند؛ و نیز نقض حریم خصوصی را چگونه می‌توان توجیه نمود تا اندازه‌ای دشوار می‌نماید.

ماهیت سری و مخفی توطئه‌ها و فعالیت‌های بر ضد امنیت ملی در فضای سایبر نیازمند استفاده از روش‌های تخصصی تجسس برای مقابله با مجرمین است. شیوه‌های اتخاذ شده

برای مقابله، گاهی جنبه پیش‌گیرانه دارد که می‌تواند حریم خصوصی افراد را با خطر مواجه سازد. بر اساس اصل اقتضا، باید دانست که آیا این اقدامات واقعاً ضروری است و آیا معیاری غیر واکنشی و بی ضررتر، برای دستیابی به این هدف وجود ندارد؟ زیانباری این اقدام البته نباید دور از نظر قرار گیرد چرا که به هر حال تا اندازه زیادی حقوق شهروندان را تحت تأثیر قرار می‌دهد (نمامیان، ۱۳۹۰: ۹۱).

موضوع دیگر مربوط به نقض حریم خصوصی مردم توسط «شرکت‌های ارائه‌کننده خدمات اینترنتی» به‌ویژه در کشورهای دارای نظام پلکانی در ارائه این خدمات می‌باشد. این شرکت‌ها که در اصطلاح «آی.اس.پی» نامیده می‌شوند بسته به ماهیت و طبیعت دولت‌ها، یا کاملاً در انحصار بخش دولتی بوده و یا قسمتی از آن منشعب شده و در اختیار بخش خصوصی قرار می‌گیرند. شرکت‌های ارائه‌کننده خدمات اینترنتی می‌توانند به بسیاری از اطلاعات حساس و خصوصی مشتریان خود دست یابند. این شرکت‌ها حتی زمانی‌که به صورت خصوصی اداره شوند ممکن است تحت تأثیر خط مشی دولت حاکم قرار گیرند. نتیجه آن‌که بسیاری از اطلاعات خصوصی شهروندان که در اختیار این شرکت‌ها قرار دارد می‌تواند در دسترس دولت گذارده شود.

تمایل دولت‌های بسته و اقتدارگرا، بیش‌تر به سمت انحصار این بخش از فعالیت خدمت عمومی در دست دولت، به دلیل کنترل همه جانبه بر زندگی مردم است. از این‌رو احتمال مصون ماندن حریم خصوصی در فضای سایبر به دلیل نظارت همه‌گیر دولت با تردیدهای جدی روبه‌رو می‌شود (پاول، ۱۹۹۹: ۱۶۲۷). در مجموع اعمال کنترل‌های وسیع و بدون انتخاب قبلی اگرچه امروزه ابزار مفید و مؤثری برای بقاء و تداوم هیأت حاکمه بوده و در مواردی تضمین امنیت و آسایش فردی و اجتماعی شهروندان را موجب شده، اما محدود ساختن و تهدیدی علیه حقوق و آزادی‌های فردی و تعرض به حریم خصوصی را نیز به دنبال داشته است. (محسنی، ۱۳۸۹: ۵۳۵-۵۳۴).

چالش پیش روی دولت (بقاء حاکمیت یا حریم خصوصی)

دولت در هر جامعه‌ای مظهر مصلحت عمومی است و اگرچه وجوه اخلاقی، مذهبی و اقتصادی دارد اما اساساً موسسه‌ای اخلاقی، مذهبی و اقتصادی نیست بلکه کارکرد ویژه و متفاوتی دارد؛ از جمله حفظ نظم و امنیت، حراست از حقوق بنیادین افراد جامعه و غیره در برخی نظریه‌های دولت بر وجه اجبارآمیز آن تأکید شده است. از این رو برخی رئالیست‌ها و مارکسیست‌ها اساساً دولت را ابزار اجبار تلقی نموده‌اند (بشیریه، ۱۳۸۴: ۲۷).

واقع‌گرایان به خوبی دریافته‌اند که انسان در غیاب قدرت و اجبار دولتی و اجتماعی به سرکشی و تجاوز روی می‌آورد. به واسطه بهره‌مندی از وجه اقتدار که یکی از ویژگی‌ها و چهره‌های پایدار و اصلی این مؤسسه است، همواره اعمال و رفتارهای دولت در درجه اول پدیده‌ای اجبارآمیز بوده است. هر دولتی از طرفی طبق تعهدات داخلی با شهروندان خود و مطابق الزمات و التزامات بین‌المللی و حقوق بشری خود باید شرایط تحقق و حفظ حقوق بنیادین را برای شهروندانش فراهم سازد. از سوی دیگر برای بقاء و حفظ موجودیت سیاسی خود ممکن است به شدیدترین ابزارها یا همان قوه قهریه متوسل گردد. با امنیتی‌شدن افراطی جامعه، آزادی و حریم خصوصی برای مردم قابل تصور نخواهد بود اما تضمین حداقلی این دو مقوله، نیازمند به‌کارگیری سازوکارهای امنیتی خواهد بود.

بنابراین پرسش آن است که ایجاد تعادل و توازن بین این دو، چگونه میسر خواهد شد؟ به راستی یک جامعه تا کجا می‌تواند به نام امنیت، پیش رود و تا چه میزان می‌تواند آزادی را قربانی کند؟ چه مقدار دخالت در زندگی شهروندان قابل توجیه است تا ثبات و نظم اجتماعی حفظ شود؟ حفظ امنیت ملی و عدم تعرض به حریم خصوصی، هر دو از حقوق لازم و ضروری برای بقاء شهروند در یک جامعه دموکراتیک محسوب می‌شوند. مهم‌ترین مقوله در مباحث راجع به امنیت، امنیت ملت – دولت است که بر پایه دو ستون ملت و دولت استوار شده است. چون دولت از سوی مردم گزینش می‌شود و این ملت است که موضوع امنیت ملی در جهان امروز برجسته‌ترین ارزش دولت‌هاست. دولت‌های مردم‌سالار از ترس مداخله

و دست‌اندازی دولت‌های غیر مردم‌سالار، امنیت ملی را پیش می‌کشند و دولت‌های غیر مردم‌سالار، رخنه‌های نادیدنی دولت‌های مردم‌سالار در نظام حکومتی فراگیر را تهدید به شمار می‌آورند (عالی‌پور، ۱۳۸۸: ۳۳-۳۲)

در دولت‌های مردم‌سالار هر چیز خارجی، دولت را مورد هجوم قرار دهد، تهدیدی علیه امنیت کشور به شمار می‌آید، ولی دولت‌های اقتدارگرا هر تهدید اعم از داخلی و خارجی مسئله‌ای امنیتی محسوب می‌شود. در نوع اخیر از دولت، فرافکنی بین مقامات حکومتی برای سلب مسئولیت و توجیه مشروعیت امری شایع است. برای مثال حتی تحولات ناخوشایند اجتماعی از قبیل نابسامانی وضع اقتصاد و فرهنگ، بیکاری، فقر، اعتیاد، طلاق و غیره مسئله‌ای بیرونی و نشأت گرفته از دشمن و عامل بیگانه محسوب می‌شود. به بهانه حفظ امنیت کشور، آزادی‌های عمومی و حقوق بنیادین افراد دستخوش چالش‌هایی شده است. به عنوان یک نمونه ملموس و مشهور می‌توان گفت فضای رعب‌آور پس از فاجعه انسانی ۱۱ سپتامبر توجیه اساسی برای اعمال مجموعه‌ای از اقدامات کنترلی بوده که آزادی‌های مدنی را به نام امنیت داخلی، محدود و سلب کرده؛ تا جایی که عده‌ای این تحول را «حالت استثناء» تلقی کرده‌اند، اما جالب آن‌که حالت استثناء به پارادایمی عادی در دولت معاصر تبدیل شده است.

محدودیت‌های اعمال شده در خصوص آزادی‌های مدنی و گسترش رویه‌های وسیع نظارتی به طور نامتناسب، برخی گروه‌های اقلیتی نظیر اعراب و مسلمانان را هدف قرار داده است. سیاست‌های پلیسی‌گری تسامح صفر، استفاده گسترده از نظارت ویدیویی و روش‌های مختلفی که امروزه برای مبارزه با تروریسم مورد استفاده قرار می‌گیرد با هدف استقرار امنیت ملی و در نهایت حفظ منافع عمومی است که هیچ توجیهی نمی‌طلبد. فضای امنیتی پس از ۱۱ سپتامبر به عنوان کاتالیزور برای معرفی فناوری‌های جدید در سطح جهان عمل کرده و به قسمتی از زندگی روزانه شهروندان تبدیل شده‌اند. جامعه نظارتی «برادر بزرگ» که در رمان «قلعه حیوانات» *جرج اورول* در ۱۹۴۸ به تصویر کشیده شد و در آن همسایه‌ها جاسوسی یکدیگر را می‌کنند، هر صدایی شنیده می‌شود و هر حرکتی به تصویر کشیده می‌شود با

شرایط کنونی ارتباط تنگاتنگی دارد (بابایی، عباسی، ۱۳۹۰: ۱۹۳). اگر نه همه هدف دولت و نه بخش بزرگ آن از این اقدامات استقرار حفظ امنیت برای دولت و مردم باشد. در این که دولت حتی به بخش کوچکی از خواسته‌های خود دست یافته باشد، جای تردید وجود دارد. تروریست‌ها در پی ایجاد هراس و وحشت در بین شهروندان و هیأت حاکمه‌اند.

با کمی تأمل می‌توان دریافت که تروریست‌ها به راحتی به آمال و اهداف خود دست یافته‌اند. استفاده بیش از حد از روش‌های وضعی در پیش‌گیری از جرم، علاوه بر شکل‌گیری دولت پدرسالار کیفری؛ به استقرار و تداوم فضای هولناک امنیتی دامن‌زده و این همان چیزی است که تروریست‌ها در پی‌آنند. افزایش ترس از جرم به واسطه اتخاذ تدابیر مختلف پیش‌گیری وضعی واکنش‌های روانی مختلفی را به دنبال دارد. به عنوان نمونه حس بدگمانی و سوءظن نسبت به دیگران، تضعیف تعاملات فردی و اجتماعی، گوشه‌گیری و انزوا و عدم حضور در اجتماع.[1] از طرف دیگر چنان‌چه در نظارت ویدیویی توضیح داده شد؛ باید شهروندان از وجود اقدامات پیش‌گیرانه و به خصوص دوربین‌های مداربسته آگاه ساخت تا نقض حقوق اساسی آنان به حداقل ممکن کاهش یابد.

این تعارضات چگونه قابل توجیه‌اند و جمع آن‌ها چگونه امکان‌پذیر است؟ در هر حال باید این واقعیت را پذیرفت که گسترش اقدامات پیش‌گیرانه وضعی، شهرها و محله‌ها را به شکل قلعه‌های نظامی درآورده است. اگرچه این کار ممکن است تا اندازای منجر به کاهش جرم شود، لیکن بهایی که برای آن پرداخت می‌شود بسیار بالاست چنان‌چه به نظر می‌رسد ضایعات افراط در اجرای این تدابیر چیزی کم‌تر از خسارات ناشی از جرم نباشد (محمد نسل، ۱۳۸۷: ۸۰).

هزینه‌های روانی و اجتماعی ناشی از ترس از جرم از آن رو که عامل مهم و مؤثری در تغییر کیفیت زندگی محسوب می‌شود حتی از خود جرم نیز می‌تواند اهمیت بیش‌تری یابد.

---

[1]. برای توضیح بیش‌تر در این زمنیه بنگرید به: نیکوکار، حمیدرضا، همت‌پور، بهاره (۱۳۹۱)، ترس از جرم، بنیاد حقوقی میزان، صص: ۷۱-۷۴.

آثار سیاسی ترس از جرم نیز قابل تامل‌اند. همان‌طور که گفتیم حاکمیت، متولی تـأمین امنیـت جامعه و اعضای آن است. به‌ویژه در جوامع دموکراتیک یکی از مهم‌تـرین مطالبـات مـردم از این قـوا تـأمین امنیـت ملـی اسـت. احسـاس نـاامنی و تـرس مـی‌توانـد مشـروعیت / مقبولیـت حاکمیت را به مخاطره بیندازد.

نتیجه‌گیری

همان‌طور که اشاره شد حریم خصوصی شـهروندی و امنیـت ملـی هـر دو از مقولـه‌هـای مهم حقوق بشری محسوب می‌شوند. تحقق این دو، از دغدغـه‌هـای اصـلی دولـت‌هـای عصـر حاضر است. آن‌چه در این مقاله گذشت پاسخ به این پرسـش بـود کـه بـر اسـاس چـه مبنـایی دولت می‌تواند مقوله امنیت ملی را بر حریم خصوصی مقدم کند؟

دولت با داشتن قدرت، به منظور حفظ امنیت داخلی می‌تواند حـریم خصوصـی افـراد را نقض کند و این خود جنبه دموکراتیک دولت را با چالش مواجـه مـی‌سـازد. مسئله‌ای کـه در این تحلیل مطرح می‌شود فلسفه سودگرایی است؛ یعنی دولـت بـا داشـتن حـق پـیش‌گیـری از جرم، نگاهی سودانگارانه به جامعـه دارد کـه مـی‌توانـد نـوعی سوءاسـتفاده از حـق حاکمیـت تعریف شود (فریمن، ۱۳۸۷: ۹۳).

در واقع دولت نمی‌تواند به بهانه حفظ امنیـت از حـق خـود سـوء اسـتفاده کـرده، آزادی شهروندان را تحدید کند و درصدد تشکیل و استقرار یک جامعه امنیتی باشـد. از سـوی دیگـر می‌توان فرض سوءاستفاده از حق توسط مردم را مطـرح کـرد، بـدین معنـی کـه شـهروندان از حقوق خود در جهت عکس منافع‌شان گام بردارند. بر اساس این نظریه شـهروند نبایـد از حـق داشتن حریم خصوصی سوءاستفاده نماید و موجب ضـرر بـرای جامعـه شـود. ایـن فـرض نیـز متضمن چالش‌هایی است، چرا که نهاد تشخیص دهنده ضرر اصولاً دولـت و نهادهـای اقتـدار عمومی می‌باشند و همچنین معیار سوءاسـتفاده از حـق، ضـرر مـی‌باشـد کـه بـاز هـم مفهـومی موسع، چند وجهی و قابل تفسـیر اسـت. تحلیـل دیگـر آن اسـت کـه هرگـاه عمـل فـرد جنبـه عمومی پیدا کند یعنی آثار رفتاری فرد اثر اجتماعی بر جـای گـذارد و یـا عمومیـت عمـل بـه

اقتضای ذات و ماهیت عمل باشد حق فردی به معنای حفظ حریم خصوصی نمی‌تواند بر حقوق جمعی ترجیح داده شود. به این معنا که هرگاه فرد با رفتار و عمل خویش حریم خود را بشکند و این شکسته شدن باعث جریحه‌دار شدن حوزه عمومی شود؛ دولت عدالت‌گرا و مردم‌سالار در این صورت به عنوان وظیفه و با استفاده از ساز و کار خود به عنوان پیش‌گیری از هرگونه جرمی به میدان آید. آن‌چه که بر اساس تحلیل آخر مورد توجه است از دو نظر مزیت پیدا می‌کند، از یک طرف، از اقدام خودسرانه دولت برای شکست حریم خصوصی افراد جلوگیری می‌شود؛ چرا که تنها آن‌جایی دولت حق ورود به حریم خصوصی را پیدا می‌کند که رفتار فرد جنبه عمومی داشته باشد و از طرفی شهروندان جامعه می‌دانند تا آن‌جا که اعمال و رفتارشان موجب اثرات منفی اجتماعی نشود، حریم خصوصی‌شان حفظ می‌شود. از نقطه نظر حقوقی، حقوق بشر می‌تواند به عنوان مجموعه‌ای از حقوق فردی و جمعی که توسط دولت‌ها به رسمیت شناخته شده و در قوانین اساسی و حقوق بین‌الملل مندرج است؛ تعریف شود. از یک نظرگاه مهم برای تحقق این مجموعه مهم نمی‌توان اصالت و اولویت به حریم خصوصی را به اندازه امنیت ملی مقوله‌ای مهم تلقی کرد. بنابراین نمی‌توان راه افراط و تفریط پیمود و یکی را فدای دیگری کرد. استفاده دولت از حق خود برای حفظ امنیت خویش نمی‌تواند به بهای نقض فراگیر حریم خصوصی تمام شود مگر با دلایل و توجیهات ویژه؛ و افراد نیز نمی‌توانند به دلیل داشتن خلوت و حق حریم خصوصی درصدد تخریب وجود امنیتی حاکمیت بر آیند. مسلماً در چنین شرایطی دولت از وجوه اجبار و اقتدار خود برای ورود به حریم خصوصی در جهت بقاء خود استفاده خواهد کرد.

فهرست منابع

- ۱.ابراهیمی، شهرام (۱۳۸۷)، **پیشگیری از جرم در چالش با موازین حقوق بشر**، پایان‌نامه دکتری حقوق کیفری و جرم‌شناسی، دانشگاه تهران، خرداد.
- ۲. ابراهیمی، شهرام (۱۳۹۰)، **جرم‌شناسی پیشگیری**، جلد اول، بنیاد حقوقی میزان، چاپ اول.
- ۳. اصلانی، حمیدرضا (۱۳۸۹)، **حقوق فناوری اطلاعات**، بنیاد حقوقی میزان، چاپ دوم.
- ۴. گیدنز، آنتونی، **جامعه‌شناسی**، ترجمه حسن چاوشیان (۱۳۹۰)، نشر نی، چاپ چهارم.
- ۵. انصاری، باقر (۱۳۸۳)، حریم خصوصی در رسانه‌های همگانی، **پژوهش و سنجش**، شماره ۳۹ و ۴۰، پاییز و زمستان.
- ۶. انصاری، باقر (۱۳۸۶)، **حقوق حریم خصوصی**، سمت، چاپ اول، زمستان.
- ۷. فرانکوآس، کاتیا، **جهانی‌سازی و جرم**، ترجمه یوسف بابایی و اصلی عباسی (۱۳۹۰)، مجد، چاپ اول.
- ۸. بشیریه، حسین (۱۳۸۴)، **آموزش دانش سیاسی (مبانی علم سیاست نظریه و تأسیسی)**، نگاه معاصر، چاپ چهارم.
- ۹. بکاریا، سزار، **رساله جرایم و مجازات‌ها**، ترجمه محمدعلی اردبیلی (۱۳۸۹)، بنیاد حقوقی میزان، چاپ ششم.
- ۱۰. بهرامی احمدی، حمید (۱۳۷۷)، **سوء استفاده از حق**، نشر اطلاعات، چاپ سوم.
- ۱۱. بوزان، باری، **مردم، دولت‌ها و هراس**، ترجمه پژوهشکده مطالعات راهبردی (۱۳۷۸)، پژوهشکده مطالعات راهبردی، چاپ اول.
- ۱۲. استنلی، پائول، **حقوق حفظ اسرار**، ترجمه محمدحسین وکیلی‌مقدم (۱۳۹۱)، کتاب همگان، چاپ اول.
- ۱۳. پاک نهاد، امیر (۱۳۸۸)، **سیاست جنایی ریسک‌مدار**، بنیاد حقوقی میزان، چاپ اول، پاییز.
- ۱۴. تدین، عباس (۱۳۸۸)، **تحصیل دلیل در آئین دادرسی کیفری**، بنیاد حقوقی میزان، چاپ اول.
- ۱۵. خانعلی پور واجارگاه، سکینه (۱۳۹۰)، **پیشگیری فنی از جرم**، بنیاد حقوقی میزان، چاپ اول.
- ۱۶. دادستان، پریرخ (۱۳۸۵)، **روانشناسی جنایی**، نشر سمت، چاپ سوم، پاییز.
- ۱۷. رئیسی، اندیشه (۱۳۹۰)، **سیاست جنایی ایران در قبال جرایم ارتکابی در حریم خصوصی**، پایان‌نامه کارشناسی ارشد دانشگاه آزاد اسلامی واحد نراق.
- ۱۸. رحمدل، منصور (۱۳۸۴)، حق انسان بر حریم خصوصی، **مجله دانشکده حقوق و علوم سیاسی**، شماره ۷۰، زمستان.
- ۱۹. صفاری، علی (۱۳۸۰)، مبانی نظری پیشگیری از وقوع جرم، **تحقیقات حقوقی**، شماره ۳۳-۳۴، بهار تا زمستان.
- ۲۰. عالی‌پور، حسن (۱۳۸۸)، **جرایم بر ضد امنیت ملی**، نشر خرسندی، چاپ اول.
- ۲۱. عباسی، بیژن (۱۳۹۰)، **حقوق بشر و آزادی‌های بنیادین**، نشر دادگستر، چاپ اول.
- ۲۲. کاشفی اسماعیل‌زاده، حسن (۱۳۸۴)، جنبش‌های بازگشت به کیفر در سیاست جنایی کشورهای غربی، علل و جلوه‌ها، **مجله تخصصی الهیات و حقوق**، شماره ۱۵ و ۱۶، بهار و تابستان.

- ۲۳. پیز، کن، جایگاه پیشگیری نخستین از جرم در انگلستان، ترجمه مهدی صبوری پور (۱۳۸۳)، **مجله حقوقی دادگستری**، سال ۶۸، دوره جدید، تابستان.
- ۲۴. گسن، ریموند، **جرم‌شناسی کاربردی**، ترجمه مهدی کی نیا (۱۳۷۰)، نشر مترجم، چاپ اول.
- ۲۵. فریمن، مایکل، **حقوق بشر**، ترجمه محمد کیوانفر (۱۳۸۷)، نشر هرمس، چاپ اول.
- ۲۶. مجتهدی، محمدرضا (۱۳۸۸)، **حقوق تأمین اجتماعی**، نشر آیدین، چاپ اول.
- ۲۷. مجیدی، سیدمحمود (۱۳۸۶)، **جرایم علیه امنیت**، بنیاد حقوقی میزان، چاپ اول، بهار.
- ۲۸. محسنی، فرید (۱۳۸۹)، **حریم خصوصی اطلاعات**، نشر دانشگاه امام صادق، چاپ اول.
- ۲۹. محمد نسل، غلامرضا (۱۳۸۷)، **پلیس و سیاست پیشگیری از جرم**، نشر دفتر تحقیقات کاربردی پلیس پیشگیری از جرم ناجا، چاپ اول.
- ۳۱. معتمدنژاد، کاظم (۱۳۸۹)، **جامعه اطلاعاتی**، نشر میراث قلم، چاپ دوم.
- ۳۲. کوسن، موریس، نظارت ویدیویی، دلایل موفقیت و شکست، ترجمه شهرام ابراهیمی (۱۳۸۴)، **مجله الهیات و حقوق**، بهار و تابستان.
- ۳۳. نمامیان، پیمان (۱۳۹۰)، **واکنش‌های عدالت کیفری به تروریسم**، بنیاد حقوقی میزان، چاپ اول.
- ۳۴. نیازپور، امیرحسن (۱۳۸۳)، پیشگیری از بزه‌کاری در قانون اساسی ایران و لایحه پیشگیری از وقوع جرم، **مجله حقوقی دادگستری**، شماره ۴۵، زمستان.

- 35. AHMAD KAMAL (2005), The law of gyber-space, published by the United Nations Institute for Training and Research Palais des Nations CH1211, Geneva 10, Switzerland,.
- 36. Majesty, Her (2010), Cyber Crime Strategy, Presented to Parliament by the Secretary of state for the home Department, March.
- 37. solbe, Daniel (2008), Understanding privacy, Harvard University Press, londen, England.
- 38. Sjaak, Nouwt (2008), Reasonable Expectations of Geo-Privacy?, Volume 5, Issue 2, August.
- 39. Nieto, Marcus (1997), Public video surveillance: is it an effective crime prevention tool?, California Research Bureau, California state library,.
- 40. Connor, Sean. O. (2002), Biomerics and Identification ofter 11/9, university of Washington School of law, quoted, , in www.ssrn.com.
- 41. Schwartz, Paul. M. (1999), Privacy and Democracy in Cyberspace, Vnderibil Law Review, VOL. 52.
- 42. Clark, Ronald. V. (1997), Situational Crime Prevention, Successful Case Studies, Harrow and Heston, Second Edition,.
- 43. www.biometrics.gov/docs/privacy/pdf.
- 44. www.estig.ipbeja.pt/~_direito/privacy.pdf
- 45. www.legal-dictionary.thefreedictionary.com/privacy.
- 46. www.parlia,emt.uk/parliamentary-offices/post/pubs2006.cfm.
- 47.www.privacynetwork.info.