**تقابل گونه­های تمامیت خواه پیشگیری از جرم با حریم خصوصی شهروندی**

محمد شمعی

**چکیده**

مقوله **امنیت ملی** و تلاش برای تحقق همه جانبه آن در یک جامعه از اصلی ترین مباحث در هر نظام سیاسی می­باشد. تحقق این مهم در مواردی با اعمال مجازات نسبت به مرتکبین و در مواردی با اتخاذ سیاست پیشگیری از جرم شکل می گیرد. اما پیش گیری از وقوع جرم به منظور تحقق امنیت ملی و توجه به اقدامات پیش دستانه **در مواردی** باعث تقابل گونه های تمامیت خواه پیشگیری از جرم با حریم خصوصی شده است. سوالی که نگارنده در پی پاسخ به آن می­­باشند، آن است که در تعارض بین پیشگیری از وقوع جرم به منظور تحقق **امنیت ملی** و حریم خصوصی کدام یک مقدم می شود؟ ادعای این نوشتار آن است که توجه به حوزه عمومی در کنار حفظ حریم خصوصی با محوریت دولت مرد سالار می­تواند پاسخی به این سوال باشد . روش این تحقیق توصیفی، تحلیلی می باشد.

*واژگان کلیدی:پیشگری، امنیت، حریم خصوصی، حوزه عمومی، دولت مرد سالار*

**مقدمه**

همه تدابیر جامعه در برابر جرم محدود به پاسخ های واکنشی نیست و بخشی از آن جنبه کنشی دارد.جامعه همیشه منتظر نمی ماند تا جرم اتفاق افتد و پس از آن با ابزار «سیاست کیفری»[[1]](#footnote-1) به چاره اندیشی پیرامون مجازات بپردازد،بلکه گاهی با توسل به «سیاست جنایی»[[2]](#footnote-2) با اتخاذ تدابیر پیشگیرانه به مقابله با جرم برمی خیزد(کن، 1383، ص123). بنابراین می توان گفت از مهمترین اهداف سیاست جنایی موثر« پیشگیری»[[3]](#footnote-3) از وقوع جرم است .

سزار بکاریا نخستین کسی است که پیشنهاد می کند برای کاهش میزان جرایم (جرم زدایی) به جای کیفر و مجازات بزه کاران 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 موثر پیشگیری از وقوع جرم است. (بکاریا، 1389، ص132) پس از او انریکو فری به بکار بردن اصطلاح «جانشین های کیفری » برای دستیابی به این هدف نظر داشت (بکاریا، پیشین، ص15). پیشگیری از وقوع جرم در مدل های مختلفی تقسیم بندی شده است که تنها به دلیل ضرورت به طور مختصر به آن اشاره می شود.در یک تقسیم پیشگیری به «اولیه»[[4]](#footnote-4)،«ثانویه» [[5]](#footnote-5)و «مرحله سوم»[[6]](#footnote-6) تقسیم بندی شده است. این مدل از پیشگیری منتسب به «برانتینگهام و فاوست» [[7]](#footnote-7) و ماخوذ و ملهم از پیشگیری و درمان بیماریهای همه گیر در علوم پزشکی است که در آن از یک سیاست سه مرحله ای سخن می گویند. 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 اقدام هایی است که در مورد یک گروه خاص یا یک گروه در معرض خطر یعنی گروهی که احتمال بروز خطر در آنها زیاد است انجام می شود.هدف این نوع از پیشگیری جلوگیری از وخیم یا مزمن شدن یک اختلال در حال گسترش است (دادستان، 1385، ص286). سطح سوم به واگیری مجدد بیماران درمان شده و مصون سازی آنها در مقابل بیماری دوباره مربوط می شود(محمد نسل، 1387، ص42).

مدل دیگر، تقسیم پیشگیری به پیشگیری «وضعی»[[8]](#footnote-8) و «اجتماعی یا اصلاحی»[[9]](#footnote-9) است. پيشگيري وضعي از وقوع جرم به شدت از جرم شناسي­اي كه در آن جهت گيري خاصي باشد اجتناب مي كند. به كارگيري اين شيوه از پيشگيري و تحليل هاي موجود در آن در انواع جرايم، مستلزم استفاده از ابزار هاي خاص مديريتي و تغييرات محيطي براي تقليل فرصتهاي ارتكاب جرم توسط مجرمين بالقوه مي باشد که بر مال انديشي از ارتكاب وقوع بزه تا شناسايي و كشف جرم و مجازات مجرمان تاكيد مي كند.اين روش اگرچه منتهي به حذف تمايلات منحرفانه و مجرمانه براي بهبود ساختارها و وضع اجتماع نمي شود اما همين بس كه موجب شيفتگي و گرايش كمتر مجرمان به ارتكاب اعمال جنايي مي گردد.تمركز و توجه در به كارگيري پيشگيري وضعي با نظام عدالت كيفري نيست اما هر روزه طيف وسيعي از سازمانهاي عمومي و خصوصي و نهاد ها،مدارس،بيمارستان ها،سيستم هاي حمل و نقل،فروشگاه ها و مراكز خريد،مشاغل توليدي،كمپاني ها،پارك هاي محلي،تفريح گاه ها،پاركينگ ها در معرض برخورد با انواع جرايم قرار دارند كه خواه ناخواه آنها را متمايل به استفاده از انواع روش پيشگيري وضعي مي نمايد(Clarke, 1997, p2). به طور خلاصه اين شيوه شامل مديريت،طراحي،كنترل با مهارت و تحت كنترل درآوردن سيستماتيك و پايدار محيط مي باشد كه به واسطه آن ارتكاب جرايم دشوار تر و با خطر بيشتري همراه است و منافع حاصله از ارتكاب جرم را آنگونه كه نزد مرتكبين نمود مي يابد كاهش مي دهد(Ibid, p4) . در مدل اجتماعی از پیشگیری از جرم بر شخصیت و منش فرد تاکید می شود تا تغییر در محیط. طرفدران اين رويكرد از پيشگيري كه به «پوزيتيويست يا تحققي»[[10]](#footnote-10) معروف اند مدعي خشكاندن ريشه هاي جرم از طريق شناسايي علل وقوع جرم و انجام اصلاحات فردي و اجتماعي مي باشند.بنابراين مرتكبين جرم افرادي متفاوت از ديگران به لحاظ ويژه گيهاي فردي و اجتماعي تلقي مي شوند و همه داراي نوعي اجبار در ارتكاب بزه مي باشند كه خطرناك ترين يا مجبورترين آنها مجرمين مادرزاد يا بالفطره هستند(صفاری، 1380، ص279) . در اين ميان براي دستيابي به آماج پيشگيرانه، حقوق كيفري به صورت ميان رشته اي با علوم حائل مانند روانشانسي و جامعه شناسي مرتبط مي شود. براي مثال در بعد اصلاحات فردي، پيشگيري اجتماعي از وقوع بزه متاثر از يافته هاي روانشناسي است و اصلاحات اجتماعي از وظايف جامعه شناسان مي باشد. بنابراين مي توان با اصلاح شخصيت مجرم و تغيير در زير ساختهاي موجود اجتماعي به هدف نهايي يعني پيشگيري از وقوع جرم دست يافت. پیشگیری وضعی و اجتماعی از جرم ممکن است نقض حریم خصوصی مردم را به دنبال داشته باشند.اما تغییرات اعمال شده در محیط یا استفاده از روش های وضعی پیشگیری، به دلیل تنوع و گستره کاربرد آن در اماکن گوناگون به ظاهر ارتباط بیشتری با حریم خصوصی دارد از این در این نوشتار تنها نقض حریم خصوصی به واسطه تقابل با سازوکارهای پیشگیری وضعی مورد تحلیل و ارزیابی قرار گرفته اند.پیش از آن تاملی در مفهوم حریم خصوصی خواهیم داشت.

**تاملی در مفهوم حریم خصوصی**

از دیدگاه بسیاری از اندیشمندان برای شناخت حریم خصوصی از همان ابتدا با یک ژولیدگی و بی نظمی مفهومی روبرو می شویم.اندیشمدانی مانند «ویلیام بی نی»[[11]](#footnote-11)،«تام گرتی»[[12]](#footnote-12)،«آرتور میلر»[[13]](#footnote-13)،«دنیل سولو»[[14]](#footnote-14) و دیگران در آثار خود به این مهم اشاره کرده اند(انصاری، 1386، ص12). «بی نی» مشکلات حریم خصوصی را از جهت تعریف به ذات و قلمرو آن مربوط می سازد،«میلر» دشواری تعریف را در ابهام و شکنندگی آن می داند و از دیدگاه «گرتی» حریم خصوصی مفهومی متلون و متغیر است.از نظرگاه «سولو» جامع ترین و باارزش ترین 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 می گردد آسودگی ذهن و آرامش فیزیکی است.وی در کتاب خود تحت عنوان «فهم حریم خصوصی»[[15]](#footnote-15) باور دارد که هیچ کس نمی تواند معنی حریم خصوصی را به صورت شمرده بیان دارد چرا که مفهومی سیال و در جریان است(solv, 2008, p1). «حریم خصوصی»[[16]](#footnote-16) به عنوان یک مفهوم هم پوشان، حوزه های مختلف مجزایی از مطالعه و موقعیت های رویه ای را در بر می گیرد..حریم خصوصی معنایی فراتر از «خصوصی»[[17]](#footnote-17) دارد و محدود به حفاظت از یک «امر نهان»[[18]](#footnote-18) نمی شود.این مقوله مدعی پوشش دادن به اطلاعات و فعالیت هایی است که اشخاص با آن هر روزه درگیراند.برای مثال اعتبار بانکی افراد،تجویز دارو توسط پزشک یا دارو ساز و... همچنین گفته شده که حریم خصوصی مشمول موقعیت فیزیکی افراد (مانند خانه و محل کار) و اطلاعات (مانند ارزش خانه و میزان دستمزد) نیز می شود. اجتماعیون بر حوزه های خاصی موازی مفهوم حریم خصوصی که در طول زمان دچار تغییر شده اند تاکید دارند.برای مثال «رابرت اسمیت»[[19]](#footnote-19) معتقد است که حریم خصوصی فضای فیزیکی ما را به دور از هر گونه گسست،مداخله خوسرانه،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 برداشت های متفاوت از این مفهوم اما ترجیع بند و وجه اشتراک همگی در یک چیز یعنی «فرد انسانی» می باشد.در یک مفهوم موسع حریم خصوصی شامل پنج حوزه می گردد:

**1-حوزه تصمیمی[[20]](#footnote-20):** این مفهوم از حریم خصوصی موضوعات مرتبط با صلاحیت شخصی نظیر تصمیم گیری در حوزه زندگی شخصی و بدن را شامل می شود و همچنین مسائل شخصی مرتبط با خانواده.

**2-حوزه فضایی[[21]](#footnote-21):** مسائلی مانند خانه،اتاق خواب و... و در واقع فضای فیزیکی به این حوزه مرتبط اند.اینکه چه اشخاصی می توانند به این حوزه وارد شوند یا آن را ببینند از جمله مسائلی است که بر روی آن تمرکز می شود.

**3-حوزه قصدی[[22]](#footnote-22):** در این بخش حریم خصوصی با فعالیتهای محرمانه یا منشی و نهادین افراد که به طور عموم قابل رویت هستند باز می گردد.تمرکز این حوزه معمولا به توانایی اشخاص در مانع شدن دیگران برای دسترسی به ارتباطاتشان در حال یا آینده بازمی گردد.

 **4-حوزه اطلاعاتی[[23]](#footnote-23):** در این از مفهوم حریم خصوصی در مورد به کارگیری اطلاعات افراد گفتگو می شود.توانایی اشخاص در چگونگی به کارگیری اطلاعات خود (برای چه کسی و چه اهدافی) و پاسخگویی آنها در ارتباط با دیگر اشخاص از موضوعات مربوط به حوزه اطلاعاتی حریم خصوصی است.

**5-حوزه ارتباطی[[24]](#footnote-24):** 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، 1389، ص28).

حریم خصوصی نیز از جمله مفاهیمی است که نسبیت در مورد آن مطرح می شود،چرا که با فرهنگ،اقتصاد،نوع رژیم سیاسی حاکم بر آن کشور مرتبط است لذا می توان گفت حریم خصوصی امری نسبی است که مفهوم آن از کشوری به کشور دیگر ممکن است متفاوت باشد (رحمدل،1384، ص129). در مجموع برای ارائه یک تعریف جامع از حریم خصوصی باید به مقوله های زیر توجه داشت:

1. نگرانی ها و مصلحت های حریم خصوصی باشد شناسایی شوند؛
2. اصول اساسی که قلمرو کلی از حمایت از حریم خصوصی را بیان می کنند باید مد نظر قرار گیرند؛
3. تخمین زود هنگام از نگرانی های حریم خصوصی به هنگام توسعه سیستم ها و فناوری اطلاعات باید وجود داشته باشد؛
4. قبول و یکپارچه نمودن فناوری های افزایش دهنده حریم خصوصی؛

به لحاظ تاریخی منشا پیدایش حق بر حریم خصوصی به قرن 19 میلادی باز می گردد.در سال 1980 «ساموئل دی وارن»[[25]](#footnote-25) و «لوییس دی براندیز»[[26]](#footnote-26) در اثر خود را با نام «حق بر حریم خصوصی»[[27]](#footnote-27) حق مزبور را به عنوان یکی از اسباب موثر و ضروری زندگی انسان در حقوق کامن لاو بدیهی تلقی کردند. **(www.estig.ipbeja.pt/~ac\_direito/privacy)** پیش از انتشار این مقاله هیچ یک از محاکم آمریکا این مقوله را به صورت صریح به عنوان یک حق قانونی مورد شناسایی قرار نداده بودند اما پس از آن دادگاه ها در سطوح و حوزه های گوناگون این حق را مورد پذیرش قرار دادند**.( http://legal-dictionary.thefreedictionary.com/privacy)** در نیمه نخست قرن بیستم به نظر می رسد برای اولین بار محققین آمریکایی «حریم خصوصی فیزیکی»[[28]](#footnote-28) را مطرح کردند.اما در نیمه دوم این قرن این قرن مفهوم دیگری از حریم خصوصی به نام «حریم خصوصی اطلاعات»[[29]](#footnote-29) توسط آمریکایی ها مورد کنکاش واقع شد. حریم خصوصی در سراسر جهان و در رژیم ها و فرهنگ های گوناگون امری شناخته شده است.از حیث بین المللی و حقوق بشری نیز اسناد جهانی و منطقه ای بر این حق مستقل حقوق بشری صحه گذارده اند.ماده 12 اعلامیه جهانی حقوق بشر،مواد 10 و 17 میثاق بین المللی حقوق مدنی و سیاسی،ماده 8 کنوانسیون اروپایی حقوق بشر،ماده 7 منشور حقوق بنیادین اتحادیه اروپا و ماده 18 اعلامیه اسلامی حقوق بشر از آن نمونه اند (عباسی، 1390، ص109). **اخیرا بسیاری از کشورها این مفهوم را در قوانین اساسی شان درج کرده اند و در دیگر کشورهایی که این حق در قوانین اساسی رسیمت نیافته،دادگاه ها حمایت از آن را به عنوان یک حق پایه ای مورد قبول قرار داده اند.(kamal,2005,p29)**

**تقابل گونه های تمامیت خواه پیشگیری از جرم با حریم خصوصی**

چنانچه در مقدمه بحث اشاره شد گونه هایی مختلف پیشگیری از جرم از سوی جرم شناسان مطرح شده است.در این بین، استفاده از شیوه پیشگرانه وضعی و اجتماعی بیش از سایر تقسیم بندی ها ،با استقبال مواجه شده ،چنانکه بسیاری از نوشته های جرم شناسان فرانسوی و آمریکای شمالی راجع به بحث در خصوص این روش هاست.در این نوشته تاکید نگارندگان بر تبیین روش های نوین وضعی پیشگیری در تقابل با حریم خصوصی شهروندان است.در صورتی که شیوه های جدید پیشگیری وضعی بدون توجیه و به صورت افراطی توسط هیات حاکم به کار گرفته شوند ،با حوزه هایی مهم از حریم خصوصی نظیر حوزه فضایی،اطلاعاتی و ارتباطی تداخل پیدا می کنند.

دیدگاه های تمامیت گرا در پیشگیری از جرم به شیوه های جدید آن نیز تسری یافته است.به لحاظ تاریخی بینش فراگیر یا تمامیت خواه از مقوله پیشگیری از جرم که در اندیشه سیاست جنایی انریکو فری مطرح و پس از آن در جنبش دفاع اجتماعی و در نوشته های برخی از جرم شناسان معاصر دنبال شد. در این زمان «جرم مداری» در نظام کیفری جای خود را به «مجرم مداری» داد به گونه ای که بسیاری این واقعیت را دریافتند که محدودیت های اعمال عدالت کیفری سنتی حکایت از آن دارد که رویکردی فراواکنشی یعنی توسل به ابزارهای پیشگیرانه باید جایگزین روش های دیرین گردد (نیازپور، 1383، ص125). اما به دنبال افزایش «جرایم خرد»[[30]](#footnote-30) و اعمال سیاست های مبتنی بر «تسامح صفر»[[31]](#footnote-31) که ریشه در تئوری جامعه شناختی«پنجره های شکسته»[[32]](#footnote-32) در آمریکا داشت ، مفهوم موسع از پیشگیری از جرم نیز با استقبال فراوانی روبرو شد.پیشگیری در مورد همه چیز،پیشگیری برای همه افراد و در نهایت پیشگیری توسط همه از آثار و نتایج اصل «هر امر پیشگیری است» خواهد بود.در این فرض همه اقدامات هیات حاکمه با توجیه پیشگیری از جرم مواجه اند و تمام اقشار و سطوح جامعه علاوه بر آنکه آماج تدابیر پیشگیرانه واقع می شوند خود وظیفه پیشگیری از جرم را عهده دار می باشند (ابراهیمی، 1387، ص53). این معضلی است که علاوه بر دولت های توتالیتر(جمع گرا) و اقتدارگرا به آفت نظام های لیبرال دموکراسی نیز بدل شده است.نوع تشکیلات پلیسی دولتهای توتالیتر که در همه امور مردم به شکل گسترده دخالت می کنند و یا دارای قدرت های مستقل پلیسی می باشند اصولا گویای حضور حداکثری دولت است درحالی که دولت حداقلی نباید نیازمند نیروی عظیم پلیسی باشد و وجود چنین نیرویی در سطح وسیع حکایت از فاصله بین دولت و مردم دارد(بوزان، 1387، ص59و57).کنترل وسیع حوزه های مختلف ارتباطی نظیر موبایل،ایمیل،فکس و تلفن،استفاده از روش های «بیومتریک»[[33]](#footnote-33) نظیر چهره نگاری یا تشخیص صورت[[34]](#footnote-34)،تصویر برداری از عنبیه[[35]](#footnote-35) و رنگ چشم،انگشت نگاری[[36]](#footnote-36)،دست نگاری،[[37]](#footnote-37) ،تشخیص صدا ، به کارگیری نیروهای امنیتی و پلیسی در سطح شهرها،موازی سازی برای تشکیل سازمانهای اطلاعاتی و امنیتی و... بیش از هر چیز زنگ خطری برای تشکیل یک حکومت امنیتی و حرکت به سوی دژواره شدن جامعه محسوب می شود.

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 می گردد.توسعه نظام تامین اجتماعی و بیمه های اجباری و همگانی با انتشار گزارش بوریج در 1942 میلادی و پس از آن تصویب اسناد بین المللی وانعقاد معاهدات عام و خاص بین المللی ادامه یافت (مجتهدی، 1388، ص67). اما تحولات منطقه ای و جهانی منجر به تعدیل و کاهش حاکمیت و گسترش فقر و بی عدالتی و طرح دولت پدرسالار با هدف مسئول ساز ،آگاه سازی و آموزش افراد جامعه و بزه دیدگان بالقوه در زمینه بزهکاری،توسعه فرآیند امنیت خصوصی،نصب دوربین های مراقبتی در معابر و امکان عمومی و خصوصی،هشدار دهنده های ضد سرقت،کارتهای اعتباری و... شده است (کاشفی، 1384، ص272). کنترل های شدید امنیتی ما را با این واقعیت وحشتناک روبرو کرده است که اندیشیدن درباره اینکه فناوری همیشه به عنوان یک راهکار باقی می ماند و به مشکل تبدیل نمی شود اشتباه است.هدایای بزرگ هزینه های سنگین به دنبال دارند.معمولا خطرها زمانی به فاجعه تبدیل می شوند که ظرافت زیاد و شکنندگی نهادهای دموکراسی،از جمله عدالت کیفری و اجتماعی را فراموش کنیم.از رو رو برخی از نسل چهارم حقوق بشر سخن به میان آورده اند که می خواهد از کرامت انسانی،زندگی خصوصی و آزادیهای فردی و اجتماعی در برابر سوء استفاده های علمی حمایت کند. توسعه تشکیلات امنیتی و نیروهای پلیس از واکنش هایی است که در برابر جرم و جنایت صورت گرفته است.حکومت هایی که مایل اند خود را در برابر جرم و جنایت قاطع نشان دهند معمولا از افزایش تعداد و امکانات پلیس برای پیشگیری از جرم طرفداری می کنند.دیدگاه عمومی در این باره این است که پلیس سنگ بنای حفظ نظم و قانون می باشد اما طبق برخی از آمارهای رسمی نه تنها این ایده تحقق پیدا نکرده که موجب افزایش هراس در بین شهروندان نیز شده است.از این رو یکی از اندیشه هایی که در سالهای اخیر محبوبیت زیادی پیدا کرده آن است که پلیس باید دوشادوش شهروندان برای بهبود کیفیت اجتماع و رفتار مدنی تلاش کند و در این راه به جای زندانی کردن،از آموزش،ترغیب،متقاعد سازی و مشاوره استفاده کند (گیدنز، 1390، ص326-322). مهمترین ایراد وارده بر مقوله پیشگیری وضعی از جرم از حیث حقوق بشری آن است که این مدل از پیشگیری در شکل حداقلی خود موجب محدود سازی افراد می شود.تکیه بر پیشگیری وضعی،منجر به ایجاد یک جامعه فوق امنیتی و دژمانند، تعدی به حریم خصوصی شهروندان و سلب آزادیهای فردی می شود.تاکید بر روش های پیشگیرانه وضعی جامعه را تبدیل به یک قلعه نظامی می کند که در آن همه چیز توسط همه کس مورد نظارت و کنترل واقع می شود.بدین ترتیب استفاده از روش های پیشگیری وضعی به جای ایجاد احساس امنیت،خود عامل مولد ترس در شهروندان می شود (پاک نهاد، 1388، 265-264).

«فیلیپ کئو» مدیر اسبق جامعه اطلاعاتی یونسکو نکاتی تکان دهنده را در حمایت از حریم خصوصی گوشزد کرده است. وی حرمت زندگی خصوصی اشخاص را یکی از مهمترین مسائل حقوق بشر در هزاره سوم می داند و یادآور شده است که «برادران بزرگ»[[38]](#footnote-38) هر حرکت انسان ها را برای حفظ برتری استراتژیک خود زیر نظر دارند. وی می­گوید ایالات متحده آمریکا با همکاری کانادا،استرالیا،انگلستان و نیوزلند از شبکه های اطلاعاتی که در اختیار دارند با شنود،کنترل و پردازش اطلاعات روزانه بیش از 3 میلیارد پیام تلفنی،دورنگار،و پست الکترونیکی در سراسر دنیا استفاده می کنند و هر گونه حرکت و فعالیت افراد در خانه،محل کار و فراغت و بیمارستان را تحت کنترل دارند (معتمد نژاد، 1389، ص333-332).

در این بین حقوق کیفری نیز امروزه صبغه و ماهیتی سخت گیرانه و امنیتی یافته است. گسترش دامنه جرم انگاری و تشدید ضمانت اجراء،توسعه جرم انگاری به رفتارهای غیر عمدی،جرم انگاری مقدمات جرم،تصویب قوانین برای پیشگیری و مقابله با بزه های امنیتی و تروریستی در حداقل زمان ممکن در مرحله وضع قانون بحث حقوق کیفری امنیت مدار را در برخی از کشورها نظیر آمریکا و فرانسه مطرح ساخته است.(مجیدی، 1386، ص77).

**حریم جفرافیایی یا مکانی[[39]](#footnote-39)**

نقش تکنولوژی برای توسعه «سرویس های مبتنی برتعیین محل»[[40]](#footnote-40) به وسیله دولت ها،در رابطه با مفهوم حریم خصوصی در این بخش مقاله مورد بررسی قرار می گیرد.مسئله اصلی آن است که «انتظار مشروع»[[41]](#footnote-41) از حریم خصوصی مفهوم شایسته و مناسبی برای حمایت از آن در برابر قدرت دولت می باشد.استفاده از سازوکارهای جدید تکنولوِژی، جمع آوری و ثبت اطلاعات مربوط به موقعیت جغرافیایی افراد را آسان کرده است. «اطلاعات جغرافیایی»[[42]](#footnote-42) گونه هایی مختلف از اطلاعات می باشند که ممکن است مورد پوشش قرار گیرند.در این خصوص تمرکز ما می تواند بر روی «داده های جغرافیایی»[[43]](#footnote-43)،«داده های محلی»[[44]](#footnote-44) و «داده های متحرک - پویا»[[45]](#footnote-45) باشند.با در دست داشتن اطلاعات مکانی افراد،دولتها قادر به توسعه سرویس های تعیین محل شهروندان می شوند،سرویس هایی که مجهز به ذخیره سازی اطلاعات مربوط به حریم خصوصی افراد می باشند. (*Sjaak,2008, ,p397*) استفاده از سامانه هایی نظیر «جی-آی-اس»[[46]](#footnote-46) و «جی-پی-اس»[[47]](#footnote-47) یکی از کاربردی ترین ابزارها در راستای سطح ایمنی شهروندان است و قابلیت های فراوان این سامانه باعث شده که در بسیاری از موضوع ها از آن مدد بگیرند.(واجارگاه،1390،ص 55)

در بسیاری از موارد شهروندان ازثبت اطلاعات مربوط توسط سرویس های تعیین محل را تهدید علیه حریم خصوصی خود تلقی کرده اند.برای مثال وفق پژوهشی که در بین سالهای 2002 تا 2007 توسط یکی از سرویس های داخلی [[48]](#footnote-48)در کشور آلمان انجام شده نشان می دهد که 39 درصد مردم این کشور حریم خصوصی را بنیادی ترین حق بشری خود قلمداد کرده اند.از میان 11 گزینه پیش رو در این نظر سنجی از منظر شرکت کنندگان 2 مورد یعنی دوربین های مراقب در مکان های عمومی و همچنین تعیین هویت الزامی برای شهروندان 12 سال به بالا به عنوان تهدیدهای کوچک علیه حریم خصوصی شهروندان اعلام شده است.اما 9 مورد دیگر تهدیدهای جدی و خطرناک در راستای نقض حریم خصوصی اعلام شده اند.این موارد عبارتند از:

1-انتقال اطلاعات مسافرین توسط سرویس های هواپیمایی به کشور مقصد

2-ردیابی و ثبت موقعیت جغرافیایی افراد به وسیله «پویشگرهای خودکار»[[49]](#footnote-49)

3-انجام عمومی آزمایش DNA

4-تجسس های پشگیرانه توسط دولت

5-ردیابی و ثبت موقعیت جغرافیایی افراد به واسطه مخابره های تلفنی

6-توقیف احتیاطی در موارد مشکوک

7-جستجوی منازل به واسطه سوء ظن

8-نظارت دولتی بر «رایانامه ها»[[50]](#footnote-50) و ارتباطات اینترنتی

9-استراق سمع مکالمات تلفنی (*Sjaak,ibid,p393*)

چنانچه مشاهده می شود برخی از این موارد که امکان نقض حریم خصوصی شهروندان را توسط دولت میسر می کند به سرویس های تعیین محل جغرافیایی مربوط می شوند.استفاده از این سرویس ها اگرچه به عنوان رایج و مرسوم برای حمایت از امنیت شخصی شهروندان معرفی شده است،اما می تواند خطری بالقوه برای تهدید این مقوله به حساب آید.به کارگیری برخی از این ابزارها،امکان نقض گسترده حقوق بشر را فراهم می سازند.بسیاری از این سیستم های ضبط و نظارت فرصت سوء استفاده را در اختیار افرادی قرار می دهند که به این اطلاعات دسترسی دارند.ابزراهای مجهز به این فناوری تنها زمانی می توانند موثر و کارا تلقی شوند که در مکان زمان مناسب و با مداخلات صحیح انسانی صورت گیرند.(واجارگاه،1390،ص 147)

بر اساس آنچه گفته شد،انتظار مشروع از حریم خصوصی می تواند با شرایطی برای شهروند به وجود آید.هر شخص باید «انتظار ذهنی و واقعی»[[51]](#footnote-51) از حریم خصوصی در شرایط مشخص داشته باشد.جامعه نیز باید آماده پذیرش «انتظار عینی »[[52]](#footnote-52) به عنوان یک امر معقول باشد.آراء مختلفی از دادگاه های اروپایی در این زمینه صادر شده است.موضوع آن است که آیا همه افراد به یک میزان می توانند از حریم خصوصی بهره مند شوند؟اگرچه انتظار مشروع از حریم خصوصی توسط بسیاری از قضات در «دادگاه اروپایی حقوق بشر»[[53]](#footnote-53) به رسمیت شناخته شده است اما استثنائاتی نیز وجود دارد.برای مثال در دعوای «لویی علیه سویس»[[54]](#footnote-54)دادگاه رای داد که شهروندی که درگیر فعالیت های مجرمانه (از قبیل حمل و نقل و قاچاق مواد مخدر)است باید انتظار کمتری از حریم خصوصی داشته باشد.در این پرونده دادگاه با استفاده از دستگاه های استراق سمع توانسته بود مکالمات منزل لویی را تحت پوشش درآورد.دادگاه اعلام داشت که لویی باید می دانست که مشغول یک عملیات جنایی بوده و همواره خطر پوشش زندگی شخصی او توسط نیروهای مخفی پلیس وجود دارد.[[55]](#footnote-55)([www.privacynetwork.info](http://www.privacynetwork.info))

امروزه بسیاری از فعالیتهای مجرمانه سازماندهی شده نظیر پولشویی،تروریسم،قاچاق مواد مخدر و... تهدیدی علیه امنیت ملی کشورها محسوب می شوند.دولت ها برای مقابله با این تهدیدات از سرویس های پیشرفته تعیین محل اشخاص به عنوان یکی از ساده ترین و معمول ترین روش ها استفاده می کنندکه البته ممکن است نقض حریم خصوصی برخی را به دنبال داشته باشد. پس انتظار مشروع از حریم خصوصی و نه هر گونه انتظاری را می توان به عنوان ابزاری کار و موثر در برابر دخالت های دولت به واسطه پیشگیری از جرم به رسمیت شناخت. در این بین باید توجه داشت که این اقدامات نباید منجر به نقض حریم خصوصی جمعی و گسترده افراد شود.در واقع راهکارهای پیشگیری از این مهم از ضروریات است.

«دوربین های مدار بسته» نظارت پیشگیرانه یا نقض حریم خصوصی؟

در واقع آنچه امروزه تلویزیون مدار بسته می نامیم یکی از شیوه های نظارت و مراقبت است که در دهه اخیر به گستردگی در محیط های اجتماعی به کار می رود.دوربین های کنترل کننده فروشگاه های بزرگ،مراکز تجاری،انبارها،بیمارستان ها،ایستگاه های قطار،خیابان ها و پارک ها از این نمونه اند (کوسن، 1384، ص325). این دوربین ها توانایی مراقبت از تمامی حرکات و رفت آمدهای شهروندان را داراست این امر به بهانه حفظ امنیت ناخوشایند مقامات دولتی نیست،اما نباید حقوق بنیادین را در کارزار امنیت قربانی کرد.

مثال های مختلفی برای این مدل از پیشگیری وضعی از جرم وجود دارد که می تواند منتهی به نقض حریم خصوصی شهروندان شود زیرا این مطلب پذیرفته شده که همه ما می توانیم در یک مکان عمومی هم در حالت خصوصی باشیم.اگرچه اخذ تصاویر در مکان های عمومی عادتا نباید نقض حریم خصوصی تلقی شود اما کاستن از انتظار افراد برای بهره مندی از حریم خصوصی در اماکن عمومی به منزله انکار حق برخورداری از حمایت های متناسب در قبال سوء استفاده از نظارت های آشکار خیابانی نیست.

زندگی خصوصی ممکن است با آزادی اطلاعات اصطکاک ایجاد نماید،در این موارد بر اساس عرف رایج،قاضی تشخیص می دهد که کدام بخش از زندگی آنها جزء حریم خصوصی و کدام بخش می تواند منتشر گردد.در کشور آمریکا موضوع قابل توجه آن است که نشریات زرد تمایل زیادی به مداخله در زندگی شخصی افراد مشهور با استناد به جریان آزاد اطلاعات دارند.برای مثال در یک مورد عکس برهنه یک هنرپیشه آمریکایی که معلوم شد توسط دوربین های مداربسته گرفته شده صفحه اول بسیاری از نشریات آمریکا را به خود اختصاص داده بود.این دوربین ها به طور 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 جنبه های 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 می شود کافی است تا تمام جنبه های زندگی وی برای رویت و نظارت عموم مجاز گردد.لذا هیچ محدودیتی برای افشاگری در مورد این افراد و انتشار اسرار زندگی خصوصی آنها وجود ندارد.» (انصاری، پیشین، ص31) مثال دیگر پخش شده فیلم ویدیویی از رییس جمهور وقت آمریکا بیل کلینتون بود.فیلم مذکور وی را در حال معاشقه با یک زن نشان می دهد که جنبه عمومی و رسانه ای پیدا کرد.به طور معمول دوربین به کار گرفته شده که صحنه مذکور را ضبط کرده به لحاظ امنیتی و برای پیشگیری از وقوع جرم به کار گرفته شده بود. در کشور انگلیس نزدیک به چهار میلیون دوربین،مکان های عمومی را تحت نظر دارند.هر شهروند انگلیسی ،300 بار در روز با حدود 30 شبکه عکس برداری می شود .700 دوربین نیز پلاک های اتومبیل هایی که در شهر لندن وارد می شوند را برای بررسی پرداخت مالیات کنترل می کنند.به همین دلیل انگلیس در ترجیح رویکرد امنیتی بر مبنای فناوری مشهور می باشد.» (ابراهیمی، پیشین، ص103) با وجود احساس امنیت شهروندان در مقابل وقوع بزه با وجود چنین سیستم های پیشگیرانه و نظارتی آیا حریم خصوصی شهروندان ایمن و مصون از تعرض خواهد ماند؟ در کانادا نظارت ویدیویی در اماکن عمومی از حدود 20 سال پیش آغاز شده ،با این وجود شیوع استفاده از آن به اندازه انگلیس نبوده است.بانکها،رستوران ها،فروشگاه ها،مکان های صنعتی،دفاتر،آپارتمان ها،مکان های گردشگری عمومی از این شیوه بهره برده اند.در سال 1995 میلادی 70 درصد کلیه بانکهای مورد سرقت واقع شده در کانادا مجهز به سیستم نظارت ویدیویی بودند.البته ادعا شده که در 75 درصد مجموع جرایم ارتکابی نقش نظارت ویدیویی در کسب اطلاعات مقدماتی برای کشف جرم موثر بوده اند.مفسران از همان زمان پیشگویی کردند که نظارت ویدیویی به طور تاسف باری به یک از ابزارهای پیشگیری از جرم در آینده تبدیل گردد(Nieto, 1977, p10). تاثیر نظارت ویدیویی در مکان ها و موقعیت های گوناگون متفاوت بوده است.بسیاری از مطالعات در کانادا نشان می دهند که دوربین های بدون صفحه نشان گر کمترین تاثیر را در بازدارندگی و پیشگیری از وقوع جرم در بانکها و فروشگاه ها داشته اند. در فرانسه استفاده از ابزارهای شنود،ابزارهای الکترونیکی و نظارت ویدیویی اگر به منظور افشای اطلاعات جنسی یا مالی اشخاص به کار گرفته شوند غیر قانونی است،اما برای کشف عملیات جاسوسی و فعالیتهای سیاسی مجاز است. در حقوق فرانسه البته تشت آراء به چشم می خورد.شعبه جنایی دیوان عالی کشور در فرانسه ضبط اعمال و رفتار کارمندان به وسیله 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 بزه دیده اجازه داده است تا بدون اطلاع و آگاهی متهم،گفتگوهای تلفنی توهین آمیز او را ضبط و به دادگاه ارائه کند، در حالی که شعبه دوم مدنی دیوان عالی کشور ضبط مکالمه تلفنی خصوصی دیگری را بدون اطلاع طرف مقابل عمل متقلبانه و دلیل اکتسابی را غیر قابل پذیرش دانسته است (تدین، 1388، ص148). شیوع عملیات تروریستی در سالهای اخیر جواز استفاده از وسائل الکترونیک و نظارت ویدیویی در اماکن عمومی را برای دولت فراهم کرده، از این رو امروزه نظارت های وسیع دیدبانی الکترونیکی در معابر و مناطق عمومی شهرها وجود دارد.صد ها دوربین تلویزیونی حومه شهر پاریس را تحت کنترل دارند،مناطق تجاری و مالی با بیش از 160 عدد از دوربین های پلیسی نظارت ویدیویی به طور 24 ساعته تحت نظر اند،بیش از 2500 دوربین در اتوبوس های شهرداری برای تشخیص اعمال جنایی تعبیه شده اند.بیشتر فروشگاه ها و امنیت ترابری هوایی از این روش به طور وسیع در پیشگیری از جرم استفاده می کنند.اسپانیا،روسیه،موناکو و دیگر کشورها در سراسر دنیا وضع مشابهی دارند و هر ساله هزینه های گزافی را صرف نصب دوربین ها و استفاده از نیروی انسانی می کنند(Nieto, op.cit, p10). با وجود واقعیت های مشابه پرسش آن است که استفاده از دوربین های مدار بسته و به طور کلی مراقبت های ویدیویی تاثیری در پیشگیری و کاهش وقوع جرم و جنایت داشته است و یا آنکه این نوع اعمال نظارت بر شهروندان با اهداف دیگری طراحی شده اند؟ در سال 2006 دادگاه قضایی آمریکا گزارشی راجع به سیستم های ویدیویی در مناطق عمومی صادر کرده که توسط پرفسور «جری راتسفیل» استاد دادگاه جنایی در دانشگاه تمپل تنظیم شده است.این گزارش توضیح کاملی از این فرآیند به دست می دهد و مضرات و مزیت های وابسته به این تکنولوژی و یافته های ارزشمند این سیستم را به طور مختصر بیان می کند.گزارش بیان می کند در حالی که مشاهدات کلی در بین سیستم های مدیریتی و مناطق عمومی حاکی از کارایی دوربین های مراقبت ویدیویی برای جلوگیری از جرم می باشد اما پیدا کردن مدارک واقعی از کاهش جرم بسیار سخت است. در سال 2002 وزارت کشور انگلستان گزارشی به نام «جلوگیری از جنایت بر اثر تلویزیون های مدار» بسته منتشر کرد .این گزارش توسط «براندن ولش» استاد اداره دادگاه جنایی در دانشگاه ماساچوست و «دیوید فارینکتن» استاد جرم شناسی روانی در موسسه جرم شناسی دانشگاه کمبریج نوشته شده است.مولفان 46 مطالعه مرتبط از هر دو کشور آمریکا و انگلیس را طبق معیارهای اسلوب شناسی دقیق بررسی کردند و دریافتند که فقط 22 مورد از مطالعاتشان برای قرار دادن در تجریه و تحلیل ها به اندازه کافی دقیق است.بر اساس این 22 مطالعه آنها نتیجه گرفتند که مراقبت ویدیویی به مقدار کمی جنایات و جرایم را کاهش می دهد و بیشتر در کاهش جرم وسایل نقلیه در پارکینگ ها موثر است.مراقبت های ویدویی تاثیر کم و یا هیچ تاثیری روی جرم در حمل و نقل عمومی و مرکز شهر ندارند. در سال 2005 وزارت کشور انگلستان گزارش دیگر روی مطالعات کارایی سیستم های مراقبت ویدیویی منتشر کرد.«مارتین گیل» استاد جرم شناسی در دانشگاه لیسیستر ارزیابی های خودش را بدین شکل نشان داد. در این گزارش وی یک ارزیابی منظم از 13 پروژه اجرا شده مراقبت ویدیویی در محل های مختلف شامل مرکز شهرها،پارکینگ ها،بیمارستان ها و مناطق مسکونی تهیه کرد.نتایج متناقض بود:جرم ها در حالی در برخی مناطق کاهش می یابند که در مناطق دیگر شاهد افزایش جرایم خواهیم بود.سیستم های ویدیویی ناظر که در مناطق مختلف شامل پارکینگ های عمومی،بیمارستان ها،و... نصب می شوند نشان می دهد که بیشترین کاهش جرم به ویژه در پارکینگ های عمومی است و همچنین گزارش متذکر می شود که سهم این سسیستم های ناظر در کمک به پلیس در حفظ نظم عمومی و کشف جرایم به صورت سیستمی که متشکل از اجزاء کوچک تر ،با سیاست هدفمند،ناظر،قانونمند و منظم گسترش یافته است.این گزارش توصیه می کند به منظور افزایش قوای زیر بنای این سیستم ناظر بهتر است این سیاست توسعه یابد. وادریسمن پرفسور جرم شناسی و رییس گروه امنیتی و انتظامی ملی از دانشگاه اوتادا ارزیابی و بررسی تحقیقات را هدایت می کرد.مروری بر این تحقیق نشان داد تاثیرات نظارت ویدیویی در مورد جرایم کاملا متغیر و نسبتا غیر قابل پیش بینی است و آن ارزش بازدانده نظارت ویدیویی در طول زمان و در مقوله های جنایی مختلف متفاوت می باشد.سیستم های نظارت ویدیویی،کمترین تاثیر را در کاهش خلاف های مربوط به بی نظمی عمومی داشتند.اهمیت عوامل بازدانده نظارتی ویدویی به موقعیت های مربوط به گردشگری مربوط می شدند. در مجموع می توان گفت در حال حاضر پیدا کردن شواهد واضح که نشان دهنده این باشد که نظارت ویدیویی موثر در پیشگیری از وقوع جرم می باشد کار سختی است.به هر حال نتیجه گرفتن عکس آن نیز مشکل است.یک نقش خیلی موثر و ارزشمند برای نظارت ویدیویی ممکن است مطرح کردن آن به عنوان منبعی از شواهد در کشف و تحقیق جرایم باشد.استفاده از دوربین های مدار بسته اگرچه با هدف پیشگیری از وقوع جرم مورد باشد اما باید علاوه بر روش های پیشگیری تدابیر لازم به منظور جلوگیری از سوء استفاده احتمالی را به ترتیب زیر مد نظر داشت:

1-باید شهروندان را از وجود دوربین های مدار بسته به وسیله تابلوهای اطلاع رسانی مطلع نمود تا این وسیله به ابزار سرکوبی مردم تبدیل نشود؛

2-حق دسترسی افراد به اطلاعات ثبت شده؛

3-حق بزه دیده سوء استفاده از این سازوکارها جهت مراجعه به دادگاه؛

4-ممنوعیت نصب دوربین در محل سکونت افراد (ابراهیمی، 1390، ص111).

**توسعه افراط گونه در به کارگیری روش های بیومتریک**

بیومتریکس به عنوان روش شناسایی منحصر به فرد انسان ها بر مبنای یک یا چند ویژگی یا مشخصه طبیعی معرفی شده است.این روش به عنوان یک شیوه مدیریت دسترسی به هویت و کنترل در گروه های تحت نظارت مورد استفاده قرار می گیرد.شایع ترین روش های یبومتریکی به شرح ذیل می باشند:

**1- انگشت­نگاری:** فرآیند بیومتریک با انگشت­نگاری و شست­نگاری، همچنان یک عملکرد متداول به حساب می­آید که علت آن می­تواند به واسطه آشنایی عامه مردم با این عمل و نیز کارایی استاندارد انگشت­نگاری به وسیله جوهر باشد. همچنین، امروزه استفاده از دستگاههای خواندن اثر انگشت بیش از حد افزایش پیدا کرده است که در میان آنها می­توان قرار دادن این دستگاه را در «موشواره»[[56]](#footnote-56) و صفحه کلید یا کارت­های هوشمند و دستگاههای کوچک مرتبط را نام برد(Sean, 2002, p15).

**2- هندسه و شکل دست:** هر چند پیشتازی فرآیند بیومتریک براساس 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.

**3- اسکن (تصویر) شبکیه چشم:** بیومتریکس بر اساس تصویربرداری شکل رگ­های شبکیه چشم افراد هرگز نتوانست آن چنان که انتظار می­رفت و حتی با وجود تمایل مردم به سمت تکنولوژی، 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، وقتی که در مقابل و یا حتی در نزدیکی دستگاه قرار گرفته­اند. موجب نگرانی استفاده کننده به لحاظ تمیز بودن دستگاه و یا تأثیرات ورود اشعه در چشم، می­شود.

ب) هزینه تصویر برداری شبکیه به ویژه 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 مطلوبی از برای تسهیلات هسته­ای و یا نظامی مورد نیاز باشد، حفظ کرده است.

**4- تشخیص عنبیه چشم:** فرآیند بیومتریک براساس تصویربرداری از خلل و 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 می­باشد.

1. **تشخیص صورت:** این سیستم متکی به تصویربرداری ویژگی­های خاص صورت از قبیل چشم­ها، بینی و دهان وغیره می­باشد .فناوری تشخیص صورت احتمالاً شرایط فناوری سایر روش­های بیومتریکی دیگر را در چند سال گذشته تغییر داده است. تعدادی از تأمین کنندگان ادعا نمودند که محصولی را دارند که می­تواند یک صورت را در یک جمعیت انبوه تشخیص دهد. اخیراً، تأمین کنندگان فراوانی این ادعا را دارند و چنین کاربردی در سال 2001 در یک مسابقه فوتبال آمریکایی، عملی گردید. متعاقباً، این می­تواند بیومتریکی باشد که پس از یازدهم سپتامبر دنبال شد، چرا که به نظر می­رسد که بتواند تروریست­ها را در میان جمعیت پیدا کند. در حقیقت، بسیاری از فرودگاهها این فناوری را مورد بررسی قرار دادند. **در آمریکا** این دستگاه در فرودگاههای بوستون و سایر شهرها یا نصب شده است و یا مورد بررسی قرار گرفته است. ولی تأثیر این سیستم در کاربردهای جهانی مورد اطمینان نبوده است. حتی تأمین کنندگان چنین سیستم­هایی پذیرفته­اند که یک تصویر خوب از روبرو از صورت اشخاص که باید شناسایی شوند باید توسط دوربین­های سیستم گرفته شود تا فرآیندهای مربوطه کارایی داشته باشد. **(Sean, op.cit, p4)**

**6- تشخیص صدا:** این بیومتریک بر اساس این تئوری قرار دارد که صدای هر فرد واحد ومشخص بوده و با اشخاص دیگر متفاوت است که قاعدتاً متکی بر تصویر دیجیتالی امواج صوتی ایجاد شده در هنگام گفتن برخی کلمات خاص می­باشد و وقتی که فردی بخواهد پس از یک ثبت نام به سیستمی وارد شود وی باید تمام یا بخشی از کلمات را دوباره تکرار کند وسیستم 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.

**7-‌ دینامیک امضاء/ صفحه کلید** **:**دو مورد که به صورت نمادین و واحد توسط هر فرد انجام می­گیرد، امضاء کردن و تایپ با صفحه کلید است. بیومتریک دینامیک امضاء، جهت، سرعت و فشاری را که در هنگام امضاء نام خود داریم بررسی کرده و با امضاءهای 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 امضاء الکترونیکی در برخی از فروشگاهها برای خرید با کارت­های اعتباری به بازارآمده است (رئیسی، 1390، ص122). استفاده از روش های بیومتریک امروزه اشکال گوناگون و متکثری یافته است.از سویی قانونی شدن سریع این فرآیند و از جهت دیگر تنوع ابزارهای مورد استفاده منجر به نقض حریم خصوصی افراد شده اند.برای نمونه سازمان «ایکائو»[[57]](#footnote-57) که در سال 1994 در شیکاگوی آمریکا تشکیل شد و بیش از 189 عضو در سراسر جهان دارد امروزه مسئولیت وضع استاندارد هایی را در جهت ارتقای امنیت برعهده دارد.این سازمان تا سال 2010 همه اعضای خود را ملزم به استفاده از ماشین های رمز خوان استاندارد در مرزهای خود نموده است.اجباری شدن استفاده از ماشین رمز خوان در قانون میهن پرستی آمریکا برای تقویت سازمان های آمریکایی در جهت مقابله با عملیات تروریستی از نمونه های دیگر توسعه همه گیر بیومتریکس است. استفاده از بیومتریکس به اندازه ای شایع شده که فرد در صورت معترض بودن و تن ندادن به انحصار این روش ها به صورت اجباری باید از رفت و آمد در بسیاری از محیط های اجتماعی از قبیل فرودگاه ها،سالن های مترو،هتل ها و فروشگاه های عظیم خود را محروم ببیند.(محسنی،1389،ص 331 و 332)

**پیشگیری وضعی از جرم در «فضای سایبر»[[58]](#footnote-58)**

نقض حریم خصوصی مقوله ای است که می تواند باعث رنجش بسیاری از افراد شود.این موضوع در فضای سایبر نیز امکان وقوع دارد.مطالعه پیش نویس لوایح قانونی و خط مشی گذاری های دولتی نشان می دهد که همواره تقاضای حمایت بیشتر از حریم خصوصی در فضای سایبرتوسط کاربران و مردم وجود دارد.مشکل از آنجا ناشی می شود که اینترنت فضایی آزاد را برای هم کاربران مهیا ساخته و این مسئله حق جمع آوری اطلاعات را برای دیگران به وجود آورده است.در این بین آزادی در جمع آوری اطلاعات خصوصی شهروندان برای دولت،بیش از سایرین میسور است.بنابراین همواره این احساس در بین شهروندان می تواند وجود داشته باشد که اینترنت به عنوان وسیله ای در راستای نظارت بر مسائل خصوصی شان تلقی گردد.(kamal,ibid,p25)اگرچه اشخاص تا اندازه ای می توانند هنگامی که «برخط»[[59]](#footnote-59) 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 می باشند.آنچه مهم است آنکه با افزایش و پیشرفت در فناوری می بایست،راهکارهایی برای جلوگیری از نقض حریم خصوصی پیش بینی شوند. ( Cyber Crime Strategy,2010,p27)

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 11 سپتامبر در آمریکا،دولت به منظور بالا بردن امنیت داخلی قانونی موسوم به «پاتریوت»[[60]](#footnote-60)به تصویب رسانید که به واسطه آن امکان دسترسی به «رایانامه» شهروندان آمریکایی وجود داشته باشد.اگر چه می توان گفت،«در صورتی که منفعت عمومی حاصل از امنیت ملی بیش از منفعت حاصل از اطلاعات محرمانه باشد،اطلاعات مورد حمایت واقع نمی شوند» و «به طور کلی دادگاه ها به امنیت ملی چنان اهمیتی می دهند که بر اساس آن حکم به افشای اطلاعات محرمانه می نمایند»،(استنلی،1391،ص 96)اما به هر حال ایجاد تعادل بین تضمین حریم خصوصی شهروند و امنیت ملی دولت و تشخیص اینکه کدام یک بر دیگری تقدم دارند،معیار تشخیص دهنده صلاحیت و بی طرفی منظور را داراست و به هر حال این نقض حریم خصوصی را چگونه می توان توجیه نمود تا اندازه ای دشوار می نماید.

ماهیت سری و مخفی توطئه ها و فعالیت های بر ضد امنیت ملی در فضای سایبر نیازمند استفاده از روش های تخصصی تجسس برای مقابله با مجرمین می باشد.شیوه های اتخاذ شده برای مقابله،گاهی جنبه پیشگیرانه دارد که می تواند حریم خصوصی افراد را با خطر مواجه سازد.بر اساس اصل اقتضاء باید دانست که آیا این اقدامات واقعا ضروری است و هیچ معیاری که غیر تهاجمی تر و بی ضرر تر باشد برای دستیابی به این هدف وجود ندارد؟البته زیانباری این اقدام البته نباید دور از نظر قرار گیرد چرا که به هر حال تا اندازه زیادی حقوق شهروندان را تحت تاثیر قرار می دهد.(نمامیان،1390،ص 91)

موضوع دیگر مربوط به نقض حریم خصوصی مردم توسط «شرکت های ارائه کننده خدمات اینترنتی»[[61]](#footnote-61) به خصوص در کشورهای دارای نظام پلکانی در ارائه این خدمات می باشد. این شرکت ها در اصطلاح «آی اس پی»[[62]](#footnote-62) نامیده می شوند بسته به ماهیت و طبعیت دولتها یا کاملا در انحصار بخش دولتی بوده و یا قسمتی از آن منشعب شده و در ید استیلاء بخش خصوصی قرار می گیرند.[[63]](#footnote-63) شرکت های ارائه کننده خدمات اینترنتی می توانند به بسیاری از اطلاعات حساس و خصوصی مشتریان خود دست یابند.این شرکت ها حتی زمانی که به صورت خصوصی اداره شوند ممکن است تحت تاثیر خط مشی گذاری دولت حاکم قرار گیرند.نتیجه آنکه بسیاری از اطلاعات خصوصی شهروندان که در اختیار این شرکت ها قرار دارد می تواند در دسترس دولت گذارده شود. تمایل دولت های بسته و اقتدارگرا بیشتر به سمت انحصار این بخش از فعالیت خدمت عمومی در دست دولت ،به دلیل کنترل همه جانبه بر زندگی مردم می باشد. از این رو احتمال مصون ماندن حریم خصوصی در فضای سایبر به دلیل نظارت همه گیر دولت با تردیدهای جدی روبرو می شود. (paul,1999,p1627)در مجموع اعمال کنترل های وسیع و بدون انتخاب قبلی اگرچه امروزه ابراز مفید و موثری برای بقا و تداوم هیات حاکمه بوده و در مواردی تضمین امنیت و آسایش فردی و اجتماعی شهروندان را موجب شده ،اما تحدید و تهدید حقوق و آزادیهای فردی و تعرض به حریم خصوصی را نیز به دنبال داشته است. (محسنی، 1389، 535-534).

**چالش کارویژه های دولت (بقا حاکمیت یا حریم خصوصی)**

دولت در هر جامعه ای مظهر مصلحت عمومی است و اگرچه وجوه اخلاقی،مذهبی و اقتصادی دارد اما اساسا موسسه ای اخلاقی،مذهبی و اقتصادی نیست بلکه کارویژه های متفاوتی دارد؛از جمله حفظ نظم و امنیت،حراست از حقوق بنیادین افراد جامعه و...در برخی نظریه های دولت بر وجه اجبار آمیز آن تاکید شده است،از این رو برخی رئالیست ها و و مارکسیست ها اساسا دولت را ابراز اجبار تلقی نموده اند. (بشیریه، 1384، ص27) واقع گرایان به خوبی دریافته اند که انسان در غیاب قدرت و اجبار دولتی و اجتماعی به سرکشی و تجاوز روی می آورد. به واسطه بهره مندی از وجه اقتدار که یکی از ویژگی ها و چهره های پایدار و اصلی این موسسه است، همواره اعمال و رفتار های دولت در درجه اول پدیده ای اجبار آمیز بوده است.هر دولتی از طرفی طبق تعهدات داخلی با شهروندان خود و مطابق الزامات و التزامات بین المللی و حقوق بشری خود باید شرایط تحقق و حفظ حقوق بنیادین را برای شهروندانش فراهم سازد.از سوی دیگر برای بقا و حفظ موجودیت سیاسی خود ممکن است به شدید ترین ابزراها یا همان قوه قهریه متوسل گردد. با امنیتی شدن افراطی جامعه آزادی و حریم خصوصی ای برای مردم قابل تصور نخواهد بود اما برای تضمین حداقلی همین دو مقوله نیازمند به کارگیری سازوکارهای امنیتی هستیم. بنابراین پرسش آن است که ایجاد تعادل و توازن بین این دو چگونه میسور است؟به راستی یک جامعه تا کجا می تواند به نام امنیت پیش رود و تا چه میزان می تواند 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 می شود. 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 می شود و این ملت است که موضوع **امنیت ملی** خواهد بود و تهدید ها بر ضد **امنیت ملی** پیوند ناگسستنی با هستی و استواری یک ملت دارد.روی هم رفته **امنیت ملی** در جهان امروز برجسته ترین ارزش دولت هاست.دولت های مردم سالار از ترس مداخله و دست اندازی دولت های غیرمردم سالار،**امنیت ملی** را پیش می کشند و دولت های غیرمردم سالار،رخنه های نادیدنی دولت های مردم سالار در نظام حکومتی فراگیر را تهدید به شمار می آورند (عالی پور، 1388، ص33-32). در دولت های مردم سالار هر چیزی از بیرون، دولت را مورد هجوم قرار دهد تهدید بر علیه امنیت کشور به شمار می رود ولی دولت های اقتدارگرا هر تهدید اعم از داخلی و خارجی مسئله ای امنیتی محسوب می شود. 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... مسئله ای بیرونی و نشات گرفته از دشمن و عامل بیگانه محسوب می شود. به بهانه حفظ امنیت کشور ،آزادی های عمومی و حقوق بنیادین افراد دستخوش چالش هایی شده است. به عنوان یک نمونه ملموس و مشهور می توان گفت فضای رعب آور پس از فاجعه انسانی 11 سپتامبر توجیه اساسی برای اعمال مجموعه ای از اقدامات کنترلی بوده که آزادی های مدنی را به نام **امنیت داخلی** محدود و سلب کرده تا جایی که عده ای این تحول را «حالت استثناء» تلقی کرده اند،اما جالب آنکه حالت استتثناء به پارادامی عادی در دولت معاصر تبدیل شده است.محدودیت های اعمال شده در خصوص آزادی های مدنی و گسترش رویه های وسیع نظارتی به طور نامتناسب برخی گروه های اقلیتی نظیر اعراب و مسلمانان را هدف قرار داده است.سیاست های پلیسی عدم مدارا،استفاده گسترده از نظارت ویدیویی و روش های مختلفی که امروزه برای مبارزه با تروریسم مورد استفاده قرار می گیرد با هدف استقرار **امنیت ملی** و در نهایت حفظ منافع عمومی است که هیچ توجیهی نمی طلبد. فضای امنیتی پس از 11 سپتامبر به عنوان کاتالیزور برای معرفی فناوری های جدید در سطح جهان عمل کرده و به قسمتی از زندگی روزانه شهروندان تبدیل شده اند.جامعه نظارتی «برادر بزرگ» که در رمان «قلعه حیوانات» «جرج اورول» در 1948 به تصویر کشیده شد و در آن همسایه ها جاسوسی یکدیگر را می کنند،هر صدایی شنیده می شود و هر حرکتی به تصویر کشیده می شود با شرایط کنونی ارتباط تنگاتنگی دارد (بابایی، عباسی، 1390، ص193). اگر نه همه هدف دولت و نه بخش بزرگ آن از این اقدامات استقرار و حفظ امنیت برای دولت و مردم باشد،در اینکه دولت حتی به بخش کوچکی از خواسته های خود دست یافته باشد جای تردید وجود دارد.تروریست ها در پی ایجاد هراس و وحشت در بین شهروندان و هیات حاکمه اند.با تاملی سطحی و اندک می توان دریافت که آنها به راحتی به آمال و اهداف خود دست یافته اند.استفاده بیش از حد از روش های وضعی در پیشگیری از جرم علاوه بر آنکه منجر به شکل گیری دولت پدر سالار کیفری در عمل شده،به استقرار و تداوم جو هولناک امنیتی دامن زده و این همان چیزی است که تروریست ها در پی آنند.افزایش ترس از جرم به واسطه تدابیر مختلف پیشگیری وضعی به شهروندان این پیام را القاء می کند که محیط زندگی آنان خطرناک است.افزایش اقدامات امنیتی آشکار موجب می شود تا شهروندان عادی به خاطر ترس از بزه دیدگی واکنش های روانی مختلفی از خود بروز دهند،حس بدگمانی و سوء ظن آنان نسبت به دیگران افزایش یابد،تعاملات فردی و اجتماعی شان تضیف گردد ،گوشه گیر و ضد اجتماعی شده و کمتر از منزل خارج شوند.از طرف دیگر چنانچه در مقوله راجع به نظارت ویدیویی توضیح داده شد شهروندان را باید از وجود اقدامات پیشگیرانه و به خصوص دوربین های مدار بسته آگاه ساخت تا نقض حقوق اساسی آنان به حداقل ممکن کاهش یابد.این تعارضات چگونه قابل توجیه اند و جمع آنها چگونه میسور است؟ در هر حال باید این واقعیت را پذیرفت که گسترش اقدامات پیشگیرانه وضعی شهرها و محله ها را به شکل قلعه های مستحکم نظامی درآورده است .این کار ممکن است تا اندازه ای منجر به کاهش جرم شود لیکن بهایی که برای آن پرداخت می شود بسیار بالاست چنانچه به نظر می رسد ضایعات افراط در اجرای این تدابیر چیزی کمتر از خسارات ناشی از جرم نباشد (محمدنسل، 1387، ص80). هزینه های روانی و اجتماعی ناشی از ترس از جرم از آن رو که عامل مهم و موثری در تغییر کیفیت زندگی محسوب می شود حتی از خود جرم نیز می تواند اهمیت بیشتری یابد.آثار سیاسی ترس از جرم نیز قابل تامل اند.همان طور که گفیتم حاکمیت متولی تامین امنیت جامعه و اعضای آن است.به ویژه در جوامع دموکراتیک یکی از مهمترین مطالبات مردم از این قوا تامین **امنیت ملی** است.احساس ناامنی و ترس می تواند مشروعیت/مقبولیت حاکمیت را به مخاطره بیندازد.

**نتیجه**

همان طور که اشاره شد حریم خصوصی شهروندی و امنیت ملی هر دو از مقوله های مهم حقوق بشری محسوب می شوند.تحقق این دو از دغدغه های اصلی دولت های عصر حاضر است. آنچه در این مقاله گذشت پاسخ به این سوال بود که بر اساس چه مبنایی دولت می تواند مقوله **امنیت ملی** را بر حریم خصوصی مقدم کند؟ دولت با داشتن قدرت،به منظور حفظ امنیت داخلی می تواند حریم خصوصی افراد را نقض کند و این خود جنبه دموکراتیک دولت را با چالش مواجه می سازد.مسئله ای که در این تحلیل مطرح می شود فلسفه سود گرایی است؛یعنی دولت با داشتن حق پیشگیری از جرم،نگاهی سودانگارانه به جامعه دارد که می تواند نوعی سوء استفاده از حق حاکمیت تعریف شود. (فریمن، 1387، ص93). در واقع دولت نمی تواند به بهانه حفظ امنیت،از حق خود سوء استفاده کرده آزادی شهروندان را تحدید کند و درصدد تشکیل و استقرار یک جامعه امنیتی باشد. از سوی دیگر می توان فرض سوء استفاده از حق توسط مردم را مطرح کرد،بدین معنی که شهروندان از حقوق خود در جهت عکس منافع شان گام بردارند. بر اساس این نظریه شهروند نباید از حق داشتن حریم خصوصی سوء استفاده نماید و موجب ضرر برای جامعه شود.این فرض نیز متضمن چالش هایی است،چرا که نهاد تشخیص دهنده ضرر اصولا دولت و نهادهای اقتدار عمومی می باشند و همچنین معیار سوء استفاده از حق، ضرر می­باشد که باز هم مفهومی است موسع،چند وجهی و قابل تفسیر. تحلیل دیگر آن است که هرگاه عمل فرد جنبه عمومی پیدا کند یعنی آثار رفتاری فرد اثر اجتماعی بر جای گذارد و یا عمومیت عمل به اقتضای ذات و ماهیت عمل ­باشد حق فردی به معنای حفظ حریم خصوصی نمی تواند 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 جریحه دار شدن حوزه عمومی شود دولت عدالت گرا و مردم سالار 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، عمل خودسرانه از طرف دولت برای شکستن حریم خصوصی افراد جلوگیری می شود چرا که تنها آنجایی دولت حق ورود به حریم خصوصی را پیدا می کند که رفتار فرد جنبه عمومی داشته باشد و از طرفی شهروندان جامعه می دانند تا آنجایی که اعمال و رفتارشان موجب اثر منفی اجتماعی نباشد، حریم خصوصیشان حفظ می شود. از نقطه نظر حقوقی، حقوق بشر می تواند به عنوان مجموعه ای از حقوق فردی و جمعی که توسط دولتها به رسمیت شناخته شده و در قوانین اساسی و حقوق بین الملل مندرج است تعریف شود.از یک نظرگاه مهم برای تحقق این مجموعه مهم نمی توان اصالت و اولویت را به یک بخش یا مقوله داد. رشد و توسعه این حقوق نیازمند حرکت همزمان و در یک راستا می باشد. باید افزود که حریم خصوصی به همان اندازه امنیت ملی مقوله ای مهم تلقی می شود. بنابراین نمی توان راه افراط و تفریط پیمود و یکی را فدای دیگری کرد. استفاده دولت از حق خود برای حفظ امنیت خویش نمی تواند به بهای نقض فراگیر حریم خصوصی تمام شود مگر با دلایل و توجیهات ویژه و افراد نیز نمی توانند به دلیل داشتن خلوت و حق حریم خصوصی در صدد تخریب وجوه امنیتی حاکمیت برآیند.مسلما در چنین شرایطی دولت از وجوه اجبار و اقتدار خود برای ورود به حریم خصوصی در جهت بقاء خود استفاده خواهد کرد.

فهرست منابع

ابراهیمی،شهرام،پیشگیری از جرم در چالش با موازین حقوق بشر،پایان نامه دکتری حقوق جزا و جرم شناسی،دانشگاه تهران،خرداد 1387

ابراهیمی،شهرام،جرم شناسی پیشگیری،جلد اول،نشر میزان،چاپ اول،1390

اصلانی،حمید رضا،حقوق فناوری اطلاعات،نشر میزان،چاپ دوم،1389

آنتونی گیدنز،جامعه شناسی،ترجمه حسن چاوشیان،نشر نی،چاپ چهارم،1390

انصاری،باقر،حریم خصوصی در رسانه های همگانی،نشریه پژوهش و سنجش، شماره 39 و 40، پائیز و زمستان 1383

انصاری،باقر،حقوق حریم خصوصی،نشر سمت،چاپ اول،زمستان 1386

بابایی،یوسف و عباسی،اصلی،جهانی سازی و جرم،نشر مجد،چاپ اول،1390

بشیریه،حسین،آموزش دانش سیاسی،(مبانی علم سیاست نظریه و تاسیسی)نشر نگاه معاصر،چاپ چهارم،1384

بکاریا،سزار،رساله جرایم و مجازاتها،ترجمه دکتر محمد اردبیلی،نشر میزان ،چاپ ششم ،1389

بهرامی احمدی،حمید، سوء استفاده از حق، نشر اطلاعات،چاپ سوم،1377

بوزان،باری،مردم،دولتها و هراس،ترجمه پژوهشکده مطالعات راهبردی،نشر پژوهشکده مطالعات راهبردی،چاپ اول،1378

پائول استنلی،حقوق حفظ اسرار،ترجمه محمد حسین وکیلی وقدم،نشر کتاب همگان،چاپ اول،1391،ص 96

پاک نهاد،امیر،سیاست جنایی ریسک مدار،نشر میزان،چاپ اول،پاییز 1388

تدین،عباس،تحصیل دلیل در آیین دادرسی کیفری،نشر میزان،چاپ اول،1388

خانعلی پور واجارگاه،سکینه،پیشگیری فنی از جرم،نشر میزان،چاپ اول،1390

دادستان،پریرخ،روان شناسی جنایی،نشر سمت،چاپ سوم،پاییز 1385

رئیسی،اندیشه،سیاست جنایی ایران در قبال جرایم ارتکابی در حریم خصوصی،پایان نامه کارشناسی ارشد،دانشگاه آزاد اسلامی واحد نراق،سال 1390

رحمدل،منصور،حق انسان بر حریم خصوصی،مجله دانشکده حقوق و علوم سیاسی،شماره 70،زمستان 1384

صفاري،علي،مباني نظري پيشگيري از وقوع جرم،مجله تحقيقات حقوقی،شماره 33-34، بهار تا زمستان 1380

عالی پور،حسن،جرایم بر ضد امنیت ملی،نشر خرسندی،چاپ اول،1388

عباسی،بیژن،حقوق بشر و آزادی های بنیادین،نشر دادگستر،چاپ اول،1390

کاشفی اسماعیل زاده،حسن،جنبش های بازگشت به کیفر در سیاست جنایی کشورهای غربی، علل و جلوه ها، مجله تخصصی الهیات و حقوق،شماره 15 و 16، بهار و تابستان 1384

کن پینز،جایگاه پیشگیری نخستین از جرم در انگلستان،ترجمه مهدی صبوری پور،مجله حقوقی دادگستری،سال شصت و هشتم،دوره جدید،تابستان 1383

گسن،ریموند،جرم شناسی کاربردی،ترجمه مهدی کی نیا،نشر مترجم،چاپ اول،1370

مایکل فریمن،حقوق بشر،ترجمه محمد کیوانفر، نشر هرمس،چاپ اول،1387

مجتهدی،محمد رضا،حقوق تامین اجتماعی،نشر آیدین،چاپ اول،1388

مجیدی،سید محمود،جرایم علیه امنیت،نشر میزان،چاپ اول،بهار 1386

محسنی،فرید،حریم خصوصی اطلاعات،نشر دانشگاه امام صادق،چاپ اول،1389

محمد نسل،غلامرضا،پلیس و سیاست پیشگیری از جرم،نشر دفتر تحقیقات کاربردی پلیس پیشگیری از وقوع جرم،چاپ اول،1387

محمد نسل،غلامرضا،پلیس و سیاست پیشگیری از جرم،اولین همایش ملی پیشگیری از جرم،چاپ اول،1387

معتمد نژاد،کاظم،جامعه اطلاعاتی،نشر میراث قلم،چاپ دوم،1389

موریس کوسن،نظارت ویدیویی،دلایل موفقیت و شکست،ترجمه شهرام ابراهیمی،مجله الهیات و حقوق،بهار و تابستان 1384

نمامیان،پیمان،واکنش های عدالت کیفری به تروریسم،نشر میزان،چاپ اول،1390

نیاز پور،امیر حسن،پیشگیری از بزه کاری در قانون اساسی ایران و لایحه پیشگیری از وقوع جرم،مجله حقوقی دادگستری،شماره 45،زمستان 1383

AHMAD KAMAL, THE LAW OF CYBER-SPACE, Published by the United Nations Institute for Training and Research, Palais des NationsCH 1211 Geneva 10,Switzerland,2005

Cyber Crime Strategy, Presented to Parliament by the Secretary of State for the Home Department ,by Command of Her Majesty, March 2010

daniel solve, Understanding privacy,Harvard university press,londen,englnd,2008

Dr. Sjaak NouwtوReasonable Expectations of Geo-Privacy?,Volume 5, Issue 2, August 2008

1. Marcus Nieto, public vidio survellance:is it an effective crime prevention tool?, California Research Bureau, California State Library,1997

O'Connor , Sean , Biometrics and Identification after 9/11 , university of washington School of law,quoted, 2002.,in www.ssrn.com

Paul M. Schwartz, Privacy and Democracy in Cyberspace, VANDERBILT LAW REVIEW ,Vol. 52,1999

Ronald V.Clarke, Situational Crime Prevention,Successful Case Studies,Second Edition,Harrow and Heston ,1997

[www.biometrics.gov/docs/privacy/pdf](http://www.biometrics.gov/docs/privacy/pdf)

[www.estig.ipbeja.pt/~ac\_direito/privacy.pdf](http://www.estig.ipbeja.pt/~ac_direito/privacy.pdf)

www.legal-dictionary.thefreedictionary.com/privacy

[www.parliament.uk/parliamentary -offices/post/pubs 2006.cfm](http://www.parliament.uk/parliamentary%20-offices/post/pubs%202006.cfm)

www.privacynetwork.info

1. Penal policy [↑](#footnote-ref-1)
2. Criminal policy [↑](#footnote-ref-2)
3. prevention [↑](#footnote-ref-3)
4. Primary prevention [↑](#footnote-ref-4)
5. Secondary prevention [↑](#footnote-ref-5)
6. Theritiary prevention [↑](#footnote-ref-6)
7. Brantinghham and faust [↑](#footnote-ref-7)
8. Situational Crime Prevention [↑](#footnote-ref-8)
9. Rehabilitative or social prevention [↑](#footnote-ref-9)
10. Positivist [↑](#footnote-ref-10)
11. Villiam beaney [↑](#footnote-ref-11)
12. Tom gerety [↑](#footnote-ref-12)
13. Arthur miller [↑](#footnote-ref-13)
14. daniel solve [↑](#footnote-ref-14)
15. Understanding privacy [↑](#footnote-ref-15)
16. Privacy [↑](#footnote-ref-16)
17. Private [↑](#footnote-ref-17)
18. Secret [↑](#footnote-ref-18)
19. Robert smith [↑](#footnote-ref-19)
20. Decisional [↑](#footnote-ref-20)
21. Spatial [↑](#footnote-ref-21)
22. Intentional [↑](#footnote-ref-22)
23. information [↑](#footnote-ref-23)
24. communication [↑](#footnote-ref-24)
25. Samuel D. Warren [↑](#footnote-ref-25)
26. louis d. brandeis [↑](#footnote-ref-26)
27. The Right to Privacy [↑](#footnote-ref-27)
28. Physical informatin [↑](#footnote-ref-28)
29. Information privacy [↑](#footnote-ref-29)
30. Pretty crime [↑](#footnote-ref-30)
31. Zero tolerance [↑](#footnote-ref-31)
32. Broken windows [↑](#footnote-ref-32)
33. در يك تعريف عام بيومتريك(biometricts) را علم و فناوري اندازه گيري و تحليل آماري داده هاي بيولوژيكي معرفي كرده اند. اما تعريف دقيق تر و فني تر آن كه امروزه رايج شده به قرار زير است: هر خصوصيت فيزيولوژيكي يا ويژگي رفتاري منحصر به فرد و متمايز كننده، مقاوم و قابل سنجش كه بتواند براي تعيين يا تأييد خودكار هويت افراد به كار رود، بيومتريك نام دارد. [↑](#footnote-ref-33)
34. scan-Facial [↑](#footnote-ref-34)
35. scan-Iris [↑](#footnote-ref-35)
36. scan- Finger [↑](#footnote-ref-36)
37. scan-Hand [↑](#footnote-ref-37)
38. اصطلاح «برادران بزرگ»(big brothers) اشاره به داستان قلعه حیوانات اثر جرج اورول دارد که استعاره از رهبر حزب یا شخصیت دیکتاتوری می باشد. [↑](#footnote-ref-38)
39. Geo-privacy or location privacy [↑](#footnote-ref-39)
40. Location based service [↑](#footnote-ref-40)
41. reasonable expectations [↑](#footnote-ref-41)
42. geo-information [↑](#footnote-ref-42)
43. geographic data [↑](#footnote-ref-43)
44. location data [↑](#footnote-ref-44)
45. movement/mobility [↑](#footnote-ref-45)
46. GIS-Geographic informatin services [↑](#footnote-ref-46)
47. GPS-Global positioninig system [↑](#footnote-ref-47)
48. Dutch National Freedom Survey 2007 (Nationaal Vrijheidsonderzoek) [↑](#footnote-ref-48)
49. automatic scanning [↑](#footnote-ref-49)
50. منظور همان ایمیل(E-Mail) یا پست الکترونیک (Electeronic-Post) می باشد. [↑](#footnote-ref-50)
51. actual (subjective) expectation [↑](#footnote-ref-51)
52. objective expectation [↑](#footnote-ref-52)
53. European Court of Human Rights (ECtHR) [↑](#footnote-ref-53)
54. Lüdi v Switzerland [↑](#footnote-ref-54)
55. European Court of Human Rights, Judgment of 15 June 1992 (Lüdi v Switzerland), Publ. ECtHR,

Series A, No. 238. The text of Ludwig Lüdi v Switzerland [↑](#footnote-ref-55)
56. mouse [↑](#footnote-ref-56)
57. ICAO(international civil aviation organization) [↑](#footnote-ref-57)
58. Cyber space [↑](#footnote-ref-58)
59. On line [↑](#footnote-ref-59)
60. Patriot [↑](#footnote-ref-60)
61. Internet service provider [↑](#footnote-ref-61)
62. ISP [↑](#footnote-ref-62)
63. [↑](#footnote-ref-63)