



دانشکده ی حقوق و علوم سیاسی

پایان نامه ی کارشناسی ارشد در حقوق جزا و جرم شناسی

هتک حیثیت اشخاص از طریق افشای سر در محیط مجازی

به کوشش: فرشاد ابراهیمی

استاد: دکتر ابراهیمی

شهریور ۹۱



برای حقوق پدیدآوران

به نام خدا

## اظہارنامہ

اینجانب فرشاد ابراہیمی (۸۸۸۵۵۸) دانشجوی رشته حقوق جزا و جرم شناسی دانشکده ی حقوق و علوم سیاسی اظہار می کنم کہ این پایان نامہ حاصل پژوهش خودم بودہ و در جاهایی کہ از منابع دیگران استفادہ کردہ ام، نشانی دقیق و مشخصات کامل آن را نوشتہ ام. همچنین اظہار می کنم کہ تحقیق و موضوع پایان نامہ ام تکراری نیست و تعہد می نمایم کہ بدون مجوز دانشگاه دستاوردهای آن را منتشر ننمودہ و یا در اختیار غیر قرار ندهم. کلیہ ی حقوق این اثر مطابق با آیین نامہ ی مالکیت فکری و معنوی متعلق بہ دانشگاه شیراز است.

فرشاد ابراہیمی

سرسبزترین بهار، تقدیم تو باد

آوای خوش هزار، تقدیم تو باد

گویند که لحظه ای است رویدن عشق

آن لحظه هزار بار تقدیم تو باد

تقدیم به

عزیزترین کسانم

مادر ارجمندم که نمونه ی والای فداکاری محبت و صبر است و من موفقیت خود

را بیش از هر کس مدیون ایشانم

پدر گرامی ام که نمونه ی بارز یک پدر تلاشگر و مهربان است

و

یگانه خواهر دوست داشتنی ام که همواره پشتیبان و حامی من بوده اند

## سپاسگزاری

«مَنْ لَمْ يَشْكُرِ الْمَخْلُوقَ، لَمْ يَشْكُرِ الْخَالِقَ»

خداوند منان را سپاس می گویم که توفیق به پایان رساندن این جستار را به این جانب عطا نمود. اکنون که کار نگارش و تدوین این پژوهش به انتها رسیده است لازم می دانم تا از تمامی اساتید گرامی که مرا در انجام این مهم یاری و راهنمایی نموده اند تقدیر و سپاسگزاری نمایم. نخست از استاد ارجمند جناب آقای دکتر شهرام ابراهیمی که راهنمایی های مستمر و بی دریغ خود را در طی نگارش این پایان نامه شامل حال من نموده و برای بهبود کیفیت کار تلاش فراوان داشتند سپاسگزاری می نمایم. همچنین ضروری است تا از اساتید محترم مشاور جناب آقایان دکتر محمدصادقی و دکتر فضل الله فروغی که زحمت نظارت بر نگارش و تدوین این پژوهش را بر عهده داشتند و همواره با ارائه ی نظرات ارزشمند و راهنمایی های خویش مرا در هرچه بهتر نمودن این نوشتار یاری نمودند تشکر و قدردانی نمایم. امید است در پرتو عنایت الهی سعادت مند و پیروز باشند.

## چکیده

### هتک حیثیت اشخاص از طریق افشای سر در محیط مجازی

#### به کوشش: فرشاد ابراهیمی

گرچه تصور حیات بشر خارج از اجتماع دور از ذهن می نماید اما بی تردید هر انسان دارای یک بعد وجودی از حیات فردی نیز می باشد. در این عرصه هر شخص دارای خطوط قرمزی است که دست یابی دیگران را بر آن بر نمی تابد. اسرار شخصی و حریم خصوصی افراد از جمله ی این محدوده های ممنوعه به شمار می روند. در حقوق جزای مدرن کنونی نیز تجاوز به این امور، مورد عنایت مقنن کیفری قرار گرفته و افشای اسرار خصوصی به عنوان یکی از جرایم علیه تمامیت معنوی جرم انگاری گردیده است.

از سویی، رشد چشمگیر تکنولوژی و به کارگیری آن در تمام شئون حیات بشری، سبب گردیده تا امکان دست یابی به نهانی های افراد و انتشار و افشای آن برای دیگران، فراهم گردد. لذا در کنار جرم انگاری رفتارهای مجرمانه ای که ممکن است بوسیله ی رایانه و از طریق فضای مجازی ارتکاب یابند، پیش بینی بزه افشای سر در محیط سایبری نیز مطمح نظر قانون گذار کیفری ایران بوده است. می توان گفت به واسطه ی ویژگی های فضای مجازی و دیجیتال، ابعاد ارتکاب این بزه به شکل رایانه ای بسی وسیع تر از ارتکاب آن به شکل سنتی است.

در این نوشتار پس از آشنایی مختصر با فضای سایبر، به بررسی ارزش و جایگاه حریم خصوصی، اسرار و اهمیت آن در طول تاریخ و در ادیان مختلف پرداخته شده است. همچنین ضمن مقایسه ی بزه افشای اسرار با دیگر عناوین مجرمانه و با شناسایی ارکان جرم مورد اشاره، به طور دقیق کلیه ی اجزای تشکیل دهنده ی این بزه بازشناسی شده و شرایط ضروری در تحقق جرم به تفصیل احصا گردیده است. نهایتاً تدابیری که مقنن کیفری در قبال این جرم اندیشیده است را تبیین نموده و نقاط قوت و ضعف قانون گذاری در این خصوص بیان شده و راهکارهایی برای پیشگیری از ارتکاب این جرم ارائه گردیده است.

کلمات کلیدی: فضای سایبری، حریم خصوصی، افشاء، هتک حیثیت، انتشار، دست یابی، اسرار

## فهرست مطالب

فصل اول: شناسایی مفاهیم کلی.....	۱
مقدمه.....	۲
مبحث اول - محیط مجازی.....	۶
گفتار اول - شناسایی محیط مجازی.....	۷
بند اول - تعریف محیط مجازی.....	۸
بند دوم - اینترنت و دیگر شبکه های رایانه ای.....	۱۰
گفتار دوم - مزیت ها و چالش های محیط مجازی.....	۱۲
بند اول - مزایای محیط مجازی.....	۱۲
بند دوم - چالش های محیط مجازی.....	۱۵
مبحث دوم - مفهوم حریم خصوصی و اهمیت آن.....	۱۷
گفتار اول - مفهوم لغوی و اصطلاحی حریم خصوصی، افشای سر و هتک حیثیت.....	۱۸
بند اول - مفهوم لغوی.....	۱۹
بند دوم - مفهوم اصطلاحی.....	۲۰
گفتار دوم - اهمیت حریم خصوصی در اسلام و دیگر مکاتب.....	۲۳
بند اول - سابقه ی توجه به موضوع حریم خصوصی.....	۲۳
بند دوم - حریم خصوصی در اسلام.....	۲۶
مبحث سوم - شناسایی مفهوم هتک حیثیت و افشای سر و مقایسه آن با دیگر عناوین.....	۲۸
گفتار اول - شناسایی مفهوم هتک حیثیت از طریق افشای سر.....	۲۸
بند اول - اسرار و تأکید بر حفظ آن در اسلام.....	۲۹
بند دوم - بزه افشای سر در حقوق ایران.....	۳۱
گفتار دوم - مقایسه ی بزه افشای اسرار با دست رسی غیر مجاز.....	۳۴
بند اول - مفهوم دست یابی غیر مجاز.....	۳۵
بند دوم - جهات اشتراک و افتراق افشای سر و دست یابی غیر مجاز.....	۳۷
گفتار سوم - مقایسه ی افشای سر با جاسوسی رایانه ای.....	۴۰
بند اول - شناسایی بزه جاسوسی رایانه ای.....	۴۰



- بند دوم - جهات اشتراک و افتراق افشای سر با جاسوسی رایانه ای ..... ۴۳
- گفتار چهارم - مقایسه ی افشای سر و نشر اکاذیب ..... ۴۶
- بند اول - باز شناسی نشر اکاذیب ..... ۴۶
- بند دوم - تشابه و تمایز نشر اکاذیب با افشای سر ..... ۴۸

## فصل دوم: ارکان تشکیل دهنده ی بزه هتک حیثیت از طریق افشای سر در محیط

- مجازی ..... ۵۰
- مبحث اول - رکن قانونی ..... ۵۱
- گفتار اول - قوانین و مقررات مرتبط ..... ۵۱
- بند اول - مقررات اسناد بین المللی ..... ۵۲
- بند دوم - قوانین و مقررات داخلی ..... ۵۴
- گفتار دوم - باز شناسی جایگاه قوانین حاکم ..... ۵۹
- بند اول - قانون تجارت الکترونیک ..... ۶۰
- بند دوم - قانون امور سمعی و بصری ..... ۶۳
- بند سوم - قانون جرایم رایانه ای ..... ۶۵
- مبحث دوم - رکن مادی ..... ۶۷
- گفتار اول - مرتکب و رفتار مجرمانه ..... ۶۷
- بند اول - مرتکب جرم ..... ۶۸
- بند دوم - رفتار مجرمانه ..... ۶۹
- گفتار دوم - موضوع جرم و شرایط ضروری برای تحقق بزه ..... ۷۲
- بند اول - موضوع جرم ..... ۷۲
- بند دوم - شرایط ضروری در تحقق جرم ..... ۷۴
- گفتار سوم - نتیجه ی حاصل از جرم ..... ۷۷
- بند اول - مطلق یا مقید بودن بزه موضوع ماده ی ۱۷ ..... ۷۸
- بند دوم - شروع به جرم ..... ۸۰
- مبحث سوم - رکن روانی ..... ۸۳
- گفتار اول - علم مرتکب ..... ۸۳
- بند اول - علم حکمی ..... ۸۴
- بند دوم - علم موضوعی ..... ۸۵

گفتار دوم - قصد مجرمانه..... ۸۷

بند اول - قصد ارتکاب رفتار مجرمانه (سوء نیت عام)..... ۸۷

بند دوم - قصد تحقق نتیجه ی مجرمانه (سوء نیت خاص)..... ۸۹

## فصل سوم: واکنش قانون گذار در قبال جرم هتک حیثیت از طریق افشای سر در

محیط مجازی..... ۹۱

مبحث اول - واکنش های کیفری..... ۹۲

گفتار اول - مجازات اصلی..... ۹۲

بند اول - مجازات اشخاص حقیقی..... ۹۲

بند دوم - مجازات اشخاص حقوقی..... ۹۴

گفتار دوم - مجازات های تبعی و تکمیلی..... ۹۶

بند اول - مجازات تبعی..... ۹۷

بند دوم - مجازات تکمیلی..... ۹۹

گفتار سوم - مجازات شریک و معاون در جرم و موارد تشدید مجازات..... ۱۰۱

بند اول - مجازات شریک و معاون در بزه..... ۱۰۱

بند دوم - موارد تشدید مجازات..... ۱۰۴

مبحث دوم - تدابیر غیر کیفری..... ۱۰۶

گفتار اول - پالایش محتوای مجرمانه..... ۱۰۶

بند اول - تکلیف ارائه دهندگان خدمات دسترسی و میزبانی..... ۱۰۷

بند دوم - موارد پالایش محتوای مجرمانه..... ۱۰۹

گفتار دوم - تدابیر مبتنی بر رفتار بزه دیده و بزهدار..... ۱۱۰

بند اول - چگونه از بزه دیده شدن بپرهیزیم؟..... ۱۱۱

بند دوم - تدارک برنامه هایی جهت فرهنگ سازی..... ۱۱۳

نتیجه گیری..... ۱۱۵

فهرست منابع و مآخذ..... ۱۲۰

## فهرست نشانه های اختصاری

- ا.ح.ق. - اداره حقوقی قوه قضائیه
- ق.م. - قانون مدنی
- ق.م.ا. - قانون مجازات اسلامی
- ق.ت.ا. - قانون تجارت الکترونیک
- ق.ا.س.ب. - قانون امور سمعی و بصری

# شناسایی مفاهیم کلی

## مقدمه

هزاران سال است که بشر در این کره ی خاکی زندگی می کند و همواره نیز رو به سوی آینده ای متحول دارد. با این حال شاید طی سال های متمادی زندگی انسان تحول آرامی داشته است تا آن هنگام که با شروع نهضت های روشن فکری پس از قرون وسطی دریچه ای روشن به روی او گشوده شد. انسان عصر جدید توانست با گشودن غل و زنجیرهای خرافه پرستی و توهم از دست و پای خویش، با سرعتی خیره کننده به سوی کشف مکنونات کاینات حرکت کند. در سده ی ۲۰، با پدید آمدن سیستم های رایانه ای، گویی آدمی بر اریکه ی قدرت تکیه زد تا بر تمام هستی فرمان براند. توفیق بشر در زمینه ی طراحی شبکه های رایانه ای محلی و سپس توسعه ی آن در سرتاسر جهان، یک گام دیگر او را به آمال دیرینه ی خود نزدیک تر کرد. از این زمان بود که جهش های علمی عمده ای در تاریخ بشر متبلور گردید. چراکه دست یابی به دست آوردهای علمی بشری بسی آسان گردید. از این رو می توان پیدایش سیستم های رایانه ای و اینترنتی را رنسانس دوم بشر نام نهاد.

با این حال توسعه ی روز افزون استفاده از سیستم های رایانه ای در زندگی بشر، مدینه ی فاضله ای را برای او به ارمغان نیاورد. گرچه به کارگیری رایانه و اینترنت تا حد زیادی توانست سرعت، دقت و سهولت کارها را افزون کند، اما گسترش پدیده ای به نام اینترنت، از میزان ارتباطات مستقیم افراد با یکدیگر به شدت کاست. هرکس به راحتی و با کمک یک رایانه ی شخصی، می تواند گام به عرصه ی محیطی بگذارد که در عین عظمت و گستردگی غیر قابل تصور خود، عملاً فاقد واقعیت مادی و خارجی است. در چنین محیطی می توان تصور کرد که زمان، مکان، ماده و جسم، بی معناست. افرادی که در این محیط حضور دارند نیز، علیرغم دارا بودن هویت الکترونیک، اما فاقد هویتی عینی و ملموسند. به طور کلی می توان گفت که فضای مجازی، محیطی است با افرادی موهوم که در بند زمان و مکان مقید نمی گردند.

این ویژگی محیط مجازی، این امکان را فراهم می آورد تا ابنای فرصت طلب بشر، فرصت بیابند تا با استفاده از هویت موهوم خود دست به رفتارهایی بزنند که دربر دارنده ی

عصر نقض حقوق خصوصی و عمومی است. اینجاست که حقوق کیفری قدم به میدان گذاشته و با توسل به مجازات، راه را بر رفتارهای مخل نظم و آسایش عمومی و خصوصی می بندد. همان گونه که امروزه صور استفاده از رایانه و اینترنت در زندگی روزمره بسیار متنوع و متکثر گردیده است، توسل به این ابزار برای لطمه زدن به فرد و اجتماع نیز به نحو غیر قابل باوری توسعه یافته است. انواع جرایم مالی، توهین و افترا، نشر اکاذیب، هرزه نگاری (پورنوگرافی)، ایجاد پایگاه های اینترنتی غیر اخلاقی، ورود غیر مجاز به پروفایل های شخصی، طراحی و انتشار ویروس ها و کرم های رایانه ای و ... همه از جمله رفتارهای نابهنجاری هستند که می توانند وصف مجرمانه داشته باشند.

از این میان هتک حیثیت اشخاص در محیط مجازی نیز یکی از پدیده هایی است که اخیراً به شکل گسترده ای رخ می دهد. انتشار تصاویر خصوصی و خانوادگی، افشای اسرار دیگران و هرگونه رفتاری که شخصیت و وجهه ی فردی و اجتماعی افراد را مخدوش کند، می تواند لطمات جبران ناپذیری را بر هر انسانی وارد کند. چه بسا یک فرد بر اثر انتشار یک عکس از خود یا خانواده اش، آنچنان متأثر گردد و دست به اقداماتی بزند که خود یا دیگران را در معرض خطر قرار دهد. همچنان که ممکن است چنین فردی دچار مرگ مدنی شده و تا پایان عمر نتواند به زندگی عادی خود باز گردد. از این رو عنوان این پژوهش را "هتک حیثیت اشخاص از طریق افشای سر در محیط مجازی" برگزیدیم تا با تأمل در این مورد بتوانیم گوشه ای تاریک از حقوق کیفری محیط سایبری را مورد کنکاش قرار داده و مطالبی هرچند اندک در این خصوص به رشته ی تحریر درآوریم.

## سؤالات تحقیق

همچنان که از عنوان پایان نامه برمی آید، موضوع پژوهش دربر دارنده ی چند قسمت است، لذا قلمرو کار در این نوشتار به شرح زیر مشخص می گردد:

۱) شناسایی محیط مجازی. ۲) شناسایی مفهوم هتک حیثیت. ۳) تعیین ارکان این بزه. ۴) چگونگی ارتکاب این جرم از طریق افشای سر.

لذا می توان گفت پرسش اصلی در این تحقیق آن است که: "مفهوم و ماهیت هتک حیثیت از طریق افشای سر در محیط مجازی چیست؟ این پرسش، خود سؤالات دیگری را متبادر به ذهن می کند: ماهیت محیط مجازی چیست؟ مفهوم هتک حیثیت چیست؟ وجه ممیزه ی هتک حیثیت از دیگر عناوین مجرمانه کدام است؟ ارکان تحقق بزه هتک حیثیت در محیط مجازی کدامند؟ منظور از اشخاص بزه دیده در این جرم چه کسانی هستند؟ واکنش کیفری در قبال این بزه چگونه است؟ و ... لذا مطالب مطروحه در این نوشتار را می توان در سه فصل ارائه نمود: شناسایی مفاهیم کلی (فصل اول) و بررسی ارکان تشکیل دهنده ی بزه هتک حیثیت در محیط مجازی (فصل دوم) و پاسخ های قانون گذار به جرم هتک حیثیت در محیط مجازی (فصل سوم)

## سابقه ی تحقیق

با توجه به گسترش روز افزون کاربرد رایانه و اینترنت در زندگی بشر امروز، مسائل حقوقی متعددی پیرامون این پدیده ی نوظهور مطرح گردیده و هریک نیز مورد مذاقه و توجه بسیاری از حقوقدانان قرار گرفته است. از مسائل مربوط به تجارت الکترونیک گرفته تا جرایم ممکن الوقوع در محیط مجازی.

کتاب ها و مقالات متعددی در زمینه ی حقوق محیط سایبر به رشته تحریر در آمده است. از جمله کتب حقوقی که در این خصوص تألیف گردیده است می توان به کتاب "بررسی فقهی حقوقی جرایم رایانه ای" تألیف حسین علی بای و بابک پورقهرمانی اشاره کرد. همچنین آقای برومند باستانی کتابی را با مقدمه ی استاد گرامی دکتر آشوری تحت عنوان "جرایم کامپیوتری و اینترنتی، جلوه ای نوین از بزهکاری" به رشته ی تحریر درآورده است. از دیگر کتب مرتبط با این موضوع می توان به "جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل" تألیف کامران شیرزاد نیز اشاره نمود. همچنین مقالات متعددی پیرامون مسأله ی محیط سایبر گردآوری و تدوین شده است که از جمله "جرایم سایبری" نگاشته ی محمدحسن دزیانی، "پیشگیری وضعی از جرایم سایبر" اثر امیرحسین جلالی فراهانی، "توسعه ی شبکه ی ملی دیتا، چالش های فرارو و ..." نوشته ی دکتر ابراهیم حسن بیگی، "حقوق

فناوری اطلاعات و ارتباطات" اثری از فرهاد شمس و بسیاری از کتب و مقالات دیگر را می توان نام برد. همچنان که در خصوص موضوع مورد بحث ما گرچه به صورت پراکنده و ضمن بحث از برخی جرایم نظیر توهین و دیگر جرایم سایبری مطالبی نگاشته شده است اما با این حال تا کنون در هیچ یک از منابع حقوقی به طور اختصاصی بحثی راجع به هتک حیثیت در محیط مجازی، آن هم از طریق افشای سر مطرح نگردیده است. در واقع شناسایی دقیق عناصر و ارکان این بزه تا کنون مطمح نظر حقوقدانان نبوده است. از این رو، انجام یک پژوهش آکادمیک که صرفاً بر این موضوع متمرکز گردد، خالی از فایده نخواهد بود.

## هدف

آنچه ما در این تحقیق در پی آنیم روشنگری در خصوص این مطلب است که هتک حیثیت و آبروی اشخاص در محیط مجازی در نظام حقوقی ما چه جایگاهی دارد؟ آیا اساساً این قبیل اقدامات جرم انگاری شده است یا خیر؟ در صورت مثبت بودن پاسخ، مستند قانونی ما چیست؟ آیا با توسل به قانون جرایم رایانه ای می توان تمامی مصادیق هتک حیثیت را مجازات کرد؟ یا این که باید برای مجازات چنین رفتارهایی در پی مستندات قانونی دیگر بود؟ تعارضات و هم پوشانی های احتمالی که در قانون جرایم رایانه ای با سایر قوانین در این خصوص وجود دارد چگونه قابل جمع اند؟ آیا قوانین ما در این زمینه از جامعیت برخوردارند یا نیازمند فرایند قانون گذاری جدیدی هستیم؟ این ها و ده ها پرسش دیگر، انگیزه ای بود تا موضوع این پایان نامه را به هتک حیثیت اختصاص دهیم. لہذا هدف اصلی ما از این پژوهش، پاسخ به پرسش ها و ابهاماتی است که در مورد این بزه وجود دارد. می توان گفت هدف از انجام چنین پژوهشی آن است که راهکارهایی ارائه گردد تا اولاً در فرایند قانون گذاری و جرم انگاری رفتار مجرمانه، بهترین روش و مؤثرترین تدابیر در پیش گرفته شود و وصف باز دارندگی قانون تا حد امکان تأمین گردد ثانیاً در بعد فرا کیفری، با بیان راهکارهای جرم شناسانه در خصوص انواع روش های پیش گیری از ارتکاب این بزه نرخ ارتکاب جرم تا حد امکان تقلیل یابد.

## مراحل سازماندهی

همانگونه که از عنوان پژوهش برمی آید، این تحقیق را می توان از زمره تحقیقات توصیفی-تحلیلی به شمار آورد. چراکه در خلال بحث ها بیشتر در پی شناسایی ارکان و عناصر تشکیل دهنده ی بزه هتک حیثیت هستیم. بنابر این پژوهش ما در چهارچوب حقوق جزای اختصاصی می گنجد. روش انجام تحقیق، اصولاً کتاب خانه ای است. در این خصوص تلاش می گردد تا از تمامی منابع و مراجع موجود که حد اقلی از ارتباط را با موضوع دارند نیز استفاده گردد. در این میان استفاده از منابع اینترنتی نیز اجتناب ناپذیر است. مضافاً به این که در طی ارائه ی مطالب، تا جایی که مقدور باشد با ارائه ی نمونه هایی از پرونده های کیفری مربوط به جرایم رایانه ای که در محاکم جزایی مطرح گردیده است، می کوشیم به این پژوهش جنبه ی عینی و میدانی نیز داده شود.

لذا مطالب این نگاره را طی سه فصل ارائه خواهیم نمود. در فصل اول به مطالعه و ارزیابی مفاهیم کلی، که در پژوهش ما محوریت دارند خواهیم پرداخت. در فصل دوم به طور خاص و جزئی تمامی ارکان و اجزای متشکله ی جرم موضوع مطالعه ی خود را بازشناسی خواهیم نمود و سر انجام، در فصل سوم واکنش هایی که قانون گذار در قبال این جرم اتخاذ نموده است را از نظر خواهیم گذراند.



## مبحث اول: محیط مجازی

مقوله‌ی جرایم رایانه‌ای و سایبری چندی است که ذهن علمای حقوق جزا را به خود مشغول کرده است. هر یک از بزرگان این عرصه به نوبه‌ی خود در این خصوص قلم فرسایی کرده و گوهرهای یگانه‌ای از دانش خویش متبلور ساخته‌اند که چراغ راه پویندگان طریق دانش و ارباب سیاست و قانون‌گذاری در این خصوص گردیده است. پژوهش حاضر نیز با الهام از آراء و نظرات بزرگان این عرصه در پی آن است تا بخشی هرچند کوچک از این پهنه‌ی وسیع را واکاوی کند.

موضوع این جستار، «هتک حیثیت افراد از طریق افشای سر در محیط مجازی» برگزیده شد. لذا به فراخور امر، در آغاز بحث ضروری است تا با طرح مفاهیم بنیادی مرتبط با موضوع، زمینه‌ی ورود به مباحث اصلی ایجاد گردد. از این رو در فصل اول - به شیوه‌ی مرسوم در نگاشته‌های اکادمیک - مسائل ساختاری تحقیق برشمرده شده و پیرامون هریک مطالبی ارائه می‌گردد.

در مبحث نخست، با عنایت به قلمرو موضوعی تحقیق که جرایم سایبری است، به شناسایی محیط سایبری می‌پردازیم. سپس در مبحث دوم، نکاتی در مورد حریم خصوصی، اهمیت و جایگاه آن بیان می‌نماییم. نهایتاً در مبحث سوم در پی آنیم تا نکاتی مقدماتی در خصوص بزه افشای سر در محیط مجازی ارائه کنیم تا زمینه‌ی ورود به فصول بعد مهیا گردد.

همانگونه که از عنوان این پژوهش برمی آید، چارچوب مطالعاتی ما محدود به یک بزه در محیط مجازی است. محیط مجازی که معادل آن را Cyber Space می دانند، پدیده ای نسبتاً نوظهور است. پیدایش این مفهوم به اواخر سده ی ۲۰ برمی گردد. از این رو برای تمهید مقدمات آغاز سخن، در این مبحث مطالبی پیرامون مفهوم و تاریخچه ی پیدایش محیط مجازی ذکر می شود.

## گفتار اول: شناسایی محیط مجازی

شاید بتوان رایانه را یکی از بزرگ ترین اختراعات بشری دانست. چرا که در تمام جنبه های زندگی انسان مدرن مانند جراحی های حساس، آموزش دوره های پیشرفته ی علوم، ارائه ی خدمات بانکی و اعتباری، آزمایش های حساس هسته ای و ... تأثیر داشته است. مزایای این فنآوری توانایی بشر را گسترش داده و به او در دست یابی و گسترش، ذخیره سازی، بازیابی، پردازش، به کارگیری و ایجاد اطلاعات با سرعت و در حجم باورنکردنی یاری می رساند. پایگاه های داده (دیتابیس) به طور روز افزون برای ذخیره ی انواع اطلاعات محرمانه سیاسی، اجتماعی و اقتصادی مورد استفاده قرار دارد. از سویی فنآوری اطلاعات و ارتباطات اصول اخلاقی را که بر اساس باورهای رفتاری و استانداردهای درست و نادرست و عادات اجتماعی شکل می گیرد، تغییر می دهد و شخصیت های جدید، گروه های سازمانی، اجتماعی و اقتصادی را پدید آورده است. این تحول شگرف در حیات بشر امروز را می توان به عنوان انقلاب فنآوری اطلاعات و ارتباطات نام نهاد. این دگرگونی، دیدگاه ما را نسبت به جهان پیرامون خود متحول کرده و جهان را به معنای واقعی کلمه تبدیل به دهکده ی جهانی اطلاعات کرده است. این جامعه ی بسیار وسیع اما در عین حال فشرده و قابل دسترس در هر آن، در مسیر حرکت به سمت نوعی آگاهی همگانی به پیش می رود. این حرکت ناخودآگاه جامعه ی جهانی به سوی

به کار گیری فناوری در تمام شئون زندگی، انسان را در برابر پدیده ای نوین قرار داده است که همان مفهوم "محیط مجازی یا سایبر" است. در قلمرو محیط سایبر کاربران که تشکیل دهنده ی پیکره ی جامعه ی مجازی هستند، آزاد هستند تا به هر سیستمی که با این محیط در ارتباط است متصل شده، از آن خدمات بگیرند و یا هر زمان که مایل باشند اتصال خود به آن را پایان دهند. از این رو می توان گفت محیط سایبر، یک فضای شناور است که در هر لحظه به گونه ای دیگر تغییر شکل می دهد.<sup>۱</sup> لذا باید ابتدا با مفهوم محیط سایبر یا مجازی آشنا گردیم.

## بند اول: تعریف محیط مجازی

از لحاظ لغوی در فرهنگ های مختلف Cyber به معنای مجازی و غیر ملموس و مترادف لغت Virtual می باشد.<sup>۲</sup> در برخی از فرهنگ های کامپیوتری به مجموعه ای از کامپیوترهای بزرگ یا ابر رایانه ها که توسط شرکت کنترل دیتا ساخته شده اطلاق شده است.<sup>۳</sup> البته با توجه به بسط مفهومی اصطلاح سایبر و اطلاق آن به تمام افعال و اقدامات در محیط شبکه های بین المللی و بی شمار بودن مصادیق آن، برخی<sup>۴</sup> معتقدند که یافتن اصطلاح معادل و نیز ترجمه آن به هر زبانی صحیح نیست. ایشان معتقدند که به لحاظ توسعه ی قلمرو کاربردی مفهوم سایبر، این لغت عملاً تبدیل به یک لغت بین المللی شده و لذا ترجمه کردن یا معادل سازی آن، ممکن است موجب محدودیت در قلمرو شمول این عنوان گردد. با این حال عدم ارائه ی تعریف و تبیین از مفهوم سایبر نیز خود باعث ایجاد ابهام و نابسامانی در تدوین اصول و مقررات حاکم بر این محیط می گردد. بنابر این ناگزیر از بیان معنای این اصطلاح هستیم.

اصطلاح فضای سایبر (cyber space) یا فضای هدایت شده، که برای اولین بار در سال ۱۹۸۲ در یک داستان علمی تخیلی به کار گرفته شد، به چند صورت مورد تعریف قرار گرفته است.<sup>۵</sup> از جمله:

---

<sup>۱</sup> ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، دادرسی، ماهنامه ی شماره ی ۷۷، سال سیزدهم، آذر و دی ۸۸، ص ۱۰.

<sup>۲</sup> باستانی، برومند، جرایم کامپیوتری و اینترنتی: جلوه ای نوین از بزهکاری، انتشارات بهنامی، تهران، ۱۳۸۳، ص ۶۳

<sup>۳</sup> بای، حسینعلی و بابک پورقهرمانی، بررسی فقهی حقوقی جرایم رایانه ای، پژوهشگاه علوم و فرهنگ اسلامی، قم، ۱۳۸۸، ص ۲۰.

<sup>۴</sup> باستانی، برومند، منبع پیشین.

<sup>۵</sup> مسعودی، امید، امنیت اطلاعات در فضای سایبر، کتاب ماه، کلیات، دی ۱۳۸۳، ص ۱۶.

- ۱- سایر اسپیس (محیط مجازی) مجموعه ی به هم پیوسته ای از موجودات زنده از طریق کامپیوتر و ارتباطات راه دور بدون در نظر گرفتن جغرافیای عینی آن هاست.
  - ۲- سایر اسپیس به تمام محیط هایی مانند اینترنت اطلاق می شود که در آن اشخاص به وسیله ی کامپیوترهای متصل به یکدیگر، با هم تعامل و تبادل دارند.<sup>۶</sup>
  - ۳- سایر اسپیس اثر فضا و اجتماع شکل گرفته توسط کامپیوتر و شبکه های کامپیوتری و کاربران است. یعنی دنیایی غیر ملموس که وقتی کاربران رایانه برخط (online) هستند به آن موجودیت می دهند.<sup>۷</sup>
  - ۴- محیط سایبری توهم و تصور باطل توافقی است که انسان ها خلق کرده اند.
  - ۵- محیط مجازی یک ناحیه ی واقعی است که فعالیت هایی در آن اتفاق می افتد مانند تبادل و جمع اطلاعات.
  - ۶- سایر جایی است که شما زمانی که با تلفن صحبت می کنید در آنجا هستید.
- از دقت در تعاریف فوق می توان نتیجه گرفت که در بیان مفهوم فضای سایر چند عامل، اساسی هستند: سیستم های رایانه ای (اعم از کامپیوتر، تلفن، رسانه ها و ...)، کاربران و اطلاعات. مفهوم رایانه تنها گزینه هایی که ذهن ما به آن معطوف می شود را در بر نمی گیرد، بلکه همانطور که کنوانسیون بین المللی جرایم سایبر مصوب ۲۰۰۱ در بند الف ماده ۱ اشاره کرده است: «سامانه ی رایانه ای یک دستگاه یا مجموعه ای از دستگاه های متصل به هم یا مرتبط با هم است که به وسیله ی یک برنامه، داده های دیجیتال را به طور خودکار پردازش می کند». حوزه ی شمول سیستم رایانه ای گسترده است و سامانه های مخابراتی، دستگاه هایی که برنامه ای داشته باشند را در برمی گیرد، مانند تلفن های همراه، تلفن های ثابت حافظه دار و ...<sup>۸</sup>. بنا بر این می توان محیط مجازی (سایبر) را چنین تعریف کرد: محیط شکل گیری ارتباط کاربران - که موجوداتی عینی یافته اند - از طریق سیستم های رایانه ای - و نه فقط کامپیوتر - که در نتیجه ی تحقق چنین فضایی اطلاعات - دیتا - مابین کاربران به گردش در می آید. در این محیط اشیاء و اطلاعات به صورت فیزیکی و ملموس وجود ندارد و در واقع

<sup>۶</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، ص ۲۱.

<sup>۷</sup> به نقل از برومند باستانی، منبع پیشین، صص ۶۳-۶۴.

<sup>۸</sup> ترکی، غلام عباس، منبع پیشین، صص ۱۰-۱۱.

آنچه عینیت می یابد، موضوعات مجازی هستند که به شکل دیجیتالی (رقومی) وارد شبکه شده است.

از مطالب فوق الذکر مشخص می شود که مفهوم شبکه در تحقق فضای مجازی نقش عمده ای دارد. از میان شبکه های مجازی و رایانه ای موجود در دنیا، اینترنت را می توان به عنوان بزرگ ترین و مهم ترین آنها نام برد. از این رو در ادامه مختصری راجع به این شبکه ها مطالبی خواهد آمد.

## بند دوم: اینترنت و دیگر شبکه های رایانه ای

اصطلاح internet مرکب از دو لفظ "inter" به معنای میانی، واسطه ای و مرتبط کننده و "net" به معنای شبکه است. بنابر این internet عبارت است از مجموعه ی شبکه های کامپیوتری که از طریق TCP/IP با یکدیگر در ارتباطند. مسائل مربوط به جزئیات TCP/IP کاملاً جنبه ی فنی داشته و ضرورتی به طرح بحث در این نوشتار نمی باشد، تنها کفایت که بدانیم IP دروازه های ارتباطی شبکه ی جهانی (internet) هستند که کار آنها انتقال و تبدیل داده ها از شبکه ی فرستنده به شبکه ی دریافت کننده می باشد.

در سال ۱۹۶۹ شبکه ی غیر متمرکزی توسط وزارت دفاع ایالات متحده برای ایجاد تسهیلات مخابراتی به هنگام وقوع یک فاجعه ی اتمی ایجاد گردید. به تدریج چند شبکه ی محلی دیگر نیز به این شبکه متصل شدند و بدین ترتیب اینترنت از بطن فعالیت های نظامی امریکا پدیدار شد<sup>۹</sup>. از این زمان به بعد بود که شبکه های رایانه ای این قابلیت را یافتند تا علاوه بر امور نظامی در سایر زمینه های زندگی انسان متمدن به کار گرفته شوند. عرصه های علمی و دانشگاهی، اقتصادی و تجاری، فرهنگی و اجتماعی نیز به سرعت به تسخیر رایانه درآمدند تا جایی که امروزه تقریباً هیچ گوشه ای از زندگی را نمی توان یافت که با رایانه و اینترنت در تعامل و ارتباط نباشد.

<sup>۹</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۱۷-۱۸

در مقابل اینترنت، اینترانت (intranet) قرار دارد که عبارت است از شبکه ای رایانه ای که برای پردازش اطلاعات و داده ها در یک شرکت یا سازمان طراحی شده است. این شبکه از این رو اینترانت نام دارد که در آن امکانات موجود در فضای مجازی اینترنت - از قبیل صفحات وب، پست الکترونیک، گروه های خبری و لیست های پستی - فقط برای کاربران داخلی سازمان قابل دسترس است.

در کنار اینترانت (شبکه ی داخلی)، اکسترانت قرار دارد. این سیستم که مبتنی بر همان اصول و قواعد حاکم بر فضای اینترنت ایجاد می گردد، این امکان را فراهم می آورد تا کاربرانی غیر از اعضای سازمان مربوطه بتوانند به برخی بخش های یک شبکه ی درون سازمانی دسترسی داشته باشند<sup>۱۰</sup>

به طور کلی می توان گفت عمده ترین بخش فضای مجازی را باید شبکه های رایانه ای دانست. این شبکه ها پیوند دهنده ی سیستم های کامپیوتری به یکدیگرند. این پیوند به اشکال مختلف ایجاد می شود. ممکن است یک خط تلفن معمولی باشد یا فیبر نوری و لیزری و یا حتی ماهواره های مخابراتی. امواج ماکرو ویو و رادیویی نیز در توسعه ی محیط مجازی نقش عمده ای دارند.<sup>۱۱</sup>

در کنار شبکه های رایانه ای که بعد جهانی دارند، ایجاد فضای مجازی در مقیاس کوچک تر نیز کاملاً قابل تصور است. به عنوان مثال، امروزه تجهیز تلفن های همراه به فناوری بلوتوث این امکان را برای دارندگان آن فراهم کرده است تا به راحتی داده های ذخیره شده در حافظه های الکترونیکی گوشی خود را با سهولت و سرعتی باور نکردنی در اختیار دیگران قرار دهند. همین امر موجب شده تا در کنار فضای سایبری جهانی بتوان از فضای سایبری نقطه ای نیز یاد کرد. به هر روی محیط مجازی در هر مقیاسی که تصور گردد دارای ویژگی هایی است که انجام هر کاری را - اعم از فعالیت های مجاز و سودمند و اعمال خطرناک و مجرمانه - برای افراد بسیار سهل و در دسترس کرده است. به ویژه که در چنین محیطی امکان شبیه سازی و

<sup>۱۰</sup> همان، ص ۱۹

<sup>۱۱</sup> همان، صص ۱۹-۲۰

اتخاذ هویت موهوم و جعلی کاری بس آسان است. از این رو در گفتار بعد به بررسی ویژگی های محیط مجازی و چالش های پیش روی انسان در تعامل با این محیط می پردازیم.

## گفتار دوم: مزیت ها و چالش های محیط مجازی

پیش از اختراع رایانه تنها راه گردآوری و نگهداری اطلاعات، شیوه های سنتی کتابت و ثبت اطلاعات در دفاتر و ایجاد گنجینه های مادی از داده ها بود. از این رو تنها برای داده ها و اسناد فیزیکی و دارای عینیت ارزش مادی قائل بودند. اما با پیدایش رایانه و امکان ذخیره ی حجم عظیمی از اطلاعات در آن، به تدریج بسیاری از ارگان ها و مؤسساتی که دارای مقادیر گسترده ای از داده های بایگانی شده یا در جریان بودند اقدام به دیجیتالی کردن اسناد خود کردند.<sup>۱۲</sup> این امر به علت سهولت استفاده از کامپیوتر روز به روز با استقبال بیشتری روبرو شد. پس از ظهور پدیده ای به نام اینترنت و امکان انجام امور جاری از طریق این شبکه، باز هم بر میزان استفاده از رایانه در پردازش و به کار گیری داده ها افزوده شد تا آنجا که امروزه می توان گفت تقریباً هر سندی در محیط ملموس و عینی، یک معادل در فضای مجازی دارد. از این رو امروزه شاید بتوان گفت که داده های موجود در حافظه ی سیستم های رایانه ای ارزشی بیش از امور ملموس و عینی یافته اند. اینترنت و رایانه دارای مزایای متعددی نسبت به فضای عینی و واقعیت که همین قابلیت ها زمینه ی ایجاد چالش هایی را در خصوص ارتکاب برخی اعمال خلاف قانون فراهم کرده است. در اینجا به برخی از این مزایا اشاره می کنیم و در ادامه به بیان ویژگی هایی از محیط مجازی و سیستم های رایانه ای می پردازیم که زمینه ی بروز رفتارهای مجرمانه را پدید آورده است.

## بند اول: مزایای محیط مجازی

یکی از قابلیت های فضای سایبر، قابلیت های رسانه ای آن است. هرکس می تواند با کمترین هزینه و محدودیت برای تولید محتوای الکترونیکی به شکل مستقل و به عنوان یک

<sup>۱۲</sup> باستانی، برومند، منبع پیشین، ص ۳۹

رسانه فعالیت داشته باشد. نمونه‌ی بارز این قابلیت گسترش وبلاگ نویسی در بین افراد جامعه از هر قشر و رده‌ی است. اشخاص با اندکی دانش فنی می‌توانند اقدام به راه‌اندازی وبلاگ شخصی نمایند. مقایسه‌ی این امر با تشریفات اداری کسب مجوز انتشار یک نشریه‌ی محلی مطلب را روشن‌تر می‌کند. ضمن اینکه ایجاد رسانه‌های دیجیتال و آنلاین محدود به مکان خاصی نبوده و یک فرد با ایجاد یک وبلاگ با تمام جهان سخن می‌گوید. علاوه بر این شبکه‌های اطلاع‌رسانی رایانه‌ای ماهیت دوسویه دارند و مخاطبان می‌توانند به شکل فعالانه‌ای در فرایند ایجاد محتوا شرکت کنند، حال آنکه دیگر رسانه‌ها فاقد چنین قابلیت‌هایی هستند. رسانه‌های دیجیتال و مجازی دارای ماهیت چند رسانه‌ای هستند و در آن واحد مخاطب خود را در ابعاد مختلفی تحت تاثیر قرار می‌دهند، حال آن‌که دیگر رسانه‌های چاپی یا رادیویی و تلویزیونی تنها بر یک بعد رسانه‌ای محوریت دارند. ضمن این‌که در محیط مجازی به علت شرایط حاکم بر آن، معمولاً افراد شهامت و آزادی بیشتری در بیان مطالب خود احساس می‌کنند. در حالی که در محیط فیزیکی معمولاً برخی ملاحظات موجب می‌شود افراد بیشتر رنگ محافظ‌کاری بگیرند.<sup>۱۳</sup>

از دیگر قابلیت‌های منحصر بفرد رایانه، امکان تراکم اطلاعات و فرایند پردازش آنهاست. تکنولوژی ذخیره‌سازی اطلاعات امکان ایجاد سیستم‌های بایگانی داده را فراهم کرده است. حافظه‌ی رایانه قادر است میلیاردها داده را در خود جای دهد. از طرف دیگر قابلیت ذخیره و پردازش داده‌ها در رسانه‌هایی چون دیسکت، فلاپی و میکروفیلم نیز زمینه‌ی مناسبی را برای امکان جابجایی اطلاعات با حجم گسترده فراهم کرده است. علاوه بر این، اگر تا چندی پیش پردازش داده‌ها تنها در فضای درون یک کامپیوتر و از طریق نرم‌افزار و ویندوز انجام می‌شد، امروزه فناوری اطلاعات تا جایی پیشرفت کرده که امکان پردازش آنلاین از طریق برخی سایت‌های اینترنتی نظیر گوگل فراهم شده است. این امر نوید شکسته شدن آخرین مرزهای دیجیتال را در عرصه‌ی محیط مجازی می‌دهد. دیگر ویژگی رایانه و اینترنت را باید در سرعت و دقت پردازش اطلاعات جستجو کرد. اگر در گذشته انجام محاسبات و

---

<sup>۱۳</sup> جلالی فراهانی، امیرحسین، مزیت‌ها و محدودیت‌های فضای سایبر در حوزه‌های آزادی بیان، آزادی اطلاعات و حریم خصوصی، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله‌ی حقوقی، شماره ۵۹، تابستان ۱۳۸۶، صص ۶۷-۶۹



پردازش و تطبیق داده‌ها امری وقت‌گیر بود، امروزه این کار در زمانی نزدیک به صفر انجام می‌گردد. درصد امکان بروز اشتباه در پردازش داده‌های دیجیتال بسیار اندک است. سهولت کار با رایانه نیز مزید بر علت گردیده تا افراد اقبال روز افزونی به استفاده از این فناوری نوین در زندگی روزانه نشان دهند.<sup>۱۴</sup>

دیگر رهاورد رایانه و اینترنت را می‌توان در بحث‌های راجع به دولت الکترونیک جستجو کرد. در سال‌های اخیر این بحث به شکل جدی مطرح شده و اجلاس‌های منطقه‌ای و جهانی شکل گرفته است. از جمله اجلاس جهانی جامعه‌ی اطلاعاتی در دسامبر ۲۰۰۳ در سوئیس است که در آن اعلامیه‌ی اصول، با حضور ۵۴ رئیس‌جمهور و نخست‌وزیر تصویب شد. بر طبق این اعلامیه دولت‌ها متعهد شدند که در راستای استقرار جامعه‌ی اطلاعاتی بکوشند.<sup>۱۵</sup> امروزه مسأله‌ی دولت الکترونیک از یک امکان به یک ضرورت تبدیل شده و فعالیت در عرصه‌ی بین‌المللی منوط به تحقق آن است. برترین دستاورد این پدیده برای شهروندان کاهش فساد اداری است. زیرا مهم‌ترین عامل فساد اداری، اعمال نظر شخصی و سوء استفاده از سمت اداری است که با دیجیتال شدن امور، حذف شده و از این پس تنها نرم‌افزارهای رایانه‌ای هستند که بجای کارمندان پاسخگوی نیازهای مراجعان که اکنون کاربران رایانه‌اند، می‌باشند. همچنین حتی اگر افرادی نیز بخواهند از طرق غیر قانونی - مثلاً پرداخت رشوه و مانند آن - به منافع دست یابند، با کامپیوتری شدن امور جاری، این امکان نیز منتفی می‌گردد.

مزیت دیگر، شفاف‌سازی امور دولتی است، چرا که اطلاعات بر طبق روالی از پیش تنظیم شده و بدون دخالت حب و بغض‌های شخصی، تولید و بدون اعمال هر گونه تبعیضی در دسترسی به افراد ارائه می‌گردد. مثلاً برگزاری معاملات دولتی از طریق پایگاه‌های اینترنتی را می‌توان نمونه‌ای از این امر دانست.

ایجاد امکان ارتباطات خصوصی مکتوب یا صوتی و تصویری با کیفیت عالی و با کمترین هزینه نیز از دیگر محاسن فضای مجازی است. همچنین فراهم آوردن امکان تمرکز اطلاعات شخصی از جمله قابلیت‌هایی است که به انسان امروز کمک شایان توجهی کرده است.

<sup>۱۴</sup> باستانی، برومند، منبع پیشین، صص ۳۹-۴۱

<sup>۱۵</sup> جلالی‌فراهانی، منبع پیشین، صص ۷۸-۷۹. همچنین برای مطالعه‌ی بیشتر ن. ک. سعیدی، رحمان، جامعه‌ی اطلاعاتی: چالش

ها و فرصت‌ها، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله‌ی حقوقی، سال دهم، شماره ۴۲، صص ۲۲۱-۲۴۵

تا چندی پیش، اطلاعات موجود در پایگاه های اطلاعاتی بخش های مختلف به شکل غیر متمرکز نگهداری می شد. اما امروزه با اتصال مراکز دیتا به شبکه ی جهانی، امکان دسترسی آنی به تمامی اطلاعات مورد نیاز فراهم گردیده است.<sup>۱۶</sup>

## بند دوم: چالش های محیط مجازی

شبکه ی جهانی یک ساختار و فضای نامحدود اطلاعات است. این فضا همگانی، بی کنترل و بدون یک مرکزیت واحد است. امروزه بیش از صدها میلیون نفر کاربر اینترنت هستند. گفته شده که در هر ۵۳ روز یک بار، حجم تبادل اطلاعات در این فضا دو برابر می شود. صدها میلیارد صفحه ی اینترنتی وجود دارد که بخش زیادی از این صفحات دارای محتوای غیر اخلاقی هستند. این گسترش سرسام آور چالش های حقوقی بزرگی را پدید آورده اما راهکار های عملی مناسبی برای رفع مشکل چندان اندیشیده نشده است، از این رو فضای سایبر به عنوان پرمخاطره ترین فضای تبادل اطلاعات در جوامع بشری شناخته می شود.<sup>۱۷</sup>

گفتیم که یکی از مزایای محیط مجازی، سهولت کار با آن است. همین مزیت خود زمینه ی بروز چالش هایی را پدید آورده است و آن سهولت دسترسی به سیستم ها است. این سهولت در دسترسی یکی از ملزومات سنتی ارتکاب جرم - یعنی حضور بزهکار در محل ارتکاب - را منتفی کرده است. این امر به ویژه با توسعه ی شبکه ی جهانی اینترنت تقویت گردیده است. اگر تا چندی پیش برای دستیابی به محیط رایانه ای نیاز به حضور فیزیکی مرتکب در مقابل سیستم رایانه ای و انجام اعمال غیر قانونی بود، امروزه اغلب این دستیابی از فاصله ی بسیار دور و بدون نیاز به حضور مرتکب انجام می شود. مرتکب می تواند با استفاده از تدابیر امنیتی ضعیف که اغلب موجب بی دفاع گذاردن پایگاه های اطلاعاتی می گردد، به آن سیستم ها دسترسی یابد.<sup>۱۸</sup>

مسأله ی دیگر امکان اتخاذ هویت جعلی است. فعالان غیر مجاز محیط سایبری همواره این امکان را دارند تا خود را به جای یک کاربر مجاز معرفی کرده و وارد سیستم شوند. یکی از

<sup>۱۶</sup> جلالی فراهانی، همان، صص ۸۴-۸۸

<sup>۱۷</sup> مسعودی، امید، منبع پیشین، صص ۱۷-۱۸

<sup>۱۸</sup> باستانی، برومند، منبع پیشین، صص ۳۹-۴۰

ابزارهای حفاظتی مرسوم در محیط مجازی، استفاده از شناسه و گذرواژه است، در حالی که فعالان عرصه ی سایبر قادرند به آسانی این سیستم را دور زده یا از آن عبور کنند.

جنبه ی دیگر ایجاد کننده ی چالش در محیط مجازی و رایانه ای، وسعت و فراگیر بودن قلمرو آن است. به این مفهوم که در فضای اینترنت هر گونه داده ای را می توان یافت. از پژوهشهای علمی و دانشگاهی تا اطلاعات سری نظامی و سیاسی و حتی خصوصی ترین اطلاعات افراد که گاه برای عضویت در یک پایگاه ارائه دهنده ی خدمات الکترونیک از آن ها درخواست می شود. این تنوع اطلاعات موجود در فضای سایبر نیز امکان دسترسی به حساس ترین داده ها و سپس مستمسک قرار دادن آن برای نیل به مقاصد غیر قانونی را بسیار آسان تر از قبل کرده است. یک هکر می تواند به راحتی کلیه ی اطلاعات موجود در پایگاه داده ی یک سازمان دولتی را در کنترل خود گرفته و از این رهگذر آن سازمان را تحت فشار قرار داده تا در ازای بازگرداندن اطلاعات مبالغی را اخاذی کند.<sup>۱۹</sup>

یک بعد دیگر محیط مجازی که در تشدید روند گرایش به ارتکاب جرایم سایبری مؤثر بوده است، از میان رفتن مرزهای موجود در فضای فیزیکی است. در جهان عینی و ملموس پیرامون ما چنانچه فردی قصد ارتکاب عملی غیر قانونی را داشته باشد، از نظر مکانی با محدودیت روبرو است. به این مفهوم که هر فرد در مکانی مرتکب جرم می شود که به راحتی بتواند در آنجا حضور یابد. اما ماهیت محیط مجازی که در آن، مکان معنای خود را از دست می دهد، باعث توسعه ی ارتکاب جرایم فراملی گردیده است. اگر در گذشته ارتکاب سرقت از یک بانک مستلزم تمهید مقدمات بسیار بود و علاوه بر این مرتکب شاید تنها به سرقت از بانک بزرگ شهر خود می اندیشد، امروزه سرقت از بانک نه تنها نیار به مسلح شدن فرد و در معرض خطر قرار گرفتن او ندارد، بلکه بزهدار می تواند در حالی که مشغول گذراندن تعطیلات خود در ساحل دریا است اقدام به سرقت از وب سایت یک بانک بزرگ بین المللی کند. ضمن این که این فرایند در اندک زمان قابل تحقق است.<sup>۲۰</sup>

<sup>۱۹</sup> همان، صص ۴۳-۴۴

<sup>۲۰</sup> همان، ص ۳۷

آزادی دسترسی به اینترنت را نیز می توان بحرانا دانست. اگرچه یکی از جنبه های حقوق و آزادی بشر، آزادی دسترسی است، اما این امر در کنار ماهیت غیر متمرکز بودن فضای مجازی، زمینه ی ایجاد شهامت در افراد در دست زدن به اعمال غیر قانونی را ایجاد می کند. علت تمایل بسیاری از افراد به استفاده از اینترنت آن است که احساس می کنند، در جهان امروز که تمام ابعاد زندگی آنها توسط دولت ها کنترل می شود، اینترنت تنها محیطی است که به علت گستردگی بیش از حد، قابلیت کنترل صد درصد را ندارد. از این رو فرصت را غنیمت شمرده و ضمن استفاده از امکانات فوق العاده ای که محیط سایبر در اختیار آن ها می گذارد، دست به ارتکاب رفتارهایی می زنند که در ابعاد بسیار وسیع آثار و تبعات مخربی به جای می گذارد. چرا که به همان نسبت که قلمرو نفوذ رایانه و اینترنت توسعه یافته است، ابعاد و میزان ضرر و زیان ناشی از ارتکاب یک فعل مجرمانه در این محیط نیز به شکل باور نکردنی عظیم و گاه غیر قابل جبران است.<sup>۲۱</sup>

مواردی که فوقاً اشاره شد، تنها بخشی از ویژگی های فضای سایبر بود که زمینه را برای ارتکاب هرچه آسان تر و کم هزینه تر اعمال مجرمانه فراهم می کرد. به عبارت واضح تر، بسط دامنه ی کاربرد رایانه، از یک سو ریسک ارتکاب جرم را تا حد قابل توجهی کاهش داده و از سوی دیگر به علت جهان شمول بودن شبکه های رایانه ای میزان تأثیرات مخرب آن را افزایش داده است.

## مبحث دوم: مفهوم حریم خصوصی و اهمیت آن

پس از آشنایی مختصر با فضای سایبر که بستر ارتکاب بزه مورد مطالعه در این نوشتار است، باید نگاه خود را معطوف بر ماهیت این جرم کنیم. بدیهی است که افشای سر نوعی تعرض به زندگی خصوصی دیگران است. بزهدکار برای ارتکاب این جرم، مرزها و خطوط قرمزی را می شکنند و در اموری دخالت می کند که اجازه ای برای مداخله در آن ندارد. این خطوط

<sup>۲۱</sup> جلالی فراهانی، منبع پیشین، صص ۶۵-۷۶

قرمز را می توان با عنوان حریم خصوصی بازشناسی کرد. لذا در این مبحث مطالبی پیرامون این نهاد حقوقی، مفهوم و اهمیت و جایگاه آن در ادیان الهی و مقررات بشری به قلم خواهد آمد.

## گفتار اول: مفهوم لغوی و اصطلاحی حریم خصوصی، افشای سر و هتک حیثیت

انسان موجودی دو بعدی است. از یک سو به عنوان موجودی اجتماعی شناخته می شود که در چارچوب زندگی اجتماعی، برخی محدودیت ها را آزادانه می پذیرد تا بتواند از مزایای محیط اجتماعی بهره مند گردد. از سوی دیگر هر انسانی، دارای نوعی فردیت و زندگی جدا از اجتماع نیز می باشد و حاضر نیست این بخش از حیات خود را در معرض دسترسی و مداخله ی همگانی قرار دهد. اجتماع نیز این امر را پذیرفته و ناگزیر به لوازم آن نیز ملتزم گردیده است. در مقام پذیرش استقلال شخصیت انسان از اجتماع است که حق انسان نسبت به تمامیت مادی و معنوی خویش معنا و مفهوم پیدا می کند. از سوی دیگر، طرح موضوع حریم خصوصی تنها در مورد انسان اجتماعی موضوعیت دارد. اگر انسان تنها و در خفا زندگی می کرد، نمی توانستیم از مسأله ی زندگی خصوصی و حریم ممنوعه ای که باید به دور از دسترس دیگران باشد سخن به میان آوریم. بنابر این چون انسان را به عنوان موجودی اجتماعی می شناسیم، لذا برای وی قائل به وجود قلمروی هستیم که تنها خود او مجاز به ورود و دخل و تصرف در آن است. این قلمرو را با نام حریم خصوصی می شناسیم و در این گفتار ابتدا به بیان مفهوم لغوی و اصطلاحی آن پرداخته و سپس اهمیت و جایگاه حریم خصوصی در اسلام و سابقه تاریخی آن را بررسی می کنیم.<sup>۲۲</sup>

### بند اول: مفهوم لغوی

---

<sup>۲۲</sup> رحمدل، منصور، حق انسان بر حریم خصوصی، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی دانشکده ی حقوق و علوم سیاسی، شماره ی ۷۰، زمستان ۱۳۸۴، صص ۱۲۰-۱۲۲

لفظ حریم با "حرمت"، "تحریم"، "حرام" و "احرام" همگی از یک ریشه بوده و دارای قرابت معنایی هستند. ریشه ی تمام این الفاظ، (حرم) می باشد. با این حال در لغت چندین معنی برای واژه ی حریم بیان شده است.

۱- حریم از حرمت به معنای منع است. جوهری گوید: حرمت آن چیزی است که هتک آن جایز نباشد.<sup>۲۳</sup> ابن منظور نیز این معنا را مورد تأکید قرار داده می نویسد: حریم را بدان روی حریم نامیده اند که «منع صاحبش از تصرف» در آن یا تصرف دیگران در آن بی اجازه ی مالک حرام است.<sup>۲۴</sup> بستانی هم می گوید: حریم در لغت به هر چیزی که مستلزم حمایت باشد گفته می شود. به همین دلیل به زنان و مسکن مردان، حریم اطلاق می گردد.<sup>۲۵</sup> طریحی نیز معتقد است: «اصل التحريم المنع» یعنی اصل در معنای تحریم، منع است.<sup>۲۶</sup>

۲- معنای دومی که برای حریم آمده است، آن را از معانی فوق متمایز می کند. اطلاق حریم در اصل، بر حریم املاک بوده است، بنابر این حریم، حقوق و محدوده ی مورد نیاز اطراف املاک را گویند. سپس این مفهوم توسعه یافته و به هر چیز حرام و ممنوع اطلاق گردید.<sup>۲۷</sup>

معنای دوم با معنای نخست حریم منافاتی ندارد. نهایت اختلاف در این دو تعریف، در شیوه ی وضع لفظ حریم برای منع است. توضیح آن که این اختلاف بیشتر جنبه ی اصولی می یابد. اصولیین در باب دلالت لفظ بر معنی، از دو نوع وضع تعینی و تعینی سخن به میان آورده اند. در وضع تعینی از آغاز یک لفظ برای معنای مقصود واضع پیشبینی شده است. اما در وضع تعینی، یک لفظ ابتدا دارای معنای خاص خود بوده، اما به تدریج و در نتیجه ی کثرت استعمال در معنای جدیدی تعین یافته است. در اینجا، می توان گفت که تعریف اول را قائلان به وضع تعینی بیان نموده اند و تعریف دوم ثمره ی اظهار نظر طرفداران وضع تعینی است. در مجموع معنای حریم به نظر اهل لغت، منع است و تعبیر دیگری از قبیل (آنچه شکستن آن جایز نباشد) و یا (آنچه مورد حمایت واقع شود و شخص از آن دفاع کند) در واقع اخذ به لوازم همان

<sup>۲۳</sup> جوهری، اسماعیل بن حماد، صحاح، جلد ۵، ص ۱۸۹۵

<sup>۲۴</sup> ابن منظور، لسان العرب، جلد ۱۲، ص ۱۲۵

<sup>۲۵</sup> بستانی، الپتیس، دایرة المعارف، جلد ۷، ص ۱۹

<sup>۲۶</sup> طریحی، مجمع البحرین، جلد ۶، ص ۳۹

<sup>۲۷</sup> حموی، یاقوت، مجمع البلدان، جلد ۲، ص ۲۸۹

معنای اصلی است. چراکه وقتی امری ممنوع شد، هتک آن جایز نخواهد بود و در برابر متجاوزین مورد حمایت خواهد بود و از آن دفاع خواهد شد.<sup>۲۸</sup>

سر در لغت به معنای امر پوشیده، پنهان، هرچیزی که حفظ آن لازم و ضروری است و آنچه در دل نهفته باشد آمده است. افشا نیز به معنای برملا ساختن، آشکار کردن، فاش نمودن و در اختیار دیگران قرار دادن و منتشر نمودن است.

حیثیت نیز در لغت به معنی آبرو، شرف، کرامت، شأن و منزلت، احترام و هر آنچه که مورد تکریم و تقدیس باشد آمده است. هتک نیز به معنای دریدن، شکافتن، پاره کردن، کنار زدن، از بین بردن، مخدوش ساختن و تخریب کردن می باشد.

## بند دوم: مفهوم اصطلاحی

از میان فهرست بین المللی موضوعات حقوق بشر، شاید دشوارتر از همه تعریف حریم خصوصی باشد. در حقیقت تعریف حریم خصوصی، با فرهنگ و زمینه های اجتماعی و محیطی بستگی قابل توجهی دارد. در بسیاری از کشورها، این مفهوم با مقوله ی حفظ اطلاعات که حریم خصوصی را در معنای مدیریت اطلاعات شخصی تفسیر می کند پیوند خورده و در آن ادغام شده است. در عین حال محافظت از حریم خصوصی معمولاً به عنوان ابزاری برای ترسیم محدوده ی خطوطی که جامعه می تواند در امور افراد دخالت کند، تلقی می شود.

برای اولین بار دو تن از قضات دادگاه عالی ایالات متحده به نام های ساموئل وارن و لوییس براندیس، در مقاله ای با عنوان "حق حریم خصوصی" این مسأله را به عنوان یک بحث جدی مطرح و حریم خصوصی را "حق افراد برای تنها بودن" تعریف کردند. به نظر این دو، حریم خصوصی از جمله ارجمندترین حقوق در یک نظام دموکراتیک است که حمایت از آن باید در متن قانون اساسی منعکس گردد.

رابرت اسمیت، سردبیر مجله ی حریم خصوصی نیز حریم خصوصی را اینگونه تعریف می کند: « تمایل هریک از ما به داشتن فضای فیزیکی که می توانیم در آن از مداخله،

---

<sup>۲۸</sup> شفایی، عبد الله، بازشناسی نهاد حریم (۱)، مرکز تحقیقات کامپیوتری علوم اسلامی، فقه، سال یازدهم، شماره ی چهل و یکم،

مزاحمت، اضطراب و آشفتگی یا پاسخگویی رها باشیم و تلاش برای کنترل زمان و شیوه ی افشای اطلاعات شخصی در باره ی خودمان». در مقدمه ی منشور حریم خصوصی استرالیا نیز آمده است که یک جامعه ی آزاد و دموکراتیک به استقلال فردی احترام می گذارد و هرگونه تعدی دولت و بخش خصوصی را محدود می کند.<sup>۲۹</sup>

در حقوق ایتالیا قضاات دادگاه عالی، در یک دعوای مربوط به نقض حریم خصوصی کوشیدند به ارائه ی تعریفی از حریمی خصوصی بپردازند. ایشان در تعریف خود سه مفهوم از حریم خصوصی ارائه دادند به این شرح:

۱- حریم خصوصی داخلی که مربوط به حمایت از منزل می شود و به نظر دادگاه شاید بتوان حق انسان بر تنها بودن را معادل آن دانست.

۲- قلمرو زندگی فردی و خانوادگی و برخی از اشکال روابط غیر قانونی و بین شخصی در بیرون منزل و مکاتبات

۳- حق انسان بر این امر که زندگی خصوصی او بوسیله ی دیگران مورد احترام واقع شود. از نظر دادگاه اولین تعریف، مضیق، مفهوم دوم معقول و منطقی و تعریف سوم بسیار موسع است.<sup>۳۰</sup>

در حقوق ایران این اصطلاح فاقد تعریف قانونی است و دامنه ی شمول و شرایط آن تابع نگرش اشخاص و مراجعی است که به بحث و بررسی آن می پردازند. در قوانین اعم از اساسی و عادی عبارت حریم خصوصی صریحاً مورد استفاده قرار نگرفته است و قانون گذار به طور کلی به استعمال الفاظی که دلالت بر این مفهوم دارند بسنده کرده است. برخی از اصول قانون اساسی از جمله اصل ۲۲ و ۲۵ بر ضرورت رعایت حریم خصوصی تاکید کرده اند. اخیراً در متن لایحه ی حمایت از حریم خصوصی که در مجلس شورای اسلامی سرانجامی نیافت، مقنن کوشیده بود تا تعریفی جامع از حریم خصوصی ارائه دهد. در ماده ی ۲ این لایحه چنین می خوانیم: « حریم خصوصی قلمروی از زندگی هر شخص است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه

<sup>۲۹</sup> نمک دوست تهرانی، حسن، اخلاق حرفه ای، حریم خصوصی و حق دسترسی به اطلاعات، مرکز تحقیقات کامپیوتری علوم اسلامی، رسانه، سال هفدهم، شماره ی دو، ص ۲۰۰

<sup>۳۰</sup> رحمدل، منصور، منبع پیشین، صص ۱۲۸-۱۲۹



یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو، وی را مورد تعرض قرار ندهند. جسم، البسه و اشیاء همراه افراد، اماکن خصوصی و منازل، محل های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می شوند.<sup>۳۱</sup> در این مفهوم می توان کلیه ی جرایم علیه شخصیت معنوی را در چارچوب حریم خصوصی قرار داد.<sup>۳۱</sup> به نظر می رسد ارائه ی تعریف از حریم خصوصی کار آسانی نیست، زیرا همان طور که بیان گردید مفهوم حریم خصوصی در هر کشوری با فرهنگ، اجتماع، اقتصاد و بویژه نوع رژیم سیاسی حاکم در ارتباط است. ممکن است در کشوری موضوعی از موضوعات داخل در مفهوم حریم خصوصی قلمداد شود و در کشور دیگر چنین نباشد. لذا می توان گفت مفهوم حریم خصوصی امری نسبی است و از کشوری به کشور دیگر ممکن است متفاوت باشد.<sup>۳۲</sup> شاید بتوان در مجموع تعریف زیر را از حریم خصوصی ارائه نمود:

«حریم خصوصی، محدوده ای از زندگی شخص است که به وسیله ی قانون و عرف تعیین شده و ارتباطی با عموم ندارد به گونه ای که دخالت دیگری در آن ممکن است باعث جریحه دار شدن احساسات شخص و تحقیر وی نزد دیگران به عنوان یک انسان گردد. به عبارت دیگر حق حریم خصوصی عبارت است از حق اولیه ی افراد در مصون ماندن حوزه ی خصوصی ایشان از هرگونه مداخله و تعرض فاقد مجوز قانونی و همچنین منع دیگران از وقوف بر اطلاعات این حوزه.»

نهایتاً باید گفت حریم خصوصی ریشه در هویت فرد دارد. حریم خصوصی برای هر فرد یک حق طبیعی به شمار می آید و با حقوق عمومی وی در جامعه متناظر است. حریم خصوصی به معنای داشتن استقلال در زمینه ی نظری و عملی است. یعنی صریح زیستن در تمام شرایط وجودی خود، زندگی مطابق با باورهای خود، یعنی "آنگونه زندگی کن که می خواهی."

مفهوم اصطلاحی افشای سر نیز از معنای لغوی آن چندان دور نیفتاده است. افشای سر به این معناست که فردی از آنچه که دیگری از سایرین نهفته می دارد مطلع گردیده و سپس

---

<sup>۳۱</sup> آقایی نیا، حسین، حقوق کیفری اختصاصی: جرایم علیه اشخاص (شخصیت معنوی)، بنیاد حقوقی میزان، چاپ دوم، تهران، ۱۳۸۶، صص ۲۱۱-۲۱۲

<sup>۳۲</sup> رحمدل، منصور، منبع پیشین، صص ۱۲۹-۱۳۰

آن اطلاعات را بدون رضایت یا مجوز از سوی صاحب آن، در اختیار سایرین قرار دهد. در چنین حالتی است که عنوان افشا موضوعیت می یابد. زیرا آنچه که قرار بر پوشیده داشتن و مخفی ماندن آن بود در معرض آگاهی و اطلاع افرادی قرار می گیرد که صلاحیتی برای دسترسی بر آن امور ندارند و تنها به واسطه ی عمل غیر قانونی دیگری از این امور باخبر گردیده اند. اما آنچه به عنوان هتک حیثیت مطرح می گردد عبارت است از نتیجه و اثر مخربی که از انتشار اسرار خصوصی متعلق به دیگری بر شخصیت معنوی صاحب سر وارد می گردد. در واقع زمانی که فردی اسرار مربوط به دیگری را منتشر می سازد گویی پوششی که او در پیرامون خانه ی خود ایجاد کرده است را کنار زده و همگان را به تماشای آن فرا می خواند. این عمل بی شک موجب ورود لطمه بر آبرو و شرف صاحب سر خواهد گردید. بنابر این هتک حیثیت در اصطلاح به معنای ریختن آبرو و لطمه بر موقعیت اجتماعی، شغلی و ... بزه دیده است.

## گفتار دوم: اهمیت حریم خصوصی در اسلام و دیگر مکاتب

پس از مختصر آشنایی با مفهوم حریم خصوصی اینک باید به بررسی جایگاه و اهمیت این مقوله در دوره های مختلف تاریخی، کشورها و مذاهب بپردازیم. لذا مطالب این گفتار طی دو بند ارائه خواهد شد.

### بند اول: سابقه ی توجه به موضوع حریم خصوصی

مسأله ی حریم خصوصی از دیرباز مورد توجه ادیان و مکاتب مختلف بوده و در تمامی جوامع، همواره اصول و قواعدی برای حفاظت از آن پیشبینی گردیده است. در انجیل اشاره های فراوانی به حریم خصوصی شده است. در احکام یهودیان نیز مفهوم رهایی از مراقبت به رسمیت شناخته شده است. در یونان باستان و چین کهن، حمایت هایی از این حریم وجود داشته است. در کشورهای غربی نیز صدها سال است که حمایت های حقوقی از حریم خصوصی در نظام حکومتی برقرار است.

در سال ۱۳۶۱ م. در انگلستان مأمورانی به کار گرفته شدند تا کسانی را که چشم چرانی می کنند یا فال گوش می ایستند، دستگیر کنند. در سال ۱۷۶۵ م. لرد کامدن در رد یک حکم ورود به خانه و توقیف اوراق چنین استدلال کرده است: براحتمی می توان گفت در این کشور هیچ قانونی وجود ندارد که آنچه را مدعیان مرتکب شده اند توجیه کند. اگر چنین قانونی وجود داشت، همه ی آرامش را از جامعه می ربود. زیرا اوراق انسان معمولاً عزیزترین دارایی اوست. ویلیام پیت، نماینده ی پارلمان نیز می گوید: تنگ دست ترین مردمان نیز حق دارد در کلبه ی خود با تمام نیروهای شاه، مخالفت کند. شاید کلبه ی او سست باشد، شاید سقف آن بلرزد، شاید باد آنرا از جا بکند، شاید طوفان وارد آن شود، شاید باران وارد آن شود، اما شاه انگلستان حق ندارد به آن وارد شود. هیچ کدام از نیروهای او نیز جرأت ندارند از آستانه ی در ویرانه ی آن گامی فراتر نهند.

کشورهای دیگر نیز طی قرون متمادی هریک کوشیدند به نحوی از حریم خصوصی حمایت نمایند. در سال ۱۷۷۶ م. مجلس سوئد قانون "دسترسی به اسناد عمومی" را به تصویب رساند که بر اساس آن تمامی اطلاعات موجود در اختیار دولت، باید برای مقاصد مشروع به کار گرفته شود.<sup>۳۳</sup>

در ایتالیا، آراء اولیه ی دادگاه ها وجود چیزی به نام حریم خصوصی را در نظام حقوقی منکر بود. احکام اولیه ی مربوط به رسمیت یافتن مسأله ی حریم خصوصی به دهه ی ۱۹۵۰ برمی گردد.

در فرانسه مظاهر مختلف حق انسان بر حریم خصوصی در زمان های مختلف نمود یافته است. طبق قانون اساسی ۲۲ اوت ۱۷۹۵، مسکن هر شهروند، پناهگاهی مصون است. قانون اساسی سوم سپتامبر ۱۷۹۱ و قانون اساسی ۱۳ دسامبر ۱۷۹۹ نیز دربر دارنده ی حمایت های مشابه بودند. قانون ۱۱ می ۱۸۶۸ انتشار هر گونه واقعیت پیرامون زندگی خصوصی را جرم شناخته است و در سال ۱۹۷۰ ماده ی ۹ اصلاحی وارد قانون مدنی شد و یک قاعده ی کلی در مورد حمایت از حریم خصوصی مقرر داشت. سرانجام در سال ۱۹۹۵، شورای قانون اساسی حق

<sup>۳۳</sup> نمک دوست تهرانی، حسن، منبع پیشین، ص ۲۰۳

انسان بر حریم خصوصی را به عنوان حق قانونی اساسی، به عنوان یک اصل قانون اساسی مورد پذیرش قرار داد.<sup>۳۴</sup>

امروزه می توان ملاک ارزیابی میزان توجه جامعه ی جهانی نسبت به حریم خصوصی را در اعلامیه ی جهانی حقوق بشر جستجو کرد. در این سند بین المللی، حریم خصوصی مکانی و ارتباطی به طور خاص مورد حمایت قرار گرفته است. در ماده ی ۱۲ این اعلامیه آمده است: «حریم خصوصی، خانواده، خانه یا مکاتبات هیچکس نباید خودسرانه مورد تعرض قرار بگیرد و به شهرت و آبروی هیچکس نباید تعرض شود. همه حق دارند از حمایت قانونی در برابر این گونه مداخلات بهره مند گردند.» در دیگر معاهدات بین المللی نیز حریم خصوصی به عنوان یک حق به رسمیت شناخته شده است، از جمله ماده ی ۱۷ میثاق بین المللی حقوق مدنی و سیاسی،<sup>۳۵</sup> ماده ی ۱۴ کنوانسیون ملل متحد در باره ی کارگران مهاجر<sup>۳۶</sup> و ماده ی ۱۶ کنوانسیون حمایت از کودکان ملل متحد.<sup>۳۷</sup>

همچنین در سطح منطقه ای می توان از کنوانسیون اروپایی حمایت از حقوق بشر و آزادی های اساسی<sup>۳۸</sup> یاد کرد که در ماده ی ۸ خود مقرر داشته: «۱- همه حق دارند به حریم خصوصی و زندگی خانوادگی، خانه و مکاتبات آنها احترام گذاشته شود. ۲- هیچ مقام دولتی نباید به استفاده از این حق تعرض کند مگر مطابق قانون و در صورتی که این امر برای مصالح امنیت ملی، امنیت جامعه، رفاه اقتصادی کشور، پیشگیری از بی نظمی یا تبه کاری، حفظ سلامت اخلاقی یا برای حمایت از حقوق و آزادی های دیگران در یک جامعه ی دموکراتیک

<sup>۳۴</sup> رحمدل، منصور، منبع پیشین، صص ۱۲۲-۱۲۳

<sup>۳۵</sup> International Covenant on Civil and Political Rights, UN General Assembly resolution ۲۲۰۰ A (XXI), December ۱۶, ۱۹۶۶

<sup>۳۶</sup> International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, UN General Assembly resolution, ۴۵/۱۵۸ December ۱۸, ۱۹۹۰

<sup>۳۷</sup> Convention on the Rights of the Child, UN General Assembly resolution ۴۵/۲۵ of November ۲۰, ۱۹۸۹

(به نقل از نمک دوست تهرانی، حسن، منبع پیشین، صص ۲۰۴)

<sup>۳۸</sup> Convention For the Protection of Human Rights and Fundamental Freedoms, Council of Europe, ۱۹۵۰

ضروری باشد.» در ماده ی ۱۱ کنوانسیون آمریکایی حقوق بشر نیز حق حریم خصوصی با تعاریفی مشابه اعلامیه ی جهانی حقوق بشر وضع شده است.<sup>۳۹</sup>

## بند دوم: حریم خصوصی در اسلام

دین اسلام به عنوان آخرین مکتب الهی می کوشد تا طریق نهایی رستگاری و سعادت بشر را پیش روی او گذارد تا در هر زمان و مکانی بتواند عزت و شرف انسان را تأمین و تضمین کند. از این رو توجه خاصی به کرامت و قداست انسان داشته است. (ولقد کرّمنا بنی آدم)<sup>۴۰</sup> یکی از مهم ترین ابعاد احترام به شخصیت و شرف انسان آن است که اسلام انسان را زیربنای هر نوع تربیت و سازندگی دانسته است. لذا حریم خصوصی افراد را با وسواس و باریک بینی فراوان پاس داشته است. در منابع مختلف اسلامی اعم از آیات قرآن و احادیث معصومین (ع) و کلام پیشوایان دین توصیه های فراوانی دیده می شود که آدمیان را از ورود به حریم خصوصی دیگران اکیداً باز می دارد.

قرآن کریم در چندین مورد بر این حق تأکید می کند، از جمله آیات ۲۷ و ۲۸ سوره ی نور و آیه ی ۱۲ سوره ی حجرات. «ای کسانی که ایمان آورده اید، در غیر منزل خودتان بدون اجازه و سلام کردن به صاحب آن وارد نشوید»<sup>۴۱</sup> و «اگر کسی در منزل نبود وارد نشوید تا به شما اجازه ی ورود دهند، و اگر به شما گفته شد برگردید پس برگردید و این برای شما پاکیزه تر است»<sup>۴۲</sup> و «ای کسانی که ایمان آورده اید، از ظن زیاد دوری کنید. همانا برخی از ظن ها گناه هستند و در احوال مردم تجسس نکنید و ...»<sup>۴۳</sup> در توضیح باید گفت انسان در انجام امور خصوصی خود آزاد است و حکومت اسلامی دخالتی در این حوزه ندارد. هرچند عمل ارتكابی قبیح و ناپسند باشد و اسلام به عنوان دین آن را تقبیح نموده و برای مرتکب وعده ی عذاب اخروی در میان باشد. در مورد این گونه اعمال اسلام اجازه ی تفتیش و بازرسی و

<sup>۳۹</sup> نمک دوست تهرانی، حسن، منبع پیشین، صص ۲۰۴-۲۰۵

<sup>۴۰</sup> اسراء، ۷۰

<sup>۴۱</sup> یا ایها الذین ءامنوا لا تدخلوا بیوتاً غیر بیوتکم حتی تستأنسوا وتسلموا علی اهلها

<sup>۴۲</sup> فان لم تجدوا فیها احداً فلا تدخلوها حتی یؤذن لکم وان قیل لکم ارجعوا فارجعوا هو اذکی لکم

<sup>۴۳</sup> یا ایها الذین ءامنوا اجتنبوا کثیراً من الظن ان الظن ان بعض الظن اثمٌ ولا تجسسوا ...

پیگیری را نداده است، انسان در داخل خانه ی خود و در اعمال شخصی خویش آزاد است، و مصون از تفتیش و تعقیب است. در این موارد تا جایی که مربوط به خود شخص می شود، تا زمانی که انعکاس اجتماعی نیافته حکومت وظیفه ای در اثبات امر و مجازات عامل آن را ندارد بلکه باید از تجسس خودداری کند.<sup>۴۴</sup> حتی در مورد انجام عمل منافی عفت، حتی در صورتی که ظن و گمانی در مورد شخصی ایجاد گردد، اسلام کسانی را که چنین عملی را به یک مسلمان نسبت می دهند مورد نکوهش قرار می دهد و حتی ممکن است مدعیان ارتکاب چنین اعمالی مجازات گردند.<sup>۴۵</sup>

در روایات نیز موارد بسیاری در باره ی حفظ حریم خصوصی وجود دارد. از پیامبر اکرم نقل است که «لغزش های مسلمانان را نجوید که هرکس لغزش های برادرش را بجوید، خداوند لغزش های او را پیگیری می کند و هرکس را که خدا عیب جویی کند، رسوایش سازد هرچند اندرون خانه ی خود باشد» (میزان الحکمه) همچنین در روایت دیگری از ایشان چنین آمده است: «من مأمور نیستم از نهان و پنهان مردم جستجو کنم»<sup>۴۶</sup> و نیز امام صادق (ع) فرمود: «از مرام و باورهای مردم جستجو نکن تا تنها و بی همراه بمانی»<sup>۴۷</sup>

همچنین این داستان در تاریخ اسلام مشهور است که شیخی خلیفه ی دوم در کوچه های مدینه مشغول گشت زنی بود. از درون خانه ای صدای غنا شنید. وارد خانه شد و به صاحب بیت گفت: ای دشمن خدا! آیا گمان کرده ای که خداوند گناهت را می پوشاند؟ مرد گفت: ای پیشوای مسلمین! شتاب مکن. اگر من مرتکب یک گناه شدم، تو مرتکب سه گناه شده ای: خداوند از جاسوسی نهی کرده و تو تجسس کردی، خدا فرمود از در خانه وارد شوید و تو از دیوار آمدی، خداوند فرمود هرگاه خواستید به خانه ای درآیید اذن بگیرید و تو بدون اذن وارد شدی.<sup>۴۸</sup>

---

<sup>۴۴</sup> خوئینی، غفور، حقوق شهروندی و توسعه ی پایدار، فرهنگ صبا، تهران، ۱۳۸۶، صص ۵۵-۵۶  
<sup>۴۵</sup> مهرپور، حسین، آزادی فردی و حدود آن در حکومت اسلامی، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی حقوقی و قضایی دادگستری، پاییز ۱۳۷۱، شماره ی ۵، صص ۳۴-۳۵  
<sup>۴۶</sup> آنی لم اؤمر ان انقب عن قلوب الناس ولا اشق بطونهم. کنز العمال، جلد ۳، ش ۱۵۳۵  
<sup>۴۷</sup> لا تفتش الناس عن اديانهم فتبقي بلا صديق. میزان الحکمه، جلد ۱، ص ۳۹۱  
<sup>۴۸</sup> مهریزی، مهدی، دولت دینی و حریم خصوصی، حکومت اسلامی، مرکز تحقیقات کامپیوتری علوم اسلامی، سال چهارم، شماره ی دوم، صص ۶۲-۶۳

امثال این قبیل احادیث و روایات در منابع اسلامی کم نیست و همگی دلالت بر میزان اهمیت و ارزشی است که دین مبین برای حرمت زندگی خصوصی مسلمین قائل است. شایان ذکر است که اعلامیه ی اسلامی حقوق بشر که یک سند بین المللی اسلامی است نیز به این مسأله توجه داشته و در ماده ی ۱۸ مقرر داشته: «... ب- هر انسانی حق دارد که در امور زندگی خصوصی خود - اعم از مسکن و خانواده و مال و ارتباطات - استقلال داشته باشد و جاسوسی و نظارت بر او یا مخدوش کردن حیثیت او جایز نیست و باید از او در مقابل هرگونه دخالت زورگویانه در این شئون حمایت شود. ج- مسکن در هر حالی حرمت دارد و نباید بدون اجازه ی ساکنین آن یا به صورت غیر مشروع وارد آن شد و نباید آن را خراب یا مصادره کرد یا ساکنینش را آواره نمود.»<sup>۴۹</sup>

## مبحث سوم: شناسایی مفهوم هتک حیثیت و افشای سر و مقایسه ی آن با دیگر عناوین

در ادامه ی مطالعه و اینک در قدم سوم، بر آنیم تا موضوع اصلی پژوهش خود را بهتر و شفاف تر بشناسیم. آشنایی با مفهوم افشای سر، سابقه و تاریخچه ی جرم انگاری این مقوله، مطالب این مبحث را به خود اختصاص می دهد. مضافاً به این که افشای سر در برخی جنبه ها، با دیگر عناوین مجرمانه دارای وجوه شباهت و تفاوت است. این مسأله را نیز در همین مبحث پی می گیریم و افشای سر را طی چند گفتار با برخی جرایم دیگر مقایسه خواهیم کرد.

### گفتار اول: شناسایی مفهوم هتک حیثیت از طریق افشای سر

از آنچه تا کنون پیرامون اهمیت و جایگاه حریم خصوصی بیان گردید به وضوح روشن شد که حیثیت و شرافت انسان تا چه اندازه دارای ارزش و قداست است. تا جایی که در برخی روایات وجوب حفظ عرض و آبروی مسلمین برابر با احترام خانه ی خدا دانسته شده است. یکی

<sup>۴۹</sup> مهرپور، حسین، منع پیشین، ص ۳۵

از مهم ترین مسائل که ممکن است به شرف و آبروی اشخاص لطمه وارد کند، آگاهی و دسترسی دیگران به اسراری است که شخص در حیطه ی حریم خصوصی خود نهان ساخته و به هیچ کس اجازه ی اطلاع بر آن را نمی دهد. شاید این اسرار حاکی از ارتکاب یک عمل خلاف اخلاق و شریعت نیز باشد، اما چنان که گفته شد در جامعه ی اسلامی بیش از هرچیز تأکید بر پوشاندن گناهان و تشویق افراد به توبه در محضر باری تعالی است. از این رو حتی در چنین شرایطی نیز اطلاع بر اسرار دیگران و بدتر از آن افشا و برملا نمودن آن نزد دیگران گناهی نابخشودنی است. از این رو در این گفتار ابتدا به بررسی مفهوم سر می پردازیم و سپس اهمیت حفظ اسرار را در اسلام بیان کرده مختصری در مورد بزه افشای اسرار سخن خواهیم گفت.

## بند اول: اسرار و تأکید بر حفظ آن در اسلام

سر در فرهنگ های مختلف به اشکال گوناگونی تعریف شده است.

۱- سر، نسبت و اسم عربی است و معنای آن راز، امر پوشیده و نهفته می باشد. سر مطلب نهفته در دل، آنچه که باید پنهان داشت. (عمید) ۲- سر یعنی کار پوشیده و مخفی، به معنای راز، لطیفه ای مودع در قلب که محل شهود است، چنان که روح محل محبت و قلب محل معرفت است. سر چیزی است که حق آنرا پنهان کرده و مردم را بدان دست رسی نیست. (معین).<sup>۵۰</sup> ۳- اسرار جمع سر است. سر یعنی نهان و مقابل جهر است. سر چیزی است که انسان آنرا در قفس خود پوشیده دارد (دهخدا)

بر این پایه معلوم می شود اولاً سر لزوماً امری زشت و مجرمانه نیست بلکه چه بسا امری نیکو و پسندیده باشد. ثانیاً سر امری نسبی است و تابعی از شرایط افراد است و انگیزه ی انسان در پنهان نمودن آن در سر بودنش نقش بازی می کند.<sup>۵۱</sup>

<sup>۵۰</sup> شقاقی، بیژن، اخلاق حرفه ای حفظ اسرار، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی کانون وکلای دادگستری، بهار و

تابستان ۸۲، شماره ی ۱۸۰ و ۱۸۱، ص ۲۶۲

<sup>۵۱</sup> قماش، سعید، بررسی جرم افشای اسرار حرفه ای (۱)، دادرسی، ماه نامه ی شماره ی ۵۸، سال دهم، مهر و آبان ۱۳۸۵، صص ۳-



افشای سر به معنای اعلام و اظهار آن به دیگران است. این اعلام ممکن است از طریق گفتگو و محاوره‌ی عادی، مکاتبه، انتشار در مطبوعات و رسانه‌ها صورت گیرد و یا از طریق سیستم‌های رایانه‌ای.<sup>۵۲</sup> طبیعتاً در حالات اخیر - انتشار در مطبوعات، رسانه‌ها و یا رایانه - ممکن است به عنوان یک کیفیت مشدده در ارتکاب جرم مطرح شود که در جای خود به آن خواهیم پرداخت.

حرمت افشای سر از حیث فقهی کاملاً پذیرفته شده است و چند دسته از روایات بر آن دلالت دارند. دسته‌ای از روایاتی که در مورد حرمت ایذاء مؤمن وارد شده است از این جمله است. افشای سر دیگران در غالب موارد موجب آزار فردی می‌شود که سر او افشا شده، لذا عملی حرام است. با این وجود، مطابق این دسته روایات تنها ایذاء مؤمن حرام شمرده شده است.

دسته‌ی دیگر از روایات در مورد حرمت فاش ساختن سر مؤمن وارد شده است. از آن جمله مضمهره‌ی عبد... بن سنان است که در آن چنین آمده است: «به امام عرض کردم: آیا عورت مؤمن بر مؤمن حرام است؟ امام فرمودند: آری. عرض کردم: یعنی قسمت پایین شکم؟ امام فرمودند: خیر، مقصود افشای سر اوست»<sup>۵۳</sup> در روایت دیگری از امام علی (ع) آمده است: «خیانت در امانت نکن، هرچند او در امانت تو خیانت کرده باشد و سر شخصی را که بر آن اطلاع داری فاش مساز...»<sup>۵۴</sup> از برخی از این دسته روایات - نظیر روایت اخیر - می‌توان مطلق حرمت افشای سر را به دست آورد.

دسته‌ی دیگر از روایات آن روایاتی هستند که در خصوص حرمت غیبت و بیان امور برادران دینی که از سایرین مخفی بوده و افشای آن موجب رنجش خاطر صاحب آن سر می‌گردد، به بیان حکم پرداخته‌اند. مطابق با این دسته روایات افشای سر در بسیاری موارد عنوان غیبت نیز می‌یابد و از این حیث نیز حرام است.

<sup>۵۲</sup> جعفری لنگرودی، محمدجعفر، ترمینولوژی حقوق، گنج دانش، تهران، ۱۳۷۲، ص ۳۵۶

<sup>۵۳</sup> قلت له: عورة المؤمن علی المؤمن حرام؟ قال: نعم. قلت یعنی سفلته؟ قال: لیس حیث تذهب انما هو اذاعة سره. ر. ک. محمد بن

حسن حر عاملی، وسائل الشیعه، جلد ۱۲، باب ۱۵۷ از ابواب احکام العشرة، ص ۲۹۴، حدیث ۱

<sup>۵۴</sup> ولا تخن من ائمتنک وان خانک فی امانته ولا تدع سر من اذاع سرک ... محمد باقر مجلسی، بحار الانوار، جلد ۷۵، صص ۱۰-۱۱

پاره ای دیگر از احادیث وجود دارد که در آن ها دیده ها و شنیده های بین چند نفر به عنوان امانت تلقی شده و افشای آن خیانت دانسته می شود. از جمله در روایتی آمده است: «گفتگویی که بین افراد صورت می پذیرد امانتی بین آنهاست و افشای سر برادر دینی خیانت به اوست پس از آن دوری کن»<sup>۵۵</sup> بعلاوه در صورتی که افشای سر مصداق اشاعه ی فحشاء و یا عنوان ظلم باشد گناه تلقی می شود.<sup>۵۶</sup>

بنابر مراتب فوق تردیدی در حرمت و ممنوعیت افشای سر در اسلام باقی نمی ماند و بر این اساس و طبق نظر فقهای امامیه که نظر بر لزوم اعمال تعزیر بر مرتکب فعل حرام دارند، ارتکاب چنین عملی موجب ثبوت تعزیر بر فاش کننده ی اسرار دیگران می گردد.

## بند دوم: بزه افشای سر در حقوق ایران

در حقوق ایران نیز از آغاز قانون گذاری توجه مقنن به این مسأله معطوف بوده که اسرار خصوصی افراد باید از تعرض مصون باشد. لهذا در قوانین مختلف بر این امر تأکید نموده است. در ماده ی ۲۲۰ قانون مجازات عمومی که از ماده ی ۳۷۸ قانون مجازات فرانسه اقتباس گردیده بود چنین مقرر می داشت: «اطباء و جراحان و قابله ها و داروفروشان و کلیه ی کسانی که به مناسبت شغل و حرفه ی خود محرم اسرار می شوند، هرگاه در غیر از مواردی که بر حسب قانون ملزم می باشند اسرار مردم را افشا کنند از یک ماه تا یک سال حبس تأدیبی و از ۲۰۵ الی ۲۰۰۰ ریال غرامت محکوم خواهند شد.»

پس از انقلاب اسلامی و در جریان دگرگونی مقررات جاری مملکتی، قوانین کیفری بیش از همه دست خوش تغییر و تحول گردید. با این حال ماده ی فوق الاشعار در متن قانون مجازات اسلامی نیز با اندکی تغییر باقی مانده است. در حال حاضر ماده ی ۶۴۸ ق. م. ا. مقرر می دارد: «اطبا و جراحان و ماماها و داروفروشان و کلیه ی کسانی که به مناسبت شغل یا حرفه ی خود محرم اسرار می شوند هرگاه در غیر از موارد قانونی اسرار مردم را افشا کنند به سه ماه

---

<sup>۵۵</sup> المجلس بالامانة وافشاؤك سر اخيك خيانة فاجتنب ذلك. گرچه در این روایات عبارت مؤمن به کار رفته و در لسان فقهای امامیه مؤمن ظهور در شیعه دارد، اما با توجه به این که بسیاری از این روایات از ناحیه ی پیامبر اکرم (ص) صادر گردیده است، نمی توان قائل به تعلق این قبیل احادیث به شیعیان گردید. همچنان که در عبارت "انما المؤمنون اخوة" نیز چنین نیست.

<sup>۵۶</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۲۹۹-۳۰۱

و یک روز تا یک سال حبس و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می شوند»

ملاحظه می شود که در هر دو قانون تنها افشای اسرار حرفه ای جرم انگاری شده است.<sup>۵۷</sup> منظور از اسرار حرفه ای اموری است که انسان از رهگذر شغل و حرفه ی خود و بر اساس موقعیتی که دارد به آنها پی می برد یا محرم اسرار اشخاص واقع می گردد. به طور کلی می توان گفت اسرار حرفه ای دو دسته اند: اول اموری که صریحاً در قوانین کیفری به عنوان اسرار مردم از آنها یاد شده است.<sup>۵۸</sup> دوم اموری که به طور صریح در قوانین ذکر نشده ولی به روشنی از ماده ی ۶۴۸ بر می آید که منظور اسراری است که افراد در هر شغلی که هستند به واسطه ی شغل خود به آن پی می برند.<sup>۵۹</sup>

علت توجه ویژه ی قانون گذار به افشای اسرار حرفه ای آن است که مردم به صاحبان برخی مشاغل اعتماد دارند و اسرار خود را برای آنها بازگو می کنند. اگر این قبیل افراد رازهای کسانی را که به ایشان اعتماد دارند فاش کنند، زیان آن بعد اجتماعی پیدا می کند. زیرا در چنین حالتی مردم تا حد امکان به پزشک و روان شناس و وکیل و امثال آن مراجعه نمی کنند و در نتیجه ی بروز این وضعیت، سلامت و امنیت جامعه به مخاطره می افتد.<sup>۶۰</sup> از این رو برخی معتقدند که این جرم دارای جنبه ی عمومی بوده و تعقیب آن منوط به شکایت شاکی خصوصی نمی باشد.<sup>۶۱</sup> با این حال بر اساس ماده ی ۷۲۷ ق.م.ا. این جرم از جمله جرایم قابل گذشت بوده که تعقیب آن منوط به شکایت شاکی خصوصی گردیده است.

<sup>۵۷</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۲۹۵-۲۸۶

<sup>۵۸</sup> از جمله می توان به موارد زیر اشاره کرد:

الف- ماده ۱۲ قانون راجع به کارشناسان مصوب ۱۳۱۷

ب- ماده ۴۲ قانون دفاتر اسناد رسمی و کانون سردفتران و دفتریاران مصوب ۱۳۴۵

ج- ماده ۳۰ قانون وکالت مصوب ۱۳۱۵

د- ماده ۲۳۲ قانون مالیات های مستقیم مصوب ۱۳۶۱

ه- قانون بورس اوراق بهادار ماده ی ۴۸ به بعد.

و- قانون مجازات افشای اسناد سری دولتی.

<sup>۵۹</sup> قماش، سعید، منبع پیشین، ص ۴

<sup>۶۰</sup> ولیدی، محمد صالح، حقوق جزای اختصاصی، جرایم علیه اشخاص، جلد دوم، مؤسسه ی انتشارات امیرکبیر، تهران، ۱۳۷۸، صص

۳۱۱-۳۰۹

<sup>۶۱</sup> یاد، ابراهیم، حقوق کیفری اختصاصی، جلد ۱- دانشگاه تهران، ۱۳۴۷، صص ۳۸۰ و ۳۸۶

با این حال در ق. م. ا. افشای اسرار غیر حرفه ای - اسراری که افراد به عنوان مثال در نتیجه ی رابطه ی دوستی با شخصی به دست می آورند - جرم انگاری نشده است. برخی معتقدند علت این امر آن است که افشای چنین اسراری ابعاد گسترده ی اجتماعی ندارد و آثار نامطلوب آن تنها متوجه یک فرد می گردد.<sup>۶۲</sup> اما بروز اتفاقاتی در کشور ما در چند سال اخیر نشان داد که افشای اسرار یک شخص تا چه اندازه می تواند موجب جریحه دار شدن عفت و اخلاق عمومی گردد. این مسأله به خصوص در مورد افراد مشهور جامعه نمود بیشتری دارد. از این رو قانون گذار در برخی قوانین دیگر که اخیراً تصویب گردیده افشای اسرار دیگران را که عمدتاً موجب هتک عرض و آبروی بزه دیده می گردد را جرم انگاری کرده و حتی در برخی موارد با حصول شرایطی، چنین عملی را در حد افساد فی الارض دانسته که مجازات آن بسیار شدید خواهد بود. مخصوصاً اگر افشای اسرار از طریق سیستم های رایانه ای یا ابزار دیجیتال و الکترونیک باشد، با توجه به ویژگی های محیط سایبری که پیشتر بیان گردید ابعاد و حجم زیان های وارده بر بزه دیده بسیار افزایش می یابد.

از جمله اولین قوانین که به حمایت از حریم خصوصی و منع افشای اسرار غیر حرفه ای در محیط مجازی پرداخت، قانون تجارت الکترونیک مصوب ۱۳۸۲ بود که در مواد ۵۸ و ۵۹ تحت عنوان (حمایت از داده پیام های شخصی) و ماده ی ۷۱-۷۳ تحت عنوان (جرایم و مجازات ها) مقرراتی پیرامون انتشار اطلاعات خصوصی افراد در بستر مبادلات الکترونیک پیش بینی نمود.<sup>۶۳</sup>

اندکی بعد در سال ۱۳۸۶ طی اصلاحیه ای قانون تشدید مجازات کسانی که در امور سمعی بصری فعالیت می کنند به تصویب رسید که ضمن اصلاح قانون سابق مصوب ۱۳۷۲ در ماده ی ۳، مجازات های بسیار شدیدی برای انتشار آثار سمعی بصری مبتذل و مستهجن مقرر داشت. بدیهی است، انتشار اسرار دیگران نیز می تواند مصداق این مقررره باشد که در جای خود آنرا بررسی خواهیم کرد.

---

<sup>۶۲</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، ص ۲۹۶  
<sup>۶۳</sup> سوادکوهی فر، سام، تحلیلی بر مقررات جزایی IT در ایران، مرکز تحقیقات کامپیوتری علوم اسلامی، دادرسی، ماهنامه ی شماره ۴۵، سال هشتم، مرداد و شهریور ۱۳۸۳، صص ۸-۹

نهایتاً در ماده ی ۱۷ قانون جرایم رایانه ای اخیر التصویب برای تغییر و تحریف فیلم یا تصویر خصوصی و خانوادگی دیگری و انتشار آن و نیز انتشار اسرار خصوصی متعلق به دیگری مجازات حبس و جزای نقدی پیش بینی کرده است. بدین ترتیب در حال حاضر افشای اسرار دیگران از طریق سیستم های رایانه ای وصف جزایی داشته و قابل مجازات خواهد بود.

سؤالی که ممکن است در اینجا مطرح شود این است که سری که از افشای آن منع گردیده است، آیا متضمن امور مجاز و غیر مجرمانه است یا حتی در صورت اطلاع بر سری که حاکی از ارتکاب یک رفتار مجرمانه است نیز افشا کننده ی آن قابل مجازات خواهد بود؟ با نگاهی به قوانین حاکم در این زمینه از جمله ماده ی ۶۴۸ ق.م.ا. و قید (جز در موارد قانونی) روشن می گردد که تنها مورد مجاز در افشای اسرار مواردی است که قانوناً چنین حقی برای برخی افراد ذی صلاح پیش بینی گردیده است. لذا باید گفت حتی در صورتی که فردی به واسطه ی شغل و حرفه ی خود از اسراری مطلع می گردد که متضمن امور مجرمانه ای باشد لیکن طبق قانون مکلف به آگاه ساختن دیگران بر آن نباشد، مجاز به افشای آن اسرار نیست. بله، اگر شخصی خارج از قلمرو ماده ی ۶۴۸ ق.م.ا. و بدون آن که به واسطه ی شغل خود محرم اسرار دیگری شده باشد، از امور مجرمانه ای مطلع گردد و سپس آن اسرار را در اختیار مقامات صلاحیت دار قرار دهد، این عمل وی تحت عنوان «اعلام جرم» قرار خواهد گرفت و مشمول بزه افشای اسرار نخواهد بود.

## گفتار دوم: مقایسه ی بزه افشای اسرار با دست رسی غیر مجاز

پس از آشنایی با مفهوم افشای سر، باید به مقایسه ی آن با دیگر عناوین مجرمانه که ممکن است دارای وجوه تشابه و تمایز با این عنوان باشند بپردازیم. اولین عنوان که می توان با افشای سر مقایسه کرد، جرم دست رسی غیر مجاز است که در قانون جرایم رایانه ای تحت عنوان (جرایم علیه محرمانگی) جرم انگاری شده است. لذا در این گفتار ابتدا با بزه دست رسی غیر مجاز آشنا شده سپس وجوه اشتراک و افتراق آن را با افشای اسرار بررسی می کنیم.

## بند اول: مفهوم دست یابی غیر مجاز<sup>۶۴</sup>

دست یابی غیر مجاز یا هکینگ چیست؟ بررسی مسأله ی هکینگ موضوعی بسیار گسترده است و از قلمرو پژوهش ما بیرون است. در اینجا تنها به اختصار با این جرم آشنا می شویم. در دهه ی ۷۰ هکر به اشخاصی اطلاق می شد که در برنامه نویسی بسیار ماهر بودند. بعدها در دهه ی ۸۰ این واژه در مورد شخصی که در نفوذ به سیستم های جدید تبحر داشت اطلاق گردید و امروزه این واژه علاوه بر این معنا، گاه به هر شخصی که مرتکب جرمی در باره ی فناوری اطلاعات گردد گفته می شود.<sup>۶۵</sup> هکرها دارای انگیزه های مختلفی هستند که مهم ترین آنها را می توان قصد کنجکاوی، تفریح و تغنن دانست. البته گاه این اقدامات به قصد آسیب رساندن و بهره برداری مالی انجام می گیرد. بر همین اساس هکرها را به گروه های مختلفی چون "کلاه سفید"، "کلاه سیاه" و "کلاه خاکستری" تقسیم می کنند.<sup>۶۶</sup>

مفهوم جرم دست یابی غیر مجاز در برخی اسناد بین المللی آمده است. به عنوان مثال در تقسیم بندی ارائه شده از سوی سازمان توسعه و همکاری اقتصادی (OECD) می خوانیم: «دست یابی یا شنود در یک سیستم رایانه ای یا ارتباطی به طور آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور اعم از آن که با تخطی از تدابیر باشد یا با هدف غیر شرافت مندانه» در توصیه نامه ی شورای اروپا نیز این جرم بدین شکل تعریف شده است: «دست یابی بدون حق به سیستم یا شبکه ی رایانه ای از رهگذر تجاوز به تدابیر و ابزارهای امنیتی».<sup>۶۷</sup>

---

<sup>۶۴</sup> یکی دیگر از جرایم موضوع قانون جرایم رایانه ای، شنود غیر مجاز است که از برخی جهات با افشای سر مشابهدت دارد اما به لحاظ شباهت آن با دست یابی غیر مجاز از بررسی مستقل آن صرف نظر کرده و تنها به اختصار به چند نکته در این مورد بسنده می کنیم. اولاً رکن قانونی این جرم ماده ی ۲ قانون جرایم رایانه ای است. ثانیاً موضوع این جرم محتوای در حال انتقال ارتباطات غیر عمومی است. ثالثاً رفتار مرتکب عبارت است از شنود موارد پیش گفته. شنود اصطلاحاً به معنای استماع مخفیانه و پنهانی مکالمات دیگران است اما با توجه به نحوه ی استعمال آن در قانون جرایم رایانه ای، اختصاصی به صوت ندارد و امور دیگر اعم از گفتار یا تصویر و نوشتار را نیز شامل می گردد. رابعاً این جرم از جمله جرایم مطلق است. خامساً در تحقق آن نقض تدابیر امنیتی بر خلاف دست یابی غیر مجاز شرط نیست. سادساً در خصوص موضوع جرم همان گونه که بیان شد محتوای ارتباط باید در حل انتقال باشد اما مطابق تبصره ی ماده ی ۴۸ همان قانون دسترسی به محتوای ارتباطات غیر عمومی ذخیره شده نیز در حکم شنود غیر مجاز است. سابقاً به لحاظ مطلق بودن این بزه، وجود سوء نیت خاص در تحقق آن ضروری نیست.

<sup>۶۵</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۱۹۰-۱۹۱

<sup>۶۶</sup> باستانی، پرومند، منبع پیشین، صص ۵۶-۵۷

<sup>۶۷</sup> بای حسینعلی و بابک پورقهرمانی، صص ۱۸۷-۱۸۸

هدف از این جرم جلوگیری از نفوذ به شبکه های کامپیوتری است. صرف دست یابی کافی است. وصف این دست یابی غیر مجاز بودن آن است. این دست یابی زمانی غیر مجاز تلقی می شود که نفوذ کننده، محقق در دست یابی نباشد.<sup>۶۸</sup>

در ماده ی ۱ قانون جرایم رایانه ای نیز این جرم مورد تعریف قرار گرفته است. «هرکس به طور غیر مجاز به داده ها یا سامانه های رایانه ای یا مخابراتی که به وسیله ی تدابیر امنیتی حفاظت شده است دسترسی یابد به حبس ... یا جزای نقدی ... یا هر دو مجازات محکوم خواهد شد» چنان که ملاحظه می شود در قانون ایران تنها حالتی از دست یابی غیر مجاز جرم انگاری شده است که در آن فرد با نقض تدابیر امنیتی به داده ها دسترسی پیدا کند. از این رو قلمرو شمول این عنوان مجرمانه نسبت به اسناد بین المللی محدودتر است. بعلاوه در این ماده مشخص نشده است که منظور از تدابیر امنیتی چیست؟ به منظور حمایت بیشتر از حریم خصوصی افراد، می توان گفت که هر گونه رمز عبور یا فایروال نیز نوعی تدابیر امنیتی هستند. زیرا در غیر این صورت این ماده تنها برای برخی سازمان های خاص و متولی امنیت شبکه موضوعیت می یابد. چرا که در این صورت هکریایی که به سیستم های رایانه ای و بانک های اطلاعاتی که دارای تدابیر خاص امنیتی نیستند ضربه می زنند، مجرم شناخته نخواهند شد. بدین ترتیب بخش وسیعی از نفوذهای غیر مجاز جرم تلقی نمی شود و بسیاری از هکرها معطوف به کاربران خانگی و دیگر سیستم های بی دفاع می شوند.<sup>۶۹</sup>

با توجه به این که طبق ماده ی ۱، دست یابی غیر مجاز نیازمند ورود غیر مجاز به داده هایی است که به وسیله ی تدابیر امنیتی حفاظت شده اند، چنانچه فردی پس از استخراج اطلاعاتی که توسط دیگری انجام شده است، به آن داده ها دست یابد، از آنجا که در هنگام دسترسی فرد دوم، داده های موضوع جرم به وسیله ی تدابیر امنیتی حفاظت نشده است لذا حکم این ماده شامل آن نمی گردد. نکته ی دیگر آن است که داده ها باید به وسیله ی تدابیر امنیتی مورد حفاظت باشند. لذا حتی در صورتی که داده محرمانه باشد اما به وسیله ی تدابیر امنیتی مورد حفاظت نباشد، جرم موضوع این ماده محقق نخواهد شد. به عنوان مثال می توان

---

<sup>۶۸</sup> دزیانی، محمدحسن، مقدمه ای بر سیاست جنایی ایران در باب جرایم سایبری، قضاوت، ماهنامه ی شماره ی ۳۸، خرداد و تیر

۱۳۸۵، ص ۴۶

<sup>۶۹</sup> سعیدی نژاد، یاسمن، جرم انگاری در فضای مجازی، تعالی حقوق، شماره ۲، صص ۲۴-۲۵

به موردی اشاره کرد که یک سند محرمانه در فضای مجازی یک سازمان نظامی در دسترس تمام کاربران آن شبکه ی داخلی قرار دارد. در اینجا اگرچه سند محرمانه است اما به علت عدم حفاظت آن توسط تدابیر امنیتی، دست یابی به آن جرم موضوع ماده ی ۱ را محقق نخواهد کرد.<sup>۷۰</sup>

## بند دوم: جهات اشتراک و افتراق افشای سر و دست یابی غیر مجاز

پس از شناسایی مفهوم دست یابی غیر مجاز باید آن را با افشای سر مقایسه نمود. در نگاه اول چنین به نظر می رسد که در هر دو جرم فردی به اطلاعاتی دست یافته که متعلق به دیگری بوده و این نقطه ی مشترک این دو بزه است. به عبارت دیگر اطلاع از مسائل خصوصی دیگران در هر دو جرم محوریت دارد. اما این دو از جهات متعددی با یکدیگر متفاوت و دارای جهات افتراق اند.

توضیح آن که نقطه ی مشترک در این دو بزه را باید در موضوع جرم جستجو نمود. موضوع بزه دست یابی غیر مجاز آنگونه که قانون جرایم رایانه ای بیان داشته، داده های حفاظت شده است. در حالی که موضوع بزه افشای اسرار، رازها و اطلاعات خصوصی افراد است. اگرچه در یک نگاه کلی می توان گفت میان داده های حفاظت شده و اسرار خصوصی متعلق به دیگران تفاوت وجود دارد، بدین توضیح که تفاوت این دو در آن است که داده های موضوع بزه اول، اصولاً باید به شکل مکتوب یا مصور در یک سیستم رایانه ای ذخیره شده باشد، در حالی که برای تحقق افشای سر این امر ضرورتی ندارد. ممکن است فرد اطلاعات خصوصی دیگری را به هر ترتیب به دست آورده باشد. مثلاً به واسطه ی رابطه ی دوستانه ای که با وی دارد یا در نتیجه ی موقعیت اجتماعی خود - به عنوان مثال یک روحانی که به واسطه ی منزلت اجتماعی خود محرم اسرار یک خانواده قرار گرفته است - و یا به سبب شغل خود آنگونه که ماده ی ۶۴۸ ق.م.ا. مقرر کرده است. اما در بزه دست یابی غیر مجاز ارتکاب بزه صرفاً نسبت به داده های رایانه ای قابلیت ارتکاب دارد. اما این تمایز ظاهری در خصوص افشای اسرار در

<sup>۷۰</sup> ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، قسمت دوم، دادرسی، ماهنامه ی شماره ۷۸، سال سیزدهم،

پهمن و اسفند ۱۳۸۸، صص ۱۳-۱۵



محیط عینی و حقیقی قابل طرح است و در خصوص افشای اسرار در فضای سایبر باید گفت که وصف رایانه ای و دیجیتالی بودن اطلاعات ضروری است و محرمانگی و جنبه ی خصوصی و سری داشتن نیز لازم است. بدین رو موضوع هر دو جرم داده های رایانه ای است که در خصوص بزه دست یابی غیر مجاز بوسیله ی تدابیری حفاظت گردیده اند و در مورد افشای اسرار وصف خصوصی و خانوادگی موجب محرمانگی آن ها می گردد.

اما وجوه تمایز این دو بزه را نیز نباید از نظر دور داشت. یکی از این جهات ممیزه، نتیجه ی حاصله از جرم است. دست یابی غیر مجاز یک جرم مطلق است. به این مفهوم که صرف دست یافتن فرد بر داده های حفاظت شده برای تحقق جرم کافی است، حال آن که بزه افشای سر محقق نمی شود مگر با مطلع ساختن دیگری از آن. فرص کنیند فردی به هر شیوه ای - مثلاً استفاده از روش های اتخاذ هویت جعلی<sup>۷۱</sup> - توانسته باشد وارد پروفایل شخصی دیگری در وب سایت دانشگاه او شده و از این طریق اطلاعاتی را به دست آورده باشد. این عمل وی تا همین میزان با جمع سایر شرایط می تواند تحت عنوان دسترسی غیر مجاز تعقیب گردد. اما تنها در صورتی بزه افشای سر تحقق می یابد که لااقل این اطلاعات را در اختیار یک شخص دیگر که صلاحیت دسترسی به آن را ندارد بگذارد.

نکته قابل ذکر دیگر آن است که دست یابی غیر مجاز چنان که در بند پیش بیان شد قائم به شخص مرتکب است و تنها باید به شکل مباشرت انجام گیرد. زیرا تحقق آن موقوف بر نقض تدابیر امنیتی است. اما بزه افشای سر این گونه نیست. فرض کنیند فردی با جمع کلیه ی شرایط لازم در ارتکاب جرم پس از اطلاع از اسرار دیگری، این اطلاعات را در اختیار دیگران قرار دهد. تا این میزان از عمل چنین فردی دارای وصف مجرمانه خواهد بود. (بزه افشای اسرار)

---

<sup>۷۱</sup> بحث در خصوص شیوه های رایج و متداول هکنینگ بسیار گسترده است. به اختصار باید گفت در نوعی از دست یابی نفوذ یابندگان سیستم خود را به جای کاربران مجاز معرفی می کنند. این امر به ویژه در سیستم هایی اتفاق می افتد که کاربران آن می توانند از اسامی رمز متداول استفاده کنند. در یک تقسیم بندی از شیوه های دست یابی دو نوع از هکنینگ را می توان تفکیک کرد. ۱- دست یابی به شیوه های فنی شامل دست رسی به گذرواژه ها، دست رسی از طریق درهای پشتی و دست رسی از طریق اسب تراوا و ... ۲- دست یابی به شیوه های غیر فنی شامل اشغال گری، جعل عنوان، نشان دادن خود به جای کاربر مجاز، ارتباط دوستانه با مدیر سیستم و ... (بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۱۸۹-۱۹۰)

برای مطالعه ی بیشتر ر. ک. دزیانی، محمدحسن، جرایم کامپیوتری، جلد ۱، دبیرخانه ی شورای عالی انفرماتیک، تهران، ۱۳۷۶، صص ۳۳. ضیایی پرور، حمید، جنگ نرم ویژه ی جنگ رایانه ای (۱)، مؤسسه ی فرهنگی مطالعات و تحقیقات بین المللی ابرار، تهران، ۱۳۸۳، صص ۱۹۳-۲۴۶

متعاقباً فرد دوم که از این اسرار آگاه شده نیز اقدام به انتشار این مطالب می کند. در این مورد نیز می توان چنین فردی را مرتکب بزه افشای سر دانست. اما در مورد دست یابی غیر مجاز این مسأله مصداق ندارد.

مسأله ی دیگر موضوعیت داشتن نقض تدابیر امنیتی است. شرط لازم و ضروری برای ارتکاب جرم دست رسی غیر مجاز - لاقلاً آنگونه که قانون جرایم رایانه ای بیان کرده - نقض تدابیر امنیتی است. لذا به عنوان مثال چنانچه کاربر یک سایت فرهنگی به گونه ای گاملاً تصادفی و در نتیجه ی اختلال در سیستم مانیتورینگ وب سایت از اطلاعات شخصی دیگر کاربران وب سایت مطلع گردد، در این وضعیت عمل او به علت عدم نقض تدابیر امنیتی وصف مجرمانه نخواهد داشت. اما چنانچه همین فرد پس از دستیابی بر تصاویر موجود در اکانت کاربری دیگری اقدام به ایجاد تغییر یا تحریف در آن بنماید و سپس تصویر مجعول را در وبلاگ خود به نمایش عمومی گذارد می توان عمل وی را مشمول ماده ی ۱۶ قانون جرایم رایانه ای قلمداد نمود.

دیگر مسأله ی قابل ذکر آن است که همانگونه که از عنوان بزه دست یابی غیر مجاز بر می آید غیر مجاز بودن عمل فرد برای کسب اطلاعات نیز موضوعیت دارد. لذا به عنوان مثال مدیر یک وب سایت علمی که برای پذیرش اعضا از ایشان می خواهد تا اطلاعاتی را در مورد زندگی خصوصی خویش در سیستم گردآوری اطلاعات سایت وارد نمایند، هرگاه بخواهد به این اطلاعات دست یابد، مرتکب بزه موضوع ماده ی ۱ نگریده است. چراکه کاربران وب سایت در زمان عضویت در حقیقت به طور ضمنی به مدیریت سایت این اجازه را داده اند تا به اطلاعات خصوصی ایشان دسترسی داشته باشد. اما همین فرد با وجود آنکه اطلاع یافتن وی بر امور خصوصی دیگران - به واسطه ی رضایت آنها - مجاز بوده است هرگاه اقدام به افشا و در اختیار دیگران قرار دادن این اطلاعات بنماید با وجود سایر شرایط می توان عملش را مشمول ماده ی ۱۷ قانون جرایم رایانه ای قرار داد. توضیح آن که ممکن است فردی با رضایت دیگری بر اسراری از وی مطلع گردد. اما این رضایت بر اطلاع، مجوزی برای افشا و در اختیار دیگران قرار دادن آن اسرار نیست. به بیان دیگر در ارتکاب بزه دست یابی غیر مجاز هیچ گونه رضایتی اعم از اولیه یا ثانویه وجود ندارد، اما در بزه افشای اسرار ممکن است رضایت اولیه برای آگاهی از اسرار موجود باشد اما رضایت ثانویه - یعنی رضایت بر افشا اسرار - وجود ندارد.

موارد فوق تنها بخشی از مهم ترین تفاوت های موجود میان این دو جرم است اما موارد دیگری از قبیل تفاوت در رکن روانی و وصف و خصوصیات مرتکب را نیز می توان از دیگر وجوه تمایز این دو جرم دانست که از توضیح آن می گذریم. تنها بیان همین نکته کافی است که در جرم دست یابی غیر مجاز - به لحاظ مطلق بودن جرم - وجود سوء نیت خاص ضرورتی ندارد، اما در بزه افشای سر وجود قصد و اراده بر مطلع ساختن دیگران از اسرار فرد بزه دیده ضروری است.

## گفتار سوم: مقایسه ی افشای سر با جاسوسی رایانه ای

دیگر عنوان مجرمانه که از برخی جهات دارای مشابهت هایی با افشای سر است، جاسوسی می باشد. چرا که موضوع جرم در این بزه مانند افشای سر، اطلاعات سری و محرمانه است. از این رو در اینجا ابتدا مختصراً با مفهوم جاسوسی و بزه جاسوسی رایانه ای آشنا شده سپس وجوه تشابه و تمایز آن را با افشای سر بررسی خواهیم کرد.

### بند اول: شناسایی بزه جاسوسی رایانه ای

یکی از قدیمی ترین جرایم علیه امنیت را جرم جاسوسی دانسته اند. سابقه ی این جرم را برخی به زمان حضرت موسی (ع) می رسانند.<sup>۷۲</sup> در آیین اسلام نیز مسأله ی جاسوس گماری از آغاز وجود داشته است. چنان که از حضرت رضا (ع) منقول است: هرگاه پیامبر سپاهی را به جایی اعزام می کرد امیری بر آنها می گماشت. فرد مورد اعتمادی را نیز همراه آنها می فرستاد تا کارهایشان را به حضرت گزارش دهد. پیغمبر را جاسوسانی بود که در منطقه ی دشمن نفوذ می کردند و تصمیمات ایشان را به اطلاع پیامبر می رساندند.<sup>۷۳</sup>

---

<sup>۷۲</sup> برای مطالعه ی تفصیلی جرم جاسوسی و سابقه ی تاریخی آن ر. ک: میرمحمد صادقی، حسین، حقوق کیفری اختصاصی: جرایم علیه امنیت و آسایش عمومی، نشر میزان، تهران، ۱۳۸۶، صص ۷۵-۱۱۰ و همچنین شامبیاتی، هوشنگ، حقوق کیفری اختصاصی،

جلد سوم، جرایم بر ضد مصالح عمومی کشور، مجد، تهران، ۱۳۸۲، صص ۹۷-۱۲۲

<sup>۷۳</sup> ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، قسمت سوم، ماهنامه ی دادرسی، شماره ی ۷۹، سال چهاردهم، فروردین و اردیبهشت ۱۳۸۹، ص ۵.

جاسوس در لغت به معنای خبرکش، جستجو کننده ی خبر، کسی که اخبار و اسرار شخصی یا اداری یا مملکتی را به دست آورد و به دیگری اطلاع دهد می باشد. (عمید) البته جاسوسی تنها جنبه ی سیاسی نداشته و ممکن است اطلاعات اقتصادی، نظامی و علمی نیز هدف جاسوسی قرار گیرند. از نظر حقوقی جرم جاسوسی در قوانین کشورهای مختلف معمولاً به طور واضح تعریف نمی شود تا دست مقنن و قاضی برای ارائه ی تعریف متناسب با مقتضیات زمان باز باشد.<sup>۷۴</sup> در برخی اسناد بین المللی سعی بر آن بوده تا تعریفی از جاسوسی ارائه گردد.<sup>۷۵</sup> در حقوق ایران نیز وضعیت مشابهی حکم فرماست و هیچ یک از مواد قانونی تعریفی مشخص از جاسوسی ارائه نمی دهد. بلکه بیشتر به شکل مصدافی در مواد مختلف برای برخی اعمال محل به امنیت کشور تحت عنوان جاسوسی مجازات هایی پیش بینی شده است.<sup>۷۶</sup>

با گسترش کاربرد رایانه، موضوع ارتکاب جاسوسی از طریق این ابزار نیز مورد توجه قرار گرفت. به عنوان مثال از ایمیل می توان برای تشویش اذهان عمومی، دعوت به بر اندازی و ارتباط با بیگانه استفاده کرد. بویژه در مواردی که امنیت در حد پایین و ناکافی وجود داشته باشد. یک پست الکترونیک با محتوای رمز نگاری شده می تواند از فیلترها بگذرد و از بهترین ابزارهای جاسوسی به شمار می آید. از این طریق می توان اطلاعات محرمانه را به تنهایی یا با یک فایل ضمیمه به مقصد مورد نظر رساند. این مسأله در قضیه ی فعالیت گروه القاعده قوت یافته است.<sup>۷۷</sup> البته جاسوسی سنتی بیشتر ناظر به کسب اسرار سیاسی و نظامی و انتقال آن به کشور بیگانه بود اما جاسوسی رایانه ای علاوه بر آن ناظر به کسب اسرار حرفه ای، تجاری، صنعتی و اقتصادی و انتقال آن به افراد فاقد صلاحیت نیز می باشد. در برخی اسناد بین المللی جاسوسی رایانه ای تعریف شده است، از آن جمله در فهرست اختیاری شورای اروپا آمده است:

<sup>۷۴</sup> شامبیاتی، هوشنگ، منبع پیشین، ص ۱۰۰.

<sup>۷۵</sup> به عنوان مثال ماده ی ۱۹ قطعنامه ی بروکسل مصوب ۱۸۷۴ مقرر داشته: جاسوس کسی است که به طور مخفیانه و با وسایل و بهانه های مجعول اطلاعات را جمع آوری یا تجسس برای تحصیل اطلاعات در نقاط اشغال شده بوسیله ی نیروی دشمن با قصد اینکه آنها را به طرف مقابل تسلیم نماید می کند. ماده ی ۲۹ آیین نامه ی ضمیمه ی قرارداد لاهه مورخ ۱۹۰۷ بیان داشته: کسی را نمی توان جاسوس دانست مگر اینکه به طور مخفیانه یا به بهانه های مجعول به نفع یکی از متخاصمین در صدد تحصیل اطلاعات یا جمع آوری اشیایی برآید.

<sup>۷۶</sup> ر. ک: قانون مجازات اسلامی، بخش تعزیرات، فصل اول، جرایم علیم امنیت داخلی و خارجی کشور و قانون مجازات جرایم نیروهای مسلح، فصل مربوطه

<sup>۷۷</sup> دزیانی، محمدحسن، نکات تحلیلی ایمیل از زاویه ی جزایی، نگاهی به جرایم سایبری، ماهنامه ی قضاوت، شماره ی ۳۱، خرداد

«کسب اسرار حرفه ای یا تجاری از راه های نادرست یا افشا، انتقال و یا استفاده از این اسرار بدون داشتن حق یا هرگونه توجیه قانونی با قصد وارد کردن زیان اقتصادی به فردی که محق در نگه داشتن اسرار است، یا تحصیل یک امتیاز اقتصادی غیر قانونی برای خود یا یک شخص ثالث.»<sup>۷۸</sup>

در ایران ضمن تصویب قانون جرایم رایانه ای، مبحث سوم از بخش اول این قانون تحت عنوان جاسوسی رایانه ای به تصویب رسید. با یک نگاه به این مبحث که شامل سه ماده است، ملاحظه می شود که نگاه مقنن صرفاً معطوف جرایم امنیتی بوده و به جنبه های دیگر جاسوسی رایانه ای عنایتی نداشته است<sup>۷۹</sup> در ماده ی ۳ قانون مزبور، هرگونه دسترسی یا شنود غیر مجاز داده های سری و یا افشا و در دسترس قرار دادن آنها برای افراد غیر صالح و بیگانگان جرم محسوب شده است.<sup>۸۰</sup>

موضوع این بزه عبارت است از داده های سری در حال انتقال یا ذخیره شده در سامانه های رایانه ای و مخابراتی.<sup>۸۱</sup> طبق تصریح ماده ۱، منظور از داده های سری نیز داده هایی است که افشای آنها به امنیت کشور و منافع ملی لطمه می زند. تضمین حقوق و آزادی های شهروندی ایجاب می کند که داده های سری صرفاً شامل داده های سری و محرمانه ی طبقه بندی شده ی کشوری، امنیتی و نظامی شود که توسط تدابیر خاص حفاظت شده و به طور مشخص به کاربر اعلام نمایند که تمامی سایت یا بخشی از آن سری و محرمانه است.<sup>۸۲</sup>

<sup>۷۸</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۴۳۷-۴۳۸

<sup>۷۹</sup> شایان ذکر است، در قانون تجارت الکترونیک طی ماده ی ۶۴ و ۷۵ مقررات جزایی پیرامون برخی رفتارها تدوین شده که تا حدودی با تعریف شورای اروپا از جاسوسی رایانه ای انطباق دارد. البته در این قانون هیچ اشاره ای به جاسوسی نشده است.

<sup>۸۰</sup> همچنین ماده ی ۴ در مقام جرم انگاری شروع به جرم جاسوسی رایانه ای بوده و ماده ی ۵ بی مبالاتی در حفظ اطلاعات طبقه بندی شده ی مربوط به رایانه را جرم دانسته است که به نظر می رسد ذکر این مورد ذیل عنوان جاسوسی خالی از اشکال نباشد. برای مطالعه ی بیشتر در این مورد ر. ک: ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، قسمت سوم، دادرسی، شماره ۷۹، سال چهاردهم، فروردین و اردیبهشت ۸۹، صص ۴-۷

<sup>۸۱</sup> ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، قسمت چهارم، ماهنامه ی دادرسی، شماره ی ۸۰، سال

چهاردهم، خرداد و تیر ۱۳۸۹، صص ۲۴-۲۵

<sup>۸۲</sup> سعیدی نژاد، یاسمن، منبع پیشین، ص ۲۵.

نکته ی دیگر آن است که وسیله ی ارتکاب - رایانه - نیز در تحقق این بزه موضوعیت دارد و چنانچه ارتکاب این اعمال بوسیله ی رایانه نباشد، جرم موضوع این ماده محقق نمی شود.<sup>۸۳</sup>

## بند دوم: جهات اشتراک و افتراق افشای سر با جاسوسی رایانه‌ای

چنان که بیان شد، جاسوسی رایانه ای از این جهت که موضوع آن داده های سری است تا حدی با افشای سر تشابه دارد. آنچه در افشای اسرار موضوع جرم قرار می گیرد عبارت است از داده های رایانه ای که دارای وصف خصوصی و خانوادگی هستند. از سویی موضوع بزه جاسوسی رایانه ای نیز عبارت است از داده های سری در حال انتقال یا ذخیره شده در سیستم های رایانه ای. ملاحظه می گردد که موضوع هر دو بزه از حیث محرمانه بودن اطلاعات با هم تشابه دارند. از سوی دیگر رفتار مجرمانه در افشای اسرار همانا در دسترس دیگران قرار دادن اسرار خصوصی و خانوادگی است. همان گونه که ماده ی ۳ قانون جرایم رایانه ای نیز بیان داشته یکی از اشکال ارتکاب جاسوسی رایانه ای نیز عبارت است از افشا و در دسترس قرار دادن اسرار برای افراد غیر صالح و بیگانگان. از این رو رفتار مجرمانه نیز در این دو جرم تا حدی و در برخی مصادیق با هم یکسان است. با این حال این دو جرم از جهاتی نیز با یک دیگر متفاوت اند. لذا باید وجوه ممیزه ی این دو بیان گردد تا مرز بحث دقیق تر روشن شود.

یکی از مهم ترین تفاوت های این دو بزه به طبقه بندی آنها مربوط است. به این مفهوم که جرم جاسوسی همان گونه که گفتیم از زمره ی جرایم علیه امنیت کشور است، در حالی که افشای سر در گروه جرایم علیه تمامیت معنوی اشخاص قرار می گیرد. این مسأله دارای آثاری است که یکی از مهم ترین آنها جنبه ی خصوصی یا عمومی داشتن جرم است که در مورد وصف قابل گذشت بودن یا نبودن جرم مؤثر است. توضیح آنکه قاعده ی کلی در مورد جرایم علیه امنیت آن است که قابلیت گذشت ندارد و تعقیب آن به درخواست مدعی العموم آغاز می گردد. اما در جرایم علیه اشخاص اصولاً جرم دارای جنبه ی خصوصی است و تعقیب آن موقوف بر طرح شکایت خصوصی است. ماده ی ۶۴۸ ق. م. ا. که به جرم انگاری بزه افشای اسرار حرفه

<sup>۸۳</sup> ترکی، غلام عباس، همان منبع، صص ۷-۸

ای اختصاص دارد، مطابق ماده ی ۷۲۷ همان قانون از جمله جرایم قابل گذشت است که تعقیب آن موقوف بر شکایت شاکی خصوصی است. اما جرم جاسوسی اعم از کلاسیک یا جاسوسی رایانه ای به لحاظ بعد امنیتی اصولاً از جمله جرایم غیر قابل گذشت بوده و تعقیب آن منوط به طرح شکایت خصوصی نیست.

نکته ی دیگر پیرامون موضوع این دو بزه آن است که به استناد قانون جرایم رایانه ای، جاسوسی نسبت به داده های سری قابل ارتکاب است و طبق تبصره ی ذیل ماده ی ۳ همان قانون منظور از داده های سری، داده هایی است که افشای آن به امنیت کشور لطمه می زند. اما در بزه افشای سر، اطلاعاتی که هدف و موضوع جرم قرار می گیرند عبارت اند از امور خصوصی و احتمالاً خانوادگی یک فرد معمولی. لذا آماج بزهکاری در جرم جاسوسی، کل یک جامعه است و در افشای سر تنها یک شخص قربانی واقع می شود.<sup>۸۴</sup> درست است که افشای چنین اموری نیز دارای آثار مخرب اجتماعی و اخلاقی است اما ابعاد زیان های وارده در نتیجه ی جاسوسی بسیار وسیع تر از افشای سر است. و این خود تفاوت دیگر موجود میان این دو مورد است. منظور نتیجه ی حاصل از جرم است که در افشای سر آبرو و حیثیت و شخصیت یک فرد خاص است اما در جاسوسی تمامیت و موجودیت یک کشور تحت الشعاع قرار می گیرد.

وجه ممیزه ی دیگر در رکن مادی به مطلق یا مقید بودن دو بزه برمی گردد. برخی از مصادیق جاسوسی رایانه ای با توجه به ماده ی ۳ از جمله جرایم مطلق است. به عنوان مثال بند (الف) از ماده ی ۳ در بیان مصادیق جاسوسی به اموری چون دسترسی به داده های سری یا تحصیل آن یا شنود محتوای سری در حال انتقال اشاره می کند. بدیهی است انجام این قبیل امور منوط به تحقق نتیجه ی خاصی نبوده لذا این جرم در برخی موارد مطلق است.<sup>۸۵</sup> حال آنکه افشای سر تنها در صورتی محقق می گردد که اسرار مطعلق به دیگری در اختیار افراد ثالث قرار گیرد.

<sup>۸۴</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۴۳۸-۴۳۹

<sup>۸۵</sup> ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، قسمت چهارم، همان منبع، ص ۲۵.

یک تفاوت دیگر میان این دو جرم به این مسأله برمی گردد که جرم جاسوسی معمولاً دارای شکلی سازمان یافته است. سازمان های جاسوسی بزرگی در جهان مشغول فعالیت هستند که تشکیلات مخوف و پیچیده ای دارند و حتی اقدام به استخدام جاسوس و آموزش نیرو می نمایند. بر این اساس ارتکاب جاسوسی - اعم از سنتی یا رایانه ای - معمولاً دارای بعد فراملی است.<sup>۸۶</sup> حال آنکه بزه افشای سر یک جرم سازمان یافته نیست. معمولاً گستره ی محدودتری دارد و اصولاً بعد بین المللی نمی یابد. منظور آن نیست که این جرم قابلیت ارتکاب در محیط بین المللی را نداشته باشد، اما معمولاً چنین وضعیتی پیش نمی آید.

رفتار مرتکب در بزه افشای سر تنها با یک فعل مثبت و تنها به شکل عمدی قابل تحقق است. (مطلع ساختن دیگران) اما در جاسوسی رایانه ای مسأله محل تأمل است. همان گونه که بیان شد در ماده ی ۵ قانون جرایم رایانه ای به موردی اشاره شده که مأموران دولتی در نتیجه ی بی احتیاطی یا بی مبالاتی یا عدم رعایت تدابیر امنیتی امکان دسترسی افراد فاقد صلاحیت را به داده های موضوع ماده ی ۳ همان قانون فراهم می آورند و این مورد را نیز ذیل عنوان جاسوسی قرار داده است. به نظر می رسد قانون گذار در جرم انگاری به قانون مجازات اسلامی نظر داشته اما در تعیین عنوان مبحث سوم دچار اشتباه گردیده و بهتر بود عنوان این مبحث (جرایم علیه امنیت کشور) تعیین می شد. با این حال به فرض این که قانون گذار را از اشتباه تبرئه کنیم، باید بپذیریم که جرم جاسوسی به ترک فعل نیز قابلیت ارتکاب دارد. ضمن این که بی احتیاطی و بی مبالاتی و عدم رعایت تدابیر امنیتی، از جمله مهم ترین خطاهای جزایی بوده که در رکن روانی جرم بررسی می گردد و وصف بزه را از عمد به غیر عمد تغییر می دهند. لذا در وضعیت کنونی، ما نوعی از جاسوسی رایانه ای را داریم که به شکل غیر عمد ارتکاب می یابد.<sup>۸۷</sup>

موضوعاتی چون تفاوت در سوء نیت عام و خاص این دو جرم نیز از دیگر موارد تمایز در ماهیت این دو می باشد که نیازی به توضیح واضحات احساس نمی گردد.

<sup>۸۶</sup> میرمحمد صادقی، حسین، منبع پیشین، صص ۷۷-۷۸.

<sup>۸۷</sup> ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، قسمت سوم، همان منبع، ص ۷.



## گفتار چهارم: مقایسه ی افشای سر و نشر اکاذیب

در این گفتار به مقایسه ی افشای سر و نشر اکاذیب می پردازیم. توضیح آنکه نشر اکاذیب نیز به عنوان یکی دیگر از جرایمی که با نشر و اشاعه ی برخی از مطالب محقق می گردد، از این حیث با افشای سر دارای شباهت است. چرا که در افشای سر نیز مطالبی به دیگران ارائه می شود. اما از جهات متعددی نیز با یکدیگر متفاوتند که پس از بیان مطالبی مختصر پیرامون ماهیت نشر اکاذیب به بیان این وجوه افتراق خواهیم پرداخت.

### بند اول: آشنایی با نشر اکاذیب

انتشار و اشاعه ی اخبار دروغ و وقایع خلاف واقع به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی را نشر اکاذیب گویند. مقصود از این بزه آن است که مرتکب مطالب و اموری را که علم بر عدم صحت آنها دارد عامداً علیه شخصی حقیقی یا حقوقی شایع و اظهار نماید بدون آنکه اعمال معینی را به افراد معینی نسبت دهد و اخبار بی اساس را بیان کند. حرمت شرعی بهتان و کذب و به طریق اولی اشاعه ی این گونه امور از مسلمات فقهی است و روایات فراوان بر آن دلالت دارد.<sup>۸۸</sup>

در حقوق ایران، سابقاً قانون مجازات عمومی طی بند ب ماده ی ۲۶۹ مکرر به جرم انگاری نشر اکاذیب پرداخته بود. در حال حاضر ماده ی ۶۹۸ ق.م.ا. با اندکی تغییر همان حکم را پیش بینی کرده است.<sup>۸۹</sup> متعاقباً طی ماده ی ۱۸ قانون جرایم رایانه ای نیز مقنن حکمی شبیه به ماده ی فوق الذکر مقرر داشته است.<sup>۹۰</sup> با نگاهی به مواد قانونی مزبور مشخص می

<sup>۸۸</sup> بای، حسینعلی و بابک پور قهرمانی، منبع پیشین، صص ۲۹۰-۲۹۱.

<sup>۸۹</sup> ماده ی ۶۹۸: «هر کس به قصد اضرار یا تشویش اذهان عمومی یا مقامات رسمی به وسیله ی نامه یا شکواییه یا مراسلات یا عرایض یا گزارش یا توزیع هرگونه اوراق چاپی یا خطی یا امضا یا بدون امضا اکاذیبی را اظهار نماید یا با همان مقاصد اعمالی را بر خلاف حقیقت رأساً یا به عنوان نقل قول به شخص حقیقی یا حقوقی یا مقامات رسمی تصریحاً یا تلویحاً نسبت دهد اعم از این که از طریق مزبور به نحوی از انحاء ضرر مادی یا معنوی به غیر وارد شود و یا نه علاوه بر اعاده ی حیثیت در صورت امکان باید به حبس از ۲ ماه تا ۲ سال یا شلاق تا ۷۴ ضربه محکوم شود.

<sup>۹۰</sup> هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله ی سیستم رایانه ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت رأساً یا به عنوان نقل قول به شخص حقیقی یا حقوقی یا مقام های رسمی به طور صریح یا تلویحی نسبت دهد، اعم از این که از طریق یاد شده به نحوی از انحاء ضرر

گردد که در ضمن این مواد، دو جرم پیش بینی شده است. یکی اظهار اکاذیب و دیگری نسبت دادن امور خلاف واقع به دیگران که لزوماً مصادیق یکسانی ندارند. مطابق با مواد مورد اشاره اظهار کردن مطالب خلاف واقع رفتار مرتکب مصداق اول این بزه را تشکیل می دهد. در این مصداق ضرورتی ندارد که اکاذیب اظهاری به فرد معینی منتسب شده باشد، برخلاف مصداق دوم که رفتار مرتکب در آن منتسب کردن امور خلاف واقع به دیگری است و لذا فرد منتسب الیه باید فی الجمله معین و مشخص باشد.

موضوع این بزه اکاذیب و امور خلاف واقع است. لذا اظهار و انتشار واقعیات موجود در جامعه هرچند موجب تشویش اذهان عمومی نیز گردد طبق این مواد قابلیت تعقیب و مجازات را ندارد. وسیله ی ارتکاب در این بزه - مصداق اول - موضوعیت دارد، چنانکه مقنن هم در ق. م. ا. و هم در قانون جرایم رایانه ای بر وسیله ی ارتکاب تأکید کرده است. نگاهی به مصادیق وسیله ی ارتکاب جرم در این مواد نشان می دهد که تمامی این وسایل مکتوب هستند لذا اظهار شفاهی اکاذیب ظاهراً مشمول حکم این مواد قرار نمی گیرد. تأکید قانون گذار بر عبارت "هرگونه اوراق چاپی یا خطی" نیز خود شاهی بر این مطلب است. البته تحقق جرم انتساب امور غیر واقع به سایرین موقوف به استفاده از وسیله ی خاصی نگردیده است.

در تحقق هیچ یک از این دو بزه حصول نتیجه ی خاصی شرط نیست لهذا هر دو مصداق بزه مقرر در این مواد از جمله جرایم مطلق هستند. چرا که مقنن در متن هر دو ماده به این مسأله تأکید نموده است: «... اعم از این که از طریق مزبور به نحوی از انحا ضرر مادی یا معنوی به غیر وارد شود یا نشود...» بر این اساس سوء نیت خاص در هر دو مصداق این بزه منتفی می باشد.<sup>۹۱</sup>

در خصوص رکن روانی این جرم علاوه بر ضرورت وجود علم بر عدم صحت اظهارات و امور انتسابی و همچنین وجود سوء نیت عام - عمد در انجام رفتار مجرمانه - برخی بر آنند که اشاره صدر مواد یاد شده به "قصد اضرار یا تشویش اذهان عمومی یا مقامات رسمی" دلالت بر

---

مادی یا معنوی وارد شود یا نشود، افزون بر اعاده حیثیت به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.  
<sup>۹۱</sup> آقایی نیا، حسین، منبع پیشین، صص ۱۰۹-۱۲۵.

ضرورت وجود سوء نیت خاص در مرتکب برای ایجاد امور یاد شده دارد.<sup>۹۲</sup> اما همان طور که در خصوص نتیجه ی حاصل از جرم اشاره رفت، تحقق این بزه منوط به حصول نتیجه ی خاصی نگردیده و چنان که می دانیم در جرایم مطلق سوء نیت خاص موضوعیت ندارد. لذا موارد "قصد اضرار و تشویش اذهان" را باید به عنوان انگیزه ی مرتکب قلمداد نمود. در این مورد قانون گذار استثنائاً انگیزه را به عنوان جزئی از رکن روانی دانسته که اثبات وجود آن برای مجرم شناختن مرتکب ضرورت دارد.

نکته ی قابل توجه در خصوص قانون جرایم رایانه ای آن است که ماده ی ۱۸ آن قانون تقریباً تکرار ماده ی ۶۹۸ ق.م.ا. است و تنها "سیستم های رایانه ای و مخابراتی" را به وسایلی که ارتکاب بزه از آن طریق ممکن است افزوده است. قبل از تصویب این قانون اداره ی حقوقی قوه ی قضائیه طی یک نظریه ی مشورتی چنین اظهار نظر کرده بود: «اگر به وسیله ی اینترنت یا مشابه آن هم جرمی به کسی نسبت داده شود و نسبت دهنده نتواند صحت آن انتساب و اسناد را ثابت نماید مورد مشمول ماده ی ۶۹۷ ق.م.ا. خواهد بود»<sup>۹۳</sup> و بنا بر وحدت ملاک این نظریه را به ماده ی ۶۹۸ نیز تسری می دادند. اما با تصویب قانون جرایم رایانه ای، این مشکل نیز مرتفع گردید. هرچند پیش از آن نیز با توجه به مصادیق وسیله ی ارتکاب در متن ماده از جمله "مراسلات" امکان مجازات ارتکاب این بزه از طریق رایانه نیز وجود داشت.<sup>۹۴</sup>

## بند دوم: تشابه و تمایز نشر اکاذیب و افشای سر

این دو جرم از جهاتی با یکدیگر دارای نقاط مشترک هستند. نخست آنکه هردو از جمله جرایم علیه تمامیت معنوی اشخاص می باشند. مرتکب این دو جرم وصف و خصوصیت خاصی ندارد و هر کس می تواند مرتکب آن باشد. اما مهم ترین وجه اشتراک نشر اکاذیب و افشای سر به رفتار مجرمانه معطوف است. رفتار مرتکب در هر دو عبارت است از اظهار و انتشار

<sup>۹۲</sup> ولیدی، محمدصالح، حقوق جزای اختصاصی، جلد دوم، جرایم علیه اشخاص، امیرکبیر، تهران، ۱۳۸۱، ص ۳۴۸.

<sup>۹۳</sup> نظریه ی شماره ی ۷/۸۵۲۴.ا.ح.ق. ۱۳۸۲/۱۱/۷، مجموعه ی قانون مجازات اسلامی، ریاست جمهوری، معاونت پژوهش، تدوین و تنقیح قوانین و مقررات، عباس علی رحیمی اصفهانی و همکاران، ص ۴۷۰.

<sup>۹۴</sup> بای، حسینعلی و بابک پورقهرمانی، منبع پیشین، صص ۲۹۲-۲۹۴.

و افشا و در دسترس قرار دادن اطلاعات برای اشخاص ثالث. اگرچه موضوع دو جرم با هم یکسان نیست اما طریقه ی ارتکاب جرم موجب تشابه آن دو با یکدیگر می گردد.

اما از برخی جهات نیز با یکدیگر دارای تفاوت اند. اولاً از حیث موضوع بزه باید گفت در نشر اکاذیب و انتساب امور خلاف واقع، عدم صحت اظهارات مرتکب شرط تحقق بزه است. در واقع امور غیر واقعی موضوع این جرم را تشکیل می دهند، در حالی که در افشای سر، باید مطالب اظهار شده حتماً با واقعیت انطباق داشته باشد والا جرم ارتکاب نخواهد یافت. چرا که در صورت عدم صحت اظهارات مرتکب، موضوع جرم - اسرار متعلق به دیگری - منتفی می گردد و بدیهی است که جرم بدون موضوع نیز محقق نمی شود.

نتیجه ی حاصل از جرم دیگر وجه تمایز میان این دو بزه است. نشر اکاذیب یک جرم مطلق است. در این جرم تحقق نتیجه ی خاصی شرط جرم بودن عمل نیست. همان گونه که مقنن نیز در انتهای مواد مربوطه بر این امر تأکید داشته است. اما در بزه افشای سر موضوع ماده ی ۱۷ قانون جرایم رایانه ای قانون گذار صریحاً بیان کرده است: "به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود". از این نحوه ی بیان برمی آید که جرم افشای سر مقید به حصول نتیجه است.

وسیله ی ارتکاب نیز یکی از وجوه تمایز این دو است. چرا که در نشر اکاذیب وسیله موضوعیت دارد اما در افشای سر این گونه نیست. در رکن روانی نیز بنابر مطالب مطروحه در بند پیشین، به فرض آنکه معتقد بر این باشیم که انگیزه ی مرتکب در جرم نشر اکاذیب موضوعیت دارد، باید بگوییم در افشای سر انگیزه ی مرتکب تأثیری در تحقق جرم ندارد و تنها ممکن است در تشدید یا تخفیف مجازات مؤثر باشد.

## فصل دوم

# ارکان تشکیل دهنده ی بزه هتک حیثیت از طریق افشای سر در محیط مجازی

اکنون که با بیان نکات بنیادین مرتبط با موضوع این نوشتار، چهارچوب فکری ما شکل گرفته است، زمان آن است تا به مطالب اصلی ورود کنیم و اجزای مختلف جرم مورد نظر خود را دقیق تر بشناسیم. پیکره ی اصلی پژوهش حاضر را بازشناسی ارکان تشکیل دهنده ی بزه مورد بحث پدید می آورد. همان گونه که در منظر ارباب دانش حقوق کیفری مشهور است، اصولاً در تحلیل یک جرم در حقوق جزای اختصاصی سه رکن را برای آن برمی شمارند. رکن قانونی، مادی و روانی.

ما نسبت به این شیوه ی نگارش کتب و مقالات جزایی ایراداتی را وارد می دانیم چراکه رکن قانونی در حقیقت یک جزء سازنده ی بزه نیست. این مجرم است که بزه را پدید می آورد، حال آنکه وی رکن قانونی جرم را صورت نبسته است. بلکه مقنن است که رکن قانونی را تدارک می بیند و چنانکه واضح است مقنن را نمی توان دخیل در ارتکاب جرم دانست.

با این وجود ما نیز به پیروی از بزرگان این عرصه همین شیوه را در پیش می گیریم و مطالب این فصل را طی سه مبحث ارائه خواهیم نمود. در مبحث نخست، رکن قانونی این جرم را به بحث خواهیم گذاشت. در مبحث دوم نگاهی خواهیم داشت بر اجزای رکن مادی جرم که در حقیقت عصاره و واقعیت عینی جرم است. در مبحث پایانی این فصل نیز رکن روانی این جرم را در بوته ی نقد و بررسی خواهیم نهاد.

## مبحث اول: رکن قانونی

همان گونه که بیان شد، عنصر قانونی را نباید به عنوان یک رکن مجزا در ارکان تشکیل دهنده ی جرم مورد بررسی قرار داد. عنصر قانونی در واقع پرتوی از اصل قانونی بودن جرم و مجازات و زیربنای دیگر عناصر جرم است. به عبارت دیگر رکن قانونی، هم عرض دیگر ارکان جرم نیست تا در کنار آنها مورد بحث قرار گیرد، بلکه هم رکن مادی و هم روانی، مبتنی بر قانون هستند و بنابه تصریح قانون است که می توان رفتار یا حالت خاصی را به عنوان عنصر مادی یک بزه تحت تعقیب قرار داد.

بر این اساس به منظور شناخت قوانین حاکم در خصوص این بزه، مطالب این مبحث در دو گفتار ارائه می گردد تا در ابتدا قانون لازم الاجرا شناسایی گردد و سپس مواردی که ممکن است قوانین با یکدیگر دارای تعارض یا هم پوشانی باشند حل و فصل شود.

## گفتار اول: قوانین و مقررات مرتبط

در بحث از رکن قانونی هر بزه، باید دو موضوع دنبال شود: یکی برشمردن مواد قانونی که در آنها به جرم انگاری رفتار مورد نظر پرداخته شده است. و دیگری شناسایی و رفع تعارض احتمالی موجود بین مقرره های قانونی مورد اشاره. لذا در این مقال ابتدا قوانین مرتبط را مورد اشاره قرار می دهیم و در گفتار بعد قانون حاکم در حال حاضر را بازشناسی خواهیم نمود.

از سوی دیگر، به لحاظ آنکه جرایم سایبری پدیده ای نوظهور و حاصل پیشرفت تکنولوژی است، لذا در آغاز توجه حقوق دانان اروپا و امریکا را - به عنوان مهد پیدایش شبکه های رایانه ای و اینترنتی - به خود جلب نموده است. از این رو پیش از ورود به مباحث حقوق داخلی شایسته است تا نگاهی کوتاه به اسناد بین المللی داشته باشیم و ببینیم آیا در این اسناد مقرره ای در خصوص هتک حیثیت از طریق افشای سر به چشم می خورد یا خیر.

## بند اول: مقررات اسناد بین المللی

نخستین سند بین المللی که در مورد حریم خصوصی مباحثی را طرح نموده است، اعلامیه ی جهانی حقوق بشر ۱۹۴۸ است. در ماده ی ۱۲ این اعلامیه آمده است: «احدی در

زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود نباید مورد مداخله های خودسرانه واقع شود و شرافت و اسم و رسمش نباید مورد تعرض قرار گیرد. هرکس حق دارد در مقابل این گونه مداخلات و حملات مورد حمایت قانون قرار گیرد.<sup>۹۵</sup> همان طور که ملاحظه می شود، ماده ی فوق الاشعار تنها به صورت یک توصیه نامه ی غیر الزام آور و بدون مخاطب قرار دادن دولت ها، حق انسان بر حریم خصوصی و خانوادگی را به رسمیت شناخته و حیثیت و شرافت انسانی را مورد حمایت قرار داده است. اما این مطلب با توجه به ماهیت این سند که یک اعلامیه است، مشکل آفرین نخواهد بود. امروزه با تأکیدات مکرری که بر محتوای آن شده به یک عرف بین المللی تبدیل شده است و برای امضا کنندگان لازم الاجرا محسوب می شود و برخی از قواعد آن به قاعده ی آمره ی بین المللی تبدیل شده اند. لذا پیشبینی برخی مقررات در حقوق داخلی را شاید بتوان متأثر از همین اعلامیه دانست.

این حق ذاتی برای انسان مجدداً در بند ۲ ماده ی ۲۹ همان اعلامیه مورد تأکید قرار گرفته است. این بند مقرر داشته: «هرکس در اجرای حقوق و استفاده از آزادی های خود فقط تابع محدودیت هایی است که به موجب قانون منحصرأ به منظور رسمیت یافتن و مراعات حقوق و آزادی های دیگران و برای مقتضیات صحیح اخلاقی و نظم عمومی و رفاه همگانی در شرایط یک جامعه ی مردم سالار وضع گردیده است.»

دیگر سند بین المللی، میثاق بین المللی حقوق مدنی و سیاسی ۱۹۷۶ است. این میثاق نیز یک سند الزام آور حقوقی است که دولت های عضو متعهد به رعایت مفاد آن گردیده اند. در ماده ی ۱۷ این سند آمده است: «۱- هیچکس نباید در زندگی خصوصی و خانوادگی و اقامتگاه یا مکاتبات خود مورد مداخله ی خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد و همچنین شرافت و حیثیت او نباید مورد تعرض غیر قانونی واقع شود. ۲- هرکس حق دارد در مقابل اینگونه مداخلات یا تعرض ها از حمایت قانون برخوردار باشد.» نظر به اینکه کشور ما نیز از امضا کنندگان اعلامیه ی جهانی حقوق بشر و همچنین عضو میثاق بین المللی حقوق مدنی و سیاسی است، لذا متعهد به مفاد این اسناد و از جمله حمایت از حریم خصوصی و خانوادگی

---

<sup>۹۵</sup> آل محمد، فاطمه، سیاست جنایی ایران در قبال جرایم رایانه ای، پایان نامه ی کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده ی حقوق و علوم سیاسی دانشگاه شیراز، فروردین ۱۳۹۰، صص ۷۸-۸۰.

افراد ملت می باشد. به ویژه که بر اساس ماده ی ۹ قانون مدنی مقررات عهدی که بر طبق قانون اساسی بین دولت ایران و سایر دول منعقد شده باشد در حکم قانون است. لذا در خصوص نقض حق بر حریم خصوصی افراد، ماده ی ۱۷ میثاق در دادگاه قابل استناد است.<sup>۹۶</sup>

دیگر سند بین المللی که حق بر حریم خصوصی را برای افراد به رسمیت شناخته است اعلامیه ی جهانی حقوق بشر اسلامی است که در برخی مواد خود تجاوز به حریم خصوصی و از آن جمله استراق سمع را ممنوع و قابل تعقیب دانسته است. این حق در اعلامیه ی جهانی حقوق بشر فرانسه نیز مورد تأیید و تأکید قرار گرفته است.

موارد پیش گفته به طور کلی به حمایت از حریم خصوصی اختصاص یافته است. اما به طور خاص و در عرصه ی فضای سایبر، در این اسناد مطلبی در حمایت از حق بر حریم خصوصی یافت نمی شود. در وضعیت کنونی، با وجود تلاش نهادهای فراملی از جمله شورای اروپایی و اتحادیه ی اروپا و دیگر سازمان ها، شاید بتوان گفت مهم ترین سند بین المللی، کنوانسیون بوداپست ۲۰۰۱ می باشد. کمیته ی وزرای شورای اروپا در سال ۱۹۹۷ (کمیته ی متخصصین جرایم سایبر) را جهت ارائه ی پیش نویس یک کنوانسیون در این خصوص تشکیل داد که نهایتاً پیش نهاد خود را در سال ۲۰۰۱ ارائه نمود است. سرانجام در ۲۳ سپتامبر همان سال در بوداپست مجارستان به امضای کشورهای عضو شورای اروپا و چهار کشور ایالات متحده، کانادا، ژاپن و افریقای جنوبی رسید. این کنوانسیون که دارای ۴ فصل است، مقررات مختلفی را پیش بینی نموده است. در برخی از مواد آن ضوابطی در خصوص حمایت از حریم خصوصی افراد به چشم می خورد. اما این مقررات بیشتر ناظر به جرم دست یابی غیر مجاز به سیستم های رایانه ای است و در مورد جرم افشای اسرار در محیط مجازی حکم خاصی دیده نمی شود.<sup>۹۷</sup> از این رو این قانون گذار داخلی است که باید در جهت تکمیل مقررات بین المللی گام بردارد و قوانین کامل تری را با جزئیات بیشتر به تصویب رساند.

---

<sup>۹۶</sup> یزدانی زوز، هرمز، حریم خصوصی در فضای سایبر، حقوق فناوری اطلاعات و ارتباطات، (مجموعه ی مقالات)، معاونت حقوقی توسعه ی قضایی قوه ی قضائیه، مرکز مطالعات توسعه ی قضایی، بزرگداشت استاد حسن دزینی، گردآوری امیرحسین جلالی فراهانی، انتشارات روزنامه ی رسمی، تهران، ۱۳۸۸، صص ۱۵۰-۱۵۲.

<sup>۹۷</sup> ترکی، غلام عباس، نگرش علمی کاربردی به قانون جرایم رایانه ای، ماهنامه شماره ۷۷، سال سیزدهم، آذر و دی ۱۳۸۸، صص ۱۲-۱۳.



## بند دوم: قوانین و مقررات داخلی

پس از گذری اجمالی بر اسناد بین المللی، در اینجا نگاهی به مقررات داخلی کشورمان خواهیم داشت که در آنها در خصوص بزه افشای اسرار خصوصی از طریق ابزار و آلات دیجیتال و رایانه ای ضوابطی پیش بینی و جرم انگاری گردیده است. مطالب این بند را در چند قسمت بنا بر تعدد قوانین موضوعه ارائه می کنیم.

### (۱) قانون تجارت الکترونیک:

این قانون که در سال ۱۳۸۲ پس از نقد و بررسی آن در کمیسیون صنایع و معادن مجلس شورای اسلامی - که خود از نکات جالب توجه این قانون به شمار می رود -<sup>۹۸</sup> در صحن علنی مجلس مطرح و به تصویب رسید، شاید نخستین جرقه در نظام تقنینی کشور ما بود که حاکی از توجه مقنن به جرم انگاری در خصوص محیط مجازی است. در این قانون برای اولین بار ضمن جرم انگاری کلاه برداری و جعل رایانه ای و برخی عناوین دیگر، برای این بزه ها مجازات هایی نیز مقرر داشت که البته چندان با میزان خسارات ناشی از این قبیل جرایم متناسب نبود.

در همین قانون بود که طی چند ماده در خصوص حمایت از داده پیام های شخصی مقرراتی وضع گردیده و مجازات هایی نیز برای ناقضان این امر پیش بینی شده است. از این رو رکن قانونی بزه نقض حمایت از داده پیام های شخصی یک عنصر قانونی مرکب است. چراکه در چند ماده حمایت های قانونی از داده پیام های شخصی را برشمرده و در چند ماده ی دیگر تخلف از این مواد را مستوجب مجازات های معینی قرار داده است. در ماده ی ۵۸ این قانون آمده است: «ذخیره، پردازش و یا توزیع داده پیام های شخصی مبین ریشه های قومی یا نژادی، دیدگاه های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیر قانونی است»

ماده ی ۵۹: «در صورت رضایت شخص موضوع داده پیام نیز، به شرط آنکه محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد، ذخیره، پردازش و توزیع داده پیام

<sup>۹۸</sup> دزیانی، محمد حسن، مقدمه ای بر سیاست جنایی جرایم سایبری، ماهنامه ی قضاوت، شماره ی ۴۰، مهر ۸۵، صص ۵۴-۵۵.

های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد: الف- اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند. ب- داده پیام باید تنها به اندازه ی ضرورت و متناسب با اهدافی که در هنگام جمع آوری برای شخص موضوع داده پیام شرح داده شده جمع آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد. ج- داده پیام باید صحیح و روزآمد باشد. د- شخص موضوع داده پیام باید به پرونده های رایانه ای حاوی داده پیام های شخصی مربوط به خود دسترسی داشته و بتواند داده پیام های ناقص یا نادرست را محو یا اصلاح کند. ه- شخص موضوع داده پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده ی رایانه ای داده پیام های شخصی خود را بنماید.»

ملاحظه می گردد که در ضمن این دو ماده به جرم انگاری پاره ای از رفتارها که متضمن نوعی از اشاعه و انتشار اطلاعات خصوصی و محرمانه است اقدام گردیده است. همان گونه که ماده ی ۵۸ مقرر نموده هر نوع ذخیره، پردازش و یا توزیع داده پیام های شخصی حساس با لحاظ سایر شرایط جرم دانسته شده است. این مقرر گامی در جهت ممانعت از انتشار اطلاعات و اسرار خصوصی افراد در فضای سایبر است. ماده ی ۵۹ نیز برای انتشار داده پیام های شخصی و اسرار خصوصی افراد در صورت رضایت آن ها شرایط پنج گانه ای مقرر داشته است. در صورت عدم رعایت این شرایط در انتشار یا ذخیره و پردازش داده های شخصی و خصوصی، ماده ی ۷۱ قانون تجارت الکترونیک قابلیت اجرا خواهد یافت که در حقیقت مکمل رکن قانونی بزه موضوع ماده ی ۵۸ و ۵۹ می باشد.

ماده ی ۷۱: «هرکس در بستر مبادلات الکترونیکی شرایط مقرر در مواد ۵۸ و ۵۹ این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می شود.»

در ادامه قانون گذار برای مواردی که جرایم راجع به نقض محرمانگی داده پیام های شخصی توسط دفاتر صدور گواهی الکترونیک ارتکاب می یابد نیز مجازات مقرر داشته است. نکته ی مهم آنکه در صورت ارتکاب این جرم به شکل غیر عمد و بر اثر بی احتیاطی یا بی مبالاتی بوسیله ی آن دفاتر یا مراجع نیز مجازات مقرر شده است.

ماده ی ۷۲: «هرگاه جرایم راجع به داده پیام های شخصی توسط دفاتر صدور گواهی الکترونیکی و سایر نهادهای مسئول ارتکاب یابد، مرتکب به حد اکثر مجازات مقرر در ماده ی ۷۱ محکوم خواهد شد»

ماده ی ۷۳: «اگر به واسطه ی بی مبالاتی و بی احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرایم راجع به داده پیام های شخصی روی دهد مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل پنجاه میلیون ریال محکوم می شود»<sup>۹۹</sup>

## ۲- قانون تشدید مجازات کسانی که در امور سمعی بصری فعالیت غیر مجاز می کنند

این قانون که زمینه ی تصویب آن یکی از جنجالی ترین حوادث چند سال اخیر در کشور ما محسوب می گردد، در سال ۱۳۸۶ و متعاقب تکثیر و توزیع یک سی دی حاوی تصاویری منسوب به یکی از بازی گران تلویزیون و با نهایت سرعت و شتاب زدگی به تصویب نمایندگان مجلس شورای اسلامی رسید و فوراً مورد تأیید شورای نگهبان نیز قرار گرفت.<sup>۱۰۰</sup> این قانون همان گونه که از نامش بر می آید، در صدد تشدید مجازات برخی افراد است که بدون توجه به ارزش ها و هنجارهای حاکم بر جامعه، با اقدامات خود موجب جریحه دار شدن احساسات مردم می گردند و آبرو و حیثیت دیگران - مخصوصاً افراد مشهور و سرشناس جامعه - را بازیچه ی امیال خویش قرار می دهند.

توضیح آنکه سابق بر این قانون، در سال ۱۳۷۲ قانون نحوه ی مجازات اشخاصی که در امور سمعی بصری فعالیت غیر مجاز دارند به تصویب مجلس شورای اسلامی رسیده بود. اما به لحاظ ضعف ضمانت اجرایی و نامتناسب بودن مجازات های مقرر در آن قانون و نیز شدت آثار سوء ناشی از اتفاق پیش گفته، نمایندگان بر آن شدند تا مجازات این قبیل بزهکاران را تشدید نمایند.

آنچه از این قانون در این نوشتار مد نظر ما است موادی از آن است که مربوط به تهیه ی فیلم و عکس از فضاهای خصوصی و خانوادگی و نیز اماکن مخصوص بانوان و سپس تکثیر و توزیع آن در جامعه است که موجب ورود صدمات و لطمات جبران ناپذیری بر حیثیت و شرافت قربانیان این جرم می گردد. در این قانون در چند ماده به طور صریح و یا ضمنی به این بزه توجه گردیده و مجازات های شدیدی نیز مقرر شده است.

<sup>۹۹</sup> جاویدنیا، جواد، جرایم تجارت الکترونیکی، نشر خورسندی، تهران، ۱۳۸۷، صص ۳۳۴-۳۳۵.

<sup>۱۰۰</sup> جوانمرد، بهروز، تسامح صفر: سیاست کیفی سخت گیرانه در قبال جرایم خرد، بنیاد حقوقی میزان، تهران، ۱۳۸۸، صص ۶۸-۷۶.

از جمله ماده ی ۳ مقرر داشته: «عوامل تولید، توزیع، تکثیر و دارندگان آثار سمعی و بصری غیرمجاز اعم از این که مجوز فعالیت از وزارت فرهنگ و ارشاد اسلامی داشته و یا بدون مجوز باشند با توجه به محتوای اثر حسب مورد علاوه بر ابطال مجوز به یکی از مجازاتهای مشروحه ذیل محکوم خواهند شد. الف - عوامل اصلی 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 (۱۰۰,۰۰۰,۰۰۰) ریال جریمه نقدی و محرومیت اجتماعی به مدت هفت سال و در صورت تکرار به دو تا پنج سال حبس و ضبط تجهیزات مربوطه و دویست میلیون (۲۰۰,۰۰۰,۰۰۰) ریال جزای نقدی و محرومیت اجتماعی به مدت ده سال محکوم می‌شوند. چنانچه عوامل فوق‌الذکر یا افراد زیر از مصادیق مفسد فی‌الارض شناخته شوند، به مجازات آن محکوم می‌گردند....»

همچنین ماده ی ۴ مقرر می‌دارد: «هر کس با سوء استفاده از آثار مبتذل و مستهجن تهیه شده از دیگری، وی را تهدید به افشاء و انتشار آثار مزبور نماید و از این طریق با وی زنا نماید به مجازات زنا به عنف محکوم می‌شود ولی اگر عمل ارتكابی غیر از زنا و مشمول حد باشد حد مزبور بر وی جاری می‌گردد و در صورتی که مشمول تعزیر باشد به حداکثر مجازات تعزیری محکوم خواهد شد.»

در ادامه ماده ی ۵ همان قانون به پیش بینی مقرراتی در خصوص تهیه ی فیلم از اماکن و مراسم خانوادگی می‌پردازد. ماده ی ۵: «مرتکبان جرائم زیر به دو تا پنج سال حبس و ده سال محرومیت از حقوق اجتماعی و هفتاد و چهار ضربه شلاق محکوم می‌شوند: الف... ب - تهیه فیلم یا عکس از محل‌هایی که اختصاصی بانوان بوده و آنها فاقد پوشش مناسب می‌باشند مانند حمامها و استخرها و یا تکثیر و توزیع آن. ج - تهیه مخفیانه فیلم یا عکس مبتذل از مراسم خانوادگی و اختصاصی دیگران و تکثیر و توزیع آن.»

ماده ی ۸ نیز به پیش بینی مجازات برای مأموران صلاحیت دار ضابطین دادگستری، مدیران و کارکنان بخش های دولتی، خصوصی عمومی و غیره که به مناسبت انجام وظیفه و اقتضای شغلی آثار مستهجن در اختیارشان قرار می‌گیرد و با سوء نیت آن آثار را تکثیر یا توزیع می‌کنند، پرداخته و حتی فراتر از آن در صورت افشای این قبیل آثار بر اثر مسامحه و

سهل انگاری، مقصر مسامحه کار نیز به حبس و جزای نقدی محکوم می گردد که نشان از شدت سخت گیری مقنن در این خصوص دارد.

در نهایت ماده ی ۱۰ توجه خود را معطوف بر ارتکاب اعمال مجرمانه از طریق سامانه های رایانه ای نموده مقرر می دارد: «انتشار آثار مستهجن و مبتذل از طریق ارتباطات الکترونیکی و سایتهای کامپیوتری یا وسیله و تکنیک مشابه دیگر از مصادیق تکثیر و انتشار محسوب و مرتکب حسب مورد به مجازات مقرر در این قانون محکوم می شود.»

ملاحظه می گردد که قانون فوق الاشعار طی مواد متعددی به جرم انگاری مصادیقی از رفتارهای ناقض حریم خصوصی افراد پرداخته است که هر یک نیاز به نقد و ارزیابی دارد. اما به فاصله ی نسبتاً کوتاهی از تصویب این قانون، در سال ۱۳۸۸ قانون جرایم رایانه ای و مخصوصاً ماده ی ۱۷ آن به تصویب رسید که قانون فوق را تا حد زیادی تحت الشعاع قرار داد. پس از اشاره ای مختصر به مقرره ی قانونی قانون جرایم رایانه ای به بررسی حدود نسخ قانون تشدید مجازات فعالان امور سمعی بصری خواهیم پرداخت.

### ۳- قانون جرایم رایانه ای

در اوایل سال ۱۳۸۸ قانونی از تصویب نمایندگان مجلس گذشت که سرگذشتی پر فراز و نشیب را طی کرده بود. اندیشه ی تدوین این قانون به سال ۱۳۸۱ برمی گردد. این قانون به صورت یک لایحه ی قضایی توسط رئیس قوه ی قضائیه تهیه و ارائه گردید. پس از نقد و بررسی های گسترده پیرامون آن و نیز ایجاد تغییراتی بنیادین در مزکز پژوهش های مجلس سر انجام این لایحه به صحن علنی مجلس رسید و پس از تصویب و ارجاع به شورای نگهبان و طرح ایرادات جزئی و رفع آن ها از سوی مجلس نهایتاً به تصویب نهایی مجلس و تأیید شورای نگهبان رسید.<sup>۱۰۱</sup> این قانون که با عنوان قانون جرایم رایانه ای به تصویب رسید و در نتیجه ی بروز ابتکار و خلاقیت برخی از نمایندگان (؟) به انتهای قانون مجازات اسلامی الحاق گردید، به تبعیت از کنوانسیون ۲۰۰۱ بوداپست در چند فصل، جرایم رایانه ای را برشمرده است و در

<sup>۱۰۱</sup> - برای مطالعه ی تفصیلی در این خصوص ر.ک: عالی پور، حسن، حقوق کیفری فناوری اطلاعات، معاونت حقوقی و توسعه ی قضایی قوه ی قضائیه، مرکز مطالعات توسعه ی قضایی، خورسندی، تهران، ۱۳۸۹، صص ۳۶۸-۳۷۹.

بخش دوم نیز آیین دادرسی این جرایم را پیش بینی نموده است. در بخش اول این قانون طی سه فصل جرایم رایانه ای مدرن مبتنی بر کنوانسیون بوداپست پیش بینی گردیده و در دو فصل بعد متأثر از حقوق بومی و داخلی دو دسته جرایم علیه عفت و اخلاق عمومی و هتک حیثیت و نشر اکاذیب پیش بینی گردیده است.

آنچه در اینجا مد نظر ما است، ماده ی ۱۷ این قانون است که در خصوص افشای اسرار خصوصی یا خانوادگی از طریق سامانه های رایانه ای اقدام به جرم انگاری نموده است. این ماده مقرر می دارد: « هرکس به وسیله سیستم های رایانه ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری راجز در موارد قانونی بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

## گفتار دوم: بازشناسی جایگاه قوانین حاکم

پس از اشاره به مواد قانونی موجود پیرامون موضوع، اکنون باید به این سؤال پاسخ داد که در مقام رسیدگی و صدور حکم نهایتاً کدام یک از مقررهای قانونی مورد اشاره را باید بر دیگری رجحان نهاد. به عبارت دیگر ناسخ و منسوخ و عام و خاص در میان این قوانین کدامند و چگونه می توان تعارض ظاهری بین آن ها را مرتفع ساخت. در این گفتار به این موضوع می پردازیم.

به نظر ما به لحاظ قلمرو و موضوع هریک از سه قانون پیش گفته نمی توان قائل به نسخ کلی یک قانون توسط قانون دیگر شد. چراکه هریک از این قوانین در نوع خود یک قانون خاص بوده و ناظر به موضوع قانون دیگر نمی باشند. هرچند که تکنولوژی و رایانه در ارتکاب بزه های موضوع این سه قانون دخالت دارد و بدین لحاظ قانون جرایم رایانه ای را می توان یک قانون عام الشمول دانست، اما به عنوان مثال قانون تجارت الکترونیک، تنها ناظر به جرایمی است که در بستر مبادلات الکترونیکی رخ می دهد و از این حیث قانون جرایم رایانه ای را نمی توان ناسخ آن - حد اقل در مورد بزه افشای داده پیام های شخصی - دانست. هرچند در مورد

برخی از جرایم مثل کلاهبرداری یا جعل رایانه ای باید قائل به نسخ جزئی قانون باشیم که از موضوع بحث ما خارج است. همچنین است در مورد قانون تشدید مجازات اشخاصی که در امور سمعی بصری فعالیت غیر مجاز می کنند که با وجود نسخ برخی از مواد آن، اما سایر مواد به قوت خود باقی هستند. از این رو به لحاظ اعتقاد به عدم نسخ کلی، باید در مورد قلمرو هر یک از قوانین جداگانه بحث کنیم. مطالب این گفتار طی سه بند ارائه خواهد شد.

## بند اول: قانون تجارت الکترونیک

در بررسی مواد مرتبط از این قانون با بزه افشای اسرار خصوصی، و در مقایسه ی آن با قانون جرایم رایانه ای باید به چند نکته توجه نمود.

اول اینکه با توجه به عنوان این قانون، قلمرو آن تنها محدود به جرایمی است که در بستر مبادلات الکترونیکی به وقوع می پیوندد. این شرط اساسی را می توان از عبارت صدر ماده ی ۷۱ که در مقام پیش بینی مجازات برای رفتارهای خلاف قانون است، برداشت نمود. از این رو استناد به قانون تجارت الکترونیک در غیر از مواردی که موضوع جنبه ی تجارت الکترونیکی یابد، فاقد وجهه ی حقوقی است.

دیگر آنکه اگرچه فصل اول از مبحث اول از باب سوم قانون تجارت الکترونیک به موضوع حمایت از داده پیام های شخصی اختصاص یافته، اما قلمرو شمول آن فراتر از بزه افشای اسرار خصوصی از طریق رایانه و در معنای وسیع تر، فضای مجازی است. با نگاهی به ماده ی ۵۸ و ۵۹ - که در مقام برشمردن رفتارهای ممنوعه ی دارای وصف مجرمانه اند می باشد - به روشنی در می یابیم که رفتارهای مجرمانه ی موضوع این مواد، بسیار متنوع و متعدداند. این موارد که اعم از فعل یا ترک فعل هستند، در دو ماده ی فوق الاشعار به این شرح برشمرده شده اند حال آنکه بزه موضوع ماده ی ۱۷ قانون جرایم رایانه ای تنها از طریق یک فعل مثبت به وقوع می پیوندد:

- ۱- ذخیره، پردازش و یا توزیع داده پیام های شخصی حساس بدون رضایت
- ۲- ذخیره، پردازش و توزیع داده پیام های شخصی حساس با محتوای خلاف قانون
- ۳- عدم تعیین و شرح اهداف ذخیره، پردازش و توزیع داده پیام های شخصی حساس

۴- جمع آوری داده پیام های شخصی حساس بدون ضرورت

۵- جمع آوری و استفاده از داده پیام های شخصی حساس خارج از اهداف تعیین شده

۶- ذخیره، پردازش و توزیع داده پیام های شخصی حساس اشتباه یا غیر روزآمد

۷- عدم ایجاد امکان دست رسی شخص به داده پیام های شخصی حساس مربوط به خود

۸- عدم ایجاد امکان محو یا اصلاح داده پیام های شخصی حساس ناقص یا نادرست

۹- عدم پذیرش و بررسی درخواست محو کامل داده پیام های شخصی حساس<sup>۱۰۲</sup>

ملاحظه می شود که به لحاظ موضوع این قانون، موارد متعددی از رفتارهای ممنوعه پیش بینی گردیده و برای آن مجازات مقرر شده است. از میان موارد نه گانه ی فوق تنها موارد ۱، ۲، ۴ و ۵ را می توان برشمرد که به نوعی با بزه پیش بینی شده در قانون جرایم رایانه ای مرتبط هستند.<sup>۱۰۳</sup> با جمع شرایط مقرر در ۴ مورد مجرمانه می توان گفت: «هر گونه جمع آوری، ذخیره، پردازش و استفاده از داده پیام های شخصی حساس بدون رضایت یا برخلاف قانون یا بدون ضرورت جرم است.» اگر عبارت فوق را رکن قانونی بزه سوء استفاده از داده پیام های شخصی حساس موضوع قانون تجارت الکترونیک بدانیم، در مقایسه ی آن با قانون جرایم رایانه ای باید گفت رفتارهای پیش بینی شده در قانون تجارت الکترونیک دارای تنوع بیشتری است و از این حیث این قانون عام تر است، چراکه شامل جمع آوری، ذخیره، پردازش و استفاده از این اطلاعات می گردد، حال آنکه قانون جرایم رایانه ای تنها دو رفتار توزیع و در دسترس دیگران قرار دادن را مورد حکم قرار می دهد.

اما موضوع بزه در قانون جرایم رایانه ای عام تر است. چراکه اعم از صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری است و محدود به قید حساس نگردیده است. اما در قانون تجارت الکترونیک تنها داده پیام های شخصی حساس مورد حمایت اند. منظور از داده پیام های شخصی حساس نیز، هر نوع داده ای است که مبین ریشه های قومی یا نژادی، دیدگاه های عقیدتی، خصوصیات اخلاقی یا راجع به وضعیت جسمانی، روانی یا جنسی اشخاص باشد. از سوی دیگر در خصوص ضرورت تحقق نتیجه، جرم افشای اسرار خصوصی موضوع ماده

<sup>۱۰۲</sup> جاویدنیا، جواد، منبع پیشین، صص ۳۳۵-۳۴۳

<sup>۱۰۳</sup> سوادکوهی فر، سام، تحلیلی بر مقررات جزایی IT در ایران، ماهنامه ی شماره ی ۴۵، سال هشتم، مرداد و شهریور ۱۳۸۳، صص



ی ۱۷ قانون جرایم رایانه ای مقید بوده و باید عنصر ضرر قربانی یا هتک حیثیت او نیز احراز گردد. حال آنکه در قانون تجارت الکترونیک بزه های مورد نظر مطلق بوده و صرف جمع آوری، ذخیره، پردازش یا استفاده از آنها به نحوی که قانون مقرر داشته، جرم است.

نکته ی پایانی در مورد این قانون آن است که وجود وصف و خصوصیتی ویژه در مرتکب موجب تشدید مجازات خواهد شد. آن هم در صورتی است که بزه های موضوع قانون تجارت الکترونیک توسط مسئولان دفاتر خدمات صدور گواهی الکترونیک یا دیگر مقامات مسئول ارتکاب یابد که در این فرض تحقق غیر عمدی بزه نیز جرم شناخته شده است.<sup>۱۰۴</sup>

در جمع بندی حدود اعتبار قانون تجارت الکترونیک در مقابل قانون جرایم رایانه ای باید گفت این قانون اساساً به لحاظ قلمرو خود همچنان دارای اعتبار بوده و نمی توان با تصویب قانون جرایم رایانه ای نظر بر نسخ آن - در مورد جرم نقض محرمانگی داده پیام های خصوصی- داشت، بلکه با لحاظ شرایط و کیفیات حاکم بر هر پرونده می توان به این قانون استناد نمود. آری، در خارج از فضای مبادلات الکترونیک افشای اسرار خصوصی افراد مشمول قانون جرایم رایانه ای خواهد بود.

## بند دوم: قانون امور سمعی و بصری

برای مقایسه ی این قانون با قانون جرایم رایانه ای و تشخیص حدود نسخ آن نیز باید به نکاتی چند عنایت داشت.

اول اینکه ماده ی ۱۰ قانون فوق الذکر را می توان به استناد مواد ۱۴، ۱۶ و ۱۷ قانون جرایم رایانه ای منسوخ دانست. چراکه ماده ی ۱۰ فوق الاشعار در خصوص انتشار آثار مستهجن و مبتذل از طریق ارتباطات الکترونیکی و سایت های کامپیوتری یا وسیله یا تکنیک مشابه دیگر است. این ماده موارد پیش گفته را از مصادیق تکثیر و انتشار محسوب نموده و مرتکب را حسب مورد مشمول مجازات های مندرج در آن قانون دانسته است. اما با تصویب قانون جرایم رایانه ای و به استناد ماده ی ۵۶ آن قانون، کلیه ی قوانین و مقررات مغایر ملغی

<sup>۱۰۴</sup> عالی پور، حسن، منبع پیشین، صص ۳۸۹-۳۹۱.

گردیده است. به لحاظ این که در مواد ۱۵، ۱۶ و ۱۷ قانون جرایم رایانه ای نیز صریحاً در مورد تکثیر و توزیع آثار مستهجن احکامی مقرر گردیده است، لذا تردیدی در خصوص نسخ ماده ی ۱۰ قانون سال ۱۳۸۶ باقی نمی ماند.<sup>۱۰۵</sup>

اما در خصوص مواد ۳، ۴، ۵ و ۸ آن قانون مسأله جای تأمل است. در این مواد علاوه بر پیش بینی برخی جرایم که از اقسام حدود است - مانند ماده ی ۴ که بدون هیچ گونه ضرورتی و در ضمن جرم انگاری وسیله ی تهدید قرار دادن آثار حاوی تصاویر و فیلم های مستهجن، به ارتکاب زنا نیز اشاره کرده و مرتکب را مستحق اعمال حد زنا دانسته است - جرایم تعزیری خاصی نیز مقرر گردیده که برخی مصادیق آن با ماده ی ۱۷ قانون جرایم رایانه ای هم پوشانی و تعارض دارد.

به عنوان مثال ماده ی ۳ قانون مذکور، برای عوامل اصلی تکثیر و توزیع عمده ی آثار سمعی بصری مستهجن در صورتی که مصداق مفسد فی الارض نباشند، مجازات های تعزیری مقرر داشته است. در مقایسه با موضوع ماده ی ۱۷ قانون جرایم رایانه ای، چنانچه تصویر تهیه شده از دیگری که بوسیله ی مرتکب منتشر می گردد، در نتیجه ی عدم رضایت قربانی به گونه ای باشد که مصداق آثار مستهجن قلمداد گردد، در این صورت مورد مشمول هر دو عنوان مذکور در ماده ی ۳ و ۱۷ خواهد بود.

در خصوص ماده ی ۴، چنان که پیش تر نیز اشاره شد، این ماده علی رغم شداد و غلاظی که در آغاز آن دیده می شود اما عملاً مجازات خاصی برای اعمال ممنوعه ی مندرج مقرر نداشته و تنها به بیان حکم ارتکاب زنا یا دیگر اعمال مستوجب حد بسنده نموده و در پایان ماده - که علی القاعده عصاره و جان مواد کیفری است چراکه در اینجاست که مجازات عمل ممنوعه تعیین می گردد - تنها با این بیان قضیه را به اجمال برگزار کرده است: « و در صورتی که مشمول تعزیر باشد به حداکثر مجازات تعزیری محکوم خواهد شد.» جالب اینجاست که این ماده در مقام تعیین همان جرم تعزیری بوده و گویا نمایندگان محترم آنچنان متأثر و متألم از حوادث جاری مملکت گردیده اند که فراموش کرده اند برای این جرم مجازاتی پیش

<sup>۱۰۵</sup> عالی پور، حسن، همان، صص ۳۹۰-۳۹۱.

بینی کنند تا مرتکب به حد اکثر آن مجازات محکوم گردد. به هر تقدیر رکن قانونی جرم در این ماده ناقص و مبهم مانده و لذا در مقام صدور حکم نمی توان به آن استناد نمود.

و اما در خصوص مواد ۵ و ۸ اگرچه مصادیق مندرج در این مواد تا حدود زیادی منطبق بر ماده ی ۱۷ قانون جرایم رایانه ای است، که ما را ناگزیر از این می سازد که نظر بر نسخ مواد تا حدی که بتوان آنها را با ماده ی ۱۷ منطبق ساخت، داشته باشیم. اما در جمع بندی حدود اعتبار قانون تشدید مجازات کسانی که در امور سمعی بصری فعالیت غیر مجاز می کنند باید گفت این قانون در اکثر موارد بوسیله ی قانون جرایم رایانه ای نسخ گردیده است. به عبارت دیگر به لحاظ مؤخر التصویب بودن قانون جرایم رایانه ای، در هر مورد که بتوان قانون اخیر التصویب را جاری نمود، باید نظر بر نسخ قانون امور سمعی بصری داشت. اما در مواردی که قانون جرایم رایانه ای دارای نقص و اجمال بوده و نتوان مورد را با ماده ی ۱۷ تطبیق داد، ناگزیر باید به قانون امور سمعی بصری استناد نمود. هرچند این اقدام مقنن، نه برخاسته از اهتمام و دقت نظر نمایندگان که ناشی از سهل انگاری و بی توجهی نسبت به امور مهم و بنیانی جامعه است. شاید از لحاظ حقوقی گفته شود که قانون امور سمعی بصری در سال ۸۸ نسخ گردیده است، اما با نگاهی به میزان مجازات مندرج در قانون سال ۸۸ - که در مقایسه با میزان آثار مخرب ناشی از بزه انتشار اسرار خصوصی و خانوادگی افراد بسیار اندک و فاقد وصف بازدارندگی است - می توان چنین نتیجه گرفت که مقنن ایرانی در تصویب قوانین عموماً دچار شتاب زدگی و درگیر احساسات خویش است. والا قانونی که با آن شدت و سخت گیری نسبت به متجاوزان به حریم خصوصی افراد و با قید یک فوریت به تصویب می رسد، نباید طی یک سال به فراموشی سپرده شده و نسخ گردد. هرچند که آن قانون نیز خالی از اشکال نبوده که فوقاً به برخی از ایرادات آن اشاره شد.

در جمع بندی نهایی باید گفت قانون جرایم رایانه ای اصولاً بر موارد افشای اسرار خصوصی و خانوادگی حاکم خواهد بود مگر در مواردی که نتوان ماده ی ۱۷ را جاری نمود که در این صورت به قانون امور سمعی بصری سال ۱۳۸۶ استناد خواهد شد. البته استناد یا عدم استناد به یک قانون به دقت نظر و میزان اهمیت دادرسی رسیدگی کننده به پرونده بستگی دارد و چه بسا به نظر برخی قضات قانون سال ۸۶ به لحاظ خاص بودن موضوع آن کماکان قابل

استناد باشد. البته این اختلاف نظر و تضارب آراء در علوم انسانی کاملاً معمول و موجب رشد و بالندگی علم و دانش است.

## بند سوم: قانون جرایم رایانه‌ای

پس از نگاهی بر دو منبع قانونی موجود در خصوص بزه افشای اسرار خصوصی در محیط مجازی، نگاهی نیز خواهیم داشت بر آخرین متن قانونی مصوب در این خصوص که کوشیده است تا تمام مقررات مربوط به جرایم مرتبط با سامانه های رایانه ای را یکپارچه کند. البته با توجه به قلمرو بحث در این گفتار تنها از جهت رکن قانونی بزه، به این مقرر ی کیفری می نگریم.

ماده ی ۱۷ قانون جرایم رایانه ای را می توان به عنوان رکن قانونی عام بزه هتک حیثیت از طریق افشای اسرار در محیط مجازی دانست. منظور این است که اولاً قانون جرایم رایانه ای در عین خاص بودن، دارای مقررات عام الشمولی در خصوص بزه های رایانه ای است. ضمن آنکه در آخرین ماده ی این قانون به طور کلی تمامی قوانین و مقررات مغایر ملغی گردیده است.

ثانیاً از لحن ماده ی فوق الاشعار نیز چنین مستفاد می گردد که مقنن با وضع یک مقرر ی واحد ضمن مرتفع ساختن خلأهای قانون در برخی موارد، با تأکید بر برخی عناوین مجرمانه که سابقاً در قانون مجازات افرادی که در امور سمعی بصری فعالیت غیر مجاز دارند، و با کاهش مجازات مقرر برای این بزه نسبت به آن قانون، به نوعی در جهت تعدیل مجازات های بسیار شدید و نامتعارف مندرج در آن قانون اقدام کند.

البته پیش بینی مجازات های نسبتاً ملایم تر از قوانین سابق در قانون جرایم رایانه ای را باید متأثر از دیدگاه های موجود در خصوص تورم کیفری و زندان زدایی و مجازات های جایگزین حبس که در سال های اخیر مطمح نظر سردمداران دستگاه قضایی بوده است، دانست. همانگونه که بیان گردید لایحه ی جرایم رایانه ای توسط رئیس وقت دستگاه قضا تهیه گردید و ایشان که دارای اندیشه ی حبس زدایی و کاهش جمعیت کیفری زندان ها بوده اند، کوشیده اند مجازات های حبس را حتی المقدور با جزای نقدی جایگزین کنند. که البته

لایحه‌ی مزبور دست خوش تغییر و تحولات بنیادین گردیده، اما روح نخستین خود را تا حدود زیادی حفظ نموده است.<sup>۱۰۶</sup> از این رو، کاهش مجازات این بزه در قانون جرایم رایانه‌ای نسبت به قوانین سابق بدین لحاظ است.

یک تغییر مهم که با تصویب قانون جرایم رایانه‌ای از نظر شکلی و آیین دادرسی در مورد رسیدگی به جرایم مرتبط با سامانه‌های رایانه‌ای موضوع قانون تشدید مجازات کسانی که در امور سمعی بصری فعالیت غیر مجاز دارند ایجاد گردیده است، این است که مطابق ماده‌ی ۱۱ قانون مشارالیه «رسیدگی به جرائم مشروحه موضوع این قانون در صلاحیت دادگاههای انقلاب» بود. اما با تصویب قانون جرایم رایانه‌ای ماده‌ی ۳۰ آن قانون مقرر می‌دارد: «قوه قضاییه موظف است به تناسب ضرورت شعبه یا شعبی از دادرها، دادگاه‌های عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد.» لذا از این پس به لحاظ نسخ قانون امور سمعی بصری توسط قانون جرایم رایانه‌ای، رسیدگی به جرایم حوزه‌ی سمعی بصری و از جمله افشای اسرار خصوصی و خانوادگی و انتشار تصاویر شخصی و محرمانه‌ی افراد و به طور کلی تمامی جرایم مندرج در قانون تشدید مجازات فعالان امور سمعی بصری مرتبط با رایانه، در صلاحیت دادرها و دادگاه‌های ویژه‌ی جرایم سایبری قرار گرفت و توسط دادگاه عمومی رسیدگی خواهد شد که اقدامی حساب شده و مناسب است. چراکه جرایم حوزه‌ی سمعی بصری و از جمله افشای اسرار و فیلم خانوادگی و خصوصی افراد با خصوصیات و شرایط حاکم بر دادگاه انقلاب که بیشتر چهره‌ای امنیتی دارد منطبق نمی‌باشند.<sup>۱۰۷</sup>

## مبحث دوم: رکن مادی

<sup>۱۰۶</sup> عالی پور، حسن، منبع پیشین، صص ۳۶۸-۳۷۹.

<sup>۱۰۷</sup> شایان ذکر است آقای امیرحسین جلالی فراهانی در ترجمه‌ی کتابی با عنوان درآمدی بر آیین دادرسی کیفری جرایم سایبری مفصلاً به بررسی امور شکلی در جرایم سایبری پرداخته است. علاقه‌مندان می‌توانند برای مطالعه‌ی بیشتر به آن منبع مراجعه نمایند: جلالی فراهانی، امیرحسین، درآمدی بر آیین دادرسی کیفری جرایم سایبری، معاونت حقوقی و توسعه‌ی قضایی قوه‌ی قضائیه، مرکز مطالعات توسعه‌ی قضایی، خورسندی، تهران، ۱۳۸۸.

رکن مادی هر جرم را در حقیقت باید پیکره ی اصلی آن بزه دانست. چرا که بی شک صرف برخورداری از نیت مجرمانه را نمی توان مجازات نمود. تا زمانی که فرد با رفتار خود مقررات حاکم بر جامعه را نقض ننموده است، هرگونه واکنش کیفری در قبال او وجاهت قانونی ندارد. رکن مادی به عنوان مهم ترین رکن جرم دارای اجزا و عناصری است که بررسی آن ها موضوع نوشتار ما در مبحث حاضر است که طی سه گفتار به آن خواهیم پرداخت.

## گفتار اول: مرتکب و رفتار مجرمانه

اولین جزء رکن مادی هر جرم را می توان مرتکب بزه دانست. چراکه بدون وجود فردی انسانی - و البته می توان اشخاص حقوقی را نیز به آن افزود - نمی توان ارتکاب یک رفتار ممنوع و خلاف قانون را که مستوجب تعقیب کیفری و اعمال مجازات باشد تصور نمود. این بزه کار است که با رفتار خود - اعم از رفتار سلبی یا ایجابی و یا حتی غیر مادی - جرم را از قوه به فعل می رساند و به آن هستی و موجودیت می بخشد. لذا نخستین موضوع در بررسی رکن مادی شناسایی مرتکب یا همان مجرم است.

علاوه بر این، جرم چیری جز رفتار مغایر با قانون کیفری نیست. از این رو پس از شناخت بزه کار نوبت به شناسایی رفتار ناقض مقررات کیفری می رسد. در میان ارکان سه گانه ی هر جرم نیز به نظر ما، رکن مادی و در این رکن، مرتکب و رفتار او جرم را می سازد. سایر موارد مرتبط با جرم را باید در درجه ی دوم اهمیت قرار داد. لهذا، مطالب این گفتار طی دو بند ارائه خواهد شد.

## بند اول: مرتکب جرم

پس از آن که قلمرو رکن قانونی بزه مورد نظر خود را در چهارچوب ماده ی ۱۷ قانون جرایم رایانه ای باز یافتیم، برای تعیین مرتکب جرم نیز باید در همین قالب عمل نمود. اطلاق

ماده ی ۱۷ مذکور، حاکی از آن است که هر فردی می تواند مرتکب این جرم باشد. از این حیث قانون محدودیتی برای اعمال مقررات ماده ی ۱۷ قائل نگردیده است.<sup>۱۰۸</sup>

اهمیت این مطلب از آن رو است که ماده ی ۶۴۸ قانون مجازات اسلامی در مقام جرم انگاری افشای اسرار، تنها افشای اسرار حرفه ای را موضوع حکم قرار داده و تنها افرادی را به عنوان مرتکب شناسایی نموده که به مناسبت شغل و حرفه ی خویش محرم اسرار می گردند.<sup>۱۰۹</sup> این محدودیت در تعیین مرتکب سبب می شد تا چنانچه فردی بدون آنکه به واسطه ی شغل خود بر اسرار دیگران دست یابد و آن اسرار را افشا کند، به استناد ماده ی ۶۴۸ نتوان او را مجرم شناخت و مجازات نمود. اما اطلاق ماده ی ۱۷ قانون جرایم رایانه ای، این نقص قانونی را مرتفع ساخته و بدون ضروری دانستن این که فرد اولاً محرم اسرار دیگری باشد و ثانیاً این موقعیت به واسطه ی شغل وی پدید آمده باشد، و با عبارت «هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی . . .» بیان می دارد که ارتکاب این رفتار توسط هر شخصی و در هر موقعیتی جرم خواهد بود. البته با عنایت به قلمرو قانون جرایم رایانه ای – که تنها نظر بر سامانه های رایانه ای دارد – باید گفت این نقص قانونی همچنان در خارج از محیط مجازی پا برجاست.

مطلب دیگر در خصوص مرتکب جرم، موضوع امکان ارتکاب بزه توسط اشخاص حقوقی است. به نظر ما با توجه به اطلاق ماده ی ۱۷ ارتکاب بزه توسط شخص حقوقی نیز ممکن و کاملاً متصور است. مؤید این نظر، فصل ششم از بخش اول قانون جرایم رایانه ای است که طی چند ماده، مفصلاً مقرراتی در خصوص مسئولیت کیفری اشخاص حقوقی پیش بینی کرده است. مفاد دو ماده ی ۱۹ و ۲۰ این قانون به روشنی نحوه ی اعمال کیفر بر شخص حقوقی را تعیین نموده و این خود گواه بر عزم قانون گذار در مجازات اشخاص حقوقی است. ضمن اینکه در عرصه ی فضای سایبری، اشخاص حقوقی بیش از اشخاص حقیقی زمینه ی فعالیت داشته و کاربران و فعالان این عرصه نیز بیش از توجه به یک فرد خاص – به عنوان دایر کننده ی یک

<sup>۱۰۸</sup> عالی پور، حسن، منبع پیشین، ص ۳۱۸.

<sup>۱۰۹</sup> شقاقی، بیژن، اخلاق حرفه ای حفظ اسرار، منبع پیشین، صص ۲۶۰-۲۶۲.

پایگاه اطلاعاتی - تحت تأثیر عنوان حقوقی مرجعی که با آن به تبادل اطلاعات می پردازند، قرار داشته و به آن اعتماد می کنند.<sup>۱۱۰</sup>

به عنوان مثال ارائه دهندگان خدمات الکترونیکی، ISP ها، مراکز میزبانی و هاستینگ و به طور کلی تمام فعالان عرصه ی اینترنت و محیط مجازی تنها با نام و شهرت تجاری یا حقوقی خود نزد مردم شناخته شده اند. بیشتر افرادی که با این پایگاه های رایانه ای و اینترنتی همکاری و تبادل اطلاعات دارند شاید کوچک ترین آگاهی از هویت دایر کننده ی این وب سایت ها نداشته باشند. لذا پیش بینی مسئولیت کیفی برای شخص حقوقی جدای از شخص حقیقی دایر کننده یا دخیل در ارتکاب جرم می تواند موجب جلب اعتماد عمومی نسبت به فعالیت مراکز خدمات مجازی و الکترونیک گردد.

### بند دوم: رفتار مجرمانه

آنچه در ماده ی ۱۷ به عنوان رفتار مجرمانه تعیین گردیده است، عبارت است از منتشر کردن یا در دسترس دیگران قرار دادن صوت یا تصویر یا فیلم یا اسرار خصوصی یا خانوادگی متعلق به دیگری. اولین نکته در مورد این دو رفتار آن است که بدانیم انتشار به معنای پخش گسترده ی مطالب در فضای سایبر است، مانند آنکه در یک وب سایت که به ارسال خبرنامه به پست الکترونیک اشخاص می پردازد، تصاویر متعلق به دیگری به صورت یک فایل به گروه کثیری از کسانی که عضویت آن را پذیرفته اند ارسال گردد. و یا در صفحه ی نخست یک تارنمای فرهنگی-اجتماعی اطلاعاتی از یک مهمانی خانوادگی یک هنرپیشه ی مشهور درج شود. اما در دسترس قرار دادن اسرار برخلاف انتشار، این گونه محقق می شود که اطلاعات و محتویات مجرمانه در اختیار افراد شناخته شده ای قرار می گیرد. شاید وجه ممیزه ی این دو رفتار همین باشد که در نخستین مصداق، مرتکب کسانی را که اطلاعات در اختیارشان قرار می گیرد را نمی شناسد و البته این به علت دامنه و گستردگی عمل است. اما در مصداق دوم اساساً مرتکب کسانی را که به آنها اطلاعات می دهد را می شناسد.<sup>۱۱۱</sup>

<sup>۱۱۰</sup> برای مطالعه ی بیشتر در این خصوص ر. ک. آل محمد، فاطمه، منبع پیشین، صص ۹۶-۱۰۸.

<sup>۱۱۱</sup> عالی پور، حسن، منبع پیشین، ص ۳۱۸.



مطلب دیگر در خصوص نوع رفتار مجرمانه آن است که هر دو از مصادیق فعل مثبت مادی اند. از این رو به هیچ وجه نمی توان موردی را تصور نمود که انتشار یا در دسترس دیگران قرار دادن اسرار خصوصی به وسیله ی ترک فعل تحقق یابد. لذا چنانچه به علت سهل انگاری و عدم رعایت ترتیبات امنیتی در یک وب سایت صوت یا فیلم یا اسرار متعلق به دیگری در دسترس عموم قرار گیرد، در این مورد نه تنها از جهت رکن روانی بلکه از این حیث که فعلی مثبت به وقوع نپیوسته است، نمی توان رفتار تشکیل دهنده ی این جرم - در دسترس دیگران قرار دادن اسرار - را محقق دانست.

البته می توان فرضی را مطرح نمود که در آن به عنوان مثال مدیر یک وب سایت دوست یابی اطلاعات کاملاً خصوصی را که از یک کاربر خود گردآوری نموده است عمداً بدون رعایت تدابیر امنیتی متداول در وب سایت یا سرور خود ذخیره کند، و با علم به این که دیگران امکان دسترسی به این اطلاعات را دارند هیچ گونه اقدامی در خصوص ایجاد محدودیت دسترسی سایر کاربران به عمل نیاورد. در چنین حالتی نیز می توان نظر بر تحقق جرم داشت. این همان موقعیتی است که در حقوق جزای عمومی از آن به "جرم فعل ناشی از ترک فعل" یاد می گردد.<sup>۱۱۲</sup> در این حالت آنچه واقعاً اتفاق افتاده همان قرار دادن اسرار خصوصی دیگری در وب سایت بدون پیش بینی تدابیر امنیتی است که در واقع فعل است و نه ترک فعل و این مغایرتی با نظریه ی فوق ندارد.

این تعبیر مقنن که مرتکب باید اسرار را در دسترس دیگران قرار دهد، به این معنا نیست که مرتکب باید صوت یا تصویر را به بیش از یک نفر ارائه دهد بلکه دیگران در اینجا مفهوم نوعی دارد و میان صاحب اسرار و دیگری که شایستگی اطلاع از آن را ندارد تمایز ایجاد می کند.

انتشار و در دسترس دیگران قرار دادن، رفتارهای ساده و آنی هستند و لذا به عنوان مثال به محض اینکه یکی از موارد ممنوعه از طریق یک سایت اینترنتی در معرض دید کاربران قرار گیرد، عنوان "در دسترس قرار دادن" محقق است و چنانچه ظرف مدت کوتاهی محتوای

---

<sup>۱۱۲</sup> بررسی موضوعات حقوق جزای عمومی از حیطة ی بحث ما خارج است. برای مطالعه ی تفصیلی این موضوع می توانید به کتب حقوق جزای عمومی نظیر زمینه ی حقوق جزای عمومی نوشته ی دکتر نوربها، حقوق جزای عمومی نوشته ی دکتر اردبیلی و بایسته های حقوق جزای عمومی دکتر گلدوزیان مراجعه فرمایید.

مجرمانه از وب سایت مربوطه حذف گردد، تأثیری در رفع اثر از بزه ارتكابی نداشته و با جمع سایر شرایط، جرم تحقق یافته است. از این نکته می توان نتیجه گرفت که در تحقق این جرم، حتی لازم نیست که عملاً کسی به اطلاعات و اسرار موضوع جرم دست یابد، بلکه همین قدر که امکان دسترسی دیگران به این گونه مطالب فراهم باشد، برای مجرم شناختن مرتکب - البته با لحاظ سایر شرایط ضروری - کافی است.

نکته ی دیگر آن است که عناوین انتشار و در دسترس دیگری قرار دادن، اصولاً مؤخر بر تهیه ی فیلم یا اسرار خصوصی متعلق به دیگری ارتکاب می یابند. در اینجا سؤالی که مطرح می گردد آن است که آیا این رفتار یعنی تهیه و یا جمع آوری اسرار و یا فیلم یا صوت و تصویر خصوصی دیگری را نیز می توان مجازات کرد؟ در پاسخ باید گفت این گونه رفتارها در واقع به منزله ی مقدماتی برای ارتکاب رکن مادی بزه موضوع ماده ی ۱۷ هستند. از اینرو نمی توان آن را به استناد ماده ی ۱۷ مجازات نمود.<sup>۱۱۳</sup> تنها نقطه ی اتکا برای جرم دانستن این قبیل رفتارها، توسل به تأسیس حقوقی شروع به جرم است. اما همان گونه که می دانیم، این تأسیس در نظام حقوقی ما چهره ای کاملاً متزلزل به خود گرفته است. از این رو تنها در صورتی که در قوانین خاص برای تهیه یا گردآوری اسرار خصوصی و یا فیلم خانوادگی دیگران مجازاتی مقرر گردیده باشد، این رفتار جرم و قابل مجازات است. این موضوع را می توان در محدوده ی اعمال قانون تشدید مجازات کسانی که در امور سمعی بصری فعالیت غیر مجاز می کنند دانست. این مورد از جمله موارد عدم نسخ قانون مربوط است که سابقاً مورد اشاره قرار گرفت. بدین معنی که در خصوص تهیه و گردآوری اموری چون فیلم یا صوت یا اسرار خصوصی یا خانوادگی دیگران که بر اساس قانون جرایم رایانه ای قابل مجازات نیست، می توان به استناد قانون مصوب سال ۸۶ موضوع را تحت تعقیب و مجازات قرار داد.

## گفتار دوم: موضوع جرم و شرایط ضروری برای تحقق بزه

<sup>۱۱۳</sup> تبصره ی ۱ ماده ی ۴۱ قانون مجازات اسلامی مقرر می دارد: «مجرد قصد ارتکاب جرم و عملیات و اقداماتی که فقط مقدمه ی جرم بوده و ارتباط مستقیم با وقوع جرم نداشته باشد شروع به جرم نبوده و از این حیث قابل مجازات نیست.» جالب آنکه همان ماده شروع به جرم را نیز تنها در صورتی قابل مجازات می داند که عمل ارتكابی خود جرم باشد. این امر موجب ابهام در خصوص مسأله ی شروع به جرم در نظام کیفری ما گردیده است.

پس از شناخت مرتکب و رفتار مجرمانه، نوبت به شناسایی موضوع جرم می رسد. در این جا باید مشخص گردد که آنچه در جرم محوریت دارد چیست؟ بزهکار رفتار مجرمانه ی خود را متوجه چه امری می سازد؟ آماج جرم چیست؟ و به طور کلی آنچه در این جرم مورد تهاجم و تجاوز بزهکار قرار می گیرد چه چیزی است؟

همچنین باید ببینیم در کنار رفتار مجرمانه چه شرایطی برای ارتکاب جرم ضرورت دارد. چرا که مقنن در تمهید رکن قانونی هر بزه، به شرایط و اوضاع و احوالی که بزهکار و بزه دیده را احاطه کرده است، عنایت دارد و از این رو در بیان اجزای تحقق جرم، همواره شرایطی را نیز برای تحقق آن پیش بینی می نماید. در اینجا طی دو بند به بررسی این دو مطلب خواهیم پرداخت.

## بند اول: موضوع جرم

موضوع این جرم به تصریح ماده ی ۱۷ عبارت است از: «صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگران». در واقع ارزش پشتیبانی شده در اینجا حریم خصوصی شهروندان در حوزه ی مربوط به محتوای دیداری و شنیداری آنهاست. این قلمرو چنانکه پیشتر گفتیم تا حد زیادی منطبق بر قلمرو قانون سال ۸۶ است که در ماده ی ۵ آن قانون، مکرراً مورد اشاره قرار گرفته است. اما در مقایسه، ماده ی ۱۷ قانون جرایم رایانه ای موضوعات گسترده تری را مورد حمایت قرار داده است.

بنابر این موضوع جرم را می توان به سه دسته کلی تقسیم نمود: محتوای خصوصی، محتوای خانوادگی و محتوای سری که می توان آن را در تحت عنوان محتوای خصوصی قرار داد. محتوای خصوصی چهره ی فردی داشته و به یک فرد خاص تعلق دارد. چه بسا این محتوا دربر دارنده ی نشست های دوستانه ی یک فرد با هم کلاسان یا دوستانش باشد ولی به اعتبار حضور یک فرد چهره ی خصوصی می یابد. محتوای خانوادگی نیز به صوت یا تصویر یا فیلمی اطلاق می گردد که در یک خانواده تهیه شده باشد. مفهوم خانواده را می توان بر اساس قانون مدنی دربر گیرنده ی تمامی خویشاوندان تا طبقه ی سوم نسبی یا سببی توسعه داد. البته خانواده مفهومی عرفی نیز دارد که در زمان و مکان های مختلف متفاوت است. به عنوان مثال

شاید بتوان کودک بی سرپرستی را که توسط یک خانواده نگهداری می شود نیز جزو آن خانواده قلمداد نمود.<sup>۱۱۴</sup>

در مورد معنای اسرار بیشتر مطالبی ارائه گردید. در اینجا تنها به بیان این مطلب بسنده می کنیم که منظور از اسرار شخصی عبارت است از هر گونه اطلاعات یا حقایقی که هرکس آن ها را به تصمیم خویش از دیگران پوشیده دارد و از اطلاع دیگران بر آن ناخرسند گردد. هرچند برخی از آن اسرار را در اختیار نزدیکان و وابستگان خود قرار دهد.

سؤال دیگر که باید به آن پاسخ داد این است که این سه نوع محتوا باید در چه قالبی در دسترس دیگران قرار گیرد؟ ماده ی ۱۷ ضمن بر شمردن شکل های مختلف از قبیل فیلم، صوت یا تصویر در ادامه به طور کلی اشاره می دارد «و یا اسرار دیگری». این طرز بیان مقنن نشانگر این مطلب است که به هر طریق که اسرار دیگری در دسترس مرتکب یا دیگران قرار گیرد، محدودیتی از نظر تحقق رکن مادی بزه ایجاد نمی گردد. به عبارت دیگر، ممکن است فردی صوت یا تصویر خانوادگی دیگری را در وبلاگ شخصی خود قرار دهد. در این حالت تردیدی در تحقق جرم وجود ندارد. اما ممکن است مطالبی پیرامون یک محفل خانوادگی - بدون ارائه ی فیلم یا صوت و تصویر - در معرض دید کاربران اینترنت قرار گیرد. در اینجا نیز با استفاده از اطلاق ماده می توان بزه را با احراز سایر شرایط محقق دانست.

در واقع قانونگذار خود را مقید به شکل خاصی از افشای اسرار مانند فیلم یا امثال آن ننموده و هرگونه افشای اسرار خصوصی و خانوادگی را - به هر شکل که باشد - در فضای مجازی جرم دانسته است. نکته دیگر آن است که در مورد فیلم یا صوت یا تصویر، این قبیل امور مقید به قید "خانوادگی" گردیده اند اما «اسرار دیگری» که در ادامه ی ماده آمده است، به این قید مقید نگردیده و از این حیث نیز دامنه ی شمول ماده را گسترش داده است.

## بند دوم: شرایط ضروری در تحقق جرم

شرایط ضروری در تحقق هر بزه را از رکن قانونی آن می توان استنباط نمود. به این معنا که در طی پیشبینی رکن قانونی، برخی کیفیات و اوضاع و احوال و شرایط که مد نظر

<sup>۱۱۴</sup> عالی پور، حسن، منبع پیشین، صص ۳۱۸-۳۱۹.

قانون گذار است ذکر می شود و جزئی از رکن قانونی بزه می گردد.<sup>۱۱۵</sup> در این بند به بیان این کیفیات که از نظر مقنن برای ارتکاب جرم موضوع ماده ی ۱۷ ضروری به نظر می رسد می پردازیم.

نخستین مطلب در این مورد به « وسیله ی ارتکاب جرم» مربوط است. می دانیم که اصولاً در ارتکاب جرم، وسیله ی ارتکاب موضوعیت ندارد مگر آنکه صریحاً بیان گردیده باشد. در چنین حالتی، چنانچه رفتار مجرمانه تحقق یابد اما وسیله ی ارتکاب منطبق با آنچه مد نظر قانون گذار است نباشد، تحقق جرم با اشکال مواجه می گردد. به عنوان مثال، در جرم کلاهبرداری توسل به وسایل متقلبانه جزئی از رکن مادی جرم است که در رکن قانونی به آن اشاره شده است. پس اگر مرتکب بدون توسل به این قبیل وسایل، اقدام به بردن مال غیر کند، بزه کلاهبرداری محقق نمی گردد.

بزه ماده ی ۱۷ نیز از جمله جرایمی است که در ارتکاب آن وسیله، موضوعیت داشته و شرط تحقق جرم است. به تصریح ماده ی ۱۷، انتشار اسرار خصوصی و خانوادگی باید از طریق سیستم های رایانه ای و مخابراتی باشد. منظور از سیستم رایانه ای، هر وسیله ای است که بر اساس ساختارهای کامپیوتری و به اصطلاح دنیای صفر و یک و دیجیتال کار می کند و نه لزوماً یک دستگاه که نام رایانه داشته باشد. هر دستگاهی که قابلیت برنامه ریزی و کنترل خودکار عملیات و پردازش داده را داشته باشد، یک سیستم رایانه ای است. سیستم مخابراتی نیز عبارت است از وسیله یا ساختاری که بوسیله ی آن بتوان مجموعه ای از داده ها - عمدتاً صوتی و تصویری - را با یک شناسه ی مشخص از نقطه ای به نقطه ی دیگر ارسال نمود. بر این اساس، یک رایانه ی شخصی که به شبکه ی اینترنت متصل باشد نیز یک سیستم مخابراتی محسوب می گردد. از سوی دیگر تلفن همراه به عنوان یکی از مهم ترین ابزارهای مخابراتی، زمانی که به عنوان یک وسیله ی ذخیره ی داده به کار می رود، خود یک سیستم رایانه ای است. ملاحظه می گردد که سیستم های رایانه ای و مخابراتی تا چه حد با هم در ارتباط اند و هر سیستم مخابراتی به نوبه ی خود یک سیستم رایانه ای را پشتیبانی می کند. بنابر این تنها وسیله ی ارتکاب جرم موضوع ماده ی ۱۷ سیستم های رایانه ای و مخابراتی است. لذا ارتکاب این رفتار

<sup>۱۱۵</sup> میرمحمد صادقی، حسین، حقوق کیفری اختصاصی، جرایم علیه اموال و مالکیت، میزان، تهران، ۱۳۷۸، صص ۵۲-۵۷.

به طریقی غیر از دو مورد فوق مضمول مجازات ماده ی ۱۷ نبوده و تنها با جمع سایر شرایط می تواند به استناد ماده ی ۶۴۸ قانون مجازات اسلامی و یا دیگر قوانین مرتبط تعقیب گردد. یکی دیگر از شرایط ضروری در تحقق جرم فقدان رضایت شخصی است که تصویر یا صوت وی منتشر یا در دسترس دیگران قرار می گیرد. اصولاً در برخی از جرایم که جنبه ی خصوصی دارند و به اصطلاح از جرایم قابل گذشت به شمار می روند، رضایت فرد یکی از عوامل توجیه کننده ی جرم است که اساساً رکن قانونی و نتیجتاً رکن مادی را منتفی می کند. در اینجا نیز مقنن به این مسأله عنایت داشته که هرچند ممکن است مرتکب اطلاعات خصوصی را بدون مجوز به دست آورده باشد اما فرد صاحب صوت و تصویر می تواند با رضایت خود به وی اجازه دهد که آن محتوا را در دسترس دیگری قرار دهد. در این حالت، به واسطه ی وجود رضایت، جرمی به وقوع نپیوسته است.<sup>۱۱۶</sup> ضمناً تصریح به این مطلب در متن ماده بیانگر آن است که این امر یک شرط ایجابی در تحقق جرم است که وجود یا عدم آن نیازمند اثبات است و فقدان رضایت مفروض نیست.

آخرین شرط ضروری در تحقق این جرم، قید «جز در موارد قانونی . . .» می باشد. این قید که در ماده ی ۶۴۸ قانون مجازات اسلامی نیز به این شکل «در غیر از موارد قانونی . . .» دیده می شود بیانگر این مطلب است که رفتارهای مجرمانه در این بزه - انتشار و در دسترس دیگری قرار دادن - باید غیر قانونی باشد. لذا اگر این رفتارها قانونی باشند، بزه رخ نمی دهد حتی اگر دارنده ی محتوای سری و خصوصی رضایت به این کار نداشته باشد. پیشبینی این شرط بدین لحاظ است که از منظر قانون گذار، در برخی موارد نهادها یا اشخاص ویژه ای شایستگی دسترسی به محتوای شخصی و خصوصی را دارند.<sup>۱۱۷</sup> گاهی ممکن است موضوعی از جمله ی اسرار خصوصی باشد اما به لحاظ اهمیتی که از بعد اجتماعی دارد، عدم افشای آن موجب ورود لطماتی بر پیکره ی اجتماع گردد. در این موارد افشای اسرار مجاز و گاه حتی تکلیف قانونی اشخاصی است که بر آن اطلاع می یابند. فرض کنیم شخصی از ارتکاب جرمی

<sup>۱۱۶</sup> عالی پور، حسن، منبع پیشین، صص ۳۱۸-۳۱۹.

<sup>۱۱۷</sup> همان.

آگاه گردد. در این حالت عدم اعلام جرم ممکن است موجب تضییع حقوق دیگران گردد. نمونه ی این تکلیف قانونی ماده ی ۶۰۶ قانون مجازات اسلامی است.

در ماده ی ۱۷ همانند ماده ی ۶۴۸ قانون مجازات اسلامی صریحاً مشخص نگردیده است که منظور از موارد قانونی چیست؟ برخی معتقدند منظور از آن تمامی اموری است که در آن شخص اجازه ی ارتکاب جرم را دارد، همانند اضطرار یا اجبار و مانند آن. اما این قبیل امور که از علل موجهه ی جرم هستند، اختصاصی به این جرم ندارد و در کلیه ی جرایم متصور است. توضیح آن که در صورت وجود عواملی از این قبیل اراده ی آزاد مرتکب تحت الشعاع آن امور قرار گرفته و نتیجتاً رکن روانی محقق نمی گردد و تردیدی نیست که فقدان یکی از ارکان متشکله جرم موجب عدم امکان تعقیب می باشد و یک علت نوعی برای توجیه ارتکاب بزه است که در کلیه ی جرایم متصور خواهد بود. لذا منظور از موارد قانونی، مواردی است که در قوانین مختلف افشای اسرار دیگران جرم دانسته نشده بلکه حتی یک تکلیف قانونی نسبت به افشای آن متوجه کسانی است که از این اسرار مطلع می گردند.

بنابر این برای تعیین موارد قانونی باید به بررسی قوانین مختلف پرداخت. از جمله ی مواردی که افشای سر جرم دانسته نشده است می توان به موارد زیر اشاره نمود: مواد ۱۳، ۱۴ و ۱۹ قانون جلوگیری از بیماری های آمیزشی، بند ۴ ماده ی ۲۶ قانون ثبت احوال در خصوص الزام به اعلام فوت اشخاص، ماده ی ۱۹ همان قانون در خصوص اعلام ولادت به ثبت احوال، ماده ی ۷۱۱ قانون مجازات اسلامی در مورد اعلام جرم توسط ضابطین دادگستری و ماده ی ۲۲۳ قانون مالیات های مستقیم در خصوص تکلیف مأموران مالیاتی در قبال اسرار و اطلاعات مربوط به مؤدیان و همچنین ماده ی ۶۰۶ قانون مجازات اسلامی در خصوص تکلیف مدیران به اعلام جرم علیه مرتکبین اختلاس یا سوء استفاده از اموال دولتی.

نکته ای که از مطالعه ی مواد فوق الذکر به دست می آید آن است که در مواردی که فرد مجاز به افشای اسرار است، باید آن را به مقامات ذی صلاح گزارش کند و گرنه چنانچه به کسانی بجز افراد یاد شده گزارش کند یا اسرار را در اختیار افراد غیر صالح قرار دهد، مرتکب افشای سر در غیر موارد قانونی گردیده و قابل مجازات خواهد بود. ضمناً افشای اسرار در موارد قانونی نیز باید در حد ضرورت باشد و لذا چنانچه بیش از حد لازم، اسرار مردم در اختیار دیگران - ولو اینکه مقام صلاحیت دار باشند - قرار گیرد، باز هم جرم موضوع این ماده تحقق

می یابد. چراکه در این حالت نیز تجاوز از حد لزوم به منزله ی این است که افشا در موارد قانونی نبوده است.<sup>۱۱۸</sup>

## گفتار سوم: نتیجه ی حاصل از جرم

یکی دیگر از عناوین که در بحث از رکن مادی جرایم مورد بررسی قرار می گیرد، آثار و نتایجی است که از انجام رفتار مجرمانه ایجاد می گردد. به عنوان مثال در بزه سرقت محروم شدن مالک از مال خویش را به عنوان نتیجه ی مجرمانه می شناسیم. یا در کلاه برداری بردن مال متعلق به دیگری نتیجه ی حاصل از جرم است. در این گفتار به بررسی نتیجه ی حاصل از بزه موضوع ماده ی ۱۷ قانون جرایم رایانه ای می پردازیم اما پیش از آن باید ببینیم آیا این جرم اساساً مقید به تحقق نتیجه ی خاصی گردیده است یا خیر؟ لذا مطالب این گفتار طی دو بند آورده می شود.

### بند اول: مطلق یا مقید بودن بزه موضوع ماده ی ۱۷

در تقسیم بندی جرایم از حیث وجود یا فقدان نتیجه ی حاصل از ارتکاب رکن مادی، به طور کلی دو دسته جرم را می توان برشمرد. جرایم مطلق و جرایم مقید. منظور از جرم مطلق، جرمی است که تحقق رکن مادی آن به صرف ارتکاب رفتار مجرمانه کامل می گردد. به عبارت دیگر، همین که بزهکار رفتارهای ممنوعه را انجام دهد، جرم ارتکاب یافته تلقی می گردد و برای تعقیب و مجازات مجرم، نیازی به وجود عنصر مستقلی به نام نتیجه ی مجرمانه نیست. از جمله جرایم مطلق می توان به توهین ساده اشاره نمود که به محض ادای الفاظ و جملات موهن، ارتکاب می یابد.

---

<sup>۱۱۸</sup> قماش، سعید، بررسی جرم افشای اسرار حرفه ای، منبع پیشین، صص ۴-۶.



اما دسته ای دیگر از جرایم هستند که تنها زمانی رکن مادی آن ها تکمیل می گردد که منتهی به نتیجه ی خاصی گردد. در غیر این صورت اعمال ارتكابی را تنها در حد شروع به جرم می توان تحت پیگرد قرار داد. یکی از بارزترین جرایم مقید به نتیجه، قتل است. چرا که بدون وقوع نتیجه - مرگ قربانی - اساساً قتلی اتفاق نیفتاده تا بتوان فردی را به عنوان قاتل محاکمه و مجازات نمود.<sup>۱۱۹</sup> بیشتر جرایم موضوعه در قوانین کیفری مقید به حصول نتیجه ی مجرمانه گردیده اند.

برای تعیین این موضوع که آیا یک جرم مطلق است یا مقید باید به رکن قانونی آن دقت نمود. معمولاً مقنن در خلال مواد کیفری اجزای مختلف تشکیل دهنده ی یک جرم را به تفصیل بیان می کند. یکی از این اجزا می تواند نتیجه ی حاصل از ارتكاب رفتار مجرمانه باشد. با نگاهی به متن ماده ی ۱۷ ملاحظه می شود که این جرم از نظر قانون گذار یک جرم مقید است. چرا که در بخش پایانی ماده چنین می خوانیم: « . . به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود . . . » از این عبارت به وضوح برمی آید که صرف ارتكاب رفتار مجرمانه به تنهایی برای تکمیل رکن مادی جرم کافی نیست بلکه این رفتار مجرم باید موجب ورود ضرر به بزه دیده گردد یا باعث هتک حیثیت و آبروی او گردد.

ممکن است گفته شود ارتكاب رفتارهای موضوع این ماده، فی نفسه دربردارنده ی چنین آثار و نتایجی می باشد. منظور قانون گذار از بیان این مطلب تأکید بر این نکته است که نتیجه ی غالبی یک رفتار نا بهنجار برای جرم انگاری آن عمل کافی است گرچه که عملاً منتهی به آن نتیجه نگردد. لازمه ی ملتزم شدن به این دیدگاه آن است که نظر بر مطلق بودن بزه مورد بحث داشته باشیم. اما این نظر با ظاهر قانون انطباق ندارد. ضمن آنکه اصل تفسیر شک به نفع متهم نیز اقتضای آن را دارد تا در جایی که تردید نسبت به وجود یا عدم شرط اضافی در تحقق جرم ایجاد می گردد، وجود آن را ضروری بدانیم.

از اینرو باید گفت این بزه یک جرم مقید است و اگرچه نتیجه ی حاصله، اصولاً نتیجه ی غالبی چنین رفتاری است اما به هر حال وجود آن ضروری است. نهایت امر آنکه وجود آن را در حالت عادی مفروض بینگاریم اما در عین حال این امکان را برای متهم فراهم سازیم تا

<sup>۱۱۹</sup> نوربها، رضا، زمینه ی حقوق جزای عمومی، دادآفرین، تهران، ۱۳۷۸، صص ۲۴۴-۲۵۵.

بتواند خلاف آن را اثبات نموده و خود را از اتهام وارده تبرئه نماید. حال آنکه با مطلق دانستن این جرم، دیگر چنین امکانی برای متهم وجود نخواهد داشت. چراکه اساساً جایگاهی برای بررسی نتیجه ی مجرمانه و تحقق یا عدم تحقق آن وجود نخواهد داشت.

در این ماده برای تحقق بزه دو نتیجه ی مجرمانه پیش بینی شده است. اما نکته ی جالب توجه آن است که تحقق هر یک از این دو برای تکمیل رکن مادی کافی است و ضرورتی بر جمع نتایج مجرمانه نیست. چنانچه دادرسی یکی از این دو را احراز کند، نیازی به دست یافتن به دیگری وجود ندارد. زیرا این امر اثری بر بزه نه از جهت تعدد جرم دارد و نه از حیث افزایش یا کاهش کیفر.<sup>۱۲۰</sup> این دو نتیجه ی مجرمانه عبارت اند از: اول رکن ضرری که تعیین میزان و نوع آن با کارشناس و تصمیم دادرسی است. دیگری هتک حیثیت که تعیین آن بر مبنای عرف و تصمیم قاضی است.

ضرر در اینجا به صورت کلی و عام آمده است و لذا هم شامل ضرر و زیان مادی و هم ضرر و زیان معنوی می گردد که متعاقب انتشار یا در دسترس دیگران گذاشتن محتوای خصوصی یا خانوادگی نمود می یابد. در نظام حقوقی ما در خصوص جبران ضرر معنوی همواره بحث و اختلاف نظر وجود داشته. قانون مسئولیت مدنی به صورت عام و کلی جبران کلیه ی زیان ها را پیش بینی نموده اما در حال حاضر نسبت به امکان یا عدم امکان استناد به آن بر اساس نظر شورای نگهبان تردید وجود دارد.<sup>۱۲۱</sup> اما در خصوص بزه مورد بحث ما، بی شک عقل سلیم حکم می کند که بیشتر زیان ناشی از انتشار اسرار خصوصی و خانوادگی جنبه ی معنوی دارد همانگونه که مقنن نیز بلافاصله به هتک حیثیت اشاره نموده است. لذا نباید خود را محدود به ضرر مادی نموده و بدین وسیله از کارایی قانون موضوعه بکاهیم.

و اما نتیجه ی دیگر، هتک حیثیت است. هتک در لغت به معنای دریدن، سوراخ کردن، گشودن و باز کردن است<sup>۱۲۲</sup> و حیثیت نیز به معنای کرامت و شرافت انسانی و آبرو و عرض هر فرد است. ترکیب این دو با هم به معنای از بین رفتن شرف و منزلت انسانی و کرامت

<sup>۱۲۰</sup> عالی پور، حسن، منبع پیشین، ص ۳۱۹.

<sup>۱۲۱</sup> برای بحث تفصیلی پیرامون مسأله ی جبران خسارت معنوی می توان به کتاب ضمان قهری نوشته ی دکتر ناصر کاتوزیان مراجعه نمود.

<sup>۱۲۲</sup> لغت نامه ی دهخدا

یک شخص و خدشه بر عرض و آبروی اوست. هتک حیثیت به معنای مرگ مدنی است و فردی که آبروی خود را از دست رفته می یابد، تمام هستی اش را بر باد رفته می داند و چه بسا دیگر امکان ادامه ی یک زندگی شرافت مندانه را در جامعه نیابد.

نکته ی مهم در خصوص احراز این نتیجه ی مجرمانه آن است که توسل به عرف محوریت دارد. می دانیم که در مقررات کیفری عرف هم منبعی راهنما و ارشادی است و هم منبعی الزامی. الزامی بودن عرف بسته به پیش بینی قانون گذار است. در این حالت اعتبار رأی قاضی وابسته به این است که به عرف استناد کند. از سوی دیگر می دانیم که در قوانین کیفری اصولاً عرف برای تشخیص موضوعات مورد استناد قرار می گیرد و نه صدور حکم و تعیین مجازات. در اینجا عرف به عنوان معیاری برای تعیین نتیجه ی مجرمانه شناخته شده و دادرس برای احراز تحقق آن ناگزیر از ارجاع و استناد به عرف است.<sup>۱۲۳</sup> منظور از عرف نیز عرف عام است که در رفتار و منش عامه ی مردم جریان می یابد.

## بند دوم: شروع به جرم

جای طبیعی بحث از شروع به جرم، در پایان بحث از رکن مادی جرم است. چراکه شروع به جرم در واقع یک جرم ناتمام است. بدین معنی که مرتکب قصد ارتکاب جرمی را کرده و در جهت تحقق آن تلاش نموده اما عنصر مادی ناتمام مانده و او موفق به اتمام جرم نشده است. در برخی از موارد همین تلاش در جهت ارتکاب جرم از نظر قانون قابل مجازات می باشد. در این حالت گرچه مرتکب به هدف نهایی خود نرسیده اما با انجام بخشی از عنصر مادی جرم در حقیقت حالت خطرناک خود را برای اجتماع نمایان ساخته و به همین لحاظ جامعه برای دفاع از خود اقدام به مجازات نمودن وی می کند.<sup>۱۲۴</sup>

نهاد کیفری شروع به جرم که در قانون مجازات عمومی ریشه دارد و بعد از انقلاب نیز در قانون راجع به مجازات اسلامی طی چند ماده مورد اشاره واقع شده بود، در قانون مجازات اسلامی سال ۱۳۷۰ کاملاً دستخوش ابهام و اجمال گردیده است. قانون فوق الذکر تنها در

<sup>۱۲۳</sup> عالی پور، حسن، منبع پیشین، صص ۳۸۲-۳۸۳.

<sup>۱۲۴</sup> میرمحمد صادقی، حسین، منبع پیشین، صص ۸۹-۹۴.

ماده‌ی ۴۱ مقرر داشته: «هرکس قصد ارتکاب جرمی کند و شروع به اجرای آن نماید لکن جرم منظور واقع نشود چنانچه اقدامات انجام گرفته جرم باشد محکوم به مجازات همان جرم خواهد شد» در این نوشتار بررسی وضعیت حقوقی شروع به جرم مورد نظر ما نیست. تنها به بیان این نکته اکتفا می‌کنیم که در وضعیت کنونی تنها در صورتی می‌توان شروع به یک جرم خاص را مجازات نمود که صریحاً در قانون برای شروع به آن جرم مجازات مقرر گردیده باشد.

اما در خصوص جرم مورد بحث ما اولاً باید دید این جرم اساساً قابلیت شروع به جرم را دارد یا نه؟ با توجه به تقسیم بندی جرایم به مطلق و مقید - که قبلاً بدان اشاره شد - اصولاً باید گفت جرایم مطلق قابلیت شروع به جرم را ندارند. چراکه بنا به یک تعریف برای تحقق شروع به جرم باید فرد وارد عملیات اجرایی رکن مادی گردد و تنها آخرین جزء رکن مادی را مرتکب نگردیده باشد. اما در جرایم مطلق به محض ارتکاب رفتار ممنوع، بزه تحقق می‌یابد و رکن مادی این قبیل جرایم معمولاً دارای اجزای متعدد نیست. اما در جرایم مقید به نتیجه تصور وجود شروع به جرم امکان پذیر است. از این رو در خصوص جرم موضوع بحث ما از بعد نظری می‌توان شروع به جرم را تصور نمود. به عنوان مثال فردی که فیلم خانوادگی متعلق به دیگری را تهیه کرده و در یک لوح فشرده ذخیره نموده است، اکنون در حال آپ لود (Upload) کردن اطلاعات بر روی وبلاگ شخصی خویش است اما به دلایلی در حین انجام این عمل از اتمام آن باز می‌ماند اما به لحاظ همین رفتار توسط شخص صاحب فیلم، علیه وی شکایتی در محکمه طرح گردیده است. آیا این فرد را می‌توان مجازات نمود؟

همان گونه که بیان شد برای آنکه فردی را به عنوان شروع به جرم مجازات نماییم، باید مستند قانونی خاص داشته باشیم که یا صراحتاً "شروع به جرم" یک بزه را قابل مجازات بداند - مانند تبصره ی ۲ ماده ی ۱ قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاه برداری - و یا آن که بدون تصریح به عنوان شروع به جرم، از جرمی سخن به میان آمده باشد که ماهیتاً شروع به جرم است - مثل جرم مذکور در ماده ی ۵۶۱ قانون مجازات اسلامی<sup>۱۲۵</sup> و

---

<sup>۱۲۵</sup> ماده ی ۵۶۱ قانون مجازات اسلامی: «هرگونه اقدام به خارج کردن اموال تاریخی-فرهنگی از کشور هرچند به خارج کردن آن نیانجامد قاچاق محسوب و مرتکب علاوه بر استرداد اموال به حبس از یک تا سه سال و پرداخت جریمه معادل دو برابر قیمت اموال موضوع قاچاق محکوم می‌گردد.»

یا ماده ی ۳۵ مکرر قانون گذرنامه<sup>۱۲۶</sup> - یعنی میزان عمل و رفتاری را که در واقع معادل شروع به جرم خاصی است را جرم انگاری نموده و قابل مجازات بداند.<sup>۱۲۷</sup>

در خصوص بزه موضوع ماده ی ۱۷ با نگاهی به قانون جرایم رایانه ای، هیچ مقرره ی قانونی را نمی توان یافت که به جرم انگاری شروع به جرم ماده ی ۱۷ اختصاص یافته باشد. لذا تنها فرضی که برای قابل مجازات دانستن این رفتار باقی می ماند، آن است که در قوانین مختلف رفتارهایی که ماهیتاً شروع به جرم هستند جرم انگاری شده باشند. از جمله قانون تشدید مجازات کسانی که در امور سمعی بصری فعالیت غیر مجاز دارند در برخی مواد به تهیه ی فیلم و عکس از محل های اختصاصی بانوان یا محافل خانوادگی اشاره داشته و برای آن گونه رفتار مجازات مقرر داشته است. به لحاظ اینکه این رفتارها در حکم شروع به جرم افشای اسرار در محیط مجازی هستند می توان آنها را قابل مجازات دانست اما به هر حال این عناوین مجرمانه مستقلاً جرم انگاری شده اند و تحت عنوان یک جرم مستقل قابل تعقیب و مجازات می باشند.<sup>۱۲۸</sup>

## مبحث سوم: رکن روانی

حقوق جزای غربی تا پایان قرن دوازدهم به انسان تنها به عنوان یک ابزار در ایجاد صدمه می نگریست و در مجازات کردن او، توجهی به سوء نیت و عنصر روانیش نداشت. اما از اواخر قرن دوازدهم تغییر مهمی روی داد و آن عبارت بود از توجه به انسان به عنوان یک عامل اخلاقی و چنین موجودی تنها در صورتی قابل مجازات بود که ارتکاب جرم را برگزیده باشد. امروزه مجرد ارتکاب عمل مجرمانه باعث ایجاد مسئولیت کیفری نبوده بلکه وجود عنصر روانی

---

<sup>۱۲۶</sup> ماده ی ۳۵ مکرر قانون گذرنامه: «هر ایرانی که بدون داشتن گذرنامه یا اسناد در حکم گذرنامه بخواهد از مرز غیر مجاز خارج شود و به هنگام عبور دستگیر گردد، به یک ماه تا یک سال حبس یا پنجاه هزار ریال تا سی صد هزار ریال جزای نقدی محکوم خواهد شد . . .»

<sup>۱۲۷</sup> پیشین، ص ۹۱.

<sup>۱۲۸</sup> عالی پور، حسن، منبع پیشین، ص ۳۱۸.

نیز ضروری است.<sup>۱۲۹</sup> در این مبحث بر تحلیل رکن روانی بزه افشای سر در محیط مجازی متمرکز خواهیم بود و مطالب خود را در دو گفتار بیان خواهیم نمود.

## گفتار اول: علم مرتکب

همان گونه که در مورد رکن مادی جرم نیز بیان گردید، در تحقق هر یک از ارکان یک بزه شرایط و کیفیاتی مدخلیت دارند. رکن روانی نیز به عنوان جنبه ای از جرم که ورای رفتار مادی و فیزیکی - و البته گاه غیر مادی - بخشی از پیکره ی جرم را تشکیل می دهد، برای محقق گردیدن، مستلزم وجود شرایطی است. مهم ترین این شرایط علم مرتکب است. به طور سنتی جزء نخست رکن روانی جرایم - علم مرتکب - در دو بخش تقسیم بندی می گردد. نخستین بخش، شامل علم و آگاهی مجرم نسبت به حکم و دیگری علم نسبت به موضوع بزه می باشد. این دو بخش طی دو بند جداگانه بررسی می گردد.

---

<sup>۱۲۹</sup> میرمحمد صادقی، حسین، حقوق کیفری اختصاصی، جرایم علیه اموال و مالکیت، منبع پیشین، صص ۹۵-۹۶.

## بند اول: علم حکمی

یکی از اصول و قواعد عقلی حاکم بر امور جزایی قاعده ی "قبح عقاب بلا بیان" می باشد. این قاعده که ریشه در قرآن نیز دارد،<sup>۱۳۰</sup> بیانگر آن است که اعمال عقوبت و کیفر نسبت به امری که سابقاً اتباع حقوق کیفری از آن ممنوعیت مطلع نگردیده اند، قبیح و خلاف عقل سلیم است. لازمه ی التزام به این قاعده آن است که برای تعقیب و مجازات نمودن هر فرد، باید وی نسبت به قاعده ی محدود کننده ی آزادی خویش - یعنی همان ضوابط جزایی - علم و آگاهی داشته باشد. همچنین بنا بر این قاعده که هر امری از شرایط ضروری برای تحقق جرم باشد، نیازمند احراز می باشد، باید قائل به این نظر گردید که احراز وجود علم و اطلاع مرتکب بر وجود مقرره ی محدود کننده ی آزادی، به منظور مجرم شناختن او ضرورت دارد.

با این حال عقل سلیم حکم می کند که ضروری دانستن چنین شرطی، عملاً تا چه میزان مشکل آفرین خواهد بود. این وضعیت زمینه ی فرار متجاوزین به هنجارهای اجتماعی را فراهم آورده و فرایند پیچیده ی دادرسی را با دشواری های بیشتری روبرو می سازد. از این رو است که قانون گذاران همواره به یک اصل کلی متوسل می شوند و وجود علم افراد بر حکم قانون را مفروض می انگارند. این مفروض دانستن علم حکمی، اختصاصی به امور جزایی نداشته و همان گونه که در قانون مدنی نیز مقرر گردیده که قوانین ۱۵ روز پس انتشار در روزنامه ی رسمی لازم الاجرا خواهد بود.<sup>۱۳۱</sup> منظور آن است که پس از گذشت این مدت، علم مردم بر وجود مقرره ی قانونی مفروض خواهد بود و نیازی به احراز آن در محکمه نیست. بدون تأسیس چنین اصلی، جریان عادی امور با وقفه و اشکال رو برو خواهد شد و افراد از وصول به حقوق خویش باز خواهند ماند.

تنها در برخی موارد نادر، در مقررات کیفری - آن هم بنا بر مصالح خاصی - دیده می شود که وجود علم بر حکم برای امکان مجرم دانستن یک فرد، ضروری دانسته شده است.<sup>۱۳۲</sup>

<sup>۱۳۰</sup> وما کنا معذبین حتی نبعث رسولا (سوره اسراء، آیه ی ۱۵)

<sup>۱۳۱</sup> ماده ی ۲ «قوانین ۱۵ روز پس انتشار در سراسر کشور لازم الاجرا است مگر آنکه در خود قانون ترتیب خاصی برای موقع اجرا مقرر شده باشد. برای مطالعه ی تفصیلی در این خصوص می توان به کتاب مقدمه ی علم حقوق نوشته ی دکتر ناصر کاتوزیان مراجعه نمود.

<sup>۱۳۲</sup> از آن جمله می توان به مواد ۶۴، ۶۵ و ۱۶۶ قانون مجازات اسلامی در باب زنا و حد مسکر اشاره نمود.

دلیل وجود چنین موارد استثنایی بی شک تأکید شارع مقدس بر ممانعت از اثبات موجبات اجرای حد شرعی بوده است اما در سایر موارد، اساساً علم بر حکم مفروض است. بنابراین مطالب یاد شده در خصوص بزه موضوع ماده ی ۱۷ قانون جرایم رایانه ای نیز که بنابر تقسیم بندی قانون مجازات اسلامی در باب "تعزیرات و مجازات های بازدارنده" قرار می گیرد،<sup>۱۳۳</sup> علم مرتکب بر وجود مقررہ ی جزایی که این رفتارها را منع نموده و قابل مجازات می شمارد مفروض است. از این رو نیازی به احراز آن در دادگاه نخواهد بود.

## بند دوم: علم موضوعی

دیگر شرط ضروری یا جزء تشکیل دهنده ی رکن روانی عبارت است از علم مرتکب به موضوع جرم. منظور آن است که فرد بداند رفتاری که از وی صادر می گردد همان رفتار ممنوعه ی پیش بینی شده در مقررہ ی کیفری است. همچنین مرتکب باید نسبت به موضوع بزه نیز عالم باشد. به عنوان مثال در بزه سرقت، مرتکب اولاً باید بداند که رفتار ارتكابی وی، مصداق ربودن است، ثانیاً باید بداند آنچه می رباید مالیت دارد و ثالثاً باید بداند که مال مورد ربایش، متعلق به دیگری است و لذا در هر یک از موارد فوق که علم مفقود بوده و یا مرتکب دچار اشتباه گردد رکن روانی جرم متزلزل خواهد شد.<sup>۱۳۴</sup> در همین جاست که مسأله ی اشتباه موضوعی مطرح می گردد. اشتباه موضوعی در برخی جرایم که دارای اشکال عمد و غیر عمد هستند - نظیر قتل - می تواند موجب استحاله ی بزه از عمد به غیر عمد گردد اما در جرایمی که تنها به شکل عمدی قابلیت ارتکاب دارند اصولاً موجب انتفای عنوان مجرمانه می گردد.<sup>۱۳۵</sup> در خصوص بزه مورد بحث ما نیز، وجود علم موضوعی ضروری است. به این مفهوم که مرتکب اولاً باید بداند رفتار وی مصداق انتشار و در دسترس دیگران قرار دادن است، از این رو چنانچه فردی اطلاعات متعلق به دیگری را در یک سیستم رایانه ای ذخیره کند به این تصور که سایرین به این اطلاعات دسترسی نخواهند یافت، اما وی در این مورد دچار اشتباه گردیده و

---

<sup>۱۳۳</sup> توضیح آنکه بر اساس ماده ی ۵۶ قانون جرایم رایانه ای، این قانون به انتهای قانون مجازات اسلامی الحاق گردید و لذا در ذیل باب پنجم آن قانون یعنی مجازات های تعزیری و بازدارنده گنجانده شد.

<sup>۱۳۴</sup> میرمحمد صادقی، حسین، حقوق کیفری اختصاصی، جرایم علیه اموال و مالکیت، منبع پیشین، صص ۲۳۴-۲۳۷.

<sup>۱۳۵</sup> نوربها، رضا، منبع پیشین، صص ۳۵۸-۳۶۳.



آن سیستم رایانه ای به عنوان سرور یک وب سایت مورد استفاده قرار می گرفته و بدین لحاظ محتوای خصوصی مورد اشاره از این طریق افشا گردد، این فرد را به لحاظ نقص در علم موضوعی یا به عبارت دیگر به واسطه ی اشتباه موضوعی نمی توان مجرم شناخت. همین طور چنانچه کارمند اداره ی مالیاتی که مکلف به وارد نمودن اطلاعات مربوط به درآمد مؤدیان خویش در پایگاه اینترنتی سازمان متبوع است، به تصور آنکه زیرساخت های امنیتی سیستم به درستی کار می کند اقدام به ورود اطلاعات خصوصی افراد در صفحه ی مرورگر رایانه ی خود نماید، اما به لحاظ ضعف در سیستم های حفاظتی، اطلاعات در دسترس نفوذگران قرار گیرد، باز هم به علت عدم وجود قصد مجرمانه از یک سو و عدم علم بر این که رفتار وی مصداق انتشار اسرار است از سوی دیگر، وی را نمی توان مجازات کرد.

ثانیاً مرتکب باید بداند آنچه را در دسترس دیگران قرار می دهد صوت یا تصویر یا فیلم خانوادگی دیگری است یا از اسرار خصوصی وی به شمار می رود. لذا چنانچه اطلاعاتی را به تصور آنکه فیلم خانوادگی خویش است و به اشتباه در وبلاگ شخصی خود قرار دهد و بازدید کنندگان آن وبلاگ بدان دست یابند اما متعاقباً معلوم گردد که محتوای موجود در پایگاه اینترنتی متعلق به یکی از دوستان نامبرده بوده و بدین لحاظ موجب خدشه بر حیثیت وی گردیده است، باز هم به لحاظ نقص در رکن روانی نمی توان چنین فردی را مجازات نمود. همچنین است اگر فرد به تصور آنکه اطلاعات اهمیتی ندارد و تنها به عنوان یک وسیله ی سرگرمی کاربران خود آن مطالب را در وب سایت قرار داده اما معلوم شود که آن اطلاعات، مصداق اسرار خصوصی بزه دیده بوده است، در این حالت نیز فرد قابلیت مجازات را ندارد چرا که نسبت به موضوع جرم عالم نبوده است.

آنچه در این دو بند اشاره کردیم تا حدی به موضوع "فرض قانونی"<sup>۱۳۶</sup> مرتبط می گردد. بنا بر یک نظر اثبات خلاف فرض قانونی امکان پذیر نیست. بدین رو نه تنها علم مرتکب مفروض است بلکه حتی وی نمی تواند به هیچ طریق عدم علم خود را اثبات کند. اما در خصوص علم موضوعی مسأله متفاوت است. به این معنا که بدواً ممکن است وجود علم بر موضوع نیز مفروض انگاشته شود، اما این فرض، یک فرض قانونی نیست بلکه به واسطه ی

---

<sup>۱۳۶</sup> Fiction in law

وجود امارات قضایی، دادرس آن را مفروض می‌داند. اما وجه ممیزه ی آن با علم حکمی آن است که متهم امکان اثبات خلاف فرض دادرس را دارد و از این حیث ممنوعیتی وجود ندارد.<sup>۱۳۷</sup>

## گفتار دوم: قصد مجرمانه

جزء دیگر تشکیل دهنده ی رکن روانی عبارت است از قصد مجرمانه. منظور از این نکته آن است که مرتکب باید عمداً با اراده ی مقنن مخالفت کند. به عبارت دیگر ضمن علم بر ممنوعیت رفتار و نیز علم بر این که رفتار وی مصداق عمل ممنوع و جرم است با اراده ی آزاد و به دور از هرگونه عامل قهر آمیز بخواهد با نقض ضابطه ی جزایی، عمل مجرمانه را مرتکب گردد. این جاست که بحث از عوامل مؤثر بر اراده ی آزاد انسان و محل رکن روانی - نظیر اکراه، اجبار و اضطرار - سخن به میان می‌آید.<sup>۱۳۸</sup>

این اراده ی آزاد مجرم که بر اساس آن اقدام به نقض ممنوعیت کیفری کرده و مرتکب جرم می‌گردد را "قصد مجرمانه"<sup>۱۳۹</sup> می‌نامیم. اساساً قصد مجرمانه در بردارنده ی خواست مرتکب بر اجزای رکن مادی جرم است. اگر بخواهیم مهم ترین اجزاء رکن مادی هر جرم را بر شماریم، باید از دو جزء "رفتار ممنوع" و "نتیجه ی مجرمانه" یاد کنیم. بر همین اساس مطالب این گفتار را در دو بند ارائه می‌کنیم.

### بند اول: قصد ارتکاب رفتار مجرمانه (سوء نیت عام)

مهم ترین جزء رکن مادی بزه، همانا رفتار مجرمانه است. در واقع این رفتار مرتکب است که جرم را می‌سازد. اندیشه ی مجرمانه را به هیچ وجه نمی‌توان به تنهایی مجازات نمود

---

<sup>۱۳۷</sup> یکی دیگر از اموری که در بحث از علم مرتکب عمدتاً مورد نظر فقها قرار می‌گیرد، مسأله ی "التفات" است. به این معنا که مرتکب عالم بر حکم و موضوع، باید حین ارتکاب رفتار مجرمانه بر علم خویش نیز التفات و توجه داشته باشد. چنانچه به علت عدم دقت و توجه مرتکب جرم گردد، ولو اینکه علم بر حکم و موضوع نیز داشته باشد، باز هم در تحقق رکن روانی تردید وجود خواهد داشت. در نظام حقوقی ما مسأله ی التفات چندان مدخلیتی در رکن روانی جرایم ندارد. تنها در خصوص سرقت مستوجب حد قانون گذار به آن اشاره نموده است. از این رو در بحث از رکن روانی به این امر نمی‌پردازیم.

<sup>۱۳۸</sup> نوربها، رضا، منبع پیشین، صص ۳۳۱-۳۵۵.

<sup>۱۳۹</sup> malice

مگر آنکه به دنبال آن رفتاری از فرد سر بزند که شایسته ی عقوبت باشد. تنها در این حالت است که از ترکیب فکر و عمل، موجودی زاده می شود که آن را جرم می خوانیم.

از سوی دیگر، تنها صدور یک رفتار خلاف مقررات کیفری از یک شخص را نمی توان کافی برای مجازات وی دانست. بلکه تردیدی نیست که باید این رفتار از یک اراده ی آزاد و سالم و عاری از هر نوع نقصان پدید آمده باشد. انسان موجودی مختار و ذی شعور است و در انجام رفتارهای خود از قوه ی عقل و ادراک بهره می برد. مسئول بودن وی در قبال اعمال و رفتارش نیز به همین سبب است. حال چنانچه به دلیلی در انجام رفتاری، آزادی اراده و اختیار از وی سلب گردد و یا قوای دماغی و عقلانی وی دچار نقیصه یا تزلزل باشد، باید نسبت به مسئولیت او در برابر رفتارهایی که مرتکب می گردد تردید نمود.<sup>۱۴۰</sup>

ما در اینجا قصد بحث از مسئولیت کیفری و عوامل رافع آن را نداریم، بلکه به اقتضای بحث در مقام آنیم تا سوء نیت عام در بزه را تشریح کنیم. همان طور که بیان شد اراده ی آزاد انسان است که جرم را می سازد و همین اراده و قصد وی نسبت به ارتکاب رفتار مجرمانه را "سوء نیت عام" جرم می گوئیم.

در بزه موضوع بحث ما، اراده ی خودآگاه مرتکب باید متوجه فعل مجرمانه گردد. به این معنا که فرد آزادانه رفتار مادی جرم را که عبارت است از انتشار یا در دسترس قرار دادن محتوای خصوصی برای دیگران، انجام دهد.<sup>۱۴۱</sup> از این رو چنانچه فرد اساساً قصد دسترسی دیگران بر محتوای مجرمانه را نداشته باشد و اطلاعات را با رعایت تدابیر امنیتی در یک سیستم رایانه ای ذخیره نماید اما افرادی با توسل به شیوه های مختلف بتوانند در آن سیستم نفوذ کرده و اطلاعات را به دست آورند، نمی توان این فرد را مجرم دانست. همچنین است فردی که مسئول فیلم برداری از مجالس خانوادگی دیگران است اما مجموعه ای از فیلم ها و عکس های تهیه شده از یک مراسم عروسی را در یک محیط عمومی مانند اتوبوس ناخواسته جا بگذارد یا گم کند و افرادی که این بسته را به دست می آورند، آن را در سطح گسترده ای منتشر نمایند.

---

<sup>۱۴۰</sup> منصورآبادی، عباس، جزوه ی درس حقوق جزای عمومی دو، دانشکده ی حقوق و علوم سیاسی دانشگاه شیراز، ۱۳۸۵، صص ۱-۲۰.

<sup>۱۴۱</sup> میرمحمد صادقی، حسین، حقوق کیفری اختصاصی، جرایم علیه اموال و مالکیت، منبع پیشین، صص ۹۵-۹۶.

در این حالت نیز نمی توان این فرد را به واسطه ی این حادثه به استناد ماده ی ۱۷ مجازات نمود.

علاوه بر این چنانچه فرد در نتیجه ی عواملی که اراده ی آزاد را تحت الشعاع قرار می دهند اقدام به انتشار یا توزیع اطلاعات محرمانه و خانوادگی متعلق به دیگری نماید، باز هم رکن روانی در مورد وی متزلزل خواهد بود. مانند فردی که بر اثر تهدید به قتل و یا هتک عرض و ناموس ناگزیر می گردد تا فیلم خانوادگی یک ورزشکار را در دسترس دیگران قرار دهد. در این حالت نیز به علت مکره بودن مرتکب، سوء نیت عام بزه محقق نگردیده است. همان گونه که اگر فردی به واسطه ی مصرف الکل یا مواد روان گردان دچار اختلال در قوای عقلی گردیده باشد و بدین لحاظ ناخواسته اسرار متعلق به دیگری را افشا نماید باز هم رکن روانی بزه ناقص است و نمی توان فرد را به سبب ارتکاب این جرم مجازات نمود.<sup>۱۴۲</sup>

### بند دوم: قصد تحقق نتیجه ی مجرمانه (سوء نیت خاص)

جرم پدیده ای واحد است که از اجزای متعددی تشکیل می یابد. بر همین اساس بزهکار نیز در هنگام اقدام به ارتکاب جرم، قصد خود را متوجه تمام ارکان مجرمانه می سازد. یکی از اجزای جرم نتیجه ای است که از ارتکاب آن متوجه قربانی می گردد. در جرایم مالی، این اموال بزه دیده است که آماج جرم قرار می گیرد. به عنوان مثال در جرم تخریب، مال بزه دیده تلف می گردد. در جرایم علیه اشخاص نیز حسب مورد جان یا عرض و آبروی قربانی مخدوش خواهد شد.

همان گونه که می دانیم جرایم از حیث وجود یا فقدان نتیجه ی مجرمانه، بر دو نوع اند: مطلق و مقید. در جرایم مطلق که به صرف ارتکاب رفتار، جرم کامل می گردد، جزء نتیجه ی مجرمانه مفقود است و بدین لحاظ، قصد خاص مجرم در تحقق نتیجه ی خاص را تنها به عنوان "انگیزه"<sup>۱۴۳</sup> می توان مد نظر داشت که در ادامه در خصوص آن بحث خواهیم

---

<sup>۱۴۲</sup> البته در این مورد، باید مقررات مندرج در ماده ی ۵۳ قانون مجازات اسلامی در خصوص مستی ارادی نیز مورد توجه قرار گیرد، چرا که در صورت ارتکاب جرم در حال مستی اگر شرب خمر به منظور ارتکاب بزه بوده باشد، رافع مسئولیت کیفری نخواهد بود.

<sup>۱۴۳</sup> Motive

کرد. اما در جرایم مقید که تمام نمی شوند مگر به تحقق نتیجه ی مجرمانه، بزهدار باید قصد تحقق آثار و نتایج مورد نظر قانون گذار را داشته باشد. البته در مقام اثبات باید توجه داشت که بر اساس امارات قضایی وجود قصد بر نتیجه ی مورد نظر، معمولاً به سهولت احراز می گردد. از آنجا که بزه موضوع ماده ی ۱۷ قانون جرایم رایانه ای از جمله جرایم مقید به نتیجه است، لذا مرتکب باید قصد تحقق ضرر دارنده ی محتوای خصوصی یا هتک حیثیت وی را داشته باشد.

به نظر ما، هتک حیثیت یا ورود ضرر بر بزه دیده در نتیجه ی چنین رفتارهایی، نتیجه ی غالبی جرم خواهند بود. به عبارت دیگر انتشار صوت و تصویر خصوصی دیگری نوعاً موجب هتک حیثیت وی خواهد شد. و قصد فعل با علم به تأثیر نوعی آن در تحقق نتیجه، مانند قصد نتیجه است.<sup>۱۴۴</sup> از این رو شاید بتوان گفت، چنانچه از لحاظ عوامل مؤثر بر اراده ی مرتکب مانعی در میان نباشد، نباید نسبت به قصد خاص وی در حصول نتیجه ی مجرمانه – هتک حیثیت – تردید نمود.

در این مورد، به فرض احراز قصد خاص مجرم، سایر اهداف وی مانند اینکه او به منظور انتقام اقدام به انتشار تصاویر قربانی داشته است و یا به این اعتقاد که فرد مورد نظر، انسان ناشایسته و پستی است که به ناحق به موقعیت اجتماعی بالایی رسیده و باید با افشای اسرار وی، موقعیت او را از میان برد و نیز ادعای این که این اقدام تنها به منظور شوخی و تفریح بوده و مانند آن تنها می توانند از حیث تخفیف و یا تشدید مجازات مؤثر باشند و از نظر تأثیر در انتفای وصف مجرمانه نقشی نخواهند داشت.

علت این مطلب آن است که موارد پیش گفته، تنها انگیزه ی مجرم در ارتکاب جرم هستند و همان گونه که می دانیم، انگیزه از اجزاء رکن روانی نمی باشد. برای احراز وجود رکن روانی تنها وجود علم و آگاهی از یک سو و عمد و اراده از سوی دیگر کافی است و وجود عنصر اضافه ای ضرورت نخواهد داشت.

---

<sup>۱۴۴</sup> صادقی، محمد هادی، حقوق جزای اختصاصی، جرایم علیه اشخاص، صدمات جسمانی، میزان، تهران، ۱۳۸۵، صص ۱۰۶-۱۲۳.

## فصل سوم

### واکنش قانون گذار در قبال جرم هتک حیثیت از طریق

### افشای سر در محیط مجازی

پدیده ی مجرمانه بنا به یک تعریف عبارت است از انحراف از مهم ترین هنجارهای شناخته شده در هر جامعه. این انحراف بی تردید عکس العمل جامعه را در پی خواهد داشت. این عکس العمل ممکن است به شکل تهاجمی یا تدافعی صورت پذیرد. به این معنا که گاه اجتماع در دفاع از ارزش های مورد تعرض خود، دست به برخورد سرکوب گرانه می زند. این نوع رفتار جامعه را با عنوان واکنش های کیفری می شناسیم.

از سوی دیگر تمامی اقدامات اجتماع در رویارویی با پدیده ی مجرمانه در سرکوب منحرفین خلاصه نمی گردد و بی شک تدابیری اتخاذ خواهد شد تا از ارتکاب بزه ممانعت شود. این اقدامات را تحت عنوان تدابیر کنشی یا غیر کیفری می شناسیم.

در این فصل که فراز پایانی این نگاره است، ما بر آنیم تا انواع تدابیری که در برخورد با بزه مورد مطالعه ی خود در چهارچوب قوانین یا به روش های فراقیفری می توان اتخاذ نمود را بررسی نماییم. لذا طی دو مبحث به مطالعه ی تدابیر کیفری (مبحث اول) و تدابیر غیر کیفری (مبحث دوم) خواهیم پرداخت.

## مبحث اول - واکنش های کیفری

مهم ترین واکنش در قبال یک جرم را باید همان مجازات بزه کار دانست. این واکنش در نظام های کیفری مدرن به شکل های مختلف نمودار است. در نظام حقوق کیفری ما، در حال حاضر می توان دو گونه مجازات را برای جرایم مختلف برشمرد. مجازات های اصلی و مجازات های تبعی و تکمیلی. از سویی در برخی موارد ممکن است مجازات یک جرم به دلایلی خاص تشدید شود. بررسی این موارد پیرامون جرم افشای سر در محیط مجازی را در این مبحث طی سه گفتار پی می گیریم.

### گفتار اول: مجازات اصلی

واکنش کیفری که مقنن به عنوان مجازات اصلی بزه هتک حیثیت از طریق افشای سر پیش بینی نموده است را می توان از دیدگاه های مختلف دسته بندی نمود. بر اساس نوع مجازات - حبس و جزای نقدی - و یا بر اساس مرتکبین جرم. همان گونه که قبلاً بیان گردید، مرتکب جرایم رایانه ای ممکن است اشخاص حقیقی و یا حقوقی باشند. بر همین اساس مجازاتی که برای هریک از این مرتکبین مقرر گردیده است، متفاوت است. این تفاوت ناشی از ماهیت وجودی اشخاص حقوقی است. همان گونه که می دانیم، ویژگی اعتباری بودن شخصیت اشخاص حقوقی سبب می گردد تا اعمال برخی مجازات ها نسبت به آن ها مقدور نباشد. از جمله مجازات حبس که مختص اشخاص حقیقی است. بر همین مبنا مطالب این گفتار را در دو بند و بر اساس مرتکب جرم ارائه می نماییم.

### بند اول: مجازات اشخاص حقیقی

آنچه قانون گذار به عنوان مجازات مرتکب بزه پیش بینی نموده است، به استناد ذیل ماده ی ۱۷ عبارت است از «نود و یک روز تا دو سال حبس و یا جزای نقدی از پنج تا چهل میلیون ریال». برای ارزیابی این میزان مجازات باید آن را با مقررات قانونی دیگر مقایسه نمود.

با نگاهی بر قوانین سابق بر این قانون مشخص می‌گردد که قانون گذار از یک رویه ی مشخص در قبال این جرم پیروی ننموده است.

در قانون مجازات اسلامی به عنوان منبع جزایی مادر در جرم انگاری برای بزه افشای اسرار حرفه ای که تقریباً مشابه بزه ماده ی ۱۷ است معادل «سه ماه و یک روز تا یک سال و یک میلیون و پانصد هزار ریال تا شش میلیون ریال» مجازات تعیین گردیده بود. این میزان مجازات نسبت به مجازات مقرر در ماده ی ۱۷ خفیف تر است. اگرچه حد اقل حبس مقرر در ماده ی ۶۴۸ قانون مجازات اسلامی برابر با ماده ی ۱۷ است اما با توجه به اینکه حد اکثر حبس ماده ی ۶۴۸ کمتر است، لذا مجازات خفیف تر خواهد بود. همچنین جزای نقدی مقرر در قانون مجازات اسلامی هم از حیث حد اقل و هم حد اکثر، اخف از ماده ی ۱۷ است. شاید علت تشدید مجازات این بزه در قانون جرایم رایانه ای، میزان و گستردگی آثار مخربی است که از جرایم سایبری ایجاد می‌گردد.

ماده ی ۷۱ قانون تجارت الکترونیک، به عنوان دومین مقررره ی قانونی در ارتباط با این بزه، مجازاتی برابر با «یک تا سه سال حبس» را پیش بینی نموده بود. ملاحظه می‌شود که این مجازات هم نسبت به قانون مجازات اسلامی و هم در مقایسه با قانون جرایم رایانه ای، شدیدتر است. این شدت مجازات از دو بعد است. نخست عدم پیش بینی جزای نقدی در عرض حبس که دست قاضی را تا حدی در انتخاب نوع مجازات می‌بندد. دیگر میزان حبس مقرر در این قانون هم از لحاظ حد اقل و هم از جهت حد اکثر مجازات، اشد از دو قانون دیگر است. اشد یا اخف بودن مجازات، به سبب نسخ جزئی این قانون و نیز با توجه به پیش بینی مجازات اخف و نتیجتاً مساعد تر به حال مرتکب این بزه در قانون جرایم رایانه ای، می‌تواند واجد آثار قضایی باشد.

و اما مواد ۳، ۴، ۵ و ۸ قانون تشدید مجازات کسانی که در امور سمعی بصری فعالیت غیر مجاز دارند – همان گونه که از نام آن برمی‌آید- مجازات های متعدد و بسیار شدیدی را برای ارتکاب برخی از مصادیق این جرم تعیین نموده است که حتی تا حد افساد فی الارض پیش می‌رود. این میزان شدت و سخت گیری نسبت به مرتکبین جرایم مندرج در آن قانون، بی‌تردید به واسطه ی جریحه دار شدن عواطف و احساسات جامعه و لطمه به حیثیت برخی



افراد سرشناس و مشهور بوده و بیشتر یک اقدام سرکوب گرانه و شاید ناخواسته متأثر از سیاست کیفری «تسامح صفر»<sup>۱۴۵</sup> بوده است.

نهایتاً قانون جرایم رایانه ای که در حال حاضر مهم ترین مأخذ قانونی کیفری در برخورد با این جرم است، با عقب نشینی از موضع تند قانون گذار، مجازاتی نسبتاً متعادل را پیش بینی نموده است. علت این امر نیز فضای فکری حاکم بر روح این قانون است که تحت تأثیر دیدگاه های مربوط به تورم جمعیت کیفری و حبس زدایی و جایگزین های زندان به تصویب رسیده است.<sup>۱۴۶</sup>

به طور کلی، با نگاهی بر متون قانونی مصوب در این خصوص از قانون مجازات اسلامی تا کنون ملاحظه می گردد که سیاست کیفری مقنن ایرانی، یک ساختار منطقی را دنبال نمی نماید. بلکه در هر دوره و بنابر مقتضیات زمان و یا بر اساس سلیقه ی زمام داران دستگاه تقنینی و قضایی و گاهی نیز تحت تأثیر احساسات، و بیشتر به شکل مقطعی و زود گذر تصمیماتی اتخاذ می گردد و چه بسا با گذشت اندک زمانی و پس از بازگشت آرامش به فضای جامعه، به دست فراموشی سپرده شوند. در واقع مقنن ایرانی در بسیاری موارد، تنها به کارکرد مقطعی و "اعلامی" قوانین کیفری تکیه می کند.

## بند دوم: مجازات اشخاص حقوقی

همان طور که گفتیم، قانون جرایم رایانه ای، در یک نوآوری، رسماً مسئولیت کیفری اشخاص حقوقی را به طور کامل پذیرفته است و این مسئولیت را مانع مجازات مرتکب اصلی نمی داند. پیش بینی مسئولیت کیفری و نتیجتاً مجازات برای اشخاص حقوقی مستلزم متناسب نمودن مجازات های عمومی و معمول است که برای جرایم در ماده ی مربوطه مقرر می گردد. چراکه اعمال برخی از مجازات ها بر شخص حقوقی موضوعاً منتفی است. به عنوان مثال آیا می

<sup>۱۴۵</sup> جوانمرد، بهروز، تسامح صفر: سیاست کیفری سخت گیرانه در قبال جرایم خرد، منبع پیشین، صص ۶۸-۷۶.

<sup>۱۴۶</sup> جهت مطالعه ی تفصیلی ر.ک. عالی پور، حسن، حقوق کیفری فناوری اطلاعات، منبع پیشین، صص ۳۶۸-۳۷۹.

توان تصور نمود که یک شخص حقوقی که به جرم اقدام به قاچاق مواد مخدر محکوم گردیده است، در دادگاه محکوم به اعدام گردد؟<sup>۱۴۷</sup>

بدین لحاظ مقنن به این امر نیز عنایت داشته و ضمن پیش بینی مسئولیت کیفری برای شخص حقوقی، به خوبی اقدام به معادل سازی مجازات های مندرج در قانون جرایم رایانه ای نموده است و در ماده ی ۲۰ مقرر می دارد: «اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتكابی، میزان درآمد و نتایج حاصله از ارتكاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتكابی، به ترتیب ذیل محکوم خواهند شد . . .»

از این فراز ماده مشخص می گردد که چنانچه رأی کیفری ناظر به تعیین جزای نقدی باشد، به منظور محکومیت شخص حقوقی باید حداکثر جزای نقدی مندرج در رکن قانونی بزه مورد نظر ملاک قرار گرفته و میزان جزای نقدی به مأخذ سه تا شش برابر حداکثر محاسبه گردد. لذا در خصوص بزه مورد بحث ما، به سبب آنکه حد اکثر جزای نقدی معادل چهل میلیون ریال است، در صورت محکومیت یک شخص حقوقی به جزای نقدی به واسطه ی ارتكاب این جرم، میزان آن معادل ۱۲۰ الی ۲۴۰ میلیون ریال خواهد بود.

ماده ی فوق الاشعار فرضی را نیز که قاصی رأی به حبس صادر نماید طی دو بند بدین شرح پیش بینی نموده است: «الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال. ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم شخص حقوقی منحل خواهد شد.»

لذا در خصوص بزه مورد بحث، با توجه به این که حد اکثر مجازات حبس آن معادل دو سال می باشد، بند (الف) فوق الذکر موضوعیت یافته و شخص حقوقی در صورت ارتكاب این بزه و رأی دادرس به حبس، شخص حقوقی به مدت یک تا نه ماه تعطیل خواهد شد.

---

<sup>۱۴۷</sup> بحث از امکان یا عدم امکان شناسایی مسئولیت کیفری اشخاص حقوقی همواره مورد عنایت حقوق دانان کیفری بوده است و در تمامی کتب حقوق جزای عمومی به تفصیل به آن پرداخته شده است. برای مطالعه ی دقیق تر این موضوع می توان به کتب مربوطه از جمله: بایسته های حقوق جزای عمومی نوشته ی دکتر نوربها، زمینه ی حقوق جزای عمومی نوشته ی دکتر گلدوزیان و جزوه ی درس حقوق جزای عمومی ۳ از دکتر منصورآبادی و دیگر آثار مرتبط مراجعه نمود.

علت پیش بینی جزای نقدی شدیدتر برای شخص حقوقی شاید تمکن مالی بیشتر شخص حقوقی است. چراکه یکی از کارکردهای هر مجازات، بازدارنده بودن آن است. پیش بینی جزای نقدی به میزان اندک، نسبت به شخص حقوقی فاقد وصف بازدارندگی است. چراکه معمولاً یک شخص حقوقی به لحاظ امکانات و موقعیتی که از آن برخوردار است دارای تمکن مالی زیادی است. اصولاً دارایی یک شرکت بیش از دارایی یک فرد است و به همین سبب مقنن میزان جزای نقدی شخص حقوقی را تشدید نموده است.

در خصوص حبس نیز، مقنن دست به معادل سازی زده است. حبس مهم ترین مجازات سالب آزادی فرد است. اما شخص حقوقی را نمی توان حبس نمود. شاید بهترین گزینه برای آنکه یک شخص حقوقی از عرصه ی اجتماع کنار گذاشته شود، همان تعطیلی شخص حقوقی است. شخصی که محبوس می گردد، مدتی از جامعه طرد شده و امکان فعالیت برای وی غیر ممکن و یا شاید بسیار دشوار می شود. حال با تعطیل نمودن یک شخص حقوقی به طور موقت، همین هدف محقق شده و شخص حقوقی بزهکار موقتاً امکان کار و فعالیت را از دست خواهد داد. از سویی فرد زندانی پس از تحمل دوران حبس می تواند به اجتماع برگردد و در چرخه ی تولید و فعالیت های سازنده وارد شود. شخص حقوقی متخلف نیز پس از پایان دوران محکومیت امکان فعالیت مجدد را می یابد و به عرصه اجتماع باز خواهد گشت.

## گفتار دوم: مجازات های تبعی و تکمیلی

اصولاً مقنن برای هر بزه مجازات معینی پیش بینی کرده و آن را در قالب رکن قانونی بیان می نماید. این امر در راستای اصل "قانونی بودن جرم و مجازات" است. تعیین مجازاتی برای یک جرم بدون وجود مقرره ی قانونی، خلاف این اصل بنیانی حاکم بر حقوق جزا است. با این حال قانون گذار در برخی موارد، کیفر پیش بینی گردیده برای بزه را از جهاتی ناکافی می داند. از جمله با توجه به نوع و کیفیت جرم، شدت آثار سوئی که از ارتکاب بزه بر پیکره ی نظام اجتماع وارد می گردد و نیز شخصیت مجرم.

بدین لحاظ علاوه بر مجازات اصلی دو نوع دیگر از مجازات ها را نیز مد نظر داشته که به فراخور هر جرم ممکن است در قبال رفتار مجرمانه، بر مجرم تحمیل گردد. این قبیل

مجازات ها، شامل مجازات های تبعی و تکمیلی هستند که در این گفتار، امکان اعمال آن را در برخورد با مرتکب بزه افشای سر در محیط مجازی بررسی می کنیم.

## بند اول: مجازات های تبعی

منظور از مجازات های تبعی، مجازات هایی هستند که به تبع محکومیت و بدون نیاز به ذکر شدن در حکم دادگاه، بر محکوم علیه بار می شوند. گفتیم که در برخی جرایم به سبب اهمیت موضوع و یا شدت جرم، علاوه بر مجازات اصلی، محرومیت هایی دیگر نیز برای بزهکار مقرر گردیده است. در عنوان فصل سوم از قانون مجازات عمومی و نیز فصل سوم از قانون راجع به مجازات اسلامی مصوب سال ۱۳۶۱، به مجازات ها و اقدامات تأمینی و تربیتی تبعی و تکمیلی اشاره شده بود. اما فصل اول از باب دوم قانون مجازات اسلامی تنها به مجازات ها و اقدامات تأمینی و تربیتی اشاره کرده و سخنی از مجازات تبعی به میان نیاورده است.

متعاقباً در سال ۱۳۷۷ با الحاق یک ماده به عنوان ماده ی ۶۲ مکرر به قانون مجازات اسلامی، مسأله ی مجازات های تبعی نیز مد نظر مقنن قرار گرفت. در این ماده، برای ارتکاب برخی از جرایم عمدی محرومیت هایی از حقوق اجتماعی مقرر شده است. منظور از حقوق اجتماعی نیز طبق تبصره ی ۱ ماده ی ۶۲ مکرر عبارت است از «حقوقی که قانون گذار برای اتباع کشور جمهوری اسلامی ایران و سایر افراد مقیم در قلمرو حاکمیت آن منظور نموده و سلب آن به موجب قانون یا حکم دادگاه صالح می باشد . . .»<sup>۱۴۸</sup> ملاک تعیین این محرومیت نوع و میزان مجازاتی است که مجرم بدان محکوم می گردد.

<sup>۱۴۸</sup> این حقوق شامل اموری از قبیل موارد زیر است:

- الف- حق انتخاب شدن در مجالس شورای اسلامی و خبرنگان و عضویت در شورای نگهبان و انتخاب شدن به ریاست جمهوری
- ب- عضویت در کلیه ی انجمن ها و شوراها و جمعیت هایی که اعضای آن به موجب قانون انتخاب می شوند.
- ج- عضویت در هیأت های منصفه و امنا
- د- اشتغال به مشاغل آموزشی و روزنامه نگاری
- ه- استخدام در وزارتخانه ها، سازمان های دولتی، شرکت ها، مؤسسات وابسته به دولت، شهرداری ها، مؤسسات مأمور به خدمات عمومی، ادارات مجلس شورای اسلامی و شورای نگهبان و نهادهای انقلابی
- و- وکالت دادگستری و تصدی دفاتر اسناد رسمی و ازدواج و طلاق و دفتریاری
- ز- انتخاب شدن به سمت داوری و کارشناسی در مراجع رسمی
- ح- استفاده از نشان و مدال های دولتی و عناوین افتخاری

در همین قانون اعاده ی حیثیت محکوم علیه نیز پیش بینی گردیده و مدت آن تعیین شده است. بر اساس این ماده، در خصوص ۴ نوع مجازات اصلی، محرومیت از حقوق اجتماعی به عنوان مجازات تبعی مقرر شده است. نخست محکومیت به قطع عضو در جرایم مشمول حد، دوم محکومیت به شلاق در جرایم مشمول حد شرعی، سوم محکومیت به حبس تعزیری بیش از سه سال و چهارم در صورتی که اجرای حکم اعدام به دلیلی متوقف گردد نیز مجازات تبعی برای آن تعیین شده است.<sup>۱۴۹</sup>

در خصوص بزه مورد بحث ما، برای تشخیص اینکه آیا امکان تحمیل مجازات تبعی بر مرتکب وجود دارد یا خیر باید به نوع و میزان مجازات قانونی مقرر توجه نمود. نوع مجازات قانونی این جرم عبارت است از حبس تعزیری و جزای نقدی. چنانکه از مطالب فوق برمی آید جزای نقدی دربر دارنده ی مجازات تبعی برای مجرم نخواهد بود، لذا بحث ما دائر مدار حبس تعزیری است. از سویی به لحاظ آنکه حد اکثر مجازات حبس مقرر برای این جرم نیز، عبارت است از ۲ سال حبس تعزیری، لذا هیچ یک از چهار قسم مجازاتی که در بر دارنده ی مجازات تبعی هستند قابل انطباق با این جرم نبوده و بدین سبب محرومیت از حقوق اجتماعی بر مرتکب این جرم بار نمی گردد.

البته لازم به ذکر است طبق ماده واحده ی «تعریف محکومیت های مؤثر در قوانین جزایی» مصوب ۱۳۶۶ و اصلاحیه ی مصوب ۱۳۸۲،<sup>۱۵۰</sup> «محکومیت لازم الاجرا به مجازات حبس از یک سال به بالا در جرائم عمدی» و «محکومیت قطعی به جزای نقدی به مبلغ بیست میلیون ریال یا بالاتر در جرائم عمدی» در زمره ی محکومیت های کیفری مؤثر قرار گرفته است.<sup>۱۵۱</sup> از آنجا که حد اکثر مجازات این جرم دو سال حبس و یا چهل میلیون ریال جزای

---

<sup>۱۴۹</sup> میر محمد صادقی، حسین، حقوق کیفری اختصاصی، جرایم علیه اموال و مالکیت، منبع پیشین، صص ۱۰۹-۱۱۵.  
<sup>۱۵۰</sup> ماده واحده: مراد از محکومیت های مؤثر کیفری مذکور در قوانین جزایی مصوب مجلس شورای اسلامی عبارت است از:  
الف- محکومیت به حد.

ب- محکومیت به قطع یا نقص عضو.  
ج- محکومیت لازم الاجرا به مجازات حس از یک سال به بالا در جرائم عمدی.  
د- محکومیت قطعی به جزای نقدی به مبلغ بیست میلیون ریال یا بالاتر در جرایم عمدی.  
ه- سابقه ی محکومیت لازم الاجرا دو بار یا بیشتر به علت جرم های عمدی مشابه با هر میزان مجازات.  
جرم های سرقت، کلاهبرداری، اختلاس، ارتشا، خیانت در امانت جزو جرم های مشابه محسوب می شوند.  
<sup>۱۵۱</sup> مجموعه ی قوانین و مقررات آیین دادرسی کیفری، تدوین جهانگیر منصور، نشر دیدار.

نقدی است، چنانچه فرد به یک سال حبس یا بیشتر و یا جزای نقدی بیست میلیون ریال و یا بالاتر از آن محکوم گردد، دارای سابقه کیفری مؤثر خواهد گردید و بدین لحاظ از برخی حقوق اجتماعی - از جمله حق استخدام در دستگاه های دولتی - محروم خواهد شد. این محرومیت که تبعاً بر وی اعمال می گردد را می توان یک مجازات تبعی ناشی از ارتکاب بزه دانست.

## بند دوم: مجازات های تکمیلی

برخلاف مجازات های تبعی، مجازات های تکمیلی تنها با قید در حکم دادگاه قابل اعمال بر محکوم علیه هستند. این مجازات ها که در قانون مجازات اسلامی و در ماده ی ۱۹ پیش بینی شده است، شامل محرومیت از حقوق اجتماعی، ممنوعیت از اقامت در نقطه یا نقاط معین و یا اجبار به اقامت در نقطه ای معین است. اعمال این نوع مجازات ها در خصوص مرتکبین جرایم عمدی مشمول مجازات های تعزیری یا بازدارنده امکان پذیر است.

در مورد بزه موضوع ماده ی ۱۷، از آنجا که این جرم در زمره ی جرایم مستوجب مجازات تعزیری بوده و همچنین یک بزه عمدی است، اعمال ماده ی ۱۹ قانون مجازات اسلامی در مورد مرتکب بلا اشکال است.

علاوه بر این قانون گذار در ماده ی ۲۷ قانون جرایم رایانه ای، نوعی مجازات تکمیلی را برای کسانی که بیش از دو بار مرتکب تکرار جرایم رایانه ای و از آن جمله افشای سر در محیط مجازی می گردند، پیش بینی نموده است. مطابق ماده ی ۲۷ قانون جرایم رایانه ای: «در صورت تکرار جرم برای بیش از دو بار دادگاه می تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نود و یک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.»

مجازات تکمیلی پیش بینی شده در این ماده نیز مانند ماده ی ۱۹ قانون مجازات اسلامی، از جمله مجازات های تکمیلی اختیاری است اما میزان و مدت آن مطلقاً در اختیار قاضی قرار داده نشده و مقنن خود حد اقل و حد اکثر مجازات تکمیلی را پیش بینی نموده است.

در تطبیق این ماده با ماده ی ۱۷ یعنی رکن قانونی بزه مورد بحث، باید گفت به لحاظ آنکه مجازات قانونی جرم افشای اسرار در فضای سایبری معادل نود و یک روز تا دو سال حبس است، لذا مورد با بند (الف) ماده ی فوق منطبق بوده و مرتکب در صورت تکرار جرم بیش از دو مرتبه، ممکن است به مدت یک ماه تا یک سال از خدمات الکترونیک عمومی محروم گردد. البته پیش بینی اعمال این قبیل مجازات ها در صورت تکرار جرم برای بیش از دو مرتبه، مانع اختیار دادرس در محکومیت مرتکب به همین مجازات تکمیلی در حالتی که وی مرتکب تکرار جرم نگردیده است، نمی باشد و قاضی همواره می تواند با استناد به ماده ی ۱۹ قانون مجازات اسلامی هر گونه مجازاتی را که برای تکمیل حکم خویش ضروری بداند نسبت به بزهکار اعمال نماید.

یکی از نکات مثبت قانون جرایم رایانه ای در پیش بینی مجازات همین توجه به ماهیت جرم است. بدین معنی که همچنان که جرم ماهیتی الکترونیک دارد، مجازات تکمیلی آن نیز باید متناسب با ماهیت جرم باشد. لهذا مرتکب به عنوان تکمیل مجازات از خدمات الکترونیکی محروم می گردد. این دقت نظر مقنن در تدوین قانون جرایم رایانه ای - علی رغم وجود برخی کاستی ها در این قانون - شایسته ی تقدیر است.<sup>۱۵۲</sup>

---

<sup>۱۵۲</sup> سعیدی نژاد، یاسمن، جرم انگاری در فضای مجازی، تعالی حقوق، شماره ی ۲، صص ۲۴-۲۸ و نیز عالی پور، حسن، منبع پیشی، صص ۳۸۰-۳۸۹.

## گفتار سوم: مجازات شریک و معاون در جرم و موارد تشدید

### مجازات

یکی دیگر از موارد قابل بررسی در هر بزه، مجازاتی است که مقنن برای شرکت در جرم یا معاونت در ارتکاب آن مقرر داشته است. از سوی دیگر موارد تشدید مجازات در خصوص جرایم را می توان به اشکال متفاوتی بررسی نمود. کیفیات مشدده را بر حسب قابلیت اعمال در قبال جرایم مختلف به کیفیات مشدده ی عام و خاص تقسیم می نمایند. به لحاظ آنکه مقنن تعدادی از مواد قانون جرایم رایانه ای را تحت عنوان "موارد تشدید مجازات" به تعیین موارد تشدید مجازات در قلمرو جرایم سایبری و رایانه ای اختصاص داده است، لذا ما نیز این مواد را با موضوع بحث خود انطباق داده و نحوه ی تشدید مجازات در واکنش قابل اعمال در برخورد با بزه افشای سر در محیط مجازی را بررسی خواهیم نمود.

### بند اول: مجازات شریک و معاون در بزه

مسأله ی شرکت در جرم یکی از تأسیسات حقوق جزا است که در نظام حقوقی ما نیز از آغاز مورد عنایت قانون گذار بوده و در طی زمان دست خوش تغییر و تحولات فراوان گردیده است. ما در اینجا به دنبال بررسی تفصیلی این نهاد کیفری نیستیم و در تمام کتب حقوق کیفری عمومی مفصلاً از آن بحث به میان آمده است.<sup>۱۵۳</sup> اما به اقتضای بحث خود که در چهارچوب حقوق جزای اختصاصی است، به آن اشاره می نماییم.

با صرف نظر از سابقه ی تاریخی این تأسیس، در حال حاضر ماده ی ۴۲ قانون مجازات اسلامی مقرر داشته است: «هرکس عالماً و عامداً با شخص یا اشخاص دیگر در یکی از جرایم قابل تعزیر یا مجازات های بازدارنده مشارکت نماید و جرم مستند به عمل همه ی آن ها باشد خواه عمل هریک به تنهایی برای وقوع جرم کافی باشد خواه نباشد و خواه اثر کار آن ها مساوی باشد خواه متفاوت، شریک در جرم محسوب و مجازات او مجازات فاعل مستقل آن جرم خواهد بود. ...»

<sup>۱۵۳</sup> نوربها، رضا، زمینه ی حقوق جزای عمومی، صص ۲۱۴-۲۲۵.



این ماده حکم کلی شرکت در جرایم تعزیری را مقرر می‌دارد و از آنجایی که قانون جرایم رایانه‌ای به انتهای کتاب پنجم قانون مجازات اسلامی الحاق گردیده است، لذا جرایم مندرج در این قانون از جمله جرایم تعزیری و بازدارنده بوده و ماده ی ۴۲ نسبت به شرکای در این جرایم و از جمله جرم موضوع ماده ی ۱۷ قانون مزبور قابل اعمال خواهد بود. لذا چنانچه افرادی با شراکت یکدیگر اقدام به راه اندازی یک وبلاگ تفریحی و سرگرمی نمایند و سپس با مداخله ی دو یا چند نفر از ایشان که نام کاربری و گذرواژه ی مربوط به وبلاگ مزبور را در اختیار دارند، محتوای صوتی یا تصویری حاوی اطلاعات خصوصی یا خانوادگی متعلق به یک شخص مشهور یا داده های متنی متعلق به وی که در بردارنده ی اسرار خصوصی اوست، در وبلاگ قرار داده شود و بدین ترتیب جرم منظور به وقوع پیوندد، افرادی که در ارتکاب رفتار مجرمانه دخالت داشته اند، به یک میزان مسئول و قابل مجازات خواهند بود. حتی به نظر می رسد بتوان فرضی را نیز که در آن یکی از افراد دارای اطلاعات ورود به وبلاگ، محتوای مجرمانه را در محیط مجازی وبلاگ قرار دهد و دوست وی که او هم امکان دسترسی به اطلاعات مندرج در وبلاگ و حذف و اصلاح آن ها را دارد، با علم بر مجرمانه بودن رفتار، عمداً از حذف آن محتویات امتناع می نماید، همانند مورد پیش گفته مشمول حکم شرکت در ارتکاب جرم دانست و اشخاص مزبور را تحت پیگرد و مجازات قرار داد.

معاونت در جرم نیز یکی دیگر از مباحث حقوق جزای عمومی است که انعکاس آن در جزای اختصاصی انکار ناپذیر است. جدا از مباحث نظری که در خصوص عاریتی بودن مسئولیت معاون جرم مطرح گردیده است، در برخی از جرایم قانون گذار برخی رفتارها را که در حقیقت معاونت در ارتکاب یک بزه خاص هستند را مستقلاً جرم انگاری نموده و لذا از بسیاری جهات متفاوت از وضعیت معاونت در جرم می گردد.

ضابطه ی عمومی حاکم در تشخیص رفتار معاون در جرم در نظام حقوقی ما ضمن ماده ی ۴۳ قانون مجازات اسلامی منعکس گردیده است. بعلاوه ماده ی ۷۲۶ همان قانون در مقام تعیین مجازات برای معاون در جرم پیش بینی نموده است: «هرکس در جرایم تعزیری معاونت نماید حسب مورد به حد اقل مجازات مقرر در قانون برای همان جرم محکوم می

شود.<sup>۱۵۴</sup> با جمع دو ماده ی فوق با نکته ای که در سطور پیشین بیان گردید و نگاهی بر قانون تشدید مجازات افرادی که در امور سمعی بصری فعالیت غیر مجاز می کنند، باید گفت برخی از مصادیق مجرمانه ی مندرج در این قانون به منزله ی نوعی معاونت در ارتکاب بزه مورد نظر ماست. مانند کسی که از مجالس خانوادگی دیگران یا از اماکن اختصاصی بانوان به طور غیر مجاز اقدام به تهیه ی فیلم یا عکس و تصویر نموده است و سپس این اطلاعات و داده ها را در اختیار دیگری قرار می دهد تا منتشر نموده و یا در دسترس دیگران قرار دهد، با جمع سایر شرایط مربوط به معاونت در جرم - از جمله وجود وحدت قصد مجرمانه - مطابق با ماده ی ۵ قانون فوق قابل مجازات خواهد بود. بند «ب» و «ج» ماده ی مزبور به جرم انگاری تهیه ی فیلم و عکس از اماکن اختصاصی بانوان و تکثیر و توزیع آن و نیز تهیه ی مخفیانه ی فیلم و عکس مبتذل از مراسم خانوادگی دیگران و تکثیر و توزیع آن پرداخته است. گرچه تکثیر و توزیع این گونه فیلم و عکس ها با تصویب قانون جرایم رایانه ای طبق ماده ی ۱۷ قابل مجازات است و قانون پیش گفته در این قسمت به صورت جزئی نسخ شده اما در مورد تهیه این قبیل فیلم و عکس ها به لحاظ سکوت قانون جرایم رایانه ای ناگزیر از آنیم که قانون فوق را لازم الاجرا بدانیم. با این وجود در خصوص سایر مصادیق معاونت در جرم - مانند تحریک و ترغیب و دسیسه و نیرنگ و ...- با توسل به ماده ی ۷۲۶ قانون مجازات اسلامی، مجازات معاون در این جرم همان حد اقل مجازات مباشر جرم یعنی نود و یک روز حبس یا پنج میلیون ریال جزای نقدی و یا هردو مجازات خواهد بود. در مورد اشخاص حقوقی که در ارتکاب این بزه معاونت داشته اند، با لحاظ ماده ی ۱۷ و با تطبیق مفاد ماده ی ۲۰ با آن باید گفت مجازات شخص حقوقی در چنین حالتی پانزده میلیون ریال و یک ماه تعطیلی موقت خواهد بود.<sup>۱۵۵</sup>

<sup>۱۵۴</sup> همان، صص ۲۲۶-۲۴۰.

<sup>۱۵۵</sup> شایان ذکر است موارد معاونت در جرم متعدد را در برمی گیرد. مانند تحریک فردی در يك کشور و ارتکاب بزه در کشور دیگر. اما این قبیل مصادیق بیشتر در قلمرو حقوق جزای بین الملل قرار می گیرد که به علت خروج از قلمرو مطالعاتی خود که حقوق جزای اختصاصی می باشد از توضیح آن صرف نظر می کنیم

## بند دوم: موارد تشدید مجازات

مرتکب یک بزه در حالت عادی مستحق اعمال میزان معینی مجازات می باشد که نوع و مقدار آن اصولاً در قوانین کیفری مشخص گردیده و تعیین میزان دقیق آن با توجه به کیفیت ارتکاب جرم و وضعیت خاص مرتکب در اختیار قاضی قرار دارد. در واقع قاضی از سوی قانون گذار تا حدی آزاد و مختار شده تا بنا به رأی و تشخیص خود مجازات را با مجرم متناسب سازد. این قاعده را تحت عنوان "فردی کردن مجازات" می شناسیم.<sup>۱۵۶</sup> با این حال مواردی وجود دارد که به تشخیص مقنن و همچنین به حکم عقل سلیم ممکن است مجازات مقرر برای بزهکار مناسب و کافی نباشد. مصداق بارز این وضعیت را می توان در خصوص تعدد و تکرار جرم مشاهده نمود. همین امر موجب گردیده که در تمام قوانین مدرن کیفری دنیا، مسأله ی تشدید مجازات مطمح نظر مقننین کیفری قرار داشته باشد. قانون مجازات اسلامی نیز با تمام نقایص خود، این تأسیس کیفری را در خود گنجانده است. مواد ۴۶-۴۸ ق. م. ا. به تعیین حکم تعدد و تکرار جرم پرداخته است.

تعدد و تکرار جرم را عوامل عام تشدید مجازات می دانند. با این حال، از سوی دیگر گاه کیفیت ارتکاب جرم به گونه ای است که مقنن را قانع می کند کیفر بزهکار را نسبت به حالت عادی ارتکاب تشدید نماید. نمونه ی بارز این موارد را می توان در فصل سرقت های تعزیری کتاب پنجم ق. م. ا. مشاهده نمود.

قانون جرایم رایانه ای در ادامه ی نوآوری های خود، فصل هشتم از بخش اول را به بیان موارد تشدید مجازات اختصاص داده است. این فصل که شامل دو ماده است، قابل اعمال در خصوص تمام جرایم مندرج در این قانون بوده و در موارد نقص یا سکوت آن می توان به ق. م. ا. استناد نمود. دو ماده ی ۲۶ و ۲۷ قانون فوق به ترتیب در بر دارنده ی کیفیات خاص و عام تشدید مجازات هستند.

ماده ی ۲۶ طی ۵ بند موارد متعددی از عوامل مشدده ی کیفر را برشمرده است. بند «الف» دربر دارنده ی حکمی نسبت به کارمندان بخش دولتی و عمومی کشور است. هرگاه

<sup>۱۵۶</sup> میان اصل فردی کردن مجازات و شخصی بودن مجازات تفاوت وجود دارد برای مطالعه ی این مطلب ر.ک. همان، صص ۴۲۰-

جرم رایانه ای توسط این قبیل افراد ارتکاب یابد، به لحاظ موقعیت اجتماعی که ایشان از آن برخوردار اند، رفتار آن ها مستحق اعمال مجازات بیشتری خواهد بود. بند «ب» خطاب به متصدیان و متصرفان قانون شبکه های رایانه ای بوده که به مناسبت شغل خود مرتکب این قبیل جرایم می گردند. بند «ج» در مورد تشدید مجازات به اعتبار اهمیتی است که داده های موضوع جرم دارند. هرگاه داده های موضوع بزه از داده های متعلق به دولت یا بخش خدمات عمومی جامعه باشد، به لحاظ گستردگی دامنه ی خساراتی که از این رهگذر بر زندگی اجتماعی وارد می گردد مرتکب با تشدید مجازات رو برو خواهد شد. البته این بند در مورد جرم مورد نظر ما موضوعیت ندارد. چراکه همچنان که پیش تر گفتیم موضوع این جرم، اسرار خصوصی و خانوادگی افراد بوده و هیچگاه متصف به وصف دولتی و عمومی نخواهد گردید. لذا بند «ج» ماده ی ۲۶ قابل استناد در این جرم نخواهد بود. بند های «د» و «ه» نیز به منظور تشدید مجازات در فرضی است که جرم به شکل سازمان یافته یا در سطح گسترده ارتکاب یافته باشد که هر فرد معقولی تأیید می کند که گستردگی ابعاد جرم و نیز سازمان یافته بودن آن، لطمات بس فراوانی بر پیکره ی حیات اجتماعی وارد می آورد و پیش بینی تشدید مجازات در این موارد منطقی است. اما میزان تشدید مجازاتی که مقنن در این مورد در نظر گرفته است عبارت است از محکومیت مرتکب به بیش از دو سوم حد اکثر مجازات قانونی بزه. از این رو هرگاه در جریان رسیدگی به بزه موضوع ماده ی ۱۷، یکی از کیفیات مشدده ی مندرج در ماده ی ۲۶ توسط دادرس احراز گردد، با توجه به سقف مجازات مندرج در ماده ی ۱۷، وی مکلف است تا به بیش از ۱۶ ماه حبس یا بیش از ۲۷ میلیون ریال جزای نقدی حکم دهد. نکته ی جالب توجه، الزامی بودن تشدید مجازات در این موارد است.

اما ماده ی ۲۷ قانون جرایم رایانه ای اختصاص به تشدید مجازات در مورد تکرار جرم آن هم برای بیش از دو مرتبه تکرار جرم دارد. تشدید مجازات مقرر در این ماده اختیاری بوده و بنا بر میزان مجازات قانونی هر بزه، میزانی از مجازات های تکمیلی به عنوان تشدید مجازات پیش بینی گردیده است. در خصوص بزه مورد بحث ما، بند «الف» ماده ی فوق قابل استناد بوده و مرتکبی که واجد شرایط تشدید مجازات باشد، ممکن است به مدت یک ماه تا یک سال از برخی حقوق اجتماعی که بیشتر جنبه الکترونیکی داشته – و منطبق با ماهیت قانون جرایم رایانه ای نیز می باشد – از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای

کشوری و بانکداری الکترونیکی محروم گردد. نکته ی قابل ذکر در مورد این قبیل مجازات ها این است که با توجه به تنوع و سهولت استفاده از خدمات الکترونیک در دنیای امروز، پیش-بینی این مجازات ها چندان کارآمد نخواهد بود. به عنوان مثال چنانچه فردی از داشتن تلفن همراه به نام خود محروم گردد به راحتی می تواند از تلفن دیگر اعضای خانواد ی خود استفاده نماید. یا هرگاه فردی از داشتن نام دامنه ی مرتبه ی بالای کشوری – یعنی همان دامین ".ir" در دایر نمودن و استفاده از تارنماهای اینترنتی – محروم گردد، به راحتی می تواند از نام دامنه ی بین المللی – از قبیل com و یا net و ... – که گاه امکانات بیشتری نیز در اختیار وی قرار می دهد استفاده نماید.

## مبحث دوم- تدابیر غیر کیفری

آنچه در این مبحث مورد بررسی قرار خواهد گرفت عبارت است از تدابیری که مقنن در قانون جرایم رایانه ای اتخاذ نموده تا حتی المقدور از ارتکاب جرایم رایانه ای و از جمله بزه مورد بحث ما جلوگیری گردد. از سوی دیگر به برخی راهکار های فنی اشاره خواهد شد که گرچه جنبه ی تقنینی ندارند اما با توسل به آن ها افراد می توانند مانع از بزه دیدگی خود شوند و جامعه از گزند ناقضان هنجارهای والای انسانی مصون بماند.

### گفتار اول – پالایش محتوای مجرمانه

یکی از تدابیری که مقنن کیفری در قانون جرایم رایانه ای اتخاذ نموده تا حتی الامکان از ارتکاب جرایم رایانه ای ممانعت نماید، عبارت است از راهکار فیلترینگ یا به اصطلاح مقنن ایرانی «پالایش محتوای مجرمانه». بررسی مسأله ی فیلترینگ در عرصه ی محیط مجازی موضوعی بس گسترده است که مجال دیگری می طلبد. اما در این مقال به اقتضای موضوع تحقیق و پلان کار ناگزیر از اشاره ای اجمالی به آن هستیم. در این قانون نمایندگان مجلس شورای اسلامی به منظور ایجاد رویه ی واحد در امر فیلترینگ، ضمن ماده ی ۲۲ قانون جرایم رایانه ای نهادی تحت عنوان "کمیته ی تشخیص مصادیق محتوای مجرمانه" را مأمور مشخص

ساختن مصادیقی که مشمول عنوان مجرمانه در محیط سایبری می گردد نموده اند. این کمیته نیز طی جلساتی به تعیین مواردی از محتوای مجرمانه پرداخته و آیین نامه ای نیز با همین نام منتشر کرده است. از سوی دیگر، قانون گذار ضمن ماده ی ۲۱ قانون فوق یک تکلیف مهم را متوجه ارائه دهندگان خدمات دسترسی به شبکه ی اینترنت نموده و تخطی از این تکلیف را مشمول اعمال مجازات دانسته است. در این گفتار طی دو بند این مسائل را بررسی می کنیم.

### **بند اول - تکلیف ارائه دهندگان خدمات دسترسی و میزبانی**

این تکلیف که طی مواد ۲۱ و ۲۳ قانون جرایم رایانه ای تعیین گردیده عبارت است از پالایش وب سایت ها و وبلاگ هایی که در بر دارنده ی مصادیق محتوای مجرمانه هستند. ارائه دهندگان خدمات دسترسی، شامل هر شخص حقیقی یا حقوقی اند که امکان ارتباط یا اتصال به اینترنت را برای کاربران فراهم می کنند. با توجه به لزوم تفسیر مضیق قانون، به نظر می رسد منظور قانون گذار از عبارت «ارائه دهندگان خدمات دسترسی»، همان ارائه دهندگان خدمات اینترنتی می باشد که کاربران با مراجعه به ایشان و پرداختن مبلغی به عنوان حق اشتراک (و یا در گذشته با خرید کارت های اینترنت) به واسطه چنین ارائه دهندگانی و از طریق رایانه های شخصی و یا گوشی تلفن های همراه خود به دنیای نامحدود اینترنت پای می گذارند و از سرویس های متنوع آن، بهره می برند. ارائه دهندگان خدمات دسترسی بر اساس مقررات و در حد متعارف مکلف می باشند که از رهگذر تدابیری هم چون پالایش (فیلتر)، نصب دیوار آتشین و مانند آن از ارائه ی محتویات غیرقانونی تعریف شده در قانون جلوگیری نمایند .

از دیدگاه دانش مهندسی نرم افزار رایانه، قانون گذار بیشترین بار مسؤلیت قانونی را بر عهده ارائه دهندگان خدمات دسترسی نهاده که بر حسب اتفاق بیشتر آن ها از بخش خصوصی بوده و مشابه سایر حوزه های تخصصی این بخش، توان مالی، انسانی و... محدودی دارند. طبقه بندی محتویات، ارزیابی و حذف آن ها، نصب نرم افزارهای مربوط به پالایش بر حسب کیفیت و کمیت عملکرد آن ها، اغلب متضمن هزینه های گزافی است که اتخاذ تدابیر حمایتی از سوی دولت را در این زمینه الزامی می سازد. تکلیف دیگر که در ماده ی ۲۳ قانون جرایم

رایانه ای پیش بینی گردیده است، مستقیماً متوجه ارائه دهندگان خدمات میزبانی<sup>۱۵۷</sup> و هاستینگ است. توضیح آنکه کاربران فضای سایبر، برای ذخیره داده‌های متنی، صوتی و تصویری خود در این محیط، به فضای حافظه نیاز دارند. ارائه‌دهندگان خدمات میزبانی، اشخاص حقیقی یا حقوقی هستند که با دریافت مبالغی، فضای لازم برای ذخیره داده‌های کاربران در فضای سایبر را فراهم می‌کنند. حال چنانچه فردی با استفاده از فضای حافظه ای که ارائه دهنده ی خدمات میزبانی در اختیار وی قرار داده است به انتشار محتوای مجرمانه بپردازد، به عنوان مثال فیلم های خانوادگی متعلق به یک شخص را که بدون رضایت وی به دست آورده است در فضای سایبری به اشتراک گذارد، ارائه دهنده ی سرویس مزبور به محض اطلاع از دستور مقام قضایی یا کمیته ی تعیین مصادیق محتوای مجرمانه، مکلف به پالایش آن خواهد بود و نیز موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه تعیین مصادیق محتوای مجرمانه اطلاع دهند.

قانون گذار برای تخطی از این تکلیف قانونی مجازات سنگینی پیش بینی کرده است. چنانچه ارائه دهندگان سرویس های اینترنتی عمداً از انجام وظیفه ی قانونی خود امتناع کنند منحل خواهند شد و در صورتی که به واسطه ی بی احتیاطی یا بی مبالاتی مرتکب آن گردند در مرتبه ی نخست به جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال و در مرتبه ی دوم به جزای نقدی از یکصد میلیون ریال تا یک میلیارد ریال و در مرتبه ی سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

البته در رابطه با شدت و میزان مجازات مقرر شده در این مواد، بهتر بود مقنن برای مرتبه اول و دوم، مجازات انضباطی، مانند تذکر کتبی و یا کم کردن پهنای باند برای مدتی مشخص و یا تعطیلی چند روزه در نظر می‌گرفت. چراکه از نظر متخصصان حوزه فناوری اطلاعات و ارتباطات، باید ضریب خطای ماشینی و یا انسانی را در این میان مد نظر قرار داد و با دیدن اولین تخلفات به سراغ مجازات نرفت .

---

<sup>۱۵۷</sup> hosting

## بند دوم - موارد پالایش محتوای مجرمانه

همان گونه که گفتیم قانون جرایم رایانه ای در ماده ی ۲۲ تشکیل کمیته ای جهت تعیین مصادیق محتوای مجرمانه در فضای سایبری را پیش بینی نموده است. پس از تشکیل کارگروه و گذشت چندین جلسه و با یک تأخیر تقریباً چهارماهه، اولین ویرایش از فهرست مصادیق محتوای مجرمانه در تاریخ هشتم دی‌ماه سال ۱۳۸۸ منتشر شد و سپس در ویرایش‌های بعدی مفاد آن مورد تغییراتی جزئی قرار گرفت.

انتشار این فهرست بازتاب‌های مختلفی را برانگیخت. از یک سو، کارگروه، افزایش گزارشات دریافتی مردمی جهت پالایش (فیلترینگ) وبلاگ‌ها و وب سایت‌هایی با مصادیق مجرمانه را تأیید می‌کند و از طرفی واکنش برخی از وبلاگ نویسان و استفاده کنندگان از سرویس‌های فارسی بیانگر انتقاد از دامنه ی وسیع این مصادیق و احساس افزایش محدودیت‌ها در فضای سایبر است. این فهرست بیش از آنکه به مصادیق مجرمانه پرداخته باشد، به گردآوری عناوین مجرمانه که پیش از آن در قوانین دیگر وجود داشت پرداخته است.<sup>۱۵۸</sup>

در این فهرست هفت دسته ی کلی از مصادیق محتوای مجرمانه برشمرده شده که هر یک دربر دارنده ی عناوین مجرمانه ی متعددی می باشد. این تقسیم بندی به شرح ذیل است: الف- محتوای علیه عفت و اخلاق عمومی. ب- محتوای علیه مقدسات اسلامی. ج- محتوای علیه امنیت و آسایش عمومی. د- محتوای علیه مقامات و نهادهای دولتی و عمومی. ه- محتوایی که برای ارتکاب جرایم رایانه ای به کار می رود (محتوای مرتبط با جرایم رایانه ای). و- محتوای مجرمانه ی مربوط به امور سمعی بصری و مالکیت معنوی. ز- محتوایی که تحریک، ترغیب یا دعوت به ارتکاب جرم می کند (محتوای مرتبط با سایر جرایم)

در اینجا می خواهیم ببینیم آیا این مصادیق شامل انتشار اسرار دیگری در محیط مجازی می گردد؟ به عنوان مثال اگر یک وبلاگ نویس اسرار متعلق به دیگری را در وبلاگ شخصی خود منتشر نمود یا فیلم خانوادگی شخصی در یک وب سایت به معرض دید عموم قرار

---

<sup>۱۵۸</sup> در حال حاضر می توان برای دسترسی به این فهرست با درج آدرس یکی از وب سایت هایی که مورد فیلترینگ قرار گرفته اند در مرورگر اینترنت ، به صفحه ی "پیوند ها" وارد شد و در بخش پایینی صفحه فهرست مصادیق محتوای مجرمانه را به طور کامل رؤیت نمود.



گرفت، آیا امکان فیلتر نمودن آن وب سایت یا وبلاگ وجود دارد؟ و آیا ارائه دهندگان خدمات دسترسی یا میزبانی تکلیفی برای پالایش این قبیل وب سایت ها دارند؟

با نگاهی به عناوین هفت گانه ی فوق الذکر ملاحظه می شود تنها عناوینی که ممکن است در بردارنده ی مصادیقی از بزه مورد نظر ما باشند، بند (الف) و (و) است. اما با بررسی موارد مذکور در ذیل این دو بند، مشخص می گردد که هیچ موردی از موارد الزامی فیلترینگ به جرم موضوع ماده ی ۱۷ قانون جرایم رایانه ای اشاره ننموده است. از این رو باید گفت ارائه دهندگان خدمات دسترسی و میزبانی رأساً تکلیفی برای پالایش این قبیل سایت ها ندارند.

با این حال تبصره ی ۲ ذیل ماده ی ۲۱ قانون فوق، به پیش بینی فیلترینگ در خصوص جرایمی اختصاص یافته که با شکایت شاکی خصوصی تعقیب می گردد. این تبصره مقرر می دارد: «پالایش (فیلتر) محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضایی رسیدگی کننده به پرونده انجام خواهد گرفت.» با توجه به ماهیت بزه موضوع ماده ی ۱۷، - که اصولاً یک جرم علیه شخصیت معنوی بوده و لذا بزه دیده اقدام به طرح شکایت می نماید - در ضمن رسیدگی به چنین پرونده ای، دادرس می تواند با درخواست شاکی خصوصی دستور پالایش وب سایت یا وبلاگی که در بر دارنده ی محتوای خانوادگی یا خصوصی یا اسرار متعلق به شاکی است را صادر نماید. در این صورت ارائه دهندگان خدمات دسترسی یا میزبانی طبق قانون جرایم رایانه ای مکلف به تمکین از دستور مقام قضایی بوده و موظف به فیلتر چنین وب سایتی خواهند بود.

## گفتار دوم - تدابیر مبتنی بر رفتار بزه دیده و بزهدار

در پایان این نوشتار درخور است اندکی به بحث های فراکیفری نیز پرداخته شود. گرچه این نگاره بنا به قلمرو موضوعی در چهارچوب حقوق جزای اختصاصی می گنجد، اما لاجرم در هر بحث جزای اختصاصی نیز مسائل مربوط به جرم شناسی کم و بیش مطرح می گردد.

در این گفتار طی دو بند به اختصار به این مطلب می پردازیم که چگونه می توان مانع از این شد که بزه افشای سر در محیط مجازی به وقوع بپیوندد.

## بند اول - چگونه از بزه دیده شدن بپرهیزیم؟

صرف نظر از بحث های جرم شناسی راجع به انواع پیش گیری از وقوع جرم - مانند پیش گیری وضعی، فنی، بزه دیده محور و ...- در اینجا به بیان نکاتی پیرامون بزه خاص افشای اسرار در محیط سایبری می پردازیم.

همچنان که زمان به پیش می رود، فناوری های نوین نیز جهش های خارق العاده ای را در سال های اخیر تجربه می کنند. به همین نسبت دست یابی بر اطلاعات و از جمله محتوای خصوصی افراد آسان گردیده است. کافی است در یکی از موتورهای جستجوی اینترنتی نام یک فرد مشهور را جستجو کنیم تا با انبوهی از اطلاعات، پیرامون زندگی وی روبرو گردیم. این داده ها که از منابع مختلف تهیه و در عرصه ی فضای سایبری به اشتراک گذاشته می شود، چه بسا حاوی مطالبی باشد که فرد مورد نظر تمایلی به اطلاع دیگران از آن ندارد. این وضعیت می تواند برای هر فردی هرچند صاحب شهرت نباشد رخ دهد.

از این رو می توان گفت در جهانی که ما در آن ادامه ی حیات می دهیم، بسیاری غیر ممکن ها ممکن گردیده است. ما برای پرهیز از بروز چنین جرمی باید تا حد امکان زمینه های ارتکاب آن را از میان برداریم. به عنوان مثال داده های شخصی و خصوصی خود را حتی الامکان در فضاهای نا امن نگهداری نماییم. رایانه هایی که معمولاً به شبکه های اینترنت و اینترانت متصل هستند، به هیچ وجه محیط مناسبی برای نگهداری و حفاظت از اسرار خصوصی ما نیستند. گوشی های تلفن همراه، به لحاظ پیشرفت تکنولوژی روز به روز کوچک تر می شوند و قابلیت حمل و نتیجتاً سرقت این دستگاه ها بیشتر گردیده است. در حالی که به واسطه ی تجهیز این دستگاه ها به دوربین های قوی، بیشتر مردم ترجیح می دهند لحظات شیرین زندگی خانوادگی خود را به این وسیله ثبت کنند. بسیاری افراد، تصاویری که با این دستگاه ضبط گردیده است را بر روی حافظه های موجود در گوشی حمل می کنند. حال اگر این دستگاه مفقود یا سرقت شود، این اطلاعات که بی تردید دارای جنبه ی خصوصی و نتیجتاً افشای آن موجب هتک عرض و آبروی افراد می گردد، چه بسا در دسترس افراد سودجو و فرصت طلبی قرار گیرد که آن را وسیله ای برای اخاذی، هتک عرض و آبرو و یا حتی اجبار

افراد به روابط نامشروع و مانند آن قرار دهند. لذا خودداری از نگهداری اطلاعات خصوصی در حافظه های قابل حمل نیز از دیگر راهکارهای مقابله با بزه دیدگی است.

از سویی افرادی که برای تهیه ی فیلم یا عکس از مراسم خانوادگی به خدمت گرفته می شوند یا افرادی که در مراسم خصوصی دیگران به عناوین مختلف حضور دارند، باید کاملاً مورد اعتماد باشند. چه بسا کسی که برای عکس برداری از مراسم عروسی یک فرد در این مراسم حضور یافته است، تصاویر تهیه شده را تکثیر نموده و در اختیار دیگران قرار دهد. این تصاویر امروزه با استفاده از نرم افزارهای کامپیوتری به سادگی قابلیت تغییر و تحریف را دارند و ممکن است با تحریف یک عکس خانوادگی شرافت و آبروی شخص در معرض خطر قرار گیرد. همچنین کسانی که به عنوان دوست یا هر عنوان دیگر در مراسم خانوادگی حضور دارند می توانند به کمک یک دستگاه تلفن همراه از تمامی لحظات مهمانی یا مراسم دوستانه فیلمبرداری کرده و آن را وسیله ای برای تهدید و امثال آن قرار دهند. لذا باید از حضور افرادی که نسبت به آن ها شناخت کافی وجود ندارد، در میهمانی های خانوادگی ممانعت نمود یا مطمئن گردید که وسیله ای به همراه ندارند که بتوان با آن فیلم یا عکس تهیه نمود.

دیگر موضوعی که می تواند افراد را در این جرم بزه دیده نماید، قرار دادن وسایل الکترونیکی دارای حافظه در اختیار اشخاصی است که به عنوان تعمیر یا ارتقای عملکرد دستگاه، به داده های موجود در آن دسترسی پیدا خواهند نمود. حال چنانچه این افراد کاملاً مورد اطمینان نباشند، هر آینه احتمال افشای اسرار یا تصاویر خصوصی یا خانوادگی که در این دستگاه نگهداری شده است وجود خواهد داشت.

مورد دیگر که اخیراً به شدت گسترش یافته وجود برخی وب سایت های اینترنتی است که به عنوان شبکه های اجتماعی امکان بارگذاری حجم عظیمی از اطلاعات را به رایگان در فضای مجازی برای افراد فراهم آورده اند. متأسفانه بسیاری افراد، ناآگاهانه و به صرف اینکه به برخی از اعضای این وب سایت ها به عنوان دوست اعتماد می کنند، بسیاری از اطلاعات خصوصی خود را در این محیط قرار می دهند. به این تصور که تنها افرادی که ایشان دوستی با آن ها را در وب سایت پذیرفته اند، بدان دسترسی دارند. غافل از این که بسیاری از افراد هستند که با اطلاع از تکنیک های نفوذ و دست یابی قادر اند به این اطلاعات رسیده و چه بسا

از آن سوء استفاده نمایند. از این رو وب سایت های دوست یابی و شبکه های اجتماعی به هیچ وجه نباید محلی برای قرار دادن اطلاعات خصوصی افراد، برگزیده شوند.

## بند دوم - تدارک برنامه هایی جهت فرهنگ سازی

آنچه در این بند مورد اشاره خواهد بود، بیشتر جنبه ی جرم شناسانه دارد. در مباحث جرم شناسی از دو نوع پیش گیری اولیه و ثانویه سخن به میان می آید. منظور از پیش گیری اولیه تدارک تدابیری است تا از ارتکاب بزه در مرتبه ی اول ممانعت به عمل آید. منظور از پیش گیری ثانویه نیز تمهید ضوابط و امکاناتی است تا از تکرار بزه جلوگیری گردد. آنچه ما در اینجا بیان می کنیم بر اساس همین تقسیم بندی می باشد.

شاید بتوان گفت همچنان که در پزشکی اعتقاد بر این است که پیش گیری بهتر از درمان است، در حقوق کیفری نیز شرایط به همین منوال می باشد. لذا بهترین تدبیر آن است که در فرایند جامعه پذیری افراد، آن ها را در معرض هنجارها و ارزش هایی قرار دهیم که به ویژه در خصوص بزه مورد بحث ما اعضای اجتماع را افرادی بسازد که بیشترین اهمیت و توجه را به موضوع حریم خصوصی و شرافت و آبروی خود و دیگران داشته باشند. هرگاه تک تک افراد عرض و آبرو و حیثیت خود و دیگران را به عنوان امری مقدس و مستلزم احترام بشناسند، بی شک موارد تجاوز و هتک این مهم به میزان قابل توجهی کاهش خواهد یافت. می توان گفت هیچ عامل بازدارنده ای به اندازه ی «خود کنترلی» نمی تواند در کاهش نرخ بزه و بزهکاری در هر جامعه ای مؤثر باشد. این فرایند جامعه پذیری و هنجارمند سازی افراد از نخستین مراحل رشد و تکوین شخصیت اجتماعی آن ها آغاز شده و تا دوران جوانی ادامه خواهد یافت. از این رو در تمام مراحل آموزشی و فرهنگی اعم از رسمی - مانند آموزش و پرورش - و غیر رسمی - رسانه ها و ...- باید به ترویج فرهنگ احترام به انسانیت و شرافت و آزادگی انسان پرداخته شود. همچنین ضمن آشنایی افراد با قابلیت ها و امکانات بی شمار محیط مجازی، بر استفاده ی سالم و مفید از این محیط تأکید گردد.

از سوی دیگر، به عنوان راهکاری در قلمرو پیش گیری ثانویه باید به ظرفیت های قانونی که در اختیار دادرسان می باشد توجه داشت. به عنوان مثال ماده ی ۱۹ قانون مجازات

اسلامی در مقام قانون مند کردن مجازات های تکمیلی این اختیار را به قاضی داده است که مجرم را علاوه بر مجازات اصلی برای مدتی از حقوق اجتماعی محروم کند. شایسته است ایجاد مراکز فرهنگی آموزشی و الزام مجرمین به شرکت در برنامه های آموزشی این مراکز نیز به عنوان یک مجازات ترمیمی در قانون پیش بینی شود. در این صورت قاضی می تواند بزهکاران را به منظور باز اجتماعی شدن و انطباق مجدد با هنجارهای شناخته شده ی جامعه مکلف نماید تا در کلاس های آموزشی که به عنوان مثال اختصاص به شناسایی قابلیت های محیط مجازی و بهره گیری از فرصت های ایجاد شده در پرتو شکل گیری فضای سایبری دارد، حضور یابند تا از طریق کسب مهارت استفاده ی بهینه از امکانات محیط مجازی امکان باز اجتماعی شدن آن ها و جلوگیری از ارتکاب مجدد جرایم سایبری و به طور خاص بزه مورد بحث ما فراهم گردد.

## نتیجه گیری

تردیدی نیست که هر نوشتاری در غایت خود در پی افاده ی مفاهیم و دست یابی به نکاتی است که تا پیش از این چه بسا از نظرگاه صاحب نظران پنهان مانده است. نوشتار حاضر نیز که به بررسی بزه هتک حیثیت از طریق افشای سر در محیط مجازی اختصاص یافت، طی فصول و گفتارهایی چند کوشید تا آنچه که برای شناسایی ماهیت و اجزای متشکله ی این جرم ضرورت دارد را به تفصیل برشمرد و در عین حال به بیان نقاط قوت و ضعف قوانین جاری مملکتی در جرم انگاری این بزه اشاره نماید. بنابر آنچه بیان گردید ماحصل تمامی بحث های مطروحه در این پژوهش را در چند مورد به اختصار بیان می نمایم:

۱- جهان امروز را به حق باید آمیزه ای از عینیت و مجاز دانست. فضای سایبری که در قرن ۲۰ پا به عرصه ی وجود نهاد، با چنان سرعتی رو به گسترش نهاده است که اکنون تمام اجزای حیات بشر از ساده ترین امور روزمره تا پیچیده ترین فعالیت های علمی وابستگی مستقیم یا غیر مستقیم با رایانه و محیط سایبری دارد. لذا امروزه ما در آن واحد در دو عرصه ادامه ی حیات می دهیم و این خود گواه اهمیت محیط مجازی و جایگاه آن در زندگی انسان در قرن ۲۱ است.

۲- این عرصه ی وسیع که باعث توسعه ی حیات اجتماعی از ابعاد گوناگون شده است، دارای قابلیت هایی است که زندگی انسان امروز را بسیار متفاوت از گذشته نموده است. این قابلیت های خارق العاده نشأت گرفته از ویژگی خاص محیط مجازی است و آن عبارت است از عدم محدودیت زمان و مکان. همین ویژگی که قابلیت های مثبت فراوانی به فضای سایبر بخشیده است، خود زمینه را برای بروز مشکلاتی فراهم نموده است. عدم تقید به زمان و مکان امکان ایجاد هویت های مجعول را به شکل گسترده ای فراهم ساخته و این امر زمینه ی مناسبی برای گسترش انحرافات و بزهکاری در محیط مجازی ایجاد نموده است.

۳- از آنجایی که محیط مجازی نیز مانند محیط عینی عرصه ای برای حضور و فعالیت انسان است، ضروری است تا بستری امن و حفاظت شده برای زندگی و فعالیت در این فضا ایجاد گردد. لازمه ی این امر پیش بینی قوانین و مقرراتی است تا بر رفتار افراد در این محیط حکم فرما شود و از ارزش های انسانی پاسداری نماید. یکی از این ارزش ها، حق انسان بر حریم خصوصی و اسرار شخصی و خانوادگی است.

۴- این حق یکی از مهم ترین حقوقی بشری است که در تمام ادیان الهی از دیرباز مورد تأکید بوده است. گذشته از آن در سده ی اخیر که مسأله ی حقوق بشر بیش از پیش مطمح نظر علما و از جمله حقوق دانان قرار گرفته است، در تمامی اسناد حقوقی بین المللی نیز این موضوع مورد توجه بوده و مکرراً توصیه و تأکید بر این بوده که حریم خصوصی افراد بازچیه ی اغراض سیاسی دولت ها نگردد.

۵- یکی از مصادیق حق انسان بر حریم خصوصی، مصون بودن او از دسترسی دیگران بر اسرار خصوصی و خانوادگی است. سر همان گونه که از معنای لغوی آن برمی آید، عبارت است از چیزی که باید از دیگری پنهان بماند. این حق بشری در نظام های حقوقی مختلف و از جمله کشور ما نیز کم و بیش به رسمیت شناخته شده است. در نظام کیفری سنتی ما تنها برای افشای اسرار حرفه ای جرم انگاری صورت گرفته بود اما به تدریج و با تدوین قوانین در خصوص محیط مجازی، حمایت از این ارزش در محیط مجازی و آن هم نه فقط در مورد اسرار حرفه ای مورد عنایت مقنن قرار گرفت.

۶- پیش بینی بزه افشای سر در محیط مجازی، در کنار برخی عناوین مجرمانه مانند دسترسی غیر مجاز، جاسوسی رایانه ای، نشر اکاذیب و افتراء، به لحاظ این که این قبیل جرایم دارای نقاط مشترکی هستند ممکن است سبب خلط مبحث و نتیجتاً دشواری در تعیین مصداق گردد. به عنوان مثال موضوع جرم در افشای سر و دسترسی غیر مجاز امور پنهان و به اصطلاح اسرار است. اما با کمی مذاقه در هر یک از عناوین مجرمانه روشن می گردد که علیرغم وجود جهات اشتراک در این جرایم، هریک دارای نقاط افتراق فراوانی با یکدیگر هستند که برای تشخیص مصداق مجرمانه باید به جهات افتراق آن ها عنایت داشت که به تفصیل در این نوشتار به آن پرداخته شده است.

۷- با روشن شدن قلمرو بحث، ضمن ورود به جزئیات مربوط به بزه افشای سر در محیط مجازی، در بررسی رکن قانونی این جرم، مشخص گردید که از آغاز قانون گذاری در خصوص جرایم رایانه ای و سایبری به شکل جسته و گریخته و به اقتضای موقعیت و شرایط مقنن به این جرم نظر داشته است. همین امر سبب گردیده که قوانین متعددی در اختیار ما باشد که در هر کدام حکمی خاص و گاهی عام در این خصوص دیده می شود. این پراکنده گویی و عدم جامعیت قوانین را می توان بزرگ ترین ایراد موجود در حقوق کیفری ایران دانست.

۸- لاجرم در جمع بین قوانین مختلف به اصول حقوق کیفری متوسل شده و با لحاظ تقدم و تأخر تصویب قوانین کیفری و همچنین با رعایت قاعده ی تفسیر قانون به نفع متهم و نیز احراز غرض قانون گذار به این نتیجه رسیدیم که تصویب برخی قوانین که بسیار سختگیرانه با این بزه روبرو شده اند تحت تأثیر شرایط حاکم بر جامعه در زمان تصویب بوده و لذا پس از تصویب قانون جرایم رایانه ای در سال ۱۳۸۸ باید تا حد امکان به این قانون استناد گردد مگر در مواردی که قانون فوق قابلیت استناد را به لحاظ سکوت در خصوص مورد نداشته باشد. البته این دوگانگی گاه مشکل ساز می شود و ممکن است تناسب مجازات با شدت آثار مخرب جرم رعایت نگردد. لذا مقنن کیفری باید در این خصوص صراحتاً تصمیم گیری نموده و با رفع ابهام و نقص از قانون جرایم رایانه ای، راه را بر هر تفسیر غیر متعارف ببندد.

۹- در بحث از رکن مادی، مشخص گردید که مرتکب این بزه هر شخصی اعم از حقیقی یا حقوقی می تواند باشد. رفتار مجرمانه ی این بزه عبارت است از انتشار یا در دسترس دیگران قرار دادن موضوع جرم که همان فیلم خصوصی و خانوادگی متعلق به دیگری یا اسرار خصوصی دیگری است. برای تحقق این جرم وجود شرایطی نیز ضروری است که مهم ترین آن عدم رضایت کسی است که اسرار متعلق به اوست. البته وسیله نیز در ارتکاب این جرم موضوعیت دارد چراکه این جرم یک بزه رایانه ای است. این جرم به تصریح قانون مقید به حصول نتیجه است و بدون تحقق نتیجه امکان مجازات مرتکب به استناد قانون جرایم رایانه ای وجود نخواهد داشت.

۱۰- رکن روانی این بزه نیز مشتمل بر اجزایی است که از جمله باید به علم مرتکب -

حکمی و موضوعی -، عمد عام و عمد خاص اشاره نمود. از آنجا که این جرم مقید به نتیجه



است، مرتکب باید علاوه بر این که در ارتکاب رفتار عامد و قاصد باشد، باید تحقق نتیجه ی مجرمانه - که همان هتک حیثیت و یا ورود ضرر بر بزه دیده است - را اراده نماید. بدیهی است در این بین، وجود عوامل زایل کننده ی اراده، رکن روانی جرم را متزلزل خواهد نمود.

۱۱- رفتار اجتماع در قبال پدیده ی مجرمانه عبارت است از مجازات و پیش گیری از ارتکاب رفتار انحراف آمیز. در خصوص مجازات مقرر برای این بزه، همچنان که گفته شد چون مرتکب ممکن است شخص حقیقی یا حقوقی باشد، نوع مجازات نیز برای این دو شخصیت در قانون جرایم رایانه ای متناسب گردیده است. از سویی پیش بینی مجازات های تبعی و تکمیلی در کنار مجازات اصلی می تواند زمینه را برای هرچه بیشتر باز اجتماعی شدن مرتکبین فراهم آورد. گرچه این قبیل مجازات ها مستقیماً در قانون جرایم رایانه ای مقرر نگردیده است اما از لابلای مقررات موجود می توان تدابیری برای این منظور اندیشید. همچنین پیش بینی تفصیلی نحوه ی تشدید مجازات در خصوص اشخاصی که مرتکب تکرار این بزه می گردند در قانون جرایم رایانه ای، از نقاط قوت این قانون می باشد.

۱۲- دیگر واکنش اجتماعی را که همان تدابیر غیر کیفری است نیز در قانون جرایم رایانه ای می توان دنبال کرد. این امر که با عنوان فیلتر نمودن محتوای مجرمانه مطرح می گردد، اگرچه در خصوص بزه مورد بحث ما به عنوان یک تکلیف برای ارائه دهندگان خدمات اینترنتی تعیین نشده است اما با دقت در قانون مشخص می گردد که با درخواست شاکی خصوصی و دستور دادرسی رسیدگی کننده به پرونده امکان اتخاذ این راهکار وجود دارد تا از دسترسی افراد غیر مرتبط به محتوای خصوصی و خانوادگی و اسرار متعلق به بزه دیده ممانعت به عمل آید.

۱۳- نهایتاً ورای بررسی ارکان و اجزای بزه افشای سر در محیط مجازی، به این نتیجه رسیدیم که هر فرد باید بکوشد تا از بزه دیده شدن در امان باشد. تدابیر قانونی برای حفاظت از افراد در محیط مجازی به هیچ وجه کافی نیست و این خود افراد هستند که باید حتی المقدور زمینه ی ارتکاب جرم را برای منحرفان اجتماعی فراهم نسازند تا در سایه ی اتخاذ تدابیر بهتر و البته وضع قوانین بازدارنده تر، شاهد جامعه ای نه عاری از بزه - که مسلماً قابل تحقق نیست - بلکه با نرخ ارتکاب جرایم کمتر باشیم.



## فهرست منابع و مآخذ

### الف - کتب

- ۱- قرآن کریم.
- ۲- اردبیلی، محمد، حقوق جزای عمومی، جلد ۱ و ۲، میزان، تهران، ۱۳۸۱ و ۱۳۸۲.
- ۳- اولریش، زیبر، جرایم رایانه ای، ترجمه ی محمدعلی نوری و دیگران، گنج دانش، تهران، ۱۳۹۰.
- ۴- آقایی نیا، حسین، حقوق کیفری اختصاصی، جرایم علیه اشخاص، (شخصیت معنوی)، بنیاد حقوقی میزان، تهران، ۱۳۸۶.
- ۵- باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، انتشارات بهنامی، تهران، ۱۳۸۳.
- ۶- بای، حسین علی و بابک پورقهرمانی، بررسی فقهی حقوقی جرایم رایانه ای، پژوهشگاه علوم و فرهنگ اسلامی، قم، ۱۳۸۸.
- ۷- پاد، ابراهیم، حقوق کیفری اختصاصی، جلد ۱، دانشگاه تهران، ۱۳۷۴.
- ۸- جاویدنیا، جواد، جرایم تجارت الکترونیکی، نشر خورسندی، تهران، ۱۳۸۷.
- ۹- جعفری لنگرودی، محمدجعفر، ترمینولوژی حقوق، گنج دانش، تهران، ۱۳۷۲.
- ۱۰- جلالی فراهانی، امیرحسین، درآمدی بر آیین دادرسی کیفری جرایم سایبری، معاونت حقوقی و توسعه ی قضایی قوه ی قضائیه، مرکز مطالعات توسعه ی قضایی، خورسندی، تهران، ۱۳۸۸.
- ۱۱- جوانمرد، بهروز، تسامح صفر، سیاست کیفری سخت گیرانه در قبال جرایم خرد، بنیاد حقوقی میزان، تهران، ۱۳۸۸.
- ۱۲- خویینی، غفور، حقوق شهروندی و توسعه ی پایدار، فرهنگ صبا، تهران، ۱۳۸۶.

- ۱۳- دزیانی، محمدحسن، جرایم کامپیوتری، جلد ۱، دبیرخانه ی شورای عالی انفورماتیک، تهران، ۱۳۷۶.
- ۱۴- دهخدا، لغت نامه.
- ۱۵- دیوید، جی، آیکا و همکاران، راهکارهای پیشگیری و مقابله با جرایم رایانه ای، ترجمه ی اکبر استرکی و دیگران، دانشگاه علوم انتظامی، تهران، ۱۳۸۳.
- ۱۶- شامبیاتی، هوشنگ، حقوق کیفری اختصاصی، جلد ۳، جرایم بر ضد مصالح عمومی کشور، مجد، تهران، ۱۳۸۲.
- ۱۷- شیرزاد، کامران، جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، نشر بهینه ی فراگیر، تهران، ۱۳۸۸.
- ۱۸- صادقی، محمدهادی، حقوق جزای اختصاصی، جرایم علیه اشخاص، صدمات جسمانی، میزان، تهران، ۱۳۸۵.
- ۱۹- ضیایی پرور، حمید، جنگ نرم ویژه ی جنگ رایانه ای (۱)، مؤسسه ی فرهنگی مطالعات و تحقیقات بین المللی ابرار، تهران، ۱۳۸۸.
- ۲۰- عالی پور، حسن، حقوق کیفری فناوری اطلاعات، معاونت حقوقی و توسعه ی قضایی قوه ی قضائیه، مرکز مطالعات توسعه ی قضایی، خورسندی، تهران، ۱۳۸۹.
- ۲۱- کاتوزیان، ناصر، حقوق مدنی، وقایع حقوقی، شرکت سهامی انتشار، تهران، ۱۳۸۵.
- ۲۲- ----- ، ----- ، مقدمه ی علم حقوق، شرکت سهامی انتشار، تهران، ۱۳۸۳.
- ۲۳- میرمحمد صادقی، حسین، حقوق کیفری اختصاصی، جرایم علیه امنیت و آسایش عمومی، نشر میزان، تهران، ۱۳۸۶.
- ۲۴- ----- ، ----- ، حقوق کیفری اختصاصی، جرایم علیه اموال و مالکیت، میزان، تهران، ۱۳۸۷.
- ۲۵- نوریها، رضا، زمینه ی حقوق جزای عمومی، نشر دادآفرین، تهران، ۱۳۸۳.
- ۲۶- ولیدی، محمدصالح، حقوق جزای اختصاصی، جرایم علیه اشخاص، جلد ۲، مؤسسه ی انتشارات امیرکبیر، تهران، ۱۳۷۸.
- ۲۷- ----- ، ----- ، جرایم علیه عفت و اخلاق عمومی و تکالیف خانوادگی، انتشارات امیرکبیر، تهران، ۱۳۸۳.

## ب- مقالات

- ۱- ترکی، غلامعباس، نگرش علمی و کاربردی به قانون جرایم رایانه ای، قسمت اول، دادرسی، ماهنامه ی شماره ی ۷۷، سال سیزدهم، آذر و دی ۸۸.
- ۲- ----- ، ----- ، نگرش علمی و کاربردی به قانون جرایم رایانه ای ، قسمت دوم، دادرسی، ماهنامه ی شماره ی ۷۸، سال سیزدهم، بهمن و اسفند ۱۳۸۸.
- ۳- ----- ، ----- ، نگرش علمی کاربردی به قانون جرایم رایانه ای، قسمت سوم، ماهنامه ی دادرسی، شماره ی ۷۹، سال چهاردهم، فروردین و اردیبهشت ۱۳۸۹.
- ۴- ----- ، ----- ، نگرش علمی کاربردی به قانون جرایم رایانه ای ، قسمت چهارم، ماهنامه ی دادرسی، شماره ی ۸۰، سال چهاردهم، خرداد و تیر ۱۳۸۹.
- ۵- توکلی، سعید، افترا و توهین در حقوق کیفری ایران، ماهنامه ی شماره ی ۳۹، سال هفتم، مرداد و شهریور ۱۳۸۲.
- ۶- جلالی فراهانی، امیرحسین، پیشگیری وضعی از جرایم سایبر، در پرتو موازین حقوق بشر، فقه و حقوق، سال دوم، شماره ی ۵۲، پاییز ۱۳۸۴.
- ۷- ----- ، ----- ، مزیت ها و محدودیت های فضای سایبر در حوزه های آزادی بیان، آزادی اطلاعات و حریم خصوصی، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی حقوقی، شماره ی ۵۹، تابستان ۱۳۸۶.
- ۸- حسن بیگی، ابراهیم، توسعه ی شبکه ی ملی دیتا، چالش های فراروی و تهدیدهای متوجه امنیت ملی، فصل نامه ی مطالعات مدیریت، شماره ی ۴۸.
- ۹- دزیانی، محمدحسن، جرایم سایبری، ماهنامه ی قضاوت، شماره ی ۳۰، فروردین و اردیبهشت ۱۳۸۴.
- ۱۰- ----- ، ----- ، مقدمه ای بر سیاست جنایی ایران در باب جرایم سایبری، قضاوت، ماهنامه ی شماره ی ۳۸، خرداد و تیر ۱۳۸۵.
- ۱۱- ----- ، ----- ، مقدمه ای بر سیاست جنایی جرایم سایبری، ماهنامه ی قضاوت، شماره ی ۴۰، مهر ۱۳۸۵.

- ۱۲- ----- ، ----- ، نکات تحلیلی ایمیل از زاویه ی جزایی، نگاهی به جرایم سایبری، ماهنامه ی قضاوت، شماره ی ۳۱، خرداد ۱۳۸۴.
- ۱۳- رحمدل، منصور، حق انسان بر حریم خصوصی، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی دانشکده ی حقوق و علوم سیاسی، شماره ی ۷۰، زمستان ۸۴.
- ۱۴- سعیدی، رحمان، جامعه ی اطلاعاتی جالش ها و فرصت ها، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی حقوقی، سال دهم، شماره ی ۴۲.
- ۱۵- سعیدی نژاد، یاسمن، جرم انگاری در فضای مجازی،، تعالی حقوق، شماره ی ۲.
- ۱۶- سوادکوهی فر، سام، تحلیلی بر مقررات جزایی IT در ایران، مرکز تحقیقات کامپیوتری علوم اسلامی، دادرسی، ماهنامه ی شماره ی ۴۵، سال هشتم، مرداد و شهریور ۱۳۸۳.
- ۱۷- شفایی، عبد ا...، بازشناسی نهاد حریم (۱)، مرکز تحقیقات کامپیوتری علوم اسلامی، فقه، سال یازدهم، شماره ی ۴۱.
- ۱۸- شقاقی، بیژن، اخلاق حرفه ای حفظ اسرار، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی کانون وکلای دادگستری، شماره ی ۱۸۰ و ۱۸۱، بهار و تابستان ۱۳۸۲.
- ۱۹- قماش، سعید، بررسی جرم افشای اسرار حرفه ای (۱)، دادرسی، ماهنامه ی شماره ی ۵۸، سال دهم، مهر و آبان ۱۳۸۵.
- ۲۰- مسعودی، امید، امنیت اطلاعات در فضای سایبر، کتاب ماه، کلیات، دی ۱۳۸۳.
- ۲۱- مهرپور، حسین، آزادی فردی و حدود آن در حکومت اسلامی، مرکز تحقیقات کامپیوتری علوم اسلامی، مجله ی حقوقی و قضایی دادگستری، شماره ی ۵، پاییز ۱۳۷۱.
- ۲۲- مهریزی، مهدی، دولت دینی و حریم خصوصی حکومت اسلامی، مرکز تحقیقات کامپیوتری علوم اسلامی، سال چهارم، شماره ی ۲.
- ۲۳- نمک دوست تهرانی، حسن، اخلاق حرفه ای حریم خصوصی و حق دسترسی به اطلاعات، مرکز تحقیقات کامپیوتری علوم اسلامی، رسانه، سال هفدهم، شماره ی ۲.
- ۲۴- یزدانی زنوز، هرمز، حریم خصوصی در فضای سایبر، حقوق فناوری اطلاعات و ارتباطات، (مجموعه ی مقالات)، معاونت توسعه ی قضایی قوه ی قضائیه، مرکز مطالعات توسعه

ی قضایی، بزرگداشت استاد حسن دزینی، گردآوری امیرحسین جلالی فراهانی، انتشارات روزنامه ی رسمی، تهران، ۱۳۸۸.

### ج- پایان نامه و جزوات درسی

۱- آل محمد، فاطمه، سیاست جنایی ایران در قبال جرایم رایانه ای، پایان نامه ی کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده ی حقوق و علوم سیاسی، دانشگاه شیراز، فروردین ۱۳۹۰.

۲- منصورآبادی، عباس، جزوه ی درس حقوق جزای عمومی ۲، دانشکده ی حقوق و علوم سیاسی، دانشگاه شیراز، ۱۳۸۵.

### د- مجموعه ی قوانین

۱- مجموعه ی قانون مجازات اسلامی، ریاست جمهوری، معاونت پژوهش تدوین و تنقیح قوانین و مقررات، عباس علی رحیمی اصفهانی و همکاران.

۲- مجموعه ی قوانین و مقررات آیین دادرسی کیفری، نشر دیدار، تدوین جهانگیر منصور.

۳- مجموعه ی قانون تجارت، مجد، به کوشش حسین ساعتچی یزدی.

### ه- سایت های اینترنتی مورد استفاده

- ۱- <http://www.noormags.ir>
- ۲- <http://www.hawzih.net>
- ۳- <http://searchwebservices.techtarget.com/definition>
- ۴- <http://www.atis.org><sup>۱</sup>
- ۵- <http://www.english.uga.edu>
- ۶- <http://www.unhchr.ch/html/menu۳>
- ۷- <http://www.unhchr.ch/html/menu۳>
- ۸- <http://www.unhchr.ch/html/menu۳>

## ABSTRACT

### AFFRONT TO THE DIGNITY OF PERSONS BY DISCLOSING THE SECRETS IN CYBER SPACE

By:

**Farshad Ebrahimi**

Although imagining human life out of society seems impossible, every person undoubtedly also has another aspect of individual life. In this dimension everyone has some redlines to which cannot tolerate other's achievement. Personal secrets & privacy are among these forbidden limitations. Also, in present modern criminal law, invading these affairs has been paid attention by criminal legislative & disclosing private secrets has been criminalized as one of the crimes against people's dignity.

On one hand, the considerable growth of technology and its use in all aspects of human life, has made the possibility to achieve people's privacy and its publication and exposition exist. Therefore in addition to criminalizing deviations that may be committed by the computers and through Cyber Space, preceding the disclosing secrets in Cyber Space has also been considered by criminal legislative of Iran. It can be said that because of the characteristics of digital and cyber space, the domain of committing this crime by means of computer is wider than its traditional commitment.

In this writing after a brief familiarity with cyber space, we have discussed the value & situation of privacy, the concept of secrets & its significance during the history & in different religions. In addition, besides comparing the crime of disclosing the secrets with other crimes, & by recognizing the elements of this referred crime, the whole elements of this crime has been studied exactly & the necessary conditions for committing the crime has been counted widely. Finally, we have mentioned the reactions considered by criminal legislative & the strong & weak points of legislation in this case & shown some methods for preventing this crime from being committed.

**Key Words:** Cyber Space, Privacy, Disclose, Affront to Dignity, Publication, Achievement, Secrets





Shiraz University  
Faculty of Law & Politics

M.A. Thesis  
In Criminal Law & Criminology  
**AFFRONTS TO THE DIGNITY OF PERSONS BY DISCLOSING THE  
SECRETS IN CYBER SPACE**

BY  
FARSHAD EBRAHIMI

Supervised by  
Dr. SHAHRAM EBRAHIMI

September ۲۰۱۲