



حمایت کیفی از حریم خصوصی در فضای مجازی

مؤلف:

پروین بادسار

با همکاری:

ستاره قیطان - احمد حمزه - حسن حضریپور



رشید پبلشرز

Rashid Publications

عنوان و نام پدیدآور :	حمایت کیفری از حریم خصوصی در فضای مجازی/ مولفین پروین بادیار... [و دیگران].
مشخصات نشر :	تهران : راشدین، ۱۳۹۳.
مشخصات ظاهری :	۱۶۰ ص.
شابک :	978-600-361-062-0
وضعیت فهرست نویسی :	فیا
یادداشت :	مولفین پروین بادیار، ستاره قیطان، احمد حمزه، حسن حضریور.
موضوع :	فضای مجازی -- جنبه‌های حقوقی
موضوع :	حریم شخصی -- قوانین و مقررات
موضوع :	شبکه‌های کامپیوتری -- قوانین و مقررات
شناسه افزوده :	بادیار، پروین، ۱۳۴۵ -
رده بندی کنگره :	۱۳۹۳ ۸ح/۸۵۱HM
رده بندی دیویی :	۴۸۳۲/۳۰۳
شماره کتابشناسی ملی :	۳۶۹۴۹۴۵



■ انتشارات راشدین

عنوان کتاب:	حمایت کیفری از حریم خصوصی در فضای مجازی
مؤلف:	پروین بادیار با همکاری ستاره قیطان احمد حمزه حسن حضریور
نظارت کیفی:	راهب عارفی
نظارت فنی:	محمد معین عارفی
صفحه‌آر و طراح جلد:	افسانه حسن‌بیگی
چاپ و صحافی:	در تاپ
نوبت چاپ:	اول-۱۳۹۳
شمارگان:	۱۰۰۰
شابک:	۹۷۸-۶۰۰-۳۶۱-۰۶۲-۰
قیمت:	۱۰۰۰۰۰ ریال
نشانی:	میدان انقلاب - کارگر جنوبی کوچه گشتاسب پلا ۴ واحد ۶
تلفن / نمابر:	۶۶۴۰۸۲۲۴ - ۶۶۴۷۶۱۴۷
پایگاه اینترنتی:	www.rashedin.info
پست الکترونیک:	Email: rashed1829@yahoo.Com

کلیه حقوق برای ناشر محفوظ است

تقدیم

به تمام پدران

www.ketab.ir

فهرست مطالب

۸	سخنی درباره این پژوهش
۱۱	پیش درآمد
۱۱	الف) بیان مسئله
۲۰	ب) اهمیت و ضرورت انجام تحقیق
۲۰	ج) اهداف تحقیق
۲۰	د) سؤالات تحقیق
۲۱	ه) فرضیه های تحقیق
۲۳	بخش نخست: مفهوم و جلوه های نقض حریم خصوصی در فضای مجازی
۲۷	فصل اول- مفهوم شناسی نقض حریم خصوصی در فضای مجازی
۲۷	مبحث اول- تعریف حریم خصوصی و انواع آن
۲۷	الف) تعریف حریم خصوصی
۲۹	ب) مفهوم نقض حریم خصوصی و مصادیق آن
۳۱	۱- حریم خصوصی در ایران
۳۳	۲- حریم خصوصی در اسناد بین الملل
۳۴	۳- حریم خصوصی و اینترنت
۳۶	گفتار دوم - انواع حریم خصوصی
۳۶	الف) حریم خصوصی جسمانی
۳۷	ب) حریم خصوصی اماکن
۳۷	ج) حریم خصوصی ارتباطات
۳۸	د) حریم خصوصی اشخاص آسیب پذیر
۴۱	گفتار اول- مبانی دینی
۴۳	الف) ممنوعیت استراق بصر
۴۴	ب) ممنوعیت اشاعه فحشا و هتك ستر
۴۴	گفتار دوم) مبانی حقوق بشری
۴۶	ب) کنوانسیون اروپایی حقوق بشر
۴۸	فصل دوم- جلوه های نقض حریم خصوصی
۴۹	مبحث اول- جرم های علیه تمامیت معنوی

- گفتار اول - توهین سایبری..... ۴۹
- الف) معنای توهین..... ۴۹
- ب) مصادیق و مستندات قانونی..... ۵۰
- گفتار دوم - نشر اکاذیب..... ۵۱
- الف) معنای نشر اکاذیب..... ۵۱
- ب) مصادیق و مستندات قانونی..... ۵۱
- گفتار سوم - شنود غیرمجاز..... ۵۲
- الف) معنای شنود غیرمجاز..... ۵۲
- ب) مصادیق و مستندات قانونی..... ۵۳
- گفتار چهارم - مزاحمت تلفنی..... ۵۳
- الف) معنای مزاحمت تلفنی..... ۵۳
- مبحث دوم - جرم‌های رایانه‌ای علیه اموال..... ۵۴
- گفتار اول - خرابکاری رایانه‌ای..... ۵۴
- الف) معنای خرابکاری رایانه‌ای..... ۵۴
- ب) مصادیق و مستندات قانونی..... ۵۵
- گفتار دوم - سرقت رایانه‌ای..... ۵۷
- الف) معنای سرقت رایانه‌ای..... ۵۷
- ب) مصادیق و مستندات قانونی..... ۵۸
- گفتار سوم - کلاهبرداری رایانه‌ای..... ۵۸
- الف) معنای کلاهبرداری رایانه‌ای..... ۵۹
- ب) مصادیق و مستندات قانونی..... ۶۰
- مبحث سوم - جرائم علیه امنیت آسایش عمومی..... ۶۰
- الف) معنای تروریسم سایبری..... ۶۱
- ب) مصادیق و مستندات قانونی..... ۶۱
- گفتار دوم - جاسوسی رایان‌های..... ۶۲
- الف) معنای جاسوسی رایان‌های..... ۶۲
- ب) مصادیق و مستندات قانونی..... ۶۳
- گفتار سوم - جعل رایان‌های..... ۶۴

- الف) معنای جعل رایانه ای ۶۴
- ب) مصادیق و مستندات قانونی ۶۷
- گفتار چهارم - استفاده از داده مجعول ۶۷
- الف) معنای استفاده از داده مجعول ۶۷
- ب) مصادیق و مستندات قانونی ۶۸
- گفتار پنجم - تعرض به حریم خصوصی اطلاعات ۶۹
- الف) تعریف حریم خصوصی اطلاعات ۶۹
- ب) نقض حریم خصوصی اطلاعاتی از جانب شهروندان ۷۰
- ج) نقض حریم خصوصی اطلاعاتی از جانب حاکمیت ۷۰
- د) انواع اطلاعات غیر قانونی ۷۱
- بخش دوم: راهکارهای حمایتی از حریم خصوصی ۷۵
- فصل اول - راهکارهای واکنشی در حمایت از حریم خصوصی ۷۹
- مبحث نخست - پاسخ های واکنشی در قانون مجازات اسلامی ۷۹
- گفتار اول - کیفر حبس ۷۹
- گفتار دوم - جزای نقدی ۹۴
- مبحث دوم - پاسخ های واکنشی حمایتی در سایر قوانین کیفری ۱۰۶
- گفتار اول - کیفر حبس ۱۰۶
- گفتار دوم - جزای نقدی ۱۱۰
- فصل دوم - راهکارهای کنشی در حمایت از حریم خصوصی ۱۱۲
- مبحث اول - تدابیر پیشگیرانه وضعی ۱۱۷
- گفتار اول - تدابیر وضعی پیشگیری از جرایم علیه حریم خصوصی ۱۱۷
- الف) تدابیر محدودکننده یا سلب کننده دسترس ۱۱۷
- ب) تدابیر نظارتی ۱۱۸
- ج) تدابیر صدور مجوز ۱۱۸
- د) ابزارهای ناشناس کننده و رمزگذاری ۱۱۹
- ه) نرم افزارهای ضد پایش ۱۲۳
- و) نرم افزارهای ضد پیام های ناخواسته ۱۲۳
- ز) سیستم تشخیص تجاوز (ورود غیر مجاز) ۱۲۴

- ۱۲۴ (ر) باروی آتشین.....
- ۱۲۵ (ج) اعتبار سنجی و رمز نگاری.....
- ۱۲۵ (خ) برنامه های ضد اختلال.....
- ۱۲۶ گفتار دوم- چالش های پیشگیری وضعی از جرائم علیه حریم خصوصی.....
- ۱۲۶ (الف) تقابل پیشگیری وضعی از جرائم رایانه‌ای با آزادی بیان و جریان آزاد اطلاعات
- ۱۲۷ ۱- مراجع تدوین‌کننده فهرست‌ها.....
- ۱۲۷ ۲- کارکرد انطباقی.....
- ۱۲۹ (ب) تقابل پیشگیری وضعی از جرائم رایانه‌ای با حریم خصوصی.....
- ۱۳۳ مبحث دوم- تدابیر پیشگیرانه اجتماعی.....
- ۱۳۳ گفتار اول- مفهوم و انواع پیشگیری اجتماعی.....
- ۱۳۴ (الف) مفهوم پیشگیری اجتماعی.....
- ۱۳۴ (ب) انواع پیشگیری اجتماعی.....
- ۱۳۵ (ج) پیشگیری جامعه مدار.....
- ۱۳۵ (د) پیشگیری رشد مدار.....
- ۱۳۶ گفتار دوم- تدابیر پیشگیرانه اجتماعی در حمایت از حریم خصوصی.....
- ۱۳۶ (الف) اقدامات مداخله آمیز والدین.....
- ۱۳۷ (ب) تدابیر همیاری همسالان.....
- ۱۳۷ (ج) تدابیر کاربری صحیح.....
- ۱۳۸ (د) تدابیر کاهنده آثار سوء.....
- ۱۳۹ (ه) تدابیر آموزشی.....
- ۱۴۰ (و) تدابیر الزام‌آور کار برای اینترنت.....
- ۱۴۱ (ز) تدابیر رسانه‌ای.....
- ۱۴۱ نتیجه‌گیری.....
- ۱۵۲ پیشنهادات.....
- ۱۵۵ فهرست منابع.....

سخنی درباره این پژوهش

حمایت کیفری با جرم انگاری، صورت می‌گیرد و بازدارندگی واکنش‌های کیفری نسبت به جرم، به عنوان ابتدایی‌ترین گونه‌ی حمایت کیفری شناخته می‌شود. این نوشتار به بررسی مفهوم و مبانی نظری حمایت کیفری از حریم خصوصی می‌پردازد. از ابتدای زندگی بشر امنیت یکی از دغدغه‌های اصلی انسان‌ها بوده است، امروزه با گسترش اینترنت و فضاهای شبکه‌ای در کشورمان لزوم امنیت برای فعالیت در این فضاهای مجازی بیش از پیش احساس می‌شود. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، و نداشتن امنیت روانی و فرهنگی ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت و فضاهای مجازی واکنشی منطقی است، زیرا هر جامعه‌ای چارچوب‌های اطلاعاتی خاص خود را دارد. طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکنند، می‌تواند سلامت و امنیت جامعه را به خطر اندازد. برخلاف وجود جنبه‌های مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد هنجارشکن، امنیت ملی را در کشورهای مختلف با خطر روبرو ساخته است. از این رو به کارگیری روش‌ها و راه‌کارهای مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. بنابراین با وجود مباحثی بسیاری که شبکه جهانی اینترنت و فضاهای سایبر را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل است. در این پایان‌نامه ابتدا با عناوینی چون امنیت در فضای سایبر و جرائم رایانه‌ای و انواع آن آشنا می‌شویم، و چالش‌ها و راهکارهای مقابله با این چالش‌ها را مرور می‌نماییم.

حریم خصوصی از جمله حقوقی است که انسانها به دلیل نیازهای شخصی از یک طرف به آن وابسته‌اند و از طرف دیگر به دلیل ضرورت زندگی جمعی مکلف‌اند این حق را نسبت به دیگران به رسمیت بشناسند. اما امروزه با گسترش ابزارهای اطلاع‌رسانی

و استفاده گسترده از اینترنت، این حق به یکی از چالش‌انگیزترین مسائل حقوق بشر تبدیل شده است. با توجه به ناشناس بودن کاربران و سهولت استفاده از اینترنت تجاوز به حریم خصوصی افراد به سرعت افزایش یافته و صاحب نظران و دولتمردان را در جهت حمایت از حریم خصوصی افراد سوق داده است.

www.ketab.ir

پیش درآمد

الف) بیان مسئله

حیثیت و آبرو، بارزترین نقطه شخصیت هر فرد در جامعه است چرا که اگر برای زندگی فردی سلامت جان ضروری است برای زندگی جمعی نیز حیثیت باید در حصار صیانت قرار گیرد. حیثیت مقوله ای است که هم در احکام دینی و هم در موازین قانونی چه در سطح ملی و چه در سطح بین المللی مورد توجه و تأکید مکرر بوده است. به زبان ساده می توان گفت؛ حریم خصوصی از آن دسته مفاهیمی است که همه آن را می فهمند و درک می کنند، لیکن نمی توانند تعریفی کامل و جامع از آن ارائه دهند، لذا در بسیاری از موارد نوعی تعارض و حتی جالش در این زمینه مشاهده می شود به طور مثال، زمانی که سخن از نصب دوربین مدار بسته در بعضی از ادارات به میان آمد عده ای مخالف آن طرح بودند و آن اقدام را معارض با صیانت حریم خصوصی افراد می دانستند. چنین اختلاف نظرهایی ناشی از آن است که تعریف اصطلاحی از حریم خصوصی ارائه نشده است. در مجموع می توان اظهار داشت که حریم خصوصی یعنی اینکه؛ خود آزادانه حق داشته باشد که در خلوت خود اطلاعات مربوط به زندگیش را پنهان نموده و بر آن کنترل داشته باشد و مانع از دسترسی دیگران به این اطلاعات گردد. همچنین خودش تصمیم بگیرد که چه وقت و تا چه حدی این اطلاعات را به دیگران منتقل نماید؛ در آموزه های دینی تأیید شده است که فرد برای زندگی خود باید حریم خصوصی داشته باشد و از افشای اطلاع های زندگیش خودداری نماید.

حریم خصوصی یکی از مهمترین مسائل روز جامعه است که از چند نظر قابل بررسی است مثلاً می توان آن را از جانب قربانیان و یا ناقضان حریم خصوصی در فضای مجازی بررسی نمود. همچنین می توان آن را از جانب حامیان خصوصی افراد در این فضا مورد کنکاش قرار داد و از طرف دیگر، راه کارهای بسیاری از متخلفین جرایم سایبری و کسانی

که حریم خصوصی آنان در فضای مجازی نقض می شود؛ استعداد قابل توجهی برای قربانی شدن بروز می دهند و به راحتی طعمه بزه کاران سایبری می شوند. برخی از کلاه برداران اینترنتی به روش های بسیار ساده از اسرار و عکس های شخصی کسب اطلاع نموده و سوء استفاده می کنند. ضعف شخصیتی، فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده ها مواردی هستند که قربانیان جرم سایبری را در بزه دیده شدنشان مساعدت می کند. مطالعه اجمالی قوانین کشورها اهمیت این امر را نشان می دهد به این شرح که دستگاه های تقنینی به رعایت حریم خصوصی و مجازان ناقضان این حریم اهتمام داشته اند. قوانین ایران نیز از این قاعده مستثنی نیست؛ به گونه ای که قانون اسلامی و هم در قوانین عادی به این امر پرداخته شده است. به عنوان مثال، در اصول ۲۳، ۲۲ و ۲۵ قانون اساسی جمهوری اسلامی ایران، هرگونه تعرض به آبرو و جان و مال و حقوق و اطلاعات خصوصی افراد ممنوع اعلام شده است. همچنین قوانین عادی نیز در حمایت از حریم خصوصی و حیثیت افراد و نحوه مجازات افرادی که در امور سمعی و بصری فعالیت های غیر مجاز می نمایند به ماده ۶۴۰ قانون مجازات اسلامی می توان اشاره کرد. طبق قانون مصوب سال ۷۲ عوامل اصلی تولید، تکثیر و توزیع عمده آثار سمعی و بصری مستهجن در مرتبه اول، به یک تا سه سال حبس و ضبط تجهیزات مربوطه و یکصد میلیون ریال جریمه نقدی و در صورت تکرار به دو تا پنج سال حبس و ضبط تجهیزات مربوطه محکوم خواهند شد و در ماده ۶۴۰ نیز برای مرتکبین این جرم حبس و جزای نقدی پیش بینی شده است. در قانون جرایم رایانه ای نیز، در مواد ۱۵، ۱۴، ۲، و ۱۶ و غیره به نحوی بارز نقض حریم خصوصی افراد جرم انگاری شده است. با توجه به حریم خصوصی افراد، حمایت از این حوزه نباید صرفاً به حمایت کیفری محکوم شود؛ بلکه برای تأمین هرچه بیشتر فضای امن شهروندان توجه به حمایت های پیشگیرانه نیاز است در بسیاری از موارد، بدون اینکه به راه کارهای کیفری نیاز باشد راهکارهای پیشگیرانه

مناسبت است. در عصر حاضر، توجه به بزه‌دیده و منافع وی در علوم جنایی از جمله جرم‌شناسی اهمیت قابل توجهی یافته است و این علوم، رویکردی حمایتی نسبت به این کنش‌گران واقعه‌ی کیفری پیدا کرده‌اند. حمایت‌های حقوقی، کیفری، مالی، عاطفی، حیثیتی، پزشکی و اجتماعی از انواع حمایت‌هایی است که از بزه‌دیده می‌شود. بزه‌دیده می‌تواند شخص حقیقی یا حقوقی و بزه‌دیدگان نامعین باشد. انسان نیز طیف گسترده‌ای از اشخاص با وضعیت‌های خاص را در بر می‌گیرد. مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دست‌یابی سریع و آسان به اطلاعات است. کنترل دست‌یابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای (خصوصاً اینترنت)، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی گردیده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند خود، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی را اجرا نماید. نبود نظام مناسب امنیتی، بعضاً پیامدهای منفی و دور از انتظاری را به دنبال دارد. توفیق در ایمن‌سازی اطلاعات، منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است؛ بدین منظور از سرویس‌های امنیتی متعددی استفاده می‌گردد. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص به موقع حملات، و واکنش سریع را داشته باشند. بنابراین می‌توان محور راهبردی انتخاب شده را بر سه مؤلفه حفاظت، تشخیص، و واکنش استوار نمود. حفاظت مطمئن، تشخیص به موقع و واکنش مناسب از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت شود. فضای مجازی یک نوع اجتماع و همسایگی بزرگی است که میلیون‌ها کامپیوتر و استفاده‌کنندگان آن را در سراسر جهان به هم می‌پیوندد. با غلبه اینترنت بر زندگی روزانه‌ی انسانها طبیعی به نظر می‌رسد که بسیاری از

مشخصه های جامعه سنتی به درون اینترنت کشیده شوند و در آنجا شکل گیرند. امروزه ، امور زیادی از قبیل خرید و فروش، تحصیل، مشاوره خانوادگی، ازدواج وحتی مشاوره های پزشکی میان پزشکان و بیماران در اینترنت انجام می گیرد. از این رو هیچ جای تعجبی نیست که مجرمان اینترنتی در فضای مجازی مرتکب جرم شوند. به خصوص گمنامی این فضا بر گسترش این نوع جرایم دامن می زند، در این فضا کمتر هویت واقعی مشخص می شود و افراد باکتمان هویت خویش به راحتی مرتکب انواع جرائم می شوند این پایان نامه دریچه ایست کوچک به معرفی جرم مجازی و عناصر آن و رابطه آن باگمنامی. بشر در طول حیات خود با دوره های گوناگونی از تحول و تکامل مواجه بوده است. زمانی کشاورزی محوریت داشت، اما بشر پس از مدتی به این نتیجه رسید که با تحقق یک جامعه صنعتی می تواند به آرزوهای خود دست یابد. لذا هم خود را در این راه نهاد و دورانی صنعتی را رقم زد که اوج آن را در سده نوزدهم میلادی شاهد هستیم . اما از اواخر قرن بیستم، زمزمه های محوریت یافتن عنصر دیگری شنیده شد . این عنصر که در همان دوران صنعتی واجد ارزش بودن خود را به اثبات رسانیده بود، به تدریج با پا گذاشتن به سده بیستم موقعیت خود را تثبیت کردو تا آنجا پیش رفت که به دوران صنعتی پایان داد و بشر را وارد عصر پسا مدرنی یا پسا صنعتی کرد.(شورای عالی انفورماتیک، شماره ۵۲، ۷۲). این عنصر با ارزش اطلاعات نام دارد و حدود یک قرن است که بشر تلاش خود را صرف تجلی آن در تمامی عرصه های سیاسی، اقتصادی، اجتماعی و فرهنگی کرده است. بی تردید هر کاری ابزاری می خواهد و ابزار تحقق یک جامعه به واقع اطلاعاتی، فناوری اطلاعات و ارتباطات است. دلیل اشاره به عامل ارتباطات در کنار اطلاعات، به لحاظ جایگاه ویژه آن در توسعه و تکامل است. ارتباط و به تبع آن ابزارهای ارتباطی، از همان ابتدا از عناصر حیاتی محسوب می شدند و می توان گفت اگر وجود نداشتند بشر هیچ گاه نمی توانست به این حد از رشد و بالندگی برسد. اوج این رشد و

بالتدگی را می توان در ظهور شبکه های اطلاع رسانی رایانه ای جهانی دانست که از دهه نود میلادی به بعد، تحولی بنیادین را در دو حوزه رایانه و مخابرات رقم زدند. این شبکه ها که خود از بسیاری سیستم های رایانه ای متصل به یکدیگر تشکیل شده اند، به مدد فناوریهای پیشرفته مخابراتی با یکدیگر ارتباط برقرار کرده و فضایی با ویژگی های کاملاً متمایز از دنیای فیزیکی به وجود آورده اند که عده ای آن را فضای مجازی نامیده اند و عده ای هم عنوان فضای سایبر را برای آن برگزیده اند. (جلالی فراهانی، ۱۳۸۳). این فضا، فضای گمنامی است، افراد در آن خود را با حرف معرفی می کنند و کسی به طور حقیقی دیگری را نمیشناسد. افراد در این فضا از طریق شبکه های بین المللی دور هم جمع می شوند، جرم هم یکی از دیده های اجتماعی است و افراد از زمانی که دور هم جمع شده اند جرم نیز با آنان همراه شده است، در این فضا افراد به طور مجازی دور هم جمع می شوند پس می توان حدس زد که این عرصه هم مانند دیگر عناصر زندگی اجتماعی، از گزند این پدیده بسیار انعطاف پذیر و لاینفک اجتماع به نام جرم در امان نمانده است. گرچه فضای سایبر - این پدیده شگفت انگیز قرن بیست و یکم - بسیاری از عرصه ها را با تحولات بنیادین مواجه کرده، سوء استفاده های فراوان از آن موجب پیش بینی تدابیر کیفری در این زمینه شده است. اما با توجه به مشکلات بسیاری که فرا روی تدابیر کیفری وجود دارد، سیاست پیشگیری از وقوع این جرائم مناسب ترین تدبیر سیاست جنایی است. در این میان، پیشگیری وضعی یکی از اقدامات مهم محسوب می شود، اما با محدودیتهایی مواجه است که از جمله آنها نقض موازین حقوق بشر است. ماهیت فضای سایبر به گونه ای است که تجلی هرچه بیشتر آزادی بیان و جریان آزاد اطلاعات را موجب شده و همچنین با امکاناتی که جهت برقراری انواع ارتباطات ایمن فراهم آورده، به نوعی در جهت حفظ حریم خصوصی افراد گام برداشته است. اما تدابیر پیشگیرانه وضعی از جرائم سایبر، عمدتاً به گونه ای اجرا می شوند که این سه اصل حقوق بشری را نقض می کنند. بشر

در طول حیات خود با دوره‌های گوناگونی از تحول و تکامل مواجه بوده است. زمانی کشاورزی محوریت داشت، اما بشر پس از مدتی به این نتیجه رسید که با تحقق یک جامعه صنعتی می‌تواند به آرزوهای خود دست یابد. لذا تمام تلاش خود را در این راه نهاد و دورانی صنعتی را رقم زد که اوج آن را در سده نوزدهم میلادی شاهد هستیم. اما از اواخر این قرن و اوایل قرن بیستم، زمزمه‌های محوریت یافتن عنصر دیگری شنیده شد. این عنصر که در همان دوران صنعتی واجد ارزش بودن خود را به اثبات رسانیده بود، به تدریج با پا گذاشتن به سده بیستم موقعیت خود را تثبیت کرد و تا آنجا پیش رفت که به دوران صنعتی پایان داد و بشر را وارد عصر پسا صنعتی یا پسامدرن کرد. (شورای عالی انفورماتیک، شماره ۵۲: ۷۲). دو فناوری در عرصه فناوری اطلاعات و ارتباطات نقش تعیین کننده ای به عهده داشته اند که عبارت‌اند از: رایانه و مخابرات. هدف از اختراع، تسریع و تسهیل این اطلاعات بود که به خوبی به ثمر نشست و مخابرات نیز به عنوان مهم‌ترین ابزار ارتباطی، در نشر این اطلاعات پردازش شده نقش بسزایی ایفا کرده است. از حدود نیم قرن اخیر، به تدریج با کشف قابلیت‌های شگرف ناشی از تلفیق این دو فناوری، انقلابی در عرصه فناوری اطلاعات و ارتباطات رقم خورد. اوج این انقلاب را می‌توان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که از دهه نود میلادی به بعد، تحولی بنیادین را در این حوزه رقم زده‌اند. این شبکه‌ها که خود از بسیاری سیستم‌های رایانه‌ای متصل به یکدیگر تشکیل شده‌اند، به مدد فناوریهای پیشرفته مخابراتی با یکدیگر ارتباط برقرار کرده و فضایی با ویژگیهای کاملاً متمایز از دنیای فیزیکی به وجود آورده‌اند که عده‌ای آن را فضای مجازی^۱ نامیده‌اند و عده‌ای هم عنوان فضای سایبر^۲ را برای آن برگزیده‌اند.

1 . Virtual Space.

2. Cyber Space.

اما ناگفته پیداست که فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نمانده است. به طور کلی، آنچه امروز تحت عنوان جرم سایبر قرار می‌گیرد، دو طیف از جرائم است: گروه اول جرائمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکاب‌شان را تسهیل می‌کند. جرائم تحت شمول این حوزه بسیار گسترده‌اند و از جرائم علیه امنیت ملی و حتی بین‌المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه اموال و اشخاص را در برمی‌گیرند. نمونه‌ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر جرائم سایبر، به سوء استفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترس غیرمجاز به داده‌ها یا سیستمها یا پنخس برنامه‌های مخرب نظیر ویروس‌ها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرائم سایبری محض^۱ نیز گفته می‌شود. (Casey, 2001: 8)

همان‌گونه که ملاحظه می‌شود، به لحاظ امکان سوء استفاده دوجانبه‌ای که از فضای سایبر وجود دارد، ضروری است برای آن چاره‌ای اندیشه شود. با توجه به رویکرد کلی مقابله با جرائم که در دهه‌های اخیر شاهد تحولات شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد که عبارت‌اند از: اقدامات کیفری و غیرکیفری. در زمینه اقدامات کیفری سعی می‌شود از طریق جرم‌انگاری هنجارشکنی‌ها و سوء استفاده‌های جدید و یا تجدید نظر در قوانین کیفری گذشته، ارباب‌انگیزی مؤثری درباره مجرمان بالقوه یا مکرر صورت گیرد تا به این ترتیب، از ارتکاب جرم بازداشته شوند. (نیازپور، ۱۳۸۲: ۱۲۴) اما رویکرد دوم که در بستر جرم‌شناسی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان‌شناسی، جامعه‌شناسی و غیره پدید آمده، اتخاذ تدابیر پیشگیرانه را در دستور کار خود

قرار داده است. در این زمینه، تاکنون الگوهای مختلفی در عرصه جرم‌شناسی پیشگیرانه ارائه شده و مورد آزمون قرار گرفته است. از مهم‌ترین و مؤثرترین این الگوها می‌توان به پیشگیری اجتماعی^۱ و پیشگیری وضعی^۲ از جرائم اشاره کرد. به طور خلاصه، در پیشگیری اجتماعی سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آنها، به ویژه قشر جوان و نوجوان جامعه، و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم، نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب گردد. اما در پیشگیری وضعی، هدف سلب فرصت و ابزار ارتکاب جرم از مجرم با انگیزه است. (نجفی ابرندآبادی، ۱۳۸۲: ۱۲۰۸) راجع به این مدل که موضوع این تحقیق نیز است، در جای خود بیشتر بحث خواهد شد.

با اینکه اتخاذ تدابیر پیشگیرانه نسبت به اقدامات کیفری از محاسن بسیاری برخوردار است، نباید از یاد برد که در اینجا نیز باید اصول و هنجارها را رعایت کرد. سیاست‌های پیشگیری، به ویژه پیشگیری وضعی، برخلاف سیاست‌های کیفری، تمامی افراد جامعه را دربرمی‌گیرند، زیرا پر واضح است که شناسایی مجرمان بالقوه امکان‌پذیر نیست. لذا این اقدامات باید به نحوی اجرا شوند که افراد جامعه از حقوق اساسی‌شان محروم نگردند. (نجفی ابرندآبادی، ۱۳۸۳: ۵۵۹)

تدابیر پیشگیری وضعی از جرائم سایبر و چالش آنها با رعایت موازین حقوق بشر است. این موضوع از آن جهت مورد توجه قرار گرفته که دو نکته اساسی را می‌توان راجع به فضای سایبر برشمرد: این فضا با امکاناتی که در اختیار مجرمان قرار می‌دهد، از یک سو ارتکاب جرائم را سهل‌تر می‌سازد و نسبت به دنیای فیزیکی خسارات بسیار بیشتری را وارد می‌کند و از سوی دیگر، به لحاظ فرامرزی بودن آن و امکان ارتکاب جرم بدون نیاز

1. Social Prevention

2. Situational Prevention

به حضور فیزیکی مجرمان، تعقیب و پیگرد و در نهایت دستگیری آنها با مشکلات بسیاری همراه شده است. به این ترتیب، پیشگیری از وقوع این جرائم بسیار باصرفه‌تر و کم‌هزینه‌تر از طی فرایند رسیدگی کیفری آنها و تحمل خسارات بی‌شمار است. همچنین نباید از خاطر دور داشت که هدف اصلی از ایجاد فضای سایبر، نزدیک شدن به آرمان‌های جامعه اطلاعاتی است. لذا مبارزه با سوء استفاده‌های این فضا، به هر شکل که باشد، نباید در تحقق این هدف خدشه‌ای ایجاد کند.

در دنیای امروز، آدمی خسته از گشت و گذار عادی و زندگی در کلان شهرهایی مملو از آلودگی‌ها، شلوغی‌ها، معطلی‌ها و خستگی‌ها به دنبال مجالی است که جلوه‌های نشاط و سرزندگی را باز یابد. فناوری اطلاعات و ارتباطات در فضای مجازی، به سوی راحتی بیشتر انسان، تعاملات و ارتباطات روان‌تر، بهتر و سازنده‌تر در اجتماع و ارائه هرچه بهتر خدمات به شهروندان یک جامعه در حرکت است. اما حضور در فضای مجازی برای هر شهروند ایرانی نیاز به آمادگی‌هایی دارد که موارد آن توسط بنیاد IDCL، با سرفصل‌هایی معین تحت عنوان استانداردهای شهروند الکترونیک مشخص شده است. در واقع از چندین سال پیش دولتمردان کشور متوجه نفوذ هراسناک فناوری اطلاعات و ارتباطات در زندگی مردم شدند، آنها دو انتخاب را پیش پای خود می‌دیدند: رفع و مقابله با این فناوری و فرار از پیامدهای نیک و بد آن یا منطبق ساختن شرایط کشور با واقعیت‌های موجود و به کارگیری جنبه‌های مثبت به کارگیری فناوری اطلاعات. طبیعی است که راه دوم، منطقی‌تر و عاقلانه‌تر به نظر می‌رسید. به همین دلیل، سران کشور تصمیم به گسترش کاربردهای مثبت فناوری اطلاعات و ارتباطات در میان مردم گرفتند. (فراهانی جم: ۱۳۸۵)

ب) اهمیت و ضرورت انجام تحقیق

زندگی خصوصی افراد و تأمین امنیت آن توأم با نواقص قانونی و پیشگیری از جرایم این حوزه، ضرورت پرداختن به این موضوع را مشخص می‌کند. حیثیت و آبرو از بارزترین نقطه شخصیت فرد در جامعه است. در بسیاری از متون قانونی و دینی، ارتکاب جرم و حتی قتل برای دفاع از حریم مجازات شمرده شده و دفاع مشروع تلقی شده است. برای بسیاری از افراد، حفظ اسرار و خانوادگی و غیره از مهمترین مسائل زندگی است به گونه ای که موارد بسیاری مشاهده شده است که با آشکار شدن اسرار بعضی اشخاص آنان اقدام به خودکشی نموده اند. به عبارت دیگر، بسیاری از افراد، حفظ و تأمین حریم خصوصی خود را با زندگی حیاتی خود برابر می‌دانند.

ج) اهداف تحقیق

۱. ارائه راه کارهای مناسب در راستای حمایت کیفری از حریم خصوصی
۲. تبیین مفاهیم و مبانی حریم خصوصی در نظام حقوقی ایران
۳. ارائه راهکارهای واکنشی برای حمایت از حریم خصوصی
۴. ارائه راهکارهایی برای بازدارندگی جرم در حوزه حریم خصوصی
۵. شناسایی بیشتر آسیب پذیری حریم خصوصی در فضای مجازی
۶. آسیب شناسی قوانین و مقررات موجود در نظام حقوقی ایران

د) سؤالات تحقیق

۱. دفاع از حریم خصوصی شهروندان در فضای مجازی بیشتر ناظر به چه جرایمی است؟
۲. آیا مجازات های پیش بینی شده برای جرایم ناقض حریم خصوصی در فضای مجازی با شدت جرایم ارتكابی تناسب دارد؟

۳. آیا پیشگیری وضعی در جلوگیری از ارتکاب جرم علیه حریم خصوصی شهروندان امکان پذیر است؟

۴. آیا قوانین و مقررات ایران در زمینه حمایت کیفری از حریم خصوصی در فضای مجازی پاسخگو می باشد؟

ه) فرضیه های تحقیق

۱. دفاع از حریم خصوصی شهروندان در فضای سایبر، سیر ناظر به انتشار فیلم یا تصویر خصوصی یا خانوادگی و اسرار خانوادگی و شخصی است.

۲. با توجه به اهمیت موضوع گاهی قانونگذار مجازات محاربه را برایش پیش بینی نموده است که شدید به نظر می رسد.

۳. استفاده از راهکار هایی همچون نصب دوربین، فیلتر برقی سایت ها، ثبت مشخصات کانل کاربر، در برخی موارد در پیشگیری از جرم می تواند مور باشد.

۴. تصویر برخی متون قانونی در ایران، از جمله قانون جرایم رایانه ای، متأثر از کنوانسیون جرایم سایبر است.