

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# جرائم علیه امنیت ملی در فضای سایبر با ارائه راهکارهای پیشگیرانه



تألیف:

علیرضا شیوافرد

(کارشناس ارشد حقوق جزا و جرم‌شناسی)

انتشارات چتر دانش

Recording and registration — Iran :	موضوع
: شیوافرد، علیرضا، ۱۳۶۹ -	سرشناسه
: جرایم علیه امنیت ملی در فضای سایبر با ارائه راهکارهای پیشگیرانه/تالیف علیرضا شیوافرد.	عنوان و نام پدیدآور
: تهران: چتر دانش ، ۱۴۰۲.	مشخصات نشر
: ۱۰۰ ص.	مشخصات ظاهری
: ۹۷۸-۶۰۰-۴۱۰-۶۵۱-۱	شابک
	وضعیت فهرست نویسی: فیپا
: چاپ قبلی: آرتاکاوا، ۱۳۹۶.	یادداشت
: کتابنامه: [۹۵] - ۱۰۰ ؛ همچنین به صورت زیرنویس.	یادداشت
: جرایم کامپیوتری Computer crimes	موضوع
جرایم کامپیوتری — ایران — پی جویی	
Computer crimes — Investigation — Iran	
جرایم کامپیوتری — قوانین و مقررات — ایران	
Computer crimes — Law and legislation— Iran	
امنیت ملی — قوانین و مقررات — ایران	
National security— Law and legislation— Iran	
HV۶۷۷۳ :	رده بندی کنگره
۳۶۴/۱۶۸ :	رده بندی دیویی
۹۴۷۰۸۵۱ :	شماره کتابشناسی ملی
	اطلاعات رکورد کتابشناسی: فیپا

: جرایم علیه امنیت ملی در فضای سایبر با ارائه راهکارهای پیشگیرانه	نام کتاب
: چتر دانش	ناشر
: علیرضا شیوافرد	تألیف
: اول - ۱۴۰۲	نوبت و سال چاپ
: ۱۰۰۰	شمارگان
: ۹۷۸-۶۰۰-۴۱۰-۶۵۱-۱	شابک
: ۱۱۰۰۰۰ تومان	قیمت

فروشگاه مرکزی: تهران، میدان انقلاب، خ منیری جاوید(اردیبهشت شمالی)، پلاک ۸۸

تلفن مرکز پخش: ۶۶۴۹۲۳۲۷ - تلفن فروشگاه کتاب: ۶۶۴۰۲۳۵۳

پست الکترونیک: nashr.chatr@gmail.com

کلیه حقوق برای مؤلف و ناشر محفوظ است.

## سخن ناشر

رشته‌ی حقوق با تمام شاخه‌ها و گرایش‌هایش، به‌منزله‌ی یکی از پرطرفدارترین رشته‌های دانشگاهی کشور، تعداد فراوانی از دانشجویان علوم انسانی را به‌خود جلب کرده است؛ دانشجویانی که پس از تحصیل، وارد عرصه‌ی خدمت شده و در مناصب و جایگاه‌های گوناگون به ایفای وظیفه مشغول می‌شوند.

منابعی که در دانشکده‌های حقوق، مبنای کار قرار گرفته و تحصیل دانشجویان بر مدار آن‌ها قرار دارد، در واقع، مجموعه‌ی کتب و جزواتی هستند که طی سالیان متممادی چنان‌که باید تغییر نیافته و خود را با تحولات و نیازهای زمانه هماهنگ نکرده‌اند.

این، درحالی است که نیاز مبرم دانش‌پژوهان به مجموعه‌های پربار و سودمند، امری انکارناپذیر است. به‌این‌ترتیب، ضرورت تدوین کتب غنی و ارزشمند برای رفع نیازهای علمی دانشجویان رشته‌ی حقوق و نیز رشته‌های متأثر از آن، باید بیش از گذشته مورد توجه قرار گیرد؛ کتاب‌هایی که روزآمدی محتوای آن‌ها از یک سو و تناسب آن‌ها با نیاز دانش‌پژوهان از سوی دیگر، مورد توجه و لحاظ ناشر و نویسنده، قرار گرفته باشد.

**مؤسسه‌ی آموزش عالی آزاد چتردانش**، در مقام مؤسسه‌ای پیشگام در امر نشر کتب آموزشی روزآمد و غنی، توانسته است گام‌های مؤثری در همراهی با دانشجویان رشته‌ی حقوق بردارد. این مؤسسه افتخار دارد که با بهره‌مندی از تجربیات فراوان خود و با رصد دقیق نیازهای علمی دانشجویان، به تولید آثارى همت گمارد که مهم‌ترین دستاورد آن‌ها، تسهیل آموزش و تسریع یادگیری پژوهندگان باشد. انتشارات چتر دانش امیدوار است با ارائه‌ی خدمات درخشان، شایستگی‌های خود را در این حوزه‌ی علمی بیش از پیش به منصه‌ی ظهور برساند.

**فرزاد دانشور**

**مدیر مسئول انتشارات چتر دانش**

فصل اول: مفاهیم و مبانی نظری ۱۳

- ۱۵..... مبحث اول: مفهوم شناسی
- ۱۵..... گفتار اول: مفهوم و ویژگی‌های امنیت ملی
- ۱۵..... بند اول: مفهوم امنیت ملی:
- ۱۸..... بند دوم: ویژگی‌های امنیت
- ۱۸..... الف) نسبی بودن امنیت
- ۱۸..... ب) ذهنی بودن امنیت
- ۱۹..... ج) جامع بودن امنیت:
- ۱۹..... گفتار دوم: مفهوم، ویژگی‌های جرائم سایبری و بازشناسی آن از مفاهیم مشابه
- ۲۰..... بند اول: تعریف جرائم سایبری
- ۲۰..... الف) رایانه موضوع جرم:
- ۲۰..... ب) رایانه واسطه جرم:
- ۲۰..... ج) جرائم محض رایانه‌ای:
- ۲۱..... بند دوم: بازشناسی جرائم سایبری از مفاهیم مشابه
- ۲۱..... الف) جرائم رایانه‌ای و جرائم سایبری
- ۲۳..... ب: جرائم سایبری و فناوری اطلاعات
- ۲۴..... ج: جرائم رایانه‌ای و جرائم مالتی مدیا (چندرسانه‌ای)
- ۲۵..... مبحث دوم: سیر تاریخی و اقسام نظری جرائم سایبری
- ۲۵..... گفتار اول: تاریخچه و چهارچوب نظری در پیدایش جرائم سایبری
- ۲۵..... بند اول: از منظر بین‌المللی
- ۲۷..... بند دوم: از منظر حقوق ایران
- ۲۹..... گفتار دوم: ویژگی‌های جرائم سایبری:
- ۲۹..... بند اول: بین‌المللی بودن:
- ۳۰..... بند دوم: حجم و وسعت ضرر و خسارات وارده:
- ۳۱..... بند سوم: ناشناخته بودن بزهکار:
- ۳۱..... بند چهارم: پیچیدگی خاص
- ۳۲..... بند پنجم: درونی بودن جرم سایبری
- ۳۲..... بند ششم: تخصصی بودن:
- ۳۳..... بند هفتم: ضعف یا فقدان کنترل اجتماعی

بند هشتم: نحوه‌ی تعقیب و رسیدگی به جرائم سایبری: .....	۳۳
گفتار سوم: طبقه‌بندی جرائم سایبری .....	۳۴
بند اول: طبقه‌بندی جرائم در حقوق بین‌الملل .....	۳۵
الف: طبقه‌بندی شورای اروپا: .....	۳۵
۱- لیست حداقل .....	۳۵
۲- لیست اختیاری .....	۳۵
ب) طبقه‌بندی اینترنتی .....	۳۵
ج) طبقه‌بندی در کنوانسیون جرائم سایبرنتیک .....	۳۶
بند دوم: طبقه‌بندی جرائم سایبری در ایران: .....	۳۶
۱- جرائم کلاسیک با توصیف سایبری .....	۳۶
۲- جرائم علیه محرمانه بودن داده‌ها و سیستم‌ها .....	۳۷
۳- جرائم علیه صحت و تمامیت داده‌ها و سیستم‌ها .....	۳۷
۴- جرائم مرتبط با محتوا .....	۳۷

### فصل دوم: بررسی جرائم علیه امنیت ملی در فضای سایبری ۳۹

مبحث اول: جرائم علیه امنیت در قانون مجازات اسلامی .....	۴۱
گفتار اول: تبیین جرائم علیه امنیت در قانون مجازات اسلامی .....	۴۱
گفتار دوم: مصادیق جرائم علیه امنیت کشور در قانون مجازات اسلامی .....	۴۳
مبحث دوم: مصادیقی از جرائم علیه امنیت ملی در فضای سایبری .....	۴۳
گفتار اول: جرم جاسوسی سایبری .....	۴۳
بند اول: مفهوم جاسوسی سایبری .....	۴۴
بند دوم: تفاوت جاسوسی سنتی و جاسوسی سایبری .....	۴۵
بند سوم: عناصر حقوقی جاسوسی سایبری .....	۴۷
الف - عنصر قانونی جاسوسی سایبری: .....	۴۷
ب) عنصر مادی .....	۴۸
عنصر مادی جرم مذکور در ماده ۶۴ قانون تجارت الکترونیک، عبارت است از: .....	۴۸
ج) عنصر معنوی .....	۴۸
گفتار دوم: جعل سایبری .....	۴۹
بند اول: مفهوم جعل سایبری .....	۴۹
بند دوم: عناصر جرم جعل سایبری: .....	۵۰
گفتار سوم: خیانت به کشور .....	۵۳
بند اول: تبلیغ علیه نظام .....	۵۴

- الف: مفهوم شناسی تبلیغ علیه نظام ..... ۵۵
- ب: عناصر جرم تبلیغ علیه نظام: ..... ۵۷
- بند دوم: جرم تهدید به بمب‌گذاری: ..... ۶۱
- الف: مفهوم شناسی جرم تهدید به بمب‌گذاری ..... ۶۱
- ب: عناصر جرم تهدید به بمب‌گذاری: ..... ۶۲
- بند سوم: جرم تحریک نیروهای نظامی به عصیان، فرار و تسلیم ..... ۶۲
- بند چهارم: تشکیل یا اداره جمعیت به قصد برهم زدن امنیت یا عضویت در این گروه‌ها ..... ۶۳
- بند پنجم: تخریب سایبری به قصد برهم زدن امنیت: ..... ۶۸

## فصل سوم: پیشگیری از جرائم علیه امنیت ملی در فضای سایبری ۷۱

- مبحث اول: مفاهیم و اقسام پیشگیری از بزهکاری ..... ۷۳
- گفتار اول: معنای لغوی و اصطلاحی پیشگیری از بزهکاری ..... ۷۳
- بند اول: مفهوم لغوی پیشگیری ..... ۷۳
- بند دوم: مفهوم اصطلاحی پیشگیری از بزه کاری ..... ۷۳
- ب: مفهوم مضیق پیشگیری ..... ۷۴
- گفتار دوم: اقسام پیشگیری از بزهکاری ..... ۷۵
- بند اول: مفهوم و اقسام پیشگیری اجتماعی ..... ۷۶
- الف) مفهوم پیشگیری اجتماعی ..... ۷۶
- ب) اقسام پیشگیری اجتماعی ..... ۷۷
- ۱- پیشگیری اجتماعی جامعه مدار ..... ۷۷
- ۲- پیشگیری اجتماعی رشد مدار ..... ۷۸
- مبحث دوم: پیشگیری از جرائم سایبری ..... ۸۰
- مبحث سوم: وظایف پلیس در پیشگیری از جرایم سایبری ..... ۸۱
- گفتار اول: پیشگیری اجتماعی از جرائم و انحرافات سایبری ..... ۸۱
- بند اول: ویژگی‌های بزهکاران و بزه دیدگان سایبری از دیدگاه پیشگیری اجتماعی ..... ۸۱
- الف: سرگرمی و تفریح ..... ۸۱
- ب: کسب منافع مالی ..... ۸۲
- ج) انتقام، اعتقادات یا گرایش‌های مختلف: ..... ۸۲
- د) انگیزه‌های جنسی ..... ۸۳
- بند دوم: راهکارهای پیشگیری اجتماعی جرائم و انحرافات سایبری ..... ۸۴
- الف - اقدامات مداخله آمیز والدین ..... ۸۴
- ب) آموزش سلامت اینترنت ..... ۸۴

- ج) تدابیر کاربری صحیح ..... ۸۵
- گفتار دوم: پیشگیری وضعی از جرائم سایبری ..... ۸۵
- بند اول: تدابیر محدودکننده یا سلبکننده دسترسی: ..... ۸۷
- بند دوم: تدابیر نظارتی ..... ۸۸
- بند سوم: تدابیر صدور مجوز ..... ۸۸
- بند چهارم: ابزارهای ناشناس و رمزگذاری ..... ۸۹
- مبحث سوم: وظایف پلیس در پیشگیری از جرائم سایبری: ..... ۸۹
- گفتار اول: پیشگیری از جرائم سایبری پلیس ایران و پلیس بین‌الملل ..... ۹۰
- گفتار دوم: نقش پلیس در کشف جرائم سایبری ..... ۹۳



## مقدمه

انسان اشرف مخلوقات خداوند است که از جانب او به قدرت تفکر آراسته شده است بدین سبب از لحظه خلق نخستین انسان تا عصر حاضر برهه‌ای از تاریخ را نمی‌توان یافت که جوامع بشری از مواهب این نعمت آسمانی برخوردار نبوده باشند و یک شیوه فکری جدید یا یک ابزار فنی جدید ایجاد نشده باشد. در این میان برخی از این نوآوری‌ها؛ تحولات اساسی را در اجتماعات بشری سبب شده است.

گاه مکاتب جدید فکری بنیان‌های اجتماع را تحت تأثیر قرار داده‌اند و گاه اختراعات مهم شیوه زندگی انسان‌ها را متحول کرده است. پس از «انقلاب صنعتی»<sup>۱</sup> که با بهره‌گیری از ابزارهای صنعتی پیشرفته در امر تولید کالا؛ تحولات شگرفی در سطح دنیا به دنبال داشت و «عصر صنعتی»<sup>۲</sup> را رقم زد؛ اکنون نوبت «انقلاب اطلاعات»<sup>۳</sup> است که با استفاده از ابزارهای الکترونیکی پیشرفته در امر انتقال اطلاعات؛ تحولات شگرف دیگری را موجب گردید و «عصر اطلاعات»<sup>۴</sup> را رقم زند. مهم‌ترین نمود این عصر ایجاد «جامعه اطلاعاتی جهانی»<sup>۵</sup> در یک دنیای مجازی با همه کارکردهای دنیای واقعی، اما فارغ از محدودیت‌های فیزیکی آن است که در لابه‌لای تاروپود «فناوری اطلاعات»<sup>۶</sup> شکل گرفته است.

در این دنیای مجازی یک فرد می‌تواند فارغ از محدودیت‌هایی چون مرزهای ملی، حاکمیت سیاسی، نظارت افراد و مراجع مختلف، زبان، ملیت، نژاد، جنسیت و ... از هرکجای دنیا و در هر زمان با دیگران ارتباط برقرار کند. دیدگاه‌های خود را منتقل کند و از دیدگاه‌های دیگران مطلع شود برای رفع نیازمندی‌های روزانه خود اقدام کند یا نیازمندی‌های دیگران را مرتفع سازد و بالاخره تمامی فعالیت‌های اجتماعی خود را به انجام برساند. این امر سبب شده است جوامع انسانی در همه ابعاد خود دچار چالش‌های جدیدی شود که چاره‌ای جز پشت سر گذاردن آن‌ها به بهترین وجه باقی

---

1- Industrial Revolution

2- Industrial Age

3- Information Revolution

4- Information Age

5- World Information Society

6- I.T Information Technology

نگذاشته است؛ چراکه نمی‌توان جلوی رشد روزافزون قابلیت‌های خیره‌کننده این دنیای مجازی و گرایش افراد جامعه جهانی به استفاده از آن‌ها در جهت تسهیل زندگی را سد نمود.

امروزه ما به‌روشنی خود را مواجه با فضایی می‌یابیم که نیازی به حضور رودررو<sup>۱</sup> و فیزیکی با طرف مقابل نداریم و وجود پاره‌ای از مطلوب‌ها، ارزش‌ها و خواسته‌ها و همچنین حاکمیت پاره‌ای از هنجارها و الزامات را در درون این فضا درک می‌کنیم که عموماً مستقل و بعضاً متفاوت از آنچه در جامعه کلاسیک بیرونی جریان دارد، می‌باشد. بنابراین می‌توانیم بشر امروز را غوطه‌ور در فضایی بدانیم که وصف اصلی آن تبادل اطلاعات است و او را در آستانه ورود به جامعه اطلاعاتی ببینیم و بر این اساس دغدغه‌ها و مطلوب‌های او (به‌ویژه دغدغه‌ها و مطلوب‌های امنیتی) را بازیابی کنیم.

در این میان نیز جرم رایانه‌ای مسیری متحول و درعین حال سریع را در عرض پنج دهه اخیر طی کرده است. بدین معنا که از دهه‌ای به دهه دیگر هم نحوه ارتکاب جرم، هم هدف حمله مرتکب جرم و هم برخی موارد دیگر بعضاً یا کاملاً دگرگون شده است. این مسیر سریع است، زیرا مبدأ و منشأ آن پیشرفت سریع را پشت سر می‌گذارد.

از سال ۱۹۵۰ به بعد رایانه و تکنولوژی اطلاعات با سرعت افسارگسیخته‌ای روزبه‌روز جلوتر آمده و به همین سرعت راه خود را طی می‌کند. این سرعت تبعات مختلفی در زمینه‌های گوناگون اقتصادی، اجتماعی و فرهنگی به دنبال دارد به تبع این پیامدها قواعد و فرم‌های مدنی - جزایی نیز دستخوش تنوع و دگرگونی شده است و چون هنوز سیر حرکت سریع تکنولوژی و اطلاعات و رایانه ادامه دارد، حقوق‌دانان مخصوصاً در زمینه حقوق جزا نتوانسته‌اند به سامان و غایت موردنظر دست یابند و هر زمان با قاعده‌ای یا تغییر روندی درگیر هستند؛ نمونه‌ای از این عدم سامان‌یافتگی را در اختلافات مندرج در تعریف جرم رایانه‌ای، ماهیت متحول و گوناگون آن و نحوه ارتکاب جرم می‌توان یافت وقتی در اصل پدیده از حیث تعریف و ماهیت اختلاف است، مسلماً در مورد مصادیق و اجزای آن اختلافات تجلی بیشتری خواهد یافت.

جرائم رایانه‌ای اولاً بر ماهیت جرائم ارتكابی ثانیاً بر توصیف جرائم ارتكابی و ثالثاً بر عناصر متشکله این جرائم آثار جالب و مهمی گذارده است. جرم رایانه‌ای ماهیتاً جرائم کلاسیک را با تحول روبرو کرده است. این جرائم دارای ماهیتی تکنیکی یا به عبارت دیگر دارای ماهیت ناشی از پیشرفت تکنولوژی مدرن هستند. همین ماهیت تکنیکی بر تفسیر و برخورد با جرم تأثیر می‌گذارد.

از این تحقیقات مقدماتی در جرائم سایبری همچون تحقیقات در جرائم سنتی دارای یک سلسله قواعد، آثار و دربردارنده برخی حقوق، تکالیف و ارزش است که سایر قواعد و مقررات حقوقی تفسیر می‌شود و البته وصف فرازمانی و فرامکانی بودن این پدیده به مفهوم فراقانونی بودن آن نیست. در جریان تحولات ناشی از عنصر فناوری اطلاعات و ایجاد شیوه‌های جدید برای انجام تحقیقات مقدماتی، روش‌های ارتكاب جرائم نیز در این حوزه متحول شده است. تغییر در روش ارتكاب جرائم، متولیان حوزه قانون‌گذاری را به سمت تجدیدنظر در محدوده‌های تعریف و توصیف جرائم و به عبارتی جرم‌انگاری‌های جدید سوق داده است تا از این طریق و با استفاده از ابزارهای حقوقی و به‌ویژه حقوق کیفری، پاسخ‌های مناسب را برای نقض حقوق و ارزش‌های تحول‌یافته در حوزه سایبری سازماندهی نمایند.

اسناد بین‌المللی و قوانین موضوعه‌ای که در بسیاری از کشورها و در زمینه‌های مرتبط با چگونگی تحقیقات مقدماتی تنظیم شده‌اند همگی شاهی برای مدعا تلقی می‌شوند. بررسی اسناد و دستورالعمل‌های مختلفی که پارلمان و شورای وزیران اتحادیه اروپا در حوزه جرائم سایبری تدوین کرده است، نشان می‌دهد که امروزه جهت‌گیری سیاست مبانی این نهاد و به تبع آن کشورهای عضو به سمت احصاء موقعیت‌های مسئله‌آفرین در این حوزه حرکت می‌کند و اولین گزینه‌ای که شورا در پی ترویج آن است، تقویت سازوکارهای فنی است که امکان ظهور و بروز انواع سوءاستفاده‌ها و جرائم سایبری را به کمترین سطح برساند.

۱- قانون‌گذار داخلی نیز با الهام از رویه بین‌المللی در این زمینه و با بهره‌گیری از اسناد و متون فوق‌اولین حرکت جدی خود را با وضع مقررات قانون تجارت الکترونیکی جمهوری اسلامی ایران و تقدیم لایحه رایانه‌ای به مجلس باهدف

روزآمدسازی نظام حقوقی و انطباق آن با شرایط و مقتضیات عصر فناوری اطلاعات تدوین نموده است. از جمله ویژگی‌های لایحه جرائم رایانه‌ای اشاره شده این است که لایحه به لحاظ ساختار با رعایت اصول کنوانسیون‌های بین‌المللی جرائم سایبری تدوین شده است. بررسی ادبیات این مقررات حاکی از تأثیر فراوان متون و اسناد بین‌المللی بر طرز تلقی قانون‌گذار از فضای سایبری و مسائل مرتبط با آن است و آثار یک تقلید تمام‌عیار در سبک قانون‌نویسی و انشاء مطالب به چشم می‌خورد. با این حال به نظر می‌رسد وجود چنین قوانینی و لوایحی با وجود ایرادات آشکار و نهانی که دارد بهتر از فقدان آن است و ابتکار قانون‌گذار در خصوص تدوین مقرراتی که مقالات و مبادلات الکترونیکی را که در عنصر فناوری‌های اطلاعات و ارتباطات ناگزیر از آن هستیم، قابل تقدیر است.<sup>۱</sup>

در پژوهش حاضر به بررسی جرائم علیه امنیت عمومی در جرائم سایبری پرداخته‌ایم. با توجه به اینکه به کارگیری فناوری اطلاعات و ارتباطی نوین چالش‌های حقوقی فراوانی را از حیث چگونگی تأمین امنیت فضای تبادل اطلاعات پیش کشیده است. به دلیل آنکه از یک سو ماهیت و جنس فعالیت‌های کاربران در عرصه‌های مختلف این فضا با یکدیگر متفاوت و از سوی دیگر مطلوب‌ها و بایسته‌های امنیتی و همچنین نوع و گستره مخاطرات امنیتی در هر یک از این عرصه‌ها با یکدیگر تفاوت‌هایی دارد. بنابراین شناسایی مؤلفه‌های فضایی تبادل اطلاعات که ممکن است امنیت آن‌ها را در معرض خطر قرار گیرد و همچنین مطلوب‌های در معرض خطر (هدف امنیتی) در هر یک از حوزه‌های فضای تبادل اطلاعات و نهایتاً انواع تخلفات؛ راهکارها و ابزارهای حقوقی کشف پیشگیری، سزا دهی ضروری است.<sup>۲</sup>

۱- زندی، محمدرضا، تحقیقات مقدماتی در جرائم سایبری، انتشارات جنگل، ۱۳۸۹، ص ۲۸

۲- همان، ص ۲۸

# فصل اول:

مفاهیم و مبانی نظری



شناخت و تعیین دقیق حدود و قلمرو بحث مستلزم شناخت مفاهیم و واژه‌ها و اصطلاحات مورداستفاده است. به بیان دیگر تعریفی ساده، روشن و مختصر از واژگان اساسی پژوهش اهمیت بسزایی در شناخت حیطه و حدود رساله دارد. بر همین اساس در فصل اول این پژوهش، قبل از ورود به مباحث اصلی، مفاهیم و واژگان اساسی پژوهش یعنی جرم سایبری و جرم علیه امنیت ملی را تعریف و شناسایی می‌کنیم.

### **مبحث اول: مفهوم شناسایی**

در این مبحث به تعریف و شناسایی مفاهیم اولیه موجود در پژوهش موردنظر همچون امنیت ملی، فضای سایبر و جرائم سایبری می‌پردازیم

### **گفتار اول: مفهوم و ویژگی‌های امنیت ملی**

مفهوم امنیت قدمتی به وسعت تاریخ بشر و از جهتی بر مفهوم «اجتماع» و «جامعه» تقدم دارد این مفهوم به تدریج و با توسعه بشری تحول و ابعاد تازه‌ای یافته است به گونه‌ای که امروز امنیت را در توسعه و نه (اسلحه) سراغ می‌گیرند. تأمین امنیت به عنوان اساسی‌ترین وظیفه حکومت برشمرده است قرآن به عنوان قانون اساسی و دستورالعمل حیات معقول انسان و جامعه انسانی نیز به این امر توجهی خاص داشته و بر آن در تأمین سعادت دنیا و آخرت انسان تأکید کرده است. در این گفتار ابتدا به تبیین مفهوم امنیت ملی می‌پردازیم و سپس ویژگی‌های آن را برمی‌شماریم.

### **بند اول: مفهوم امنیت ملی:**

مفهوم امنیت مانند سایر مفاهیم اساسی و رایج در علوم انسانی نظیر صلح، عدالت و آزادی در معرض تفسیرها و تعبیرهای گوناگونی قرار دارد و در طول تاریخ بشری با تغییر و تحولات گسترده‌ای مواجه شده است و مکاتب متعددی نظریات خود را پیرامون این مفهوم ارائه کرده‌اند. برخی آن را برابر با رهایی از تهدید تعریف می‌نمایند و معتقدند امنیت در نبود مسئله دیگری به نام تهدید درک می‌شود<sup>۱</sup>

---

۱- عبدالله خانی، علی، نظریه‌های امنیت مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی، موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، چاپ نخست، تهران، ۱۳۸۳، ص ۱۳۵

برخی دیگر امنیت در یک مفهوم عینی به فقدان تهدیدها نسبت به ارزش‌های اکتسابی تلقی می‌شود و در یک مفهوم ذهنی بر اساس دلهره و نگرانی از به مخاطره افتادن ارزش‌ها و توانمندی‌های لازم در کسب نتایج منصفانه ارزیابی می‌شود<sup>۱</sup>

همان‌گونه که دیده می‌شود مفهوم امنیت دارای پیچیدگی و ابهام‌های بسیاری می‌باشد. از سوی دیگر، امنیت صرفاً در یک قلمرو یا محدوده خاص قابل پیگیری و دستیابی نیست بلکه امنیت در قلمروهای مختلف که در عین حال به هم پیوسته و وابسته و دارای تأثیرات متقابل نسبت به یکدیگر می‌باشند، قابل پیگیری و تحلیل است. قلمروهای گوناگون امنیت عبارت است از امنیت فردی، ملی، منطقه‌ای و بین‌المللی که از نظر معنی لغوی و اهداف، هر کدام از این اصطلاحات ترکیبی، گسترده و دامنه‌ی ویژه‌ای از مفهوم امنیت را در سطوح فردی، ملی، بین‌المللی و جهانی به ذهن انسان متبادرمی سازند. قطعاً امنیت، در تمامی الگوهای یادشده، مفهومی مشخص و یکسان دارد، لیکن آنچه در این جملات متفاوت است، گستره و دامنه امنیت و کیفیت تحقق آن می‌باشد که از سطح امنیت فردی تا سطوح امنیت ملی، بین‌المللی و جهانی را شامل می‌شود و تحقق هر یک از آنها نیز مستلزم پیروی از الگوی ویژه‌ای است که این امر نمی‌تواند به منزله‌ی وجود ابهام در مفهوم واژه‌ی امنیت باشد.<sup>۲</sup>

گر چه کاربرد واژه امنیت در قانون اساسی جمهوری اسلامی ایران ناچیز است اما محتوای بسیاری از اصول قانون اساسی در ارتقای تأمین امنیت عمومی است.

مواردی که به واژه امنیت صراحتاً اشاره شده است عبارت است از:

۱- چگینی زاده، غلامعلی، رویکردی نظری به مفهوم امنیت ملی در جهان سوم، مجله سیاست خارجی،

سال ۱۴، شماره ۱، ص ۶۸

۲- تهامی، مجتبی، امنیت ملی، دکترین، سیاست‌های دفاعی و امنیتی، کانون پژوهش‌های دریای پارس: ۱۳۹۰، ص ۵۵



۱- اصل سوم، بند ۱۴: تأمین امنیت قضایی عادلانه  
 ۲- اصل ۱۶۹ (رعایت امنیت کشور در تشکیل جلسات غیرعلنی)  
 ۳- فصل ۱۳ (شورای عالی امنیت شامل بندهای ۱ و ۲ اصل ۱۷۶ در خصوص تعیین سیاست‌های دفاعی - امنیتی کشور و نیز هماهنگ نمودن کلیه فعالیت‌های در ارتباط با تدابیر کلی دفاعی - امنیتی به‌عنوان وظایف شورا و نیز تشکیل شورای امنیت کشور به‌عنوان یکی از شوراها فرعی شورای عالی امنیت ملی<sup>۲</sup>

۲- به‌هرحال جایگاه امنیت در سلسله‌مراتب نیازها و انگیزه‌های آدمیان، جایگاه خطیری است. بحث ما در اینجا امنیت ملی می‌باشد. مفهوم اصلی «امنیت ملی» برای بسیاری از کشورها حاکی از نیاز به حفظ استقلال و تمامیت ارضی، حفظ شیوه‌ی زندگی ملی و جلوگیری از مداخله بیگانگان در امور داخلی کشورهاست. پس امنیت ملی یک کشور در درجه‌ی اول به معنای تأمین شرایطی است که کشور را از تعرض دیگران به استقلال سیاسی، ارزش‌های فرهنگی و رفاه اقتصادی دور نگه دارد. برطرف کردن عوامل ترس و ناامنی - چه داخلی و چه خارجی - از اساسی‌ترین هدف‌های یک کشور است.<sup>۳</sup>

به‌عبارت‌دیگر مراد از امنیت ملی، ایمن و درامان بودن نسبی تمامی نیازها و ارزش‌های حیاتی مردم در برابر تهدیدها و نیز ادامه‌ی روند روبه‌تزايد قدرت دولت در بستر زمان برای پاسخ‌گویی به انتظارات فزاینده تمامی افرادی است که ملت را تشکیل داده‌اند. بدیهی است سطح ملی امنیت از اهمیت و اولویت بیشتری در مقایسه با سطح فردی آن برخوردار است. در امنیت فردی، علایق و ارزش‌های یک فرد موردنظر است؛ در صورتی که امنیت ملی، علایق و ارزش‌های جمع‌کثیری از افراد

۱- مذاکرات مجلس شورای ملی باید علنی باشد و گزارش کاملان از طریق رادیو و روزنامه رسمی برای اطلاع عموم منتشر شود. در شرایط اضطراری، در صورتی که رعایت امنیت کشور ایجاب کند، به تقاضای رئیس‌جمهور یا یکی از وزراء یا ده نفر از نمایندگان، جلسه غیرعلنی تشکیل می‌شود. مصوبات جلسه غیرعلنی در صورتی معتبر است که با حضور شورای نگهبان به تصویب سه‌چهارم مجموع نمایندگان برسد. گزارش و مصوبات این جلسات باید پس از برطرف شدن شرایط اضطراری برای اطلاع عموم منتشر شود.

۲- مؤذن‌زاده جامی، محمدهادی، مقاله مقدمه‌ای بر امنیت و مؤلفه‌های آن، فصلنامه‌ی دانش انتظامی، شماره

۱۳۷۸، ص ۴۵

۳- روشندل، جلیل، امنیت ملی و نظام بین‌المللی، سمت، چاپ اول، تهران، ۱۳۷۴، ص ۱۸

را در قالب ملت دربرمی گیرد. امنیت فردی در جامعه ضرورتی حیاتی دارد و باید تأمین شود، ولی اولویت منافع جمعی بر منافع فردی نیز دارای ضرورتی انکارناپذیر است. بنابراین امنیت ملی برای هر کشوری به مفهوم وجود شرایطی نسبتاً پایدار است که علاوه بر امکان پاسخ‌گویی به نیازهای حیاتی مردم، در هرزمانی نیز تمامی نیازها، ارزش‌ها و منافع حیاتی آن کشور از خطر تهدیدهای گوناگون داخلی، خارجی و طبیعی در ابعاد نظامی، سیاسی، اقتصادی، اجتماعی، فرهنگی و زیست‌محیطی به‌طور نسبی درامان باشند.<sup>۱</sup>

### بند دوم: ویژگی‌های امنیت

امنیت یک موضوعی است که معیارهای آن از جامعه‌ای به جامعه‌ی دیگر فرق می‌نماید اما درهرحال در اکثریت جوامع دارای ویژگی‌های مشترکی است که در اینجا به شرح آن می‌پردازیم. ۴ ویژگی که به شرح آن می‌پردازیم بدین شرح است: نسبی بودن، ذهنی بودن، جامع و ذاتی بودن امنیت.

#### الف) نسبی بودن امنیت

امنیت پدیده‌ای ثابت و مشخص نیست بنابراین عامل زمان، ایدئولوژی، اوضاع و احوال بین‌المللی، موقعیت کشور و دید و نظر رهبران، نخبگان و مردم در کیفیت و کمیت امنیت و نحوه تحصیل و حفظ آن تأثیر بسزایی دارد. دولت‌ها برحسب مقام و موقعیتی که در عرصه مناسبات بین‌المللی دارند و نیز بر اساس مبانی ارزشی خود، تصورات و تلقی‌های متفاوتی از مفهوم امنیت دارند.<sup>۲</sup>

#### ب) ذهنی بودن امنیت

یکی دیگر از صفات مسلم امنیت ذهنی بودن آن است. ذهنی بودن امنیت را می‌توان ناشی از ۴ امر دانست:

الف- میزان اعتباری که نخبگان و تصمیم‌گیرندگان یک کشور برای نیروهای تهدیدکننده قائل می‌شوند

ب- میزان ارتباطی که آنان می‌توانند با عامل یا عوامل تهدیدزا برقرار کنند

۱- مؤذن‌زاده، پیشین، ص ۴۶

۲- مجموعه مقالات ارائه شده در همایش توسعه و امنیت عمومی، ۱۳۷۶، ص ۲۱

ج- میزان توانایی (محدودیت و مقدرات) خودی در مقابله با دیگری (تهدید)  
 د- میزان و درجه اعتبار، فوریت، اولویت و مرکزیت ارزش‌ها و منافع مورد تهدید.<sup>۱</sup>  
**ج) جامع بودن امنیت:**

یعنی هر حوزه‌ای را که برای اداره امور جامعه ضروری است، در برمی‌گیرد. امنیت فی‌الواقع عبارت است از: حالتی که فرد یا جامعه از تهدید و خطر مصون باشد و ناامنی حالتی است تهدیدآمیز که در معرض خطر بودن را القا می‌کند. خطر یا همان عاملی که وجودش سلب‌کننده امنیت است، هر عامل با وضعی را در برمی‌گیرد که مخل بر وجود و کمالات آن باشد (چه نابودکننده و چه کاهنده) و نیازها، کمبودها، نقصان‌ها و اختلاف‌ها را افزایش دهد و یا از اساس ایجاد کند. البته عوامل متعددی چون زمان، ایدئولوژی، اوضاع و احوال بین‌المللی، موقعیت کشور و دیدگاه رهبران در میزان امنیت و نحوه آسیب یا حفظ آن مؤثر است.

#### د) ذاتی بودن امنیت:

ذاتی هم به معنای عدم نیاز به علت و دلیل و هم به معنای ضروری و نیاز اولیه غیرقابل‌رفع و ویژگی ناگزیر و غیرقابل‌گریز، لذا امنیت یعنی مصونیت و نیاز به مصونیت و عامل مصونیت و مدافع مصونیت می‌باشد.

#### گفتار دوم: مفهوم، ویژگی‌های جرائم سایبری و بازشناسی آن از مفاهیم مشابه

پیوند و اتصال شبکه‌ی جهانی اینترنت، به‌روشنی گویای این واقعیت است که ویرانگری و آسیب‌رسانی می‌تواند در یک لحظه، سراسر جهان را فراگیرد. سوءاستفاده از فناوری‌های رایانه‌ای و اینترنتی می‌تواند امنیت ملی، آسایش عمومی و موجودیت یک جامعه را به مخاطره انداخته و تأثیرهای منفی بی‌شماری را بر زندگی افراد جامعه تحمیل کند. در این گفتار ابتدا به مفهوم جرائم سایبری و ویژگی‌های آن خواهیم پرداخت سپس جرائم سایبری را از جرائم مشابه، از یکدیگر بازشناسی می‌کنیم.

در ابتدای بحث می‌بایست در خصوص واژه‌ی رایانه و علل استفاده‌ی آن در این تحقیق توضیح مختصری ارائه شود. در حقیقت تکنولوژی رایانه را

۱- روزنامه‌ی جام جم، مؤلفه‌های امنیت، شماره ۲۵۳۶، در تاریخ ۲۹/۱/۸۸، ص ۱۰

باید مبنا و بستر تمامی جرائم و تخلفات سایبری و اینترنتی دانست. اینترنت یا شبکه‌ی جهانی را باید یکی از مظاهر فن‌آوری اطلاعات دانست که با پیدایش و گسترش رایانه‌های شخصی و امکانات وسیع ارتباطات راه دور شبکه‌ای و مخابراتی به منصفه‌ی ظهور رسید و این رسانه‌ی جهانی که اکنون بیش از ۶۰۰ میلیون نفر - و یا حتی بیشتر - کاربر دارد، موجب شده است که آمار بالایی از جرائم را در سطح منطقه‌ای و جهانی به خود اختصاص دهد. لذا در این پایان‌نامه باینکه جرائم سایبری مورد تحقیق و بررسی قرار می‌گیرد، جایگاه رایانه به‌عنوان زیربنای این عرصه تبیین می‌شود.

### بند اول: تعریف جرائم سایبری

جرم رایانه‌ای بر دو نوع است: در تعریف محدود (مضیق) جرمی که در فضای مجازی (سایبر) رخ می‌دهد جرم رایانه‌ای است و بر اساس این دیدگاه، اگر رایانه ابزار و وسیله ارتکاب جرم باشد آن جرم را نمی‌توان در زمره جرائم رایانه‌ای قلمداد کرد. در تعریف گسترده (موسع) هر فعل یا ترک فعلی که «از طریق» یا «به کمک سیستم‌های رایانه‌ای» رخ می‌دهند جرم رایانه‌ای قلمداد می‌شود. از این دیدگاه جرائم به ۳ دسته تقسیم می‌شوند:

#### الف) رایانه موضوع جرم:

در این دسته از جرائم رایانه و تجهیزات رایانه‌ای، موضوع جرائم سنتی (کلاسیک) مثل سرقت، تخریب تجهیزات و ... هستند.

#### ب) رایانه واسطه جرم:

رایانه وسیله و ابزار ارتکاب جرم است و از آن برای جعل مدرک، گواهینامه و ... استفاده می‌شود.

#### ج) جرائم محض رایانه‌ای:

دسته سوم جرائم محض جرمی مانند هک یا ویروسی کردن که صرفاً در فضای سایبر «مجازی» اتفاق می‌افتد.<sup>۱</sup>

۱- خرم‌آبادی، عبدالصمد، تاریخچه، تعریف و طبقه‌بندی جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، قوه قضاییه، معاونت حقوقی و توسعه قضایی، ۱۳۸۴، ص ۷۴