

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

تحلیلی بر

جرایم رایانه‌ای و مخابراتی

(جرایم در بستر رایانه، فضای مجازی، شبکه‌های اجتماعی و پیام‌رسان‌ها)

سید مهدی صنعتی

مجید عطایی جنتی

(قضات دادگستری)

سرشناسه: صنعتی، سید مهدی
 شبکه‌های اجتماعی و پیام‌رسان‌ها
 عنوان: تحلیلی بر جرایم رایانه‌ای و مخابراتی: جرایم در بستر رایانه فضای مجازی،
 تکرار نام پدیدآور: مؤلفین سید مهدی صنعتی، مجید عطائی جنتی
 مشخصات نشر: قم: حقوق پویا، ۱۳۹۷
 مشخصات ظاهری: ۲۰۸ ص.
 ISBN: 978-622-99074-9-8
 وضعیت فهرستنویسی: فیپا
 یادداشت: عنوان در بستر رایانه فضای مجازی، شبکه‌های اجتماعی و پیام‌رسانی‌ها
 یادداشت: کتابنامه
 موضوع: جرایم کامپیوتری
 موضوع: مسئولیت جزایی - ایران
 موضوع: اینترنت - چینه‌های اجتماعی
 شناسه افزوده: عطائی جنتی، مجید،
 رده‌بندی مکره: ۱۱۹۷ / ۶ ص / HV ۶۷۷۳
 رده‌بندی دیوبی: ۳۶۴/۱۶۸
 شماره مکتوب: ۴۸۰/۱۶۶

هرگونه تکرار (اعم از چاپ کپی و...) از این اثر بدون أخذ مجوز از ناشر خلاف
 قانون بوده و پیگرد قانونی دارد.
 لطفاً در صورت مشاهده موارد را به شماره تلفن‌های ذیل اطلاع دهید.

تحلیلی بر جرایم رایانه‌ای و مخابراتی

(جرایم در بستر رایانه فضای مجازی، شبکه‌های اجتماعی و پیام‌رسان‌ها)



حقوق پویا

سید مهدی صنعتی، مجید عطائی جنتی (قضات دادگستری)

ناشر:	حقوق پویا
چاپ:	پشت / اول پاییز ۱۳۹۷
شمارگان:	۱۰۰۰ نسخه
قیمت:	۲۵۰۰۰ تومان
شابک:	۹۷۸-۶۲۲-۹۹۰۷۴-۹-۸

مراکز پخش:

قم / خیابان ارم / جنب بانک ملی / پاساژ ناشران / پلاک ۲۲
 ۰۹۱۲۶۵۲۵۰۷۰ / ۰۲۵-۳۷۷۴۹۲۷۴

کانال تلگرام: @nashrehoghoghepoya
 فروشگاه اینترنتی: www.hpbook.ir

تهران / نشر میزان ۶۶۴۶۷۷۷۰
 تهران / کتاب آوا ۶۶۹۷۴۱۳۰

تقدیر به:

رمانده جاوید الاثر «حاج احمد متوسلیان»

سلام ای شیر درز خیر صهیون

سلام ای یوسف گشته‌ی ما

چو یعقوب آرزو داریم هر ده

«عزیزِ قدس» روزی خواهد آمد...

فهرست مطالب

فهرست مطالب.....	۵
مقدمه.....	۷
بخش یکم: جرایم و مجازات ها.....	۲۱
فصل یکم: جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی.....	۲۱
مبحث یکم: دسترسی غیر مجاز.....	۲۱
مبحث دوم: شنود غیر مجاز.....	۳۲
مبحث سوم: دسترسی رایانه‌ای.....	۳۸
فصل دوم: جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه و مخابراتی.....	۵۵
مبحث یکم: جعل رایانه‌ای.....	۵۵
مبحث دوم: تخریب و اخراج داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی.....	۶۲
فصل سوم: سرقت و کلاهبرداری مرتکبانه.....	۷۳
فصل چهارم: جرایم علیه عفت و اخلاق عمومی.....	۸۷
فصل پنجم: هتک حیثیت و نشر اکاذیب.....	۱۰۵
فصل ششم: مسئولیت کیفری اشخاص [حقوقی].....	۱۱۵
فصل هفتم: سایر جرائم.....	۱۳۶
فصل هشتم: تشدید مجازات‌ها.....	۱۳۹
پیوست شماره یک: فهرست مصادیق محتوای مجرمانه.....	۱۶۵
پیوست شماره دو: آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی.....	۱۹۵
منابع.....	۲۰۴

مقدمه

زمانی در اصطلاح به مجموعه امکانات موجود در بستر اینترنت (تبادل پیام، انتشار مفاهیم در قالب‌های گوناگون، ارتباطات...) فضای مجازی گفته می‌شد که در برابر فضای واقعی قرار می‌گرفت. به نظر می‌رسد که امروزه با پیشرفت برق آسای تکنولوژی و اشتیاق بشر به ارتباطات سریع تر و گسترده تر، دیگر اطلاق فضای مجازی بر پیام رسان‌ها، شبکه‌های اجتماعی و ارتباطات اینترنتی، از روی مسامحه و عادت بوده و فضای مجازی، با فضای واقعی در هم آمیخته است. به عنوان نمونه آیا می‌توان ارتباطات موجود در بستر پیام رسان‌ها (اعم از مکالمه صوتی و تصویری، اسال آنلاین فیلم و عکس، گفت و گوی همزمان چند صد یا چند هزار نفره، خرید و فروش آنلاین...) را مجازی تلقی کرد؟ چه تفاوتی بین این اقدامات با اقدامات موجود در فضای واقعی هست؟!

آمارهای موجود حکایت از فعالیتهای گسترده اقشار مختلف مردم در پیام رسان‌ها و شبکه‌های اجتماعی دارد مثلاً گفته می‌شود که در دهه‌های نالغ بررس میلیون ایرانی در تلگرام فعالیت داشته‌اند! واقعا آیا در سطح جامعه و در فعالیتهای زیرکی این تعداد جمعیت فعال وجود دارد؟! یا در سطح وسیع تر گفته می‌شود که آمار کاربران پیام رسان فیس بوک به بیش از دو میلیارد نفر می‌رسد!

پیام رسان‌ها و شبکه‌های اجتماعی، از چالش‌های مهم عصر ارتباطات است. در کنار مزایای بسیار این ابزارهای ارتباطی (توسعه کسب و کار، اطلاع رسانی، شفاف سازی و الیت‌های دولت‌ها، کاهش آلودگی محیط زیست از طریق کاهش تردهای شهری و بین شهری و یا کاهش نیاز به کاغذ، بهبود روابط انسانی، سهولت و تسریع در خدمت رسانی به مردم...)، سوء استفاده‌های بسیاری نیز از این ابزارها می‌شود از جمله: خرید و فروش آنلاین کالاهای ممنوعه (سلاح - مواد مخدر - مشروبات الکلی -...)، کلاهبرداری، نشر اکاذیب، تشکیل باندهای تبهکاری، ترویج و هماهنگی اقدامات تروریستی و خرابکارانه، القای یأس و تشویق به خودکشی و مصرف مواد مخدر، تشویق به فحشاء، توهین و افتراء... همه‌ی این آسیب‌ها لزوم اعمال نظارت بر این ابزارها از سوی دولت را تقویت می‌نماید.

شاید در وهله اول اگر از کاربران پیام رسان‌ها و شبکه‌های اجتماعی سؤال شود که آیا با اعمال نظارت بر فعالیت‌های این شبکه‌ها موافقت یا خیر؟ اکثر کاربران مخالف این نظارت بوده و بیشتر به دنبال پیام رسان‌های خارجی هستند تا امکان نظارت بر فعالیت آنان نباشد! لکن اگر همین کاربران در بستر این ابزارهای ارتباطی، مجنی علیه واقع شوند مثلاً مورد اهانت قرار گیرند، یا مال خود را از دست دهند، آبروی آنان لکه دار شود، حریم خصوصی آنان نقض شود،...، توقع دارند که پلیس و قوه قضاییه به داد آنان برسد و اگر پلیس در پاسخ به آنان بگوید نه کاری از دست ما بر نمی‌آید یا امکان شناسایی مجرم وجود ندارد، سرخورده می‌شوند و حاکمیت قانون تلقی نمی‌کنند!

چالش پیام رسان‌ها و شبکه‌های اجتماعی، زمانی به اوج می‌رسد که این ابزارها از خارج از مرزهای کشور مدیریت شود و امکان هر گونه نظارت و کنترل بر آن از سوی حاکمیت منتفی باشد. در این هنگام است که باید این ابزارهای ارتباطی را بهشت تبهکاران بین المللی نامید که بدون هیچ پروایی از دولت‌ها، به ربح فعالیت‌های مجرمانه خود مشغول بوده و به جای ارتکاب اعمال مجرمانه در سطح جامعه، به ریسک‌پذیری مواجه است، با آرامش خیال و از طریق نرم افزارهای پیشرفته به اهداف شوم خود دست می‌یابند. بی جهت نیست که اخیراً بسیاری از کشورها از جمله روسیه، فرانسه و ایران^۱ پی فیلتر کردن پیام رسان‌های خارجی و ترغیب کاربران به استفاده از ابزارهای مشابه داخلی هستند. قبل از ورود به مباحث قانونی در خصوص جرایم رایانه‌ای و مخابراتی لازم است کلیات و نکاتی در خصوص این جرایم بیان شود:

۱ - مفهوم سامانه‌های رایانه‌ای: در خصوص مفهوم رایانه^۱ تعاریف گوناگونی^۲ ارائه شده است که از جمله گفته شده: کامپیوتر یا رایانه، وسیله یا دستگاهی است که می‌تواند اطلاعات مربوط به برنامه‌های کار را در حافظه‌اش نگه داری کند و طبق دستورات موجود در برنامه‌های مزبور، اطلاعات را بپذیرد و پس از پردازش به صورت اطلاعات و گزارش‌های خروجی مشخص ارائه

دهد.^۱ به نحو خلاصه می‌توان گفت رایانه یک دستگاه مربوط به اطلاعات است؛ اطلاعاتی که به آن داده می‌شود را ورودی و اطلاعات دریافتی از آن را خروجی گویند. عملیاتی که اطلاعات ورودی را تبدیل به اطلاعات خروجی می‌کنند پردازش نام دارد. رایانه از دو بخش سخت افزار (تمامی تجهیزات فیزیکی یک سامانه‌ی رایانه‌ای مانند صفحه کلید و صفحه نمایش) و نرم افزار (مجموعه دستورات و اطلاعاتی است که به کامپیوتر داده می‌شود تا کار خاصی را انجام دهد مانند ویندوز و آفیس) تشکیل شده است. اینترنت نیز شبکه‌ای از رایانه‌های متصل به هم است که از طریق خط تلفن با یکدیگر ارتباط برقرار می‌نمایند. اینترنت دو جزء اصلی دارد که عبارتند از شبکه جهانی وب و پست الکترونیک. شبکه جهانی وب برای خواندن صفحات اینترنت، تجارت الکترونیک، دریافت نرم افزار و... و پست الکترونیک برای ارسال و دریافت سریع و امن پیام، در طریق اینترنت کاربرد دارد.^۲

در خصوص سامانه (سیستم) رایانه‌ای تعریف قانونی هم داریم:

مقنن در بند و ماده ۲ قانون تجارت الکترونیک در مورد خصوص بیان نموده: «سیستم رایانه‌ای (Computer System) هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری - نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده پیام» عمل می‌کند.»

همچنین بند ب ماده ۱ آیین نامه "نحوه استفاده از سامانه‌های رایانه‌ای مخابراتی" (موضوع مواد ۱۷۵ و ۱۷۶ قانون آیین دادرسی کیفری) سامانه رایانه‌ای را این گونه تعریف نموده: «مجموعه‌ای از نرم‌افزارها و سخت‌افزارهای مرتبط که از طریق یک شبکه رایانه‌ای جهت اجرای فرایندهای کار مشخصی، به یکدیگر متصل‌اند.»

۲ - مفهوم سامانه‌های مخابراتی: بند پ ماده ۱ آیین نامه اخیر الذکر سامانه مخابراتی را این گونه تعریف نموده: «هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات»

۱ - آریا، ناصر، فرهنگ اصطلاحات کامپیوتر و شبکه‌های کامپیوتری، مرکز تحقیقات تخصصی حساب داری و حساب رسی، چاپ اول، تهران ۱۳۷۲، ص ۳۲.

۲ - مهدوی عرب، مهندس مهدی، آشنایی با کامپیوتر، انتشارات بهینه، چاپ پنجم، ۱۳۷۹، تهران، صص ۱۵ و ۱۶.

۳ - موران، جیمز، آموزش ICDL به زبان ساده، مهارت هفتم: اطلاعات و ارتباطات، مترجم علی اکبر متواضع، مؤسسه دیباگران تهران، چاپ یازدهم، ۱۳۸۳، صص ۱۹ و ۲۰.

میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله قراردادهایی که برای گیرنده قابل فهم و تفسیر باشد.»

در بند ب ماده ۱ لایحه جرایم رایانه‌ای پیشنهادی قوه قضاییه، که در زمان تصویب حذف شده، سیستم مخابراتی^۱ این چنین تعریف شده بود: هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات بین یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله پروتکل‌هایی که برای گیرنده قابل فهم و تفسیر باشد.

سیستم مخابراتی شامل سه جزء اصلی است:

الف - فرستنده: اطلاعات را گرفته و آن را به سیگنال تبدیل می‌کند.

ب - کانال مخابراتی: سیگنال را حمل می‌کند و شامل محیط انتقال نیز می‌گردد. فیبر نوری را می‌توان امن ترین کانال مخابراتی دانست.

ج - گیرنده: سیگنال را دریافت نموده و آن را به اطلاعات قابل استفاده تبدیل می‌کند.

نکته مهم

امروزه سامانه‌های رایانه‌ای و مخابراتی آن چنان در هم تنیده شده‌اند که تفکیک این دو بسیار دشوار است چرا که از یک طرف ارتباط بین دو رایانه و یا اتصال رایانه‌ها با شبکه‌ی جهانی اینترنت، از طریق سامانه‌های مخابراتی برقرار می‌شود و از دیگر سو، مدیریت سامانه‌های مخابراتی بدون سامانه‌های رایانه‌ای میسر نیست. بنابراین رابطه سامانه‌های رایانه‌ای با سامانه‌های مخابراتی مانند رابطه‌ی جسم و روح در بدن موجود زنده است که مکمل همدیگرند. بر همین مبنا است که مقنن در فصل جرایم رایانه‌ای همه جا برای رایانه‌ای و مخابراتی را در کنار هم آورده است. در همین خصوص برخی معتقدند که مقنن بایستی به جای «جرایم رایانه‌ای و مخابراتی» از اصطلاح جرایم سایبری استفاده می‌نمود زیرا که جرایم رایانه‌ای و مخابراتی را شامل می‌شود. هم چنین این که گسترش واژه سایبر، آن را به یک واژه بین المللی تبدیل نموده که یافتن معادلی برای آن، ممکن است دایره شمول و

مفهوم آن را محدود می‌نماید.^۱

۳- مفهوم جرایم رایانه‌ای^۲: از جرم رایانه‌ای نیز تعاریف متعددی ارائه شده: از جمله گفته شده که هر فعل یا ترک فعلی که علیه کامپیوتر یا شبکه‌های کامپیوتری صورت گرفته، یا با واسطه کامپیوتر یا شبکه‌های کامپیوتری محقق شود، جرم رایانه‌ای است.^۳ و یا هر فعل یا ترک فعل که به وسیله رایانه یا با اخلاف یا نفوذ در سامانه‌های رایانه‌ای صورت پذیرد و به موجب قانون برای آن مجازات تعیین شده باشد جرم رایانه‌ای است.^۴ همچنین گفته شده: با توجه به ماده ۲ قانون مجازات اسلامی مصوب ۱۳۹۲ خورشیدی می‌توان جرم رایانه‌ای را چنین تعریف نمود که هر رفتاری عم از فعل یا ترک فعل، که در فضای مجازی ارتکاب یافته و در قانون برای آن مجازات تعیین شده باشد.^۵

نکته:

صرف نظر از تقسیم بندی متداول جرایم رایانه‌ای به سه نسل مختلف (جرایم علیه رایانه، جرایم علیه داده و جرایم سایبری) و یا تقسیم بندی جرایم مرتبط با بحث به جرایم رایانه‌ای، اینترنتی و سایبری، نباید جرایم رایانه‌ای را محدود به جرایم ارتكابی در بستر اینترنت و فضای مجازی نمود بلکه با توجه به جرایم مطرح در قانون جرایم رایانه‌ای، مهم ارتكاب جرم علیه سامانه‌های رایانه‌ای یا علیه داده‌ها و یا به وسیله رایانه است اعم از آن که سامانه مورد نظر آنلاین یا آفلاین باشد، مجرم به صورت مستقیم و فیزیکی به سامانه هدف دسترسی یابد و یا از طریق فضای مجازی و یا از طریق بدافزار مرتکب جرم شود...

۴- مفهوم جرایم مخابراتی: جرایم مخابراتی شامل جرایمی می‌شود که به وسیله ابزاری مخابراتی و نیز جرایم علیه سامانه‌های مخابراتی است. از این رو به نظر می‌رسد که جرایم

۱- نوریان، علیرضا، آیین دادرسی کیفری جرایم رایانه‌ای و مخابراتی، نشر میزان، چاپ اول، تهران، ۱۳۹۶، ص ۲۰.

2 - Cyber crime; computer crime; electronic crime; e - crime

۳- بای، حسینعلی/پور قهرمانی، بابک، بررسی فقهی و حقوقی جرایم رایانه‌ای، ناشر پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول، قم، ۱۳۸۸، ص ۳۸.

۴- ترکی، غلامعباس، نگرش علمی و کاربردی به قانون جرایم رایانه‌ای، قسمت اول، ماهنامه دادرسی، شماره ۷۷، آذر و دی ۱۳۸۸، ص ۱۲.

۵- نوریان، علیرضا، همان، صص ۱۹ و ۲۰.

مخابراتی باید این گونه تعریف شود: فعل یا ترک فعل مجرمانه که با استفاده از وسایل و شبکه‌های ارتباطی - مخابراتی و یا علیه آن‌ها روی دهد در قانون نیز برای آن‌ها مجازات تعیین شده باشد.^۱ در مواد مربوط از فصل جرایم رایانه‌ای اگر چه به تصریح تعریفی از جرایم مخابراتی نیامده اما همچنان که در ماده ۷۸۰ این قانون به صورت ضمنی، جرایم مخابراتی را جرایمی دانسته که در آنها از سامانه مخابراتی به عنوان وسیله ارتکاب جرم استفاده شده باشد. جرایم مخابراتی همانند جرایم رایانه‌ای به دو دسته تقسیم می‌شوند: الف: جرایم مخابراتی محض - یعنی جرایمی که فقط با سامانه‌های مخابراتی یا علیه این سامانه‌ها ارتکاب می‌یابند. ب: جرایم ارتباطات مخابراتی. ب: جرایم مخابراتی سنتی (مشترک): به آن دسته از جرایم سنتی گفته می‌شود که با استفاده از سامانه‌های مخابراتی نیز قابل ارتکاب هستند همانند تخریب و جعل داده‌های موجود در سامانه‌های مخابراتی.

۵ - وجوه تشابه و افتراق جرایم رایانه‌ای و مخابراتی با جرایم سنتی: نقطه اشتراک همه جرایم، تعارض آنها با هنجارهای پذیرفته شده جامعه است که مقنن برای ارتکاب آنها مجازات در نظر گرفته است، بنابراین وسیله و محیط ارتکاب جرم تغییری در اصل جرم بودن عمل ندارد. به عنوان نمونه جعل، کلاهبرداری، انتشار مطالب خلاف عفت عمومی، جاسوسی،... در کشور ما جرم محسوب می‌شود و از نظر ماهیت عمل و عنصر تشکیل دهنده جرم تفاوتی ندارد که جعل به وسیله قلم و کاغذ انجام شده باشد یا به وسیله رایانه و کلید را آنه؛ و یا جاسوسی در یک کارخانه غنی سازی اورانیوم اتفاق افتاده باشد یا در سامانه‌ای رایانه‌ای سازمان انرژی اتمی.

در عین حال این اشتراکات نباید ما را از وجوه افتراق جرایم رایانه‌ای از سایر جرایم غافل نماید، بلکه تفاوت‌های این دو به حدی است که به رغم وجود قانون مجازات اسلامی و جرم انگاری اعمالی چون جعل، جاسوسی و جرایم علیه عفت و اخلاق عمومی، مقنن قانون جرایم رایانه‌ای را نیز مصوب و به مواد پایانی قانون مجازات اسلامی افزوده تا جعل و جاسوسی رایانه‌ای را از شکل سنتی این جرایم تفکیک نماید. در ادامه به برخی از این وجوه افتراق پرداخته می‌شود:

الف - برخلاف سایر جرایم، ارتکاب جرایم رایانه‌ای معمولاً از ناحیه هر فردی ممکن نیست بلکه کسانی می‌توانند در ارتکاب آن مباشرت داشته باشند که از تخصص لازم در این زمینه برخوردار باشند. بدیهی است که برای نفوذ در یک سامانه‌های رایانه‌ای و مخابراتی و ارتکاب جعل یا جاسوسی، صرف آشنایی با رایانه برای ارتکاب این جرم کافی نبوده و نیاز به تخصص در این زمینه است.

ب - کشف جرایم رایانه‌ای و دستیابی به مجرم در فضای مجازی امری بسیار پیچیده و دشوار است و آیین دادرسی کیفری متعارف در این زمینه کارایی چندانی ندارد. چرا که دلایلی و اماراتی چون وجود شاهد، اثر انگشت، آثار جنایت،... در این زمینه منتفی بوده و امکان وقوع بزه از ناحیه اتباع سایر کشورها بر دشواری موضوع می‌افزاید.

ج - آثار و نتایج بجا ماندن جرایم رایانه‌ای به لحاظ دامنه انتشار وسیع و بین المللی آن، قابل قیاس با سایر جرایم نبوده؛ به عنوان نمونه، فردی که با تأسیس یک شرکت صوری اقدام به کلاهبرداری از افراد می‌نماید دامنه فعالیت وی محدود به یک شهر و یا به ندرت یک استان بوده و مجالی برای فعالیت بیشتر نمی‌یابد اما جرایم در محیط مجازی حد و مرزی ندارند.

د - برخلاف ایستایی جرایم سنتی در طول زمان‌های متمادی، رفتارهای مجرمانه یا خلاف هنجار قابل ارتکاب در فضای مجازی (به تبع سرعت بالای تحولات و پویایی آن) مدام در حال شکل‌گیری و تحول هستند. مثلاً سرقت و تخریب اموال، ضرب و جرح و قتل، تجاوز به عفت،... از قرن‌های اولیه تاریخ بشر تا کنون جرم بوده لکن سرقت داده، سرقت هویت، تخریب داده، دسترسی غیرمجاز به سامانه‌های رایانه‌ای، جعل داده، کلاهبرداری رایانه‌ای از طریق فیشینگ و اسکیمینگ، سایبر تروریسم،... موضوعات جدیدی هستند که سابقه جرم‌انگاری آنها مربوط به قرن اخیر است. سرعت این تحولات در حدی است که مقنن فرصت کافی برای رویارویی با برخی رفتارهای خلاف هنجار جدید را ندارد و مجرمان رایانه‌ای با استفاده از خلأ قانونی به فعالیت‌های خود تا مدت‌ها ادامه می‌دهند مانند کلاهبرداری تلفنی و پیامکی (مانند وعده برنده شدن در قرعه‌کشی)، استفاده از فیلتر شکن، مبادله ارزهای دیجیتال، جعل هویت،... حتی فضای مجازی شیوه ارتکاب جرایم سنتی را نیز تسهیل و پیچیده نموده و

تفکیک جرایم رایانه‌ای از جرایم سنتی را دشوار نموده است مثل قتل عمدی از طریق ترساندن افراد در فضای مجازی، توهین به افراد در بستر پیام رسان‌ها، اقدام علیه امنیت ملی از طریق شایعه سازی و تشویق افراد به آشوب و خرابکاری...

۶- پیام رسان‌ها و شبکه‌های اجتماعی: تعبیراتی مثل وبلاگ‌ها، شبکه‌های دوست‌یابی، ریچی‌ها، سایت‌های اشتراک گذاری، پیام رسان‌ها، تالارهای گفتگو، گروه‌های ایمیلی و خبرخوان‌ها، همه و همه جلوه‌هایی از شبکه‌های اجتماعی^۱ هستند. پیام رسان‌ها^۲ جزئی از شبکه‌های اجتماعی مجازی هستند که در بستر اینترنت و تلفن همراه فعالیت دارند. شبکه‌های اجتماعی، پیام رسان‌ها هر دو تعبیراتی برای اشاره به ابزارهای ارتباط جمعی مجازی هستند. در مصوبه شورای عالی فضای مجازی راجع به «سیاست‌ها و اقدامات ساماندهی پیام رسان‌های اجتماعی» پیام رسان‌ها چنین تعریف شده‌اند: «منظور از پیام رسان‌های اجتماعی، سامانه‌های کاربر محور فراهم کننده بستر تعاملات اجتماعی برای برقراری ارتباطات فردی و گروهی از طریق تبادل انواع محتواهای چند رسانه‌ای است.» در حال حاضر پر مخاطب ترین شبکه‌های اجتماعی، شبکه فیس بوک است به این دلیل که نسخه پیام رسان فیس بوک نیز پر مخاطب ترین پیام رسان دنیا با بیش از دو میلیارد کاربر است. در کشور ما گرچه شبکه‌های اجتماعی خارجی (مثل فیس بوک) و پیام رسان‌های خارجی (مثل تلگرام و اینستاگرام) محبوبیت زیادی دارند لکن شبکه‌های اجتماعی ایرانی (مثل فیس نما، کلوب و تیبان) و یا پیام رسان‌های ایرانی (مثل سروش، گپ، بیسفون...) نیز فعال و در حال گسترش می‌باشند.

۷- مباشرت و تسبیب در ارتکاب جرم: همانند سایر جرایم، جرایم رایانه‌ای نیز ممکن است به مباشرت و یا به تسبیب ارتکاب یابد. در مباشرت، شخص مجرم اقدام به ارتکاب جرم در سامانه رایانه‌ای و ارتکاب جرم می‌نماید لکن در تسبیب، شخص مجرم با استفاده از نرم افزار (بدافزارها، ویروس‌های رایانه‌ای...) مرتکب جرم می‌شود. در هر حال مطابق مواد ۴۹۲، ۴۹۴ و ۵۰۶ قانون مجازات اسلامی مصوب ۹۲ شخص مجرم (حقیقی و یا حقوقی) به مباشرت و یا تسبیب مسؤول است.

1 - Social network service (s n s)
2 - messenger

۸- سابقه تقنینی: در خصوص جرایم مخابراتی در مواد ۵۸۲ و ۶۴۱ قانون مجازات اسلامی - تعزیرات (مصوب ۱۳۷۵) بحث شود غیرمجاز توسط کارمندان دولت و مزاحمت تلفنی جرم انگاری شده است. لکن نخستین سابقه تقنینی در خصوص جرایم رایانه‌ای در کشور ما، الحاق بند ۳ ماده ۱ قانون مطبوعات در تاریخ ۷۹/۱/۳۰ بود که مقرر شد: «کلیه نشریات الکترونیکی مشمول مواد این قانون است.» تصویب قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه‌ای در تاریخ ۷۹/۱۰/۴ را می‌توان به عنوان اولین واکنش قانونی مستقل در مورد جرایم رایانه‌ای در ایران دانست.

با تصویب قانون مجازات جرایم نیروهای مسلح در سال ۱۳۸۲، مقنن در ماده ۱۳۱ این قانون ارتکاب جرایم نظامی با استفاده از رایانه را نیز جرم انگاری نمود. همچنین در همین سال قانون تجارت الکترونیک به تصویب رسید. مواد ۶۷ تا ۷۷ این قانون در خصوص جرایم تجارت الکترونیک (از قبیل جعل کامپیوتری، نقض حق مؤلف، نقض اسرار تجاری...) است. اما قانون جرایم رایانه‌ای در سال ۱۳۸۸ به تصویب رسید. اختصاصاً به جرایم رایانه‌ای و مخابراتی پرداخت. ساختار و محتویات این قانون تا حدودی از مقررات کنوانسیون جرایم سایبر (مصوب سال ۲۰۰۱ بوداپست)، که کاملترین کنوانسیون بین‌المللی در این زمینه است، پیروی نموده است. جرایم مندرج در این قانون و آیین دادرسی آن‌ها، از نظر کلی، با جرایم و آیین دادرسی مندرج در این کنوانسیون انطباق زیادی دارد (به استثناء جرم سوءاستفاده از نظر مقررات بین‌المللی جرم محسوب نمی‌شود).

نکته مهم

در حال حاضر قانون مستقلی به نام «قانون جرایم رایانه‌ای» وجود خارجی ندارد چرا که مطابق ماده ۵۵ قانون اخیرالذکر مصوب ۱۳۸۸، مواد ۱ تا ۵۴ این قانون به قانون مجازات اسلامی - تعزیرات الحاق شده است. البته مقنن تکلیف مواد ۵۵ و ۵۶ قانون جرایم رایانه‌ای را مشخص ننموده و لذا قانون جرایم رایانه‌ای صرفاً مشتمل بر دو ماده است: مواد ۵۵ و ۵۶!

بعد از سال ۱۳۸۸ قوانین پراکنده دیگری نیز در خصوص جرایم رایانه‌ای به تصویب رسیده که مهمترین آنها الحاق بخش دهم به آیین دادرسی کیفری تحت عنوان «آیین دادرسی جرایم

رایانه‌ای» است. همچنین در بندهای «د» و «ذ» ماده ۳ قانون جرم سیاسی مصوب ۱۳۹۵ ارتکاب برخی جرایم رایانه‌ای از شمول جرم سیاسی مستثنی شده است.^۱ در ماده ۲۳ قانون اصلاح موادی از قانون انتخابات مجلس شورای اسلامی مصوب ۱۳۹۵ نیز آمده است: «کلیه جرائم و تخلفات در خصوص شناسه (کد)ها، صورتجلسات و اسناد الکترونیکی در انتخابات الکترونیکی مشمول مجازات‌های موضوع مواد (۳) تا (۱۱)، (۱۹) تا (۲۱)، (۲۶) تا (۲۹)، (۳۵) تا (۴۸) قانون جرائم رایانه‌ای مصوب ۱۳۸۸/۲۰/۳ می‌باشند.»

البته، برات را به فضای مجازی محدود به موارد فوق نبوده و ما صرفاً به قوانین راجع به جرایم رایانه‌ای اشارة کرده‌ایم.

۹- نرخ جرم در خصوص وضعیت فعلی جرایم فضای مجازی در کشور ما، رئیس پلیس تولید و تبادل اطلاعات ناجا (فتا) در نشست خبری ۹۷/۲/۹ بیان داشته: «جرایم سایبری در کشور از سال ۱۳۹۰ تاکنون ۹۰۰ درصد افزایش یافته است. افزایش این میزان جرم در فضای مجازی به این معناست که به ازای هر یک هزار و ۴۰۰ نفر یک جرم در فضای سایبری در حال رخ دادن است... طبق اطلاعات ارزیابی، جرایم فضای مجازی در تلگرام اتفاق می‌افتد.

روزانه بین ۶ تا ۷ میلیون حمله سایبری در کشور انجام می‌شود که اکثریت آنها دفع می‌شود به طوری که در سال گذشته، ۲۹۶ حمله سایبری جدی گزارش داشتیم که مبدأ و منشاء ۵۰ درصد از این حملات سایبری از سوی آمریکا، چین و ۳۰ درصد از سوی برخی از کشورهای اروپایی مثل هلند و آلمان بوده است. وی با اشاره به اینکه در اجرای این حملات سایبری سازمان یافته از سوی دشمنان؛ بانک‌ها و موسسات پولی و مالی در اولویت اهداف اصلی قرار دارند، گفت: همچنین زیرساخت‌های مخابراتی، حوزه‌های انرژی مثل برق و گاز، صنایع بخش فرآورده‌های نفتی نیز جزء اهداف حملات سایبری اخیر بوده‌اند و اساساً این حملات به دنبال

۱- «د» - اختلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به کار گرفته شده برای ارائه خدمات ضروری عمومی یا حاکمیتی

ذ - کلیه جرائم علیه عفت و اخلاق عمومی اعم از جرائم ارتكابی به وسیله سامانه‌های رایانه‌ای یا مخابراتی یا حاملهای داده یا غیر آن»

اختلال در نظام پولی و بانکی و زیرساخت‌های کشور صورت می‌گیرد و در حوزه پولی و بانکی بیشتر بانک‌هایی مورد هدف واقع شدند که دارای بیشترین مشتری و گردش مالی بودند و بیشترین حملات از نوع دیداس (یعنی ایجاد اختلال) بوده است اما با وجود تلاش‌های بسیار زیاد از سوی مجرمان فضای مجازی و سایبری باید بگوییم تاکنون هیچ آسیب جدی به زیرساخت‌های کشور نداشتیم و با هم افزایی دستگاه‌های مسؤول اقدامات مقابله‌ای و پیشگیرانه مطلوبی صورت گرفته است.

از ۳۰۷ میلیارد جمعیت دنیا، ۲۰۴ میلیارد نفر در زمان حاضر به اینترنت و فضای مجازی دسترسی دارند که در کشور ما در سال ۹۲ این عدد ۳ میلیون و ۴۰۰ هزار نفر بود و امروز بر اساس آمار وزارت ارتباطات، به ۵۶ میلیون نفر افزایش یافته است.

برداشت‌های غیرمجاز از حساب‌های بانکی، مزاحمت‌های اینترنتی، کلاهبرداری‌های رایانه‌ای، هتک حیثیت و نشر اکاذیب و انتشار فیلم‌های خصوصی افراد در شبکه‌های اجتماعی در صدر جرایم سایبری هستند که برداشت‌های غیرمجاز از حساب بانکی افراد در سال ۹۶ نسبت به سال ۹۵، شصت و یک و نیم درصد، مزاحمت‌های اینترنتی، ۶۰ درصد (اساساً این مزاحمت‌ها برای دختر خانم‌ها و خانم‌ها)، کلاهبرداری رایانه‌ای بیش از ۵۵ درصد، هتک حیثیت و نشر اکاذیب بیش از ۳۱ درصد، انتشار فیلم‌های خصوصی و خانوادگی بیش از ۲۲ درصد افزایش داشته که بیشترین جرایم سایبری مربوط به تهران بزرگ، خراسان رضوی، فارس و اصفهان و کمترین جرایم نیز در استان‌های یزد، لرستان، ایلام، کهگیلویه و بویراحمد و جزیره کیش اتفاق افتاده است.^۱

۱۰ - گر چه به لحاظ رویکرد ضد استعماری و ضد استکباری کشور ما در چهل سال اخیر، مواجهه با انواع تحریم‌های ظالمانه (حتی تحریم دارو!) بوده‌ایم اما بخش عمده فضای مجازی کشور در کشور ما هیچ گاه تحریم نبوده است!

* هزاران شبکه ماهواره‌ای و اینترنتی رایگان با محتویات مستهجن، ضد دین، ضد امنیت، تفرقه افکن، ... مدام در حال تأثیرگذاری بر فرهنگ عمومی ما هستند در حالی که دسترسی به

این شبکه‌ها در کشورهای گرداننده‌ی آنها رایگان نیست!

* خبره‌ترین هک‌های بین‌المللی در استخدام شبکه‌های جاسوسی غربی هستند و مدام در صدد هک و نفوذ به سامانه‌های رایانه‌های و مخابراتی حیاتی کشور ما هستند.

* در بحران‌های اجتماعی، شبکه‌های اجتماعی و ماهواره‌ای کشورهای متخاصم نقشی کلیدی در مدیریت بحران و تداوم آن دارند.

* القای باس و ناامیدی، تحقیر ملی و مذهبی، گرایش دادن مردم به سمت ذائقه غربی، ترویج بی‌بند و باری، دلسرد کردن مردم از حاکمیت، ایجاد نارضایتی اجتماعی و آشوب‌های خیابانی در جمله سیاست‌های مشخص و هدفمند بسیاری از شبکه‌های ماهواره‌ای و اجتماعی خارجی است و حتی بخشی از ارتش رژیم صهیونیستی^۱ مأمور اجرای این سیاست‌ها در فضای مجازی ایران است.

با توجه به نمونه‌های اخیرا ذکر، جرایم مطرح در فضای مجازی ما با جرایم و انحرافات مطرح در فضای مجازی سایر کشورها متفاوت بوده و ضرورت دارد که جدا از تدوین سیاست کیفری متناسب، سیاست جنایی مشخصی در بین جرایم و انحرافات فضای مجازی تدوین و اجرا شود مضاف بر این که نهادهای متعین مسئول (شورای عالی فضای مجازی، وزارت ارتباطات، کمیته فیلترینگ...) بایستی تدابیر و اقدامات مناسب و به موقعی را در زمینه مدیریت فضای مجازی اتخاذ و به اجرا در آورند. بدیهی است که سعادت فضای مجازی برای فرهنگ، تمدن، ملت و کشور ما اموری واقعی و ملموس بوده و ارتباطی با اختلافات جناحی نداشته لذا با اختلاف سلیقه و نگرش اعضای این نهادهای مسئول در مورد بحران مدیریت فضای مجازی، همچنان مدیریت فضای مجازی ما در اختیار بیگانگان باقی مانده و به ادعای اطلاع فضای مجازی ما در اشغال دشمن است!

۱۱- با توجه به اینکه مقنن در ماده ۱۰۳ قانون مجازات اسلامی (مصوب ۹۲) اصل را بر قائل شدن گذشت بودن کلیه جرایم گذاشته و استثنائات را در ماده ۱۰۴ همین قانون به تصریح آورده است، یکی از ایرادات عمده در خصوص فصل جرایم رایانه‌ای این است که مقنن در خصوص

قابل گذشت بودن برخی از جرایم رایانه‌ای دارای شاکی خصوصی سکوت نموده و لذا کلیه جرایم رایانه‌ای غیرقابل گذشت هستند حتی هتک حیثیت، کلاهبرداری رایانه‌ای، دسترسی غیر مجاز و انتشار داده‌های خصوصی! به جاست که مقنن در اصلاحات بعدی، این مطلب مهم مورد توجه قرار دهد.

۴- همچنان که در ماده ۵۵ قانون جرایم رایانه‌ای آمده: «شماره مواد ۱ تا ۵۴ این قانون به عنوان مواد مجازات اسلامی (بخش تعزیرات) با عنوان فصل جرایم رایانه‌ای منظور و شماره ماده ۷۲۹ قانون مجازات اسلامی به شماره ۷۸۳ اصلاح گردد.» بنابراین شماره مواد مجازات اسلامی اصلاحیه فوق درج گردیده است. شایان ذکر است که به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری، مواد ۷۵۶ الی ۷۷۹ قانون مجازات اسلامی - تعزیرات (مواد ۲۸ تا ۵۱ قانون جرایم رایانه‌ای) نسخ شده و مواد ۶۶۴ تا ۶۸۷ قانون آیین دادرسی کیفری جایگزین آن شده است.

در ادامه به بررسی ماده به ماده «فصل جرایم رایانه‌ای» این قانون مجازات اسلامی - تعزیرات و مواد مرتبط از قانون آیین دادرسی کیفری مصوب می‌پردازیم. امید آنکه مباحث مطروحه مفید واقع شده و صاحب نظران محترم، مؤلفان را از انتقادات و پیشنهادات خود بی نصیب نگذارند.