Culminatin of Law Quarterly
14nd Year, No.1, Spring 2023
http://dx.doi.org/10.22034/thdad.2023.538659.1946

Scope and criteria for recognizing cyber security crimes

Farokh Hadaie[1], Hassan Alipour*[2], Sayed Mahmood Mirkhalili[3]

1. Doctoral student, Department of Criminal Law and Criminology, Qom branch, Islamic Azad University, Qom, Iran
2. Assistant Professor, Department of Criminal Law and Criminology, Farabi Campus, University of Tehran, Qom, Iran.
3. Associate Professor, Department of Criminal Law and Criminology, Farabi Campus, University of Tehran, Qom, Iran.

Abstract

Today, there is no less hesitation in accepting cyber security crimes as a new type of cyber crimes. However, views and opinions on recognizing the scope and criteria of cyber security crimes are diverse and different based on this necessity and due to the importance of space. Cyber has opportunities and threats, and the prominent role of cyber power in the position of countries in the global power hierarchy. The main challenge is to know the scope and criteria of cyber security crimes, which has caused controversy, so that different divisions the types and examples of security crimes have been presented. It has been stated and it is possible to commit it, including the Law on Punishment of Crimes of the Armed Forces, which has also examined the procedure for investigating these crimes. Showed that for a comprehensive and accurate understanding of cyber security crimes should be intercepted an adaptive-comparative finding was used and a framework based on interdisciplinary perspective and integration of all approaches was considered. Accordingly, an alternative analytical framework based on the linkage of these approaches is presented.

Keywords: Cyberspace, National Security, Security crimes, Political crimes.

Article Type:
Original Research

Pages: 229-258

Received: 2021 September 10

Revised: 2021 November 8

Accepted: 2022 March 28

*. Corresponding Author: Hassan.alipour@ut.ac.ir

فصلنامه تعالی حقوق
سال چهاردهم، شماره ۱، بهار ۱۴۰۲
http://dx.doi.org/10.22034/thdad.2023.538659.1946

محدوده و ملاک شناخت جرایم امنیتی سایبری[۱]

فرخ هدائی[۱]، حسن عالی‌پور*[۲]، سیدمحمود میرخلیلی[۳]

۱. دانشجوی دکتری گروه حقوق کیفری و جرم شناسی، دانشکده علوم انسانی، واحد قم، دانشگاه آزاد اسلامی،قم، ایران.

۲. استادیار گروه حقوق کیفری و جرم شناسی، پردیس فارابی دانشگاه تهران،قم، ایران.

۳. دانشیار گروه حقوق کیفری وجرم شناسی، پردیس فارابی دانشگاه تهران، قم،ایران.

نوع مقاله: علمی پژوهشی

صفحات: ۲۲۹-۲۵۸

تاریخ دریافت: ۱۴۰۰/۰۶/۱۹

تاریخ بازنگری: ۱۴۰۰/۰۸/۱۷

تاریخ پذیرش: ۱۴۰۱/۰۱/۰۸

چکیده

امروزه در پذیرش جرایم امنیتی سایبری به عنوان نوع جدیدی از جرایم سایبری کمتر تردیدی وجود ندارد.با وجود این،دیدگاه‌ها در مورد شناخت محدوده و ملاک جرایم امنیتی سایبری متفاوت است،بر اساس این ضرورت و به دلیل اهمیتی که فضای سایبر در بعد فرصت‌ها و تهدیدات دارد،تقسیم بندی‌های مختلفی از انواع جرایم امنیتی ارائه شده است. پژوهش حاضر با هدف شناخت محدوده جرایم امنیتی سایبری در قوانین مختلف، همچنین بررسی مقررات حاکم برآنها و بررسی مراجع رسیدگی کننده صورت گرفته است که از لحاظ هدف کاربردی و از نظر ماهیت،توصیفی-تحلیلی است.روش جمع آوری اطلاعات به شیوۀ کتابخانه‌ای از کتب معتبر و با ابزار فیش‌برداری بوده است.یافته ها نشان داد برای شناخت جامع جرایم امنیتی سایبری باید از رهیافت تلفیقی-تطبیقی استفاده شود و چارچوبی مبتنی بر نگاه بین رشته‌ای را مدنظر قرار داد.بر همین اساس،چارچوب تحلیلی بدیلی مبتنی بر پیوند این رویکردها ارائه شده است.نتایج کاربردی این پژوهش نشان داد که امکان تحقق بعضی از مصادیق جرایم امنیتی از طریق رایانه وجود دارد.همچنین یافته های تحقیق حاضر در حل و فصل دعاوی کیفری در مراجع قضایی،کاربردی است و بدلیل تشتت آراء در این زمینه تشکیل دادگاه ویژه جرایم امنیتی سایبری گره‌گشاست.

واژگان کلیدی: فضای سایبر، امنیت ملی، جرایم امنیتی، جرایم سیاسی.

---

۱. برگرفته از رساله دکتری رشتۀ حقوق کیفری و جرم شناسی دانشگاه آزاد اسلامی واحد قم با عنوان«پیشگیری از جرایم امنیتی سایبری

*. نویسنده مسئول: Hassan.alipour@ut.ac.ir

درآمد

جرایـــم امنیتی،به دلیل ویژگی‌های خاص این فضـــا، موضوعات مبتلا به ایجاد نمـــوده که معمولا مخاطبین آن حاکمیت ملی می‌باشـــند.این امـــر وقتی حائز اهمیت بیشـــتری می‌شـــود که بدانیم برخی از این گونه جرایم که مربوط به امنیت ملی باشد قابلیت ارتکاب در بســـتر فضای ســـایبر را دارند. در مورد پدیـــده جرایم امنیتی که در فضای سایبر ارتکاب می‌یابد، تهدیدها حساس‌تر و حصار امنیت ملی شکننده‌تر می‌شود، زیرا فضای ســـایبر پدیده سطحی نیست تا به راحتی در مسیر موافق با امنیت ملی قرار گیـــرد. هدف کلی در این پژوهش شـــناخت محدوده جرایم امنیتی ســـایبری و تبیین سازوکارهای حقوقی حاکم بر ملاک های تحقق آن است.اهداف جزئی نیز بررسی نظری جرایم امنیتی و تحلیل فهرست مصادیق محتوای مجرمانه می‌باشد. فناوری‌های جدید همـــواره مورد توجه مجرمین بوده، زیرا تأثیر به ســـزایی در افزایش تهدیدات اثربخش دارنـــد. دلیل این امر از یک طـــرف مخاطره آمیز بودن حیطه این گونه جرایم و ازطرف دیگر گستردگی فضای سایبر و داشتن مخاطبین بیشتراست و به همین دلیل است که وقتی یک جرم امنیتی توسط شخص واحدی در فضای سایبر رخ دهد، تبعات بیشتری خواهد داشت. سوال اساسی که در این پژوهش بررسی می‌شود، شناخت محدوده جرایم امنیتی ســـایبری است. به نظر می‌رســـد که در قانون جرایم رایانه‌ای، مصادیق جرایم امنیتی ســـایبری کمتر مورد توجه واقع شده اســـت و در میان حقوقدانان نیز تعاریف متعددی وجود دارد. همین اختلاف تفاســـیر مضیّق و موسّـــع در ذکر مصادیق، سبب ایجاد اِشـــکال در بیان رفتارهای منطبق با جرایم امنیتی نموده است. لذا ضرورت دارد دقت نظر اعمال تا خلأهای موجود شناســـایی و قانونگـــذار درصدد رفع آنها برآید .باید اذعان داشـــت که موضوع مقالهٔ حاضر مسئله‌ای دشـــوار و حساس، با توجه به موقعیت کنونی کشـــور است که در چند سال اخیر به موضوع قابل تأملی تبدیل شده که نیاز به پژوهش مضاعف در این زمینه احســـاس می‌شود. با این توضیح و به دلیل نوظهور بودن این نوع جرایم لازم اســـت محدوده شناخت آن به طور دقیق‌تر شناخته شود که این از لحاظ جرم‌شناسی و حقوق کیفری پژوهش‌های جدیدی را می‌طلبد. جدید بودن جرایم امنیتی به اعتبار جدید بودن بستری است که در آن ارتکاب می‌یابد ولی متفاوت بودن آن با خود جرایم امنیتی به معنای تمایز در برخی اجزای رکن مادی یا به تعبیر دقیق‌تر

رفتار سرزنش پذیر است. برعکس، جرایم امنیتی سایبری چهره نوین خود جرایم امنیتی اســـت؛ اما نه این که یکی از شکل‌های ساده آن باشد، بلکه این چهره نوین با ویژگی‌های منحصر به فردی همراه است. در تلاقی جرایم امنیتی و جرایم سایبری، جرایم امنیتی با ویژگی‌های جدید در فضای ســـایبر رخ می‌دهند. این ویژگی‌ها به طور مشخص از جرایم امنیتی ســـنتی فاصله می‌گیرند. از ســـوی دیگر طرز تلقی نسبت به اینکه آیا امنیت ملی باید با معیاری شناســـایی شود که تهدیدهای سایبری بر ضد آن کارساز باشند یا این که تهدیدهای ســـایبری اساساً بیشتر از آنکه به واقع علیه امنیت تهدیدآور باشند یک مقوله روزنامه‌ای است خود بحثی مبنایی است. بطور کلی هر جرمی تا حدودی امنیت را متزلزل می‌نمایـــد و با اضافه کردن برخی ویژگی‌ها رنگ امنیتی به خود گرفته؛ این تلقی مربوط به مفهوم عام جرایم امنیتی اســـت لیکن مفهوم خاص جرایم امنیتی مدنظر ماست و آن عبارت از این اســـت که برخی جرایم هستند که به صورت اخص ارزش‌هایی که شاخصه امنیت به شمار می‌روند و تنها بر ضد امنیت ملی ارتکاب می‌یابند، می‌باشد.

پیشینه پژوهش

درخصـــوص این پژوهش بـــه علت نوین بـــودن موضوع، نویســـندگان مقاله با محدودیـــت منابع روبرو بوده‌اند. با این وجود، می تـــوان به پژوهش‌های زیر که به نوعی مرتبط با تحقیق حاضر می‌باشند، به شرح زیر اشاره کرد. بر اساس نوشته های پروفسور الریش زیبر در کتاب پیدایش بین المللی حقوق کیفری اطلاعاتی اولین مواردی که جرم رایانه‌ای نامیده شـــده ابتدا در مطبوعات عمومی و در ادبیـــات علمی دهه ۱۹۶۰ ظاهر شـــد. نتایج پژوهش نشان داد این موارد شـــامل سوءاستفاده‌های ابتدایی از رایانه بود. از اواســـط ۱۹۷۰مطالعات تجربی در مورد جرم رایانه‌ای با اســـتفاده از متدهای تحقیقاتی رشـــتهٔ جرم شناسی انجام شد. این مطالعات ناظر به برخی از جرائم رایانه‌ای می‌شد. اما در همان حال تعداد زیادی موارد، غیرمکشـــوف مانده وخطرات زیادی نیز در بطن خود داشـــت. نان[1] و باخمـــن[2] در اثر اخیر خود(۲۰۱۰) به معرفی برخی از اشـــتباهات روش شناختی ویژه در زمینه تحقیقات جرم شناسی سایبری پرداخته‌اند. این محققین معتقدند

1. nan
2. bakhman

که مشـــکل نبود یک تعریف عمومی،مسائل مربوط به اندازه‌گیری و مشکلات تحقیقاتی باید به دســـت جرم شناسان سایبری آینده برطرف شـــوند. در بیشتر نوشته‌ها بزه‌های رایانه‌ای را بزه‌هایی دانســـته‌اند که در تحقق آنها رایانه و فضای ســـایبر یا نقش موضوع جرم دارد یا نقش وسیله جرم.در اولی یعنی موضوع جرم رایانه نقش منفعل و پذیرا دارد و موضوع رفتار مجرمانه قرار می‌گیرد، اما در وسیله جرم نقش فعال دارد و جرم با کمک آن ارتـــکاب می‌یابد.(عالی پور،۱۳۹۳: ۱۴۶-۱۴۵). ازحیث نقش رایانه در ارتکاب جرم، جرایم رایانه‌ای را می توان به سه دسته تقسیم کرد دسته اول جرایم هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند :مانند سرقت، دسته دوم جرایم هســـتند که در آنها رایانه به عنوان وســـیله ارتکاب جرم استفاده می‌شود و دسته سوم جرایم هســـتندکه می توان آنها را جرایم رایانه‌ای محض نامید. این نوع از جرایم کاملا با جرایم کلاســـیک تفاوت دارند و در دنیای مجازی به وقوع می پیوندند. اما آثار آنها در دنیای واقعی ظاهرمی شود مانند دسترسی غیرمجاز) جلالی فراهانی،۱۳۸۳:۹۰). بطور کلی با بررسی آراء مختلف ملاحظه می‌شود که تاکنون حقوقدانان و قانونگذاران تعریف و مصادیق واحدی از جرایم امنیتی ارائه نکرده و برخی این جرایم را به انواعی تقســـیم نموده‌اند مانند جرایم شبه امنیتی، عمومی (امنیتی)، جرایم امنیتی و حفاظتی، جرایم سیاســـی و امنیتی و جرایم علیه امنیت داخلی و خارجی یاجرایم علیه امنیت و جرایم مرتبط با امنیت (جعفری دولت آبادی ،۱۳۹۵: ۱۵۱). برخی دیگر امنیت ملی-سایبری را یکی از دســـته‌بندی‌های امنیت ملی دانسته که با معیارهای فضای سایبری سنجیده می‌شود(بهره مند و داودی،۱۳۹۷: ۲۹). اما این که محدوده جرایم امنیتی که در فضای ســـایبر اتفاق می‌افتد تا چه اندازه اســـت و جرایم امنیتی بـــا توجه به ماهیت حدی یا تعزیری بودن آنها دارای اقســـام حدی یا تعزیری است می تواند تحقیق حاضر را با سایر تحقیقات اجرا شده متمایز سازد.

روش تحقیق

پژوهـــش حاضرازلحاظ نوع در زمـــره تحقیقات کاربردی جـــای می‌گیرد، زیرا بکارگیری نتایج این تحقیق می‌تواند نقش مؤثری در شـــناخت محدوده جرائم امنیتی سایبری کشور داشته باشد. در تنظـیم و گردآوری اطلاعات و داده‌ها از روش مطالعات

کتابخانه‌ای و با استفاده از کتاب‌های معتبر و از طریق فیش برداری و بر اساس ترکیبی از روش توصیفی ـ تحلیلی بوده است.

۱. مفهوم شناسی

شناسایی جرایم امنیتی بیش از هر چیز در گرو شناخت جرایم امنیتی است و برای شناخت بیشتر آن، مفهوم شناسی فضای سایبری و جرایم امنیتی بسیار حائز اهمیت است.

۱-۱. مفهوم فضای سایبر

محیط سایبر از همان بدو ظهورش علیرغم وجود نظم فنی فوق العاده، از منظر رفتار کاربران محیطی مبتنی بر هرج ومرج بوده است (carey,1999,176). این فضا شامل اینترنت و دیگر سیستم های اطلاعاتی است که از کسب و کار، زیرساختها و خدمات پشتیبانی می‌کند(Lehto ,183,2013). در مورد فضای سایبر تعاریف مختلفی صورت گرفته است.در مجموع سه معیار ارائه شده است یا متضمن این هستند که فضای سایبر در اصل جهان سایبر است که در عرض جهان فیزیکی و بر پایه گستردگی تاکید دارد یا بر پایه کارکرد آن را همچون مسیری برای تبادل اطلاعات دانسته‌اند و یا بر پایه ماهیت آن را تشکیل یافته از اتصال بیشماری از رایانه‌ها و سامان‌ها می‌دانند. در معیار نخست تعبیر فضای سایبر به دنیایی دیگرصرفاً با ظهور اینترنت شهرت یافته وگرنه فضای سایبر پیش از این ها نیز وجود داشته است. از این رو است که بروس استرلینگ معتقد است: فضای سایبر مکانی است که مکالمات تلفنی در آن اتفاق می‌افتد؛ مکانی مبهم که انسان‌های زنده با هم ارتباط برقرار می‌کنند اما خارج از آن قرار دارند[1]. انسان درروياروبی با این فضا دچار نوعی سردرگمی شد که نمی‌توانست بسیاری از مؤلفه‌های آن را با بدیهیاتی که از دنیای واقعی داشت تطبیق دهد؛ لذا آن را دنیایی جدید تصور کرد که ساخته دست بشر می‌باشد و هم‌عرض با دنیای واقعی است. (Brenner,2004,55) این معیار برای شناخت فضای سایبر به عنوان بستر ارتکاب جرائم معیاری صحیح نیست چراکه تنها به بیان گستردگی این فضا می‌پردازد، درحالی

1. http://pesmcl.vub.ac.be/CYBSPACE.html

که وسعت مکان ارتکاب در بررسی جرائم از اهمیت کمتری برخوردار است(عالی پور،۱۳۹۵: ۴۰). در معیار دوم، پایه شناخت فضای سایبر منابع اطلاعاتی است به طوری که فضای سایبر، فضای منابع فراوان اطلاعات است. تعریف فضای سایبر به منبع اطلاعاتی هرچند این مزیت را دارد که بر عنصر اساسی این فضا یعنی اطلاعات انگشت می‌گذارد ولی با این حال منبع اطلاعاتی شمردن فضای سایبر بیشتر تأکید بر ایستایی بودن آن است تا قابلیت‌های فراوان آن؛ به همین دلیل باید به قابلیت اصلی فضای سایبر که همانا تبادل اطلاعات در پرتو اتصالات عدیده است، اندیشید(عالی‌پور،۱۳۹۵: ۴۱). در معیار سوم، پراکندگی سامانه‌های رایانه‌ای در همه نقاط جهان است تا با اتصال آنها با همدیگر فضای سایبر آشکار شود. بر این اساس در تعریف فضای سایبر گفته شده که همان محیط اینترنت است که رایانه‌ها را به هم پیوند می‌دهد و محل پیوند همین فضا موسوم به فضای سایبر است[1]. همچنین این دیدگاه وجود دارد که فضای سایبر اشاره به مکان مجازی دارد که با خاصیت الکترونیکی، مجموعه‌ای از اطلاعات را از طریق اینترنت ارائه می‌دهد[2].گفته شده که فضای سایبر شبکه جهانی است که محل پیوند سیستم‌های ارتباطی می‌باشد[3]. به نظر می‌رسد معیار سوم که به گونه‌ای ماهیت فضای سایبر را آشکار می‌کند مناسب‌تر باشد؛ زیرا برای شناسایی هر چیزی قبل از بررسی کارکرد باید به ماهیت آن اشاره کرد و از این منظر فضای سایبر در اصل اتصال سامانه‌های رایانه‌ای است.

۱-۲. مفهوم جرایم امنیتی

واژه جرایم ضد امنیت ملی در حال حاضر در مقررات کیفری ما وجود ندارد و به عنوان دسته بندی جداگانه‌ای از جرایم کمتر شناخته شده است، لذا باید این دسته از جرایم را برابر با جرایم علیه امنیت در کتاب پنجم ق.م.ا دانست.این جرایم به برجسته‌ترین جرایم امنیتی که به ناکارآمدی نظام سیاسی یا امنیت داخلی انگشت می‌گذارد. به عبارت دیگر این گونه جرایم بر سه ارزش مرتبط با امنیت که شامل

1. www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html
2. www.iarchive.com/_library/terminology/c.htm
3. www.psycom.net/iwar.2.html

اطلاعات، ساختار سیاسی و مقامات می‌شود، محقق می‌شود.در تعریف جرایم علیه امنیت گفته شده که اعمال مجرمانه‌ای است که ارتکاب آنها باعث ایجاد هرج و مرج در نظم داخلی یک کشور می‌شود مثل جاسوسی(رسولی، ۱۳۹۰: ۴۵).گرچه این قبیل جرایم ممکن است منافع خصوصی اشخاص حقیقی و حقوقی را نیز به خطر اندازد ولی هدف مرتکبین این گونه جرایم در حقیقت حکومت و دولت من حیث المجموع می‌باشد. با بررسی آراء مختلف ملاحظه می‌شود که تاکنون قانونگذار از جرایم امنیتی تعریفی ننموده و تنها به ذکر مصادیق آن اکتفا نموده‌اند، ق.م.ا چهارچوب جرایم ضد امنیتی را مشخص ننموده و با توجه به قوانین متفرقه لازم الاجرا روشن نیست که جرایم ضد امنیت داخلی و خارجی کدام‌اند. در این رابطه می‌توان گفت: مراد از جرایم امنیتی، جرایمی است که عنصر معنوی آن به قصد مقابله با نظام و مصالح عمومی می‌باشد. این جرایم دارای دو مفهوم عام و خاص است. بطور کلی هر جرمی تا حدودی امنیت را متزلزل می‌نماید و با اضافه کردن برخی ویژگی‌ها، رنگ امنیتی به خود گرفته؛این تلقی مربوط به مفهوم عام جرایم امنیتی است، لیکن مفهوم خاص جرایم امنیتی مدنظر ماست و آن عبارت از این است که برخی جرایم هستند که به صورت اخص ارزش‌هایی که شاخصه امنیت به شمار می‌روند و تنها بر ضد امنیت ملی ارتکاب می‌یابند، می‌باشد. با نگاهی به جرایم امنیتی خاص به خوبی آشکار می‌شود که غالب این جرایم مانند جاسوسی، موجود است، زیرا حاکمیت متولی تضمین امنیت به شمار می‌رود و مقصود ما نیز در اینجا از جرایم امنیتی واقعی،مفهوم اخیر و خاص است. درفقدان یک تعریف مورد اجماع، می‌توان این تعریف از امنیت ملی را در شرایط جدید جهانی پذیرفت؛ امنیت ملی شامل تعقیب روانی و مادی ایمنی و جزء مسئولیت حکومت‌های ملی است تا از تهدیدات خارجی و داخلی نسبت به بقای حکومت خود ممانعت به عمل آورند. نکته محوری این تعریف، بیشتر کلمه تعقیب است تا کسب آن، ضمن آن که ایده تهدید در درون آن نهفته است و نوع تهدید مشخص نشده چرا که دامنه آن می‌تواند بسیار فراتر از تهدید نظامی باشد و شامل تهدیدات اقتصادی، سیاسی شود (انتظامی،۱۳۹۵: ۴۵).

۲. ویژگی‌های جرایم امنیتی

جرایم ضد امنیت ملی دارای ویژگی‌هایی است که قانونگذاری شایسته در پیوند

با این جرایم، جز با شناخت این ویژگی‌ها ممکن نیست. بدین حال بیان ویژگی‌های زیر برای بزه‌های ضد امنیت ملی همه آن چیزی است که در قانون‌های کیفری ایران دیده می‌شود وگرنه ویژگی‌های دیگری نیز در رویه قضایی دادگاه یا دادسرای انقلاب می‌توان یافت که با معیارهای قانونی همخوانی ندارد.

۲-۱. ویژگی‌های مرتبط با جرم

نگرانی قانونگذار درجرم‌انگاری رفتارهای تهدیدآمیز امنیتی از دو موضوع ناشی می شود.اول این که قانونگذار به شهروندان اعتماد ندارد و به این امید نیست که مدتی با آرامش با شـــهروندان به سر ببرد.از این جهت می‌کوشـــد تا اگر روزی شهروندانی بر ضد دولت جرمی مرتکب شـــدند،آن‌ها را مجازات نماید.اما چون نمی‌داند که شهروندان چگونه امنیت را تهدید می‌کنند، ازجرم‌انگاری توســـعه‌گرا اســـتفاده می‌نماید.این گونه دولت‌ها در فرآیند قضایی می‌کوشند تا نسبت به رفتارهای قابل تردید، تفسیری موسع داشته باشند و اختیار وسیعی را برای مجریان قانون فراهم نموده و بدین وسیله آنها را مجازات کنند. درحالی‌که علمای حقوق معتقدند که قوانین کیفری باید به طور محدود تفسیر شود(کاتوزیان، ۱۳۹۰: ۲۱۸). کشور ما در مرحله دوم قرار دارد. این رویکرد نشان می‌دهد که نوع و روش قانونگذاری نیز می‌تواند دامنه مداخله حقوق کیفری را وسیع‌تر نماید. دوم این که قانونگذار محدوده امنیت را مشـــخص نمی‌کند و با این که باید برای پاســـداری از هر دو آنها تلاش کند ولی ســـرانجام به سمت امنیت ملی سوق پیدا کرده و چون محدوده این واژه برای او مشـــخص نیســـت، به جرم‌انگاری حداکثری سعی در حفظ ارزش‌های مدنظر خودش دارد. این رویکرد بیشتر در کشورهای اقتدارگرا بوده که امنیت را بر آزادی برتری می‌دهند.دو نمونه از مهم‌ترین شکل‌های جرم‌انگاری گسترده در زمینـــه امنیت ملی عبارتند از:۱- توســـعه مصادیق رفتار مجرمانـــه، قانونگذار برای صیانت از امنیت از اصطلاحات مبهم، کلی سود جسته است و سعی در توسعه قانون جزا نسبت به مصادیق رفتاری مخاطره‌آمیز برای امنیت ملی دارد.هدف قانونگذار در جرایم امنیتی این اســـت که به نفع امنیت ملی باشد لذا قانونگذار سعی کرده اصطلاحاتی که در این قوانین بکار می‌برد مبهم و کلی باشـــد که اگر لازم شـــد قاضی کیفری بتواند هر شخصی که متهم به این جرایم هستند داخل در این اصطلاحات جای دهد. به عنوان مثال

طبق ماده ۵۰۰ هر نحو فعالیت تبلیغی علیه نظام یا به نفع سازمان‌های مخالف نظام را مستوجب کیفر شناخته شده است. مشخص نیست که واژه‌های به هر نحو نسبت به رفتار فیزیکی فعالیت تبلیغی به چه میزان این رفتارها تحت شمول این ماده قرار می‌گیرد. به عنوان نمونه نقد، مصاحبه علیه حکومت، از طرف دیگر در همین ماده از سازمان‌های مخالف نظام نام برده، حال منظور از سازمان مخالف نظام چه سازمان‌هایی هستند؟ همین ابهام در اصطلاح دول خارجی متخاصم دست قاضی را باز گذاشته است.هر چند که در قانون جرایم نیروهای مسلح بیان شده که شورای عالی امنیت ملی آن را توضیح می‌دهد و تکلیف سازمان را در جرایم نیروهای مسلح مشخص کرده ولی در ماده۵۰۰ منظور از سازمان ابهام دارد. بکارگیری اصطلاحات کلی در جرایم ضد امنیت ملی از جهاتی نباید به اندازه‌ای باشد که قضات از آن سوءاستفاده کنند۲- بحث امنیت ملی به اندازه‌ای مهم است که علیرغم این که حقوق کیفری قصد را مجازات می‌کند، در این حال حتی بی‌مبالاتی را هم مسئول می‌شناسد. علیرغم این که اصل بر عمدی بودن جرایم است، اما استثنائاً رفتارهای از روی تقصیر افراد نیز بعضاً در دایره جرم انگاری قرار می‌گیرد که این استثنائات در حوزه‌های امنیتی بیشتر است. لذا در صورتی که شک نماییم که آیا برای عملی عنوان غیرعمدی نیز در نظر گرفته شده یا خیر بایستی قائل به عدم جرم انگاری شویم. به عنوان مثال ماده ۵۰۶ و ماده ۲۸ق.م.ن.م در مورد بی‌مبالاتی در تخلیه اطلاعاتی شدن، ماده۲۷ در مورد بی‌مبالاتی، توسط فرد نظامی در افشای اطلاعات. نتایج حاصله از جرم موجب تعیین مجازات محارب برای عملی شده است که در ظاهر چندان مهم و قابل توجه نیست. از طرفی در هیچ کشوری، امنیت ملی به طور کامل وجود ندارد و تا زمانی که کشورهای دیگر وجود دارند همواره تهدیدات بالقوه و بالفعل کشور مورد نظر را متوجه خود خواهد کرد. دستیابی به امنیت مطلق، قابل تصور نیست، کشوری ممکن است از لحاظ نظامی دچار ناامنی نباشد، اما تهدیدهایی با ماهیت فرهنگی و اجتماعی،امنیت آن را در معرض خطر قرار دهد.همچنین توانایی‌های نسبی دولت‌ها برای مقابله با تهدید نیز نسبی است (درویشی سه ثلاثی،۱۳۷۶: ۶۳). زیرا قدرت که مبنای تحصیل امنیت است متغیر و نسبی است و بالطبع امنیت حاصل برای دولت‌ها نیز نسبی است.

۲-۲. ویژگی‌های مرتبط با ضمانت اجرا

رفتارهای مجرمانه علیه امنیت ملی نسبت به سایر جرایم بیشترین تاثیر را بر امنیت می‌گذارد و اصولاً موجب بی اعتمادی عمومی نسبت به دولت در کنترل ناامنی می‌شود، لذا قانونگذار شدیدترین مجازات‌ها را برای جرایم علیه امنیت پیش‌بینی کرده است. در ایران باستان قوانینی که برای کیفر خیانت پیشگان وضع شده بود بسیار سخت و ازجمله این بود که خیانت یک فرد موجب هلاک همه خویشانش میشد(صانعی،۱۳۷۲ ۳۲۸:). محبوس کردن مجرمان سیاسی به همراه جانوران موذی یا انداختن این افراد درقلعه فراموشی نیز از جمله مجازات‌های معمول در ایران باستان بوده است (راوندی،۱۹:۱۳۶۸). اگر به مقررات مربوط به حدود مراجعه کنیم، در سه جرم ضد امنیتی (بغی،افساد فی‌الارض و محاربه) می‌بینیم که هر سه این جرایم دارای مجازات اعدام هستند. همچنین استفاده از عبارت‌هایی مانند(اگر محارب شناخته نشود) درماده ۴۹۸ راجع به تشکیل یا اداره به قصد بر هم زدن امنیت،فراهم کردن امکان اعمال مجازات اعدام از بسیاری از جرایم مرتبط با امنیت، بیانگر استفاده زیاد از مجازات در این نوع جرایم است. البته قانونگذار در برخی مواد قانونی مانند مواد۲۰،۳۰، بند الف ماده ۲۴ و مواد۳۰،۳۱ و۳۲ ق.م.ن.م برای بسیاری از جرایم امنیتی بدون آن که عنوان محاربه بر عمل بار شود مجازات محارب قرار داده است. بیشتر مجازات‌ها در جرایم ضد امینت شامل اعدام و حبس‌های طولانی مدت می‌باشد به ویژه این مجازات‌ها در ق.م.ن.م به اوج خود رسیده است. شدت عمل قانونگذار گاهی از حد عقلانیت می‌گذرد و افراد را با توجه به موقعیتی که در آن قرار دارند، به خاطر رفتارهایی همچون خواب به بدترین شکل کیفر می‌دهد. جالب این که بر اساس ماده ۴۴ ق.م.ن.م اگر بهم خوردن امنیت کشور در اثر خواب ارادی یک نظامی در حین نگهبانی باشد، باز هم مجازات محارب را خواهد داشت.آن چه در این ماده آمده است، از نظر نوع رفتار نیز، با ابهام مواجه است، شاید بتوان به طور ارادی مقدمات خواب را فراهم آورد، اما خوابیدن که به واسطه از کار باز آمدن حواس ظاهره در انسان و سایر حیوانات بروز می‌کند امری ارادی نیست(جعفری دولت آبادی،۱۳۹۵: ۱۹۸).ازآنجایی که طبق ماده ۲۸۲ برای محاربه چهار مجازات در نظر گرفته شده است، ممکن است قاضی مجازات قتل را برای یک جرم امنیتی متوسط و مجازات نسبتاً خفیف تبعید را برای یک جرم امنیتی بزرگ در نظر بگیرد. در هر حال در باب امنیت، قانونگذار از اهداف مجازات فاصله می‌گیرد.

۲-۳. ویژگی‌های مرتبط با رسیدگی

در قانون مجازات اسلامی چندین اصل در مورد اعمال قوانین کیفری داریم مانند اصل سرزمینی بودن،اصل شخصی بودن و اصل واقعی بودن.مقررات کیفری نسبت به جرایم ارتکابی در محدودهٔ سرزمینی قابل اجرا می‌باشند (ماده۳ق.م.ا)، این مقررات بر رفتارهای مجرمانه ایرانیان نیز حاکم خواهد بود؛ خواه در محدودهٔ سرزمینی مرتکب جرم شوند و خواه خارج از محدوده سرزمینی(ماده۷ق.م.ا). بنابراین نسبت به مقررات کیفری دو اصل مهم حاکم است: اصل سرزمینی بودن و اصل شخصی بودن. اما در مورد جرایم امنیتی اصل واقعی بودن مقررات کیفری نیز حاکم است. به موجب این اصل رسیدگی به جرایم مهم از جمله اقدام علیه امنیت(بند یک ماده۵ ق.م.ا) اعم از این که مکان ارتکاب ایران باشد یا خارج، طبق مقررات جزایی ایران خواهد بود. در واقع اصل واقعی بودن، عدول از اصل سرزمینی مقررات کیفری است که پیش‌بینی چنین اصلی برای پاسداری هر چه بیشتر از امنیت ملی است. جرایم امنیتی در فرآیند رسیدگی همواره با حساسیت‌هایی همراه بوده که پایه برخی از آنها را خود قانون نهاده است.گاهی تا جایی این سخت‌گیری‌ها ادامه دارد که مطرح می‌شود نسبت به جرایم امنیتی رسیدگی افتراقی[1] وجود دارد و رسیدگی در این جرایم نسبت به رسیدگی‌های عادی فرق می‌کند. برخی از این مقررات در آیین دادرسی کیفری وجود دارد، نظیر برخی از مقررات که در ارتباط با حق گرفتن وکیل و یا مواردی که تجویز رئیس قوه قضائیه برای بررسی اسناد مرتبط با امنیت ملی هست همه این موارد نشان می‌دهد جرایم امنیتی در فرایند رسیدگی کیفری با سخت‌گیری‌هایی مواجه هستند. قانون آیین دادرسی کیفری در مرحله دادرسی در ماده ۳۵۲ به اصل بودن رسیدگی علنی تصریح نموده و استثنائات آن را در دو بند قرار داده است، امنیت نیز یکی از جهات غیر علنی شدن رسیدگی است. در بند ب ماده ۳۵۲ از عبارت مخل امنیت عمومی استفاده شده است که می‌توان امنیت عمومی را از ارکان نظم عمومی تلقی کنیم. باید توجه نمود که انتشار جریان دادرسی مخل اصل برائت بوده و زمینه انتشار اتهام وارده به متهم و خدشه به حیثیت وی را فراهم می‌سازد به همین دلیل است که ممنوعیت انتشار جریان دادرسی در ماده ۳۵۳ همین قانون مورد توجه قرار گرفته است و بر این

1. Differential hearing

اســـاس است که در ماده یاد شده مقرر می‌کند خبرنگاران می‌توانند با حضور در دادگاه از جریان رســـیدگی گزارش مکتوب تهیه کرده و بدون ذکر نام آن را منتشـــر نمایند. اجرای این ماده به خصوص در جرایم امنیتی با موانعی مواجه است. این موانع در جرایم عادی شـــامل عدم وجود امکانات در دادگاه‌ها بـــرای حضور عموم و به ویژه عدم تمایل قضات به وجود ناظر بر عملکرد خویش اســـت. خدشه به این اصل در دستورالعمل‌های قوه قضاییه به وضوح دیده می‌شـــود. از جمله به دستورالعمل ساماندهی نظارت بر تردد مراجعین و ارتقاء رفتار ســـازمانی مصوب ۸۴ اشاره کرد. این دستورالعمل به‌رغم عنوان خود نه تنها امکان حضور افراد غیرذینفع را در محاکم دادگستری منتفی می کند، بلکه به خلاف اصل صحت اقوال،صحت ادعای مراجعه کننده را به بررســـی موضوع در رایانه دفتر کل منوط می‌نماید. ممنوعیت تردد عموم به دادگســـتری، در دادگاه‌های انقلاب نمود بیشـــتری دارد؛ این امر مبین رویکرد ســـختگیرانه دستگاه قضایی در جرایم علیه امنیت است(جعفری دولت آبادی،۱۳۹۵: ۲۶۱). مطابق ماده ۴۲۰ق.آ.د.ک، حفظ نظم و امنیت،از جهات احاله اســـت. قید امنیت صرفا معطوف به جرایم علیه امنیت نیست، اما این ماده حفظ امنیت را به عنوان یکی از ضرورت‌های احاله قرار داده است.

۳. گونه شناسی

۳-۱. گونه شناسی جرایم امنیتی

از لحاظ قانونگذاری، گونه شناسی جرایم علاوه بر اعلام ارزش‌های مورد حمایت قانونگذار، می‌تواند به ایجاد یک سیاست جنایی منسجم کمک کند. گونه شناسی جرایم امکان شناســـایی ماهیت جرایم، نوع و شدت رفتارهای تشکیل دهنده را فراهم می‌کند. روی هم رفته می‌توان به برخی از تهدیدات برجسته امنیتی را برشمرد که در قانون‌های کیفری ایران عنوان‌های مجرمانه یافته‌اند.

۳-۱-۱. جرایم امنیتی مرتبط با اطلاعات

اطلاعات طبقه‌بندی شـــده برای مجرمین حکـــم آب را دارد. آنها از اطلاعات و داده‌ها برای تزریق و تکثیر اندیشه‌ها خود استفاده می‌کنند و در همان حال ممکن است اصالت اطلاعات و داده‌ها موضوع حمله آنها واقع شود. هدف از جرم‌انگاری جرایم امنیتی

مرتبط با اطلاعات، حفظ و صحت اطلاعات در برابر آسیب همه آنها است. بنابراین هر گونه خسارت در اطلاعات بدون مجوز قانونی موجبات تجاوز را فراهم می‌آورد.

۳-۱-۱-۱. جاسوسی

متاسفانه در هیچ کدام از قوانین کیفری تعریفی از این جرم نشده است و صرفاً به ذکر مصادیقی از آن بسنده کرده‌اند.حتی در رویه قضایی و دادگاه انقلاب نیز با ابهامات قانونی مواجه هستیم. دلیل این امر هم دو موضوع می‌تواند باشد؛ یکی رعایت امنیت است چه آن که در صورت تعریف روشن، امکان سوء استفاده زیاد می‌باشد، دیگری این است که وقتی به فصل اول کتاب پنجم ق.م.ا با عنوان جاسوسی رجوع می‌کنیم یک ماده قانونی که نشان دهنده تعریف و بیان ارکان آن مواجه نمی‌شویم، در حالی که می‌بایست قانون جرایم امنیتی را شفاف بیان می‌نمود. با توجه به ابهامات موجود باید مقررات جاسوسی را به دو صورت مراحل تحقق جاسوسی و موضوعات مرتبط با جاسوسی که درمواد ۵۰۲،۵۰۳ و۵۰۶ قرار دارد، مد نظر قرار داد. جاسوسی یک جرم فرآیند محور به حساب می‌آید و چون اطلاعات حساس هستند قانونگذار مراحل آن را جرم انگاری نموده که شامل مرحله ورود به محل و موضع نگهداری اطلاعات که در ماده۵۰۳ قانون آمده است. مرحله دستیابی به مفاد اطلاعات که در ماده۵۰۵ مطرح گردیده است و مرحله افشا یا در دسترس‌گذاری اطلاعات به افراد یا نهادهای فاقد صلاحیت که در ماده ۵۰۱ ذکر شده است. به دلیل حساس بودن این جرایم باید به دنبال مقرراتی باشیم که این سه فرآیند را معرفی نماید، هر چند هر کدام از این رفتارها به تنهایی عنوان مجرمانه هستند، اما فرآیندوار بودن آنها به منزله این نیست که این سه مرحله باید با هم اتفاق بیافتد تا متهم به جاسوسی باشد، بلکه اصل بر این است که رفتارهای جاسوسی به تنهایی نیز جرم هستند و منظور از فرآیند محور بودن در واقع در مورد نحوه تحقق جاسوسی است (عالی‌پور،۱۳۹۷: ۳۰). البته این امکان وجود دارد که خود قانونگذار بخواهد در بعضی مواقع یک یا دو مرحله فوق را عنوان مجرمانه خاصی تلقی نماید. مانند ماده ۵۰۵ راجع به مرحله دوم که جمع‌آوری اطلاعات که خودش مستقلا جرم محسوب می‌شود و در ادامه ماده گفته اگر موفق بشود که اطلاعات جمع‌آوری شده را در اختیار دیگران قرار بدهد هم یک جرم تلقی می‌شود اما مجازات

آن افزایش می‌یابد. بنابراین در انتهای ماده ۵۰۵ یکی از مصداق‌های تبصره۲ماده۱۳۴تلقی می‌شـــود و راجع به جایی اســـت که قانون دو عنوان مجرمانه را در یک عنوان در نظر گرفته اســـت. در مـــاده ۵۰۳ هیچ تعبیری از جرم جاسوســـی در متن ماده آورده بیان نکرده اســـت. چون دلیل ورود به محل اطلاعات توســـط مرتکب مشخص نیست. البته قانونگذار قصد خاصی را شـــرط کرده به دلیل این که احراز شود که ورود به این مواضع برای سرقت بوده یا نقشه‌برداری و نه احیاناً برای قصد خاص دیگر. نتیجه این که ورود به اماکن امنیتی فی نفسه امری سرزنش پذیر نیست و نیاز به قیدی دارد که بتواند آن رفتار و عمل را سرزنش‌پذیر کند و آن قصد مرتکب است. لذا در جاسوسی از نظر رکن روانی باید مرتکب علم و عمد داشـــته باشد، منتهی چون مرحله اول نسبت به اطلاعات طبقه بندی شده انجام نمی‌شود، بلکه نسبت به مکان است لذا قصد دسترسی و تحصیل اطلاعات را باید داشـــته باشـــد که در مرحله دوم فعل آن را انجام دهد. از این رو تنها مرحله اول نیاز به قصد خاص می‌باشد. به عبارتی ورود به محل اطلاعات از جهت سنتی موضوع ماده ۵۰۳ که قصد ذکر شـــده است جرم مطلقی است که دارای سوءنیت خاص اســـت.ضمن این کـــه ورود به مواضع ممنوعه برای اینکه از آنجا اطلاعات را به دســـت آورد، به تنهایی ذکر نشـــده، از طرفی اشخاصی که بدون کسب اجازه مأمورین ذیصلاح در حال نقشـــه‌برداری یا گرفتن فیلم یا عکســـبرداری از استحکامات نظامی باشند این مورد خودش یک نوع دسترسی اطلاعات قلمداد می‌شود و می‌بایست در در مرحله دوم فرآیندها آورده می‌شد. ماده ۵۰۵ به جمع‌آوری یا تبدیل اطلاعات و اسناد اشاره می‌کند کـــه با هدف بر هم زدن امنیت صورت می‌گیرد. بر هم زدن امنیت در این ماده در واقع یک تخلیه اطلاعاتی عالمانه است و یک خلای است که در قانون آمده زیرا معمولا این اهداف ملاکی ندارد و برای دادگاه به راحتی قابل احراز هســـتند(عالی پور،۱۳۹۷: ۳۱). در ادامه ماده بیان شـــده چنانچه بخواهد در اختیار دیگران قرار دهد و در واقع مرحله ســـوم را انجام دهد در اینجا هر دو جرم را به صـــورت یکپارچه انجام داده در غیر این صورت به حبس از یک تا پنج سال محکوم می‌شود.

از طرفی باید بیان کرد جاسوســـی ســـایبری عنوانی غیر قابل اعمال است، زیرا جاسوســـی سایبری منوط به نگارش آئین نامه‌ای شده که در تبصره ۲ ماده ۷۳۱ آمده که در این تبصره، نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی آنها ذکر

شـــده و چون هنوز این آئین نامه به تصویب نرســـیده لذا می‌توان گفت داده‌های سری وجود ندارد، وقتی داده ســـری وجود نداشته باشد، اساساً وجود جرم جاسوسی سایبری در ارتباط با مقرر ماده ۷۳۱ تا ۷۳۳ زیر ســـوال اســـت. بنابراین اگر شـــخصی افشاء یا جاسوســـی را از طریق رایانه انجام بدهد ماده ۷۸۰ ق.ج.رحاکم می‌شود. این ماده برای جرایم رایانه‌ای وســـیله محور هست و چنانچه جرایم رایانه‌ای وسیله محور محقق شوند در اصل جرم سنتی تلقی شده و مجازات همان ماده مربوطه را تحمل می‌کند. پس در وضعیت فعلی جاسوســـی رایانه‌ای هویت قضایی و اجرایی ندارد، ولی اگر رایانه وســـیله ارتکاب جاسوســـی یا افشای مستقل شود.برحســـب مقررات مرتبط و نه براساس ماده ۷۸۰ تا زمان تصویب آئین نامه و هویت بخشـــی به داده‌های ســـری جاسوسی از طریق رایانه جانشـــین جاسوســـی رایانه‌ای خواهد بود(عالی پور،۱۳۹۷ :۱۱۸). لذا باید گفته شـــود جاسوسی از طریق رایانه داریم لیکن جاسوســـی رایانه‌ای نداریم. به همین دلیل باید سراغ جاسوسی در مقررات سنتی برویم و همان مقررات سنتی جاسوسی از طریق رایانه حاکم می‌شود.

۳-۱-۱-۲. افشای غیرمجاز

افشای غیرمجاز به لحاظ نقض محرمانگی در محدوده جاسوسی قرار نمی‌گیرد و رابطـــه تنگاتنگی با مرحله ورود به محل و موضع نگهداری و مرحله دســـتیابی ندارد، زیرا وقتی که دو مرحله قبلی انجام گیرد دیگر نقض محرمانگی صورت گرفته و در این مرحله می‌خواهد افراد بیشـــتری از مفاد آن آگاه شـــوند و قانونگذار برای این که افراد بیشـــتری آگاه نشوند افشای اطلاعات را جرم انگاری نموده است. لذا این مرحله شامل بخش ذاتی جاسوسی نمی‌شـــود و با عنوان مجرمانه دیگری که در قانون انتشار و افشا مصوب ۵۳ پیش‌بینی شـــده مشـــابهت دارد. افشـــای غیر مجاز در ماده۵۰۱ق.م.ا بیان گردیده اســـت. این ماده برخلاف دو ماده قبل به واژه جاسوسی اشاره شده، هر چند ما تعریفی از جاسوسی را مشـــاهده نمی‌کنیم. در واقع در اختیار گذاشتن و مطلع کردن از مفاد اطلاعات طبقه‌بندی شده باید متضمن نوعی جاسوسی باشد تا ماده۵۰۱ را جاسوسی تلقـــی نماییم و از همین نگاه بیان می‌شـــود که قانونگـــذار در ارتباط با ماده ۵۰۳ و ۵۰۵ بدون نام بردن از عنوان جاسوسی فرض را بر این گذاشته که این موارد، مراحل جاسوسی

هستند، ولی در ماده ۵۰۱ مرحله سوم که مرحله اصلی است مشروط نموده به متضمن نوعی جاسوسی. بدین معنا که فرد مرتکب این کار را در راستای انجام وظیفه به عنوان جاسوس انجام دهد، هر چند که با توجه به عبارت به کار برده شده، جاسوس حرفه‌ای بـــودن مرتکب ضرورت ندارد(میرمحمدصادقی،۱۳۹۵: ۵۸). بنابراین ما دو نوع افشـــای اطلاعات داریم؛ یک نوع افشـــای که مرحله سوم جاسوسی است که در ماده ۵۰۱ بیان گردیده و یک نوع افشـــای دیگر به عنوان رفتار مستقل افشای اطلاعات طبقه بندی به جهت وجود رابطه امانی که طبق قانون مجازات انتشـــار و افشـــا اسناد محرمانه مصوب ۵۳ که قابل بررسی هستند و به نظر می‌رسد در اینجا رکن روانی را می‌توان ملاک قرار داد و بیان نمود اگر مرتکب قصد جاسوســـی داشـــته باشد جاسوسی و اگر قصد افشای اطلاعات داشته باشد افشا محسوب می‌شود. اما در مرحله دوم و سوم اساساً دیگر قصد خاص شرط نیست که ما بخواهیم از آن کمک بگیریم و جرایم را از هم تفکیک نماییم و در هر دو مرتکب عمد در افشـــا دارد و هم علم به اسناد طبقه‌بندی شده و چون ماده ۵۰۳ از لحاظ رکن مادی به ما ملاکی نمی‌دهد ناگزیر هســـتیم به سراغ قانون انتشار و افشای مصوب ۵۳ رجوع کنیم تا مشخص شود این قانون چگونه افشای طبقه‌بندی شده را معرفی می‌کند. لازم به ذکر اســـت، به تاسی از سه نوع جاسوسی لزوماً باید سه آیین نامه داشـــته باشیم یکی آیین نامه اجرایی قانون مجازات انتشار و افشای اسناد مجرمانه و سری مصوب ۵۴ که یک سال پس از تصویب قانون سال ۵۳ برای طبقه‌بندی کردن اطلاعات غیرنظامی به تصویب رســـیده اســـت که به طور کلی در کشور ما طبقه‌بندی اطلاعات طبق همین آیین نامه ســـال ۵۴ انجام می‌شـــود، هر چند هنوز اصلاح نشده اســـت. دومی آیین نامه مربوط به نظامیان که دارای مقرره خاص است سومی داده‌های رایانه‌ای هم که هنوز آیین‌نامه آن به تصویب نرســـیده اســـت و در این رابطه مشـــکل موضوع وجود دارد. بر اساس قانون سال ۵۳ افشای اسناد طبقه‌بندی شده در قالب جرم مستقل به دو دسته قابل تقسیم هستند: الف- افشای اصلی: در این نوع از افشا، مرتکب امین یا اختیاردار، اطلاعات طبقه‌بندی را انتشار یا افشا می‌کند. به دلیل این که مرتکب امین یا اختیاردار اســـت و رابطه امانت برقرار می‌باشـــد لذا می‌تواند به صورت عمدی و غیرعمدی قابل انجام باشـــد، هر چند مجازات آن‌ها متفاوت است. لذا مرتکب دو مرحله اول جاسوسی را نمی‌تواند انجام دهد و تنها می‌توانند مرحله سوم که بحث افشای

اطلاعات اســـت انجام دهند.ب- افشای حکمی: این نوع افشـــا ناظر به افشا توسط غیر امین و اختیار دار رســـمی است و حکم افشای اسناد طبقه بندی شده را دارد که فقط در حالت عمدی انجام می گیرد. در قانون ســـال ۵۳ به دو دسته از این مرتکبین اشاره شـــده یکی کارمندان دولت، از باب این که در معرض اطلاعات طبقه‌بندی هســـتند و دیگری سایر اشخاص عادی. نتیجه این که متضمن نوعی جاسوسی درماده ۵۰۱ منظور مرتکبی است که امین و اختیاردار نباشد. حال اگر بین کارمندان دولت و دیگر اشخاص رابطه امانی وجود داشـــت در این صورت مشمول موضوع قانون سال ۵۳ می‌شود و اگر رابطه امانی نداشتند مشمول ماده ۵۹۳ ق.م.ا خواهد بود.

۳-۱-۲. جرایم امنیتی مرتبط با مقامات

درجرایم امنیتی اشـــخاص و مقامات نسبت به جایگاه سیاسی که دارند، معمولاً از بین رفتن این اشخاص بیشتر از آنکه به امنیت ملی لطمه بزند، سبب انسجام امنیت ملی و همبســـتگی ملی می‌شـــود در ارتباط با این مقامات می‌بینیم در برخی از جرایم ســـوءقصد به جان مقامات سیاسی پیش‌بینی شده است و به مراتب از حفظ محرمانگی اطلاعات حساس‌تر می‌باشد.

۳-۱-۲-۱. سوء قصد به مقامات

تعبیر ســـوءقصد به مقامـــات در دو ماده ۵۱۵ و۵۱۶ نشـــان می‌دهد که رفتار مرتکب دو حالت می‌تواند داشته باشد: یکی این که می‌تواند در مقام شروع به قتل باشد که با ماده ۶۱۳ مشمول مقررات تعدد معنوی نمی‌شود، چون شروع به قتل در اینجا با عنوان ویژه‌ای یاد شده است. همچنین چون از جهت ماهیت یکی‌اند، در نتیجه تنها یک عنوان مطرح شـــده و تعدد معنوی کنار می‌رود. دیگری ســـوء قصد به جان تا جایی نیز پیش می‌رود که رفتار مرتکب به ضرب و جرح بزه دیده بیانجامد؛ در اینجا قتل به طور عقیم رخ داده اســـت ولی همچنان در گســـتره سوءقصد است؛ زیرا تا هنگامی که رفتار مرتکب به قتل انجام نگیرد، ســـوءقصد به جان دیگری خواهد بود.بدیهی است سوءقصد به جان مقام سیاســـی تنها با بند الف ماده ۲۹۰ منطبق اســـت. به عبارتی هم شروع به قتل عمد و هم سوءقصد به جان مقامات هنگامی معنا دارد که کسی از قبل قصد کشتن

آنها را داشـــته باشـــد و گرنه در رفتاری که موجب جنایت می‌شود، قصد آغازین برای کشـــتن دیگری نیســـت تا در صورت ناکامی بتوان آن را ســـوء قصد دانست. ترور نیز می‌تواند به اندازه ســـوءقصد باشـــد و هم خود قتل عمد. بنابراین بهتر است بیان نمود ترور در جایی که به قتل می‌انجامد باید نســـبت به همان مقام‌های پیش بینی شده در دو ماده ۵۱۵ و ۵۱۶ باشـــد، هر چند رویه عملی کشـــتن هر کس با انگیزه سیاسی یا از سوی عامل بیگانه ترور دانسته می‌شود که از منطق به دور است (عالی پور،۱۳۹۷: ۷۰). آن چه که در دو ماده ۵۱۵ و ۵۱۶ به عنوان محارب بیان شـــده این نیست که مرتکب ســـوء نیت خاص برای رویارویی با نظام داشـــته باشد (میرمحمد صادقی،۱۳۹۵: ۱۴۸) بلکه برای محارب دانستن کسی که سوءقصد داشته باید به ماده ۲۷۹ مراجعه نمود،که اگر ســـوء قصد با سلاح باشد و بر ضد مقامات سیاســـی، در همان حال قصد ترساندن مردم را داشـــته باشد، در این حال محارب خواهد بود.این بحث در منابع مختص جرایم ســـایبری، پرداخته نشده است؛ اما مواردی را می‌توان فرض کرد که امکان سوءقصد به جان مقامات از طریق رایانه باشد. به عنوان مثال در موردی که هدایت هواپیما یا کشتی از طریق رایانه صورت گیرد، ممکن اســـت شخصی پس از هک کردن سیستم رایانه‌ای، کنترل آن را به دســـت گرفته و موجب اختلال در هدایت آنها شـــود و عمداً هواپیمای مقامات را به مسیر دیگری منحرف می‌کند تا اینکه به کوه برخورد نماید، هر چند منجر به قتل یا سقوط هواپیمای مقامات نشود. در اینجا رایانه فقط ابزار ارتکاب جرمی است که جانشـــین تفنگ قرار می‌گیرد و به نظرمی‌رســـد که لازم نیست استفاده از رایانه در ســـوءقصد را در قوانین کیفری سنتی نیز وارد کنیم، زیرا مراجع قضایی اغلب این مورد را بر اساس آلت قتاله ارزیابی نمی‌کنند.

۳-۱-۲-۲. بغی

بغی در قانون مجازات اســـلامی تعریف نشـــده و صرفاً مصادیق آن آمده است. مصادیق بغی، ماده ۲۸۷ و ماده ۱۷ق.م.ن.م اســـت.به نظر می‌رسد علت اینکه مقنن این بحث در قســـمت حدود مطرح کرده به این علت باشـــد که در بخش تعزیرات قانونگذار نمی‌توانســـته به میزان جرایم حدی، مجـــازات برای تعزیـــرات پیش‌بینی نماید(عالی پور،۱۳۹۷: ۱۷۶). بغی عبارت است از قیام مسلحانه بر ضد حاکم اسلامی است. باید

دانست جهاد با بغات یک چهره جنگی داشته و اصلاً صحبت از جرم نیست که برای آن مجازات حدی اعمال شود. به همین دلیل است که هرچند بغی جایگاهی در متون فقهی ما دارد ولی این ارتباطش نه درارتباط با جرم بلکه ارتباط با جنگ دارد.از طرفی می‌دانیم قواعد جنگ با قواعد مرتبط با جرم فرق می‌کند، ق.م.ا آن چیزی که به عنوان پیشینه اسلام بوده است را به عنوان جرم قانونگذاری می‌کند و این امر باعث گردیده که اگر مثلا گروهی علیه حاکم قیام کردند تا سر حد جنگ بجنگد چون که به هر حال با آنها به عنوان مجرم تلقی می‌شود. ولی شیوه پیشینیان ما این طور نبوده است زیرا آنها باغی هستند و از لحاظ عقیدتی با حاکم اختلاف نظر دارند. راجع به امکان تحقق بغی از طریق رایانه‌ای عده‌ای معتقدند: اجتماع شروط تحقق بغی از طریق رایانه بنابر آنکه خروج بر حاکم اسلامی مقید به خروج با اسلحه باشد، ممکن نبوده و در نتیجه بغی رایانه‌ای متصور نیست، اما بر فرض آن که خروج بر امام عادل و شورش بر ضد وی، به طریق غیرمسلحانه متصور باشد. موضوع بغی رایانه‌ای محقق می‌شود(عمید زنجانی،۱۳۷۷: ۳۳۵). لذا به نظر می‌رسد بغی در فضای سایبری صلاحیت برای اجرای احکام بغی را دارا می‌باشد. با این حال هرگاه گروهی با استفاده از ارتباطات رایانه‌ای درصدد تهیه مقدمات، شورش و خروج علیه حکومت باشند، از باب مقدمهٔ حرام و به سبب اعداد مقدمات بغی، امکان تعزیر آنها وجود خواهد داشت(مکارم شیرازی،۱۳۷۵: ۴۸۷).

۳-۱-۲-۳. جرم سیاسی

بر اساس مادهٔ ۱ قانون جرم سیاسی هر یک از جرایم ماده ۲ چنانچه با انگیزه اصلاح امور کشور علیه مدیریت یا سیاست‌های داخلی یا خارجی ارتکاب یابد، بدون این که قصد ضربه زدن به اصل نظام را داشته باشد، جرم سیاسی محسوب می‌شود و دو معیار انگیزه و نیز نداشتن قصد ضربه زدن به اصل نظام را مدنظر قرار داده است. انگیزه ماده ۱ قانون جرم سیاسی بیشتر مصلحت جویانه است. منتها این انگیزه با رفتارهای بد انجام می‌شود و قصد ضربه زدن به نظم کنونی سیاسی امنیتی را دارد و یا نوع حکومت را قبول ندارد. واژه انگیزه در اینجا ممکن است قابل دفاع باشد؛ زیرا استفاده از واژه انگیزه در اینجا اصلاح امور یک کار مثبت است و نمود این انگیزه اصلاحی با رفتارهای کلان نمایانگر شده است و همین انگیزه است که غالباً مجرم سیاسی را از مجرمین عادی جدا

می‌کند. بنابراین در قانون جرم سیاسی انگیزه با قصد تناسبی ندارد. ماده ۲ جرایمی که در صورت انطباق با شرایط مقرر در ماده ۱ این قانون جرم سیاسی محسوب نموده بیان کرده اســـت. مواد ۱و ۲ این قانون نشان می‌دهد که قانون جرم سیاسی، شخص محور و جزئی محور اســـت. در حالی که جرم سیاسی عموماً حول محور موضوعات کلان‌تر مثل مخالفت با نظام سیاســـی یا مخالفت با تصمیمات مســـئولین و نقد آنها که در واقع این موارد است که ماهیت جرم سیاســـی را تشکیل می‌دهد زیرا مجرم سیاسی یک مخالف نرم بر ضد نظام سیاســـی محسوب می‌شود، البته ممکن است باکلام خود نقدی از نظام کند که برای افرادی این نقد ناراحت‌کننده باشد. در عین حال این فرد یک منتقد است نـــه مخالف، هر چند که این رویکرد را در حال حاضر در قانون جرم سیاســـی نمی‌بینیم و قانون جرم سیاســـی مصوب ۹۵ مجرم را در حد یک توهین کننده تلقی کرده است. از دید ما در اینجا جرم امنیتی است و مستند آن ماده ۵۰۰ است که مصادیق آن می تواند برگزاری تظاهرات و گردهمایی در فضای سایبر از طریق شبکه های اجتماعی، راه اندازی برنامه‌های رادیو و تلویزیونی در فضای سایبر، چاپ و مصاحبه‌های متعدد با ضدانقلاب و تبلیغ به نفع آنان باشـــد. در حالی که قانون جرم سیاسی باید یک مرحله جلوتر می‌رفت و جرمی که تبلیغ علیه نظام تلقی می‌شـــود تلقی می‌کرد نه این که همچنان جرم تبلیغ علیه نظام در ماده ۵۰۰ حفظ شـــود(عالی‌پور،۱۳۹۷: ۲۱۲). لـــذا بهتر بود بجای اینکه جرم سیاســـی را مطرح کنیم بخشـــی از جرایم موجود در جرایـــم امنیتی را تبدیل به جرم سیاســـی نمائیم ولی متاسفانه درجرایم سیاسی حتی یک مورد هم پیدا نمی کنیم که جرم امنیتی در قالب جرم سیاســـی قرارگرفته باشـــد. جرم تبلیغ علیه نظام اسلامی کـــه به قصد براندازی جمهوری اســـلامی صورت می‌گیرد، می‌توانـــد از طریق رایانه نیز محقق گردد. به نظر می‌رســـد باید ارتکاب جرم تبلیغ علیه نظام در صورتی که از طریق فضای ســـایبری صورت گرفته باشـــد، به عنوان کیفیت مشّدد در میزان مجازات‌ها مؤثر باشـــد زیرا حجم وسیع مخاطبین و آثار خسارت بار آن، مجازات شدیدتری را می‌طلبد. هرگاه فعالیت تبلیغی در فضای ســـایبر علیه امنیت توسط شخص یا گروهی با همکاری دول متخاصم با جمهوری اســـلامی صورت گیرد به مجازات مقرر در ماده ۷۳۹ محکوم می‌شـــود. براساس بندهای الف و ب ماده ۲۶ ق.م.ن.م می‌توان مجازات مجرم را با توجه به سمت مرتکب در جرم تبلیغ علیه نظام تشدید نمود.

۳-۱-۳. جرایم امنیتی مرتبط با شهروندان

هدف اصلی از تشکیل حکومت‌ها، تأمین امنیت شهروندان است و این فرض که تمامی جرایم دارای جنبه عمومی هستند یعنی هر رفتاری علاوه بر بزه‌دیدگان جرم، امنیت شهروندان را مخدوش می‌سازد، پذیرفته شده است.

۳-۱-۳-۱. اقدامات تروریستی

از دیدگاه برخی تروریسم، گونه‌ای از خشونت است که توأم با استفادهٔ نظام‌مند یا تهدید به قتل برای ترساندن گروه موردنظر که وسیعتر از قربانیانِ آنی جرم می‌باشند و یا به منظور ایجاد هراس صورت می‌گیرد (نجفی ابرندآبادی و هاشم بیگی،۱۳۹۷:۲۷۲). بعضی نیز در تعریف تروریسم نقش حکومت‌ها را برجسته کرده‌اند و بر این باور هستند که ترور به کارهای خشونت‌آمیز حکومت‌ها برای سرکوبی مخالفان خود و ترساندن آنها و به عبارت دیگر به کشتار سیاسی اطلاق می‌شود (آشوری،۱۳۹۸: ۹۸). نظام حقوقی ایران با تصویب ماده واحده الحاق دولت ایران به کنوانسیون سازمان کنفرانس اسلامی جهت مبارزه با تروریسم بین‌المللی مصوب ۸۷ تعریف این کنوانسیون را که در بند ۲ ماده ۱ آمده پذیرفته است. مطابق این بند اصطلاح تروریسم به هرگونه عمل خشونت آمیز اطلاق می‌شود که علیرغم انگیزه به منظور اجراء طرح جنایی فردی یا گروهی که با هدف ایجاد رعب بین مردم یا تهدید به آسیب رساندن یا به خطر انداختن جان آنان انجام می‌گیرد. از نظر حقوقی هدف اصلی تروریسم امنیت است که با ایجاد وحشت در مردم تحقق می‌یابد. گروه‌های تروریستی از فضای سایبر برای هدف‌های خود استفاده می‌کنند مانند تبلیغ اندیشه‌های گروه یا ترساندن همگانی. این رفتار تنها با ابزار رایانه انجام می‌شود و در حقیقت تروریسم سایبری نیستند ولی در قانون ضد تروریسم از آنها نام برده شده است.به عبارتی اگر رفتار یا نتیجه در بیرون واقع شوند مانند این که کسی یک ساختمان تامین کننده ارتباطات الکترونیکی را منفجر کند و در نتیجه شبکه تامین کننده خدمات اینترنتی آن ساختمان مختل گردد یا این که بر عکس، رفتار در فضای سایبر واقع شود ولی نتیجه آن خشونت یا عواقب سوء بیرونی باشد مانند اخلال در سیستم ناوبری هواپیما و کشته شدن برخی از شهروندان؛ در اینجا عمل مرتکب، ذیل عنوان تروریسم قرار می‌گیرد.البته این امر منافاتی با جمع دو ویژگی تروریست

و مجرم رایانه‌ای نسبت به یک فرد ندارد؛ در واقع در اینجا باید حکم تعدد مادی جرم را در نظر گرفت.مصداق‌هایی که زیر عنوان جرایم تروریستی می‌شوند غالباً در مقررات کیفری پراکنده پیش‌بینی شده‌اند و در این راستا بیشتر از آن که نظام حقوقی ایران خلأ قانونی داشته باشد خلأ عنوانی دارد(عالی پور،۱۳۹۷: ۱۴۰).که برحسب اهمیت با عناوینی مانند تهدید به بمب‌گذاری در هواپیما و وسایل نقلیه در ماده ۵۱۱ ،تخریب تاسیسات عمومی و دولتی در ماده ۶۸۷ و تامین مالی تروریسم مورد توجه قرار گرفته است. فعل مادی این جرم از طریق رایانه نیز قابل ارتکاب است. عنصر روانی این ماده علاوه بر عمد در تهدید یا ادعا، عبارت از سوء نیت خاص یعنی قصد بر هم زدن امنیت کشور می‌باشد لیکن به نظر می‌رسد کسی که از طریق فضای مجازی اقدام به تهدید کرده و یا ادعای بمب گذاری می‌کند، قطعاً سوءنیت مذکور را دارا می‌باشد، در نتیجه در صورتی که فردی اقدام به تهدید یا ادعای بمب‌گذاری کند، می‌توان وی را به صرف این اقدام به مجازات مذکور محکوم کرد. روی هم رفته ترویسم سایبری را می‌توان بر دو دسته جرایم ابزار محور و جرایم هدف محور دسته‌بندی کرد. جرایم ابزار محور یعنی تروریسم از طریق رایانه، به رفتارهای بزهکارانه سنتی گفته می‌شود که گروه‌های تروریستی از فضای سایبر برای هدف‌های خود بهره می‌جویند مانند تامین مالی و یا ترساندن همگانی. این رفتار تنها با ابزار رایانه انجام می‌شوند و به راستی تروریسم سایبری نیستند ولی در قانون‌های ضد تروریسم از آن‌ها یاد شده که به سایبر تروریسم معروفند(Hancock,2001,553). جرایم هدف محور همان رفتارهایی است که از سوی گروه‌های تروریستی بر ضد رایانه انجام می‌گردد.

۳-۱-۳-۲. افساد فی الارض

مقنن در قانون صراحتاً جرم افساد فی‌الارض را از محاربه تفکیک کرده و ماده ۲۸۶ و تبصره را به آن تخصیص داده است. در واقع مقنن خواسته که محاربه را اقدامی خشونت بار با اسلحه و افساد فی‌الارض یک اقدام نرم ولی اثرگذار. منظور از افساد فی الارض رفتارهایی است که در صورت ارتکاب موجب اخلال نظام اجتماعی می‌شود، به گونه‌ای که ثبات شهروندان را از بین می برد.که در شرع مقدس پیش‌بینی نشده و مستندات فقهی ذکر شده برای آن، تکافوی اثبات چنین جرمی را نمی‌دهد. هر چند

برخی آیات ۳۲و ۳۳ سوره مائده را به دلیل تصریح شارع مقدس به عبارت افساد فی الارض مستند جرم‌انگاری آن قرار داده اند. اما بیشتر مفسران، افساد فی‌الارض را معنا و پی‌آمد محاربه می‌دانند، هم چنان که در آیه۳۲ فساد در زمین، پی‌آمد قتل دانسته شده است. بر پایه دیدگاه علامه طباطبایی جمله یسعون فی‌الارض فساداً که دنبال محاربه و جنگ ذکر شده معنای منظور را معین می‌کند که همان فساد در زمین یا اخلال به امنیت عمومی است نه هر جنگ با مسلمانان. بنابراین روشن است که منظور همان اخلال به امنیت عمومی است. که طبعاً جز با به کار بردن اسلحه و تهدید نمی‌شود و به همین جهت در روایات فساد را به کشیدن شمشیر و نظیر آن تفسیر نموده‌اند (طباطبایی،بیتا: ۱۸۸). این تفسیر از سوی فقیهان نیز پذیرفته شده است.قانونگذار هشت دسته جرایم کلی را موضوع این ماده قرار داده است ۱- جنایت علیه تمامیت جسمانی افراد ۲-جرایم علیه امنیت داخلی یا خارجی ۳- نشر اکاذیب ۴- اخلال در نظام اقتصادی کشور ۵- احراق ۶- تخریب ۷- پخش مواد سمی و میکروبی ۸- دایر کردن مراکز فساد و فحشا. ظاهر ماده ۲۸۶ نشان می‌دهد که در آن تنها ضابطه عینی ملاک قرار گرفته است. لکن تبصره این ماده نشان می‌دهد که ضابطه ذهنی نیز برای مرتکب ضروری است. در تحقق افساد فی‌الارض رایانه‌ای موضوع ماده ۲۸۶ ق.م.ا مانند (وارد کردن بوی مواد سمی یا مزه شیمیایی به قصد برهم زدن امنیت) نیز نباید به خود تردید راه داد، زیرا امروزه بی‌شک، یکی از آسان ترین راه‌های به فساد کشاندن در ابعادگسترده، از طریق نرم‌افزارهای رایانه‌ای و در ابعاد بالاتر از طریق شبکه‌های جهانی وب می‌باشد(شریفی و سپهری،۱۳۹۴: ۸). لذا شایسته است مقنن با اصلاح مواد و یا الحاق تبصره‌ای براین نکته تصریح گردد که اگر این گونه از فسادها در فضای سایبری صورت گیرد می‌تواند از مصادیق جرایم افساد فی‌الارض قرار گیرند. همچنین مطابق با نظر مشهور و با در نظر گرفتن مقتضای بنای عقلاء و تنقیح مناط وجهی برای فقدان نص و قانون خاص و حاکمیت اصالت برائت وجود ندارد و ماهیت این دو نوع از افساد) سنتی و اینترنتی (یکی است و منطقی به نظر نمی‌رسد که افساد فی‌الارض سنتی را جرم بدانیم و لکن نوع اینترنتی آن را جرم نشماریم. هر چند در این مورد نظر مخالف وجود دارد و معتقدند که اولاً قانون مجازات جدید بوده و بعد از قانون جرائم رایانه‌ای به تصویب رسید ثانیاً، تحقق عنوان افساد فی‌الارض با شرایط آن در ماده ۲۸۷ بندرت

اتفاق می‌افتد، نه مانند جرائم سایبری که گستردگیِ آثار آن جزو خصوصیات ذاتی آن محسوب می‌شود و از آن جایی که در بسیاری از موارد، جرائم سایبری دارای آثار گسترده هستند لذا در صورت داخل بودن جرائم رایانه‌ای در عنوان مجرمانه ماده ۲۸۷ بایستی در اکثر موارد بزهکاران سایبری اعدام شوند که به نظر برخلاف روح ماده ۲۸۷ و مقصود قانون گذار است(کرمی،۱۳۹۴: ۲۲۵).

۳-۱-۳-۳. محاربه

قانونگذار تعریف محاربه را در ماده ۲۷۹ بیان نموده که آن، اقدام مستقیم علیه مردم است. به موجب این ماده محاربه جرمی است که امنیت مردم را به خطر می‌اندازد؛ بنابراین، در صورتی که ربودن مال مردم، امنیت عمومی مردم را به خطر اندازد و ایجاد رعب کند جرم ارتکابی سرقت نبوده و از مصادیق محاربه محسوب می‌شود. ترساندن مردم یکی از اجزا بنیادین تعریف فقهاء از محاربه است، در حالی که این ویژگی در آیه ۳۳ سوره مائده پیش‌بینی نشده است. با این حال ماده ۲۷۹ نیز از نظرات فقها پیروی کرده و قصد ترساندن مردم را به عنوان یکی از اجزا تشکیل دهنده رکن مادی محاربه دانسته است. محاربه جرمی است بر پایه ابزار. ماده ۱ قانون اصلاح موادی از ق.م.ا مصوب ۸۷ تبصره ۳ زیر ماده ۶۵۱ منظور از سلاح مذکور در این بند را بیان نموده است. مطابق قول مشهور فقهاء و ق.م.ا، امکان تحقق جرم محاربه رایانه‌ای وجود ندارد، زیرا در جرایم رایانه‌ای نوعاً اسلحه‌ای به کار نمی‌رود تا محاربه تحقق یابد. البته اگر در آینده اسلحه‌ای الکترونیکی پدید آید که قابلیت به وجود آوردن آسیب‌های جسمانی و ایجاد وحشت را داشته باشد و عرفاً سلاح نامیده شود می‌توان محارب رایانه‌ای به حساب آید. در مقابل دیده‌گاه مشهود، قول دیگری نیز در بین فقهای معاصر به چشم می‌خورد که براساس آن اسلحه کشیدن در تحقق محاربه موضوعیت ندارد، بلکه محاربه با سلب امنیت عمومی به هر طریقی که باشد محقق می‌شود(موسوی اردبیلی،۱۴۱۳: ۷۸۷).با توجه به تشتت آراء در این زمینه به نظر می‌رسد اگر اخلال رایانه‌ای به یکی از پیامدهای پیش بینی شده در ماده ۶۸۷ بیانجامد و همراه با قصد مقابله با حکومت اسلامی باشد براساس تبصره ۱ ماده ۶۸۷ محکوم خواهد شد.

برآمد

با توجه به نفوذ همه جانبه فناوری اطلاعات در کشـــورها و گره خوردن امنیت ملی کشورها با این فضا، این امر مورد توجه مقنن قرار گرفت. لیکن از آن جایی که در قانون جرایم رایانه‌ای مبحثـــی به جرایم علیه امنیت اختصاص پیدا نکرده تا مختصات هر جرم دقیقا مشخص شود و مقنن صرفاً تعیین مصادیق محتوای مجرمانه را به عهده کارگروه مذکور در ماده ۲۱ ق.ج.رگذاشته است و بند ج فهرست، مربوط به محتوا علیه امنیت می باشـــد، لذا در این پژوهش به تحلیل عنصر مادی و ابهامات پرداخته شـــده است.پس از بررسی موارد فوق از یک طرف پیشنهاد می‌گردد با توجه به این که بعضی از جرایم علیه امنیت از طریق فضای ســـایبری قابلیت ارتکاب دارند لیکن در فهرســـت کارگروه تعیین مصادیق مجرمانه ذکـــر نگردیده جا دارد، کارگروه مذکور یک بازنگری کلی در فهرســـت مزبور بنماید و قانونگذار در ق.م.ا رویکرد شـــفافتری نسبت به تعیین کیفر نســـبت به آن دســـته از جرایم حدی یا تعزیری کـــه دارای کیفر متعدد تخییری هســـتند، اتخاذ نماید. از طرف دیگر برای شـــناخت دقیق جرایم امنیتی سایبری باید از رهیافت تلفیقی-تطبیقی اســـتفاده شود و چارچوبی مبتنی بر نگاه بین رشته‌ای و را مدنظر قرار داد.همچنین بدلیل تشـــتت آراء در این زمینه تشـــکیل دادگاه ویژه جرایم امنیتی ســـایبری گره‌گشاست. جرایم امنیتی ســـایبری جدیدترین تهدید علیه بشریت به شـــمار می‌آید. این جرایم در سیاهه کیفری نظام حقوقی ایران شامل جرایم امنیتی اســـتفاده کننده از فضای سایبر می‌شود که در بستری متفاوت و با کیفیتی منحصر به فرد ارتکاب می‌یابند. در خصوص جاسوسی از طریق رایانه در صورت ارتکاب این موارد با مشکلی مواجه نیستیم ولی به نظر می‌رسد جاسوسی رایانه‌ای نداریم. به همین دلیل باید سراغ جاسوسی در مقررات سنتی برویم و همان مقررات سنتی جاسوسی از طریق رایانه حاکم شود. همچنین در خصوص سوءقصد به مقامات در قانون جرایم رایانه‌ای با مشکل مواجه هستیم که انتظار می‌رود قانونگذار اقدام به بازنگری در قانون نماید و این مشـــکل را برطرف نماید زیرا مواردی را می‌توان فرض کرد که امکان سوءقصد به جان مقامات از طریق رایانه باشـــد هر چند ممکن اســـت که تعدادی از این مصادیق امروزه از شـــیوع بسزایی برخوردار نباشـــد. در خصوص ارتکاب بغی در فضای سایبری به نظر می‌رسد که بغی در فضای سایبری صلاحیت برای اجرای احکام بغی را دارا می‌باشد. با

این حال هرگاه گروهی با اســـتفاده از ارتباطات رایانه‌ای درصدد تهیه مقدمات، شورش علیه حکومت باشـــند، از باب مقدمهٔ حرام و به ســـبب اعداد مقدمات بغی، امکان تعزیر آنها وجود خواهد داشـــت. همچنین با توجه به ماده ۲۸۶ تبلیغ علیه نظام اســـلامی که به قصد برانـــدازی صورت می‌گیرد، می‌تواند از طریق رایانه نیز محقق گردد. لیکن باید ارتکاب جرم تبلیغ علیه نظام در صورتی که از طریق فضای سایبری صورت گرفته باشد، به عنوان کیفیت مشّدد در میزان مجازات‌ها موثرباشد. تهدید به بمب‌گذاری در هواپیما و وســـایل نقلیه در ماده ۵۱۱ تخریب تاسیسات عمومی و دولتی در ماده ۶۸۷ و تامین مالی تروریســـم نیز از طریق رایانه قابل ارتکاب اســـت که در این خصوص قانونگذار با اصلاح قانون می تواند تعیین تکلیف کند.در تحقق افساد فی‌الارض رایانه‌ای موضوع ماده ۲۸۶ نیز نباید به خود تردید راه داد لذا شایســـته اســـت مقنن با اصلاح مواد و یا الحاق تبصره‌ای براین نکته تصریح کند که اگر این گونه از فســـادها در فضای سایبری صورت گیرد می‌تواند از مصادیق جرایم افســـاد فی‌الارض قرار گیرنـــد. بالاخره درتحقق جرم محاربه رایانه‌ای با توجه به تشتت آراء در این زمینه به نظر می‌رسد اگر اخلال رایانه‌ای به یکی از پیامدهای پیش‌بینی شـــده در مـــاده ۶۸۷ بیانجامد و همراه با قصد مقابله با حکومت اسلامی باشد براساس تبصره ۱ ماده ۶۸۷ محکوم خواهد شد.

منابع

الف) فارسی

۱. آشـــوری، داریوش، ۱۳۹۸، دانشـــنامه سیاسی، چاپ بیست و هشـــتم، ***انتشارات مروارید***، تهران.

۲. انتظامی، حســـین، ۱۳۹۵، امنیت ملی و فضای اطلاعات و ارتباطات، ***نشر دانشگاه عالی دفاع ملی***،تهران.

۳. بهـــره مند، حمید؛ داودی، ذوالفقار، ۱۳۹۷، ***پشگیری اجتماعی از جرایم امنیتی ســـایبری***، مجله مطالعات حقوق کیفری و جرم شناســـی، دوره ۴۸شـــماره ۱ بهار و تابستان ص۴۶ تا ۲۷.

۴. جعفری دولت آبادی،عباس، ۱۳۹۵، جایگاه امنیت در سیاســـت کیفری ایران، چاپ اول، ***انتشارات فکر سازان***، تهران.

۵. جلالی فراهانی، امیرحسین،۱۳۸۴، ***پیشگیری وضعی از جرایم سایبری در پرتو موازین حقوق بشر***، مجله فقه و حقوق، شماره ۲.

۶. درویشی سه تلانی، فرهاد،۱۳۷۶، ***تاملی نظری بر امنیت ملی تهدیدات و رهیافت ها***، انتشارات معاونت تحقیق و پژوهشکده سپاه پاسداران انقلاب اسلامی، تهران.

۷. رسولی، محمد، ۱۳۹۰، ***جرایم امنیتی در نظام حقوقی ایران***، چاپ اول، تهران

۸. راوندی، مرتضی،۱۳۶۸، ***سیر قانون و دادگستری در ایران***، نشر سرچشمه، تهران

۹. شـــریفی، مهـــرداد؛ ســـپهری، روح الله،۱۳۹۴، ***بررسی تحقق افساد فی الارض و محاربه در فضای مجازی***، همایش ملی هزاره سوم و علوم انسانی.

۱۰. صانعی، پرویز،۱۳۷۲، ***حقوق جزای عمومی***، چاپ پنجم، گنج دانش، تهران

۱۱. طباطبایی، ســـید محمد حســـین، بیتا، ***تفسیر المیزان***، جلد پنجم، چاپ ششم، بنیاد علمی فکری علامه طباطبایی. قم.

۱۲. عالی‌پور، حســـن،۱۳۸۸، ***امنیت و ناامنی در فضای سایبر، تهدیدات رایانه‌ای علیه امنیت ملی***، مجموعه مقالات حقوق فناوری اطلاعات، به کوشـــش امیر حسین جلالی فراهانی، چاپ اول،انتشارات روزنامه رسمی، تهران.

۱۳. عالی‌پـــور، حســـن؛ کارگری، نوروز،۱۳۸۹، ***جرایم ضـــد امنیت ملی***، چاپ اول، انتشارات خرسندی، تهران.

۱۴. عالی‌پور، حســـن،۱۳۹۵،***حقوق کیفری فناوری اطلاعات***، چاپ چهارم، انتشارات خرسندی، تهران.
۱۵. عالی‌پور، حســـن؛ یکرنگی، حسن،۱۳۹۷، ***حاکمیت قانون اساسی در رویارویی با بزه های رایانه ای***، مجله حقوقی دادگستری، سال هشتاد دوم، شماره۱۰۲.
۱۶. عالی‌پور، حســـن و توحیدی نافع، جلال،۱۳۹۷، ***کیفرگزینی برای محکومان بزه های رایانه‌ای از قانون تا رویه قضایی***، مجموعه مقالات همایش جنبه‌های حقوقی فناوری اطلاعات.
۱۷. عمید زنجانی،عباسعلی،۱۳۷۷،***فقه سیاسی***،چاپ سوم، انتشارات امیر کبیر، تهران.
۱۸. کرمی،داود،۱۳۹۴، ***سیاســـت کیفری افتراقی در جرایم ســـایبر با تاکید بر حقوق کیفری ایران***، رساله دکتری، حقوق جزا و جرم شناسی، دانشگاه قم.
۱۹. کاتوزیان،امیر ناصر،۱۳۹۰، ***مقدمه علم حقوق و مطالعه در نظام حقوقی ایران***، چاپ هفتادو دوم،نشر شرکت سهامی انتشار،تهران.
۲۰. مکارم شیرازی، ناصر،۱۳۷۵،***گنجینه آرای فقهی قضایی***،چاپ اول،قم.
۲۱. موســـوی اردبیلی، عبدالکریم، ۱۴۱۳، ***فقه الحدود و التعزیرات***، چاپ اول، نشـــر العلم، قم.
۲۲. میرمحمد صادقی، حسین،۱۳۹۵، ***جرایم علیه امنیت و آسایش عمومی***، چاپ بیست و نهم، نشر میزان،تهران.
۲۳. نجفـــی ابرندآبـــادی، علی حســـین و هاشـــم بیکی، حمید،۱۳۹۷، ***دانشـــنامه جرمشناسی***، چاپ پنجم، انتشارات گنج دانش، تهران.

ب) انگلیسی

1. Brenner, S (2004), Toward a Criminal Law for Cyberspace: Distributed Security, ***university of Dayton School of law***, p:55
2. Carey, P (1999), Media Law, ***sweet&Maxwell***, Second Edition, London, :176p
3. Hancock, B. (2001) "***Cyber-Tracking, Cyber-terrorism***". Computers and Security. Vol. 20, No 7, p. 553.

4. Lehto, martti (2013) the ways, ***means and ends in cybersecurity strategies, in rauno kuusisto***, proceeding of the 12th european conferences on information warfare and security, academic conferenceslimited, p: 183.
5. http://pesmcl.vub.ac.be/CYBSPACE.html
6. WWW.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html
7. www.iarchive.com/_library/terminology/c.htm
8. www.psycom.net/iwar.2.html