

به نام خدا

جرائم رایانه‌ای

مفاهیم، مصادیق، علل و روش‌های مقابله

مؤلف:

رشید تقوایی ابریشمی

با مقدمه

دکتر عباس شیخ الاسلامی

انتشارات ارسطو

(چاپ و نشر ایران)

۱۴۰۱

سرشناسه: تقوائی ابریشمی، رشید، ۱۳۷۳-
عنوان و نام پدیدآور: جرایم رایانه‌ای: جامع مباحث جرائم رایانه‌ای و جرائم حوزه
فضای مجازی/مؤلف رشید تقوائی ابریشمی.
مشخصات نشر: ارسطو (سامانه اطلاع رسانی چاپ و نشر ایران)، ۱۴۰۱.
مشخصات ظاهری: ۴۰۷ص.
شابک: ۹۷۸-۶۰۰-۴۳۲-۸۸۰-۷-۷
وضعیت فهرست نویسی: فیپا
یادداشت: کتابنامه.
عنوان دیگر: جامع مباحث جرائم رایانه‌ای و جرائم حوزه فضای مجازی.
موضوع: جرایم کامپیوتری Computer crimes
فضای مجازی Cyberspace
فضای مجازی -- ایران Cyberspace -- Iran
جرایم کامپیوتری -- قوانین و مقررات -- ایران
Computer crimes -- Law and legislation -- Iran
رده بندی کنگره: HV۶۷۷۳
رده بندی دیویی: ۳۶۴/۱۶۸
شماره کتابشناسی ملی: ۸۸۳۷۸۲۹
اطلاعات رکورد کتابشناسی: فیپا

نام کتاب: جرائم رایانه‌ای
مؤلف: رشید تقوائی ابریشمی
ناشر: ارسطو (سامانه اطلاع رسانی چاپ و نشر ایران)
تیراژ: ۱۰۰۰ جلد
نوبت چاپ: اول - ۱۴۰۱
چاپ: مدیران
قیمت: ۱۱۰۰۰۰ تومان
فروش نسخه الکترونیکی - کتاب‌رسان:
<https://chaponashr.ir/ketabresan>
شابک: ۹۷۸-۶۰۰-۴۳۲-۸۸۰-۷-۷
تلفن مرکز پخش: ۰۹۱۲۰۲۳۹۲۵۵
www.chaponashr.ir



ای عدالت، مراد زمره عاشقان خودبیز

وفیضی بخش تاسیامی تو را در پرده هر پندار و ریاز ستم باز شناسم

من نیز در برابر سراسر منطق را به پای تومی ریزم

و همه قوانین را به سوی تومی کشم

باشد که این معامله به هدایت اندیشه من و چیرگی تو بر لشکر ظلم انجامد.

«مرحوم دکتر کاتوزیان»

به نام خدا

ظهور و فراگیری فضای مجازی را می‌بایست مهمترین واقعه قرن اخیر دانست، فضایی که به تعبیر بسیاری از اندیشمندان تبدیل به فضای واقعی‌تر از فضای حقیقی شده است. این فرا محیط محصول تکنولوژی رایانه و سپس اتصال رایانه‌ها به یکدیگر و به تبع ایجاد شبکه ارتباطی است. شخصا معتقدم فضای مجازی و سایر تکنولوژی‌های تبعی در حال ظهور، نظیر هوش مصنوعی و رباتهای هوشمند و ... واقعیات عصر ارتباطات نوین هستند که نباید با دیدگاه منفی بدان نگریست تا مانعی بر تحولات مثبت و پویای این حوزه از فناوری نباشد.

همدوره‌های تحصیلی ما حتما به یاد دارند که معلمان ریاضی در آن دوره چگونه ماشین حساب را پدیده‌ای بر خلاف مصلحت دانش آموزان می‌دانستند و مخالف جدی استفاده از آن بودند و به تعبیری همراه داشتن آن در محیط‌های آموزشی قاچاق محسوب می‌شد، آن‌ها بر این باور بودند که این وسیله نوظهور شرور، مانعی جدی در حفظ جدول ضرب و ارتقاء حافظه دانش آموزان است که در نهایت ذهن‌ها را متوقف می‌سازد، ولی بر خلاف آنچه تصور می‌شد ماشین حساب به کلاسها راه یافت و ذهن هم از حفظ جدول ضرب عاجز نشد. دهها تکنولوژی دیگر از جمله همین فضای مجازی با همه موانع و مقاومت‌ها در دنیا پذیرفته و فراگیر شده‌است، به نحوی که اخلاص در آن موجب پیامدهای ناگواری از قبیل از دست دادن کسب و کارها و تعطیلی پژوهش‌ها و اختلال در حرکت هواپیماها، قطارها و ... می‌شود.

اما طبعا این فضا نکاتی منفی نیز دارد که نباید از آن غافل شد، چرا که این نوآوری نیز به تمثال یک چاقو می‌تواند جراحی کند و انسانی را از مرگ نجات دهد و در عین حال به قلب انسان مظلومی فرو رود و جانی را سلب کند.

آنچه مسلم است اینکه فضای مجازی به ذاته خبیث نیست و شرارت نمی‌کند، بلکه این انسانها هستند که می‌توانند این ابزار کاربردی و نافع را در مسیر شر و به نحو شرورانه به کار گیرند. این بهره‌برداری مجرمانه می‌تواند در قالب جرائم، تخلفات و انحرافات رایانه‌ای در طیف وسیعی (بخصوص جرائم علیه داده‌ها و جرائم محتوایی) تقسیم‌بندی و تحلیل شود. حقوق جزا با شناخت اصول حاکم بر این جرائم و نیز عناصر آن می‌تواند ابهامات موجود را برطرف و با نقاط سیاه این پدیده مقابله کیفی کند. علم جرم‌شناسی نیز با شناخت علل، عوامل و فرایندهای این پدیده مجرمانه می‌تواند بهترین شیوه‌های پیشگیری از این پدیده را ارائه نماید.

به طور خلاصه در ادامه تنازع خیر و شر، امروزه نمادهایی از این ستیزه در فضای مجازی نیز در جریان است و برای قضاوت در خصوص اینکه در نهایت کدامیک بر دیگری فائق خواهند آمد حاجت به مزی مدت بیشتری است، ولی طبعا امید اندیشمندان پیروزی نیکی بر بدی و کنترل منطقی این فضا است، به نحوی که در وهله اول آزادی‌های اساسی انسانها و کارکردهای مثبت متعدد این فضا تقویت و تثبیت گردد و در وهله دوم از جرائم، تخلفات و انحرافات این فضا پیشگیری گردد و در وهله سوم مرتکبین جرائم رایانه‌ای در حد استحقاق به سزای خود برسند.

جناب آقای رشید تقوایی ابریشمی، پژوهشگر و دانشجوی مقطع تحصیلات تکمیلی حقوق جزا و جرم‌شناسی که به عنوان کارشناس ارشد حقوقی متخصص در حوزه فضای مجازی، در نهاد تخصصی مقابله با جرائم رایانه‌ای (دادسرای ناحیه ۷ مشهد) نیز دارای تجربه و در خدمت دستگاه قضایی جمهوری اسلامی ایران بوده‌اند در این کتاب سعی نموده خوانندگان

را با اینگونه جرائم، مفاهیم و مبانی جرم‌انگاری، اصول حاکم، شناخت مصادیق آن و نهایتاً علل و عوامل و راهکارهای پیشگیری آشنا سازند و باب را برای مطالعه جزئی‌تر و عمیق‌تر در مفاهیم و نیز رویه قضایی باز کنند. اینجانب بر تلاش این محقق جوان که در آغاز راه دغدغه تولید علم در این مبحث مهم را دارد صحنه گذاشته و به خوانندگان عزیز مطالعه این کتاب را توصیه می‌کنم و امیدوارم حال که کلیاتی در خصوص موضوعات جرائم رایانه‌ای توسط محقق گردآوری شده‌است، در آینده شاهد تعدد آثاری جزئی‌تر و عمیق‌تر از این پژوهشگر فرهیخته باشیم.

عباس شیخ‌الاسلامی

دانشیار دانشکده حقوق و علوم سیاسی دانشگاه آزاد اسلامی واحد مشهد

پیشگفتار

جرائم رایانه‌ای در سالیان اخیر به صورت فراگیر و با سرعت قابل توجهی در حال گسترش است. آثار این دست جرائم اغلب با عنایت به خصوصیات آن، به مراتب زیان‌بارتر از معادل جرائم سنتی آن است، به عبارت دیگر جرم و جنایت تکنولوژی را در اختیار گرفته تا اهداف نامیمون خود را محقق سازد. بر همین اساس و به طبع در حوزه جرائم رایانه‌ای با طیف وسیعی از جرائم مواجه هستیم که این امر ضرورت سیاست‌گذاری اختصاصی و متناسب را مبرهن ساخته و راهبردی ایمن و فعالانه در مقیاس جرائم این حوزه را می‌طلبد. حساسیت این موضوع زمانی افزایش می‌یابد که متوجه گستره آثار جرائم رایانه‌ای در سطوح مختلف اقتصاد (خرد و کلان)، فرهنگ و ... در یک جامعه باشیم، چراکه بی‌شک هدف آن برهم زدن توازن و تعادل زیست اجتماعی اعضای جامعه در قامت تضییع حقوق اشخاص است که این خود زمینه‌ساز وقوع گستره قابل توجهی از انواع جرائم است. آنچه در صدر اولویت‌های سیاست‌گذاری هر جامعه در قبال جرائم می‌توان یاد کرد، سیاست جنایی و کیفری آن جامعه است. سیاست کیفری اجرایی، اقدامات و تدابیری است که ارکان یک حکومت در مقام مواجهه و مقابله با جرائم اتخاذ می‌نمایند. جمهوری اسلامی ایران در حوزه جرائم رایانه‌ای مسیری متناسب را در پیش گرفته، ولیکن به نظر می‌رسد

آن گونه که می‌بایست، پیش نرفته‌است. فقدان راهبری مقتدر و راهبردی واحد و موثر در حوزه جرائم رایانه‌ای به‌نظر نقیصه اصلی این حوزه در جمهوری اسلامی ایران است. قوانین حاضر تکافوی تعمیم به جرائم این حوزه را نمی‌کند و از طرفی اختصاصاً در این دست جرائم ابتکار عمل با مجرمین بوده و مسیر ارتکاب و تحقق جرم را آنان معین می‌کنند، گرچه توفیقاتی نیز در مقابله با این دست جرائم بوده است، اما ناکافی است. ارکان نظام جمهوری اسلامی ایران می‌توانند حسب وظیفه با بهره‌گیری از ظرفیت‌های علمی و عملی داخلی و با امعان در تدابیر و سیاست‌های کشورهای موفق در حوزه مقابله با جرائم رایانه‌ای، فضایی ایمن و جذاب، و بستری مناسب برای ارتباطات و تجارت الکترونیکی در کشور عزیزمان فراهم سازند، بی‌تردید امروزه این مهم برابر سیاست‌های حوزه فضای مجازی و موافق راهبرد فراگیری جهانی ارتباطات رایانه‌ای، محیطی امن، پویا و موفق را با رویکرد تعالی زیست اجتماعی اسلامی و در تراز کشورهای موفق این حوزه به ارمغان خواهد آورد. درواقع نظم‌گریزی حال حاضر در فضای مراودات رایانه‌ای، زینده هیچ جامعه‌ای و اخص ایران عزیزمان نیست، فلذا قانون‌گذاری متناسب و اجرای صحیح قوانین، تقویت سیستم قضائی و نیروی انتظامی تخصصی، آموزش و آگاه‌سازی عمومی، پیشگیری موثر از بروز زمینه‌های ارتکاب و اصل وقوع جرائم رایانه‌ای، تعامل و همگام‌سازی سیاست‌های داخلی با نظامات بین‌المللی و ... می‌تواند نقش موثری در بهبود این حوزه ایفا نماید.

فهرست مطالب

صفحه	عنوان
۲۷.....	بخش اول
۲۷.....	فصل اول
۲۸.....	مقدمه
۲۸.....	مبحث اول: شرح مختصر موضوع
۳۵.....	مبحث دوم: اهمیت موضوع
۳۵.....	بیشتر بدانیم: چند نکته
۳۷.....	بیشتر بدانیم: تالیفات مرتبط
۳۹.....	فصل دوم
۳۹.....	مفاهیم، مبانی، پیشینه و درآمدی بر جرائم رایانه‌ای
۴۰.....	مبحث اول: جرائم رایانه‌ای
۴۱.....	گفتار اول: فضای مجازی (سایبر)
۴۱.....	گفتار دوم: داده پیام
۴۲.....	مبحث دوم: ویژگی‌های جرائم رایانه‌ای
۴۳.....	گفتار اول: امکان بی‌هویتی و جعل هویت
۴۴.....	گفتار دوم: نقض محدودیت‌های زمانی و مکانی
۴۴.....	گفتار سوم: گستردگی، تنوع و تعدد فرصت‌ها
۴۵.....	گفتار چهارم: ازدیاد سرعت و سهولت ارتکاب
۴۶.....	گفتار پنجم: ماهیت بین‌المللی (فرامرزی)
۴۶.....	گفتار ششم: ضعف نظارت و کنترل

- ۴۷..... گفتار هفتم: کم‌هزینگی
- ۴۸..... گفتار هشتم: بالا بودن رقم سیاه
- ۴۹..... گفتار نهم: اتوماتیک‌بودن
- ۵۰..... گفتار دهم: ناملموس و درونی بودن بزه
- ۵۱..... مبحث سوم: انواع جرائم سایبری
- ۵۴..... مبحث چهارم: مجرمین رایانه‌ای
- ۵۵..... گفتار اول: هکرها
- ۵۶..... گفتار دوم: کرکرها(هکرها) کلاه سیاه)
- ۵۷..... گفتار سوم: واکرها(هکرها) کلاه خاکستری)
- ۵۷..... گفتار چهارم: سایر مجرمین رایانه‌ای
- ۵۸..... گفتار پنجم: معاونت در ارتکاب جرائم رایانه‌ای
- ۵۹..... مبحث پنجم: محیط سایبر (فضای مجازی)
- ۵۹..... گفتار اول: تعریف محیط سایبر
- ۶۰..... مبحث ششم: چالش‌های پیش‌روی محیط سایبر(فضای مجازی) در ایران
- ۶۲..... مبحث هفتم: ویژگی‌های فضای مجازی
- ۶۲..... گفتار اول: سرعت و سهولت دسترسی
- ۶۳..... گفتار دوم: دقت، هوشمندی و فراست
- ۶۴..... گفتار سوم: انعطاف و پیشرفت
- ۶۴..... گفتار چهارم: گستردگی
- ۶۵..... گفتار پنجم: ماهیت محیط
- ۶۶..... مبحث هشتم: پیکره فضای مجازی و رایانه‌ای
- ۶۷..... گفتار اول: مخازن اطلاعات
- ۶۷..... گفتار دوم: سیستم‌های ارتباطی
- ۶۸..... گفتار سوم: ارائه‌دهندگان خدمات شبکه‌ای
- ۶۸..... مبحث نهم: عوامل جرم‌زا در وقوع جرائم رایانه‌ای

- گفتار اول: عوامل اقتصادی ۶۹
- گفتار دوم: عوامل فرهنگی و اجتماعی ۷۲
- گفتار سوم: عوامل فردی ۷۳
- گفتار چهارم: عوامل محیطی ۷۶
- مبحث دهم: مزیت‌ها و محدودیت‌های فضای مجازی ۷۷
- گفتار اول: در حوزه آزادی اطلاعات ۷۷
- گفتار دوم: در حوزه حریم خصوصی ۷۸
- مبحث یازدهم: امنیت فضای مجازی ۷۹
- گفتار اول: پلیس فضای مجازی ۷۹
- گفتار دوم: پلیس فضای مجازی در ایران ۸۰
- مبحث دوازدهم: مصادیق تبدیل جرائم سنتی به جرائم رایانه‌ای ۸۲
- گفتار اول: جرائم تجاری ۸۲
- گفتار دوم: جاسوسی ۸۳
- گفتار سوم: تروریسم ۸۳
- گفتار چهارم: سابوتاژ ۸۵
- گفتار پنجم: پولشویی ۸۵
- گفتار ششم: خرید و فروش کالاهای ممنوعه ۸۶
- گفتار هفتم: قاچاق مواد مخدر ۸۷
- گفتار هشتم: جعل ۸۸
- گفتار نهم: افترا و نشر اطلاعات ۸۹
- گفتار دهم: جرائم ناظر بر کپی‌رایت و برنامه‌ها ۸۹
- مبحث سیزدهم: سیر تاریخی جرائم رایانه‌ای ۹۰
- گفتار اول: سیر تاریخی جرائم رایانه‌ای در نظام حقوق بین‌الملل ۹۰
- گفتار دوم: سیر تاریخی جرائم رایانه‌ای در حقوق جزای ایران ۹۳
- گفتار سوم: پیشینه تقنینی جرائم رایانه‌ای ۹۴

- مبحث چهاردهم: لزوم حفظ و افزایش امنیت فضای مجازی ۹۶
- گفتار اول: چالش‌ها و موانع اساسی فراروی امنیت در فضای مجازی ۹۷
- گفتار دوم: راه‌کارها و اقدامات مؤثر بر امنیت فضای مجازی ۹۹
- بخش دوم** ۱۰۳
- فصل اول** ۱۰۳
- جرم‌انگاری جرایم رایانه‌ای** ۱۰۳
- مبحث اول: مبانی نظری ۱۰۴
- گفتار اول: اصول عام جرم‌انگاری در فضای مجازی ۱۰۵
- بند اول: اصل مشروعیت جرم‌انگاری ۱۰۵
- بند دوم: اصل ضرورت ۱۰۷
- بند سوم: احترام به حریم خصوصی و رعایت موازین حقوق بشری ۱۰۸
- بند چهارم: اصل تناسب جرم و مجازات ۱۰۹
- گفتار دوم: اصول خاص جرم‌انگاری در فضای مجازی ۱۱۱
- بند اول: لزوم توجه به راهبردها، رویکردها و همکاری‌های بین‌المللی ۱۱۱
- بند دوم: لزوم توجه ویژه مقنن به اقشار آسیب‌پذیر در فضای مجازی ۱۱۲
- ۱- بانوان ۱۱۲
- ۲- کودکان ۱۱۳
- بند سوم: لزوم اتخاذ راهبردهای علمی و دانش‌بین‌رشته‌ای برای مقابله با جرایم رایانه‌ای ۱۱۵
- مبحث دوم: مسئولیت قانونی در فضای مجازی ۱۱۶
- گفتار اول: مسئولیت مدنی ۱۱۶
- گفتار دوم: مسئولیت کیفری ۱۱۷
- بیشتر بدانیم: مصادیق و مبانی قانونی محتوای مجرمانه ۱۲۲
- گفتار اول: مصادیق محتوای مجرمانه (موضوع ماده ۲۱ قانون جرایم رایانه‌ای) ۱۲۲
- الف) محتوا علیه عفت و اخلاق عمومی ۱۲۲

۱۲۳.....	ب) محتوا علیه مقدسات اسلامی.....
۱۲۳.....	ج) محتوا علیه امنیت و آسایش عمومی
۱۲۴.....	د) محتوا علیه مقامات و نهادهای دولتی و عمومی
۱۲۵.....	ه) محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود (محتوای مرتبط با جرائم رایانه‌ای).....
۱۲۶.....	و) محتوایی که تحریک، ترغیب، یا دعوت به ارتکاب جرم می‌کند (محتوای مرتبط با سایر جرائم).....
۱۲۷.....	ز) محتوای مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی
۱۲۸.....	ح) محتوای مجرمانه مرتبط با انتخابات مجلس شورای اسلامی و مجلس خبرگان رهبری
۱۳۰.....	ط) محتوای مجرمانه مرتبط با انتخابات ریاست جمهوری
۱۳۴.....	گفتار دوم: قوانینی که در فهرست مصادیق محتوای مجرمانه مورد استناد قرار گرفته‌اند
۱۳۴.....	الف) قانون مجازات اسلامی
۱۳۸.....	ب) قانون مطبوعات
۱۳۹.....	ج) قانون جرائم رایانه‌ای
۱۴۴.....	ه) قانون بازار و اوراق بهادار
۱۴۴.....	و) قانون جامع کنترل و مبارزه ملی با دخانیات (مصوب ۱۳۸۵)
۱۴۴.....	ز) قانون ممنوعیت به کارگیری تجهیزات دریافت ماهواره (مصوب ۱۳۷۳)
۱۴۵.....	ح) قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز دارند
۱۴۵.....	ط) قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای.....
۱۴۵.....	ع) قانون تجارت الکترونیکی
۱۴۶.....	ف) قانون انتخابات مجلس شورای اسلامی
۱۴۸.....	ک) آئین‌نامه قانون انتخابات مجلس شورای اسلامی
۱۴۸.....	ن) قانون انتخابات ریاست جمهوری
۱۵۲.....	م) آئین‌نامه قانون انتخابات ریاست جمهوری
۱۵۳.....	ی) قانون اخلال در نظام اقتصادی کشور
۱۵۷.....	فصل دوم
۱۵۷.....	مصادیق جرائم رایانه‌ای

- مبحث اول: جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی ۱۶۰
- گفتار اول: دسترسی غیرمجاز ۱۶۰
- بند اول: رکن مادی ۱۶۱
- ۱- موضوع جرم ۱۶۱
- ۲- رفتار مرتکب ۱۶۲
- بند دوم: رکن روانی ۱۶۳
- بند سوم: رکن قانونی ۱۶۳
- گفتار دوم: شنود غیرمجاز ۱۶۴
- بند اول: رکن مادی ۱۶۵
- ۱- موضوع جرم ۱۶۵
- ۲- رفتار مرتکب ۱۶۵
- بند دوم: رکن روانی ۱۶۶
- بند سوم: رکن قانونی ۱۶۶
- گفتار سوم: جاسوسی رایانه‌ای ۱۶۷
- بند اول: رکن مادی ۱۶۸
- ۱- موضوع جرم ۱۶۸
- ۲- رفتار مرتکب ۱۶۹
- بند دوم: رکن روانی ۱۷۰
- بند سوم: رکن قانونی ۱۷۱
- مبحث دوم: جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی ۱۷۳
- قسمت اول: جعل رایانه‌ای و استفاده از داده‌های مجعول ۱۷۳
- گفتار اول: جعل رایانه‌ای ۱۷۳
- بند اول: رکن مادی ۱۷۴
- ۱- موضوع جرم ۱۷۴
- ۲- رفتار مرتکب ۱۷۵

- بند دوم: رکن روانی ۱۷۸
- بند سوم: رکن قانونی ۱۷۹
- بند چهارم: عوامل جرم‌زای جعل داده‌ها و اسناد الکترونیکی ۱۸۱
- بند پنجم: پیشگیری از جعل داده‌ها و اسناد الکترونیکی ۱۸۲
- گفتار دوم: استفاده از داده مجعول ۱۸۲
- گفتار سوم: جعل هویت رایانه‌ای ۱۸۳
- قسمت دوم: تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی ۱۸۵
- گفتار چهارم: تخریب یا اخلال داده ۱۸۵
- بند اول: رکن مادی ۱۸۵
- ۱- موضوع جرم ۱۸۵
- ۲- رفتار مرتکب ۱۸۶
- بند دوم: رکن روانی ۱۸۷
- بند سوم: رکن قانونی ۱۸۷
- گفتار پنجم: اخلال در سامانه‌های رایانه‌ای یا مخابراتی ۱۸۷
- بند اول: رکن مادی ۱۸۸
- ۱- موضوع جرم ۱۸۸
- ۲- رفتار مرتکب ۱۸۸
- بند دوم: رکن روانی ۱۸۸
- بند سوم: رکن قانونی ۱۸۹
- گفتار ششم: ممانعت از دسترسی ۱۸۹
- گفتار هفتم: تروریسم سایبری (رایانه‌ای) ۱۹۰
- بند اول: رکن مادی ۱۹۰
- ۱- موضوع جرم ۱۹۰
- ۲- رفتار مرتکب ۱۹۰
- بند دوم: رکن روانی ۱۹۱

- بند سوم: رکن قانونی ۱۹۱
- مبحث سوم: سرقت و کلاهبرداری مرتبط با رایانه ۱۹۲
- گفتار اول: سرقت رایانه‌ای ۱۹۲
- بند اول: تعریف و ارکان سرقت سنتی و رایانه‌ای ۱۹۲
- بند دوم: تعریف فقهی و حقوقی سرقت تعزیری و حدی ۱۹۶
- بند سوم: تحلیل و تطبیق شرایط حد سرقت بر سرقت‌های رایانه‌ای ۱۹۷
- بند چهارم: ویژگی‌های سرقت رایانه‌ای ۲۰۳
- بند پنجم: ارکان و عناصر سرقت رایانه‌ای ۲۰۴
- بند ششم: رکن مادی ۲۰۴
- ۱- موضوع جرم ۲۰۴
- ۲- رفتار مرتکب ۲۰۵
- بند هفتم: رکن روانی ۲۰۶
- بند هشتم: رکن قانونی ۲۰۶
- بند نهم: عوامل جرم‌زای سرقت رایانه‌ای ۲۰۷
- بند دهم: پیشگیری از سرقت رایانه‌ای ۲۰۸
- گفتار دوم: کلاهبرداری رایانه‌ای ۲۰۹
- بند اول: تبیین مفهوم جرم کلاهبرداری رایانه‌ای ۲۱۰
- بیشتر بدانیم: کلاهبرداری رایانه‌ای از دیدگاه شورای اروپا ۲۱۳
- بیشتر بدانیم: پیشینه تاریخی جرم کلاهبرداری رایانه‌ای ۲۱۳
- بند دوم: تفاوت کلاهبرداری سنتی و رایانه‌ای ۲۱۴
- بند سوم: علل ارتکاب کلاهبرداری رایانه‌ای ۲۱۶
- ۱- علل فردی جرم کلاهبرداری رایانه‌ای ۲۱۶
- ۲- علل اجتماعی جرم کلاهبرداری رایانه‌ای ۲۱۶
- ۳- علل اقتصادی جرم کلاهبرداری رایانه‌ای ۲۱۶
- ۴- علل فرهنگی جرم کلاهبرداری رایانه‌ای ۲۱۷

- بند چهارم: ویژگی‌های کلاهبرداری رایانه‌ای ۲۱۷
- بند پنجم: مبانی جرم‌انگاری کلاهبرداری رایانه‌ای ۲۱۸
- بند ششم: رکن مادی ۲۱۹
- ۱- موضوع جرم ۲۱۹
- ۲- رفتار مرتکب ۲۱۹
- بند هفتم: وجوه افتراق رکن مادی جرم کلاهبرداری سنتی و کلاهبرداری رایانه‌ای ۲۲۱
- بند هشتم: رکن روانی ۲۲۱
- بند نهم: رکن قانونی ۲۲۲
- بند دهم: مصادیق کلاهبرداری رایانه‌ای ۲۲۴
- بند یازدهم: انواع کلاهبرداری رایانه‌ای در جهان ۲۲۸
- بند دوازدهم: پیشگیری از کلاهبرداری رایانه‌ای ۲۲۹
- گفتار سوم: فیشینگ ۲۳۵
- بند اول: دستکاری و تقلب در لینک‌ها و آدرس‌ها ۲۳۶
- بند دوم: وب سایت جعلی ۲۳۷
- بند سوم: فیشینگ از طریق تلفن ۲۳۸
- بند چهارم: فیشینگ با دستگاه‌های POS و ATM تقلبی ۲۳۹
- بند پنجم: پیام‌رسان‌های اجتماعی و فیشینگ ۲۳۹
- بند ششم: سایر روش‌های فیشینگ ۲۴۰
- بند هفتم: روش‌های کاربردی در مقابله با فیشینگ ۲۴۱
- گفتار چهارم: رمالی و فالگیری رایانه‌ای ۲۴۲
- گفتار پنجم: قمار و شرط‌بندی رایانه‌ای ۲۴۴
- بند اول: دیدگاه فقهی نسبت به قماربازی رایانه‌ای ۲۴۶
- بند دوم: قمار رایانه‌ای در حقوق ایران ۲۴۸
- مبحث چهارم: جرائم علیه عفت و اخلاق عمومی ۲۵۰
- گفتار اول: هرزه‌نگاری ۲۵۰

- بند اول: رکن مادی ۲۵۱
- ۱- موضوع جرم ۲۵۱
- ۲- رفتار مرتکب ۲۵۱
- بند دوم: رکن روانی ۲۵۲
- بند سوم: رکن قانونی ۲۵۲
- گفتار دوم: معاونت در دسترسی به محتویات هرزه ۲۵۴
- بند اول: رکن مادی ۲۵۴
- ۱- موضوع جرم ۲۵۴
- ۲- رفتار مرتکب ۲۵۴
- بند دوم: رکن روانی ۲۵۵
- بند سوم: رکن قانونی ۲۵۵
- مبحث پنجم: هتک حیثیت و نشر اکاذیب (جرایم علیه شخصیت معنوی) ۲۵۶
- گفتار اول: تغییر یا تحریف محتوای دیگری ۲۵۷
- بند اول: رکن مادی ۲۵۷
- ۱- موضوع جرم ۲۵۷
- ۲- رفتار مرتکب ۲۵۷
- بند دوم: رکن روانی ۲۵۸
- بند سوم: رکن قانونی ۲۵۹
- گفتار دوم: انتشار اسرار خصوصی و محتویات خانوادگی ۲۵۹
- بند اول: رکن مادی ۲۶۰
- ۱- موضوع جرم ۲۶۰
- ۲- رفتار مرتکب ۲۶۰
- بند دوم: رکن روانی ۲۶۱
- بند سوم: رکن قانونی ۲۶۱
- بیشتر بدانیم: جرم انتشار اسکرین‌شات ۲۶۲

۲۶۳ گفتار سوم: نشر اکاذیب
۲۶۴ بند اول: رکن مادی
۲۶۴ ۱- موضوع جرم
۲۶۴ ۲- رفتار مرتکب
۲۶۵ بند دوم: رکن روانی
۲۶۵ بند سوم: رکن قانونی
۲۶۶ مبحث ششم: پولشویی رایانه‌ای
۲۶۶ گفتار اول: پولشویی رایانه‌ای
۲۶۹ بند اول: ویژگی‌های پولشویی رایانه‌ای
۲۷۰ بند دوم: سیاست جنایی تقنینی در قبال پولشویی رایانه‌ای
۲۷۲ بند سوم: رکن مادی
۲۷۳ بیشتر بدانیم: فرایند پولشویی
۲۷۴ بند چهارم: رکن روانی
۲۷۵ بند پنجم: رکن قانونی
۲۷۶ بند ششم: پولشویی رایانه‌ای در نظام حقوقی بین‌المللی
۲۸۰ بند هفتم: پولشویی و کلاهبرداری در بستر استفاده از رمزارزها
۲۸۴ بند هشتم: عوامل جرم‌زا در خصوص جرم پولشویی رایانه‌ای
۲۸۵ بند نهم: پیشگیری از پولشویی رایانه‌ای
۲۸۶ مبحث هفتم: سایر جرائم
۲۸۶ گفتار اول: تولید یا انتشار یا توزیع یا در دسترس‌گذاری یا معامله نرم‌افزارهای مجرمانه
۲۸۶ بند اول: رکن مادی
۲۸۶ ۱- موضوع جرم
۲۸۷ ۲- رفتار مرتکب
۲۸۷ بند دوم: رکن روانی
۲۸۷ بند سوم: رکن قانونی

- گفتار دوم: فروش یا پخش یا دردسترس‌گذاری داده‌های رخنه‌گر..... ۲۸۸
- بند اول: رکن مادی ۲۸۸
- ۱- موضوع جرم ۲۸۸
- ۲- رفتار مرتکب ۲۸۹
- بند دوم: رکن روانی ۲۸۹
- بند سوم: رکن قانونی ۲۸۹
- گفتار سوم: پخش یا دردسترس‌گذاری محتویات آموزنده جرائم خاص رایانه‌ای ۲۹۰
- بند اول: رکن مادی ۲۹۰
- ۱- موضوع جرم ۲۹۰
- ۲- رفتار مرتکب ۲۹۱
- بند دوم: رکن روانی ۲۹۱
- بند سوم: رکن قانونی ۲۹۱
- تشدید مجازات‌ها ۲۹۲
- بخش سوم** ۲۹۵
- فصل اول** ۲۹۵
- جرایم رایانه‌ای از دیدگاه جرم‌شناختی و سیاست جنایی** ۲۹۵
- مبحث اول: دیدگاه جرم‌شناختی نسبت به جرائم رایانه‌ای ۲۹۶
- گفتار اول: مرتکبین جرائم رایانه‌ای ۲۹۷
- گفتار دوم: بزه‌دیدگان جرائم رایانه‌ای ۲۹۸
- گفتار سوم: علل ارتکاب جرائم رایانه‌ای ۲۹۹
- گفتار چهارم: تأثیر تهدیدات مرتبط با جرائم رایانه‌ای بر امنیت اقتصادی ۳۰۱
- فصل دوم** ۳۰۵
- سیاست جنایی مقابله با جرائم رایانه‌ای** ۳۰۵
- بیشتر بدانیم: مفهوم شناسی سیاست جنایی ۳۰۶

- گفتار اول: انواع سیاست جنایی ۳۰۸
- ۱- سیاست جنایی تقنینی ۳۰۹
- ۲- سیاست جنایی مشارکتی ۳۱۰
- ۳- سیاست جنایی قضائی ۳۱۰
- مبحث اول: سیاست جنایی جمهوری اسلامی ایران در مقابله با جرائم رایانه‌ای ۳۱۱
- گفتار اول: سیاست جنایی تقنینی ایران در جرائم رایانه‌ای ۳۱۱
- قسمت اول: روش‌های قانون‌گذاری در فضای مجازی ۳۱۸
- بند اول: روش قانون‌گذاری ملی ۳۱۸
- ۱- صلاحیت سرزمینی ۳۱۹
- ۲- صلاحیت شخصی ۳۲۰
- ۳- صلاحیت واقعی ۳۲۰
- ۴- صلاحیت جهانی ۳۲۱
- بند دوم: روش قانون‌گذاری بین‌المللی ۳۲۲
- بند سوم: روش خودانتظامی ۳۲۵
- بند چهارم: روش مختلط ۳۲۶
- قسمت دوم: رویکرد کیفی افتراقی و انعکاس آن در بخش جرائم رایانه‌ای قانون مجازات اسلامی .. ۳۲۷
- بند اول: عدم حمایت از بزه‌دیده سهل‌انگار ۳۲۸
- بند دوم: تعریف عملیات مقدماتی جرم به‌عنوان جرم تام ۳۳۰
- بند سوم: گسترش مسئولیت کیفی معاونتی ۳۳۱
- بند چهارم: وضع جرائم مطلق ۳۳۲
- بند پنجم: کاهش عناصر تشکیل‌دهنده جرم ۳۳۳
- گفتار دوم: سیاست جنایی قضائی ایران در قبال جرائم رایانه‌ای ۳۳۴
- بند اول: مراجع صالح رسیدگی به جرائم رایانه‌ای ۳۳۷
- صلاحیت مراجع عمومی در رسیدگی به پرونده‌های حوزه جرائم رایانه‌ای ۳۳۷
- بند دوم: نحوه رسیدگی به جرائم رایانه‌ای ۳۳۷

- گفتار سوم: سیاست جنایی مشارکتی ایران در جرائم رایانه‌ای ۳۳۸
- مبحث دوم: بررسی چالش‌های حقوقی رسیدگی به جرائم رایانه‌ای ۳۴۲
- گفتار اول: چالش‌های حقوق بین‌الملل عمومی ۳۴۲
- گفتار دوم: چالش‌های حقوق بین‌الملل خصوصی ۳۴۳
- بند اول: تعارض مراجع صالح رسیدگی ۳۴۴
- ۱- استفاده از حاکمیت قضائی ۳۴۵
- ۲- استفاده از رسیدگی قضائی مبتنی بر ملیت ۳۴۶
- ۳- استفاده از سایر نهادهای رسیدگی کننده قضائی ۳۴۷
- بند دوم: تعارض قوانین ۳۴۸
- گفتار سوم: چالش‌های حقوق ماهوی ایران ۳۴۹

بخش چهارم ۳۵۱

فصل اول ۳۵۱

پیشگیری از ارتکاب جرائم رایانه‌ای ۳۵۱

- مبحث اول: مفهوم شناسی پیشگیری و انواع تقسیم‌بندی آن ۳۵۲
- گفتار اول: تعریف پیشگیری ۳۵۲
- بند اول: تعریف مفهومی پیشگیری از وقوع جرم ۳۵۲
- بند دوم: مفهوم موسع پیشگیری ۳۵۳
- بند سوم: مفهوم مضیق پیشگیری ۳۵۴
- گفتار دوم: تفکیک انواع پیشگیری از وقوع جرم ۳۵۴
- بند اول: پیشگیری مرحله‌ای ۳۵۴
- ۱- پیشگیری اولیه ۳۵۴
- ۲- پیشگیری ثانویه ۳۵۵
- ۳- پیشگیری ثالثیه ۳۵۵
- بند دوم: پیشگیری کیفری و غیر کیفری ۳۵۶

- ۱- پیشگیری کیفی ۳۵۶
- ۱-۱- پیشگیری عام ۳۵۷
- ۲-۱- پیشگیری خاص ۳۵۷
- ۲- پیشگیری غیر کیفی ۳۵۷
- ۱-۲- پیشگیری اجتماعی ۳۵۸
- ۲-۲- پیشگیری وضعی ۳۵۹
- مبحث دوم: پیشگیری از وقوع جرائم رایانه‌ای ۳۵۹
- گفتار اول: پیشگیری کیفی از وقوع جرائم رایانه‌ای ۳۶۰
- گفتار دوم: پیشگیری غیر کیفی از وقوع جرائم رایانه‌ای ۳۶۲
- بند اول: پیشگیری اجتماعی از جرائم رایانه‌ای ۳۶۳
- ۱- پیشگیری اجتماعی رشد مدار رایانه‌ای ۳۶۴
- ۲- پیشگیری اجتماعی جامعه مدار رایانه‌ای ۳۶۵
- الف- فرهنگ سازی ۳۶۶
- ب- آموزش ۳۶۷
- ج- بزه دیده زدایی ۳۶۹
- د- اطلاع رسانی ۳۷۰
- ه- معضلات اقتصادی ۳۷۱
- بند دوم: پیشگیری وضعی از جرائم رایانه‌ای ۳۷۲
- ۱- حفاظت از سیستم‌های رایانه‌ای ۳۷۳
- ۲- حفاظت فیزیکی ۳۷۴
- ۳- حفاظت کارکنان ۳۷۵
- ۴- حفاظت ارتباطات ۳۷۵
- ۵- حفاظت عملیات ۳۷۷
- ۶- پلیس سایبر ۳۷۸
- ۷- ایمن سازی فضای مجازی ۳۸۰

- ۳۸۲..... ۸-افزایش خطر ارتکاب جرم.....
- ۳۸۳..... مبحث سوم: موانع تحقق پیشگیری از جرائم رایانه‌ای.....
- ۳۸۳..... گفتار اول: موانع مدیریتی.....
- ۳۸۵..... گفتار دوم: موانع حقوقی و قضائی.....
- ۳۸۶..... گفتار سوم: موانع اجتماعی.....
- ۳۸۶..... گفتار چهارم: موانع ساختاری.....
- ۳۸۷..... گفتار پنجم: موانع علمی- آموزشی.....
- ۳۸۷..... گفتار ششم: موانع فرهنگی.....
- ۳۸۸..... گفتار هفتم: موانع فنی.....
- ۳۹۱..... مبحث چهارم: جرم‌شناسی پیشگیرانه در حوزه جرائم رایانه‌ای.....
- ۳۹۲..... مبحث پنجم: تبیین چرایی پیشگیری از وقوع جرائم رایانه‌ای.....
- ۳۹۳..... مبحث ششم: نقد سیاست جنایی تقنینی ایران در پیشگیری از وقوع جرائم رایانه‌ای.....
- ۳۹۵..... **بخش پنجم**.....
- ۳۹۵..... **سخن آخر و پیشنهاد**.....
- ۳۹۶..... سخن آخر.....
- ۳۹۹..... پیشنهاده‌ها.....
- ۳۹۹..... ۱- راهکارهای اصلاحی.....
- ۴۰۰..... ۲- راهکارهای کوتاه مدت.....
- ۴۰۱..... ۳- راهکارهای بلند مدت.....
- ۴۰۳..... **فهرست منابع**.....
- ۴۰۳..... منابع فارسی.....
- ۴۰۶..... منابع انگلیسی.....

بخش اول

فصل اول

کلیات

مقدمه

مبحث اول: شرح مختصر موضوع

فضای مجازی در دهه اخیر به واسطه توسعه و فراگیری کاربری تجهیزات هوشمند الکترونیکی، به عنوان عضو جدایی ناپذیر زیست بشر میهمان هر کوی و برزن است، به گونه ای که لحظه ای فارغ از آن برای جوامع بشری حاضر قابل تصور و تحمل نیست، نفوذ عمیق این شکل از فناوری در زندگی افراد در همه اقصاء علیرغم ایراد جهات مثبت و فراهم آوری اسباب پیشرفت، آثار سوء و خطراتی را نیز به دنبال دارد. گاهی این موازنه خیر و شر از چهارچوب های تحت کنترل بشر خارج شده و موجبات اغتشاش و تخلفات انتظامی، اقتصادی، سیاسی، فرهنگی، اجتماعی و ... را حادث می شود. با نگاهی اجمالی به آمار و اخبار حوزه فناوری اطلاعات درمی یابیم که رشد و توسعه جرائم در فضای مجازی با سرعت بسیار زیادی در حال تحقق است و به تبع تامین امنیت این حوزه به یکی از بزرگترین دغدغه های هر حکومت بدل شده است. بی تردید مطالعات اساسی، فرهنگ سازی، اجرای صحیح ضوابط و ... می تواند آثار مطلوب فراگیری این فناوری را موجب گردد، تا بدین سان بشر از عواید و برکات این فناوری منتفع شود.

گرچه تاکنون تعاریف متعددی در خصوص دو مولفه جرائم سایبری^۱ و جرائم رایانه‌ای^۲ به صورت کلی و همچنین به صورت مصداقی تبیین شده، ولیکن تعریف جامع و دقیقی که مورد توجه و تایید قانون‌گذار جمهوری اسلامی ایران بوده باشد درباره این قسم جرائم ارائه نشده است. شاید یکی از دلایل آن، تفاوت در دیدگاه‌ها یا گستردگی مفهوم رایانه، فضای سایبر و تخلفات مختص به آن‌ها باشد. با این حال، در تعریف کلی آمده است که هر فعل یا ترک فعلی که به واسطه اتصال به اینترنت و فضای سایبر تحقق یابد و آن رفتار از حیث قوانین جاری کشور ممنوع و برای آن مجازات مقرر شده باشد جرم سایبری نامیده می‌شود. از طرفی می‌توان در تعریفی جامع‌تر جرم رایانه‌ای را رفتار مجرمانه‌ای اعم از فعل یا ترک فعل دانست که به واسطه کاربری رایانه و تجهیزات رایانه‌ای به وقوع می‌پیوندد. نظام قضائی و قوای قانون‌گذار جمهوری اسلامی ایران به موجب رصد و ارزیابی جرائمی که با ارتباطی حتی جزئی با فضای مجازی محقق می‌شود و با تطبیق عناصر جرائم مذکور با مولفه‌های اطلاق جرم سایبری و جرم رایانه‌ای به یک رفتار مجرمانه، نسبت به انواع جرائم ارتكابی در این حوزه قائل به تفکیک است، از این رو تاسیسات مدون احکام در قالب قانون جرائم رایانه‌ای مصوب ۱۳۸۸ مشتمل بر ۳ بخش و ۵۶ ماده و ۲۵ تبصره قانونی تصویب شده است، این مصوبات با بهره‌گیری از ابزار مقرر قانونی، به عدالت، بر همگان اعمال می‌گردد.

^۱ cyber crime

^۲ computer crime

بیشتر بدانیم: تعاریف جرائم رایانه‌ای

در نظام مدون حقوق ایران، نه در قانون تجارت الکترونیک و نه در قانون جرائم رایانه‌ای هیچ تعریف مشخصی از مفهوم جرائم رایانه‌ای ارائه نشده‌است. شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرائم رایانه‌ای وجود دارد. اما می‌توان به‌عنوان نمونه تعریف زیر را ارائه نمود: «آن دسته از جرائمی که با سوءاستفاده از یک سیستم رایانه‌ای برخلاف قانون ارتکاب می‌یابد جرائم رایانه‌ای نام دارد». البته این دسته از جرائم را می‌توان شامل جرائم سنتی که به‌واسطه رایانه صورت می‌گیرد از قبیل کلاهبرداری و سرقت و ... و نیز جرائم نوظهوری که با تولد رایانه پا به عرصه حیات گذاشته‌اند مانند جرائم علیه صحت و تمامیت داده‌ها و ... دانست.

درخصوص جرائم رایانه‌ای تعاریف متعددی در دیگر کشورها مطرح شده‌است، برخی از این تعاریف عبارتند از:

پلیس جنایی فدرال آلمان در تعریفی از جرائم رایانه‌ای چنین تبیین داشته‌است: «جرم رایانه‌ای دربرگیرنده همه اوضاع و احوال و کیفیاتی است که در آن شکل‌های پردازش الکترونیک داده‌ها، وسیله ارتکاب و یا هدف یک جرم قرار گرفته است و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است».

کمیته اروپایی مسایل جنایی در شورای اروپا در سال ۱۹۸۹ گزارش کاری تبیین نمود که در آن یکی از متخصصان درخصوص جرائم رایانه‌ای چنین تعریفی ارائه نموده‌است: «هر فعل مثبت غیرقانونی که رایانه، ابزار یا موضوع جرم باشد جرم رایانه‌ای است، یا به‌عبارتی هر جرمی که ابزار یا هدف آن تاثیرگذاری بر عملکرد رایانه باشد جرم رایانه‌ای است».

پروفسور شیک (Robert Schick) یکی از حقوقدانان اُتریشی در تعریف جرم رایانه‌ای بیان می‌دارد: «جرم رایانه‌ای به هر عمل مجرمانه‌ای گفته می‌شود که در آن رایانه، وسیله یا هدف ارتکاب جرم باشد».

همچنین در ایالات متحده آمریکا تعریف موسعی از جرم رایانه‌ای به عمل آمده مبنی بر آن‌که: «هر اقدام غیرقانونی که با یک رایانه یا به‌کارگیری آن مرتبط باشد را جرم رایانه‌ای می‌گویند یا هر اقدامی که به هر ترتیب با رایانه مرتبط بوده و موجب ایجاد خسارت به بزه‌دیده شود و مرتکب از این طریق منفعی را تحصیل کند، جرم محسوب می‌شود».

در کانادا نیز در تعریف جرائم رایانه‌ای این چنین تبیین شده‌است: «جرم رایانه‌ای شامل هر فعالیت مجرمانه‌ای است که دربرگیرنده کپی، استفاده، جابجایی، مداخله، دسترسی یا سوء استفاده از سیستم‌های رایانه‌ای، عملکرد رایانه، داده‌ها یا برنامه‌های رایانه است».

آنچه مورد توجه است این‌که باعنایت به پیشرفت تکنولوژی در عصر حاضر مجرمان مجرب و حرفه‌ای از همکاری هکر^۳ها و متخصصین برای نفوذ به سیستم‌های حساس و مهم جهت ارتکاب جرم بهره می‌جویند. برابر آمار رسمی در دنیا در هر ۱۲ ثانیه حداقل یک نفر قربانی جرائم رایانه‌ای می‌شود. البته نکته حائز اهمیت در این زمینه این‌که جمهوری اسلامی ایران رتبه برتر کشف جرائم رایانه‌ای را در بین کشورهای منطقه و حتی نسبت به برخی کشورهای توسعه‌یافته دارد. باید توجه‌داشت که گستره جرائم رایانه‌ای به قدری فراگیر و منشعب است که برای تحلیل آن مجلدات فراوان مورد نیاز است. بی‌شک جرائم رایانه‌ای حسب اهمیت از حیث تعدد ارتکاب و فزونی آثار زیانبار آن، مقابله جدی و

^۳ Hacker

اعمال اشد مجازات بر مرتکبین را می‌طلبد، تا شاهد ضربات خطر آن بر جامعه نباشیم، چراکه از حقوق مسلم هر اجتماع سالم محیط سالم است، تا اعضای جامعه با خاطری آسوده و با امنیت کامل در آن به فعالیت بپردازند و این مهم در فضای مجازی محقق نمی‌شود جز با گسترش امنیت در فضای مجازی و خودآگاهی کاربران. طبعاً فقدان سواد رسانه‌ای (چالش فرهنگی، اجتماعی و خانوادگی) عموماً در بزه‌دیده و گاهی در بزه‌کار سبب اصلی وقوع جرائم حوزه فضای مجازی است، همچنین باید توجه داشت که شکاف دیجیتالی میان نسل‌ها به‌عنوان نقیصه جدی در جامعه، باعث شده والدین در تربیت فرزندان خود در این حوزه دچار ناتوانی شده و نتوانند به نحو شایسته بر اعمال فرزندان خود نظارت نمایند، این درحالی است که کودکان و نوجوانان در زمره آسان‌ترین اهداف (قربانیان) بزه‌کاران مربوطه هستند.

بی تردید ابعاد ناشناخته فضای مجازی و گستره فعالیت‌های رایانه‌ای و سایبری مبین ضرورت وجود تخصص و تسلط جامع متصدیان امر است، حال این‌که، به تبع در حوزه جرائم رایانه‌ای این ابهامات مشدد است. مجرمین فضای مجازی و رایانه‌ای عموماً به‌صورت تخصصی در حوزه‌ای خاص بر بستر این تکنولوژی مرتکب رفتار مجرمانه می‌شوند و طبعاً پیش از این، در حوزه مربوطه تجربه و دانش کافی را کسب نموده‌اند، بر همین اساس همواره به‌دنبال مفر از تشبیت مجرمیت و نقض ادله انتساب جرائم مزبور به خود هستند، به‌عبارتی تمام هوش، توانایی و تلاش خود را به کار گرفته تا به طریقی آثار اعمال خود در فرایند ارتکاب جرم را محو سازند. در این میان سیاست‌گذاری جنایی صحیح و اجرای بی‌نقص قوانین می‌تواند تحقق انضباط و امنیت در جامعه را تضمین نماید. رویکرد

جمهوری اسلامی ایران نسبت به جرائم حوزه فضای مجازی با امعان نظر در سیاست تقنینی و سیاست قضائی کشور مبین ضرورت تدقیق و تحلیل گام به گام این دست جرائم است، چراکه در اکثر موارد بداعت ویژه و پیچیدگی جرائم رایانه‌ای مسیر ناهموار تعقیب جرائم را منتج به بیراهه می‌کند، ضمن این‌که سیاست‌های پیشگیرانه و هدایت‌گر می‌تواند تهدیدگران حوزه ارتکاب جرائم رایانه‌ای که در قامت کاربران باهوش و بااستعداد نقش آفرینی می‌کنند را بدل به کنشگران مثبت و فرصت‌های رشد و تعالی ملی و بین‌المللی نماید. از دیدگاه جرم‌شناسی، این قبیل جرائم، که قربانیان خود را از میان عامه مردم برمی‌گزینند و بعضاً حقوق عامه را هدف سوءاستفاده و آسیب قرار می‌دهد فارغ از بُعد معنوی جرم به موجب اضرار به غیر موجد مسئولیت است و به تبع "مرتکب" مستحق کیفر خواهد بود، مضافاً باید توجه داشت که عاملین به جرائم مزبور صرف‌نظر از تقبیح رفتار، بعضاً خود قربانیان نظامات سازمان‌یافته بزهکاری هستند که قریب به اتفاق نقطه اشتراکی در خارج از مرزهای کشور عزیزمان دارند، گاهی این اشتراک به واسطه سوءنیت بر اهداف اختصاصی صورت می‌پذیرد و گاه به نیت تضعیف و ضربه به پیکره فرهنگی، اجتماعی و اقتصادی کشور تحقق می‌یابد. پلیس تخصصی این حوزه موسوم به پلیس سایبر و یا پلیس فتا (فضای تولید و تبادل اطلاعات ناجا) بازوان توانمند نظام قضائی و مقتدرترین مرجع تخصصی انتظامی رسمی در جمهوری اسلامی ایران است که در دوایر معین به اختصاص موضوع خاص جرائم حوزه فضای مجازی به خدمت‌رسانی می‌پردازد. این یگان به واسطه تعامل با متخصصین و همچنین با بهره‌گیری از معلومات و اندیشه‌های موثر، سعی در ریشه‌یابی، شناسایی فرصت‌های ارتکاب، مهندسی جرائم ارتکابی، بررسی آثار اجتماعی،

فرهنگی، اقتصادی و ... دارد. ارائه راهکارهای مقابله و تدوین دستورالعمل‌های پیشگیرانه موثر، اتخاذ سیاست‌های لازم جهت رفع و پوشش خلاءهای موجود در فضای مجازی که زمینه ارتکاب اکثر جرائم این حوزه را فراهم می‌آورد بخشی از ره‌آورد خدمات دستگاه‌های خدمت‌رسان این حوزه است. همیاران و همراهان مرکز فوریت سایبر پلیس فتا جمهوری اسلامی ایران در درجه اول مردم و در درجه بعد نهادهایی نظیر مرکز ملی فضای مجازی (شورای عالی فضای مجازی)، معاونت امنیت فضای تولید و تبادل اطلاعات وزارت ارتباطات و فناوری اطلاعات جمهوری اسلامی ایران، مرکز مدیریت راهبردی افتا ریاست جمهوری (امنیت فضای تولید و تبادل اطلاعات)، مراکز دانشگاهی و پژوهشی آپا (آگاهی رسانه، پشتیبانی و امداد رایانه‌ای)، پلیس آگاهی، پلیس امنیت و اطلاعات، مرکز ماهر (مدیریت امداد و هماهنگی عملیات و رخدادهای رایانه‌ای)، دادسراهای تخصصی و شعب اختصاصی رسیدگی به جرائم حوزه فضای مجازی، مرکز واکنش سریع جرائم رایانه‌ای (وابسته به دادسراهای عمومی و انقلاب سراسر کشور) و ... هستند که در تمامی سطوح مطالعات، فرهنگ‌سازی و پیشگیری تا تادیب و مجازات متخلفان در کنار این پلیس به نقش‌آفرینی مثبت و موثر می‌پردازند. حال این‌که تشریح مساعی این نظام مبسوط بر چه مداری موثر افتد و چه برآیندی حاصل شود، تا حدود زیادی معطوف به سیاست جنایی حکومت در قبال جرائم نوظهور رایانه‌ای است. در این مرقومه دغدغه اصلی مولف تبیین اساس خلاءهای موجود در رویکرد و قوانین حوزه مبارزه با جرائم رایانه‌ای است، که در نهایت منتج به پیشنهادهای اثربخش در راستای سالم‌سازی فضای مجازی-رایانه‌ای کشور و ارتقاء نظام قضائی در این حوزه شده‌است.

مبحث دوم: اهمیت موضوع

پیشرفت و توسعه همه‌جانبه کشور در حال حاضر اولویت اصلی تمامی نهادها و تشکیلات حکومتی مرتبط است. امروزه انباشت آثار بحران‌های فرهنگی، اجتماعی و اقتصادی که طی سالیان اخیر متوجه کشور عزیزمان شده‌است مزید نابسامانی‌هایی در این حوزه‌ها است که علاوه بر آثار زیانبار بر زیست اجتماعی ملت، زینده نظام اسلامی ایران نیست. ایجاد سازوکار متناسب با شرایط کنونی کشور نیازمند حمایت همه‌جانبه اعضای جامعه است، این درحالی است که تحقق چنین ساختار راهگشایی مرهون تلفیق علم و عمل در این حوزه است. جرائم رایانه‌ای به‌عنوان عارضه نوین جوامع امروزی، آسیب‌های فراوانی بر پیکره امنیتی کشور از هر حیث وارد آورده‌است که بن‌مایه گسترش خود را از جذابیت‌های کاربری و منافع بعضا نامشروع این قسم جرائم می‌گیرد، لذا متخلفین امر از هیچ تلاش مخربی در این حیطه مجرمانه مضایقه نمی‌کنند، تا حدی که امروزه گاهی با پدیده‌هایی در حوزه جرائم رایانه‌ای مواجه می‌شویم که امنیت کشور را در مقاطع مختلف به انحطاط کشانده و دچار بحران‌های جدی می‌سازد. از این رو اصلاح نگرش و سیاست‌گذاری قوی در حوزه مقابله با جرائم رایانه‌ای اهتمام ویژه مسئولین امر را می‌طلبد، که میسر نمی‌شود مگر به‌موجب تحقیقات جامع و تحلیل تخصصی اساس و جوانب امر.

بیشتر بدانیم: چند نکته

۱- سیاست جنایی جمهوری اسلامی ایران در قانون‌گذاری و اجرای قوانین حوزه جرائم رایانه‌ای با توجه به فقدان قدمت مطول این قسم جرائم، تا حدود زیادی به‌روز و منطبق

با رویکرد جنایی جدید جمهوری اسلامی ایران است، مضاف بر این که احتمالاً بعثت عمر کوتاه شناسایی و مقابله با جرائم مزبور می‌توان نقایص فراوان و ایرادات اساسی بر سیاست جنایی و تقنینی جمهوری اسلامی در این حوزه وارد دانست.

۲- مقنن در قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و قانون مجازات اسلامی مصوب ۱۳۹۲ با توجه به اهمیت موضوع، مجازات سختگیرانه و به شدت بازدارنده را در دستور کار قرار داده است. لہذا به سبب پیشرفت، سهل‌الوصول بودن و قابل توجه بودن منافع مکتسبه در فرایند ارتکاب اکثر جرائم رایانه‌ای، در عصر حاضر شاهد فزونی جدی در این عرصه و نقض قوانین مقرر نسبت به گذشته هستیم.

۳- بخش قابل توجهی از وقوع جرائم رایانه‌ای مرهون حمایت مافیای قدرتمند و سازمان‌های تبهکاری خارجی است که با انگیزه‌های انتفاع مادی و تاثیرات سیاسی و فرهنگی بر جامعه هدف صورت می‌پذیرد. باین حال ناتوانی برخی متولیان داخلی کشور از حیث عدم شناخت و تسلط کافی بر حوزه جرائم رایانه‌ای را نمی‌توان نادیده گرفت. با این وصف که عمده بزهداران حوزه جرائم رایانه‌ای را جوانان و نوجوانان تشکیل می‌دهند. اطلاعات قابل توجه و تکثیر مدلهای ارتکاب جرائم رایانه‌ای در میان قشر جوان و نوجوان مستعد، مزید بر تحریک و تطمیع نامبردگان به تصور کسب منافع حداکثری و نامشروع، فزونی عجیب این پدیده در جامعه را موجب شده است.

بیشتر بدانیم: تالیفات مرتبط

تا کنون علاوه بر مصوبات مجلس شورای اسلامی در قالب قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و بخش‌هایی از قانون مجازات اسلامی مصوب ۱۳۹۲ و ... تالیفات متعددی در ارتباط با سیاست جنایی ایران در حوزه جرائم رایانه‌ای تدوین و انتشار یافته‌است، این تالیفات اغلب براساس دیدگاه صاحب‌نظران در جمهوری اسلامی ایران از حیث قوانین و مقررات صورت گرفته‌است، همچنین تالیفات باارزشی در سایر ملل در این حوزه منتشر شده‌است. از جمله تالیفات یادشده می‌توان به موارد ذیل اشاره نمود:

- در سال ۱۳۸۷ کتابی با عنوان جرائم تجارت الکترونیکی (جرائم سایبری در بستر تجارت الکترونیکی) به قلم دکتر جواد جاویدنیا و دکتر جعفر کوشا تالیف شده‌است، این اثر که مشخصاً به جرائم حوزه تجارت الکترونیکی پرداخته است بر اساس پایان‌نامه دوره کارشناسی ارشد دکتر جواد جاویدنیا تدوین، انتشار و در دسترس عموم قرار گرفته‌است. در این رساله پژوهشگر ضمن تعریف و تحلیل مولفه‌های اصلی جرائم حوزه تجارت الکترونیکی به طبقه‌بندی این جرائم از حیث ماهیت پرداخته، همچنین به لحاظ شکلی به ابعاد مختلف جرائم مزبور توجه، و برآیند تطبیق قوانین و سیاست‌های جمهوری اسلامی ایران با جامعه بین‌المللی را با مذاقه در کنوانسیون‌ها و منابع موثق خارجی به رشته تحریر درآورده‌است.

- در سال ۲۰۰۰ میلادی مقاله‌ای از جانب مؤسسه تحقیقات جرائم اقتصادی کالج اوتیکا منتشر شد. این مؤسسه تحقیقاتی تا به امروز بیش از دو دهه به تجزیه و تحلیل و مبارزه با جرائم اقتصادی اشتغال داشته‌است. این مقاله ضمن تبیین انواع جرائم اقتصادی سایبری، به فرایند تحقق و سیاست جنایی نظام حاکمه ایالات متحده آمریکا نسبت به

مصادیق جرائم اقتصادی سایبری می‌پردازد. همچنین در این مقاله به تحلیل نقش تعامل و همکاری جهانی در ریشه‌یابی و مبارزه با جرائم اقتصادی سایبری توجه ویژه شده است. - در سال ۱۳۹۶ کتابی تحت عنوان حقوق کیفری سایبری به قلم دکتر فرهاد الهوردی و با دیباچه استاد حسین میرمحمدصادقی تالیف شده است. در این کتاب به جرائم حوزه فضای مجازی به تفکیک موضوعات پرداخته شده است.

- همچنین تالیفات متعددی در قالب کتب و مقالات علمی- پژوهشی و ... تا کنون انتشار یافته است، آثاری به قلم اساتید گرانمایه از جمله دکتر مونا خلیل‌زاده (حاشیه بر قانون جرائم سایبری)، دکتر محمدسعید شفیعی و محمد محسنی و محسن شفیعی دستگردی (بررسی و پیگرد جرم در فضای سایبری)، دکتر غلامرضا محمدنسل (حقوق جزای اختصاصی جرائم سایبری در ایران)، دکتر مهدی مقیمی (ترجمه کتاب مطالعه جامع جرائم سایبری)، دکتر مرتضی اکبری (ترجمه کتاب جرائم سایبری: راهنمایی برای کشورهای در حال توسعه)، دکتر امیر صادقی نشاط (حقوق تجارت الکترونیک)، دکتر بهزاد رضوی فرد و سیدنعمت‌اله موسوی (محدودیت‌ها و راهبردهای صلاحیت در جرائم سایبری)، دکتر امیر وطنی و حمید اسدی (سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم)، نرگس زنگنه (تاثیر افزایش آگاهی‌های عمومی در پیشگیری از بزه‌دیدگی در فضای سایبر (با تأکید بر جرائم اقتصادی))، سمانه خالقی (بررسی فقهی حقوقی هک‌های سایبری در حوزه پول و معاملات اقتصادی)، جلال انصاری (بررسی تطبیقی سیاست جنایی ایران و آمریکا نسبت به جرائم کلاهبرداری و سرقت سایبری (با نگاهی اجمالی بر فقه امامیه))، محمد حاجی‌مشهدی (حمایت کیفری از زیان‌دیده‌گان جرائم اقتصادی در فضای مجازی (سایبری)) و ... که به‌موجب پرهیز از اطاله نوشتار از ذکر جزئیات آن در این بخش صرف نظر شده است.

فصل دوم

مفاهیم، مبانی، پیشینه و درآمدی بر جرائم رایانه‌ای

مبحث اول: جرائم رایانه‌ای

علیرغم فقدان تعریف متقن از گزاره جرم رایانه‌ای، با تفحص در منابع و تعاریف موجود چنین استنباط می‌گردد که جرائم رایانه‌ای در اصطلاح به جرائمی گفته می‌شود که به واسطه ابزار رایانه‌ای در محیطی غیر فیزیکی، علیه فناوری اطلاعات^۴ با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد. امروزه بسیاری از جرائم سنتی، هم‌زمان با پیشرفت فناوری اطلاعات و ارتباطات به شدت متحول شده و به جرائم رایانه‌ای تبدیل شده‌اند. پیش‌نویس کنوانسیون بین‌المللی جرائم سایبری (۲۰۰۱، بوداپست^۵) همواره به تقویت مکانیزم حفاظت در برابر جرائم سایبری و تروریسم اشاره دارد. در جامعه بین‌الملل برخی تعاریف در تلاش برای در نظر گرفتن اهداف و نیت هستند و جرائم رایانه‌ای را دقیق‌تر تعریف می‌کنند، اما باید توجه داشت که در ابعاد بین‌المللی و داخلی، تعریف دقیق و شفاف از جرم رایانه‌ای ارائه نشده است.

^۴ به جرائم رایانه‌ای، جرائم علیه فناوری اطلاعات نیز می‌گویند.

^۵ Budapest