جهت تهیه این کتاب می‌توانید با شماره تلفن‌های ذیل تماس حاصل نمایید.

۰۲۵-۳۷۷۴۹۲۷۴

۰۹۱۲۶۵۲۵۰۷۰

همچنین می‌توانید در شبکه‌های اجتماعی ایتا و تلگرام با شماره فوق سفارش خود را ثبت فرمایید.

- کانال ایتا: nashrehoghoghepoya
- کانال تلگرام: hoghoghepoyapub
- کانال پیام رسان بله: pooya_law
- کانال پیام رسان سروش: pooyalaw
- فروشگاه اینترنتی: www.hpbook.ir

بسم الله الرحمن الرحیم

تحلیلی بر

جرایم رایانه‌ای و مخابراتی

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

سید مهدی صنعتی

مجید عطایی جنتی

(قضات دادگستری)

تقدیم به:

فرمانده جاوید الاثر «حاج احمد متوسلیان»

سلام ای شیرِ درزنجیرِ صهیون

سلام ای یوسفِ گمگشته‌ی ما

***

چو یعقوب آرزو داریم هر دم

«عزیزِ قدس» روزی خواهد آمد...

فهرست مطالب

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 وگسترده 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، ارسال آنلاین فیلم و عکس، گفت و گوی همزمان چند صد یا چندهزار 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 فعالیت گسترده اقشار مختلف مردم در پیام رسان‌ها و شبکه‌های اجتماعی دارد مثلا گفته می‌شود که در برهه‌ای بالغ بر چهل میلیون ایرانی در تلگرام فعالیت داشته‌اند! واقعا آیا در سطح جامعه و در فعالیت‌های فیزیکی 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 فعالیت‌های دولت‌ها، کاهش آلودگی محیط زیست از طریق کاهش ترددهای 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 موافقند 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 مثلا 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 که کاری از دست ما بر نمی‌آید یا امکان شناسایی مجرم وجود ندارد، سرخورده می‌شوند و حاکمیت را ناتوان تلقی می‌کنند!

چالش پیام رسان‌ها و شبکه‌های اجتماعی، زمانی به اوج می‌رسد که این ابزارها از خارج از مرزهای کشور مدیریت شده 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 ارتکاب فعالیت‌های مجرمانه خود مشغول بوده و به جای ارتکاب اعمال مجرمانه در سطح جامعه که با ریسک بالایی مواجه است، با آرامش خیال و از طریق نرم افزارهای پیشرفته به اهداف شوم خود دست می‌یابند. بی جهت نیست که اخیرا بسیاری از کشورها از جمله روسیه، فرانسه و ایران در 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[1] تعاریف گوناگونی ارائه شده است که از جمله گفته شده: کامپیوتر یا رایانه، وسیله یا دستگاهی است که می‌تواند اطلاعات و 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

1 - Computer

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 می‌کنندپردازش 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. [۲]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 اینترنتی، تجارت الکترونیک، دریافت نرم افزار و...، و پست الکترونیک برای ارسال و دریافت سریع و ارزان پیام‌ها از طریق اینترنت کاربرد دارد. [۳]

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

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

همچنین بند ب ماده ۱ آیین نامه "نحوه استفاده از سامانه‌های رایانه‌ای یا 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 چنین 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، ص۳۲.

۲ – مهدوی عرب، مهندس مهدی، آشنایی با کامپیوتر، انتشارات بهینه، چاپ پنجم، ۱۳۷۹، تهران، صص۱۵و ۱۶.

۳ – موران، جیمز، آموزش ICDLبه زبان ساده، مهارت هفتم: اطلاعات و ارتباطات، مترجم علی اکبر متواضع، مؤسسه دیباگران تهران، چاپ یازدهم، ۱۳۸۳، صص۱۹و۲۰.

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

در بند ب ماده ۱ لایحه جرایم رایانه‌ای پیشنهادی قوه قضاییه، که در زمان تصویب حذف شده، سیستم مخابراتی[1] 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 بوسیله پروتکل‌هایی که برای گیرنده قابل فهم و تفسیر باشد.

سیستم‌های 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 سوی کنترل و مدیریت سامانه‌های مخابراتی بدون سامانه‌های رایانه‌ای میسر نیست. بنابراین رابطه سامانه‌های رایانه‌ای با سامانه‌های مخابراتی مانند رابطه‌ی جسم و روح در بدن موجودات زنده است که مکمل همدیگرند. بر همین مبنا است که مقنن در فصل جرایم رایانه‌ای، همه جا جرایم 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

1 - Communication System

مفهوم آن را محدود می‌نماید. [۱]

۳ – مفهوم جرایم رایانه ای[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 اخلال 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 اعم 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 ارتکابی در بستر اینترنت و فضای مجازی نمود بلکه با توجه به جرایم مطرح در قانون جرایم رایانه‌ای، مهم ارتکاب جرم علیه سامانه‌های رایانه‌ای یا علیه داده‌ها و یا به وسیله رایانه است اعم از این 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 وسیله‌ی ابزارهای 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، ص۳۸.

۴ – ترکی، غلامعباس، نگرش علمی و کاربردی به قانون جرایم رایانه‌ای، قسمت اول، ماهنامه دادرسی، شماره ۷۷، آذر و دی ۱۳۸۸، ص۱۲.

۵ – نوریان، علیرضا، همان، صص۱۹ و ۲۰.

مخابراتی باید این گونه تعریف شود: فعل یا ترک فعـل مجرمانـه کـه بـا اسـتفاده از وسـایل و شبکه‌های ارتباطی – مخابراتی و یا علیه آن‌ها روی دهد در قانون نیـز بـرای آن‌هـا مجـازات تعیین شده باشد. [۱] در مواد مربوط از فصل جرایم رایانه‌ای اگر چه به تصریح تعریفـی از جـرایم مخابراتی نیامده اما همچنان که در ماده ۷۸۰ این قانون به صورت ضمنی، جرایم مخـابراتی را جرایمی دانسته که در آنها از سامانه مخابراتی به عنوان وسیله‌ی ارتکـاب جـرم اسـتفاده شـده باشد. جرایم مخابراتی همانند جرایم رایانـه‌ای بـه دو دسـته تقسـیم مـی‌شـوند: الـف: جـرایم مخابراتی محض – یعنی جرایمی که فقط با سامانه‌های مخابراتی یا علیه این سامانه‌ها ارتکاب می‌یابند همانند شنود غیر مجاز ارتباطات مخابراتی. ب: جرایم مخابراتی سـنتی (مشـترک): بـه آن دسته از جرایم سنتی گفته می‌شود که با استفاده از سامانه‌های مخابراتی نیز قابـل ارتکـاب هستند همانند تخریب و یا 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، تأثیری در اصل جرم بودن عمـل نـدارد. بـه عنوان نمونه جعل، کلاهبرداری، انتشار مطالب خلاف عفت عمومی، جاسوسی،... در کشـور مـا جرم محسوب می‌شود و از نظر ماهیت عمل و عناصر تشکیل دهنده جـرم تفـاوتی نـدارد کـه جعل به وسیله قلم و کاغذ انجام شده باشد یا به وسیله صفحه کلید رایانـه؛ و یـا جاسوسـی در یک کارخانه غنی سازی اورانیوم اتفاق افتاده باشد یا در سامانه‌هـای رایانـه‌ای سـازمان انـرژی 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 انگـاری 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 رایانـه‌ای را از شکل سنتی این جرایم تفکیک نماید. در ادامه به برخی از این وجوه افتراق پرداخته می‌شود:

---

۱ – زررخ، احسان، جرایم مخابراتی، مجله حقوقی دادگستری، شماره ۶۹ بهار ۱۳۸۹، ص۴۱.

الف – برخلاف سایر جرایم، ارتکاب جرایم رایانه‌ای معمولا از ناحیه هر فـردی ممکـن نیسـت بلکه کسانی می‌تواند در ارتکاب آن مباشرت داشته باشد کـه از تخصـص لازم در ایـن زمینـه برخوردار باشد. بدیهی است که برای نفوذ در یک سامانه‌های رایانـه‌ای و مخـابراتی و ارتکـاب جعل یا جاسوسی، صرف آشنایی با رایانه برای ارتکاب این جرم کافی نبوده و نیاز به تخصـص 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 چنـدانی نـدارد. چـرا کـه دلایلـی 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 مانده از جرایم رایانه‌ای به لحاظ دامنه انتشار وسیع و بین المللی آن، قابـل قیاس با سایر جرایم نبوده؛ به عنوان نمونه فردی که با تأسیس یک شرکت صـوری اقـدام بـه کلاهبرداری از افراد می‌نماید دامنه فعالیت وی محدود به یک شهر و یا به ندرت یـک اسـتان بوده و مجالی برای فعالیت بیشتر نمی‌یابد اما جرایم در محیط مجازی حد و مرزی ندارند.

د – بر خلاف ایستاییِ جرایم سنتی در طول زمان‌های متمادی، رفتارهای مجرمانه یـا خـلاف هنجارِ قابل ارتکاب در فضای مجازی (به تبع سرعت بالای تحـولات و پویـایی آن) مـدام در حال شکل گیری و تحول هستند. مثلا سرقت و تخریب اموال، ضرب و جرح و قتل، تجاوز به عنف،... از قرن‌های اولیه تاریخ بشر تا کنون جرم بوده لکن سرقت داده، سرقت هویت، تخریب داده، دسترسی غیرمجاز به سامانه‌های رایانه‌ای، جعـل داده، کلاهبـرداری رایانـه‌ای از طریـق فیشینگ و اسکیمینگ، سایبر تروریسم،... موضوعات جدیدی هستند که سـابقه جـرم انگـاری 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 اسـتفاده از خـلا قانونی به فعالیت‌های خود تا مدت‌ها ادامه می‌دهند مانند کلاهبرداری تلفنی و پیـامکی (ماننـد وعده برنده شدن در قرعه کشی)، اسـتفاده از فیلتـر شـکن، مبادلـه ارزهـای دیجیتـال، جعـل هویت،.... حتی فضای مجازی شیوه ارتکاب جرایم سنتی را نیـز تسـهیل و پیچیـده نمـوده 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، ویکی‌ها، سایت‌های اشتراک گذاری، پیام رسان‌ها، تالارهای گفتگو، گروه‌های ایمیلی و خبرخوان‌ها، همه و همه جلوه‌هایی از شبکه‌های اجتماعی[1] هستند. پیام رسان ها[2] جزئی از شبکه‌های اجتماعی مجازی هستند که در بستر اینترنت و تلفن همراه فعالیت دارند. شبکه‌های اجتماعی و 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 که اتفاقا نسخه پیام رسان فیس بوک نیز پر مخاطب ترین پیام رسان دنیا با بیش از دو میلیارد کاربر است. در کشور ما گر چه شبکه‌های اجتماعی خارجی (مثل فیس بوک) و پیام رسان‌های خارجی (مثل تلگرام و اینستاگرام) محبوبیت زیادی دارند لکن شبکه‌های اجتماعی ایرانی (مثل فیس نما و کلوب و تبیان) 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 ممکن است به مباشرت و یا به تسبیب ارتکاب یابد. در مباشرت، شخص مجرم اقدام به نفوذ در سامانه رایانه‌ای و ارتکاب جرم می‌نماید لکن در تسبیب، شخص مجرم با استفاده از نرم افزارها (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 - massenger

۸ – سابقه تقنینی: در خصوص جرایم مخابراتی در مواد ۵۸۲ و ۶۴۱ قانون مجازات اسلامی – تعزیرات (مصوب ۱۳۷۵) بحث شنود غیرمجاز توسط کارمندان دولت و مزاحمت تلفنی جرم انگاری شده است. لکن نخستین سابقه تقنینی در خصوص جرایم رایانه‌ای در کشور ما، الحاق تبصره 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 که 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 که اختصاصا به جرایم رایانه‌ای و مخابراتی پرداخت. ساختار و محتویات این قانون تا حدودی از مقررات کنوانسیون جرایم سایبر (مصوب سال۲۰۰۱ بوداپست)، که کاملترین کنوانسیون بین المللی 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 جاسوسی که از نظر مقررات بین المللی 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 صرفا 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

بخش یکم : جرایم و مجازات ها

فصل یکم: جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

مبحث یکم: دسترسی غیر مجاز[1]

ماده ۷۲۹ قانون مجازات اسلامی - تعزیرات: «هر کس به طور غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله‌ی تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال و یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هردو مجازات، محکوم خواهد شد.»

شرح ماده :

۱ - «**هر کس**»: از ظاهر ماده چنین به نظر می‌رسد که مرتکب جرم موضوع این ماده، با توجه به ترکیب "هر کس" در صدر ماده و با توجه به مجازات حبس در نظر گرفته شده، باید شخص حقیقی باشد و شامل اشخاص حقوقی نمی‌شود؛ اما با مراجعه به فصل ششم این قانون ملاحظه می‌شود که مسؤولیت کیفری برای اشخاص حقوقی نیز در قبال کلیه جرایم مندرج در این قانون در نظر گرفته شده است و علاوه بر این که آمر و مرتکب جرم را مستحق مجازات مربوطه شناخته، برای شخص حقوقی نیز مجازات‌هایی وضع شده است. بنابراین کلیه جرایم مندرج در این قانون از ناحیه اشخاص حقیقی و حقوقی قابل ارتکاب و قابل مجازات است.

ماده ۱۴۳قانون مجازات اسلامی مصوب ۹۲ نیز در همین خصوص مقرر داشته: «در مسؤولیت کیفری اصل بر مسؤولیت شخص حقیقی است و شخص حقوقی در صورتی دارای مسؤولیت کیفری است که نماینده قانونی شخص حقوقی به نام یا در راستای منافع آن مرتکب جرمی شود. مسؤولیت کیفری اشخاص حقوقی مانع مسؤولیت اشخاص حقیقی مرتکب جرم نیست.»

۲ - «به طور غیر مجاز... دسترسی یابد»: دسترسی در لغت به معنی قدرت، توانایی، توانگری و قدرت دست یافتن به چیزی است[2]؛ در اصطلاح دسترسی توانایی یک کاربر جهت مشاهده

---

1 - Unauthorized Access

۲ - عمید، حسن، فرهنگ عمید، جلد اول، انتشارات امیر کبیر، چاپ بیست و هفتم، تهران، ۱۳۸۴، ص۹۴۹.

کردن، تغییر دادن و ارتباط برقرار کردن با یک فایل در یک سامانه‌ی رایانه‌ای است. [۱] در اصطلاح حقوقی، دسترسی غیر مجاز عبارت است از رخنه غیرقانونی به سامانه رایانه‌ای حفاظت شده. [۲]

داده‌های رایانه‌ای یا مخابراتی از نظر سطح دسترسی افراد به آنها در این قانون به سه دسته قابل تقسیم‌اند: ۱ – داده‌ها و ارتباطات عمومی: مانند داده‌های موجود در سایت‌های خبری، ۲ – داده‌ها و ارتباطات غیر عمومی (محرمانه): مانند نامه‌های الکترونیکی خصوصی و یا اطلاعات مربوط به حساب‌های بانکی افراد و سازمان‌ها و یا مکالمات تلفنی افراد و مقامات رسمی؛ این داده‌ها ممکن است به وسیله تدابیر امنیتی محافظت شوند. ۳ – داده‌های سری: موضوع ماده ۷۳۱ قانون مجازات اسلامی(تعزیرات).

بدیهی است که دسترسی همگان به داده‌ها و ارتباطات عمومی مجاز است و اساسا این داده‌ها و ارتباطات عمومی شده‌اند که افراد آزادانه از محتویات آن‌ها اطلاع یابند. اما دستیابی به داده‌ها و ارتباطات غیر عمومی و سری فقط برای افراد و مقامات خاصی مجاز است که مالک و یا متصرف قانونی داده های خصوصی و یا مسؤول حفاظت و بهره برداری داده های عمومی و یا دولتی باشند. بنابراین مراد قانون گذار از عبارت «غیر مجاز»، یعنی بدون اذن و یا رضایت شخص مالک یا متصرف قانونی رایانه (در رابطه با رایانه‌های شخصی) و یا بدون اذن مقام صالح عمومی و یا دولتی(در مورد رایانه‌های دولتی).

به طور کلی آنچه که از عبارت دسترسی غیر مجاز به ذهن متبادر می‌شود این است که دسترسی توأم با توسل به شگردهای متقلبانه و نقض تدابیر امنیتی بوده است و شخص مستقیم و یا غیر مستقیم ، با توسل به ترفند ها و مهارت های لازم، به داده‌های رایانه‌ای یا مخابراتی که تحت حفاظت تدابیر امنیتی قرار دارند، دست می‌یابد. بنابراین دسترسی همیشه با فعل مثبت مادی قابل تحقق است و امکان وقوع این جرم با ترک فعل منتفی است.

پرسش ۱ :

آیا صرف دستیابی بدون مجاز به داده‌ها و سامانه‌ها (صرف نظر از اینکه فرد متهم قدرت فهم

---

۱ – ترکی، غلامعباس، نگرش علمی و کاربردی به قانون جرایم رایانه‌ای، قسمت دوم، ماهنامه دادرسی، شماره ۷۸، ص۱۳.

۲ – عالی پور، حسن، حقوق کیفری فناوری اطلاعات، انتشارات خرسندی، چاپ چهارم، تهران، ۱۳۹۵، ص ۱۵۹

و استفاده از داده ها را داشته یا نداشته)، موجب تحقق جرم دسترسی غیرمجاز می‌گردد یا این که قابلیت استفاده از داده‌ها نیز برای متهم شرط است؟ به عنوان نمونه فردی به داده‌های موجود در شبکه بانکی دست می‌یابد اما چون این داده‌ها به زبان انگلیسی است و فرد نفوذ کننده با این زبان آشنا نیست، قادر به مطالعه و اطلاع یافتن از مفاد آن نیست در این قبیل موارد آیا جرم دسترسی غیر مجاز محقق شده است یا خیر؟

پاسخ:

اصل بر این است شخصی که به داده‌ها دسترسی یافته توانایی درک محتوای آنها و یا بهره برداری از داده ها را نیز دارد مگر اینکه متهم بتواند خلاف این اصل را اثبات کند؛ چرا که حتی اگر خود فرد فاقد این توانایی باشد با وجود امکانات پیشرفته موجود، به راحتی می‌تواند داده‌ها را به هر زبانی ترجمه نماید و یا برای درک محتوای تخصصی آنها، با متخصصین مربوط ارتباط صوتی یا تصویری برقرار نماید و یا بعد از دسترسی داده ها را ذخیره یا منتقل نماید.

پرسش ۲ :

شاکی بعد از طرح شکایت تحت عنوان دسترسی غیر مجاز ، در اثنای رسیدگی ، اعلام می دارد که نسبت به دسترسی متهم به سامانه رایانه ای تحت مالکیت خود رضایت داشته و شکایتی در این خصوص ندارد. تکلیف قاضی پرونده در این خصوص چیست؟

پاسخ:

اولا: جرم دسترسی غیر مجاز مانند همه جرایم این فصل غیر قابل گذشت بوده و صدور قرار موقوفی پیگرد منتفی است. ثانیا: دسترسی در شرایطی غیر مجاز است که بدون اذن و یا رضایت ذینفع باشد و به محض اینکه رضایت شاکی برای دسترسی جلب شد (چه قبل و چه بعد از طرح شکایت) ، اتهام دسترسی غیر مجاز منتفی بوده و به لحاظ عدم احراز شرایط تحقق جرم و عدم تحقق عنصر معنوی جرم، قاضی پرونده بایستی نسبت به صدور قرار منع تعقیب و یا حکم برائت اقدام نماید.

۳ – «**داده‌ها**»: در بند الف ماده ۲ قانون تجارت الکترونیکی از داده (اطلاعات) به عنوان داده پیام یاد شده است و در تعریف آن مقرر می‌دارد: «داده‌پیام» (Data Message): هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسائل الکترونیکی، نوری و یا فناوری‌های جدید

اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.»

به طور کلی مراد از «داده»، کلیه‌ی ورودی‌ها و خروجی‌های رایانه اعم از نوشته، صوت، تصویر و فیلم است. باید توجه داشت که منظور از داده لزوماً یک داده‌ی دسته بندی شده نیست بلکه حتی یک مرحله قبل از دسته بندی اطلاعات ورودی را نیز داده می‌نامند. داده‌ها از نظر حجمی دارای سلسله مراتبی به شرح آتی هستند: ۱ – بیت (Bit): کوچک ترین واحد داده‌های رایانه‌ای است که تنها می‌تواند دو نوع داده صفر و یک را کد بندی نماید. نکته قابل توجه این که رایانه‌ها برای خواندن و پردازش داده‌ها الزاما آنها را به صورت صفر و یک در می‌آورند. ۲ – بایت (Byte): هر هشت بیت یک بایت را تشکیل می‌دهد. ۳ – کیلو بایت (Kilobyte): هر ۱۰۲۴ بایت یک کیلو بایت را تشکیل می‌دهد. ۴ – مگا بایت (Megabyte): هر ۱۰۲۴ کیلو بایت یک مگا بایت را تشکیل می‌دهد. ۵ – گیگابایت (Gigabyte): هر ۱۰۲۴ مگابایت یک گیگابایت را تشکیل می‌دهد. ۶ – ترابایت (Terabyte): هر ۱۰۰۰ گیگابایت یک ترابایت را تشکیل می‌دهد. ۷ – پتابایت (Petabyte): هر ۱۰۰۰ ترابایت یک پتابایت را تشکیل می‌دهد.[۱]

البته محققین داده‌ها را به انواع مختلفی تقسیم نموده‌اند که از جمله آن می‌توان به داده‌های رایانه‌ای و داده محتوا (داده پیام) اشاره نمود.[۲] به نظر می‌رسد تفصیل این بحث، در خصوص این قانون فاقد فایده عملی است چرا که مقنن در این قانون داده‌ها را به صورت مطلق مورد نظر داشته که شامل هر نوع داده‌ای می‌گردد و قیدی برای تخصیص این مفهوم نیامده است.

پرسش ۳:

متهمی به داده های موجود در رایانه شخصی شاکی دسترسی غیرمجاز یافته لکن مدعیست که هیچ داده ارزشمند یا محرمانه ای در این رایانه نبوده و صرفا حاوی داده های عمومی (از قبیل فایل های موسیقی) بوده است در فرض صحت ادعای متهم، آیا جرمی اتفاق افتاده است یاخیر؟

پاسخ:

فلسفه جرم انگاری دسترسی غیر مجاز، حمایت از حریم خصوصی اشخاص است و صرف نظر

---

۱ – خلیق، غلامرضا، اپراتوری مقدماتی، انتشارات راهی، چاپ هفتم، تهران، ۱۳۸۱، ص۲۰.

۲ – ر. ک. جاوید نیا، جواد، جرایم تجارت الکترونیکی، انتشارات خرسندی، چاپ دوم، تهران، ۱۳۸۸، صص۵۸ إلی ۶۶

از اینکه چه نوع داده ای در سامانه نگهداری می شود، صرف دسترسی غیـر مجـاز بـه سـامانه مجهز به تدابیر امنیتی جرم است.

۴ – «**سامانه‌های رایانه‌ای یا مخابراتی**»: در بند های ۱ و ۲ مقدمه همین کتاب در خصوص مفهوم سامانه های رایانه ای و مخابراتی به میزان نیاز بحث شده است که ضمن ارجاع بـه آن، از تکرار مباحث خودداری می شود.

۵ – «**تدابیر امنیتی**»: منظور از تدابیر امنیتـی ایجـاد محـدودیت یـا ممنوعیـت دسترسـی بـه اطلاعات برای افراد غیر مجاز با توجه به طبقه بندی و ارزش اطلاعـاتی داده هاسـت[۱]. بنـد ح ماده ۲ قانون تجارت الکترونیک در تعریف اصطلاح مشابه «سیستم اطلاعاتی مطمئن[۲]» مقرر می‌دارد: سیستم اطلاعاتی است که: ۱ – به نحوی معقول در برابر سوء استفاده و نفوذ محفـوظ باشد. ۲ – سطح معقولی از قابلیت دسترسـی و تصـدی صـحیح را دارا باشـد. ۳ – بـه نحـوی معقول متناسب با اهمیت کاری که انجام می‌دهـد پیکربنـدی و سـازماندهی شـده باشـد. ۴ – موافق با رویه ایمن باشد.»

به طور کلی در یک تقسیم بندی، تدابیر امنیتی به دو بخش فیزیکـی و غیـر فیزیکـی تقسـیم می‌گردد:

الف – تدابیر امنیتی سخت افزاری (فیزیکی): مانند مکانی امن جهت نگهداری رایانه‌ها، داده‌هـا و سامانه‌های مخابراتی ، استفاده از قفل‌های رمز دار، گماردن افرادی جهت حراست ، ... .

ب – تدابیر امنیتی نرم افزاری: شامل کلیه برنامه ریزی‌هایی است که جهت حفاظت از داده‌هـا وسامانه‌های رایانه‌ای و مخابراتی انجام می‌گیرد. برخی از مصادیق تدابیر امنیتی نرم افزاری بـه شرح ذیل است:

– ایجاد گذر واژه یا رمزنگاری داده ها[۳]: بـه ایـن مفهـوم کـه ورود بـه سـامانه رایانـه‌ای و یـا مخابراتی و همچنین دسترسی به فایل‌ها و حافظه‌های جانبی مستلزم وارد نمودن کـدی باشـد که از قبل برای سامانه تعریف شده و فقط شخص یا اشخاصی از ایـن کـد آگـاهی دارنـد کـه مجاز به دسترسی به سامانه هستند. معمولا افراد برای تلفن همراه و تبلت خود از رمـز عـددی

---

۱ – ترکی، غلامعباس، پیشین، ص۱۴.

2 - System Secure Information

3 - password

یا الگویی استفاده می‌کنند.

– روش فایروال[۱]؛ این روش از جمله تدابیر امنیتی مدیریتی است که در آن کلیه درگاه‌های ورودی و خروجی داده‌ها تحت کنترل بوده به برخی از داده‌ها اجازه خروج داده و از خروج برخی دیگر جلوگیری می‌شود. همچنان که از نام فایر وال پیداست، این روش دیواری آتشین و مستحکم در مقابل نفوذ و دسترسی مجرمین رایانه‌ای و خروج داده‌ها ایجاد می‌نماید.

– استفاده از آنتی ویروس[۲]: ویروس ها[۳]، کرم‌های رایانه ای[۴]، اسب تروا [۵]و بمب‌های ساعتی[۶] در واقع بد افزارهای مخربی هستند که از سوی مجرمین رایانه‌ای برای ایجاد اختلال در سامانه رایانه‌ای خاص و یا کلیه سامانه‌های رایانه‌ای نوشته و منتشر می‌شوند و به همه‌ی این برنامه‌های مخرب اصطلاحا ویروس گفته می‌شود. آنتی ویروس‌ها نیز نرم افزارهایی هستند که برای مقابله و خنثی کردن این برنامه‌های مخرب بر روی سامانه‌های رایانه‌ای نصب و اجرا می‌شوند و در مواردی که، ویروس‌های مخرب وارد سامانه‌ای می‌شود، آنتی ویروس‌ها آن ویروسهای مخرب را شناسایی و از ورودشان جلوگیری کرده و یا آنها را از بین می‌برند.[۷]

– رعایت تدابیر امنیتی در استفاده از پیام رسانها: پیام رسان‌ها با نصب روی حافظه تلفن همراه، طعمه‌هایی مناسبی برای هکرها بوده و با هک و نفوذ در این پیام رسان‌ها، امکان دسترسی به تمام محتویات تلفن همراه (فایل‌های ذخیره شده، مخاطبین، ارتباطات آنلاین، تراکنش‌های بانکی،...) برای هکر به وجود می‌آید. برخی روش‌ها برای ارتقای امنیت کاربران در پیام رسان‌ها عبارت‌اند از: رمزنگاری پیام رسان و فایل‌های مهم، فعال نمودن تنظیمات امنیتی پیام رسان، بررسی مداوم نشست‌های فعال و حذف نشست‌های غیرمجاز، خودداری از در اختیار قرار ندادن تلفن همراه به افراد غیر مطمئن (جهت جلوگیری از ایجاد نشست جدید با نام کاربری قبلی)، خودداری از نصب نرم افزارهای ناشناس، حذف اشتراک (delete accont) قبل از حذف و خروج از پیام رسان‌ها...

---

۱ – fire wal (دیوار آتشین)

۲ – Anti –virus (ضد ویروس)

3 - Viruses
4 - Computer worms
5 - Trojan horses
6 - Logic bombs

۷ – بای، حسینعلی/پور قهرمانی، پیشین، صص۱۶۰ – ۱۷۰.

در هر حال تدابیر امنیتی محدود به این موارد نبوده و به تناسب پیشرفت علوم رایانه‌ای، مجرمین راههای جدیدی برای نفوذ در سامانه‌های حفاظت شده رایانه‌ای پیدا می‌نمایندکه به تناسب آن تدابیر امنیتی نیز در حال پیشرفت است.

نکته مهم

به تصریح ماده ۷۲۹ قانون مجازات اسلامی(تعزیرات) شرط اساسی برای تحقق بزه دسترسی غیرمجاز این است که سامانه های مورد نظر به وسیله یک یا چند مورد از تدابیر امنیتی، حفاظت شده باشند. مفهوم مخالف این جمله این است که اگر سامانه ای به هیچ یک از تدابیر امنیتی مجهز نباشد و شخص غیرمجازی به محتویات آن دسترسی یابد ، اتهام دسترسی غیر مجاز محقق نشده است گر چه ممکن است که با توجه به اقدامات بعدی متهم، مشمول عناوین اتهامی دیگری چون سرقت داده ، جعل، ... باشد.

پرسش ٤ :

خانم الف شکایتی را علیه آقای ب مبنی بر دسترسی غیر مجاز به محتویات تلفن همراه خود مطرح نموده و اعلام داشته که متهم با هک پیامرسان وی، به عکس‌های خصوصی‌اش دسترسی یافته و آنها را در فضای منتشر نموده است. متهم در دفاع از خود اعلام نموده که ادعای خانم الف کذب بوده و این خانم عکس‌ها را در پروفایل خود گذاشته که قابل دانلود برای هر کسی بوده است. با فرض صحت دفاع آقای ب، آیا اتهامی به وی منتسب است یا خیر؟

پاسخ :

اولا: از آنجا که شاکیه شخصا عکس هایش را در معرض دید عموم قرار داده و برای دسترسی به این عکس‌ها هیچ محدودیت یا تدبیر امنیتی اتخاذ نشده، تبعا اتهام دسترسی غیر مجاز منتفی است. **ثانیا:** از آنجا که شاکیه با رضایت خود عکس هایش را در پروفایلش قرار داده، تبعا اتهام انتشار عکس‌های خصوصی (موضوع ماده ۷۴۵ قانون مجازات اسلامی – تعزیرات) منتفی است. **ثالثا:** صرفا در صورتی که عکس‌ها مبتذل و یا مستهجن باشند با رعایت شرایط ماده ۷۴۲ قانون مجازات اسلامی – تعزیرات، موضوع قابل تعقیب کیفری است.

٦ – به نحوه‌ی نگارش ماده این اشکال وارد است که در ابتدای فصل اول از این قانون آمده

است «جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی» و بین واژه‌ها از حرف عطف «واو» استفاده شده است. اما در متن ماده‌ی ۱ از همین قانون مقرر شده است «هرکس به طور غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی....» و به جای «واو» که در ابتدای فصل ذکر شده بود، از حرف ربط «یا» استفاده می‌شود. حال آن که «یا» به نوعی رابط ترادف است ولی «واو» حرف عطف بوده و با وجود آن مفهومی غیر از ترادف به ذهن متبادر می‌شود. بنابراین شایسته بود که در این خصوص دقت نظر بیشتری اعمال می‌شد و بهتر بود برای تفکیک داده‌ها از سامانه‌های رایانه‌ای و از سامانه‌های مخابراتی، «واو» و «یا» را در کنار هم ذکر می‌کرد و بیان می‌نمود: "داده‌ها و یا سامانه‌های رایانه‌ای و یا سامانه‌های مخابراتی "؛ چرا که اصل بر این است که قانونگذار حکیم است و تشریع قوانین از سوی او توأم با حکمت صورت می‌گیرد.

۷ – استثناء قانونی: تبصره ماده ۶۸۳ قانون آیین دادرسی کیفری دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده نظیر پست الکترونیکی یا پیامک را از شمول ماده ۷۲۹ قانون مجازات اسلامی(تعزیرات) استثناء نموده و مشمول مقررات راجع به شنود مکالمات تلفنی (ماده ۷۳۰ قانون) قرار داده است. از آنجا که مجازات مقرر در ماده ۷۳۰ این قانون اشد از ماده ۷۲۹ می‌باشد، به نظر می‌رسد که مقنن با این استثناء قصد داشته که اولا اهمیت حریم خصوصی افراد را در رابطه با نامه‌های الکترونیک و پیامک‌های آنان برجسته نماید؛ ثانیا از آنجا که افراد معمولا برای این پیام‌های خصوصی خود تدابیر امنیتی را لحاظ نمی‌نمایند مقنن خواسته که قید لزوم وجود تدابیر امنیتی برای این پیام‌ها را که در ماده ۷۲۹ آمده، بردارد و دسترسی به آنها را مشمول ماده ۷۳۰ نموده که چنین قیدی برای شنود قرار نداده است؛ ثالثا شنود ارتباطات مخابراتی مستلزم طی نمودن تشریفات خاص و کسب اجازه از قاضی ویژه شنود می‌باشد در حالی که دسترسی به محتویات رایانه‌ای با مجوز از قاضی پرونده ممکن است.

۸ – عناصر جرم: عنصر قانونی جرم دسترسی غیرمجاز ، ماده ۷۲۹ ق.م.ا. است و عنصر مادی آن فعل دسترسی به این داده ها و یا سامانه هاست مشروط به اینکه این داده‌ها و سامانه‌ها به وسیله‌ی تدابیر امنیتی حفاظت شده و دسترسی به آن‌ها به صورت غیر مجاز باشد. عنصر معنوی این جرم، سوءنیت عام مجرم در دسترسی یافتن عالمانه، عامدانه و غیرمجاز به این موارد است .

۹ – دسترسی غیر مجاز از جمله جرائم خاص رایانه‌ای می‌باشد که در محیط سایبر به وقوع می‌پیوندد. به همین دلیل آن را در زیر مجموعه جرائم رایانه‌ای صرف (محض) نیز قرار می‌دهند. دسترسی غیرمجاز در میان جرائم رایانه‌ای جرمی زاینده یا مادر تلقی می‌شود؛ زیرا دارای نقشی مؤثر در وقوع سایر جرائم رایانه‌ای می‌باشد. در برخی موارد دسترسی غیرمجاز عامل تسهیل کننده در وقوع سایر جرایم رایانه‌ای (و حتی جرائم سنتی) است و در برخی موارد دیگر به عنوان مقدمه ارتکاب جرم تلقی می‌شود. از بعد آماری، چه از نظر میزان وقوع و چه از نظر میزان خسارات در سطح بالایی قرار دارد. به همین دلیل، کنوانسیون بوداپست، در ماده ۲ خود هر یک از اعضا را ملزم به وضع قوانین و مقرراتی نموده که هر نوع دسترسی عمدی من غیر حق را به تمام یا قسمتی از سیستم رایانه‌ای خود، یک فعل مجرمانه تلقی کنند. [۱]

جرم دسترسی غیرمجاز در واقع مقدمه‌ای برای اکثر جرایم مندرج در قانون و به عبارتی جرم پایه است. چرا که لازمه وقوع جرایمی چون جعل، جاسوسی، شنود، سرقت داده‌ها، ...دسترسی به این داده هاست. بنابراین اگر هدف مجرم از دسترسی به داده‌ها مشخص نبود، حداقل می‌توان وی را به عنوان دسترسی غیر مجاز تحت پیگرد قرار داد.

۱۰ – دسترسی به این داده‌ها در صورتی جرم است که متهم یا متهمین شخصا در عملیات اجرایی نقض تدابیر امنیتی سامانه‌ها و دست یافتن به داده‌ها و سامانه‌ها نقش داشته باشد در غیر این صورت، اگر بعد از ارتکاب این جرم، شخص دیگری به این داده‌ها یا سامانه‌ها دسترسی یابد، شخص اخیر مرتکب جرم موضوع این ماده نشده است مگر اینکه از قبل توافق و تبانی بین آنان وجود داشته باشد که در این صورت بحث مشارکت در جرم مطرح می‌شود.

۱۱ – به طور کلی نفوذ به هر سیستم امنیتی کامپیوتری را هک [۲]می گویند. این نوع عمل مجرمانه شامل دسترسی غیر مجاز به کامپیوترها و نفوذ به سیستم‌های کامپیوتری می‌شود که دارای انگیزه‌های گوناگونی می‌باشد که مهمترین آنها قصد کنجکاوی، تفریح و تفنن بوده و اصولا به قصد آسیب رساندن و بهره برداری مالی انجام نمی‌گیرد و از نظر سِنی بیشتر خدشه زنندگان (Hackers) جوانان و در رده‌ی سنی ۱۵ إلی ۲۴ قرار دارند.... امروزه سیستم‌های

---

۱ – لایحه قانون جرائم رایانه‌ای (گزارش توجیهی)، مرکز مطالعات راهبردی و توسعه قضایی و شورای عالی توسعه قضایی قوه قضائیه، کمیته مبارزه با جرائم رایانه‌ای، فروردین ۱۳۸۳، ص۲۲.

2 - hack

مخابراتی مدرن نیز همچون سایر سیستم‌های کامپیوتری در معرض سوءاستفاده از طریق دستیابی از راه دور قرار می‌گیرند. نفوذ یابندگان با دستیابی به یک سیستم مخابراتی می‌توانند به تمامی شبکه‌ی ارتباطی یک شهر و یا یک کشور نفوذ کنند و از آن سوءاستفاده نمایند. ۱
البته این دسته از هکرها که به قصد سوءاستفاده‌های مختلف از فضای اینترنت، اقدامات خود را انجام می‌دهند کرکرها[۲] می‌نامند، که در واقع هکرهایی بدخواه هستند. آنها به سیستم‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر کنند، فایل‌ها را پاک کنند یا بعضی انواع دیگر ویرانی را ببار آورند. اختلاس، کلاهبرداری یا جاسوسی تنها بخش کوچکی از اهداف احتمالی کرکرها می‌باشد. جاسوسی رایانه‌ای همانطور که بین شرکت‌ها وجود دارد، میان کشورها نیز در جریان است بنابراین امنیت ملی ما را با مخاطره مواجه می‌کند. ارتکاب تروریسم رایانه‌ای، توسعه رایانه‌ای دهشتناک دیگری است که شاید امنیت میلیون‌ها انسان را در سراسر دنیا تهدید کند. هیچ بحثی در این نیست که آنچه کرکرها انجام می‌دهند همان قدر که غیر قانونی است، مخاطره آمیز نیز می‌باشد. [۳] لکن هکرها اصولا برای مقاصد مجرمانه اقدام به هک نمی‌نمایند بلکه هدف برخی از آنان نشان دادن میزان اطمینان تدابیر امنیتی سامانه‌ها و امکان رخنه به آنها است تا مسؤولان مربوط را نسبت به حفره‌های امنیتی سامانه‌های تحت مدیریتشان آگاه نمایند. بنابراین بین هکرها و کرکرها تفاوت اساسی وجود دارد و چه بسا اگر هکری صرفا به اتهام دسترسی غیرمجاز دستگیر شود و برای قاضی پرونده محرز شود که وی صرفا قصد داشته که حفره‌های امنیتی سامانه‌ها را گوشزد نماید، ممکن است که قصد مجرمانه (عنصر روانی) وی محرز نگردد و پرونده منتهی به صدور قرار منع پیگرد و یا رأی برائت گردد.

پرسش ۵ :

آیا استفاده از فیلترشکن (vpn) جرم محسوب می‌شود یا خیر؟

---

۱ – باستانی، برومند، جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، انتشارات بهنامی، چاپ اول، ۱۳۸۳، تهران، صص ۴۷الی۴۹

2 - kracker
3 - www. ilaw. ir

پاسخ :

ممکن است تصور شود کـه اسـتفاده از فیلترشـکن، مصـداق جـرم دسترسـی غیـر مجـاز بـه سامانه‌های رایانه‌ای است. چرا که دولتها با تدابیر امنیتی دسترسی کاربران را به برخی صفحات و محتویات فضای مجازی قطع می‌نمایند و استفاده از فیلترشـکن موجـب نقـض ایـن تـدابیر امنیتی می‌گردد. در این پاسخ بایستی اندکی تأمل نمود؛ کاربرد فیلترشکن، دور زدن و عبـور از فیلترینگ فضای مجازی است. در حقیقت دولت‌ها با لحاظ مصالحی اقدام بـه مسـدود سـازی برخی صفحات فضای مجازی (فیلترینگ برخی نشانی‌های اینترنتی خاص) و یا مسدود سازی برخی محتویات مجرمانه (فیلترینگ هوشمند) می‌نمایند. در حقیقت فیلترینگ، تدبیری امنیتـی از سوی صاحبان صفحات اینترنتی برای عدم دسترسی کاربران به محتویـات آن نیسـت بلکـه تدبیر حکومت‌ها برای عدم دسترسی کاربران به برخی محتویات فضای مجازی است.

مضاف بر اینکه مفهوم «حفاظت» در ماده ۷۲۹ قانون تعزیرات با مفهوم فیلتر یا مسدود نمودن متفاوت است چرا که حفاظت کردن، به منظـور جلـوگیری از دسترسـی افـراد غیـر مجـاز بـه داده‌های با ارزش است در حالی که مسـدود کـردن بـه مفهـوم جلـوگیری از دسترسـی همـه کاربران به داده‌های دارای ارزش مجرمانه است لـذا بایسـتی بـین داده‌هـای حفاظـت شـده و داده‌های مسدود شده فرق گذاشت. با این وصف صرف استفاده کاربران از فیلترشکن، مصـداق دسترسی غیر مجاز موضوع ماده ۷۲۹ قانون مجازات اسلامی – تعزیـرات نمـی‌باشـد و لـذا در حال حاضر برای استفاده از فیلتر شکن جرم انگاری نشـده اسـت. البتـه انتشـار فیلترشـکن در فضای مجازی مشمول عنوان مجرمانه موضوع بند الف ماده ۷۴۳ قانون اخیر است.

پرسش ٦

۱ـ درماده۱ قانون جرایم رایانه‌ای اشاره دارد به دسترسی غیر مجاز به داده‌هـا حـال، منظـور از دسترسی غیرمجاز چیست؟ و این دسترسی به صورت مجازی را از طریق رهگذر سـامانه‌هـای رایانه‌ای می‌باشد یا می‌تواند از طریق فیزیکی و اسنادی نیز صورت پذیرد توضیحاً اینکه برخـی از همکاران معتقدند که دسترسی غیرمجاز با توجه به فصل یکم قانون جرایم رایانـه‌ای تحـت عنوان جرایم علیه محرمانگی و داده‌ها و سیستم‌های رایانـه‌ای و مخـابراتی تـن‌هـا از طریـق دانش فنی و نرم افزاری و از طریق کنش روی داده‌ها در محیط مجازی می‌باشد.

۲ـ اگر فـردی از طریق فیزیـکی رمز ورودی به ایمیل شخصی را بدست آورد با فریب یا سـوء استفاده از اعتماد صاحب ایمیل آیا مشمول ماده۱ قانون جرایم رایانه‌ای می‌شود؟

پاسخ

نظریه مشورتی شماره ۱۳۹۳/۳/۲۴ ـ ۷/۹۳/۶۵۶ اداره کل حقوقی قوه قضائیه:

۱ـ با توجه به اطلاق ماده یک قانون جرائم رایانه‌ای، صرف دسترسی غیرمجـاز بـه داده‌هـا یـا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده باشد مشمول مقـررات ماده مذکور می‌باشد و طریق دسترسی اعم از مستقیم (فیزیکی) یا با واسطه (از طریـق شـبکه) تأثیری در قضیه ندارد.

۲ـ در فرض سؤال صرف به دست آوردن رمز ورودی به ایمیـل اشـخاص جـرم نیسـت ولـی چنانچه از طریق رمزی که به دست آورده، به طور غیر مجاز به داده یا سـامانه دسترسـی پیـدا کند، می‌تواند از مصادیق جرم موضوع ماده یک قـانون جـرائم رایانـه‌ای باشـد. بـه هـر حـال تشخیص مصداق با قاضی رسیدگی کننده است.

مبحث دوم: شنود غیر مجاز[1]

ماده ۷۳۰ قانون مجازات اسلامی – تعزیرات: "هرکس به طور غیر مجـاز محتـوای در حـال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی یـا امـواج الکترومغناطیسـی یـا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیـون (۱۰،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هردو مجازات محکوم خواهد شد."

مقررات مرتبط:

بند و ماده ۱ آیین‌نامه جمع‌آوری و اسـتنادپذیری ادلـه الکترونیکـی: «شـنود: عبـارت اسـت از هرگونه دستیابی به محتوای در حال انتقال ارتباطات غیر عمومی در سـامانه‌هـای رایانـه‌ای یـا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه‌ها و تجهیزات سخت‌افزاری و نرم‌افزاری مربوط.»

1- Sniffing ،Illegal Interception

شرح ماده :

۱ – "محتوای در حال انتقال ارتباطات غیر عمومی": همچنان که پیش تر گفته شد ارتباطات غیر عمومی به ارتباطات بین دو یا چند شخص حقیقی و یا حقوقی اطلاق می‌شود که فقط طرفین ارتباط مجاز به اطلاع یافتن از مفاد آن هستند. منظور از محتوای در حال انتقال این ارتباطات می‌تواند: پیام نوشتاری، صوت، تصویر، فیلم و یا همه این موارد به صورت همزمان باشد که از طریق تلفن ثابت، تلفن همراه، بیسیم‌های اختصاصی، نمابر، چت، ارتباطات ماهواره‌ای، رادیویی، ویدئو کنفرانس، پیام رسان‌ها و شبکه‌های اجتماعی به صورت آنلاین (برخط) در حال تبادل باشد.

از عبارت "محتوای در حال انتقال" استفاده می‌شود که باید متهم به صورت زنده و همزمان با طرفین ارتباط، اقدام به شنود ارتباط نماید البته مقنن در تبصره‌ی ماده‌ی ۶۸۳ قانون آیین دادرسی کیفری دسترسی به محتوای ارتباطات عمومی ذخیره شده نظیر پیام نگار (ایمیل) یا پیامک، همچنین پیام‌های خصوصی موجود در حریم خصوصی پیام رسان‌ها و شبکه‌های اجتماعی، مکالمات ضبط شده توسط نرم افزار موجود در حافظه تلفن همراه،...، را نیز در حکم کنترل محتوای ارتباطات غیر عمومی قرار داده و لذا شنود غیر مجاز تلقی شده است.

۲ – " امواج الکترومغناطیسی یا نوری": امواج الکترومغناطیسی (Electromagnetic waves) عبارتست از انتشار موجی شکل میدان‌های الکتریکی و مغناطیسی که به صورت تشعشعی (عمود بر هم) با فرکانس‌های مختلف از آنتن فرستنده، در محیط اطراف پخش می‌گردد. این امواج شامل امواج رادیویی و راداری,تشعشعات مادون قرمز,امواج نورانی قابل رؤیت تشعشعات ماوراء بنفش، اشعه‌ی ایکس و اشعه‌ی گاما می‌باشد. هنگامی که از سیمی امواج متناوب عبور نماید در اطراف این سیم امواجی پدید می‌آید که مخلوطی از موج مغناطیسی و الکتریکی می‌باشد که عمود بر هم هستند این امواج را امواج الکترومغناطیسی می‌نامند. بنابراین در اطراف سیم‌های برق شهر امواج الکترومغناطیسی وجود دارد. [۱]

* امواج الکترومغناطیسی یک رده از امواج است که دارای مشخصات زیر است:

الف – امواج الکترومغناطیسی دارای ماهیت و سرعت یکسان هستند و دارای سرعتی معادل

۱ – رستمی، محمود، فرهنگ واژه‌های نظامی، انتشارات ستاد مشترک ارتش ج. ا. ا، چاپ اول، تهران، ۱۳۷۸، ص۱۱۷.

سرعت نور هستند و فقط از لحاظ فرکانس، یا طول موج باهم تفاوت دارند.
ب – در طیف امواج الکترومغناطیس هیچ شکافی وجود ندارد. یعنی هر فرکانس دلخواه را می‌توانیم تولید کنیم.
ج – از جمله منابع زمینی امواج الکترومغناطیسی می‌توان به امواج دستگاه رله تلفن، چراغهای روشنایی و نظایر آن اشاره کرد.
د – این امواج برای انتشار خود نیاز به محیط مادی ندارند. قسمت عمده این فیزیک امواج دارای منبع فرازمینی هستند.
ه – امواج الکترومغناطیسی جزو امواج عرضی هستند.
کاربردهای امواج الکترومغناطیسی متنوع و در حال گسترش است که می‌توان به موارد آتی اشاره نمود:
الف – کاربردهای امواج الکترومغناطیسی در مخابرات: از این جمله می‌توان فیبر نوری، دستگاه رله تلفن، موج برها، ماهواره و... اشاره کرد.
ب – کاربردهای امواج الکترومغناطیسی در صنایع نظامی: مانند بمب الکترومغناطیسی، انواع رادار، ردیابهای موشک و....
ج – کاربردهای امواج الکترو مغناطیسی در پزشکی: از قبیل عکسبرداری مغناطیسی، رادیولوژی، سونوگرافی با لیزر، کاربرد اشعه ایکس و گاما درفیزیک پزشکی و...
د – کاربردهای امواج الکترومغناطیسی در صنعت: انواع برشکاریهای لیزری، قطار الکترومغناطیسی و صندلی مغناطیسی و....
ه – کاربردهای امواج الکترومغناطیسی در اخترشناسی: با مطالعه طیف الکترومغناطیسی گسیل شده از جو می‌توان به ساختار اجرام آسمانی پی‌برد. [1]
* گر چه که به نظر می‌رسد مقنن با آوردن ترکیب امواج الکترومغناطیسی یا نوری، امواج الکترومغناطیسی و امواج نوری را معادل هم قرار داده است؛ اما باید دانست که این دو با هم رابطه عموم وخصوص مطلق داشته و امواج نوری بخشی از امواج الکترومغناطیسی هستند. منظور از امواج نوری، امواجی است که در محیط نوری نور تولید شده و با سرعت نور نیز

1 - www. roshd. ir

حرکت می‌کنند.

برای ارسال امواج(سیگنال های) نوری به فاصله‌های بسیار طولانی از کابل نوری(فیبر نوری)[۱] استفاده می شود. کابل نوری به عنوان محیطی امن و سریع برای انتقال امواج نوری مورد استفاده قرار می‌گیرد. این فناوری به لحاظ سرعت، دقت و کیفیت خارق العاده‌ی آن در حال حاضر در تمامی عرصه‌ها، به ویژه در صنایع مخابراتی به سرعت گسترش یافته است و بر تمامی امواج الکترومغناطیسی برتری یافته است. در کشور ما این در سالهای اخیر گسترش فراوانی داشته و در همین راستا قانون صیانت از حریم مسیرهای شبکه کابل فیبر نوری شبکه مادر مخابراتی کشور در مورخ ۸۸/۲/۱ به تصویب مجلس شورای اسلامی به تصویب رسیده است.

۳ – "شنود ": شنود مصدر مرخم از شنودن (شنیدن) است و در اصطلاح حقوقی شنود به هر گونه دریافت محتوای در حال ارسال امواج در فضای تبادل ارتباطات به طور غیر قانونی و پنهانی[۲]گفته می‌شود. شنود کردن به عمل فردی اطلاق می‌شود که با استفاده از تجهیزات مخابرتی یا رایانه‌ای و با قرار گرفتن بر سر راه ارتباطات غیر عمومی، مخفیانه اقدام به دریافت اطلاعات در حال انتقال می‌نماید.

اصل بیست و پنجم قانون اساسی استراق سمع (شنود) مکالمات تلفنی و ضبط و افشای آن را ممنوع اعلام نموده مگر این که به حکم قانون انجام پذیرد. ماده ۵۸۲ قانون مجازات اسلامی، انجام شنود غیر قانونی از سوی مأموران دولت را جرم و مجازات حبس از یک سال تا سه سال و یا جزای نقدی از شش تا هجده میلیون ریال را برای آن در نظر گرفته است.

شنود غیر مجاز مورد نظر ماده ۷۳۰ قانون مجازات اسلامی (تعزیرات)، با جرم شنود موضوع ماده ۵۸۲ همین قانون تفاوت‌هایی به شرح زیر دارد:

الف – جرم شنود موضوع ماده ۵۸۲ قانون مجازات اسلامی (تعزیرات) ویژه جرایم مخابراتی سنتی می‌باشد در حالی که شنود غیر مجاز موضوع ماده ۷۳۰ راجع به شنود در فضای مجازی

---

[۱] - فیبرنوری متشکل از رشته‌های خالص شیشه‌ای است که قطر هر کدام از آنها در حدود قطر موی سر انسان است. فیبرهای نوری، نازک و دراز هستند و در پوششی، به صورت مجموعه‌ای دسته بندی شده‌اند که کابل نوری نامیده می‌شود.

۲ – ترکی، غلامعباس، پیشین، ص۱۶.

نیز می‌شود؛

ب – جرم شنود موضوع ماده ۵۸۲ قانون مجازات اسلامی (تعزیرات) راجع به شنیدن غیر مجاز در حین مکالمات صوتی و احیاناً ضبط آن می‌باشد، در حالی که شنود غیر مجاز (موضوع ماده ۷۳۰ قانون تعزیرات) به کنترل یا نظارت یا مراقبت یا هر نوع رهگیری یا مسیریابی یا بررسی یا تجزیه و تحلیل داده‌ها یا امواج الکترومغناطیسی در حال انتقال جهت اطلاع از محتوای آن و اقدامات مشابه، اطلاق می‌گردد.

ج – جرم موضوع ماده ۵۸۲ قانون مجازات اسلامی (تعزیرات) صرفا از ناحیه‌ی مأموران دولت قابل ارتکاب است؛ در حالی که جرم شنود غیر مجاز موضوع ماده ۷۳۰ از ناحیه‌ی هر شخصی قابل ارتکاب است.

نکته مهم

هر شنودی غیر قانونی و غیر مجاز نیست، مقنن در ماده ۱۵۰ قانون آیین دادرسی کیفری، مقرر نموده: «کنترل ارتباطات مخابراتی افراد ممنوع است، مگر در مواردی که به امنیت داخلی و خارجی کشور مربوط باشد یا برای کشف جرایم موضوع بندهای (الف)، (ب)، (پ) و (ت) ماده (۳۰۲) این قانون لازم تشخیص داده شود. در این‌صورت با موافقت رییس کل دادگستری استان و با تعیین مدت و دفعات کنترل، اقدام می‌شود. کنترل مکالمات تلفنی اشخاص و مقامات موضوع ماده (۳۰۷) این قانون منوط به تأیید رییس قوه قضاییه است و این اختیار قابل تفویض به سایرین نمی‌باشد.

تبصره ۱ – شرایط و کیفیات کنترل ارتباطات مخابراتی به موجب مصوبه شورای عالی امنیت ملی تعیین می‌شود.

تبصره ۲ – کنترل ارتباطات مخابراتی محکومان جز به تشخیص دادگاه نخستین که رأی زیر نظر آن اجراء می‌شود یا قاضی اجرای احکام ممنوع است.»

۴ – عناصر جرم: عنصر قانونی جرم شنود غیر مجاز، ماده ۷۳۰ قانون تعزیرات می‌باشد و عنصر مادی آن فعل شنود کردن می‌باشد و لذا این جرم با ترک فعل محقق نمی‌شود. مقنن شرایط و اوضاع و احوالی را نیز برای این فعل در نظر گرفته که عبارتند از: ۱ – شنود باید به

طور غیر مجاز انجام گیرد. ۲ – محتوایی که مورد شنود غیر مجاز قرار می‌گیرد، در حال انتقال باشد؛ ۳ – محتوای ارتباطات بایستی غیر عمومی باشد ۴ – شنود در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری انجام گیرد.

این جرم مطلق بوده و مقید به نتیجه خاصی نیست. عنصر معنوی این جرم سوءنیت عام متهم در دریافت عالمانه، عامدانه و غیر مجاز محتوای در حال انتقال ارتباطات غیر عمومی است و نیازی به سوء نیت خاص در این جرم نیست؛ چرا که با توجه به مطلق بودن جرم موضوع این ماده، سوءنیت خاص و انگیزه از اجزاء تشکیل دهنده این جرم محسوب نمی‌شوند. [۱]

۵ – به نظر می‌رسد که اگر مکالمات یا پیام‌ها به صورت اتوماتیک و برنامه ریزی شده توسط دستگاههای شنود، ضبط شود تا در فرصت مناسب شنیده شود، در این صورت نیز جرم شنود تحقق یافته است.

۶ – علاوه بر شنود مکالمات تلفنی، شنود ارتباطات رادیویی و تصویری و ماهواره‌ای غیر عمومی، شنود ارتباطات اینترنتی (چت)، و...، همچنان که قبلا گفته شد مطابق تبصره‌ی ماده‌ی ۶۸۳ قانون آیین دادرسی کیفری استثنائا دسترسی به محتوای ارتباطات عمومی ذخیره شده نظیر پست الکترونیکی، پیامک، پیام‌های خصوصی موجود در حریم خصوصی پیام رسان‌ها و شبکه‌های اجتماعی، مکالمات ضبط شده توسط نرم افزار موجود در حافظه تلفن همراه،... نیز شنود غیر مجاز تلقی شده است. لذا دادسراها و دادگاههای کیفری نیز اگر برای کشف یا اثبات جرایم مصرح در ماده ۱۵۰ قانون آیین دادرسی کیفری، نیاز به پیام‌های موجود در تلفن همراه متهمی داشته باشند، بایستی از رئیس کل دادگستری استان کسب مجوز نمایند.

۷ – شنود کننده لازم نیست که خود در عملیات اجرایی شنود کردن نیز دخالت داشته باشد، بلکه نفس شنود کردن ارتباطات غیرعمومی جرم است. بنابراین اگر یک نفر با استفاده از دستگاههای شنود، مفاد ارتباطی را دریافت نماید و عده‌ای نیز همزمان، به این وسیله، آن را شنود نمایند، جرم شنود توسط همه آنها محقق شده است.

---

۱ – آقایی نیا، حسین، جرایم علیه اشخاص (شخصیت معنوی)، نشر میزان، چاپ دوم، تهران، ۱۳۸۶، ص۲۳۸.

مبحث سوم: جاسوسی رایانه‌ای

ماده ۷۳۱ قانون مجازات اسلامی - تعزیرات: «هر کس به طور غیر مجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا شصت میلیون (۶۰،۰۰۰،۰۰۰) ریال یا هردو مجازات.

ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج سال تا پانزده سال.

تبصره۱ - داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره۲ - آئین نامه‌ی نحوه‌ی تعیین و تشخیص داده‌های سری و نحوه‌ی طبقه بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیأت وزیران خواهد رسید.»

قوانین و مقررات مرتبط:

ماده ۱ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳:

« اسناد دولتی عبارتند از هر نوع نوشته یا اطلاعات ثبت یا ضبط شده مربوط به وظایف و فعالیتهای وزارتخانه‌ها و مؤسسات دولتی ووابسته به دولت و شرکتهای دولتی از قبیل مراسلات - دفاتر - پرونده - عکس‌ها - نقشه‌ها - کلیشه‌ها - نمودارها - فیلم‌ها - میکرو فیلم‌ها ونوارهای ضبط صوت که در مراجع مذکور تهیه و یا به آن رسیده باشد.

بدیهی است که اگر کسی بدون این قصد مرتکب این افعال شود موضوع از شمول این ماده خارج و مشمول مواد قبلی است.

۳ – در این ماده واژه «امنیت» یکبار به صورت بسیط ویکبار دیگر به صورت ترکیب اضافی (امنیت عمومی) به کار رفته است و در ظاهر چنین به ذهن متبادر می‌کند که هم به خطر انداختن امنیت خصوصی و هم امنیت عمومی مشمول این ماده می‌شود؛ در حالی که با عنایت به ادامه ماده و مثال‌های ذکر شده، فقط به خطر انداختن امنیت عمومی مورد نظر مقنن بوده است و به خطر انداختن امنیت داده‌های افراد مشمول مواد قبلی این قانون می‌گردد. بنابراین ذکر واژه امنیت به صورت بسیط در ابتدای این ماده زائد به نظر می‌رسد.

۴ – علت تشدید مجازات در این ماده، اهمیت موضوع آن است زیرا موضوع این ماده سامانه‌هایی است که جهت ارائه‌ی خدمات ضروری عمومی به کارگرفته می‌شوند و طبیعتاً ایجاد اخلال یا غیر قابل دسترسی نمودن آنها سبب خلال در نظم عمومی و... می‌گردد. پس چنانچه اقدامات مذکور علیه سامانه‌هایی که خدمات ضروری غیر عمومی ارائه می‌دهند (مثل تجهیزات رایانه‌ای شرکت‌های خصوصی تجاری) صورت پذیرفته باشد مشمول این ماده نخواهد شد چرا که به تصریح ماده و نیز از مثال‌های مذکور درآن، واضح است که مراد وسایل ارائه خدمات ضروری عمومی است. خدمات عمومی مورد نظر ماده اخیر تمثیلی بوده و شامل تجهیزات انتقال داده شرکت مخابرات، سِرورهای پیام رسانهای عمومی،... می‌شود.

فصل سوم: سرقت و کلاهبرداری مرتبط با رایانه

ماده ۷۴۰ قانون مجازات اسلامی –تعزیرات: «هرکس به طور غیر مجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون (۱،۰۰۰،۰۰۰) ریال تا بیست میلیون ریال (۲۰،۰۰۰،۰۰۰) ریال و در غیر این صورت به حبس از ۹۱ روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون ریال (۲۰،۰۰۰،۰۰۰) ریال یا هردو مجازات محکوم خواهد شد.»

شرح ماده :

۱ – قید به طور غیر مجاز در این ماده زائد است و منطقی نیست که کسی بـه صـورت مجـاز داده‌های دیگری را برباید! شایسته بود قانون گذار در این ماده نیز به جای عبارت «به طور غیر مجاز»، از عبارتی نظیر «بدون رضایت» استفاده می‌نمود.

۲ – ربودن داده: سرقت در ماده ۲۶۷ قانون مجازات اسلامی مصوب ۹۲ این گونه تعریف شده: «سرقت عبارت از ربودن مال متعلق به غیر است.» به منظور تبیین و تطبیـق ایـن تعریـف بـر جرم سرقت رایانه‌ای، عناصر این تعریف را به شرح آتی واشکافی می‌نماییم:

الف – ربودن در لغت به معنی ربابیدن، چیزی را با تردستی و چابکی از جایی برداشتن و بـردن آمده است. [۱] مقصود از ربودن، برداشتن و اثبات ید بر مال بدون اجازه و رضایت مالک اسـت. [۲] با این وصف ربودن داده‌ها عبارتست از دریافت داده‌های دیگری بدون اطلاع و رضایت مالـک آن‌ها. به عنوان نمونه فردی با دسترسی به رایانه‌ی دیگری، از تحقیق انجام شـده توسـط وی، کپی برداری کرده و یا اصل تحقیق را بریده [۳] و می‌رباید.

از عموم و اطلاق این ماده چنین برمی آید که کلیه‌ی داده‌ها اعم از ایـن کـه در سـامانه‌هـای رایانه‌ای و یا مخابراتی باشند یا در حامل‌های داده، مشمول این ماده می‌شوند.

پرسش ۱۸:

چنانچه سارقی به قصد سرقت داده‌های دیگری، لپ تاپ یا حامل داده‌هـای وی را برایـد آیـا موضوع مشمول این ماده از فصل جرایم رایانه‌ای است یا موضوع مشـمول جـرایم منـدرج در باب سرقت قانون مجازات اسلامی (تعزیرات) قرار می‌گیرد؟

پاسخ:

با توجه به مفاد ماده ۱۳۴ قانون مجازات اسلامی، فعل ارتکابی متهم دارای دو وصـف کیفـری بوده و مشمول مقررات تعدد معنوی است که بایستی مجازات اشد را در نظر گرفت.

ب – تحقق سرقت رایانه‌ای مستلزم آن است که داده‌های رایانه‌ای مال تلقی شود تا به تبع آن سرقت نیز قابل تحقق باشد؛ به عبارت دیگر، مقدمه تحقق بزه سرقت رایانـه‌ای آن اسـت کـه

---

۱ – عمید، حسن، فرهنگ عمید، جلد دوم، انتشارات امیر کبیر، چاپ بیست و هفتم، تهران، ۱۳۸۴، ص۱۰۳۱.

۲ – شکری، رضا/سیروس، قادر، پیشین، ص۲۱۹.

3 - Cut

داده‌های رایانه‌ای، مال محسوب شوند. با توجه به خرید و فروش نرم افزارها، نام‌های دامنه و... در عصر حاضر و پرداخت مبالغ هنگفتی در ازای آن، تردیدی نیست که این امور در زمره اموال هستند.[۱]

ج – منظور از تعلق مال به غیر، تعلق عین مال به شخص دیگری (اعم از شخص حقیقی یا حقوقی) است. بنابراین از اطلاق ماده برمی آید که داده‌های کلیه‌ی داده‌ها اعم از داده‌های اشخاص حقیقی و حقوقی، دولتی و غیر دولتی مشمول حمایت این ماده قرار می‌گیرد.

نکته:

داده‌ها از این جهت با سایر اموال متفاوت و منحصر به فردند که قابلیت تکثیر از آنها، به هر تعداد، وجود دارد و بر خلاف سایر اموال که با سرقت عین آن‌ها، آن مال کلا از اختیار صاحب آن خارج می‌شود، داده‌ها ممکن است که دارای چندین مورد کپی و نسخه پشتیبان باشند که در صورت ربودن یکی از آن‌ها، امکان استفاده از دیگری و جود دارد. در ضمن با توجه به تأکید قانون بر امکان تحقق بزه سرقت داده‌ها، نباید در مالیت داشتن و با ارزش بودن داده‌های رایانه‌ای تردید نمود.

۳ – در تفسیر عبارت «**چنانچه عین داده در اختیار صاحب آن باشد...**» چند فرض در خصوص این بند متصور است: اول این که شخص مجرم از داده‌های دیگری کپی[۲] برداری کرده و عین داده نزد صاحب آن باقی مانده است، دوم این که مجرم داده‌ها را عینا ربوده اما صاحب داده‌ها نسخه‌ی دیگری از آن را داشته است، سوم اینکه مجرم بعد از سرقت داده و استفاده از آن، داده‌ها را عینا نزد شاکی رها نموده است... از آنجا که تفاوتی بین داده‌های اولیه و داده‌های کپی شده از آن وجود ندارد، بنابراین در هر صورت صاحب داده به داده دسترسی دارد اما از آنجا که شخص دیگری نیز با سرقت داده‌ها به آنها دسترسی یافته و امکان هر گونه سوءاستفاده از آن‌ها متصور است، بنابراین مقنن مجازات جزای نقدی یک میلیون (۱،۰۰۰،۰۰۰) ریال تا بیست میلیون ریال (۲۰،۰۰۰،۰۰۰) ریال را برای آن پیش بینی نموده است.

---

۱ – زررخ، احسان، پیشین، ص۵۳.

نکته :

از عبارت «در غیر این صورت» در این ماده چنین بر می‌آید که مراد قانون گذار مواردی است که شخص داده را به شکل بریدن (cut) و یا با سرقت حامل داده، بدون بقا اثری از آن نزد صاحبش، می‌رباید. در این صورت مقنن با توجه به تبعات منفی جرم، مجازات حبس از ۹۱ روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون ریال (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات را پیش بینی نموده است. در این ماده اشاره‌ای به رد داده‌ها به صاحبش و جبران خسارت وارده نشده است. بی شک در این خصوص بایستی به عمومات آیین دادرسی کیفری مراجعه نمود. [۱]

پرسش ۱۹:

آیا حضور فیزیکی سارق در محل نگهداری سامانه‌های رایانه‌ای و یا مخابراتی لازم است و یا اینکه چنانچه سارق با استفاده از ویروس‌ها (اسب‌های تروا[۲]) اطلاعات سامانه‌ی دیگری را سرقت نماید باز هم این جرم قابل تحقق است؟

پاسخ:

مشابه همین سؤال در خصوص سایر مواد این قانون نیز قابل طرح است. در پاسخ باید گفت که با توجه به عمومیت ماده تفاوتی از این لحاظ وجود نداشته و در هر دو صورت بزه مورد نظر قابل تحقق است. مقررات مربوط به تسبیب در قانون مجازات اسلامی مصوب ۹۲ نیز مؤید همین برداشت است.

---

۱ – ماده ۱۴ق. آ. د. ک. – شاکی می‌تواند جبران تمام ضرر و زیان‌های مادی و معنوی و منافع ممکن‌الحصول ناشی از جرم را مطالبه کند.

تبصره ۱ – زیان معنوی عبارت از صدمات روحی یا هتک حیثیت و اعتبار شخصی، خانوادگی یا اجتماعی است. دادگاه می‌تواند علاوه بر صدور حکم به جبران خسارت مالی، به رفع زیان از طرق دیگر از قبیل الزام به عذرخواهی و درج حکم در جراید و امثال آن حکم نماید.

تبصره ۲ – منافع ممکن‌الحصول تنها به مواردی اختصاص دارد که صدق اتلاف نماید. همچنین مقررات مرتبط به منافع ممکن‌الحصول و نیز پرداخت خسارت معنوی شامل جرایم موجب تعزیرات منصوص شرعی و دیه نمی‌شود.

ماده ۱۵ – پس از آنکه متهم تحت تعقیب قرار گرفت، زیان دیده از جرم می‌تواند تصویر یا رونوشت مصدق تمام ادله و مدارک خود را جهت پیوست به پرونده به مرجع تعقیب تسلیم کند و تا قبل از اعلام ختم دادرسی، دادخواست ضرر و زیان خود را تسلیم دادگاه کند. مطالبه ضرر و زیان و رسیدگی به آن، مستلزم رعایت تشریفات آیین‌دادرسی مدنی است.

2 - Trojan horses

۴ – علاوه بر عنصر قانونی جرم که در این ماده جرم انگاری شده، عنصر مادی جرم سرقت داده‌های رایانه‌ای عبارتست از ربودن داده‌های متعلق به دیگری، که این عمل با فعل مثبت مادی قابل تحقق است. نتیجه‌ی این جرم، قرار گرفتن داده در اختیار سارق است که ممکن است به صورت کلی داده‌ها از اختیار صاحب آن خارج شود و یا نسخه‌ای از آن در اختیار وی باقی بماند. عنصر معنوی این جرم نیز عبارتست از سوءنیت عام مرتکب در انجام عالمانه و عامدانه فعل غیرقانونی، و سوءنیت خاص وی در اراده‌ی تحقق نتیجه جرم که همان ربایش و تسلط بر داده‌های غیر است.

* در پایان بحث سرقت رایانه‌ای توجه مخاطبین محترم را به نظریه اداره حقوقی قوه قضاییه، در پاسخ به سؤالات مطرح شده در همین خصوص جلب می‌نماید:

پرسش ۲۰:

الف) سرقت اطلاعات سری کد شده و رمز دار از شبکه‌های کامپیوتری یا کامپیوترهای شخصی و کشف رمز آن‌ها چه حکمی دارد؟

ب) سرقت و فروش غیر مجاز شماره‌های تلفن همراه (موبایل) توسط آشنایان به تکنیک الکترونیکی مرکزی آن چه حکمی دارد؟

ج) آیا با وجود سایر شرایط امکان اجرای حد سرقت وجود دارد؟

پاسخ:

الف) سرقت اطلاعات سری کد شده و رمز دار از شبکه‌های کامپیوتری یا... مشمول ماده ۱۲ قانون جرائم رایانه‌ای است.

ب) سرقت و فروش غیر مجاز شماره‌های تلفن همراه توسط آشنایان با مقررات ماده ۱۳ قانون منطبق است.

ج) اجرای حد سرقت در جرائم رایانه‌ای محمل قانونی ندارد. (نظریه شماره ۷/۴۴۶۵مورخ ۱۳۸۸/۷/۲۱). [۱]

۱ – ویژه نامه قوانین و مقررات، ضمیمه نشریه پیام آموزش قوه قضاییه، شماره شانزدهم، سال دوم، مهرماه ۱۳۸۹، ص۴۴.

ماده ۷۴۱ قانون مجازات اسلامی –تعزیرات: «هرکس به طور غیر مجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن، به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال یا هردو مجازات محکوم خواهد شد.»

قوانین مرتبط :

ماده ۱ قانون تشدید مجازات جرایم اختلاس ارتشاء و کلاهبرداری: «هرکس از راه حلیه و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌ها یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیر واقع امید وار نماید یا از حوادث و پیش آمدهای غیر واقع بترساند و یا اسم یا عنوان مجعول اختیار کند و به یکی از و سایل مذکور و یا و سایل تقلبی دیگر وجوه یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصا حساب و امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردار محسوب و علاوه بر رد اصل مال به صاحبش، به حبس از یک تا ۷ سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود.

در صورتی که شخص مرتکب بر خلاف واقع عنوان یا سمت مأموریت از طرف سازمان‌ها و مؤسسات دولتی یا وابسته به دولت یا شرکت‌های دولتی یا شوراها یا شهرداری‌ها یا نهادهای انقلابی و به طور کلی قوای سه گانه و همچنین نیروهای مسلح و نهادها و مؤسسات مأمور به خدمت عمومی اتخاذ کرده یا اینکه جرم با استفاده از تبلیغ عامه از طریق وسایل ارتباط جمعی از قبیل رادیو، تلویزیون، روزنامه و مجله یا نطق در مجامع و با انتشار آگهی چاپی یا خطی صورت گرفته باشد یا مرتکب از کارکنان دولت یا مؤسسات و سازمان‌های دولتی یا وابسته به دولت یا شهرداری‌ها یا نهادهای انقلابی و یا به طور کلی از قوای سه گانه و همچنین نیروهای مسلح و مأمورین به خدمت عمومی باشد علاوه بر رد اصل مال به صاحبش، به حبس از ۲تا ۱۰ سال و انفصال ابد از خدمات دولتی و پرداخت جزای نقدی معادل مالی که

اخذ کرده است محکوم می‌شود.

تبصره ۱ در کلیه موارد مذکور در این ماده در صورت وجود جهات و کیفیات مخففه داگاه می‌تواند با اعمال ضوابط مربوط به تخفیف، مجازات مرتکب را فقط تا حداقل مجازات مقرر در این ماده (حبس) و انفصال از خدمات دولتی تقلیل دهد ولی نمی‌تواند به تعلیق اجرای کیفر حکم دهد.

تبصره ۲ –مجازات شروع به کلاهبرداری حسب مورد حداقل مجازات مقرر در همان مورد خواهد بود ودر صورتی که نفس عمل انجام شده نیز جرم باشد، شروع کننده به مجازات آن جرم نیز محکوم می‌شود. مستخدمان دولتی علاوه بر مجازات مذکور چنان چه در مرتبه مدیر کل یا بالاتر یا همطراز انها باشند به انفصال دائم از خدمات دولتی و در صورتی که در مراتب پایین تر باشند به شش ماه تا سه سال انفصال موقت از خدمات دولتی محکوم می‌شوند.»

ماده ۶۷قانون تجارت الکترونیک: «هرکس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده غیر مجاز[1] از «داده پیام»ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف «داده پیام»، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد، مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود.»

شرح ماده :

۱ – هر کس: درکنوانسیون بوداپست و قوانین اکثر کشورها مخصوصاً در زمینه جرایم ارتکابی در محیط سایبر مسئوولیت اشخاص حقوقی پیش‌بینی شده است و قاعدتاً لازم می‌بود که به جای واژه «هر کس»، «هرشخص» آورده شود تا اشخاص حقوقی را نیز شامل شود. اما از آنجایی که برای کلیه جرایم رایانه‌ای، موادی در مورد مسئوولیت کیفری اشخاص حقوقی پیش‌بینی شده (ماده ۱۴۳ قانون مجازات اسلامی مصوب ۹۲) و از طرفی هم مجازات حبس

---

۱ – در تفسیر دوعبارت «سوء استفاده» و «استفاده غیر مجاز» می‌توان گفت: در حالت «سوء استفاده» فرد مجوز استفاده دارد اما استفاده‌ی او به طور صحیح و در محدوده‌ی اختیاراتی که برایش معین گردیده است نبوده اما در حالت «استفاده‌ی غیر مجاز»، فرد اساساً مجوز استفاده نداشته و با توجه به مباحث سابق، مراد، استفاده‌ی غیر قانونی است.

مقرر در ماده مربوطه بر اشخاص حقوقی تحمیل ناشدنی است، از واژهٔ «هر کس» استفاده شده است تا در مورد اشخاص حقیقی به این مواد و در مورد اشخاص حقوقی به مواد مربوطه که ضمانت اجرای مرتبط با مسؤولیت اشخاص حقوقی را پیش‌بینی کرده است، مراجعه شود. [۱]

۲ – در تعریف کلاهبرداری گفته شده: کلاهبرداری عبارتست از بردن مال دیگری از طریق توسل توأم با سوءنیت به وسایل یا عملیات متقلبانه. [۲] انجام عملیات متقلبانه و اغفال قربانی، مشخصه‌ی اصلی جرم کلاهبرداری است که آن را از سایر جرایم مشابه ممتاز می‌نماید. با توجه به عنوان فصل سوم جرایم رایانه‌ای که سرقت و کلاهبرداری مرتبط با رایانه را مطرح نموده و در ماده ۷۴۰ به سرقت پرداخته، مقنن در ماده ۷۴۱ این قانون بی تردید قصد جرم انگاری کلاهبرداری رایانه ای[۳] را داشته است، لکن در این ماده اشاره‌ای به فریب یا همان «مانور متقلبانه» نشده است. علاوه بر این قانون، در ماده ۸ کنوانسیون جرایم سایبر بوداپست نیز در مورد کلاهبرداری رایانه‌ای انجام عملیات متقلبانه را شرط تحقق کلاهبرداری ندانسته است. شاید بتوان علت این امر را در تفاوت کلاهبرداری سنتی با کلاهبرداری رایانه‌ای جستجو نمود؛ به این مفهوم که در کلاهبرداری سنتی بزه دیده انسانی است که کلاهبردار تمام تمرکز خود را بر روی شخص وی معطوف می‌دارد و با انجام عملیات متقلبانه و فریفتن او، اقدام به بردن مال وی می‌نماید. اما در کلاهبرداری رایانه‌ای، قربانی مستقیم جرم سامانه‌های رایانه‌ای یا مخابراتی هستند که کلاهبردار با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل می‌کند. بنابراین در کلاهبرداری رایانه‌ای، از آنجا که امکان فریب دادن سامانه‌های رایانه‌ای یا مخابراتی وجود ندارد، مجرم با ایجاد تغییراتی در این سامانه‌ها، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل می‌کند. در همین خصوص در گزارش توجیهی لایحه جرائم رایانه‌ای آمده است: "در کلاهبرداری رایانه‌ای لازم نیست که شخصی فریب بخورد و یا حتی لزومی به تصور فریب ماشین که همان رایانه است، نمی‌باشد و بنابراین در تدوین لایحه قانونی لزومی به ذکر شرط

---

۱ – لایحه جرائم رایانه‌ای (گزارش توجیهی)، پیشین، ص۴۹.

۲ – میر محمد صادقی، حسین، جرایم علیه اموال و مالکیت، نشر میزان، چاپ نوزدهم، تهران، ۱۳۸۶، ص۵۱.

3 - Computer Fraud

استفاده از وسایل متقلبانه احساس نمی‌شود. [۱]

۳ – «اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه»: اعمالی که در این ماده قید شده تمثیلی بوده و هر عمل دیگری که شباهت با اعمال مذکور در این ماده داشته باشد، مشمول مقررات این ماده قرار می‌گیرد.

الف – وارد کردن داده‌ها: یعنی افزودن داده‌های جدیدی به داده‌های قبلی؛ مثلا شماره حساب خود یا دیگری را در سایت یک شرکت دولتی یا خصوصی برای واریز هزینه خدمات وارد می‌کند.

ب – تغییر داده‌ها: یعنی داده‌های موجود را کاهش، افزایش و یا تعویض می‌نماید؛ مانند این که شماره حساب موجود را با شماره حساب خود جابجا می‌نماید.

ج – محو داده‌ها: یعنی داده‌های موجود را به نحو کلی و یا جزئی از بین می‌برد، مانند این که بخشی از مشخصات و امکانات ثبت شده خود را در سامانه بانکی محو می‌کند تا شرایط اخذ تسهیلات بانکی را بدست آورد.

د – ایجاد داده‌ها: یعنی داده‌های جدیدی را بوجود می‌آورد مانند این که کد رمزی را به تلفن همراه دیگری وارد می‌نمایدکه هزینه‌های تماس خود را به خط دیگری منتقل می‌نماید.

ه – متوقف کردن داده‌ها: یعنی تمام و یا بخشی از دادهای موجود را غیر قابل پردازش نماید مانند این که در مشخصات ثبت شده مربوط به بدهی‌های خود را به بانکی را به نحوی غیر قابل پردازش نماید که بدهکار بودن بودن وی مخفی بماند.

و – مختل کردن سامانه: یعنی اینکه سامانه رایانه‌ای را از نظم و برنامه‌ی جاری خود به صورت کلی و یا جزئی خارج نماید؛ مانند اینکه سامانه ثبت تخلفات راهنمایی و رانندگی را به نحوی مختل نماید که سوابق تخلفات رانندگی خود و دیگران حذف شود.

۴ – «وجه یا مال یا منفعت یا خدمات یا امتیازات مالی»: به طور کلی هر چیزی که دارای ارزش مالی باشد، مشمول این ماده می‌شود؛ اعم از وجه رایج (پول ملی و یا ارزهای خارجی)، مال (هر آنچه که عرف آن را دارای ارزش مادی می‌داند)، منفعت (مانند سود حاصله از سرمایه گذاری دیگری و یا استفاده از اشتراک اینترنت یا تلفن غیر) و خدمات یا امتیازات مالی (مانند

---

۱ – لایحه جرائم رایانه‌ای (گزارش توجیهی)، پیشین، ص۴۸.

استفاده از تسهیلات بانکی و یا هدایای غیر). بنابراین چنانچه کسی با ارتکاب اعمال مذکور در این ماده مدرک تحصیلی اخذ نماید و یا با زنی ازدواج نماید موضوع از شمول این ماده خارج است.

۵ – «برای خود یا دیگری تحصیل کند»: گاهی مجرم به دنبال کسب مال و یا منفعتی برای خود است و گاهی برای دیگری؛ دیگری می‌تواند از بستگان وی باشد و یا غیر آنها. نکته دیگر این که با توجه به عبارت "تحصیل کند"، این جرم مقید به نتیجه تحصیل کردن مال است و بدون محقق شدن این نتیجه، جرم کلاهبرداری رایانه‌ای امکان تحقق ندارد.

۶ – در این ماده، همچون قانون تشدید مجازات جرایم اختلاس ارتشاء و کلاهبرداری، رد مال به صاحب آن به عنوان یکی از مجازات مجرم در نظر گرفته شده و در عدم امکان رد، مثل و یا حداقل قیمت آن باید پرداخت شود. با توجه به سیاق ماده در مواردی که مجرم مال را برای دیگری تحصیل نموده، باز هم مجرم اصلی به رد مال محکوم می‌شود و فرد دیگر که مال به وی رسیده، فقط در صورت اطلاع و هماهنگی قبلی،می تواند به عنوان معاون و یا شریک جرم قابل پیگرد باشد.

۷ – عنصر مادی این جرم ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه است و نتیجه این جرم تحصیل نمودن وجه یا مال یا منفعت یا خدمات یا امتیازات مالی است. عنصر معنوی این جرم عبارتست از سوءنیت عام مرتکب در انجام عالمانه و عامدانه فعل مجرمانه و سوءنیت خاص وی، اراده‌ی تحقق نتیجه جرم که همان تحصیل نمودن وجه، مال، منفعت، خدمات و امتیازات مالی متعلق به غیر است. جرم مذکور در این ماده نیز فقط با فعل مثبت مادی قابل ارتکاب است.

۸ – ممکن است تصور شود که با تصویب این ماده، ماده ۶۷قانون تجارت الکترونیک و همچنین ماده ۱ قانون تشدید مجازات جرایم اختلاس ارتشاء و کلاهبرداری، نسخ شده است، حال آنکه اولا قانون تجارت الکترونیک در مقایسه با قانون جرایم رایانه‌ای که الحاق به قانون مجازات اسلامی شده، قانون خاص به شمار می‌آید و همچنان که در صدر ماده ۶۷قانون تجارت الکترونیک آمده است این ماده فقط در خصوص کلاهبرداری رایانه‌ای در بستر مبادلات الکترونیک بوده و در غیر موارد مبادلات الکترونیک ساکت است. همچنین موضوع ماده ۱ قانون تشدید مجازات جرایم اختلاس ارتشاء و کلاهبرداری خصوص کلاهبرداری به

شکل سنتی است که در آن انجام عملیات متقلبانه منجر به فریب قربانی از شرایط اصلی وقوع جرم است، اما در کلاهبرداری رایانه‌ای چنین شرطی منتفی است. علاوه بر این در کلاهبرداری رایانه‌ای، بزهکار دستورالعمل‌ها، اطلاعات و داده‌های رایانه‌ای را هدف اصلی ارتکاب جرم قرار می‌دهد. در این شیوه تحصیل مال، امتیازات و خدمات مالی، نه از طریق اغفال شخص، بلکه با ارتکاب افعال متقلبانه نسبت به داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی صورت می‌گیرد[۱].

در کلاهبرداری با رایانه فرد کلاهبردار در سلسله عملیات متقلبانه خود از سامانه‌های رایانه‌ای و مخابراتی به عنوان وسیله فریفتن قربانی استفاده می‌نماید مثلا با ارسال ایمیلی به قربانی خود را مدیر عامل یک کارخانه خودروسازی در آلمان معرفی می‌نماید که قصد دارد یک خودرو گران قیمت به شرکت قربانی هدیه نماید و در مقابل تقاضا می‌نماید که مبالغی به عنوان مالیات و هزینه‌های گمرکی و ارسال خودرو به حساب کلاهبردار واریز شود و در همین راستا اقدام به ارسال تصاویری از خودرو و سند مالکیت آن به نام آن شرکت می‌نماید که در نتیجه قربانی وجوهی به حساب کلاهبردار واریز می‌نماید. اما در کلاهبرداری رایانه‌ای فرد با ایجاد تغییراتی در این سامانه‌ها وجوه و یا منافعی برای خود تحصیل می‌نماید مانند این که با وارد نمودن کدی به تلفن همراه دیگری، هزینه‌های تماس خود را به خط قربانی منتقل می‌نماید.

۹ – یکی از رایج ترین شیوه‌های کلاهبرداری رایانه‌ای، فیشینگ[۲] است. فیشینگ در واقع تلاش برای بدست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و... از طریق جعل یک وب‌سایت، آدرس ایمیل و... است. فیشینگ در عمل به صورت کپی دقیق گرافیکی یک وبگاه معتبر مانند درگاه بانک‌ها انجام می‌شود. در این روش فیشر اغلب با تبلیغات وسوسه‌انگیز خود، طعمه را به سمت درگاه بانکی جعلی که خود طراحی کرده انتقال می‌دهد و قربانی با وارد کردن اطلاعات بانکی خود در این وبگاه جعلی عملا تمام اطلاعات بانکی خود را در اختیار فیشر قرار می‌دهد. در سایت‌های فیشینگ در نهایت فرد نمی‌تواند عملیات بانکی خود را انجام دهد یا وارد ایمیل خود شود چرا که سایت جعلی می‌باشد. لکن

---

۱ – شریعتی، محسن، کلاهبرداری رایانه‌ای از طریق سرقت اطلاعات، دو ماهنامه علمی – آموزشی تعالی حقوق، دادسرای عمومی و انقلاب تهران، سال دوم، شماره ۵، خرداد و تیر ۱۳۸۹، ص۷۳.

2 - Phishing

فیشر به داده‌های کاربر دسترسی یافته و می‌تواند با وارد کردن این داده‌ها حساب بانکی کاربر را تخلیه نماید.

* اسکیمینک روش دیگری برای کلاهبرداری رایانه‌ای است. در این روش دستگاه‌هایی به نام "اسکیمر" با قابلیت کپی کردن کارت‌های اعتباری بانکی وجود دارد که در کنار دستگاه کارت‌خوان استفاده می‌شود. نمونه‌ای از اسکیمر، دقیقا شبیه دستگاه کارت خوان بانکی است که اگر کارت اعتباری را در چنین کارت‌خوانی بکشید، یک کپی از اطلاعات کارت خریدار گرفته می‌شود و در اختیار فرد مجرم قرار می‌گیرد. فروشنده خاطی با در اختیار داشتن رمز خریدار و با استفاده از دستگاه اسکیمر که اطلاعات کارت اصلی را بر روی یک کارت خام دیگر ذخیره و می‌تواند از حساب کارت خریدار سوءاستفاده و موجودی آن را خالی کند. دستگاه اسکیمر دیگری به نام اسکیمر ATM وجود دارد که در قسمت ورودی کارت در دستگاه‌های ATM خودپردازهای بانک‌ها نصب می‌شود و هنگام وارد کردن کارت به خودپرداز، یک کپی از اطلاعات کارت اعتباری گرفته می‌شود[۱]. روش‌های کلاهبرداری رایانه‌ای محدود به موارد گفته شده نبوده و این روش‌ها مدام در حال تحول هستند.

۱۰- برداشت غیر مجاز از حساب افراد به وسیله سامانه های مخابراتی (که معمولا ذیل عنوان کیفری کلاهبرداری رایانه ای مطرح است)، جزء شایعترین جرایم ارتکابی در فضای مجازی است که هوش و ذکاوت مجرمین رایانه ای در کنار سهل انگاری قربانیان این جرایم، از علل رشد آمار ارتکاب جرایم است. اخیرا معاونت فضای مجازی دادستانی کل کشور با مشارکت بانک مرکزی سامانه ای را تحت عنوان «سامانه کاشف» راه اندازی نموده اند که در مرحله اول به قضات مربوط در سراسر کشور این مکان را می دهد که با دسترسی به این سامانه، در پرونده هایی از قبیل کلاهبرداری رایانه ای، پولشویی، ... به فوریت دستورات لازم را به بانکهای مربوط جهت مسدودی حساب ، مسدودی درگاه، رهگیری گردش حساب،اخذ پرینت و ... صادر و ابلاغ نمایند و بانکها مکلفند دستورات مربوط به مسدودی حساب را ظرف یک ساعت انجام دهند.

---

۱ – به نقل از سایت پلیس فتا

پرسش ۲۱:

۱ ـ نظر به اینکه مطابق ماده ۷۴۱ قانون مجازات اسلامی الحاقی ۱۳۸۸/۳/۵ در خصوص کلاهبرداری مرتبط با رایانه قید شده: «هر کس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن تغییر و... وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند...»، آیا منظور از کلمه وارد کردن در متن ماده به طور مطلق است؟ یعنی هرگونه وارد کردن اعم از اینکه کلاهبردار داده‌ها را با این فرض که در دسترس او باشد یا داده‌ها در دسترس او نبوده و با استفاده از فرامین یا افعالی آنها را وارد کند، می‌باشد یا صرفاً عمل وارد کردن ناظر به آن است که کلاهبردار اطلاعات و داده‌ها را در اختیار نداشته و با توسل به وسایل متقلبانه اعم از هک کردن یا روش‌های دیگر آنها را تحصیل وارد نماید؟

۲ـ در فرض سؤال چنانچه فردی یک عابر بانک را که متعلق به دیگری است سرقت نماید سپس با مراجعه به باجه خودپرداز با وارد کردن رمز که روی کارت نوشته شده است وجوه آن را سرقت نماید آیا امر فوق مشتمل بر یک عنوان که همان سرقت است، می‌باشد یا اینکه سرقت توأم با کلاهبرداری مرتبط با رایانه را نیز شامل می‌گردد؟

پاسخ:

نظریه شماره ۷/۹۳/۱۱۶۱ ـ ۱۳۹۳/۵/۱۸ نظریه مشورتی اداره کل حقوقی قوه قضاییه:

۱ـ منظور از فعل وارد کردن، در ماده ۷۴۱ الحاقی مصوب ۱۳۸۸/۳/۵ قانون مجازات اسلامی در فصل مربوط به جرایم رایانه‌ای، وارد کردن داده‌ها به هر ترتیبی است که منتهی به تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا اشخاص دیگر باشد؛ اعم از اینکه شخص مذکور قبلاً اطلاعات مربوط به داده‌ها را در اختیار داشته یا به وسائل متقلّبانه، اطلاعات مورد نظر خود را کسب نماید.

۲ـ چون ملاک تحقق جرایم مندرج در قانون جرایم رایانه‌ای، استفاده از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده است و در فرض سؤال به لحاظ اینکه سرقت انجام شده با استفاده غیرمجاز از داده‌های رایانه‌ای و وارد نمودن رمز کارت عابر بانک دیگری صورت گرفته است، موضوع مشمول ماده ۷۴۱ الحاقی به قانون مجازات اسلامی (موضوع ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵) است.

پرسش ۲۲:

اگر یک نفر به دیگری تماس تلفنی گرفته و با مطالب دروغین و متقلبانه وی را تا پای دستگاه خود پرداز برده و طی تماس تلفنی فریبنده، شاکی وجوهی به حساب فرد تماس گیرنده واریز نماید، کلاهبرداری صدق می‌نماید یا خیر؟ اختلاف نظر وجود دارد عده‌ای معتقدند تماس گیرنده فقط دروغ گفته هیچ عملیات فیزیکی انجام نداده و شاکی سادگی نموده وچون مانور متقلبانه‌ای صورت نگرفته پس جرم نیست. با توجه به اینکه مقنن در ماده یک قانون تشدید مجازات مرتکبین ارتشاء اختلاس – کلاهبرداری مانور متقلبانه را منحصر در مانور فیزیکی ننموده است، آیا این نوع عملیات تلفنی نمی‌تواند مصادیق مانور متقلبانه کلاهبرداری باشد؟

پاسخ:

شماره نظریه ۲۸۳۰/۹۳/۷ مورخ ۹۳/۱۱/۱۴ اداره حقوقی قوه قضاییه:

«صرفنظر از اینکه اصطلاح «مانور متقلبانه» در ادبیات و نظریات حقوقدانان، رایج و متداول است و در مادّه یک قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری مصوب ۱۳۶۷ مجمع تشخیص مصلحت نظام، چنین اصطلاحی به کار نرفته است و در مادّه فوق-الذکر، قانونگذار در عنصر مادی بزه کلاهبرداری، «به کار بردن وسایل متقلبانه» را مدنظر قرارداده است که مصادیقی از آن را (نظیر مغرور کردن مردم به داشتن اختیارات واهی) به تصریح نامبرده ولکن با آوردن عبارت «یا وسایل تقلبی دیگر»، مقصود خود بر تمثیلی بودن این موارد را بیان داشته است، در فرض سؤال که شخصی ناشناس از طریق تلفن با شخص دیگری تماس حاصل و با فریب وی از طریق صندوق خودپرداز بانک و با دادن دستورات فریبکارانه، مبالغی را از حساب قربانی خارج و به حساب خود وارد می‌کند، علی رغم مباشرت قربانی در عملیات بانکی، به نظر، عمل یاد شده مصداق عملیات متقلبانه بوده و می‌تواند از مصادیق کلاهبرداری مقرر در مادّه ۱ قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری محسوب باشد. با این حال، تشخیص مصداق بر عهده مرجع قضایی رسیدگی کننده است.»

فصل چهارم – جرایم علیه عفت و اخلاق عمومی

ماده ۷۴۲ قانون مجازات اسلامی –تعزیرات: «هر کس به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

تبصره۱ – ارتکاب اعمال فوق در خصوص محتویات مبتذل، موجب محکومیت به حداقل یکی از مجازات‌های فوق می‌شود. محتویات و آثار مبتذل به آثاری اطلاق می‌شود که دارای صحنه و صور قبیحه باشد.

تبصره ۲ – هر گاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک میلیون (۱،۰۰۰،۰۰۰) ریال تا پنج میلیون (۵،۰۰۰،۰۰۰) ریال جزای نقدی محکوم خواهد شد.

تبصره۳ – چنانچه مرتکب اعمال مذکور در این ماده را حرفه‌ی خود قرار داده باشد یا به طور سازمان یافته مرتکب شود چنانچه مفسد فی الارض شناخته نشود، به حد اکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره٤ – محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیر واقعی یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.»

قوانین مرتبط:

مواد ۳ تا ۱۲ «قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند» مصوب ۱۳۸۶

ماده ۳ – عوامل تولید، توزیع، تکثیر و دارندگان آثار سمعی و بصری غیرمجاز اعم از این که مجوز فعالیت از وزارت فرهنگ و ارشاد اسلامی داشته و یا بدون مجوز باشند با توجه به محتوای اثر حسب مورد علاوه بر ابطال مجوز به یکی از مجازات‌های مشروحه ذیل محکوم خواهند شد:

الف – عوامل اصلی تکثیر و توزیع عمده آثار سمعی و بصری مستهجن در مرتبه اول بـه یـک تا سه سال حبس و ضبط تجهیزات مربوطـه و یکصـد میلیـون (۱۰۰۰۰۰۰۰) ریـال جریمـه نقدی و محرومیت اجتماعی به مدت هفت سال و در صورت تکرار به دو تا پنج سال حـبس و ضبط تجهیزات مربوطه و دویست میلیـون (۲۰۰۰۰۰۰۰) ریـال جـزای نقـدی و محرومیـت اجتماعی به مدت ده سال محکوم می‌شوند. چنانچه عوامل فوق الذکر یا افراد زیـر از مصـادیق مفسدفی الارض شناخته شوند، به مجازات آن محکوم می‌گردند.

۱ – تولید کنندگان آثار مستهجن با عنف و اکراه

۲ – تولید کنندگان آثار مستهجن برای سوء استفاده جنسی از دیگران

۳ – عوامل اصلی در تولید آثار مستهجن

تبصره ۱ – عوامل اصلی تولید آثار سمعی و بصری عبارت هستند از تهیه کننده (سرمایه گذار)، کارگردان، فیلمبردار، بازیگران نقش‌های اصلی.

تبصره ۲ – تعداد نوار یا لوح فشرده و مانند آن بیش از «ده نسخه» به عنـوان «عمـده» تلقـی می‌گردد.

تبصره ۳ – سایر عوامل تولید، تکثیر و توزیع موضوع بند «الف» چنانچه از مصادیق افساد فـی الارض نباشند به مجازات شلاق از سی تا هفتاد و چهار ضـربه و جـزای نقـدی از ده میلیـون (۱۰۰۰۰۰۰۰) ریال تا پنجاه میلیون (۵۰۰۰۰۰۰۰) ریال و محرومیت اجتماعی از دو تا پنج سال محکوم می‌شوند.

تبصره ۴ – تکثیر و توزیع کنندگان آثار سمعی و بصری کمتـر از ده نسـخه حسـب مـورد بـه جریمه نقدی از یک میلیون (۱۰۰۰۰۰۰) تا ده میلیون (۱۰۰۰۰۰۰۰) ریـال و سـی تـا هفتـاد و چهار ضربه شلاق محکوم خواهند شد.

تبصره ۵ – آثار سمعی و بصری «مستهجن» به آثاری گفته می‌شود که محتوای آنهـا نمـایش برهنگی زن و مرد و یا اندام تناسلی و یا نمایش آمیزش جنسی باشد.

تبصره ۶ – چنانچه تولید، تکثیر، توزیع و یا داشتن آثار مستهجن از مصادیق افساد فـی الارض نباشد مجازات مفسدفی الارض ندارد.

ب – تهیه و توزیع و تکثیرکنندگان نوارها و دیسکت‌ها و لوح‌های فشرده شـو و نمـایش‌هـای مبتذل چنانچه از مصادیق افساد فی الارض نباشند در مرتبه اول به سه ماه تا یک سال حـبس

و یا دو میلیون (۲۰۰۰۰۰۰) ریال تا ده میلیون (۱۰۰۰۰۰۰۰) ریال جزای نقدی و در مرتبه دوم به تحمل یک سال تا سه سال حبس و یا پنج میلیون (۵۰۰۰۰۰۰) ریال تا سی میلیون (۳۰۰۰۰۰۰۰) ریال جزای نقدی و در صورت تکرار به سه تا ده سال حبس و یا ده میلیون (۱۰۰۰۰۰۰۰) ریال تا پنجاه میلیون (۵۰۰۰۰۰۰۰) ریال جزای نقدی و ضبط کلیه تجهیزات مربوطه بنا به مراتب به عنوان تعزیر محکوم می‌شوند.

تبصره ۱ – آثار سمعی و بصری «مبتذل» به آثاری اطلاق می‌گردد که دارای صحنه‌ها و صور قبیحه مخالف شریعت و اخلاق اسلامی را تبلیغ و نتیجه گیری کند.

تبصره ۲ – دارندگان نوارها و دیسکت‌ها و لوح‌های فشره مستهجن و مبتذل موضوع این قانون به جزای نقدی از پانصد هزار (۵۰۰۰۰۰) ریال تا پنج میلیون (۵۰۰۰۰۰۰) ریال و نیز ضبط تجهیزات محکوم می‌شوند و نوارها و دیسکت‌ها و لوح‌های فشرده مکشوفه امحاء می‌گردد.

تبصره ۳ – استفاده از صغار برای نگهداری، نمایش، عرضه، فروش و تکثیر نوارها و لوح‌های فشرده غیرمجاز موضوع این قانون موجب اعمال حداکثر مجازات‌های مقرر برای عامل خواهد بود.

ج – عوامل تهیه، تکثیر و توزیع نوارها و لوح‌های فشرده سمعی و بصری که برابر قانون باید دارای پروانه و مجوز عرضه و فروش باشند در صورت نداشتن پروانه نمایش و مجوز عرضه و فروش ولو آنکه فاقد صحنه‌های مستهجن و مبتذل باشد، به دو میلیون (۲۰۰۰۰۰۰) ریال تا ده میلیون (۱۰۰۰۰۰۰۰) ریال جرای نقدی و در صورت تکرار به پنج میلیون (۵۰۰۰۰۰۰) ریال تا پنجاه میلیون (۵۰۰۰۰۰۰۰) ریال جزای نقدی و ضبط کلیه تجهیزات مربوط به عنوان تعزیر محکوم می‌شوند.

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

ماده ۵ – مرتکبان جرایم زیر به دو تا پنج سال حبس و ده سال محرومیت از حقوق اجتماعی و هفتاد و چهار ضربه شلاق محکوم می‌شوند:

الف – وسیله تهدید قرار دادن آثار مستهجن به منظور سوء استفاده جنسی، اخـاذی، جلـوگیری از احقاق حق یا هر منظور نامشروع و غیرقانونی دیگر.
ب – تهیه فیلم یا عکس از محل‌هایی که اختصاصی بانوان بوده و آن‌ها فاقد پوشش مناسـب می‌باشند مانند حمام‌ها و استخرها و یا تکثیر و توزیع آن.
ج – تهیه مخفیانه فیلم یا عکس مبتذل از مراسم خانوادگی و اختصاصـی دیگـران و تکثیـر و توزیع آن.
ماده ۶ – رابطه زوجیت مانع از اعمال مجازات مرتکب جرم تکثیر، انتشار و یا توزیع عمـده اثـر مستهجن نمی‌باشد.
ماده ۷ – زیان دیده از جرایم مذکور در این قانون حق مطالبه ضـرر و زیـان را دارد. دادگـاه بـا احراز مکره بودن بزه دیده موضوع صدر ماده (۴)، ضمن صدور حکـم کیفـری، مرتکـب را بـه پرداخت ارش البکاره، مهر المثل یا هر دو (حسب مورد) محکوم می‌نماید. بزه دیـده مـی‌توانـد دعوی مطالبه هزینه درمان و ضرر و زیان وارده را در دادگاه کیفری صـالحه یـا دادگـاه محـل اقامت خود اقامه نماید.
ماده ۸ – مأموران صلاحیت دار و ضابطان دادگستری، مدیران، کارکنـان بخـش‌هـای دولتـی، عمومی، خصوصی و قضایی که بنا بر اقتضاء شغلی آثار مستهجن در اختیار آنها قرار می‌گیـرد، چنانچه با سوء نیت یا برای استفاده مالی مبادرت به انتشار آنها نمـوده و از مصـادیق مفسـدفی الارض نباشند، به دو تا پنج سال حبس و ده سال محرومیت از حقوق اجتماعی و هفتاد و چهار ضربه شلاق محکوم می‌شوند.
در صورتی که موارد یاد شده در اثر سهل انگاری افشاء گردد، مسامحه کننـده بـه مجـازات تـا یـک سـال حـبس و مجـازات نقـدی از ده میلیـون (۱۰۰۰۰۰۰۰) ریـال تـا بیسـت میلیـون (۲۰۰۰۰۰۰۰) ریال محکوم می‌شود.
ماده ۹ – اماکن کسب، تولید و توزیع انواع آثار مستهجن (در صورت اطـلاع قبلـی مالـک) بـه مدت شش ماه و در مورد آثار مبتذل به مدت سه ماه پلمپ می‌شود. در صورت برائت متهم یـا صدور قرار منع تعقیب، از ملک رفع توقیف می‌شود. این دسـتور ظـرف ده روز از تـاریخ ابـلاغ قابل اعتراض در مرجع قضایی ذی صلاح می‌باشد.
ماده ۱۰ – انتشـار آثـار مسـتهجن و مبتـذل از طریـق ارتباطـات الکترونیکـی و سـایت‌هـای

کامپیوتری یا وسیله و تکنیک مشابه دیگر از مصادیق تکثیر و انتشار محسوب و مرتکب حسب مورد به مجازات مقرر در این قانون محکوم می‌شود.

ماده ۱۱ – رسیدگی به جرایم مشروحه موضوع این قانون در صلاحیت دادگاه‌های انقلاب است.

ماده ۱۲ – کلیه وسایل و تجهیزات مربوطه که بر اساس این قانون از محکومان ضبط می‌گردد به وزارت فرهنگ و ارشاد اسلامی تحویل می‌شود و در خصوص وسایل و تجهیزات تحویل شده از سوی مراجع ذی صلاح در شهرستان‌ها نیز به همین نحو عمل می‌شود.

ماده ۶۴۰ قانون مجازات اسلامی – تعزیرات: «ماده ۶۴۰ – اشخاص ذیل به حبس از سه ماه تا یک سال و جزای نقدی از یک میلیون و پانصد هزار ریال تا شش میلیون ریال و تا (۷۴) ضربه شلاق یا به یک یا دو مجازات مذکور محکوم خواهند شد:

۱ – هر کس نوشته یا طرح، گراور، نقاشی، تصاویر، مطبوعات، اعلانات، علایم، فیلم، نوار سینما و یا بطور کلی هر چیز که عفت و اخلاق‌عمومی را جریحه‌دار نماید برای تجارت یا توزیع به نمایش و معرض انظار عمومی گذار یا بسازد یا برای تجارت و توزیع نگاه دارد.

۲ – هر کس اشیاء مذکور را به منظور اهداف فوق شخصا یا به وسیله دیگری وارد یا صادر کند و یا به نحوی از انحاء متصدی یا واسطه تجارت و یاهر قسم معامله دیگر شود یا از کرایه دادن آن‌ها تحصیل مال نماید.

۳ – هر کس اشیاء فوق را به نحوی از انحاء منتشر نماید یا آنها را به معرض انظار عمومی بگذارد.

۴ – هر کس برای تشویق به معامله اشیای مذکور در فوق و یا ترویج آن اشیاء به نحوی از انحاء اعلان و یا فاعل یکی از اعمال ممنوعه فوق و یامحل بدست آوردن آن را معرفی نماید.

تبصره ۱ – مفاد این ماده شامل اشیائی نخواهد بود که با رعایت موازین شرعی و برای مقاصد علمی یا هر مصلحت حلال عقلائی دیگر تهیه یا خرید و فروش و مورد استفاده متعارف علمی قرار می‌گیرد.

تبصره ۲ – اشیای مذکور ضبط و محو آثار می گردد و جهت استفاده لازم به دستگاه دولتی ذیربط تحویل خواهد شد.

ماده ۶۴۱ – هر گاه کسی به وسیله تلفن یا دستگاههای مخابراتی دیگر برای اشخاص ایجاد

مزاحمت نماید علاوه بر اجرای مقررات خاص شرکت مخابرات، مرتکب بـه حـبس از یـک تـا شش ماه محکوم خواهد شد.

شرح ماده :

۱ – معنای لغوی پورنوگرافی[۱] عبـارت اسـت از فاحشـه نگـاری، تحریـرر و توصـیف فعالیـت روسپی‌ها و به تعبیر فرهنگستان زبـان و ادب فارسـی، هـرزه نگـاری. اصـطلاح پورنـوگرافی، اصطلاحی حقوقی نیست... بلکه متعلق به عالم هنر است که در طبقه بندی آثار هنـری، بـرای تفکیک میان برخی تصاویر مکشوف و بی پـرده جنسـی از سـایر تصـاویر بـه کـار مـی‌رود... مهمترین سند بین المللی در زمینه هرزه نگاری، پروتکل اختیاری پیمان نامـه حقـوق کـودک درباره خرید و فروش، فحشاء و هرزه نگاری کودکان است که از تاریخ هجـدهم ژانویـه ۲۰۰۲ لازم الاجرا شده است. این پروتکل، به عنوان مکمل مهمترین سند بین المللی راجع به حقـوق کودکان یعنی پیمان نامه حقوق کودک به تصویب رسـیده اسـت؛ در بنـد ج مـاده ۲ پروتکـل مذکور، هرزه نگاری کودکان این گونه تعریف شده است: «هرزه نگاری کودکان به معنـی هـر گونه نمایشی می‌باشد که در آن کودکان به صورت واقعی و یا مجازی مشغول فعالیت‌های بارز جنسی باشند و یا آلت تناسلی کودکان برای مقاصد جنسی به نمایش گذاشته شـود.» [۲] شـایان ذکر است که پروتکل اخیر الذکر در تاریخ ۸۶/۵/۹ به تصویب مجلس شورای اسـلامی رسـیده است و لذا تعریف این پروتکل از پورنو گرافی ارزش قانونی دارد. گر چه تعبیرات به کار رفته در متن قانون اندکی با ترجمه فوق از هرزه نگاری کودکان متفاوت است. [۳]

این نوع اعمال مجرمانه که ماهیتا در جرایم کلاسیک نیـز وجـود دارد، بـا توسـعه و پیشـرفت تکنولوژی کامپیوتر و اینترنت وارد این رسـانه‌ی جمعـی شـده اسـت و از لحـاظ گسـتردگی و وسعت، در زمینه پخش و توزیع، در نوع خود بی نظیر می‌باشد. به عنوان مثـال صـندوق‌هـای

---

1 - Pornography

۲ – حبیب زاده، محمد جعفر و رحمانیان، حامد، هرزه نگاری در حقوق کیفری ایران، مجله حقوقی دادگستری، شـماره ۷۶، زمستان ۱۳۹۰، ص ۹۱.

۳ – بند پ ماده ۳ قانون الحاق دولت جمهوری اسلامی ایران به پروتکل اختیاری کنوانسیون حقوق کـودک در خصـوص فروش، فحشاء و هرزه نگاری کودکان: «پ – هرزه‌نگاری کودک به هرگونه نمایش کودک درگیر در فعالیتهای واقعـی یـا مشابه‌سازی شده آشکار جنسی، با هر وسیله یا هرگونه نمایش اندام جنسی کـودک بـرای اهـداف عمـدتاً جنسـی اطـلاق می‌شود.»

پستی، آدرس‌های الکترونیکی و سایت‌هایی در اینترنت وجود دارد که به تبلیغ، پخش و عرضه تصاویر پورنو می‌پردازند.[1] البته با دقت در مواد ۷۴۲ و ۷۴۳ قانون تعزیرات مشخص می‌شود که دایره‌ی شمول اعمال مشمول عنوان پورنوگرافی در این مواد، گسترده تر از معنای بین المللی آن است.

۲ – در تقسیم بندی متعارف جرائم رایانه‌ای، جرائم مندرج در مواد ۷۴۲ تا ۷۴۶ این قانون در دسته‌ی جرائم علیه محتوا قرار می‌گیرند که در این قانون شامل: هرزه‌نگاری و جرایم مرتبط با آن، تحریف هویت، افشا یا انتشار اسرار خصوصی و نشر اکاذیب می‌شوند. مواد ۷۴۲ و ۷۴۳ این قانون در فصل چهارم با عنوان جرائم علیه عفت و اخلاق عمومی قرار گرفته‌اند. برخی از حقوق دانان این جرایم را در زمره جرایم علیه اشخاص دانسته‌اند که موضوع اصلی مورد حمایت این جرایم و قربانی مستقیم آن‌ها افراد هستند. به نظر می‌رسد با توجه به این که این جرایم محدود به زنا، لواط، مساحقه،... نبوده و اعمالی مانند انتشار محتویات مبتذل و مستهجن، تشویق افراد به فساد و فحشاء نیز در زمره‌ی این جرایم قرار می‌گیرند و در بسیاری از موارد قربانیان جرم، اشخاصی نیستند که تصاویر مستهجن آنان منتشر می‌شود، بلکه قربانیان واقعی کلیه افرادی هستند که با مشاهده این محتویات آلوده، دچار تشویش خاطر، اشتغال فکری و سپس جسمی به هواهای نفسانی و در نتیجه باز ماندن از ارزشهای والای انسانی می‌شوند و فضای عمومی جامعه از فضای کار و تلاش و سازندگی، تبدیل به فضای شهوت رانی و جولان اندیشه‌ها و مدهای غربی می‌شود. بنابراین نمی‌توان جرائم علیه عفت و اخلاق عمومی را صرفا در زمره‌ی جرایم علیه اشخاص دانست بلکه باید به صورت مستقل در رابطه با آن بحث نمود.

۳ – جدا از فواید غیر قابل انکار و بی بدیل فضای مجازی، این فضا بستر پر زرق و برق، سحرآمیز و افسار گسیخته‌ای است که اکنون بلای سلامت روحی، جسمی و اخلاقی برخی افراد شده است. به همین دلیل اکثر دولتها و نهادهای بین‌المللی از این خطرات بیمناک شده و در صدد کنترل تصاویر و محتویات هرزه موجود در فضای سایبر برآمده‌اند. به ویژه در این میان بیشترین توجه نسبت به اطفال صورت گرفته است؛ زیرا اطفال در برابر تصاویر محرک و

---

۱ – باستانی، برومند، پیشین، ص۵۰.

مستهجن بسیار آسیب‌پذیر هستند و دو خطر عمده آنها را تهدید می‌کند: نخست: احتمال بلـوغ زودرس، انحراف جنسی و بزهکار شدن اطفال وجود داشته چرا که تصاویر و محتویات هرزه به نوعی تعلیم ارتکاب عمل جنسی است که عمدتاً به صورت غیرطبیعی و خطرنـاک اسـت. دوم: احتمال بزه‌دیده شدن اطفال تحت تأثیر فضای مجازی بسیار زیاد اسـت و مهـم‌تـرین توجیـه جرم‌انگاری در زمینه هرزه‌نگاری است .

برای حمایت از کودکان در برابر هرزه‌نگاری و استثمار جنسـی، عـلاوه بـر اینکـه کشـورها در مقررات کیفری خویش از آن غفلت نورزیده‌اند، معاهدات و کنوانسیونهای بین‌المللـی متعـددی نیز در همین زمینه به تصویب رسیده‌اند. ماده ۳۴ کنوانسـیون حقـوق کـودک مصـوب ۱۹۸۹، پیشگیری از فعالیت جنسی غیرقانونی علیه کودکان و استثمار کودکان در راسـتای فحشـاء یـا تهیه تصاویر هرزه را پیش‌بینی کرده است. همچنین پروتکل اختیاری کنوانسیون حقوق کودک در همین زمینه است که پیش تر در بند اول شرح همین ماده به آن پرداخته‌ایم.

۴ – تبصره۴ ماده ۷۴۲ قانون مجازات اسـلامی – تعزیـرات، محتویـات مسـتهجن را تعریـف نموده و مقرر داشته: «محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیر واقعی یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یـا عمـل جنسـی انسان است.» بنابراین محتویات مستهجن ممکن است یک فیلم کوتاه و یـا بلنـد واقعـی و یـا نمایشی باشد که روابط جنسی انسان را نمایش می‌دهد و یا عکسی باشد که این صحنه را بـه تصویر کشیده و حتی داستانی واقعی و یا تخیلی باشد که روابط جنسی زن و مردی را تشـریح می‌نماید. البته این محتویات فقط گویای روابط جنسـی زن و مـرد نیسـت و مـی‌توانـد شـامل نمایش برهنگی کامل زن (ها) و یا مرد (ها) و یا حداقل نمایش اندام تناسلی آنها باشد. "منظور از اندام جنسی شامل اندام‌هایی در زن می‌شود که مرد فاقد آن است که صـرفاً دو چیـز اسـت: آلت تناسلی و پستانها و در مردها نیز شامل یک اندام برجسته است وآن آلـت تناسـلی مردانـه است. اندام جنسی در مفهومی کلی، علاوه بر این شامل مقعد و مجموعه باسن نیز مـی‌شـود و بنابراین نمایش اندام جنسی زن و مرد مجموعاً منحصر به مـوارد زیـر اسـت و بیشـتر از آن را شامل نمی‌شود: آلت تناسلی زنانه ـ پستانهای جنس مونث ـ آلت تناسلی مردانه ـ مقعد و باسن

زن و مرد. "[۱]

البته نمایش آمیزش جنسی حیوانات، شامل این ماده نمی‌گردد و فقط در مورد انسان‌ها مصداق دارد. مشابه تعریف حاضر در تبصره ۵ بند الف ماده ۳ قانون نحوه‌ی مجازات اشخاصی که در امورسمعی وبصری فعالیت‌های غیر مجاز می‌نمایند، نیز آمده است: «آثار سمعی و بصری مستهجن به آثاری گفته می‌شود که محتوای آنها نمایش برهنگی زن و مرد و یا اندام تناسلی و یا نمایش آمیزش جنسی باشد.» البته به نظر می‌رسد که تعریف اخیر با تصویب قانون عام موخر جرایم رایانه‌ای (ماده ۷۴۲ قانون مجازات اسلامی) نسخ شده است.

۵ – «محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند»: ملاحظه می‌شود که در این ماده تولید، ذخیره و نگهداری محتویات مستهجن به قصد تجارت یا افساد و همچنین انتشار، توزیع و یا معامله این محتویات به هر قصدی به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، جرم تلقی شده است. برای تبیین و تفکیک این اصطلاحات، به شرح زیر این موارد تشریح می‌گرد:

الف – تولید محتویات مستهجن: یعنی ساختن فیلم و یا تصویر و یا متن گویای محتویات مستهجن. این محتویات ممکن است به صورت واقعی و یا به صورت غیر واقعی و به عبارتی ساختگی باشند.

ب – ذخیره[۲] محتویات مستهجن: یعنی این که محتویات مستهجن واقعی را در ابزارهای رایانه‌ای ذخیره نماید. مانند این که از استخر زنانه‌ای فیلم برداری نموده و در حامل‌های داده ذخیره نماید.

ج – نگهداری محتویات مستهجن: یعنی این که محتویات مستهجن واقعی و یا غیر واقعی را در حامل‌های داده نگهداری نماید مانند این که یک داستان جنسی را در حافظه رایانه خود نگهداری نماید

د – «به قصد تجارت یا افساد»: صرف تولید، ذخیره و یا نگهداری محتویات مستهجن جرم نمی‌باشد بلکه اگر این محتویات را به قصد تجارت و یا افساد تولید، ذخیره و یا نگهداری نماید در این صورت مرتکب جرم موضوع این ماده شده است. قصد تجارت با این محتویات، یعنی

---

۱ – همان، ص۶۰

2 - Save

این که هدف مجرم از تولید، ذخیره و یا نگهداری آن‌ها، به فروش رساندن محتویات مذکور و کسب منفعت مالی باشد. اما افساد در مقابل اصلاح قرار می‌گیرد و به معنای فاسد کردن و آلوده نمودن می‌باشد که در اینجا منظور آلوده نمودن فضای مجازی و به تبع آن کاربران این فضا به محتویات مستهجن می‌باشد. بنابراین اگر اثبات شود که فرد صرفا برای تفریح ویا هر قصد دیگری غیر از تجارت و افساد، این محتویات را در تلفن همراه و یا سامانه‌ی خود نگهداری می‌نموده، مشمول این ماده نمی‌باشد. به نظر نگارنده در مواردی که فرد این محتویات را می‌سازد، نباید در داشتن قصد تجارت و یا افساد وی تردید نمود بلکه قطعا به یکی از این دو هدف این محتویات را می‌سازد. در هر حال باید توجه داشت که حتی اگر این قصد تجارت یا افساد نیز احراز نشود، با شرایطی برابر تبصره‌ی ۲ بند ب ماده ۳ قانون نحوه‌ی مجازات اشخاصی که درامورسمعی وبصری فعالیت‌های غیر مجاز می‌نمایند قابل تعقیب است.

* ابهامی که در خصوص نگهداری آثار مبتذل و مستهجن وجود دارد این است که به موجب تبصره ۲ ماده ۳ قانون نحوه مجازات افرادی که در امور سمعی و بصری فعالیت غیر مجاز می‌نمایند، صرفِ نگهداری آثار مبتذل و مستهجن جرم تلقی شده است لکن در مواد ۶۴۰ و ۷۴۲ قانون مجازات اسلامی – تعزیرات، نگهداری این آثار به قصد تجارت و توزیع و افساد جرم تلقی شده است حال آیا در خصوص صرف نگهداری آثار مبتذل و مستهجن (بدون قصد تجارت و افساد) باید قائل به جرم بودن موضوع باشیم یا خیر؟ مثلا اگر کسی یک فلش مموری حاوی فیلم‌های مستهجن در اختیار داشت و یا در حافظه گوشی تلفن همراه خود عکس‌های مبتذل داشت آیا به موجب تبصره ۲ ماده ۳ قانون نحوه مجازات افراردی که در امور سمعی و بصری فعالیت غیر مجاز می‌نمایند، قابل مجازات است؟

گر چه برخی پاسخ مثبت به این پرسش می‌دهند و استدلال می‌نمایند که رأی وحدت رویه شماره ۶۴۵ هیأت عمومی دیوان عالی کشور با تصویب قانون جدید نحوه مجازات افراردی که در امور سمعی و بصری فعالیت غیر مجاز می‌نمایند، نسخ شده است و در تبصره ۲ ماده ۳ این قانون صرف نگهداری آثار مبتذل و مستهجن جرم انگاری شده است، لکن «قانون نحوه مجازات افرادی در امور سمعی و بصری فعالیت غیر مجاز می‌نمایند » ، منصرف به افرادی است که امور سمعی و بصری را حرفه خود قرار داده‌اند، اما در خصوص سایر اشخاص باید به همان ماده عام ۶۴۰ قانون مجازات اسلامی و نیز ماده‌ی ۷۴۲ اخیر التصویب این قانون، استناد

جسته و نگهداری را تنها در صورت وجود سوء نیت خاص واجد وصف جزایی دانست. این دیدگاه با اصل تفسیر مضیق نصوص جزایی نیز سازگارتر است. [۱]» با پذیرش این دیدگاه ، رأی وحدت رویه شماره ۶۴۵ هیأت عمومی دیوان عالی کشور مورخ ۷۸/۹/۲۳ نیز به قوت خود باقی می‌ماند[۲].

ه – انتشار و توزیع محتویات مستهجن: در مقام تفکیک »انتشار« از «توزیع» می‌توان گفت، هرگاه محتویات مستهجن ازطریق سامانه‌های رایانه‌ای یا مخابراتی به صورت غیرمشخص وگسترده بدون اینکه فرد یا افراد خاصی مد نظر باشند، پخش می‌گردد، واژه‌ی انتشار به ذهن متبادر می‌شود اما آنچه که از واژه‌ی «توزیع» برمی آید، این است که هرگاه محتویات مستهجن ازطریق سامانه‌های رایانه‌ای یا مخابراتی، در میان اشخاصی که مشخصاً مد نظر توزیع کننده هستند، پخش می‌شود، عمل توزیع انجام شده است.

و – معامله محتویات مستهجن: عرفا مراد از معامله ، خرید و فروش است اما به نظر می‌رسد اگر فرد در ازاء دریافت یک فیلم دیگر از طرف مقابل، فیلم خود را برای وی بفرستد، باز هم معامله (از نوع پایاپای) تحقق یافته است. نکته مهم این که اتهام معامله محتویات مستهجن هم در مورد خریدار و هم فروشنده این محتویات صادق است. نکته دیگر این که برخلاف تولید، ذخیره و یا نگهداری محتویات مستهجن، انتشار و توزیع و معامله این محتویات به هر قصدی که صورت گرفته باشد تفاوتی نداشته و جرم محقق است.

۶ – محتویات و آثار مبتذل نیز در تبصره ۱ این ماده تعریف شده است به این شرح که: «محتویات و آثار مبتذل به آثاری اطلاق می‌شود که دارای صحنه و صور قبیحه باشد.» اگر چه این تعریف کلی است می‌توان برای آن حد و مرزی قرار داد؛ به این صورت که محتویات مستهجن از این تعریف خارج است و محتویاتی که عرف جامعه آنها را زشت نمی‌داند و برخلاف عفت و اخلاق عمومی نیست نیز ازاین تعریف خارج است. پس محتویاتی که از نظر

---

۱ – حبیب زاده، محمد جعفر و رحمانیان حامد، همان، ص ۱۱۱.

۲ – رأی وحدت رویه شماره ۶۴۵ هیئت عمومی دیوان عالی کشور: «نظر به این که برطبق ماده ۶۴۰ قانون مجازات اسلامی (تعزیرات مصوب ۱۳۷۵) که به موجب ماده ۷۲۹ همان قانون کلیه مقررات مغایربا آن ملغی شده، نگهداری، طرح، نقاشی، نوارسینما و ویدئو یا به طور کلی هر چیزی که عفت و اخلاق عمومی را جریحه دار نماید در صورتی که به منظور تجارت وتوزیع باشد جرم محسوب می‌شود بنابراین صرف نگهداری وسائل مزبور در صورتی که تعداد آن معد برای امر تجاری و توزیع نباشد، از شمول ماده۶۴۰ قانون مذکور خارج بوده و فاقد جنبه جزائی است...»

عرف اخلاقی جامعه زشت و زننده باشد مشمول این تعریف قرار می‌گیرد مانند بوسیدن جنس مخالف (تقبیل)، رقص زنان، نمایش عریان قسمتی از بدن زن (غیر از اندام تناسلی). تبصره۱بند ب ماده ۳ قانون نحوه‌ی مجازات اشخاصی که درامورسمعی وبصری فعالیت‌های غیر مجاز می‌نمایند نیز تعریف مشابهی از این آثار ارائه داده است: «آثار سمعی و بصری «مبتذل» به آثاری اطلاق می‌گردد که دارای صحنه‌ها و صورقبیحه بوده و مضمون مخالف شریعت و اخلاق اسلامی را تبلیغ و نتیجه‌گیری کند.» البته به نظر می‌رسد که تعریف اخیر با تصویب قانون عام موخر جرایم رایانه‌ای (ماده ۷۴۲ قانون مجازات اسلامی) نسخ شده است.

۷ – تبصره یک این ماده، ارتکاب اعمال فوق در خصوص محتویات مبتذل را موجب محکومیت به حداقل یکی از مجازات‌های فوق می‌داند. البته این بند ابهام دارد که آیا مقصود این بوده که مجرم به حداقل یک مجازات از دو مجازات مقرر محکوم می‌شود و یا اینکه مقصود این بوده که مجرم به حداقلِ یکی از این دو مجازات محکوم می‌شود، به نظر می‌رسد که تفسیر دوم منطقی تر باشد یعنی مجرم به حداقلِ جزای نقدی (پنج میلیون ریال) و یا حداقلِ میزان حبس (نود و یک روز) محکوم می‌شود.

۸ – با توجه به مفاد تبصره‌ی ۲ که مقرر می‌دارد: «هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود مرتکب به یک میلیون ریال تا پنج میلیون ریال جزای نقدی محکوم خواهد شد»، می‌توان مجازات‌های مقرر در این ماده برای ارسال داده‌های مستهجن را به دو دسته تقسیم نمود:

الف – هرگاه محتویات مستهجن به بیشتر از ده نفر ارسال شود مرتکب به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال و یا هر دو مجازات محکوم خواهد شد (صدر ماده).

ب – هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود مرتکب به یک میلیون ریال تا پنج میلیون ریال جزای نقدی محکوم خواهد شد (تبصره ۲ ماده).

پرسش ۲۳:

آیا محتویات ارسال شده همگی بایستی مشابه هم باشند مثلا یک فیلم خاص را برای همه ارسال نماید و یا اینکه اگر یک عکس برای یکی، متنی برای دیگری و فیلمی برای شخص دیگری بفرستد باز هم مشمول این تبصره می‌گردد؟

پاسخ:

با توجه به اطلاق تبصره ۲، تفاوتی از این جهت وجود ندارد و لزومی به مشابهت محتویات ارسالی نیست.

۹ – تبصره ۳ این ماده مقرر داشته: «چنانچه مرتکب اعمال مذکور در این ماده را حرفه‌ی خود قرار داده باشد یا به صورت سازمان یافته مرتکب شود چنانچه مفسد فی الارض شناخته نشود، به حداکثر هر دو مجازات محکوم خواهد شد.»

مقنن در این تبصره دو عامل تشدید مجازات را بیان نموده که عبارتستای که اولا: مرتکب اعمال مذکور در این ماده را حرفه‌ی خود قرار داده باشد یعنی این که شغل مرتکب معامله، توزیع و یا انتشار محتویات مستهجن و مستهجن باشد و ثانیا: به صورت سازمان یافته مرتکب این جرم شود یعنی این که متهمین در قالب یک تشکل و یا سازمان و به صورت هدفمند اقدام به معامله، توزیع و یا انتشار این محتویات مبتذل یا مستهجن نمایند.

قانون گذار از یک طرف در ماده ۷۴۲، تجارت و معامله این محتویات را مطرح نموده و از طرف دیگر در تبصره‌ی۳ این ماده عبارت «این عمل را حرفه‌ی خود قرار داده باشد» را آورده است. در توجیه این مطلب باید گفت، اگر مرتکب یک بار این محتویات را تجارت و یا معامله کند، عمل مذکور مصداق جرم موضوع صدر ماده ۷۴۲ است. اما اگر شخص این عمل را حرفه‌ی خود قرار داده است به نحوی که شغل او محسوب می‌شود مشمول تبصره‌ی ۳ این ماده می‌شود.

۱۰ – عنصر مادی جرایم مذکور در این ماده عبارتست از انتشار، توزیع و معامله محتویات مبتذل و مستهجن و همچنین تولید، ذخیره و نگهداری این محتویات به قصد تجارت و یا افساد به وسیله‌ی سامانه‌های رایانه‌ای و یا مخابراتی، با شرایط و اوضاع و احوالی که پیشتر گفته شد. جرم انتشار، توزیع و معامله محتویات مبتذل و مستهجن مقید به نتیجه بوده و نتیجه آن انتشار، توزیع و یا معامله این محتویات است؛ اما جرم تولید، ذخیره و نگهداری این محتویات مطلق بوده و منوط به تحقق نتیجه‌ای نیست. عنصر معنوی جرم انتشار، توزیع و معامله محتویات مبتذل و مستهجن عبارتست از سوءنیت عام مرتکب (علم و عمد وی) در ارتکاب اعمال خلاف قانون؛ و سوءنیت خاص مرتکب عبارتست از اراده وی برای تحقق نتیجه جرم که همانا انتشار، توزیع و معامله محتویات مبتذل و مستهجن است. عنصر معنوی جرم

تولید، ذخیره و نگهداری این محتویات عبارتست از سوءنیت عام مرتکب (علم و عمد وی) در ارتکاب اعمال خلاف قانون؛ و به لحاظ مطلق بودن جرم نیازی به سوءنیت خاص نیست.

۱۱ – ممکن است که تصور شود با تصویب مواد ۷۴۲ و ۷۴۳ این قانون، قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیتهای غیرمجاز می‌نمایند، نسخ شده است؛ اما باید توجه داشت که فصل جرایم رایانه‌ای صرفا در مورد محتویات مبتذل و مستهجنی که از طریق سامانه‌های رایانه‌ای تولید و ارسال می‌شوند جرم انگاری کرده حال آنکه قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیتهای غیرمجاز می‌نمایند، به صورت عام تر در خصوص این محتویات که از هر طریقی و به هر صورتی تولید و منتشر می‌شوند جرم انگاری کرده و در مورد آثار سمعی و بصری غیرمجاز نیز جرم انگاری کرده است. بنابراین قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیتهای غیرمجاز می‌نمایند، به صورت کلی نسخ نشده و فقط در حدودی که مواد ۷۴۲ و ۷۴۳ قانون تعزیرات جرم انگاری نموده (از جمله ماده ۱۰ قانون نحوه مجازات اشخاصی که...)، نسخ ضمنی شده است. در خصوص ماده ۶۴۰ قانون مجازات اسلامی نیز همین بحث قابل طرح است.

ماده ۷۴۳ قانون مجازات اسلامی –تعزیرات: «هرکس از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به منظور دستیابی افراد به محتویات مستهجن آنهارا تحریک، ترغیب، تهدید یا تطمیع کند یا فریب دهد یا شیوه‌ی دستیابی به آنهارا تسهیل نموده یا آموزش دهد، به حبس از ۹۱روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هردو مجازات محکوم خواهد شد.

ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو میلیون (۲،۰۰۰،۰۰۰) ریال تا پنج میلیون (۵،۰۰۰،۰۰۰) ریال است.

ب) چنانچه افراد را به ارتکاب جرایم منافی عفت یا استعمال مواد مخدر یا روان گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز تحریک یا ترغیب یا تهدید یا دعوت کرده یا فریب دهد یا شیوه‌ی ارتکاب یا استعمال آنهارا تسهیل کند یا آموزش دهد، به حبس از ۹۱روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون

(۲۰،۰۰۰،۰۰۰) ریال یا هردو مجازات محکوم می‌شود.
تبصره: مفاد این ماده و ماده‌ی ۱۴ شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هرمصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می‌شود.»

قوانین مرتبط

ماده ۶۳۹ قانون مجازات اسلامی (تعزیرات): «افراد زیر به حبس از یک تا ده سال محکوم می‌شوند و در مورد بند «الف« علاوه بر مجازات مقرر، محل مربوطه به طور موقت با نظر دادگاه بسته خواهد شد: الف – کسی که مرکز فساد و یا فحشا دایر یا اداره کند.
ب – کسی که مردم را به فساد یا فحشا تشویق نموده یا موجبات آن را فراهم نماید.
تبصره: هر گاه بر عمل فوق عنوان قوادی صدق نماید علاوه بر مجازات مذکور به حد قوادی نیز محکوم می‌گردد.»

شرح ماده :

۱- این ماده به جرم انگاری معاونت در ارتکاب جرایم علیه عفت و اخلاق عمومی و آسیب‌های اجتماعی پرداخته است و معاونت را به عنوان جرم مستقل جرم انگاری نموده است. در این قسم از معاونت، بدون توجه به این که مباشر جرم کیست و آیا مجرم است یا خیر، مستقلا معاون مجازات می‌گردد. این ماده شامل دو قسمت است: الف –معاونت در دستیابی افراد به محتویات مستهجن ومبتذل؛ ب – معاونت در ارتکاب جرایم منافی عفت و یا استعمال مواد مخدر یا روان گردان یا خودکشی و یا انحرافات جنسی و یا اعمال خشونت آمیز.

نکته :

در این ماده معاونت در خودکشی جرم انگاری شده است (بند ب ماده ۷۴۳) در حالی که خودکشی در قوانین ما جرم نیست. این از ابداعات مفید قانون است که با توجه به ترویج ناامیدی و تشویق به خودکشی در برخی شبکه‌های اجتماعی و بازی‌های رایانه‌ای، این تدبیر مناسبی برای برخورد با مجرمان است.
۲ – «به منظور دستیابی افراد به محتویات مستهجن»: از این عبارت برداشت می‌شود که این

جرم مطلق بوده و نیازی به تحقق مقصود مجرم (دستیابی افراد به محتویات مستهجن) نیست. دستیابی، به معنی دست یافتن و در دسترس قرار گرفتن است به نحوی که مثلا فیلمی مستهجن از سایتی فیلتر شده دانلود شود و یا تصویر عریان زن بدکاره‌ای در حافظه‌ی تلفن همراه فرد قرار گیرد.

۳ – شیوه‌های معاونت در این عمل، در بند الف احصاء شده که عبارتند از تحریک، ترغیب، تهدید، تطمیع، فریب دادن، تسهیل شیوه دستیابی و آموزش این شیوه‌ها؛ به شرح آتی به توضیح این اصطلاحات می‌پردازیم:

الف – تحریک: تحریک در لغت به معنی به حرکت در آوردن، جنباندن و نیز در معنی واداشتن و برانگیختن دیگران آمده است. تحریک به جرم یعنی واداشتن دیگری به ارتکاب جرم به هر دستاویزی، خواه با دادن مال، وعده.... مانند این که با توصیف محتویات یک سایت غیر اخلاقی دیگران را به بازدید از آن تحریک نماید.

ب – ترغیب: ترغیب از کلمه رغبت است یعنی ایجاد میل و علاقه در دیگری به انجام دادن کاری. مثلا با بیان تجربیات واقعی یا تخیلی خود از دسترسی به محتویات مستهجن و بیان برخی فواید غیرواقعی برای آن، در دیگران این رغبت را ایجاد نماید که این موضوع را تجربه کنند.

ج – تهدید: تهدید در لغت به معنای ترساندن و بیم دادن است در قوانین کیفری نیز همان معنی عرفی و لغوی مراد است و مقصود از واداشتن دیگری است به ارتکاب جرم چنانکه ترس از عاقبت فعل یا ترک فعل مذکور فاعل را مطیع ساخته باشد. مثلا تهدید فردی به بازدید روزانه از یک سایت غیر اخلاقی در ازای عدم افشای راز وی.

د – تطمیع: تطمیع در لغت به معنی طمع انداختن و آزمند ساختن است. بنابراین اگر کسی دیگری را با دادن وعده یا امتیاز مالی و یا قول به تحصیل مقام و منزلت اجتماعی در ارتکاب جرم راسخ کند معاون جرم محسوب می‌شود.[۱] مثلا دادن وعده پرداخت وجه در قبال دستیابی افراد به تصاویر مستهجن و ارسال آنها به فرد یا شبکه خاصی.

ه – فریب دادن: مثلا فردی را فریب دهد که اگر داستان‌های غیر اخلاقی را نخواند نمی‌تواند

۱ – اردبیلی، محمد علی، حقوق جزای عمومی، جلد دوم، نشر میزان، چاپ چهارم، تهران، ۱۳۸۱، ص۴۲الی ۴۵.

در روابط زناشویی موفق باشد.

و – تسهیل شیوه دستیابی به محتویات مستهجن: مثلا با انتشار نسخه‌های متعدد نرم افزارهای فیلتر شکن، راه را برای دستیابی افراد به محتویات فیلتر شده، باز نماید.

ز – آموزش نحوه دستیابی به محتویات مستهجن: مثلا سایت‌های غیر اخلاقی و آدرس‌های آن‌ها را اعلام نماید.

مقنن در ادامه این بند معاونت در دسترسی افراد به محتویات مبتذل را نیز موجب جزای نقدی از دو میلیون تا پنج میلیون ریال دانسته است.

۴ – بند ب این ماده معاونت، از طرق مذکور در بند قبل را، در مورد جرایم منافی عفت (مثلا ارتکاب زنا و لواط)، معاونت در استعمال مواد مخدر و مواد روانگردان (مصرف تریاک، حشیش، کراک، اکستازی، ...) معاونت در خودکشی (مثلا با القای ناامیدی به زندگی و تشویق افراد به خودکشی برای رهایی از دشواری‌ها)، معاونت در انحرافات جنسی (مثلا تشویق افراد به استبراء) و معاونت در اعمال خشونت آمیز (مثلا ارائه راهکار برای تخریب اموال عمومی، ترور، اسید پاشی، ...) را جرم انگاری نموده است. جرم مذکور در این بند نیز مطلق بوده و تحقق جرایم منافی عفت و یا خودکشی از این طریق، شرط تحقق معاونت نیست. مثلا همین که متهم با ایجاد یک کانال در پیام رسانی اقدام به انتشار داده هایی با مضمون تحریک مردم به تخریب اموال عمومی و یا دعوت به شرکت در مراسم فحشاء نمود ، جرم محقق شده است.

۵ – تبصره این ماده تهیه، تولید، نگهداری، ارائه، توزیع و انتشار مفاد مذکور در مواد ۷۴۲ و ۷۴۳ را برای مقاصد علمی و یا هر مصلحت عقلای دیگری، مجاز دانسته است. از جمله مصادیق این ماده می‌توان به تهیه و پخش فیلم‌های آموزشی روابط صحیح زناشویی اشاره نمود که توسط وزارت بهداشت یا سایر مراکز مجاز تهیه می‌شود.

۶ – عنصر مادی جرم معاونت در بند الف عبارتست از تحریک، ترغیب، تهدید، تطمیع، فریب دادن، تسهیل شیوه دستیابی به محتویات مستهجن و مبتذل و آموزش این شیوه‌ها با شرایط و اوضاع و احوالی که پیشتر اشاره شد. همچنین این جرم مقید به نتیجه نیست. عنصر معنوی این جرم نیز عبارتست از سوءنیت عام مرتکب در علم و عمد وی به انجام اعمال فوق به منظور ارتکاب اعمال غیر قانونی مذکور.

عنصر مادی جرم معاونت در بند ب نیز عبارتست از تحریک، ترغیب، تهدید، دعوت کردن، فریب دادن، تسهیل شیوه ارتکاب جرایم منافی عفت یا استعمال مواد مخدر یا روان گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز و آموزش این شیوه‌ها با شرایط و اوضاع و احوالی که پیشتر اشاره شد. همچنین این جرم مقید به نتیجه نیست. عنصر معنوی این جرم عبارتست از سوءنیت عام مرتکب در علم و عمد وی به انجام اعمال فوق به منظور معاونت در ارتکاب اعمال غیر قانونی (ارتکاب جرایم منافی عفت یا استعمال مواد مخدر یا روان گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز).

پرسش ۲٤:

ماده۱۱ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیتهای غیرمجاز می‌نمایند، رسیدگی به جرائم مشروحه موضوع این قانون را در صلاحیت دادگاههای انقلاب قرار داده است؛ حال سؤال اینجاست که آیا رسیدگی به جرایم مذکور در مواد ۷۴۲ و ۷۴۳ قانون تعزیرات نیز در صلاحیت دادگاههای انقلاب است؟

پاسخ:

این قانون در خصوص موضوع صلاحیت ساکت است و از طرفی این جرایم در فهرست جرایم مندرج در ماده ۳۰۳ قانون آیین دادرسی کیفری نیز نمی‌گنجد[۱]. مطابق اصل، رسیدگی به کلیه جرایم در صلاحیت دادسراهای عمومی وانقلاب و دادگاههای کیفری است مگر خلاف آن تصریح شده باشد؛ بنابراین رسیدگی به جرایم مواد ۷۴۲ و ۷۴۳ قانون تعزیرات در صلاحیت دادسراهای عمومی و انقلاب و دادگاههای کیفری ۲ است.

---

۱ – ماده ۳۰۳ – به جرایم زیر در دادگاه انقلاب رسیدگی می‌شود:

الف – جرایم علیه امنیت داخلی و خارجی، محاربه و افساد فی‌الارض، بغی، تبانی و اجتماع علیه جمهوری اسلامی ایران یا اقدام مسلحانه یا احراق، تخریب و اتلاف اموال به منظور مقابله با نظام

ب – توهین به مقام بنیانگذار جمهوری اسلامی ایران و مقام رهبری

پ – تمام جرایم مربوط به مواد مخدر، روان‌گردان و پیش‌سازهای آن و قاچاق اسلحه، مهمات و اقلام و مواد تحت کنترل

ت – سایر مواردی که به موجب قوانین خاص در صلاحیت این دادگاه است.

فصل پنجم: هتک حیثیت و نشر اکاذیب

ماده ۷٤٤ قانون مجازات اسلامی –تعزیرات: «هر کس به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر و تحریف، منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او بشود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هردو مجازات، محکوم خواهد شد.

تبصره: چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حد اکثر هر دو مجازات مقرر محکوم خواهد شد.»

شرح ماده :

۱ – عنوان کیفری این ماده هتک حیثیت افراد به وسیله سامانه‌های رایانه‌ای یا مخابراتی است به این صورت که فردی فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر و تحریف، منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او بشود. بنابراین شامل مواردی که فردی رأسا با تقلید صدای دیگری مطالبی جدید را بیان می‌کند و یا فردی شبیه دیگری حرکاتی را انجام می‌دهد نمی‌شود مگر این که صوت و یا تصویر و یا فایلی از فرد مورد نظر موجود باشد و این موارد مشابه به آن اضافه شود.

۲ – این جرم فقط با فعل مثبت مادی تحقق می‌یابد با ترک فعل امکان تحقق آن وجود ندارد. همچنین مقید به نتیجه بوده و بدون اینکه عرفا موجب حیثیت طرف مقابل شود، این جرم محقق نمی‌شود. بنابراین تحقق هتک حیثیت نتیجه‌ی این جرم است. تعقیب آن جز با شکایت شاکی میسر نیست اما گذشت شاکی پیش بینی نشده است.

۳ – این جرم به دو صورت تحقق می‌یابد:

الف – فردی فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و سپس آن را منتشر کند.

ب – فردی با علم به تغییر و تحریف فیلم یا صوت یا تصویر دیگری، آن را منتشر کند.

بنابراین اگر فردی فقط فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند، بدون اینکه آن را منتشر نماید، این جرم محقق نشده است. همچنین در صورتی که فیلم یا صوت یا تصویر دیگری را بدون تغییر ویا تحریف منتشر کند، مشمول این ماده نمی‌شود هر چند که موجب هتک حیثیت دیگری شود؛ و یا اگر بدون آگاهی از این که فیلم و یا صوت و یا تصویر تغییر یافته و یا تحریف شده آن را منتشر نماید باز هم مشمول این عنوان کیفری قرار نمی‌گیرد. البته بار اثبات عدم آگاهی بر دوش فرد منتشر کننده است.

۴ – تغییر با تحریف دو مفهوم متفاوت دارد؛ در مورد مفهوم لغوی تغییر گفته شده: از حالی به حالی برگرداندن، دگرگون کردن، چیزی را به شکل و حالت دیگر در آوردن. اما در مورد مفهوم لغوی تحریف گفته شده: کج کردن، گردانیدن، تغییر و تبدیل و گردانیدن کلام کسی از وضع و حالت اصلی خود، بعضی حروف کلمه را عوض کردن و تغییر دادن معنی آن.[۱] بنابراین تغییر شکلی است اما تحریف محتوایی است. به این صورت که در تغییر کلیت محتوا و مفهوم کلی فیلم، صوت و یا تصویر باقی می‌ماند و فقط چند جمله، حرکت و یا نقش به آن اضافه شده و یا از آن کاسته می‌شود و یا جابجا می‌شوند مانند این که کلمه زشتی را به بیانات یک نماینده مجلس اضافه می‌کند؛ اما در تحریف این تغییرات به حدی است که محتوای فیلم، صوت و یا تصویر نیز عوض می‌شود مانند این که راه رفتن فرد سرشناسی را با استفاده از برنامه‌های رایانه‌ای به رقصیدن تبدیل می‌نمایند و یا سخنرانی یک سیاست مدار علیه رژیم غاصب صهیونیسم را به نحوی تغییر می‌دهند که گویا در حمایت از آن رژیم جعلی سخن می‌گوید و یا بطری آب مقابل فردی را در تصویر، تبدیل به بطری مشروبات الکلی می‌نماید.

۵ – دیگری در این ماده می‌تواند هر شخص حقیقی محترمی باشد اعم از اشخاص عادی و مقامات دولتی. البته اصل بر این است که حیثیت همه‌ی افراد جامعه معتبر است مگر در موارد استثایی که فرد خود معمولا اعمال و رفتاری انجام می‌دهد که حیثیت خود را زیر سؤال می‌برد و مردم از این جهت حیثیتی برای وی قائل نیستند . با توجه به اینکه مقنن از عباراتی چون « فیلم یا صوت یا تصویر دیگری» و « هتک حیثیت او » استفاده نموده به نظر می رسد که این ماده در خصوص هتک حیثیت اشخاص حقوقی قابل استناد نیست.

---

۱ – عمید، حسن، پیشین، جلد اول، صص۵۹۳ و ۵۴۵.

۶ – مطابق تبصره این ماده چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حد اکثر هر دو مجازات مقرر محکوم خواهد شد یعنی به دو سال حبس و چهل میلیون ریال جزای نقدی محکوم می‌شود. مانند این که دیگری را در حال زنا و یا لواط به نمایش بگذارد و یا آلت جنسی او را به تصویر کشد.

۷ – اشکال وارد بر این ماده این است که به متنی که در سامانه‌های رایانه‌ای یا مخابراتی مورد تغییر یا تحریف واقع می‌شود، اشاره‌ای ننموده است. به عنوان مثال متهم در متنِ مصاحبه یک سیاست مدار یا استاد دانشگاه، تغییر یا تحریفی ایجاد می کند و نقل مطالب سخیف و یا اشتباه فاحشی را به وی منتسب می کند و منتشر می‌کند.

۸ – ارتکاب جرم موضوع این ماده ممکن است با مشارکت چند نفر تحقق یابد به این صورت که با هماهنگی قبلی یکی از متهمان که گرافیست ماهری است اقدام به تغییر یا تحریف تصویری نموده و دیگری که دارای یک کانال تلگرامی پر مخاطب است آن را منتشر نماید که در این صورت هر دو نفر شریک جرم محسوب و مجازات هر کدام مجازات فاعل اصلی است.

۹ – عنصر مادی این جرم به دو صورت قابل تحقق است الف – تغییر یا تحریف فیلم و یا صوت و یا تصویر دیگری به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی و سپس انتشار دادن آن؛ ب – منتشر کردن فیلم و یا صوت و یا تصویر دیگری به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی با علم به تغییر و تحریف، با شرایط و اوضاع و احوالی که گفته شد. نتیجه این جرم نیز هتک حیثیت دیگری است. عنصر معنوی این جرم نیز عبارتست از سوء نیت عام فرد در ارتکاب عالمانه و عامدانه این جرم، و سوء نیت خاص وی در اراده‌ی تحقق نتیجه‌ی جرم یعنی هتک حیثیت دیگری.

ماده ۷۴۵ قانون مجازات اسلامی –تعزیرات: «هرکس به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هردو مجازات محکوم خواهد شد[۱].»

۱ – مجازات جرم موضوع این ماده عیناً مجازات مقرر در ماده‌ی ۱۶ است.

شرح ماده :

۱ – فلسفه وضع این ماده حفظ کیان خانواده و حفظ حریم خصوصی زندگی اشخاص است. از آنجا که با انتشار تصاویر و فیلم‌های خصوصی و خانوادگی افراد، اساس زندگی آنان به خطر افتاده و حیثیت آنان خدشه دار می‌گردد، مقنن برای کسانی که به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، مجازات نسبتا سنگینی را وضع نموده است.

۲ – به نظر می‌رسد تفاوت انتشار دادن و در دسترس دیگران قرار دادن، این است که انتشار در سطح وسیع تری است و مثلا وقتی فیلمی در فضای مجازی منتشر می‌شود در دسترس همه کاربران قرار می‌گیرد اما در دسترس قرار گرفتن، به این صورت است که مثلا متهم فیلم را فقط در صفحه شخصی خود قرار می دهد و یا در وبلاگ شخصی اش قرار می دهد که مخاطبان خاصی دارد . منظور از کلمه دیگران در این ماده شامل هر فردی می‌شود که از دید صاحب فیلم و یا تصویر و یا صوت غریبه به شمار می‌آید و راضی نیست که به آن دسترسی یابد. اما اگر فردی تصویر خصوصی غیر مستهجن همسر خود را برای مادر و خواهران خود بفرستد، به نظر نمی رسد که این جرم محقق می‌شود اما در همین مورد اگر زن و شوهری که از هم جدا شده‌اند، اقدام به در دسترس قرار دادن تصاویر خصوصی همسر سابق خود برای دیگران از طریق سامانه های رایانه‌ای نماید، این جرم محقق می‌شود.

۳ – صوت و یا فیلم و یا تصویر خصوصی یا خانوادگی: هر صوت و یا فیلم و یا تصویر خانوادگی، خصوصی نیز هست اما هر صوت و یا فیلم و یا تصویرخصوصی الزاما خانوادگی نیست. مثلا فایل صوتی صحبت‌های یک نفر با همسرش، یک صوت خانوادگی محسوب می‌شود اما فیلم جشن تولد یک دانشجوی دختر در یک خوابگاه دخترانه، یک فیلم خصوصی است و نه خانوادگی. نکته مهم این که تصاویر باید خصوصی و خانوادگی باشد و هر تصویری در این تعریف نمی‌گنجد مثلا تصویر یک مرد با کت و شلوار و یا چهره پوشیده‌ی یک زن شامل مقررات این ماده نمی‌شود.

۴ – اسرار افراد شامل اطلاعاتی است در مورد خود فرد و یا خانواده و یا شغل وی که از نظر او

نباید دیگران از این اسرار آگاه شوند، مثلا فرد قبلا نامزدی داشته و یا مبتلا به بیماری پوستی است که نمی‌خواهد کسی از آن مطلع شود. البته برخی از اقشار خاص مانند پزشکان موظف به اعلام مبتلایان به بیماری‌های مسری به وزارت بهداشت هستند که اعلام در این حد مشمول این ماده نمی‌شود. [۱] ماده ۶۴۸ قانون مجازات اسلامی نیز در همین خصوص مقرر می‌دارد: «اطبا و جراحان و ماماها و داروفروشان و کلیه‌ی کسانی که به مناسبت شغل یا حرفه‌ی خود محرم اسرار می‌شوند هر گاه در غیر از موارد قانونی، اسرار مردم را افشا کنند به سه ماه و یک روز تا یک سال حبس و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می‌شوند.».

۵ – این جرم مقید به نتیجه بوده و نتیجه‌ی آن این است که منجر به ضرر شخص و یا عرفاً موجب هتک حیثیت او شود. مقصود از ضرر هر نوع زیان و خسارت مادی و معنوی است و منظور از هتک حیثیت، از بین رفتن و یا خدشه دار شدن آبرو و اعتبار فرد نزد مردم است. بنابراین اگر با وجود منتشر کردن و یا در دسترس دیگران قرار گرفتن صوت و یا فیلم و یا تصویر خانوادگی و یا خصوصی، ضرری به فرد وارد نشود و یا آبروی وی لکه دار نشود این جرم محقق نمی‌شود. مثلا فیلمی خانوادگی از فردی منتشر شود که در حال قدم زدن در پارک و یا مسافرت هستند.

۶ – بدون رضایت فرد یعنی این که متهم قبلا از فرد صاحب فیلم و یا عکس اذن نگرفته باشد و یا بعد از انتشار از او اجازه نگرفته و یا فرد شکایتی نداشته باشد. مقصود از رضایت، رضایت در انتشار و در دسترس اغیار قرار گرفتن این محتویات است. رضایت گرفتن همیشه به صورت دریافت اجازه کتبی و یا شفاهی نیست و گاهی عملی است مثلا کسی که تصویر خانوادگی خود را در یک شبکه اجتماعی یا پیام رسان قرار می‌دهد، عملا به کاربران اجازه می‌دهد که آن را منتشر نماید. همچنین گاهی این محتویات به دستور مرجع قضایی در اختیار قاضی دادسرا و ضابطین دادگستری برای کشف جرم قرار می‌گیرد که در این صورت رضایت مالک آن لازم نیست.

---

۱ – در این خصوص قانون طرز جلوگیری از بیماری‌های آمیزشی و بیماری‌های واگیر دار (مصوب ۱۳۲۰) و قانون راجع به ثبت و گزارش اجباری بیماری‌های سرطانی (مصوب ۱۳۶۳) قابل توجه است.

۷ – از ظاهر این ماده چنین بر می‌آید که تفاوتی وجود ندارد که متهم این محتویات را بـه چـه صورت بدست آورده، اعم از این که دستیابی فرد با رضایت صـاحب آن باشـد (مـثلا فـیلم بـه صورت امانت نزد متهم بوده) و یا نباشد (مانند این که متهم فیلم را از حافظه موبایل دیگری با استفاده از نرم افزارهای جدید سرقت نموده باشد) و یا اینکه ابتدای آن با رضایت بوده اما مجوز انتشار نداشته است (مانند فیلم برداری که فیلم عروسی فردی را منتشر می‌کند). مگر ایـن کـه نفس طریقه‌ی دسترسی فرد خود جرم مستقلی باشد، مثلا مشـمول مـاده ۱ ایـن قـانون قـرار گیرد.

۸ – عنصر مادی این جرم منتشر کردن و یا در دسترس دیگران قرار گرفتن صوت و یا فیلم و یا تصویر خانوادگی و یا خصوصی دیگری به وسیله‌ی سامانه‌های رایانه‌ای یا مخـابراتی اسـت. شرایط و اوضاع و احوال تحقق این جرم این است که اولا: وسیله ارتکـاب جـرم سـامانه‌هـای رایانه‌ای یا مخابراتی باشد؛ ثانیا: موضوع جرم صـوت و یـا فـیلم و یـا تصـویر خـانوادگی و یـا خصوصی و یا اسرار باشد، ثالثا: صوت و یا فیلم و یا تصویر و اسرار متعلق به غیـر باشـد، رابعـا: صاحب آن راضی به انتشار آن نباشد، خامسا: این موارد منتشر شود و یا در دسترس غیـر قـرار گیرد. نتیجه‌ی این جرم نیز ورود ضرر به شخص و یا هتک حیثیت او است. عنصر معنوی ایـن جرم عبارتست از سوء نیت عام فرد در ارتکاب عالمانه و عامدانه جرم، و سوءنیت خاص وی در اراده تحقق هتک حیثیت.

پرسش ۲۵:

آیا عکس گرفتن(اسکرین شات) از متن مکالمه خصوصی(چت) توسط یکی از طرفین مکالمـه و انتشار آن جرم است یا خیر؟

پاسخ:

اولا: صرف عکس گرفتن (اسکرین شات) و نگهداری آن جرم انگاری نشده مگر اینکه تهدید به انتشار آن نماید که در این صورت می تواند از مصادیق تهدید باشد.ثانیا: بـدیهی اسـت کـه انتشار هر مکالمه ای جرم نیست و صرفا مکالمه ای که حاوی اسرار شخصی طرف دیگر باشد جرم است و برابر ماده ۷۴۵ قانون مجازات اسلامی قابل پیگرد است.

پرسش ۲۶:

اگر شاکی بعد از طرح شکایت و در خلال تحقیقات و یا دادرسی ، رضایت خود در مورد انتشار اسرار شخصی اش اعلام نماید تکلیف دادسرا یا دادگاه چیست؟

پاسخ:

با دقت در متن ماده ۷۴۵ قانون مجازات اسلامی، ملاحظه می گردد که مقنن انتشار و یا در دسترس قرار دادن محتویات خصوصی و خانوادگی و اسرار شخصی را در صورتی جرم دانسته که بدون رضایت شاکی باشد، این رضایت ممکن است قبل و یا بعد از انتشار اخذ شود و حتی اگر بعد از اعلام شکایت نیز شاکی رضایت خود را به انتشار اعلام نماید، موضوع قابل تعقیب نیست و بایستی قرار منع پیگرد یا رأی برائت صادر شود. همین بحث عینا در مورد جرایم مندرج در مواد ۷۲۹، ۷۳۰ ، ۷۳۴ تا ۷۳۸ ،۷۴۰ تا ۷۴۱، ۷۴۴ تا ۷۴۶ همین قانون نیز صادق است.

ماده ۷٤٦ قانون مجازات اسلامی –تعزیرات: «هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله‌ی سامانه‌های رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت رأساً یا به عنوان نقل قول به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یاد شده به نحوی از انحا ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده‌ی حیثیت (در صورت امکان)، به حبس از۹۱ روز تا ۲سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴،۰۰۰،۰۰۰) ریال یا هردو مجازات محکوم خواهد شد.»

قوانین مرتبط

ماده‌ی ۶۹۸ قانون مجازات اسلامی – تعزیرات: «هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله‌ی نامه یا شکواییه یا مراسلات یا عرایض یا گزارش یا توزیع هرگونه اوراق چاپی یا خطی با امضا یا بدون امضا اکاذیبی را اظهار نماید یا با همان مقاصد اعمالی را برخلاف حقیقت راساً یا به عنوان نقل قول به شخص حقیقی یا حقوقی یا

فصل ششم ـ مسئولیت کیفری اشخاص[حقوقی]

ماده ۷۴۷ قانون مجازات اسلامی –تعزیرات: «در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهدبود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته‌باشد.

تبصره۱ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره۲ـ مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهدبود و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسؤول خواهدبود.»

قوانین مرتبط:

ماده ۵۸۳ قانون تجارت: «کلیه شرکت‌های تجارتی مذکور در این قانون شخصیت حقوقی دارند.»

ماده ۵۸۴ قانون تجارت: «تشکیلات و مؤسساتی که برای مقاصد غیر تجارتی تأسیس شده یا بشوند از تاریخ ثبت در دفتر ثبت مخصوصی که وزارت عدلیه معین خواهد کرد شخصیت حقوقی پیدا می‌کنند.»

ماده ۵۸۸ قانون تجارت: «شخص حقوقی می‌تواند دارای کلیه حقوق و تکالیفی شود که قانون برای افراد قائل است، مگر حقوقی و وظایفی که بالطبیعه فقط انسان ممکن است دارای آن

باشد، مانند حقوق و وظایف ابوت – بنوت و امثال ذلک.»
ماده ۵۸۹ قانون تجارت: «تصمیمات شخص حقوقی به وسیله مقاماتی که به موجب قانون یا اساسنامه صلاحیت اتخاذ تصمیم دارند، گرفته می‌شود.»
ماده ۱۴۳ قانون مجازات اسلامی مصوب ۹۲: «در مسؤولیت کیفری اصل بر مسؤولیت شخص حقیقی است و شخص حقوقی در صورتی دارای مسؤولیت کیفری است که نماینده قانونی شخص حقوقی به نام یا در راستای منافع آن مرتکب جرمی شود. مسؤولیت کیفری اشخاص حقوقی مانع مسؤولیت اشخاص حقیقی مرتکب جرم نیست.»

شرح ماده :

۱ – شخص حقوقی عبارتست از مجموعه‌ای از افراد که دارای منافع و فعالیت مشترک هستند و یا پاره‌ای از اموال که به هدف خاصی اختصاص داده شده است و قانون آن‌ها را طرف حق می‌شناسد وبرای آن‌ها شخصیت حقوقی مستقل قائل است؛ مانند دولت، شهرداری‌ها، دانشگاه‌ها، شرکت‌های تجارتی، انجمن‌ها و موقوفات[۱]. به عبارت دیگر شخصیت حقوقی عبارت از مجموعه‌ی سازمان یافته‌ی اموال و یا اشخاص حقیقی است که برای تحقق هدفی مشترک و مطابق ضوابط قانونی و تشریفات خاصی شکل یافته و صلاحیت دارا شدن حقوق و تکالیف را به طور مستقل دارد. بدیهی است که اطلاق شخص حقوقی به هر مجموعه و نهادی زمانی صادق است که به صورت قانونی تشکیل شده باشد والا گروه‌ها و مجموعه‌هایی که مطابق تشریفات قانونی به ثبت نرسیده‌اند، صلاحیت دارا شدن حقوق و تکالیف را ندارند و شخصیت حقوقی به شمار نمی‌آیند.

پرسش ۲۸:

آیا با تصویب ماده ۱۴۳ قانون مجازات اسلامی مصوب ۹۲، ماده ۷۴۷ قانون مجازات اسلامی مصوب ۸۸ نسخ ضمنی شده یا خیر؟

پاسخ:

در این خصوص دو نظر وجود دارد برخی معتقدند با توجه به این که قانون جرایم رایانه‌ای قانون خاص خاص است هم چنان به قوت خود باقی و لازم الاجراست؛ زیرا قانون عام مؤخر

۱ – طاهری، حبیب الله، حقوق مدنی ۱و۲، جلد اول، دفتر انتشارات اسلامی، چاپ دوم، قم، ۱۳۷۶، ص۱۱۲.

نمی‌تواند ناسخ خاص مقدم باشد[۱].

اما به نظر می‌رسد که اساس این استدلال (تلقی قانون جرایم رایانه‌ای به عنوان قانون خاص) صحیح نمی‌باشد چرا که برابر ماده ۵۵ قانون اخیر الذکر، مواد این قانون عینا به قانون مجازات اسلامی – تعزیرات (فصل جرایم رایانه‌ای) الحاق گردیده و قانون مستقلی تحت عنوان قانون جرایم رایانه‌ای باقی نمانده است که بخواهیم آن را عام یا خاص بدانیم! لذا مواد مربوط به فصل جرایم رایانه‌ای، بخشی از قانون مجازات اسلامی – تعزیرات هستند که قانون اخیر در مقایسه با قانون مجازات اسلامی مصوب ۹۲، قانون عام مقدم می‌باشد لذا به نظر می‌رسد که با تصویب قانون مجازات اسلامی مصوب ۹۲ به عنوان قانون عام مؤخر، مواد مرتبط از قانون عام مقدم (از جمله ماده ۷۴۷ قانون مجازات اسلامی – تعزیرات نسخ شده است.

۲- برابر ماده ۱۴۳ قانون مجازات اسلامی مصوب ۹۲ جرم در صورتی از سوی شخصیت حقوقی قابل تحقق می‌باشد که نماینده قانونی شخص حقوقی به نام شخص حقوقی یا در راستای منافع آن ارتکاب یابد. تفاوتی که ماده اخیر با ماده ۷۴۷ قانون مجازات اسلامی – تعزیرات نموده این است که در ماده اخیر الذکر قید شده «جرایم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد». به بیان دیگر در ماده ۷۴۷ ق. م. ا. تعزیرات، دو شرط مکمل برای انتساب جرم به شخص حقوقی مقرر شده بود: اول اینکه به نام شخص حقوقی باشد، دوم اینکه جرم در راستای منافع شخص حقوقی باشد لذا اگر هر یک از این شرایط محقق نباشد، جرم قابل انتساب به شخص حقوقی نیست. لکن در ماده ۱۴۳ ق. م. ا. مصوب ۹۲ همین که جرم به نام شخص حقوقی ارتکاب یابد یا اینکه جرم در راستای منافع شخص حقوقی باشد، در هر دو صورت جرم به شخص حقوقی منسب می‌گردد. نکته مهم اینکه در هر حال (چه شخص حقوقی مسؤولیت داشته باشد و چه نداشته باشد) شخص حقیقی در قبال جرم ارتکابی مسؤول خواهدبود.

برای این که تشخیص دهیم که جرمی در راستای منافع شخص حقوقی ارتکاب یافته یا خیر؟ باید بررسی کنیم که منافع آن شخص چیست و چگونه تأمین می‌شود. مثلا منافع یک شرکت تجاری، منافع مالی است و یا منافع یک حزب سیاسی، تضعیف رقبای سیاسی و مطرح نمودن

---

۱ – مصدق، محمد، شرح قانون مجازات اسلامی، انتشارات جنگل، چاپ ششم، تهران، ۱۳۹۳، ص۱۰۱

خود است.

۳- علاوه بر شرط مقرر در بند قبل (جرم به نام شخص حقوقی یا در راستای منافع او باشد)، جرم در صورتی قابل انتساب به شخص حقوقی است که توسط «نماینده قانونی» شخص حقوقی ارتکاب یابد. منظور از نماینده قانونی شخص حقوقی، شخصی است که به جهتی قانونی (مانند مصوبه هیأت مدیره، دستور کتبی یا شفاهی مقام مسؤول، حکم کارگزینی،...) صلاحیت تصدی تمام یا بخشی از امور مربوط به شخص حقوقی را بر عهده دارد مثل رئیس هیأت مدیره، مدیر عامل، کارشناس امور رایانه،...

بدیهی است اگر شخصی که نمایندگی قانونی در تصدی امور شخص حقوقی ندارد مرتکب جرم رایانه‌ای به نام شخص حقوقی یا در راستای منافع او گردد، فقط شخص حقیقی (مرتکب جرم) مسؤول می‌باشد.

ماده ۷۴۸ قانون مجازات اسلامی –تعزیرات: «اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد.

تبصره ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگر را نخواهد داشت.»

قوانین مرتبط:

ماده ۲۰ قانون مجازات اسلامی مصوب ۹۲: «درصورتی که شخص حقوقی براساس ماده (۱۴۳) این قانون مسؤول شناخته شود، با توجه به شدت جرم ارتکابی و نتایج زیانبار آن به یک تا دو مورد از موارد زیر محکوم می‌شود، این امر مانع از مجازات شخص حقیقی نیست:

مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یابد.
ت ـ جرائم رایانه ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعـم از اینکـه بـزه دیده یا مرتکب ایرانی یا غیرایرانی باشد و مرتکب در ایران یافت شود.»

قوانین مرتبط:

ماده ۳ قانون مجازات اسلامی: «قوانین جزائـی ایـران دربـاره کلیـه اشخاصـی کـه در قلمـرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران مرتکب جرم شوند اعمـال مـی‌شـود مگر آنکه به موجب قانون ترتیب دیگری مقررشده باشد.»

ماده ۴ قانون مجازات اسلامی: «هر گاه قسمتی از جرم یا نتیجه آن در قلمرو حاکمیـت ایـران واقع شود در حکم جرم واقع شده در جمهوری اسلامی ایران است.»

ماده ۵ قانون مجازات اسلامی «هر شخص ایرانی یا غیرایرانی که در خارج از قلمرو حاکمیـت ایران مرتکب یکی از جرائم زیر یا جرائم مقرر در قوانین خاص گردد، طبـق قـوانین جمهـوری اسلامی ایران محاکمه و مجازات می‌شود و هرگاه رسیدگی به این جرائم در خارج از ایـران بـه صدور حکم محکومیت و اجرای آن منتهی شود، دادگاه ایران در تعیـین مجازاتهـای تعزیـری، میزان محکومیت اجراء شده را محاسبه می‌کند: الـف – اقـدام علیـه نظـام، امنیـت داخلـی یـا خارجی، تمامیت ارضی یا استقلال جمهوری اسلامی ایران

ب – جعل مهر، امضاء، حکم، فرمان یا دستخط مقام رهبری یا استفاده از آن

پ – جعل مهر، امضاء، حکم، فرمان یا دستخط رسمی رئـیس جمهـور، رئـیس قـوه قضـائیه، رئیس و نمایندگان مجلس شورای اسلامی، رئیس مجلس خبرگان، رئـیس دیوانعـالی کشـور، دادستان کل کشور، اعضای شورای نگهبان، رئیس واعضای مجمع تشخیص مصـلحت نظـام، وزرا یا معاونان رئیس جمهور یا استفاده از آنها

ت – جعل آراء مراجع قضائی یا اجرائیه‌های صادره از این مراجع یا سـایر مراجـع قـانونی و یـا استفاده از آنها

ث – جعل اسکناس رایج یا اسناد تعهدآور بانکی ایران و همچنین جعـل اسـناد خزانـه و اوراق مشارکت صادرشده یا تضمین شده از طرف دولـت یـا تهیـه یـا تـرویج سـکه قلـب در مـورد

مسکوکات رایج داخل.»

ماده ۶ قانون مجازات اسلامی: «به جرائم مستخدمان دولت اعم از ایرانی یا غیرایرانی که در رابطه با شغل و وظیفه خود در خارج از قلمرو حاکمیت ایران مرتکب شده‌اند و به جرائم مأموران سیاسی و کنسولی و دیگر وابستگان دولت ایران که از مصونیت سیاسی برخوردارند طبق قوانین جمهوری اسلامی ایران رسیدگی می‌شود.»

ماده ۷ قانون مجازات اسلامی: «علاوه بر موارد مذکور در مواد فوق هریک از اتباع ایران در خارج از کشور مرتکب جرمی شود، در صورتی که در ایران یافت و یا به ایران اعاده گردد، طبق قوانین جمهوری اسلامی ایران محاکمه و مجازات می‌شود مشروط بر اینکه:

الف – رفتار ارتکابی به موجب قانون جمهوری اسلامی ایران جرم باشد.

ب – در صورتی که جرم ارتکابی از جرائم موجب تعزیر باشد، متهم در محل وقوع جرم محاکمه و تبرئه نشده یا در صورت محکومیت، مجازات کلاً یا بعضاً درباره او اجراء نشده باشد.

پ – طبق قوانین ایران موجبی برای منع یا موقوفی تعقیب یا موقوفی اجرای مجازات یا سقوط آن نباشد.»

ماده ۸ قانون مجازات اسلامی: «هرگاه شخص غیرایرانی در خارج از ایران علیه شخصی ایرانی یا علیه کشور ایران مرتکب جرمی به جز جرائم مذکور در مواد قبل شود و در ایران یافت و یا به ایران اعاده گردد، طبق قوانین جزائی جمهوری اسلامی ایران به جرم او رسیدگی می‌شود، مشروط بر اینکه:

الف – متهم در جرائم موجب تعزیر در محل وقوع جرم، محاکمه و تبرئه نشده یا در صورت محکومیت، مجازات کلاً یا بعضاً درباره او اجراء نشده باشد.

ب – رفتار ارتکابی در جرائم موجب تعزیر به موجب قانون جمهوری اسلامی ایران و قانون محل وقوع، جرم باشد.»

ماده ۹ قانون مجازات اسلامی: «مرتکب جرائمی که به موجب قانون خاص یا عهدنامه‌ها و مقررات بین المللی در هر کشوری یافت شود در همان کشور محاکمه می‌شود، اگر در ایران یافت شود طبق قوانین جزائی جمهوری اسلامی ایران محاکمه و مجازات می‌گردد.»

ماده ۳۱۶ قانون آیین دادرسی کیفری: «به اتهامات اشخاصی که در خارج از قلمرو حاکمیت جمهوری اسلامی ایران مرتکب جرم می‌شوند و مطابق قانون، دادگاه‌های ایران صلاحیت

رسیدگی به آنها را دارند، چنانچه از اتباع ایران باشند، حسب مورد در دادگاه محل دستگیری و چنانچه از اتباع بیگانه باشند حسب مورد، در دادگاه تهران رسیدگی می‌شود.»

* رأی وحدت رویه شماره ۷۲۹ ـ ۱۳۹۱/۱۲/۱ هیأت عمومی دیوان عالی کشور:

«نظر به اینکه در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل در قانون جرایم رایانه‌ای نیز ـ مستفاد از ماده ۲۹ ـ مورد تأکید قانون‌گذار قرار گرفته، بنابراین در جرم کلاهبرداری مرتبط با رایانه هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضائی مختلف صورت گرفته باشد، دادگاهی که بانک افتتاح‌کننده حساب زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشت شده در حوزه آن قرار دارد صالح به رسیدگی است. بنا به مراتب آراء شعب یازدهم و سی و دوم دیوان عالی کشور که براساس این نظر صادرشده به اکثریت آراء صحیح و قانونی تشخیص و تأیید می‌گردد. این رأی طبق ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در موارد مشابه برای شعب دیوان عالی کشور و دادگاه‌ها لازم‌الاتباع است.»

* رأی وحدت رویه شماره ۷۲۱ ـ ۱۳۹۰/۴/۲۱ هیأت عمومی دیوان عالی کشور:

«وقوع بزه مزاحمت برای اشخاص به وسیله تلفن یا دستگاه‌های مخابراتی دیگر ـ موضوع ماده ۶۴۱ قانون مجازات اسلامی ـ منوط به آن است که نتیجه آن که مقصود مرتکب است محقق گردد، بنابراین در مواردی که اجرای مزاحمت از یک حوزه قضایی شروع و نتیجه آن در حوزه قضایی دیگر حاصل شود، محل حدوث نتیجه مزبور، محل وقوع جرم محسوب و مناط صلاحیت دادگاه رسیدگی کننده نیز همین امر خواهد بود. بر این اساس رأی شماره ۱۰۴۵ـ۱۳۸۵/۷/۲۰ شعبه بیست و هفتم دیوان عالی کشور که با این نظر مطابقت دارد به اکثریت آراء صحیح و منطبق با موازین قانون تشخیص می‌گردد. این رأی طبق ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در موارد مشابه برای شعب دیوان عالی کشور و دادگاه‌های سراسر کشور لازم الاتباع است.»

شرح ماده :

۱- منظور از «دیگر قوانین» در این ماده، مواد ۳ تا ۹ قانون مجازات اسلامی مصوب ۹۲ (راجع به قلمرو اجرای قوانین جزایی در مکان) و ماده ۳۱۶ قانون آیین دادرسی کیفری (راجع

به تعیین دادگاه صالح برای رسیدگی به جرایمی که در خارج از کشور توسط اتباع ایران یا اتباع بیگانه ارتکاب می‌یابد) است.

۲- این ماده در مقام تبیین صلاحیت‌های محاکم ایران در رسیدگی به جرایم رایانه‌ای است: بندهای الف و ب ماده ۶۶۴ در واقع گویای صلاحیت سرزمینی محاکم ایران بوده و منطبق با مواد ۳ و ۴ قانون مجازات اسلامی است. بند پ ماده ۶۶۴ در مقام تبیین صلاحیت واقعی محاکم ایران بوده و می‌تواند منطبق با ماده ۵ قانون مجازات اسلامی باشد.

همچنین بند ت ماده ۶۶۴ در مقام تبیین صلاحیت جهانی محاکم ایران بوده و منطبق با ماده ۹ قانون مجازات اسلامی است. اعمال این صلاحیت منوط به حضور متهم در قلمرو ایران است. بند اخیر در راستای ایفای تعهد ایران در الحاق به «پروتکل اختیاری کنوانسیون حقوق کودک درخصوص فروش، فحشاء و هرزه‌نگاری کودکان» به قانون آیین دادرسی کیفری الحاق شده است. [۱]

---

۱ – ماده ۳ قانون الحاق دولت جمهوری اسلامی ایران به پروتکل اختیاری کنوانسیون حقوق کودک درخصوص فروش، فحشاء و هرزه‌نگاری کودکان: «۱ – هر کشور عضو حداقل از تحت پوشش قرارگرفتن کامل اقدامات و فعالیتهای زیر به موجب حقوق جزائی یا کیفری خویش اطمینان حاصل خواهد نمود، خواه این جرائم در سطح داخلی یا فراملی، یا برمبنای فردی یا سازمان یافته صورت گرفته باشد: الف – در زمینه فروش کودکان به‌گونه‌ای که در ماده (۲) تعریف گردید: (۱) – عرضه، تحویل یا پذیرش کودک به هر وسیله، به منظور: (الف) – استثمار جنسی از کودک. (ب) – انتقال اندام کودک برای کسب سود. (پ) – به کارگیری کودک در کار اجباری. (۲) – توافق غیر ارادی نامناسب، به صورت یک واسطه، به منظور فرزندخواندگی کودک با نقض اسناد حقوقی بین‌المللی حاکم درمورد فرزندخواندگی. ب – عرضه، ابتیاع، تحصیل یا تدارک کودک به‌منظور فحشاء کودک به‌گونه‌ای که در ماده (۲) تعریف گردید. پ – تولید، توزیع، انتشار، ورود، صدور، عرضه، فروش یا مالکیت هرزه‌نگاری کودک برای مقاصد فوق به‌گونه‌ای که در ماده (۲) تعریف گردید. ۲ – با رعایت مقررات قانون ملی یک کشور عضو، همین امر در مورد کوشش برای مبادرت به هر یک از این اقدامات و همدستی در جرم یا مشارکت در هر یک از این اعمال خواهد گردید. ۳ – هر کشور عضو این جرائم را با کیفرهای مقتضی که ماهیت خطرناک این جرائم را درنظر گیرد، قابل مجازات خواهد ساخت. ۴ – هر کشور عضو در صورت اقتضاء با رعایت مقررات قانون ملی خود، اقداماتی را درخصوص ایجاد مسؤولیت اشخاص حقوقی در زمینه جرائم مذکور در بند (۱) این ماده به‌عمل خواهد آورد. با رعایت اصول حقوقی کشور عضو، این مسؤولیت اشخاص حقوقی ممکن است کیفری، مدنی یا اجرائی باشد. ۵ – کشورهای عضو کلیه اقدامات حقوقی و اجرائی مقتضی را به‌عمل خواهند آورد تا اطمینان حاصل شود که کلیه افراد دخیل در فرزند خواندگی کودک، طبق اسناد حقوقی بین‌المللی حاکم اقدام می‌نمایند.»

ماده ۴ این قانون: «۱ – هر کشور عضو چنانچه جرائم در قلمرو یا کشتی یا هواپیمای ثبت شده در آن کشور روی دهد اقداماتی را که برای احراز صلاحیت قضائی خویش در مورد جرائم موضوع بند (۱) ماده (۳) که ممکن است ضروری باشد، به عمل خواهد آورد. ۲ – هر کشور عضو می‌تواند اقداماتی را که ممکن است برای احراز صلاحیت قضائی خویش درمورد جرائم موضوع بند (۱) ماده (۳) ضروری باشد، درموارد زیر به‌عمل آورد: الف – چنانکه متهم مورد ادعا تبعه آن کشور یا شخصی باشد که در قلمرو آن اقامت دائم دارد؛ ب – چنانچه قربانی تبعه آن کشور باشد. ۳ – همچنین هر کشور عضو چنانچه متهم مورد ادعا در قلمرو آن کشور حضور داشته باشد و براساس اینکه جرم توسط یکی از اتباع آن روی داده است ←

۳ – مقنن در بند الف ماده ۶۶۴ ق. آ. د. ک.، به درستی «داده‌های مجرمانه» را از «داده‌هایی که برای ارتکاب جرم به کار رفته‌اند» تفکیک نموده است: داده‌های مجرمانه، داده‌هایی هستند که تولید، نگهداری و تبادل آنها ذاتا ممنوع است مانند داده‌های مبتذل و مستهجن. «داده‌هایی که برای ارتکاب جرم به کار رفته‌اند» داده‌هایی هستند که نفس داده هیچ ممنوعیت قانونی ندارد و در اصطلاح فقهای عظام، مباح است لکن از این داده‌ها برای مقاصد مجرمانه استفاده شده و یا این که جرمی علیه داده‌ها به وقوع پیوسته باشد مثل عکس‌های خانوادگی شهروندان، داده‌های دارای طبقه بندی دولتی، محتویات در حال تبادل مخابراتی،...

صرف ذخیره شدن داده‌ها، به هر نحو، در سامانه‌های رایانه‌ای و مخابراتی یا حاملهای داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری‌اسلامی‌ایران، برای محاکم ایران ایجاد صلاحیت می‌نماید.

۴ – برابر بند پ ماده اخیر الذکر، پیگرد قضایی حملات سایبری (هک و نفوذ) از خارج از کشور، نسبت به سامانه‌های رایانه‌ای و مخابراتی دولتی و عمومی، در صلاحیت محاکم ایران است که در صورت شناسایی متهم و وجود قرارداد استرداد مجرمین با کشور متبوع وی، امکان رسیدگی قضایی موضوع در ایران وجود دارد.

ماده ٦٦٥ قانون آیین دادرسی کیفری: «چنانچه جرم رایانه ای در صلاحیت دادگاههای ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. درصورتی‌که محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و در صورت اقتضاء صدور کیفرخواست می کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌کند.»

شرح ماده :

۱– مشابه ماده قانونی اخیر الذکر در ماده ۵۳ قانون آیین دادرسی دادگاههای عمومی و

→

وی را به دیگر کشور عضو مسترد نکند، اقداماتی را که ممکن است برای احراز صلاحیت قضائی خویش درمورد جرائم فوق‌الذکر ضروری باشد، به عمل خواهد آورد. ۴– این پروتکل هیچ‌گونه صلاحیت کیفری اعمال شده طبق قانون داخلی را نفی نمی‌نماید.»

انقلاب در امور کیفری نیز آمده بود که در بخش عمومات قانون جدید آیین دادرسی کیفری این موضوع مسکوت مانده و مقنن فقط در خصوص جرایم رایانه‌ای به آن پرداخته است. البته در حال حاضر با استفاده از ملاک ماده ۶۵۵ ق. آ. د. ک. می‌توان در خصوص سایر جرایم نیز، در صورت مشخص نبودن محل وقوع جرم، دادسرا و دادگاه محل کشف جرم را صالح دانست.

۲- چنانچه جرایم رایانه‌ای در بستر اینترنت ارتکاب یابند با استفاده از ip سامانه‌ای که متهم به اینترنت وصل شده است معمولا امکان شناسایی محل وقوع جرم وجود دارد لکن اولا: همه جرایم رایانه‌ای و مخابراتی در بستر اینترنت ارتکاب نمی‌یابند، ثانیا: با توجه به تنوع تجهیزات رایانه‌ای و مخابراتیِ همراه و همچنین برخی شگردهای مجرمان حرفه‌ای در استفاده از ip دیگران، کشف محل وقوع جرم در فضای مجازی با مشکلاتی مواجه می‌شود. مقنن برای حل مشکل صلاحیت محلی در این قبیل جرایم، دادسرا و دادگاه محل کشف جرم را مکلف به رسیدگی و صدور رأی نموده است.

ماده ٦٦٦ قانون آیین دادرسی کیفری: «قوه قضائیه موظف است به تناسب ضرورت، شعبه یا شعبی از دادسراها، دادگاههای کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه ای اختصاص دهد.

تبصره ـ مقامات قضائی دادسراها و دادگاههای مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب می‌شوند.»

شرح ماده :

۱ – شعب مورد نظر این ماده دادسراها و دادگاه‌های تخصصی بوده و نباید آنها را با دادگاههای اختصاصی اشتباه گرفت. بنابراین امکان ارجاع سایر پرونده به شعب تخصصی وجود دارد. البته در ماده اخیر بایستی به دادگاه‌های انقلاب نیز اشاره می‌شد چرا که رسیدگی به برخی از جرایم رایانه‌ای در صلاحیت دادگاه‌های انقلاب است.

۲ – در تهران دادسرای ناحیه‌ی ۳۱ ویژه‌ی رسیدگی به جرایم رایانه‌ای و فناوری اطلاعات است که رسیدگی تخصصی به موضوع جرایم رایانه‌ای را به عهده دارد. در سایر شهرستان‌ها نیز به تناسب نیاز، شعبی در دادسرا و دادگاه مشغول به کار هستند.

ماده ٦٦٧ قانون آیین دادرسی کیفری: «ارائه دهندگان خدمات دسترسی موظفند داده های ترافیک را حداقل تا شش‌ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش‌ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره ۱ـ داده ترافیک، هرگونه داده ای است که سامانه های رایانه ای در زنجیره ارتباطات رایانه ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می شود.

تبصره ۲ـ اطلاعات کاربر، هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، نشانی جغرافیایی یا پستی یا قرارداد اینترنت (IP)، شماره تلفن و سایر مشخصات فردی را شامل می‌شود.»

مقررات مرتبط:

بند الف ماده ۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی: «ارائه دهندگان خدمات دسترسی: اشخاصی هستند که امکان ارتباط کاربران را با شبکه‌های رایانه‌ای یا مخابراتی و ارتباطی داخلی یا بین‌المللی یا هر شبکه مستقل دیگر فراهم می‌آورند از قبیل تأمین کنندگان، توزیع کنندگان، عرضه کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابراتی.»

شرح ماده :

۱- به زبان ساده ارائه دهندگان خدمات دسترسی، در کشور ما شرکت‌هایی از قبیل مخابرات، ایرانسل، رایتل،.. هستند که امکان دسترسی کاربران را به اینترنت فراهم می‌نمایند. کاربر هر شخص حقیقی یا حقوقی است که از فضای مجازی استفاده می‌نماید.

۲- داده ترافیک در مقابل داده محتوا (اطلاعات) به کار می‌رود. اطلاعات عبارت است از آنچه برای انسان قابل فهم و درک است و داده‌هایی در مفهوم اطلاعات وارد می‌شوند که حاوی مفاهیم قابل فهم و درک برای انسان می‌باشند. این نوع داده‌های رایانه‌ای را اصطلاحاً «داده محتوا» نامیده‌اند. در مقابل «داده محتوا» داده‌های رایانه‌ای وجود دارند که حاوی یک سری اطلاعات غیر قابل فهم برای انسان هستند و نمی‌توان به آنها داده محتوا گفت مانند

داده‌هایی که هنگام راه اندازی یک سیستم رایانه‌ای به اجزای مختلف آن دستور می‌دهد یا داده‌هایی که هنگام انتقال داده‌های اصلی در شبکه برای تعیین مسیر، توسط رایانه‌ها ایجاد و ضمیمه آنها می‌گردد این داده‌ها را داده ترافیک نامیده‌اند. [۱]

۳- مهلت شش ماهه برای نگهداری اطلاعات کاربران و داده ترافیک ایجاد یا تبادل شده، در واقع ضرب الاجلی برای بزه دیدگان و ضابطان است که اگر قصد شکایت یا تعقیب جرایم رایانه‌ای را دارند تا قبل از اتمام این مهلت قانونی، اقدام نمایند و الا در مورد داده‌های ترافیک با گذشت شش ماه از تاریخ ایجاد داده ها و اطلاعات کاربران با گذشت حداقل شش‌ماه پس از خاتمه اشتراک اینترنتی، دسترسی به این داده‌ها و اطلاعات با مشکل مواجه خواهد شد.

ماده ٦٦٨ قانون آیین دادرسی کیفری: «ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش‌ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند.»

مقررات مرتبط:

بند ب ماده ۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی: «ارائه دهندگان خدمات میزبانی: اشخاصی هستند که امکان دسترسی کاربران به فضای ایجاد شده توسط سامانه‌های رایانه‌ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می‌کنند تا راساً یا توسط کاربر متقاضی، داده‌های رایانه‌ای را جهت نگهداری، انتشار، توزیع یا ارائه در شبکه‌های داخلی یا بین‌المللی یا هر منظور دیگر ذخیره یا پردازش کنند.»

شرح ماده :

۱ – منظور از ارائه دهندگان خدمات میزبانی در واقع شرکت‌های تخصصی هستند که با دارا بودن سِرورها و دیتا سنترها، به متقاضیان راه اندازی سایت‌های اینترنتی، شبکه‌های اجتماعی و پیام رسان‌ها، فضای لازم جهت فعالیت را ارائه می‌نمایند. کلیه سایت‌های اینترنتی برای شروع و ادامه فعالیت خود بایستی علاوه بر مجوزهای قانونی، فضای لازم را از شرکت‌های

۱ – جاوید نیا، جواد، جزوه آموزشی جرایم رایانه‌ای کاربردی، تیر ماه ۱۳۹۴، ص ۶

ارائه دهنده خدمات میزبانی خریداری نمایند.

۲ – مقنن برای ارائه دهندگان خدمات میزبانی علاوه بـر تکـالیف مقـرر در مـاده ۷۵۱ قـانون مجازات اسلامی (تعزیرات) در خصوص پالایش محتویات مجرمانـه، دو تکلیـف دیگـر را نیـز برای در نظر گرفته است: الف) نگهداری اطلاعات کاربران خود را حداقل تا شـش‌مـاه پـس از خاتمه اشتراک؛ ب) نگهداری محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجادشـده حداقل تا پانزده روز از زمان ایجاد. در واقع تکالیف اخیر الذکر به منظور حفظ ادله الکترونیکی و استفاده احتمالی از آنها در مقام اثبات جرم و یا دفاع است.

پرسش ۳۲:

جرایمی که در بستر پیام رسان‌های خارجی (از قبیل نسخه اصـلی تلگـرام، اینسـتاگرام، فـیس بوک،...) اتفاق می‌افتند آیا در دستگاه قضایی ایران قابل پیگیری هستند یا خیر؟

پاسخ:

به طور کلی پیام رسان‌های خارجی پاسخگوی پلیس فتـا و دسـتگاه قضـایی ایـران نیسـتند و امکان شناسایی مجرمان از این طریق وجود ندارد لکن در صورت وجود شاکی، شناسایی متهم از طریق محتویات موجود یا حافظه پنهان (در صورت حـذف حسـاب کـاربری) گوشـی تلفـن همراه شاکی و شبکه مخابراتی امکان پذیر است. حتی در صورتی که متهم در خـارج از کشـور باشد امکان دستیابی به وی با استفاده از پلیس بین الملل (در صـورت وجـود قـرارداد اسـترداد مجرمان بین ایران و کشور مورد نظر) متصور است. در حال حاضر سِرورهای نسخه‌هـای غیـر اصلی تلگرام (تلگرام طلایی و هاتگرام) در داخل کشور مسـتقر هسـتند و هماننـد سـایر پیـام رسان‌های داخلی، امکان پیگیری سریع تر جرایم ارتکابی در بسنر آنها وجود دارد.

ماده ٦٦٩ قانون آیین دادرسی کیفری: «هرگاه حفظ داده های رایانه ای ذخیره‌شـده بـرای تحقیق یا دادرسی لازم باشد، مقام‌قضائی می تواند دستور حفاظت از آنها را برای اشخاصی کـه به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب دیـدن یـا تغییر یا از بین رفتن داده ها، ضابطان قضائی می توانند دستور حفاظت را صادر کننـد و مراتـب را حداکثر تا بیست و چهار ساعت به اطلاع مقام قضائی برسانند. چنانچه هـر یـک از کارکنـان دولت یا ضابطان قضائی یا سایر اشخاص از اجرای این دستور خودداری یا داده هـای حفاظـت

شده را افشاء کنند یا اشخاصی که داده های مزبور به آنها مربوط مـی شـود را از مفـاد دسـتور صادره آگاه کنند، ضابطان قضائی و کارکنان دولت به مجازات امتناع از دستور مقـام قضـائی و سایر اشخاص به حبس از نود و یک روز تا شش‌ماه یا جزای نقدی از پنج تا ده میلیـون ریـال یا هردو مجازات محکوم می‌شوند.

تبصره ۱ـ حفظ داده ها به منزله ارائه یا افشاء آنها نیسـت و مسـتلزم رعایـت مقـررات مربـوط است.

تبصره ۲ـ مدت زمان حفاظت از داده‌ها حداکثر سه‌ماه است و در صورت لزوم بـا دسـتور مقـام قضائی قابل تمدید است.»

مقررات مرتبط:

ماده ۵۷۶ قانون مجازات اسلامی (تعزیرات) چنانچه هر یک از صاحب‌منصبان و مستخدمین و مامورین دولتی و شهرداریها در هر رتبه و مقامی که باشند از مقام خود سوء استفاده نمـوده و از اجرای اوامر کتبی دولتی یا اجرای قوانین مملکتی و یا اجرای احکام یا اوامر مقامات قضائی یـا هر گونه امری که از طرف مقامات قانونی صـادر شـده باشـد جلـوگیری نمایـد بـه انفصـال از خدمات دولتی از یک تا پنج سال محکوم خواهد شد.

بند ه ماده ۱ آیین نامه جمع آوری و استناد پذیری ادله الکترونیکی: «زنجیره حفاظتی: مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذیصلاح به منظور حفظ صحت، تمامیـت، اعتبار و انکارناپذیری ادله الکترونیکی با بکـارگیری ابزارهـا و روش‌هـای اسـتاندارد در مراحـل شناسایی، کشف، جمع آوری، مستندسازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجـرا درآورده و ثبت می‌کنند؛ به نحوی که امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد.»

بند ز ماده ۱ آیین نامه جمع آوری و استناد پذیری ادله الکترونیکی: «مجری حفاظت: شخصـی است که به نحوی داده‌های رایانه‌ای ذخیره شده را تحت تصرف یا کنترل دارد و مطـابق مـاده ۳۴ قانون و سایر قوانین و مقررات جهت حفاظت آنها تعیین می‌شود.»

شرح ماده :

۱ – حفاظت از داده‌ها با توقیف آنها متفاوت است. در حفاظت داده‌ها، به دستور مقـام قضـایی،

داده‌ها توسط اشخاصی که به نحوی آنها را تحت تصرف یا کنترل دارند، حفظ و مصون از تعرض می‌ماند تا در مراحل دادرسی ارائه شود. لکن در توقیف، داده‌ها توسط ضابطان کپی برداری شده و یا با حامل داده ضبط می‌شوند و در هر حال تا تعیین تکلیف نهایی از دسترس سایرین مصون می‌مانند. دستور حفاظت از داده‌ها، دستوری موقتی بوده و حداکثر برای سه ماه است. ممکن است که بعد از این مدت، دستور حفاظت تمدید شود، یا از دستور رفع اثر شود و یا دستور توقیف داده‌ها صادر شود. در هر حال دستور حفاظت از داده‌ها معمولا در موارد فوری که امکان توقیف داده‌ها یا سامانه‌ها وجود ندارد صادر می‌شود و اگر امکان تفتیش و توقیف داده‌ها وجود دارد بایستی از صدور دستور حفاظت خودداری نمود.

پرسش ۳۳:

قانونگذار در ماده ۳۴ قانون جرایم رایانه‌ای[۱] ماده اخیر به موجب ماده ۶۶۹ قانون آیین دادرسی کیفری نسخ شده است لکن مصوبه جدید تفاوت چندانی با ماده ۳۴ ندارد] مقرر نموده در صورتی که برای تحقیق و دادرسی حفظ داده‌های رایانه‌ای ذخیره شده لازم باشد می‌تواند دستور حفاظت از آنها را برای اشخاص که به نحوی داده را تحت تصرف یا کنترل دارد صادر نماید و در شرایط فوری نظیر خطر آسیب‌دیدن یا تغییر یا از بین رفتن داده‌ها ضابطان قضایی می‌توانند راساً دستور حفاظت را صادر و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضایی برسانند اما قانونگذار در خصوص داده‌های در حال انتقال و یا انباشت‌شده موقت تعیین تکلیف ننموده است که آیا در شرایط فوری که بیم از بین رفتن ادله می‌باشد ضابط می‌تواند بدون اخذ دستور قضایی و به موجب این ماده دستور حفاظت را صادر نماید؟

---

۱ – ماده۳۴ قانون جرایم رایانه‌ای: «هرگاه حفظ داده‌های رایانه‌ای ذخیره شده برای تحقیق یا دادرسی لازم باشد، مقام قضائی می‌تواند دستور حفاظت از آنها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضائی می‌توانند رأساً دستور حفاظت را صادر کنند و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضائی برسانند. چنانچه هر یک از کارکنان دولت یا ضابطان قضائی یا سایر اشخاص از اجرای این دستور خودداری یا داده‌های حفاظت شده را افشاء کنند یا اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضائی و کارکنان دولت به مجازات امتناع از دستور مقام قضائی و سایر اشخاص به حبس از نودویک روز تا شش ماه یا جزای نقدی از پنج میلیون (۵. ۰۰۰. ۰۰۰) ریال تا ده میلیون (۱۰. ۰۰۰. ۰۰۰) ریال یا هر دو مجازات محکوم خواهند شد.

تبصره۱ ـ حفظ داده‌ها به منزله ارائه یا افشاء آنها نبوده و مستلزم رعایت مقررات مربوط است.

تبصره۲ـ مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضائی قابل تمدید است.»

پاسخ:

نظریه شماره ۷/۹۲/۱۹۱۸ – ۴/۱۰/۱۳۹۲ اداره کل حقوقی قوه قضائیه:

«مقررات ماده ۳۴ قانون جرایم رایانه‌ای مصوب ۵/۳/۱۳۸۸ موضوعاً منصرف از داده‌های در حال انتقال ارتباطات غیر عمومی است و به آنها تسری ندارد و در خصوص صدور دستور حفاظت از داده‌های یادشده، با توجه به مواد ۲ و ۴۸ این قانون و نیز تبصره ماده ۵۲ قانون مزبور می‌بایست مطابق قانون آیین دادرسی کیفری اقدام گردد، اما در خصوص داده‌های انباشت‌شده موقت ناشی از ارتباطات عمومی، در حکم داده‌های ذخیره‌شده می‌باشد و لذا مقررات ماده ۳۴ قانون فوق‌الذکر در این خصوص قابل اعمال است، بدیهی است که مقررات ماده اخیرالذکر صرفاً ناظر به صدور دستور حفاظت داده‌های مربوطه است و به موارد دیگر نظیر دسترسی و ارائه اطلاعات تسری ندارد.»

۲ – اجرای دستور حفاظت از داده‌ها ممکن است به ضابطان دادگستری، مدیران و کارکنان دولتی و عمومی، شرکت‌های ارائه دهنده خدمات میزبانی،... محول شود البته بدیهی است که صدور چنین دستوری برای شاکی یا متهم پرونده یا اشخاصی که از عدم حفاظت از داده‌ها منتفع می‌شوند، معقول نمی‌باشد و بایستی شخص بی طرفی به عنوان مجری دستور انتخاب شود.

۳ – مقنن به منظور تضمین حفاظت از داده‌ها توسط این اشخاص، ضمانت اجرای کیفری قرار داده و برای سه رفتار مجریان حفاظت، جرم انگاری نموده است: الف) مجریان از اجرای این دستور خودداری نمایند، ب) داده های حفاظت شده را افشاء کنند، ج) اشخاصی که داده های مزبور به آنها مربوط می شود را از مفاد دستور صادره آگاه کنند.

پرسش ۳٤:

از آنجا که مقنن علاوه بر مقامات قضایی، در موارد فوری به ضابطان نیز اجازه داده که دستور حفاظت از داده‌ها را صادر نمایند، اگر مجریان حفاظت از اجرای دستور ضابطان استنکاف نمایند و یا مرتکب سایر رفتارهای مندرج در قسمت اخیر ماده ۶۶۹ قانون آیین دادرسی کیفری شوند، آیا موضوع جرم بوده و قابل مجازات است یا اینکه صرفا در صورتی که دستور دهنده مقام قضایی باشد موضوع واجد وصف مجرمانه است؟

پاسخ:

ممکن است که گفته شود چون مقنن در متن ماده مجازات امتناع از دستور مقام قضائی را برای ضابطان و کارمندان دولت در نظر گرفته است لذا در صورتی که صادر کننده دستور مقام قضایی نباشد، موضوع واجد وصف مجرمانه نیست.

لکن در مورد این پاسخ بایستی قدری تأمل نمود، مقنن در صدر ماده اخیر الذکر فلسفه صدور این دستور را «حفظ داده های رایانه ای ذخیره‌شده برای تحقیق یا دادرسی» بیان کرده و چه بسا با تأخیر چند ثانیه‌ای در صدور دستور حفاظت، داده‌ها توسط مجرمان از بین بروند یا تغییر ماهیت یابند، بر همین مبنا مقنن در موراد فوری به ضابطان نیز اجازه داده که دستور حفاظت را صادر نمایند و اگر این دستور را فاقد ضمانت اجرا بدانیم، نقض غرض مقنن است. مضاف بر اینکه مقنن عالما و عامدا مقرر نموده که خاطیان «به مجازات امتناع از دستور مقام قضائی» محکوم می‌شوند و در واقع موضوع را در حکم بزه امتناع از دستور مقام قضائی قرار داده است. لذا به نظر می‌رسد که با توجه به اطلاق ماده، از این حیث تفاوتی بین دستور مقام قضایی و ضابطان نباشد.

ماده ٦٧٠ قانون آیین دادرسی کیفری: «مقام قضائی می تواند دستور ارائه داده های حفاظت شده مذکور در مواد (۶۶۷)، (۶۶۸) و (۶۶۹) این قانون را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. خودداری از اجرای این دستور و همچنین عدم نگهداری وعدم مواظبت از این داده‌ها موجب مجازات مقرر در ماده (۶۶۹) این قانون می‌شود.»

مقررات مرتبط:

بند ج ماده ۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی: «ارائه داده‌های الکترونیکی: عبارت است از در اختیار قراردادن تمام یا بخشی از داده‌های حفظ یا نگهداری شده توسط ارائه دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده‌ها را تحت تصرف یا کنترل دارند.»

شرح ماده :

۱ – پس از صدور دستور حفاظت از داده‌ها، گام بعدی ارائه داده‌های حفاظت شده به ضابطان، جهت بهره برداری در روند تحقیقات و رسیدگی است. ارائه داده‌ها ممکن است که به صورت

ذخیره کردن داده‌ها در حامل‌های داده، پرینت گرفتن متن یـا عکـس و یـا اسـکرین شـات،... باشد.

۲ – ضابطان جرایم رایانه‌ای عمدتا مأموران پلیس فتا هستند، پلیس فتا (پلیس فضای تولیـد و تبادل اطّلاعات) در بهمن‌ماه سال ۱۳۸۹ تشکیل گردیده که در شرح وظایف این پلـیس آمـده است: ایجاد امنیت و کاهش مخـاطرات بـرای فعّالیّـت‌هـای علمـی، اقتصـادی، اجتمـاعی در جامعه‌ی اطّلاعاتی، حفاظت و صیانت از هویت دینی و ملّی، مراقبت و پایش از فضای تولیـد و تبادل اطّلاعات برای پیش‌گیری از تبدیل شدن این فضا به بستری برای انجام هماهنگی‌هـا و عملیات برای انجـام و تحقّـق فعّالیّـت‌هـای غیرقـانونی و ممانعـت از تعـرّض بـه ارزش‌هـا و هنجارهای جامعه در فتا از جمله‌ی وظـایف و مأموریـت‌هـای پلـیس فضـای تولیـد و تبـادل اطّلاعات ناجاست[۱].

۳ – در ذیل ماده ۶۷۰ برای «عدم نگهداری وعدم مواظبت از این داده‌ها» جرم انگاری نمـوده که به نظر می‌رسد اعم از اینکه عمدا یا سهوا در اثر عدم نگهداری و عدم مواظبـت از داده‌هـا، آسیبی به داده‌ها برسد، جرم محقق شده لذا این جرم با فعل و ترک فعل قابلیت تحقق دارد.

ماده ٦٧١ قانون آیین دادرسی کیفری: «تفتیش و توقیف داده‌ها یا سامانه‌هـای رایانـه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می آید که ظن قوی به کشـف جـرم یا شناسایی متهم یا ادله جرم وجود دارد.»

قوانین مرتبط:

ماده ۵۵ قانون آیین دادرسی کیفری: «ورود به منازل، اماکن تعطیـل و بسـته و تفتـیش آنهـا، همچنین بازرسی اشخاص و اشیاء در جرایم غیرمشهود با اجازه موردی مقام قضایی است، هـر چند وی اجرای تحقیقات را به‌طور کلی به ضابط ارجاع داده باشد.»

شرح ماده :

۱ – تفتیش در لغت به معنای بازرسی، جستجو کردن و تفحص کردن آمده است. در اصطلاح حقوقی نیز تفتیش به معنای جستجو در منازل، اماکن یا اشیاء در ماردی است که دلیل یا ظـن قوی به کشف اسباب، آلات و دلایل جرم یا شناسایی متهم در آنها وجود دارد. به عبارت دیگر

۱ – به نقل از سایت پلیس فتا https: //www. cyberpolice. ir

تفتیش اختیاری است که بیانگر ورود به یک منزل یا مکان و یا بازرسی یک شیء بـر خـلاف اراده مالک یا متصرف آن است.

توقیف در لغت به معنای بازداشت کردن و ضبط کردن آمده است و در اصطلاح حقوقی، حفـظ و تأمین (در امنیت قرار دادن) اماکن، منازل و اشیاء موضوع تفتیش بـه منظـور تحصـیل ادلـه مرتبط و مناسب از آنها، در مواردی که تفتیش محتاج صرف وقت زیادتری بوده یا این کـه بـه هر دلیل ضبط کردن موضوع تفتیش برای ادامه تحقیقات ضرورت داشته باشد، است. [۱]

۲ – از آنجا که معمولا داده‌ها و سامانه‌های رایانه‌ای رمز نگاری می‌شوند تفتیش آنهـا مسـتلزم این است که ضابطان رمز ورود به سامانه را داشته باشند. ضابطان در اجرای دستور تفتیش بدوا بایستی که این رمز را از مالک یا متصرف سامانه دریافت نمایند کـه اگـر ایـن شـخص مـتهم پرونده نیز باشد احتمال عدم همکاری وی متصور است. در ایـن صـورت ضـابطان بـا کسـب دستور قضایی جدید، می‌توانند نسبت به باز نمودن قفل سامانه به شیوه‌های فنی اقدام و دستور تفتیش سامانه را به اجرا نمایند. قسمت اخیر ماده ۶۷۲ ق. آ. د. ک. مؤید برداشت اخر است.

۳ – در اصول فقه مراتب علم را به این صـورت تقسـیم کـرده‌انـد: گـاهی انسـان نسـبت بـه موضوعی علم پیدا می‌کند و آن را صد در صد باور می‌کند که به آن یقین می‌گویند. گاهی باور انسان به آن حد نمی‌رسد ولی بیش از پنجاه درصد است که آن را ظن گویند. گاهی باور انسان نسبت به موضوعی کمتر از پنجاه درصد اسـت کـه آن را وهـم گوینـد. گـاهی هـر دو طـرف احتمال، مساویند مانند دو کفه ترازو که این را شک گویند که هیچ کدام نسبت به طرف دیگـر رجحان ندارد. [۲] ظن قوی در واقع بسیار نزدیک به یقین است.

ماده ٦٧٢ قانون آیین دادرسی کیفری: «تفتیش و توقیف داده ها یا سامانه هـای رایانـه ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحـت کنتـرل قـانونی دارند، نظیر متصدیان سامانه ها انجام می‌شود. درصورت عدم حضور یا امتنـاع از حضـور آنـان چنانچه تفتیش یا توقیف ضرورت داشته باشدیا فوریت امر اقتضاء کند، قاضـی بـا ذکـر دلایـل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر می‌کند.»

---

۱ – نوریان، علیرضا، همان، ص ۱۲۷.

۲ – مصدق، محمد، کاربرد علم اصول در فقه و حقوق، انتشارات سادات رضوی، چاپ اول، ۱۳۹۲، تهران، ص ۱۷۹.

اسلام به نحوی که تبلیغ از آنها باشد. (بند ۹ ماده ۶ قانون مطبوعات)
۶ – اهانت به امام خمینی (ره) و تحریف آثار ایشان (ماده ۵۱۴ قانون مجازات اسلامی)
۷ – اهانت به مقام معظم رهبری (امام خامنه‌ای) و سایر مراجع مسلم تقلید (بند ۷ ماده ۶ قانون مطبوعات)

ج) محتوا علیه امنیت و آسایش عمومی

۱ – تشکیل جمعیت، دسته، گروه در فضای مجازی (سایبر) با هدف برهم زدن امنیت کشور. (ماده ۴۹۸ قانون مجازات اسلامی)
۲– هر گونه تهدید به بمب گذاری. (ماده ۵۱۱ قانون مجازات اسلامی)
۳ – محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند. (بند ۱ ماده ۶ قانون مطبوعات)
۴ – انتشار محتوا علیه اصول قانون اساسی. (بند ۱۲ ماده ۶ قانون مطبوعات)
۵ – تبلیغ علیه نظام جمهوری اسلامی ایران. (ماده ۵۰۰ قانون مجازات اسلامی)
۶ – اخلال در وحدت ملی و ایجاد اختلاف مابین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی. (بند ۴ ماده ۶ قانون مطبوعات)
۷ – تحریک یا اغوای مردم به جنگ و کشتار یکدیگر. (ماده ۵۱۲ قانون مجازات اسلامی)
۸ – تحریک نیروهای رزمنده یا اشخاصی که به نحوی از انحا در خدمت نیروهای مسلح هستند به عصیان، فرار، تسلم یا عدم اجرای وظایف نظامی. (ماده ۵۰۴ قانون مجازات اسلامی)
۹ – تحریص و تشویق افراد و گروه‌ها به ارتکاب اعمالی علیه امنیت، حیثیت و منافع جمهوری اسلامی ایران در داخل یا خارج از کشور. (بند ۵ ماده ۶ قانون مطبوعات)
۱۰ – تبلیغ به نفع گروه‌ها و سازمانهای مخالف نظام جمهوری اسلامی ایران (ماده ۵۰۰ ق م. ا.)
۱۱ – فاش نمودن و انتشار غیرمجاز اسناد و دستورها و مسایل محرمانه و سری دولتی و عمومی. (بند ۶ ماده ۶ قانون مطبوعات و مواد ۲و۳ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۳ قانون جرائم رایانه‌ای)

۱۲ – فاش نمودن و انتشار غیرمجاز اسرار نیروهای مسلح. (بند ۶ ماده ۶ قانون مطبوعات)
۱۳ – فاش نمودن و انتشار غیرمجاز نقشه و استحکامات نظامی. (بند ۶ ماده ۶ قانون مطبوعات)
۱۴ – انتشار غیرمجاز مذاکرات غیرعلنی مجلس شورای اسلامی. (بند ۶ ماده ۶ قانون مطبوعات)
۱۵ – انتشار بدون مجوز مذاکرات محاکم غیرعلنی دادگستری و تحقیقات مراجع قضایی. (بند ۶ ماده ۶ قانون مطبوعات)
۱۶ – انتشار محتوای که از سوی شورای عالی امنیت ملی منع شده باشد. (تبصره ۲ ماده ۵ قانون مطبوعات)

د) محتوا علیه مقامات و نهادهای دولتی و عمومی

۱ – اهانت و هجو نسبت به مقامات، نهادها و سازمان‌های حکومتی و عمومی. (بند ۸ ماده ۶ قانون مطبوعات و مواد ۶۰۹ و ۷۰۰ قانون مجازات اسلامی)
۲ – افترا به مقامات، نهادها و سازمان‌های حکومتی و عمومی. (بند ۸ ماده ۶ قانون مطبوعات و ۶۹۷ قانون مجازات اسلامی)
۳ – نشراکاذیب و تشویش اذهان عمومی علیه مقامات، نهادها و سازمانهای حکومتی. (بند ۱۱ ماده۶ قانون مطبوعات و ۶۹۸ قانون مجازات اسلامی)
ه) محتوای که برای ارتکاب جرایم رایانه‌ای به کار می‌رود (محتوا مرتبط با جرایم رایانه‌ای)
۱ – انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم افزارهایی که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می‌رود. (ماده ۲۵ قانون جرائم رایانه‌ای)
۲ – فروش انتشار یا در دسترس قرار دادن غیرمجاز گذرواژه‌ها و داده‌هایی که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی دولتی یا عمومی را فراهم می‌کند. (ماده ۲۵ قانون جرائم رایانه‌ای)
۳ – انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، تحریف و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی. (ماده ۲۵ قانون جرائم رایانه‌ای)

۴ – آموزش و تسهیل سایر جرایم رایانه‌ای. (ماده ۲۱ قانون جرائم رایانه‌ای)
۵ – انتشار فیلترشکن‌ها و آموزش روشهای عبور از سامانه‌های فیلترینگ. (بند ج ماده ۲۵ قانون جرائم رایانه‌ای)
۶ – انجام هرگونه فعالیت تجاری و اقتصادی رایانه‌ای مجرمانه مانند شرکت‌های هرمی، فعالیت‌های غیرمجاز مرتبط با بازار اوراق بهادار (قانون اخلال در نظام اقتصادی کشور و بند الف ماده ۴۹ قانون بازار و اوراق بهادار ج. ا. ا. و سایر قوانین مرتبط)
۷ – ایجاد مراکز قمار در فضای مجازی (مواد ۷۰۵، ۷۰۸ و ۷۱۰ قانون مجازات اسلامی)
۸ – بکارگیری و وارد کردن کلمات کلیدی (tag) نامرتبط با محتوای سایت یا سوء استفاده از نرم افزارهایی نظیرپاپ آپ که منجر به بازکردن اجباری صفحات غیرمرتبط با درخواست بازدید کننده شده و درنتیجه موجب اتلاف وقت و هزینه بازدیدکنندگان و افزایش متقلبانه رتبه سایت و کسب درآمد و امتیاز برای مالک سایت می‌گردد (ماده ۷۴۱ بخش تعزیرات قانون مجازات اسلامی (جرایم رایانه‌ای) و مصوبه هشتاد و هشتمین جلسه کارگروه تعیین مصادیق محتوای مجرمانه)
۹ – جعل پایگاه‌های اینترنتی بانک‌ها، سازمان‌ها و نهادهای دولتی و عمومی (مواد ۶ و ۷ قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸)
و) محتوای که تحریک، ترغیب، یا دعوت به ارتکاب جرم می‌کند (محتوای مرتبط با سایر جرایم)
۱ – انتشار محتوای حاوی تحریک، ترغیب، یا دعوت به اعمال خشونت آمیز و خودکشی. (ماده ۱۵ قانون جرائم رایانه‌ای)
۲ – تبلیغ و ترویج مصرف مواد مخدر، مواد روان گردان و سیگار. (ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵)
۳ – درج پیوند (لینک) یا تبلیغ تارنماهای فیلتر شده یا باز انتشار محتوای مجرمانه نشریات توقیف شده و رسانه‌های وابسته به گروه‌ها و جریانات منحرف و غیر قانونی.
۴ – تشویق تحریک و تسهیل ارتکاب جرائمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم، تخریب اموال عمومی، ارتشاء، اختلاس، کلاهبرداری، قاچاق مواد مخدر، قاچاق مشروبات الکلی و غیره. (ماده ۱۲۶ قانون مجازات اسلامی)

۵ – تبلیغ و ترویج اسراف و تبذیر. (بند ۳ ماده ۶ قانون مطبوعات)
۶ – فروش، تبلیغ، توزیع و آموزش استفاده از تجهیزات دریافت از ماهواره (ماده ۱ قانون ممنوعیت بکارگیری تجهیزات دریافت ماهواره مصوب ۱۳۷۳/۱۱/۲۵)
۷ – فروش، تبلیغ، توزیع و هرگونه معامله بدون مجوز تجهیزات نظامی و تجهیزاتی که دارای کاربرد دو گانه و نیز اقلام و موارد تحت کنترل از قبیل انواع مواد محترقه، ناریه، منفجره اعم از نظامی و غیرنظامی، شیمیایی، رادیواکتیو، میکروبی، گازهای بیهوش‌کننده، بی‌حس‌کننده و اشک‌آور و شوک‌دهنده‌ها (شوکرها) و تجهیزات نظامی و انتظامی. (مواد ۱ تا ۴ قانون مجازات قاچاق اسلحه و مهمات و دارندگان سلاح و مهمات غیر مجاز و مصوبه چهل و هفتمین جلسه کارگروه تعیین مصادیق محتوای مجرمانه)
۸ – راه اندازی رادیو و تلویزیون اینترنتی و انتشار و پخش برنامه‌های صوتی و تصویری از طریق سیستم‌های فنی قابل انتشار فراگیر، بدون مجوز سازمان صدا و سیمای جمهوری اسلامی ایران (پاسخ شورای نگهبان به استفساریه رییس وقت سازمان صدا و سیما درباره اصل ۴۴ قانون اساسی و مصوبه شصت و دومین جلسه کارگروه تعیین مصادیق محتوای مجرمانه)

ز) محتوا مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی

۱ – انتشار و سرویس دهی بازی‌های رایانه‌ای دارای محتوای مجرمانه یا فاقد مجوز از وزارت فرهنگ و ارشاد اسلامی (بنیاد ملی بازی‌های رایانه‌ای) (مواد مختلف قانون مجازات اسلامی و قانون جرائم رایانه‌ای)
۲ – معرفی آثار سمعی و بصری غیرمجاز به جای آثار مجاز. (ماده ۱ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز دارند)
۳ – عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی (ماده ۲ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز دارند)
۴ – تشویق و ترغیب به نقض حقوق مالکیت معنوی (ماده ۱ قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه‌ای و ماده ۷۴ قانون تجارت الکترونیکی)

ح) محتوای مجرمانه مرتبط با انتخابات مجلس شورای اسلامی و مجلس خبرگان رهبری

۱ – انتشار هرگونه محتوا با هدف ترغیب و تشویق مردم به تحریم و یا کاهش مشارکت در

انتخابات (ماده ۷۵ آیین نامه اجرایی قانون انتخابات مجلس خبرگان رهبری و بند ۳ و ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی و ماده ۴۶ آیین نامه اجرایی آن)

۲ – انتشار هرگونه ادعای غیرواقع مبنی بر توقف انتخابات و یا دعوت به تجمع اعتراض‌آمیز، اعتصاب، تحصن و هر اقدامی که به نحوی موجب اخلال در امر انتخابات گردد (ماده ۷۵ آیین نامه اجرایی قانون انتخابات مجلس خبرگان رهبری و بند ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی)

۳ – انتشار و تبلیغ علائم گروه‌های ضدانقلاب و معاند مرتبط با انتخابات (ماده ۵۰۰ قانون مجازات اسلامی)

۴ – انتشار هجو یا هجویه و یا هرگونه محتوای توهین‌آمیز در فضای مجازی علیه انتخابات (ماده ۷۰۰ قانون مجازات اسلامی و بند ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی)

۵ – انتشار هرگونه مطلب خلاف واقع مبنی بر انصراف گروه‌های قانونی از انتخابات (ماده ۶۹۸ قانون مجازات اسلامی، ماده ۶۴ قانون انتخابات مجلس شورای اسلامی و ماده ۷۵ آیین نامه اجرایی قانون انتخابات مجلس خبرگان رهبری)

۶ – استفاده از سایت‌ها و وبلاگ‌های رسمی نهادها و دستگاه‌های دولتی جهت بهره‌برداری در تبلیغات نامزدهای انتخاباتی. شایان ذکر است تمامی شرکت‌ها، موسسات، شهرداری‌ها، سازمان‌ها و نهادهایی که قسمتی از دارایی آنها جزء بودجه و اموال عمومی است مشمول این ماده می‌شوند. (ماده ۵۹ قانون انتخابات مجلس شورای اسلامی و ماده ۲۵ و ۲۶ آیین نامه اجرایی قانون انتخابات مجلس خبرگان رهبری)

۷ – درج محتوای تبلیغاتی نامزدهای انتخاباتی خارج از مدت زمان مقرر شده برای فعالیت انتخاباتی. (ماده ۵۶ قانون قانون انتخابات مجلس شورای اسلامی و ماده ۴۵ آیین‌نامه اجرایی آن و ماده ۲۳ آیین نامه اجرایی قانون انتخابات مجلس خبرگان رهبری)

۸ – انتشار هرگونه محتوا در جهت تحریک، ترغیب، تطمیع و یا تهدید افراد به خرید و فروش آراء، رای دادن با شناسنامه جعلی و شناسنامه دیگری، جعل اوراق تعرفه، رای دادن بیش از یک‌بار و سایر روش‌های تقلب در رای‌گیری و شمارش آراء. (ماده ۷۵ آیین نامه اجرایی قانون انتخابات مجلس خبرگان رهبری و ماده ۶۶ قانون انتخابات مجلس شورای اسلامی و ماده ۱۲۶ قانون مجازات اسلامی)