فهرست مطالب

قسمت اول

از قانون جرائم رایانه‌ای

مصوب ۱۳۸۸

بخش یکم- جرائم و مجازات‌ها

فصل یکم- جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

مبحث یکم- دسترسی غیرمجاز

دسترسی بدون مجاز

ماده ۱ (ماده ۷۲۹ ق.م.ا)- هر کس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از ۹۱ روز تا ۱ سال یا جزای نقدی از ۵ میلیون ریال تا ۲۰۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد.

■ ۱- قانونگذار ما تعریفی از «جرائم رایانه‌ای» ارائه نداده است بلکه فقط مصادیق این جرائم را معرفی کرده است که عبارتند از: کلاهبرداری رایانه‌ای، جعل رایانه‌ای، جاسوسی رایانه‌ای، تخریب رایانه‌ای، دستیابی غیرمجاز، سابوتاژ رایانه‌ای، شنود غیرقانونی و غیره.

«دسترسی غیرمجاز» (Unauthorized access) عنوان عامی است که شامل این جرائم نیز می‌شود اما این عنوان مجرمانه تا زمانی است که منتهی به جرائم مزبور نشده باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۲)

■ ۲- جرائم تجارت الکترونیکی یعنی «جرائم رایانه‌ای خاص حیطه تجارت الکترونیکی» و زیرمجموعه‌ای از جرائم رایانه‌ای در معنای عام است.

به طور تخصصی‌تر، دو تعریف خاص و عام از این واژه به عمل می‌آوریم:

الف- تعریف خاص: «هر جرمی که قانونگذار به صراحت وقوع در بستر مبادلات مالی الکترونیکی را شرط تحقق آن اعلام کرده باشد؛» این تعریف صرفاً موارد مندرج در ق.ت الکترونیکی را در بر می‌گیرد.

ب- تعریف عام: «هر جرمی که قانونگذار به صراحت وقوع در بستر مبادلات مالی الکترونیکی را شرط تحقق آن اعلام کرده باشد یا عملاً در بستر مبادلات مالی الکترونیکی به وقوع بپیوندد.» (جاویدنیا، جواد، جرائم تجارت الکترونیکی، چ ۳، چکیده)

■ ۳- منظور از «سیستم رایانه‌ای» تنها رایانه‌های شخصی یا مستقل نیستند، هر چند مثال اجلای آن را شامل می‌شوند، و باید مفهوم موسع آنها را مورد توجه قرار داد. بر این اساس، کنوانسیون جرائم سایبر در بند (الف) از ماده ۱ در تعریفی از این سیستم‌ها چنین اشعار می‌دارند: «منظور از «سیستم رایانه‌ای» (Computer system) هر دستگاه یا مجموعه‌ای از دستگاه‌های مرتبط یا متصل به هم است که یک یا چند تا از آنها مطابق یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهد.» به همین ترتیب، هر دستگاهی که تحت شمول این تعریف قرار گیرد، موضوع این بحث و به تبع آن قواعد و ضوابط مربوط خواهد بود. با این حال، بعضی دستگاه‌ها هستند که از لحاظ مفهومی با این تعریف هم خوانی دارند، ولی در یکجا ثابت نیستند تا بتوان به طور

مشخص یک محل را به آنها منتسب کرد. نمونه بارز آنها ماهواره‌ها هستند. بدیهی است این مصنوعات نیز در ارتکاب جرائم سایبر نقش آفرین هستند. حتی مبالغه نیست که در هر لحظه هزارن جرم سایبری از طریق آنها ارتکاب می‌یابد. مشکلی که در خصوص این مصنوعات وجود دارد این است که هیچ گاه در یک نقطه ثابت نیستند و به طور مداوم به دور زمین می‌گردند. لذا هیچگاه نمی‌توان به آنها در قالب صلاحیت سرزمینی استناد کرد. البته گروهی از جمله نویسندگان پیش‌نویس کنوانسیون بوداپست معتقدند مشکلی پیش نمی‌آید زیرا می‌توان مراجع قضایی کشور ثبت‌کننده ماهواره را صالح به رسیدگی دانست. همچنین هیچ داده‌ای بر روی ماهواره باقی نمی‌ماند و بالاخره به زمین باز می‌گردد که در این صورت، می‌توان با تمسک به دیگر قواعد، نسبت به محل برخورد یا حتی محل ارسال آنها تصمیم‌گیری کرد. (جلالی فراهانی، امیرحسین، درآمدی بر آیین دادرسی کیفری جرائم سایبر، چ ۱، صص ۶۹-۶۸)

Explanatory Report To The Convention On Cyber Crime; Para 234

■ ۴- سامانه‌های رایانه‌ای و مخابراتی در برخی موارد، وسیله ارتکاب جرم بوده و گاهی به عنوان موضوع جرم مطرح می‌شوند؛ لیکن در صورتی که هر دو مورد توسط یک فرد انجام شود، مقررات تعدد جرم حاکم خواهد بود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۱۷)

■ ۵- دیدگاه‌های حقوقدانان در مورد اصطلاح «تدابیر امنیتی»:

۱- منظور از آن، کلیه اقدامات سخت‌افزاری یا نرم‌افزاری است که تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را از نظر فنی ایمن و مصون از تعرض می‌نماید. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

۲- منظور از آن، ایجاد محدودیت یا ممنوعیت دسترسی به داده‌ها و اطلاعات برای افراد غیرمجاز با توجه به طبقه‌بندی و ارزش محتویات آنها است. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۱۴)

■ ۶- واژه «دسترسی» فاقد معنای خاص حقوقی است پس باید به عرف خاص یعنی متخصصان علوم رایانه‌ای مراجعه کرد و از دیدگاه ایشان، دسترسی به معنای عملیات در اختیار قرار گرفتن یا کنترل یا نظارت می‌باشد. جرم دسترسی نیاز به وسیله یا اقدام خاصی ندارد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

■ ۷- «دسترسی غیرمجاز»، به معنای دستیابی بدون مجوز (غیرقانونی) به محتوای ذخیره شده یا در حال پردازش در یک یا چند سامانه رایانه، مخابراتی یا شبکه‌ای می‌باشد؛ این محتوا می‌تواند شامل طیف متفاوت و گسترده‌ای از داده‌های رایانه‌ای در قالب فایل‌هایی با پسوندهای مختلف باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۱۳)

■ ۸- در مورد رابطه واژه «هک کردن» و «دسترسی غیرمجاز» اختلاف نظر وجود دارد. در حالی که غالباً مترادف به حساب می‌آیند اما کارشناسان، این واژه را که بیش‌تر در عرف کارشناسان به کار می‌رود خاص‌تر از دسترسی

غیرمجاز می‌دانند. هک کردن نیز به معنای حمله به سامانه‌ها می‌باشد اما معنای اصلی آن، نفوذ کردن است که فقط به سامانه‌های رایانه‌ای صورت می‌گیرد و همراه با اعمالی همچون تجزیه و تحلیل و مداخله در پردازش می‌باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

■ ۹- فلسفه جرم انگاری دسترسی غیرمجاز، حمایت از محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی است زیرا اشخاص نسبت به داده‌های متعلق به خود این حق را دارند که آنها مصون از افشا، کسب اطلاع، مداخله، بررسی، تجزیه و تحلیل، رویت و غیره بمانند. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

■ ۱۰- دسترسی غیرمجاز، نیازمند داشتن دانش بالا در زمینه علوم «رایانه» و «مخابرات» می‌باشد؛ لذا افرادی که در این زمینه تبحر داشته و امکانات فنی (سخت افزاری و نرم افزاری) و مالی لازم را در اختیار دارند، قادر به ارتکاب این جرم «محرک» (جرم محرک، جرمی است که مجرم را به سمت و سوی ارتکاب جرم خای دیگر، سوق می‌دهد. دلیل این تحریک مختلف است و می‌تواند منشا بیرونی یا درونی داشته باشد) و «مادر» (جرم مادر، جرمی است که جرم‌های دیگر را به دنبال دارد و درواقع، زاینده جرم‌های دیگر است) می‌باشند. مرتکب جرم دسترسی غیرمجاز، شخص حقیقی و حقوقی می‌باشد لیکن تعیین مجازات شخص حقوقی از طریق حکم این ماده صورت نمی‌پذیرد. زیرا در فصل ششم از بخش اول ق.ج.ر به اشخاص حقوقی و مسئولیت کیفری ایشان اشاره شده است. (البته نظر مخالفی نیز در این زمینه ابراز شده است. یکی از حقوقدانان در اظهارنظری مخالف بیان می‌دارد: «مرتکب جرم دسترسی غیرمجاز فقط اشخاص حقیقی میباشند. از این رو قانونگذار به عمد از واژه «شخص» که در علم حقوق هم در مورد اشخاص حقیقی و هم حقوقی استعمال می‌شود استفاده نکرده و به جای آن از واژه «هر کس» استفاده نموده است. بنابراین، هر فرد ایرانی یا خارجی، زن و مرد، ادارای یا دارای شغل آزاد، نظامی یا غیرنظامی می‌توانند از مرتکبان این جرم باشند.» غلام عباسی، ترکی، نگرش علمی و کاربردی به ق.ج.ر (قسمت دوم)، ماهنامه دادرسی، ش ۷۸، سال ۱۳، بهمن و اسفند ۱۳۸۸، ص ۱۴) همچنین مواد ۲۰ تا ۲۲ ل.م.ا نیز به این امر اختصاص یافته است. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۱۸)

■ ۱۱- دسترسی غیرمجاز، جرم مطلق است یعنی صرف دسترسی کفایت نمی‌کند و لازم نیست داده‌ها، مورد سوءاستفاده نیز قرار گیرد. دلیل مطلق انگاشتن جرم، آن است که دسترسی غیرمجاز زمینه تحقق جرائم دیگر مانند افشاء و ربودن را فراهم می‌سازد و در حقیقت، مقدمه و زمینه ارتکاب جرائم دیگر است. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

■ ۱۲- جرم دسترسی غیرمجاز و بسیاری از جرائم رایانه‌ای جزو جرائم فنی و تخصصی هستند که اصطلاحاً «جرم یقه سفیدها» نامیده می‌شوند. از همین روی مرتکب جرم باید فردی آگاه و متخصص باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

■ ۱۳- دسترسی غیرمجاز ممکن است منتهی به ربودن یا افشاء جرائم دیگر شود. در این

خصوص باید به مقررات عمومی عمل نمود یعنی مقدمه منطقی یک جرم، جرم جداگانه محسوب نمی‌شود. ممکن است گفته شود در اینجا مقررات تعدد معنوی جرم اجرا می‌شود اما باید توجه داشت که تعدد معنوی منصرف از مواردی است که یک جرم مانند ورود غیرقانونی به منزل دیگری، مقدمه منطقی جرم دیگری مانند سرقت می‌باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

■ ۱۴- دسترسی غیرمجاز، جرمی «مستمر»، «عمدی» و «مطلق» محسوب می‌شود و مقید به هیچ نتیجه خاصی نمی‌باشد؛ لذا نیاز به هیچ قصد خاصی نداشته و برای تحقق رکن روانی آن، سوءنیت عام کفایت می‌کند و مرتکب باید از روی علم و عمد، دسترسی غیرمجاز را انجام دهد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۳)

■ ۱۵- تحقق جرم دسترسی غیرمجاز در این ماده، به سامانه‌های امن و نیز نقض تدابیر ایمنی مقید شده و سامانه‌های غیر ایمن و نیز دسترسی بدون نقض تدابیر ایمنی، از شمول ماده ۱ بیرون هستند که این یک خلأ قانونی جدی محسوب می‌شود. (این به مثابه آن است که سارق در جرم ورود به منزل غیر به قصد سرقت، به بهانه باز بودن درب منزل عمل خود را توجیه نماید.) از طرف دیگر تاکنون، ملاک و معیار مشخصی برای تعیین ایمنی (امنیت) و یا ناامنی برای یک سامانه یا شبکه یارانه‌ای یا مخابراتی ارائه نشده و عموماً این گونه موارد، سلیقه‌ای است؛ به طوری که از نگاه عده‌ای با نصب یک نرم افزار امنیتی و یا دیوار آتشین (Firewall)، سامانه یا شبکه، ایمن محسوب می‌شود اما به نظر برخی دیگر از متخصصان حرفه‌ای، چنین سامانه‌هایی از امنیت مطلوبی برخوردار نیستند و لازم است تجهیزات نرم افزاری و سخت افزاری خاصی بر روی آنها نصب گردد. بهتر است عرف متعارف که بر اساس ضابطه نوعی (عینی) تعیین می‌شود را مورد نظر قرار داد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۱۴)

■ ۱۶- جرم دسترسی غیرمجاز می‌تواند به عنوان جزیی از عنصر مادی جرایم مهمتر به کار رود؛ آن گاه فقط جرمی مستقل نخواهد بود؛ بلکه قسمتی از جرمی مهمتر می‌باشد. اگر قانونگذار در یک تبصره، در مورد مجازات این گونه جرایم و همچنین موارد تعدد جرم، تعیین تکلیف می‌نمود، موجب رفع سوء تعبیرهای احتمالی می‌شد (ر.ک به: عالی پور، حسن، حقوق کیفری فناوری اطلاعات، چ ۱، صص ۱۷۱-۱۶۸، انتشارات خرسندی، ۱۳۹۰) لیکن از آنجا که ق.ج.ر به عنوان فصلی مستقل از ق.م.ا تعیین شده است، راجع به این موضوع بایستی به ق.م.ا مراجعه نمود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، صص ۱۵-۱۴)

■ ۱۷- دسترسی غیرعمدی رافع مسئولیت کیفری است اما رافع مسئولیت مدنی نمی‌باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۳)

■ ۱۸- با توجه به عدم جرم انگاری دسترسی غیرمجاز در ق.م.ج.ن.م مصوب ۱۳۸۲ اگر فرد نظامی به مناسبت انجام وظایف محوله، مرتکب جرم دسترسی غیرمجاز شود، دادگاه نظامی مکلف است با استناد به ماده ۱ ق.ج.ر (ماده ۷۲۹ ق.م.ا) حکم لازم را صادر نماید. (الهی

منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۱۹)

■ ۱۹- کسانی که عملیات دسترسی غیرمجاز توسط آنان انجام نمی‌گیرد ولی بسترهای دسترسی غیرمجاز را از طریق «فروش»، «انتشار»، «آموزش» و.. فراهم می‌سازند، مطابق بندهای (ب) و (ج) ماده ۲۵ ق.ج.ر (ماده ۷۵۳ ق.م.ا) مجازات خواهند شد. (ترکی، نگرش علمی و کاربردی به ق.ج.ر (قسمت دوم)، ماهنامه دادرسی، ش ۷۸، سال ۱۳، بهمن و اسفند ۱۳۸۸، ص ۱۵. شرح و نقل از: الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۷. ر.ک به: پاورقی ۲ ص ۱۹)

■ ۲۰- برای تحقق جرم دسترسی غیرمجاز، رفتار مرتکب باید به صورت فعل مثبت باشد؛ لذا با ترک فعل نمی‌توان وقوع این جرم را محرز دانست. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۲)

■ ۲۱- اگر کسی اطلاعات سری یا محرمانه دولتی را از شبکه‌های رایانه‌ای و یا رایانه شخصی متلعق به دیگری برباید و رمز آنها را کشف نماید وفق مقررات ماده یک ق.ج.ر با مرتکب رفتار خواهد شد. (شامبیانی، هوشنگ، جرائم علیه اموال و مالکیّت، چ ۱، ص ۴۶)

■ ۲۲- اصل بر مجاز بودن دسترسی به داده‌هاست، بنابراین جرائم رایانه‌ای هم تابع اصل قانونی بودن جرائم و مجازات‌ها هستند. پس عملی جرم است که در قانون برای آن مجازات تعیین شده باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۴)

■ ۲۳- مجازات این جرم را باید وفق ق.م.ا مصوب ۱۳۹۲/۰۲/۰۱، از نوع درجه ششم دانست؛ لذا وفق ماده ۶۲ قانون اخیر، «در جرائم تعزیری از درجه پنج تا درجه هشت، دادگاه می‌تواند در صورت وجود شرایط مقرّر در تعویق مراقبتی، محکوم به حبس را با رضایت وی در محدوده مکانی مشخص تحت نظارت سامانه (سیستم)های الکترونیکی قرار دهد.»

■ ۲۴- مستفاد از بند (ت) ماده ۱۰۵ ق.م.ا مصوب ۱۳۹۲/۰۲/۰۱، مرور زمان تعقیب این جرم به واسطه درجه شش بودن، در صورتی تعقیب جرائم موجب تعزیر را موقوف می‌کند که از تاریخ وقوع جرم تا انقضای مواعد زیر تعقیب نشده یا از تاریخ آخرین اقدام تعقیبی یا تحقیقی تا انقضای این مواعد به صدور حکم قطعی منتهی نگردیده باشد، با انقضای پنج سال محقّق می‌گردد.

■ ۲۵- مستفاد از بند (ت) ماده ۱۰۷ ق.م.ا مصوب ۱۳۹۲/۰۲/۰۱، مرور زمان اجرای احکام قطعی راجع به ماده ۱ ق.ج.ر که این جرم تعزیری را موقوف می‌کند، به واسطه درجه ۶ بودن آن با انقضای مدت ۷ سال از تاریخ قطعیت حکم مزبور محقّق می‌گردد.

■ ۲۶- سامانه‌های رایانه‌ای و مخابراتی در برخی موارد، وسیله ارتکاب جرم بوده و گاهی به عنوان موضوع جرم مطرح می‌شوند؛ لیکن در صورتی که هر دو مورد توسط یک فرد انجام شود، مقررات تعدد جرم حاکم خواهد بود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۱۷)

■ ۲۷- نظریه ۷/۹۳/۶۵۶-۱۳۹۳/۳/۲۴ ا.ح.ق.ق: س: اگر فردی از طریق فیزیکی رمز ورودی به ایمیل شخصی را بدست آورد با فریب یا سوءاستفاده از اعتماد صاحب ایمیل آیا مشمول ماده ۱ ق.ج.ر می‌شود؟

ج: در فرض سؤال صرف به دست آوردن رمز ورودی به ایمیل اشخاص جرم نیست ولی چنانچه از طریق رمزی که به دست آورده، به طور غیرمجاز به داده یا سامانه دسترسی پیدا کند، می‌تواند از مصادیق جرم موضوع ماده ۱ ق.ج.ر باشد. به هر حال تشخیص مصداق با قاضی رسیدگی کننده است.

■ ۲۸- نظریه ۷/۹۳/۶۵۶-۱۳۹۳/۳/۲۴ ا.ح.ق.ق:

س: در ماده ۱ ق.ج.ر اشاره دارد به دسترسی غیرمجاز به داده‌ها. حال، منظور از دسترسی غیرمجاز چیست؟ و این دسترسی به صورت مجازی را از طریق رهگذر سامانه‌های رایانه‌ای می‌باشد یا می‌تواند از طریق فیزیکی و اسنادی نیز صورت پذیرد توضیحا اینکه برخی از همکاران معتقدند که دسترسی غیرمجاز با توجه به فصل یکم ق.ج.ر تحت عنوان جرائم علیه محرمانگی و داده‌ها و سیستم‌های رایانه‌ای و مخابراتی تنها از طریق دانش فنی و نرم‌افزاری و از طریق کنش روی داده‌ها در محیط مجازی می‌باشد.

ج: با توجه به اطلاق ماده ۱ ق.ج.ر، صرف دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده باشد مشمول مقررات ماده مذکور می‌باشد و طریق دسترسی اعم از مستقیم (فیزیکی) یا با واسطه (از طریق شبکه) تأثیری در قضیه ندارد.

■ ۲۹- قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷/۱۱/۱۶:

فصل اول- تعاریف و کلیات

بند اول- تعاریف:

ماده ۱- در این قانون اصطلاحات زیر در معانی مشروح مربوط به کار می‌رود:

الف- اطلاعات: هر نوع داده که در اسناد مندرج باشد یا به صورت نرم‌افزاری ذخیره گردیده و یا با هر وسیلهٔ دیگری ضبط شده باشد.

ب- اطلاعات شخصی: اطلاعات فردی نظیر نام و نام خانوادگی، نشانیهای محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادتهای فردی، ناراحتیهای جسمی، شماره حساب بانکی و رمز عبور است.

ج- اطلاعات عمومی: اطلاعات غیرشخصی نظیر ضوابط و آیین‌نامه‌ها، آمار و ارقام ملی و رسمی، اسناد و مکاتبات اداری که از مصادیق «مستثنیات» فصل چهارم این قانون نباشد.

د- مؤسّسات عمومی: سازمانها و نهادهای وابسته به حکومت به معنای عام کلمه شامل تمام ارکان و اجزاء آن که در مجموعه قوانین جمهوری اسلامی ایران آمده است.

هـ- مؤسّسات خصوصی: از نظر این قانون، مؤسّسه خصوصی شامل هر مؤسّسه انتفاعی و غیرانتفاعی به استثناء مؤسّسات عمومی است.

بند دوم- آزادی اطلاعات:

ماده ۲- هر شخص ایرانی حق دسترسی به اطلاعات عمومی را دارد، مگر آن که قانون منع کرده باشد.

استفاده از اطلاعات عمومی یا انتشار آنها تابع قوانین و مقررات مربوط خواهد بود.

ماده ۳- هر شخصی حق دارد از انتشار یا پخش اطلاعاتی که به وسیله او تهیه شده ولی در جریان آماده سازی آن برای انتشار تغییریافته است جلوگیری کند، مشروط به آن که اطلاعات مزبور به سفارش دیگری تهیه نشده باشد که در این صورت تابع قرارداد بین آنها خواهد بود.

ماده ۴- اجبار تهیه کنندگان و اشاعه دهندگان اطلاعات به افشاء منابع اطلاعات خود ممنوع

است مگر به حکم مقام صالح قضائی و البته این امر نافی مسئولیت تهیه کنندگان و اشاعه دهندگان اطلاعات نمی‌باشد.

بند سوم- حق دسترسی به اطلاعات:

ماده ۵- مؤسّسات عمومی مکلفند اطلاعات موضوع این قانون را در حداقل زمان ممکن و بدون تبعیض در دسترسی مردم قرار دهند.

تبصره- اطلاعاتی که متضمن حق و تکلیف برای مردم است باید علاوه بر موارد قانونی موجود از طریق انتشار و اعلان عمومی و رسانه‌های همگانی به آگاهی مردم برسد.

فصل دوم- آیین دسترسی به اطلاعات

بند اول- درخواست دسترسی به اطلاعات و مهلت پاسخگویی به آن

ماده ۶- درخواست دسترسی به اطلاعات شخصی تنها از اشخاص حقیقی که اطلاعات به آنها مربوط می‌گردد یا نماینده قانونی آنان پذیرفته می‌شود.

ماده ۷- مؤسّسه عمومی نمی‌تواند از متقاضی دسترسی به اطلاعات هیچ گونه دلیل یا توجیهی جهت تقاضایش مطالبه کند.

ماده ۸- مؤسّسه عمومی یا خصوصی باید به درخواست دسترسی به اطلاعات در سریعترین زمان ممکن پاسخ دهد و در هر صورت مدت زمان پاسخ نمی‌تواند حداکثر بیش از ده روز از زمان دریافت درخواست باشد. آیین‌نامه اجرائی این ماده ظرف مدت شش ماه از تاریخ تصویب این قانون بنا به پیشنهاد کمیسیون انتشار و دسترسی آزاد به اطلاعات، به تصویب هیأت وزیران می‌رسد.

بند دوم- نحوه پاسخ به درخواستها:

ماده ۹- پاسخی که توسط مؤسّسات خصوصی به درخواستهای دسترسی به اطلاعات داده می‌شود باید به صورت کتبی یا الکترونیکی باشد.

فصل سوم- ترویج شفافیت

بند اول- تکلیف به انتشار

ماده ۱۰- هر یک از مؤسّسات عمومی باید جز در مواردی که اطلاعات دارای طبقه‌بندی می‌باشد، در راستای نفع عمومی و حقوق شهروندی دست کم به طور سالانه اطلاعات عمومی شامل عملکرد و ترازنامه (بیلان) خود را با استفاده از امکانات رایانه‌ای و حتی الامکان در یک کتاب راهنما که از جمله می‌تواند شامل موارد زیر باشد منتشر سازد و در صورت درخواست شهروند با اخذ هزینه تحویل دهد:

الف- اهداف، وظایف، سیاستها و خطی مشی‌ها و ساختار.

ب- روشها و مراحل اتمام خدماتی که مستقیماً به اعضاء جامعه ارائه می‌دهد.

ج- ساز و کارهای شکایت شهروندان از تصمیمات یا اقدامات آن مؤسّسه.

د- انواع و اشکال اطلاعاتی که در آن مؤسّسه نگهداری می‌شود و آیین دسترسی به آنها.

هـ- اختیارات و وظایف مأموران ارشد خود.

و- تمام ساز و کارها یا آیین‌هایی که به وسیله آنها اشخاص حقیقی و حقوقی و سازمانهای غیردولتی می‌تواند در اجراء اختیارات آن واحد مشارکت داشته یا به نحو دیگری مؤثر واقع شوند.

تبصره- حکم این ماده در مورد دستگاههایی که زیر نظر مستقیم مقام معظم رهبری است، منوط به عدم مخالفت معظم له می‌باشد.

ماده ۱۱- مصوبه و تصمیمی که موجد حق یا تکلیف عمومی است قابل طبقه‌بندی به عنوان

اسرار دولتی نمی‌باشد و انتشار آنها الزامی خواهد بود.
بند دوم- گزارش واحد اطلاع رسانی به کمیسیون انتشار و دسترسی آزاد به اطلاعات
ماده ۱۲- مؤسّسات عمومی موظفند از طریق واحد اطلاع رسانی سالانه گزارشی درباره فعالیتهای آن مؤسّسه در اجراء این قانون به کمیسیون انتشار و دسترسی آزاد به اطلاعات ارائه دهند.
فصل چهارم- استثنائات دسترسی به اطلاعات
بند اول- اسرار دولتی
ماده ۱۳- در صورتی که درخواست متقاضی به اسناد و اطلاعات طبقه‌بندی شده (اسرار دولتی) مربوط باشد مؤسّسات عمومی باید از در اختیار قرار دادن آنها امتناع کنند. دسترسی به اطلاعات طبقه‌بندی شده تابع قوانین و مقررات خاص خود خواهد بود.
بند دوم- حمایت از حریم خصوصی:
ماده ۱۴- چنانچه اطلاعات درخواست شده مربوط به حریم خصوصی اشخاص باشد و یا در زمره اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود.
ماده ۱۵- مؤسّسات مشمول این قانون درصورتی که پذیرش درخواست متقاضی متضمن افشای غیرقانونی اطلاعات شخصی درباره یک شخص حقیقی ثالث باشد باید از در اختیار قرار دادن اطلاعات درخواست شده خودداری کنند، مگر آن که:
الف- شخص ثالث به نحو صریح و مکتوب به افشاء اطلاعات راجع به خود رضایت داده باشد.
ب- شخص متقاضی، ولی یا قیم یا وکیل شخص ثالث، در حدود اختیارات خود باشد.
ج- متقاضی یکی از مؤسّسات عمومی باشد و اطلاعات درخواست شده در چهارچوب قانون مستقیماً به وظایف آن به عنوان یک مؤسّسه عمومی مرتبط باشد.
بند سوم- حمایت از سلامتی و اطلاعات تجاری:
ماده ۱۶- در صورتی که برای مؤسّسات مشمول این قانون با مستندات قانونی محرز باشد که در اختیار قرار دادن اطلاعات درخواست شده، جان یا سلامت افراد را به مخاطره می‌اندازد یا متضمن ورود خسارت مالی یا تجاری برای آنها باشد، باید از در اختیار قرار دادن اطلاعات امتناع کنند.
بند چهارم- سایر موارد:
ماده ۱۷- مؤسّسات مشمول این قانون مکلفند در مواردی که ارائه اطلاعات درخواست شده به امور زیر لطمه وارد می‌نماید از دادن آنها خودداری کنند.
الف- امنیت و آسایش عمومی.
ب- پیشگیری از جرائم یا کشف آنها، بازداشت یا تعقیب مجرمان.
ج- ممیزی مالیات یا عوارض قانونی یا وصول آنها.
د- اعمال نظارت بر مهاجرت به کشور.
تبصره ۱- موضوع مواد (۱۳) الی (۱۷) شامل اطلاعات راجع به وجود یا بروز خطرات زیست محیطی و تهدید سلامت عمومی نمی‌گردد.
تبصره ۲- موضوع مواد (۱۵) و (۱۶) شامل اطلاعاتی که موجب هتک عرض و حیثیت افراد یا مغایر عفت عمومی و یا اشاعه فحشاء می‌شود، نمی‌گردد.
فصل پنجم- کمیسیون انتشار و دسترسی آزاد به اطلاعات
بند اول- تشکیل کمیسیون:

ماده ۱۸- به منظور حمایت از آزادی اطلاعات و دسترسی همگانی به اطلاعات موجود در مؤسّسات عمومی و مؤسّسات خصوصی که خدمات عمومی ارائه می‌دهند، تدوین برنامه‌های اجرائی لازم در عرصه اطلاع رسانی، نظارت کلی بر حسن اجراء، رفع اختلاف در چگونگی ارائه اطلاعات موضوع این قانون از طریق ایجاد وحدت رویه، فرهنگسازی، ارشاد و ارائه نظرات مشورتی، کمیسیون انتشار و دسترسی آزاد به اطلاعات به دستور رئیس جمهور با ترکیب زیر تشکیل می‌شود:

الف- وزیر فرهنگ و ارشاد اسلامی (رئیس کمیسیون)

ب- وزیر ارتباطات و فناوری اطلاعات یا معاون ذی‌ربط.

ج- وزیر اطلاعات یا معاون ذی‌ربط.

د- وزیر دفاع و پشتیبانی نیروهای مسلح یا معاون ذی‌ربط.

هـ- رئیس سازمان مدیریت و برنامه ریزی کشور یا معاون ذی‌ربط.

و- رئیس دیوان عدالت اداری.

ز- رئیس کمیسیون فرهنگی مجلس شورای اسلامی.

ح- دبیر شورای عالی فناوری اطلاعات کشور.

تبصره ۱- دبیرخانه کمیسیون یادشده در وزارت فرهنگ و ارشاد اسلامی تشکیل می‌گردد. نحوه تشکیل جلسات و اداره آن و وظایف دبیرخانه به پیشنهاد کمیسیون مذکور به تصویب هیأت وزیران خواهد رسید.

تبصره ۲- مصوبات کمیسیون انتشار و دسترسی آزاد به اطلاعات پس از تأیید رئیس جمهور لازم الاجراء خواهد بود.

ماده ۱۹- مؤسّسات ذی‌ربط ملزم به همکاری با کمیسیون می‌باشند.

بند دوم- گزارش کمیسیون:

ماده ۲۰- کمیسیون باید هر ساله گزارشی در باره رعایت این قانون در مؤسّسات مشمول این قانون و فعالیتهای خود را به مجلس شورای اسلامی و رئیس جمهور تقدیم کند.

فصل ششم- مسئولیتهای مدنی و کیفری

ماده ۲۱- هر شخصی اعم از حقیقی یا حقوقی که در نتیجه انتشار اطلاعات غیرواقعی درباره او به منافع مادی و معنوی وی صدمه وارد شده است حق دارد تا اطلاعات مذکور را تکذیب کند یا توضیحاتی درباره آنها ارائه دهد و مطابق با قواعد عمومی مسئولیت مدنی جبران خسارتهای وارد شده را مطالبه نماید.

تبصره- در صورت انتشار اطلاعات واقعی بر خلاف مفاد این قانون، اشخاص حقیقی و حقوقی حق دارند که مطابق قواعد عمومی مسئولیتهای مدنی، جبران خسارتهای وارد شده را مطالبه نمایند.

ماده ۲۲- ارتکاب عمدی اعمال زیر جرم می‌باشد و مرتکب به پرداخت جزاء نقدی از سیصدهزار ریال تا یکصد میلیون ریال با توجه به میزان تأثیر، دفعات ارتکاب جرم و وضعیت وی محکوم خواهد شد:

الف- ممانعت از دسترسی به اطلاعات برخلاف مقررات این قانون.

ب- هر فعل یا ترک فعلی که مانع انجام وظیفه کمیسیون انتشار و دسترسی آزاد به اطلاعات یا وظیفه اطلاع رسانی مؤسّسات عمومی برخلاف مقررات این قانون شود.

ج- امحاء جزئی یا کلی اطلاعات بدون داشتن اختیار قانونی.

د- عدم رعایت مقررات این قانون در خصوص مهلتهای مقرر.
چنانچه هر یک از جرائم یادشده در قوانین دیگر مستلزم مجازات بیشتری باشد همان مجازات اعمال می‌شود.
ماده ۲۳- آیین‌نامه اجرائی این قانون حداکثر ظرف سه ماه از تاریخ تصویب، توسط وزارت فرهنگ و ارشاد اسلامی و با همکاری دستگاههای ذی‌ربط تهیه و به تصویب هیأت وزیران خواهد رسید.
■ ۳۰- آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات:
ماده ۱- اصطلاحات زیر در این آیین‌نامه در معانی مشروح مربوط به کار می‌روند:
الف- اطلاعات: هر نوع داده از جمله صوت، تصویر، فیلم، نوشته، نشانه، نقشه، اعداد و یا ترکیبی از آنها که در اسناد مندرج باشد یا به صورت نرم‌افزاری ذخیره گردیده و یا با هر وسیله دیگری ضبط شده باشد.
ب- اطلاعات شخصی: اطلاعات مربوط به هویت، احوال شخصی، وضعیت فردی، عقاید و باورها، پست الکترونیکی، عکس و فیلم و صوت و تصویر و عادات رفتاری و فردی از قبیل نام و نام خانوادگی، محل و تاریخ تولد، ازدواج، طلاق، مشخصات همسر، والدین و فرزندان، نسبت خانوادگی، ناراحتی‌های جسمی و روحی، شماره حساب بانکی و رمز عبور، محل کار و سکونت و همچنین اطلاعات شخصی مربوط به انجام امور تجاری، شغلی، تحصیلی، مالی، آموزشی، اداری، پزشکی و حقوقی.
پ- حریم خصوصی: قلمروی از زندگی شخصی فرد که انتظار دارد دیگران بدون رضایت یا اعلام قبلی وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، وارد شدن، نظاره کردن، شنود و دسترسی اطلاعات فرد از طریق رایانه، تلفن همراه، نامه، منزل مسکونی، خودرو و آن قسمت از مکان‌های اجاره شده خصوصی نظیر هتل و کشتی، همچنین آنچه که حسب قانون فعالیت حرفه‌ای خصوصی هر شخص حقیقی و حقوقی محسوب می‌شود؛ از قبیل اسناد تجاری و اختراعات و اکتشافات.
ت- اطلاعات طبقه‌بندی شده (اسرار دولتی): اسناد سری و محرمانه دولتی موضوع قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳ و آیین‌نامه اجرایی آن مصوب ۱۳۵۴.
ث- قانون: قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۸.
ج- نشر اطلاعات: قرار دادن اطلاعات در معرض دسترسی عموم.
چ- مؤسّسات خصوصی: اشخاص حقوقی که با تجویز قانون یا به موجب قانون خاص تأسیس شده یا می‌شوند و دارای فعالیت انتفاعی یا غیرانتفاعی می‌باشند؛ از قبیل شرکت‌ها، مؤسّسات غیرتجاری، احزاب و سازمان‌های مردم نهاد.
ح- مؤسّسات عمومی: سازمان‌ها و نهادهای وابسته به حکومت به معنای عام آن شامل دستگاه‌های اجرایی موضوع ماده ۵ قانون مدیریت خدمات کشوری، نهادهای انقلابی، نیروهای مسلح، قوای قضائیه و مقننه و مؤسّسات، شرکت‌ها، سازمان‌ها، نهادهای وابسته به آنها و بنیادها و مؤسّساتی که زیر نظر مقام معظم رهبری اداره می‌شوند با رعایت تبصره ذیل ماده (۱۰) قانون و همچنین هر مؤسّسه، شرکت یا نهادی که تمام یا بیش از پنجاه درصد

سهام آن متعلق به دولت یا حکومت که در مجموعه قوانین جمهوری اسلامی ایران آمده است.

خ- مؤسّسات خصوصی ارایه دهنده خدمت عمومی: آن دسته از مؤسّسات غیردولتی که اقدام به ارایه خدمات عمومی به مردم می‌کنند، از قبیل سازمان‌های صنفی و حرفه ای، بانک‌ها و بورس اوراق بهادار.

د- کمیسیون: کمیسیون ماده ۱۸ قانون.

ذ- مؤسّسات مشمول قانون: مؤسّسات خصوصی، عمومی و خصوصی ارایه دهنده خدمات عمومی.

ر- درگاه: شامل پرتال، وب سایت، وب گاه یا رسانه بر خط مؤسّسات مشمول قانون.

ماده ۲- مؤسّسات مشمول قانون موظفند ذخایر اطلاعاتی مذکور در ماده ۷ این آیین‌نامه را از سال اول ابلاغ این تصویبنامه به تدریج طی سه سال به صورت رقومی تبدیل و با رعایت قوانین و مقررات مربوط در دسترس کاربران در سطوح مختلف قرار دهند.

ماده ۳- مؤسّسات مشمول قانون موظفند عناوین اطلاعات عمومی و غیرطبقه‌بندی شده خود و شیوه دسترسی به آنها را در درگاه خود قرار دهند.

تبصره- مؤسّسات مشمول قانون باید کاربرگ (فرم) الکترونیکی و نسخه قابل چاپ درخواست اطلاعات را در درگاه خود قرار دهند. پس از پر نمودن و ارسال نمودن و ارسال کاربرگ به مؤسّسه، شماره پیگیری در اختیار متقاضی قرار می‌گیرد تا از وضعیت درخواست خود مطلع شود.

ماده ۴- مؤسّسات مشمول قانون موظفند از طریق درگاه خود یک امکان ارتباطی امن و قانونی برای انجام رویه‌های اداری برقرار کنند تا کاربران بتوانند با استفاده از ابزارهای دسترسی و ارتباطی نظیر تلفن، رایانه یا تلفن همراه خود با مؤسّسه مربوط ارتباط برقرار کنند.

به دست آوردن اطلاعات و با ارایه اسناد و مدارک کاغذی، دریافت یا پر کردن کاربرگ‌های اداری آن نباید منوط به مراجعه حضوری شهروندان و صاحبان مشاغل به مؤسّسات مشمول قانون باشد.

تبصره- در صورت تأمین زیر ساخت کلید عمومی، امضای این اسناد نیازمند مراجعه حضوری نیست.

ماده ۵- مؤسّساتی که متقاضیان زیادی برای دریافت اطلاعات عمومی دارند، می‌توانند با رعایت سطوح دسترسی جهت ارایه نسخ کاغذی یا الکترونیکی اطلاعات، این خدمات را با نظارت کامل و ایجاد شیوه ارزیابی رضایت‌مندی مردم با رعایت مقررات مربوط و سطوح دسترسی، برون‌سپاری نمایند. داده ترافیک دسترسی به این اطلاعات باید تا شش ماه نگهداری شود.

ماده ۶- مؤسّسات مشمول قانون موظفند گزارش آماری انتشار اطلاعات و عملکرد دسترسی به اطلاعات مشتمل بر موارد زیر را اعلام کنند:

الف- آمار درخواست‌های اطلاعات و تعداد پاسخ داده شده و رد شده.

ب- متوسط حجم اطلاعات ارایه شده و زمان ارایه اطلاعات برای هر عنوان اطلاعات.

پ- گزارش آمار اطلاعات منتشر شده و میزان بازدید از آن.

ماده ۷- مؤسّسات مشمول قانون موظفند اطلاعات زیر را در درگاه خود بر اساس ضوابط و استانداردهای مندرج در تصویبنامه شماره ۱۹۲۶۳۰/ت۴۲۶۳۵ ک مورخ ۱۳۹۱/۱۰/۳

طراحی، درج و امکان دسترسی بر خط و بیست و چهار ساعته در هفت روز هفته برای مراجعان فراهم نمایند:
الف- شرح وظایف و الزامات قانونی.
ب- قوانین و مقررات حاکم بر فعالیت‌های مؤسّسه.
پ- ساختار سازمانی و وظایف هر پست تا پایین‌ترین سطح سازمانی.
ت- فهرست کلیه مدیران سازمان به همراه تلفن ثابت و رایانامه (ایمیل) سازمانی ایشان.
ث- فهرست و امکان دسترسی به کلیه نهادهای تابعه و بالادست.
ج- صفحه اعلام اعتراض به فعالیت‌های مؤسّسه، واحد تابعه یا کارکنان (ایجاد سامانه دریافت تلفنی یا پیامکی یا رایانامه (ایمیل) داخلی برای اعلام اعتراض ضروری است)
چ- طرح‌های تملک دارایی سرمایه‌ای مؤسّسه به همراه گزارش آخرین وضعیت پیشرفت آنها.
ح- صفحه اعلام نیازمندی‌های مناقصات و مزایده‌ها و اعلام آخرین وضعیت آنها.
خ- شناسنامه کلیه خدمات قابل ارایه مؤسّسه به همراه متولی پاسخگویی هر خدمت.
د- فرآیند ارایه هر خدمت به همراه کلیه نیازمندی‌های مربوط.
ذ- زمان بندی ارایه خدمات و فهرست و شیوه دسترسی به کارکنان پاسخگوی خدمات.
ر- اعلام شیوه‌های ارایه خدمت در صورت برون سپاری از طریق دفاتر پیشخوان خدمات و تعهدات ایشان.
ز- ایجاد صفحه راهنمای پیشخوان و سؤالات مکرری که از مؤسّسه شده و پاسخ‌های مربوط.
ژ- ایجاد صفحه پیگیری خدمت یا درخواست اطلاعات به همراه اطلاعات فرآیند طی شده برای ارایه خدمت.
س- گزارش زمان‌هایی که پیش خوان جهت به روز رسانی یا مسایل فنی از دسترس خارج می‌شود یا شده است.
ش- اطلاعات مربوط به وظایف مؤسّسات عمومی مشمول قانون که مطابق قوانین و مقررات کشور ارایه آن الزامی است.

ماده ۸- ناشران اطلاعات در مورد صحت اطلاعاتی که از مؤسّسات موضوع قانون در اختیار آنها گذاشته شده و انتشار آنها منع قانونی ندارد، در صورت منتشر نمودن عین اطلاعات مسئولیتی نخواهند داشت.

ماده ۹- مؤسّسات مشمول قانون موظفند اطلاعاتی را که بر اساس قانون ملزم به انتشار آنها هستند، بلافاصله در درگاه خود درج نمایند
تبصره- مؤسّسات مشمول قانون حق انتشار یا ارایه اطلاعات مربوط به حریم خصوصی و سایر موارد منع شده در قانون را ندارند، مگر در مواردی که قوانین و مقررات، انتشار یا ارایه آنها را الزامی اعلام کرده باشد.

ماده ۱۰- مؤسّسات مشمول قانون موظفند نسبت به انتشار اطلاعات دربردارند حقوق و تکالیف مردم از طریق رسانه‌های همگانی اقدام نمایند.

ماده ۱۱- وظایف و مسئولیت‌های مربوط به اجرای قانون و این آیین‌نامه به عهده بالاترین مقام مؤسّسات مشمول قانون می‌باشد.
تبصره- بالاترین مقام مؤسّسات مشمول قانون می‌تواند در چارچوب اختیارات قانونی خود تمام یا بخشی از وظیفه ارایه و انتشار اطلاعات را به اشخاصی دیگر در مؤسّسه تحت امر خود تفویض نماید.

مبحث دوم- شنود غیرمجاز

شنود بدون مجوز محتوای در حال انتقال ارتباطات غیرعمومی

ماده ۲ (ماده ۷۳۰ ق.م.ا)- هر کس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از ۶ ماه تا ۲ سال یا جزای نقدی از ۱۰ میلیون ریال تا ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد.

■ ۳۱- «شنود مجاز»، شنودی است که بر اساس مقررات، شنود مکالمات تلفنی صورت گیرد وگرنه جرم محسوب می‌شود. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۵)

■ ۳۲- «شنود غیرمجاز» را می‌توان «هرگونه دریافت غیرقانونی محتوای در حال انتقال ارتباطات غیرعمومی در بستر فضای تولید و تبادل اطلاعات به طور پنهانی» تعریف نمود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۴)

■ ۳۳- شنود غیرمجاز (همانند دسترسی غیرمجاز) می‌تواند مقدمه و زمینه ساز جرایم سایبری باشد؛ لذا در زمره جرایم «مادر» و «محرک» می‌باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۴)

■ ۳۴- وجه تمایز جرم «شنود غیرمجاز» از جرم «دسترسی غیرمجاز»، موضوع جرم می‌باشد. موضوع جرم دسترسی غیرمجاز، داده‌های ذخیره شده و یا در حال پردازش در سامانه‌های رایانه‌ای یا مخابراتی است که به طور غیرمجاز توسط افراد ناصالح مورد رصد قرار می‌گیرند؛ ولی موضوع جرم شنود غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای و مخابراتی یا امواج الکترومغناطیسی یا نوری می‌باشد و هرگونه کیفیت اضافه بر آن، جرم را با توصیف‌های دیگر همراه کرده و حتی می‌تواند موجب تحقق تعدد جرم باشد. درواقع شنود غیرمجاز هم جرم مستقل و هم جزئی از عنصر مادی جرایم رایانه‌ای است که در مورد اخیر، موجب تشدید مجازات می‌شود. لذا توصیف ماده قانونی حاوی جرم مستقل می‌تواند سنگ بنای طرح‌های تقنینی باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۵)

■ ۳۵- «شنود غیرمجاز محتوای در حال انتقال»، پدیده‌ای خاص است و با «استراق سمع» تفاوت دارد؛ زیرا استراق سمع به صورت شنیداری و در بستر مکالمات تلفنی-مخابراتی صورت می‌گیرد؛ اما عمل شنود تنها در خصوص سیگنال‌ها و امواج مطرح می‌باشد. این سیگنال‌ها و امواج ممکن است به صورت نوری، صوتی و الکترومغناطیسی (رادیویی، مادون قرمز، ماورای بنفش) باشد. هر یک از موارد ذکر شده می‌توانند به صورت آنالوگ و دیجیتال مبادله شوند. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۵)

■ ۳۶- منظور از عبارت «در حال انتقال»، این است که شنود غیرمجاز در سامانه‌ها یا امواج مذکور در طول مسیر انتقال صورت می‌پذیرد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۸)

■ ۳۷- به نظر می‌رسد در این ماده، ایراد ماده ۱ مبنی بر عدم لحاظ تناسب بین اهمیت محتوای شنود شده و مجازات مقرر و همچنین ناچیز بودن مجازات، وجود دارد. مجازات باید بر طبق میزان اهمیت و شدت جرم تعیین شود. در ماده ۱ ق.ج.ر (ماده ۷۲۹ ق.م.ا) برای دسترسی غیرمجاز، مجازات کمتری نسبت به شنود غیرمجاز در نظر گرفته شده؛ در صورتی که دسترسی غیرمجاز جرم سنگین‌تری می‌باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۶)

■ ۳۸- تبصره ماده ۴۸ ق.ج.ر (ماده ۷۷۶ ق.م.ا)، دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده را «در حکم شنود» می‌داند. ابهامی که در اینجا وجود دارد، آن است که شرط تحقق جرم شنود غیرمجاز، «در حال انتقال بودن ارتباطات» است اما با توجه به تبصره ماده ۴۸ ق.ج.ر (ماده ۷۷۶ ق.م.ا) شنود محتوای ذخیره شده یا آماده انتقال نیز مشمول ماده ۲ (ماده ۷۳۰ ق.م.ا) می‌باشد؟ ظاهر قانون اقتضای پاسخ مثبت را دارد. زیرا ظاهر تبصره، حرف تفسیر است پس در حکم شنود دانسته است. امکان دارد گفته شود حرف «و» در تبصره، حرف تفسیر است پس در حکم شنود بودن به معنای لزوم رعایت مقررات شنود می‌باشد نه این که مجازات شنود نیز نسبت به آن اعمال شود. نتیجه این که شرط «در حال انتقال بودن» برای تحقق این جرم، لازم است. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۴)

■ ۳۹- ماده ۴۸ ق.ج.ر (ماده ۷۷۶ ق.م.ا) نیز درباره شنود است منتها در آن مقررات شنود را بیان می‌کند که مانند مقررات شنود مکالمات تلفنی است اما در اینجا شنود غیرمجاز، جرم انگاری شده و مجازات آن تعیین گردیده است. ماده ۴۸ ق.ج.ر (ماده ۷۷۶ ق.م.ا) درباره شنود مجاز و احکان آن است اما ماده ۲ (ماده ۷۳۰ ق.م.ا) درباره شنود غیرمجاز می‌باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۴)

■ ۴۰- قطع داده در حال انتقال مشمول این ماده نیست بلکه اعمالی همچون کنترل، نظارت و مراقبت را شامل می‌شود. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۴)

■ ۴۱- شنود غیرمجاز، جرم وسیله‌ای نیست بلکه از هر راه فنی ممکن است صورت گیرد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۵)

■ ۴۲- در تحقق عنصر معنوی جرم شنود غیرمجاز سوءنیت یا قصد عام (یعنی قصد انجام فعل شنود غیرمجاز محتوای درحال انتقال ارتباطات غیرعمومی سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری) لازم است؛ ولی وقوع آن، نیاز به قصد خاص ندارد. همچنین، انگیزه در پیدایش این جرم از جایگاه خاصی برخوردار نمی‌باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۸)

■ ۴۳- تحقق رکن مادی جرم در این ماده از طریق انجام فعل مثبت است و ترک فعل نمی‌تواند عنصر تشکیل دهنده آن باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۱)

■ ۴۴- در وقوع این جرم (برخلاف جرم دسترسی غیرمجاز) الزامی به حفاظت داده‌ها به وسیله تدابیر امنیتی وجود ندارد و صرف شنود محتوای ارتباطات غیرعمومی، موجب تحقق این جرم می‌شود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۵)

■ ۴۵- ملاک شناسایی عمومی بودن یا نبودن محتوای اطلاعات، محتوای پیام ارسالی و قصد ارسال کننده می‌باشد؛ مثلاً ارسال امواج رادیویی یا تلویزیونی، عمومی است ولی ارسال پیامک (متنی و یا تصویری) میان دو نفر، و نیز امواج و سیگنال‌های حاوی داده‌های ادارات دولتی موجود در سامانه‌های آنها در بستر فضای سایبر، غیرعمومی است. ۹.قانونگذار در جرم‌انگاری شنود غیرمجاز بیشتر به معنای عرفی آن توجه داشته است؛ چرا که برخی از پیام‌ها به گونه‌ای است که پس از دریافت محتوای ارتباطات، حتماً بایستی به وسیله یک سری عملیات به صورت اصلی -که ممکن است متن، تصویر، صدا و غیره باشد- درآید تا قابل کاربرد و شناسایی باشد. لذا، این واژه دارای ابهام است. (ترکی، غلام عباس، نگرش علمی و کاربردی به ق.ج.ر: قسمت دوم، ماهنامه دادرسی، ش ۷۸، سال سیزدهم، ۱۳۸۸، ص ۱۷. شرح و نقل از: الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۲۵)

■ ۴۶- به نظر می‌رسد این نکته در تبصره ۱ دور از نظر نگه داشته شده که احتمال دارد افشای داده‌های غیر سری نیز به امنیت کشور یا منافع ملی لطمه وارد نماید. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۵)

■ ۴۷- ر.ک به: مادتین ۲-۱ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷/۱۱/۶، در ذیل ماده ۱ ق.ج.ر (ماده ۷۲۹ ق.م.ا)

مبحث سوم- جاسوسی رایانه‌ای

حفاظت و طبقه‌بندی داده‌های سری درحال انتقال یا ذخیره شده

ماده ۳ (ماده ۷۳۱ ق.م.ا)- هر کس به طور غیرمجاز نسبت به داده‌های سری درحال 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 ۱ تا ۳ سال یا جزای نقدی از ۲۰ میلیون ریال تا شصت میلیون ریال یا هر دو مجازات.

ب- در دسترس قراردادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج- افشاء یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از ۵ تا ۱۵ سال.

تبصره ۱- داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره ۲- آیین‌نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی 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.

■ ۴۸- نظـــرات مورخـــه ۱۳۸۷/۱۲/۱۴ و ۱۳۸۷/۱۲/۲۱ ش.ن پیرامون پیش‌نـویس اولیـه ماده:

نظر مخالف: در تبصره ۲ ماده مزبـور، مسـئولیت تهیه آیین‌نامه تعیین و تشخیص داده‌های سـری و نحوه طبقه‌بندی و حفاظـت از آنهـا بـه عهـده وزارت اطلاعات با همکاری سایر وزارتخانـه‌هـای ذکر شده سپرده شده است که به نظر می‌رسد با توجه به ماهیت لایحه، می‌بایسـت در صـلاحیت وزیر دادگستری قـرار مـی‌گرفـت؛ چـه آنکـه بـر اساس اصل ۱۶۰ ق.ا، وزیر دادگستری مسئولیت کلیه مسائل مزبور به روابط قوه قضاییه بـا دیگـر قوا را بر عهده دارد.

نظر موافق: نظری ابراز نشد.

■ ۴۹- گرچه در عنـوان مبحـث سـوم، عبـارت «جاسوسی رایانه‌ای» بیان شده است اما در متن ماده ۳ ق.ج.ر (ماده ۷۳۱ ق.م.ا) اشاره‌ای بـه واژه «جاسوسی» نشـده و فقـط چنـد مصـداق آمـده است. این رویـه در ق.م.ا نیـز وجـود دارد امـا در عرف حقوقی، این اعمال را به عنـوان جاسوسـی می‌شناسند. ماده ۵۰۵ ق.م.ا (تعزیـرات) مصـوب ۱۳۷۵ آورده است: «هر کس با هدف بـرهم زدن امنیت کشور به هر وسیله، اطلاعات طبقه‌بنـدی شده را با پوشـش مسـئولین نظـام یـا مـأمورین دولت یا به هر نحو دیگر جمع‌آوری کند چنانچه بخواهد آن را در اختیار دیگران قرار دهد و موفق به انجام آن شود به حبس از دو تا ده سـال و در غیر این صورت به حـبس از یـک تـا پـنج سـال محکوم می‌شود.» در مورد رابطه این ماده و ماده ۳ ق.ج.ر (مـاده ۷۳۱ ق.م.ا) بیـان چنـد مطلـب، ضرورت دارد. عبارت «بـه نحـو دیگـر» در مـاده ۵۰۵ شامل جاسوسی رایانه‌ای نیز میشود اما هـر دو ماده بـه اعتبـار خـود بـاقی هسـتند. مـاده ۳ ق.ج.ر (ماده ۷۳۱ ق.م.ا) اشـارهای بـه اطلاعـات محرمانه و خیلی محرمانه ندارد و از ایـن جهـت اطلاعات مزبور، مشمول جاسوسی رایانه‌ای قـرار نمی‌گیرد زیـرا مـاده ۳ ق.ج.ر (مـاده ۷۳۱ ق.م.ا) فقط به اطلاعات سری و بـه کلـی سـری اشـاره دارد. این اطلاعات دارای تعریف خاص می‌باشـند و اطلاعات طبقه‌بندی شده بـه موجـب مقـررات خاص به چهار دسته تقسیم شده است: سری، به کلی سری، محرمانه و خیلـی محرمانـه. بـا ایـن وجود، به نظر می‌رسد تعریـف آیـین‌نامـه مـورد اشاره در ماده ۳ ق.ج.ر (ماده ۷۳۱ ق.م.ا) مـلاک خواهد بود. اطلاعات سری، اطلاعاتی هستند کـه افشای آنها به امنیت کشـور لطمـه مـی‌زنـد امـا افشای اطلاعات به کلی سـری، صـدمات جبـران ناپذیر وارد می‌کند.

ماده ۳ ق.ج.ر (ماده ۷۳۱ ق.م.ا) بـه «جمـع‌آوری اطلاعات» اشاره‌ای ندارد اما عبارت «دسترسـی» که در بند (الف) آمده است مفهوم عام‌تری دارد. مـاده ۵۰۵ عبـارت «در اختیـار دیگـران قـرار دهد»را به صورت عام بیـان کـرده اسـت امـا در ماده ۳ ق.ج.ر مصادیق دیگران را به تفصیل بیان کرده است. در مجموع مجازات پیش‌بینـی شـده در ماده ۳ شـدیدتر از مجـازات مـذکور در مـاده ۵۰۵ می‌باشد و دلیل این امر، خطرنـاکتر بـودن جاسوسی رایانه‌ای است. به هر حال ماده ۳ نـوع خاصی از جرم جاسوسی را بیان مـی‌کنـد کـه از نظر موضوع و مکان و نحوه ارتکاب با جاسوسـی سنتی تفاوت دارد. موضوع این جرم، «داده‌هـای سـری» اسـت و مکـان ارتکـاب جـرم نیـز، سیستم‌های رایانه‌ای یا مخابراتی یـا حامـل‌هـای داده می‌باشد همان گونه که ارتکاب جاسوسی از راه‌هـای فنـی و تخصصـی صـورت مـی‌گیـرد. از همین روی می‌توان جاسوسی رایانه‌ای را یکی از

مصادیق جرائم یقه سفیدها به شمار آورد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، صص ۳۷۶-۳۷۷)

■ ۵۰- جرم «دسترسی غیرمجاز» نیز مانند جاسوسی سایبری» در ذیل «جرائم علیه محرمانگی داده‌ها یا سامانه‌های سایبری و مخابراتی» آمده و جرم انگاری شده است زیرا علیه موضوع «محرمانه بودن داده‌ها یا سامانه‌ها» که هدفی در جاوسی سایبری است، ارتکاب می‌یابد. این دو جرم، تنها از طریق سامانه‌های سایبری و یا مخابراتی یا حامل‌های داده در بستر فضای سایبر محقّق می‌شوند. علاوه بر تشابه مزبور، در خصوص جاسوسی سایبری علیه امنیت، در ماده ۳ ق.ج.ر، سه گام برای تحقق رفتار مادی جرم در نظر گرفته شده است:

۱- دسترسی به سامانه‌های سایبری و مخابراتی که داده‌های سرّی در آنها انباشت یا نگهداری می‌شوند.

۲- دسترسی به داده‌های سری یا تحصیل یا شنود آنها.

۳- در دسترس قرار دادن برای کسانی که شایستگی آگاهی از محتوای داده‌های سرّی را ندارند یا در دسترس قرار دادن داده‌های سری یا افشای آنها به دولت یا نهادهای بیگانه یا عاملان آنها. (عالی پور، حسن، حقوق کیفری فناوری اطلاعات، چ ۱، ص ۱۹۳)

در گامهای پیش گفته، دسترسی به سامانه‌های دربردارنده داده‌ها و نیز دسترسی به خود داده‌های سرّی، در اصل، همان «جرم دسترسی غیرمجاز» هستند. از این رو می‌گوییم پیکره اصلی جاسوسی سایبری، «جرم دسترسی غیرمجاز» است. (قاسم خواه، مهدی، دسترسی غیرمجاز در فضای سایبر، پایان نامه دوره کارشناسی ارشد رشته حقوق جزا و جرمشناسی دانشگاه شیراز، ص ۷۸، سال ۱۳۹۰. شرح و نقل از: الله وردی، فرهاد، حقوق کیفری سایبری، چ ۱، ص ۵۸)

■ ۵۱- ماده ۵۰۱ ق.م.ا (تعزیرات) مصوب ۱۳۷۵، در مقایسه با بند (ب) ماده ۳ ق.ج.ر از لحاظ حداقل مجازات، برخورد خفیف‌تری محسوب می‌شود اما اگر به ماده ۷۵ ق.ت.ا نگاه کنیم در می‌یابیم این قانون، برای بزه ارتکابی، مجازاتی به مراتب خفیف‌تر از هر دو قانون پیش‌گفته در نظر گرفته است. (الله وردی، فرهاد، حقوق کیفری سایبری، چ ۱، ص ۶۰)

■ ۵۲- در ق.ج.ر، جاسوسی رایانه‌ای و جرایم مرتبط با آن، در ذیل طبقه جرایم علیه محرمانگی داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی گنجانده و جرم‌انگاری شده است زیرا علیه دو موضوع «محرمانه بودن داده‌ها یا سامانه‌ها» و «امنیت ملی» که هدف نهایی جاسوسی رایانه‌ای است، ارتکاب می‌یابد؛ اما به نظر می‌رسد ذیل گروه جرایم علیه امنیت و آسایش عمومی، جایگاه مناسب‌تری برای آنها باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، صص ۳۰-۲۹)

■ ۵۳- قانونگذار ایران با هدف تضمین امنیت ملی، ماهیت، اقسام و مراحل جاسوسی را در هیچ یک از قوانین کیفری به طور شفاف تعریف ننموده است. ق.ج.ر نیز از این امر مستثنا نمی‌باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۰)

■ ۵۴- بنا بر استعمال لفظ «جاسوس» در معنای اصطلاحی و حقوقی آن در ماده ۳، به نظر می‌رسد به کارگیری لفظ «غیرمجاز» مذکور در ماده فوق زائد باشد. مویّد این دیدگاه عدم

استعمال عبارت مزبور در ماده ۲۴ قانون مجازات جرائم نیروهای مسلّح و مادتین ۵۰۲-۵۰۱ ق.م.ا (تعزیرات) مصوب ۱۳۷۵ است که از نقطه نظر قانونگذار، حاجت به بیان قید مزبور نبوده است. دو تقنین اخیر در تقنین ق.ج.ر می‌توانست مورد استفاده قرار گیرد.

■ ۵۵- تعریف ارائه شده از «جرم جاسوسی رایانه‌ای» توسط شورای اروپا:

تفتیش و دقّت نظر غیرموجه و ناحق در ابزارهای لازم یا افشای انتقال یا استفاده توأم با قصد از اسرار تجاری خواه متضمّن ضرر اقتصادی باشد و یا در بردارنده کسب یک منفعت اقتصادی نامشروع برای خود یا دیگری باشد.

■ ۵۶- واژه «هر کس» در اینجا اطلاق دارد اما در عرف حقوقی به چنین شخصی جاسوس گفته می‌شود. «جاسوس» در لغت به معنای کسی است که اخبار و اطلاعات شخص، مؤسّسه یا کشوری ررا به صورت مخفیانه گردآوری نموده و در اختیار شخص یا مؤسّسه یا کشور دیگری قرار می‌دهد. (فرهنگ، معین، ج ۲، واژه جاسوس) جاسوس رایانه‌ای از منظر حقوقی به شخصی گفته می‌شود که یکی از اعمال مذکور در ماده ۳ ق.ج.ر (ماده ۷۳۱ ق.م.ا) را انجام دهد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۷)

■ ۵۷- جاسوسی رایانه‌ای از نظر نحوه ارتکاب مانند جاسوسی سنتی و کلاسیک است یعنی اسرار حرفه‌ای، تجاری، سیاسی و نظامی را کسب نموده و مورد استفاده قرار داده یا افشاء کرده و به اشخاص غیرمجاز انتقال می‌دهند. این جرم نیز ممکن است با انگیزه‌های اقتصادی، نظامی و سیاسی رخ دهد و امنیت ملی را به مخاطره اندازد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۵)

■ ۵۸- منظور از «حامل‌های داده»، ابزارهایی هستند که می‌توان داده‌های سامانه‌های رایانه‌ای مخابراتی را در آنها ذخیره نمود؛ مانند انواع فلش‌های حافظه، دیسکت و غیره. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۵)

■ ۵۹- منظور قانونگذار از عبارات «اشخاص فاقد صلاحیت» و «بیگانه»، عام می‌باشد. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۴)

■ ۶۰- منظور از «دسترسی»، معنای عام و لغوی آن می‌باشد نه معنای حقوقی مذکور در ماده ۱ ق.ج.ر (ماده ۷۲۹ ق.م.ا) (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۴)

■ ۶۱- داده سری مهم‌ترین رکن و موضوع این جرم می‌باشد که در تبصره اول تعریف شده است اما این تعریف، بسیار عانم و کلی و مبهم است. عبارت «امنیت کشور» و «منافع ملی»، عبارتی پر وسعت و قابل تفسیرهای گوناگون می‌باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۵)

■ ۶۲- در حال انتقال بودن داده، شرط تحقق این جرم نیست بلکه داده ذخیره شده نیز موضوع جرم قرار می‌گیرد اما اشارهای به داده آماده انتقال نشده است. البته در بند (الف) به در حال انتقال بودن در جرم شنود محتوا اشاره دارد که موجب ابهام می‌باشد. در بند (ب) و (ج) عبارت «داده‌های مذکور» بیان شده که اشاره به داده‌های مذکور در متن دارد و اعم داده‌های در حال انتقال و ذخیره سازی می‌باشند. (زراعت،

شـرح مختصـر ق.م.ا، ج ۲، چ ۱، صـص ۳۷۶-۳۷۵)

■ ۶۳- دسترسی و شنود محتوای غیرسـری، در جرم متفاوت با مجازات‌های متفاوت هسـتند امـا در اینجا یک جرم به حساب آمده است. یکـی از ملاک‌های تعیین حداقل و حـداکثر مجـازات در اینجا نوع جـرم مـی‌باشـد یعنـی مجـازات جـرم دسترسی اصولا باید کمتر از مجازات شنود باشد. (زراعـت، شـرح مختصـر ق.م.ا، ج ۲، چ ۱، ص ۳۷۶)

■ ۶۴- جرم موضوع بند (الف) جرم مطلق اسـت و اطـلاق آن شـامل حـالتی نیـز مـی‌شـود کـه دسترسی به داده‌ها با هدف در اختیار قـرار دادن دیگران باشد. بر این اساس جرم‌هـای مـذکور در بند (ب) و (ج) مقیـد بـه حصـول نتیجـه اسـت یعنی چنانچه داده در اختیار این اشـخاص قـرار نگیرد یا افشاء نشود مشـمول بنـد (الـف) اسـت. (زراعت، شـرح مختصـر ق.م.ا، ج ۲، چ ۱، صـص ۳۷۸-۳۷۷)

■ ۶۵- عبارت «اشخاص فاقد صلاحیت» در بند (ب) اعم از اشخاص بیگانه یا خودی اسـت پـس شخص بیگانه مشمول بند (ج) نخواهـد بـود. بـا وجود این اگر شـخص بیگانـه، عامـل دولـت یـا سازمان یا شرکت یا گروه بیگانـه باشـد مشـمول بند (ج) می‌باشد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۷)

■ ۶۶- با توجه بـه قابـل تفسـیر بـودن عبـارت «منافع ملی»، باید منافع را به صورت محـدود و مضیق تفسیر نمود، زیرا از طرفی، میزان مجازات جاسوسـی رایانـه‌ای، سـنگین اسـت و از رطـف دیگر، اصل تفسیر مضیق قوانین کیفـری ایجـاب میکند که از تفسیر موسـع پرهیـز شـود. (الهـی مـنش، محمدرضـا؛ سـدره نشـین، ابوالفضـل؛ محشّای ق.ج.ر، چ ۲، ص ۳۵)

■ ۶۷- به موجب معیار شخصی حمایت از اسرار تجاری، اطلاعات محرمانه در فضای مجازی تنهـا برای افرادی ایجـاد مسـئولیت مـی‌کنـد کـه بـه موجب قانون یا قرارداد، مکلف به حفاظـت از آن اسرار می‌باشند. به عبارت دیگـر تعهـد بـه عـدم افشاء فقط برای افـرادی قابـل تصـور اسـت کـه اسرار از هر قسـم بـه طـور مسـتقیم در اختیـار ایشان قرار گرفته و تعهد به عـدم افشـاء نیـز بـه آنها یادآوری شده است. مـاده ۲ قـانون مجـازات انتشار و افشای اسناد محرمانه و سـری دولتـی و مـاده ۵۰۱ ق.م.ا در مـورد اسـرار امنیتـی، علی‌الظاهر بر همین مبنا تنظیم شده‌اند. چرا که در ماده ۲ افشاء یا انتشار اسرار توسـط کارکنـان سازمان و تعیین مجازات برای این عمل، مطـرح گردیده و در ماده ۵۰۱ ق.م.ا افشای اسـرار «بـه نحوی که متضمن نوعی جاسوسی باشـد» قابـل مجازات شناخته است. (السان، مصطفی، حقـوق فضای مجازی، چ ۱، ص ۷۲)

■ ۶۸- اشخاصی که به حکم قانون (وظیفـه) یـا قرارداد ملزم به عدم افشای اسرار مرتبط بـا کـار خود هستند، به طور مستقیم و به موجب قـانون مسـئولند. بـه لحـاظ عـدم و اطـلاع ایشـان و آموزش‌های لازم، بایـد مسـئولیت کیفـری و یـا مدنی ایشان را محقق و در صورت علم و عمد در افشای اسـرار، مجـازات مشـددی را بـرای افـراد مذکور در نظر گرفت. (السان، مصـطفی، حقـوق فضای مجازی، چ ۱، ص ۷۳)

■ ۶۹- اشخاصی که به طور ناخواسته اطلاعـاتی را به دست می‌آورند، علی‌الاصـول در قبـال آنهـا مسئولیتی ندارند، مگر اینکه با علم به محرمانه و سری بودن آن، نسبت بـه افشـاء اقـدام نماینـد.

مسئولیت این دسته از افراد چون بر مبنای انصاف محقق می‌شود، بیشتر صبغه مدنی و مالی دارد. البته در صورت وضع قانون خاص، مسئولیت کیفری نیز منتفی نخواهد بود. (السان، مصطفی، حقوق فضای مجازی، چ ۱، ص ۷۴)

■ ۷۰- ماده ۷۵ ق.ت.ا با مواد ۵۸ و ۶۴ تداخل پیدا می‌کند و معلوم نیست که این تداخل (در جرم‌انگاری و میزان مجازات) چگونه حل خواهد شد. به علاوه، افشای اسرار تجاری، در صورتی که با اقتصاد ملی ارتباط یابد، در زمره «جرائم علیه امنیت اقتصادی» قرار می‌گیرد. به همین دلیل، در ماده ۳ ق.ج.ر مجازات بیشتری برای دسترسی و افشای داده‌های سری در نظر گرفته شده است. (السان، مصطفی، حقوق فضای مجازی، چ ۱، صص ۷۵-۷۴)

■ ۷۱- جرم جاسوسی رایانه‌ای عموما از دسترسی غیرمجاز غیرقابل تفکیک است. زیرا تا دسترسی غیرمجازی صورت نگیرد جاسوسی رایانه‌ای رخ نخواهد داد. البته برای تحقق جرم نخست باید تدابیر حفاظتی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی هم نقض شود که عموما چنین هم هست. همچنین انتشار یا توزیع محتوای مستهجن مستلزم تولید آنهاست. لذا می‌توان این دو را غیرقابل تفکیک از یکدیگر دانست. (جلالی فراهانی، امیرحسین، درآمدی بر آیین دادرسی کیفری جرائم سایبر، چ ۱، صص ۹۵-۹۴)

■ ۷۲- کشورهای تابع نظام حقوقی نوشته برای اعمال صلاحیت کیفری خود به قاعده دیگری نیز متوسل می‌شوند و آن در جایی است که یک فعل سرزنش‌آمیز امنیت و منافع ملی کشور را تهدید کند. البته این سخن به این معنا نیست که کشورهای تابع نظام حقوق عرفی به آن متوسل نشوند، اما میزان اتکاء متفاوت است. به هر حال، این اصل در جایی نظر قانونگذار کیفری را به خود جلب می‌کند که قربانی فعل سرزنش‌آمیز، دولت یا حتی خود حاکمیت باشد. (جلالی فراهانی، امیرحسین، درآمدی بر آیین دادرسی کیفری جرائم سایبر، چ ۱، ص ۲۹)

Council of Europe; European Committee on Crime Problems; Extraterritoral Jurisdiction; Strasbourg; 1990, p 12

■ ۷۳- به موجب معیار شخصی حمایت از اسرار تجاری، اطلاعات محرمانه در فضای مجازی تنها برای افرادی ایجاد مسئولیت می‌کند که به موجب قانون یا قرارداد، مکلف به حفاظت از آن اسرار می‌باشند. به عبارت دیگر تعهد به عدم افشاء فقط برای افرادی قابل تصور است که اسرار از هر قسم به طور مستقیم در اختیار ایشان قرار گرفته و تعهد به عدم افشاء نیز به آنها یادآوری شده است. ماده ۲ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۵۰۱ ق.م.ا در مورد اسرار امنیتی، علی‌الظاهر بر همین مبنا تنظیم شده‌اند. چرا که در ماده ۲ افشاء یا انتشار اسرار توسط کارکنان سازمان و تعیین مجازات برای این عمل، مطرح گردیده و در ماده ۵۰۱ ق.م.ا افشای اسرار «به نحوی که متضمن نوعی جاسوسی باشد» قابل مجازات شناخته است. (السان، مصطفی، حقوق فضای مجازی، چ ۱، ص ۷۲)

■ ۷۴- اشخاصی که به حکم قانون (وظیفه) یا قرارداد ملزم به عدم افشای اسرار مرتبط با کار خود هستند، به طور مستقیم و به موجب قانون مسئولند. به لحاظ عدم و اطلاع ایشان و آموزش‌های لازم، باید مسئویلت کیفری و یا مدنی ایشان را محقق و در صورت علم و عمد در

افشای اسرار، مجازات مشددی را برای افراد مذکور در نظر گرفت. (السان، مصطفی، حقوق فضای مجازی، چ ۱، ص ۷۳)

■ ۷۵- اشخاصی که به طور ناخواسته اطلاعاتی را به دست می‌آورند، علی‌الاصول در قبال آنها مسئولیتی ندارند، مگر اینکه با علم به محرمانه و سری بودن آن، نسبت به افشاء اقدام نمایند. مسئولیت این دسته از افراد چون بر مبنای انصاف محقق می‌شود، بیشتر صبغه مدنی و مالی دارد. البته در صورت وضع قانون خاص، مسئولیت کیفری نیز منتفی نخواهد بود. (السان، مصطفی، حقوق فضای مجازی، چ ۱، ص ۷۴)

■ ۷۶- ماده ۷۵ ق.ت.ا با مواد ۵۸ و ۶۴ تداخل پیدا می‌کند و معلوم نیست که این تداخل (در جرم‌انگاری و میزان مجازات) چگونه حل خواهد شد. به علاوه، افشای اسرار تجاری، در صورتی که با اقتصاد ملی ارتباط یابد، در زمره «جرائم علیه امنیت اقتصادی» قرار می‌گیرد. به همین دلیل، در ماده ۳ ق.ج.ر مجازات بیشتری برای دسترسی و افشای داده‌های سری در نظر گرفته شده است. (السان، مصطفی، حقوق فضای مجازی، چ ۱، صص ۷۵-۷۴)

■ ۷۷- «در رابطه با نسخ یا عدم نسخ ماده ۱۳۱ ق.م.ج.ن.م مصوب ۱۳۸۲، دو نظریه وجود دارد:

۱- برخی معتقدند با تصویب قانون جدید جرایم رایانه‌ای -که در ماده ۲۶ (۷۵۴ ق.م.ا) صریحاً به رسیدگی جرایم نیروهای مسلح اشاره شده- و نیز ماده ۳۰ ق.ج.ر (ماده ۷۵۸ ق.م.ا) که قوه قضاییه را به تعیین شعبی از دادسراها و دادگاه‌های نظامی جهت رسیدگی به جرایم رایانه‌ای موظف نموده است، ماده ۱۳۱ ق.م.ج.ن.م نسخ شده و رسیدگی به جرایم رایانه‌ای تمامی افراد نیروهای مسلح، برابر ق.ج.ر اخیر التصویب خواهد بود.

۲- در مقابل این نظر، تعداد قابل توجهی از قضات سازمان قضایی نیروهای مسلح نیز معتقدند از آنجا که ماده ۱۳۱، نسبت به ق.ج.ر که گستردگی و مصادیق آن بیشتر است، خاص تلقی می‌شود و طبق یک قاعده کلی پذیرفته شده توسط اکثریت حقوقدانان، عام لاحق، ناسخ خاص سابق نخواهد بود؛ (چنان چه موضوع حکم قانون در عالم خارج متعدد باشد، آن را در اصطلاح "عام" و اگر حکم، ناظر به موضوع معینی باید "خاص" می‌نامند. در رابطه بین قانون قدیم و جدید، هرکدام که مصداق بیشتری داشته باشد، نسبت به دیگر عام و حکمی که قلمروی اجرای آن وسعت کمتری دارد، خاص است. چنان که اگر حکمی ناظر به کارمندان دولت و دیگری مربوط به قضات باشد، حکم نخست، عام و دیگری خاص است. (کاتوزیان، ناصر، مقدمه علم حقوق، چ ۴۹، ص ۱۷۱، ۱۳۸۱) لذا ماده ۱۳۱ ق.م.ج.ن.م در خصوص جرایم پیش‌بینی شده در آن ماده به قوت خود باقی بوده و در مورد نظامیان قابلیت اعمال دارد و ق.ج.ر در مورد جرایم مندرج در ماده ۱۳۱ قابل استناد نیست. لیکن در مواردی که ق.ج.ر متضمن جرایمی است که در ق.م.ج.ن.م پیش‌بینی نشده است؛ از قبیل دسترسی غیرمجاز و شنود غیرمجاز و جرایم علیه عفت و اخلاق عمومی و غیره در مورد نظامیان نیز در صورت ارتکاب، حاکم خواهد بود. بنا بر دیدگاه اخیر، اگر یک پایور نظامی مرتکب یکی از جرایم رایانه‌ای شود، نخست باید آن رفتار را بر اساس ماده ۱۳۱ ق.م.ج.ن.م با عناوین مجرمانه پیش‌بینی شده در آن قانون تطبیق داد و چنان

چه آن رفتار با یکی از این عناوین منطبق بود، به استناد قانون یاد شده درباره آن رای مقتضی صادر می‌شود ولی در صورتی که آن رفتار با هیچ یک از عناوین مجرمانه آن قانون منطبق نبود، با مراجعه به ق.ج.ر تعیین تکلیف خواهد شد. با این توضیح، حکم ماده ۵۶ ق.ج.ر که قوانین مغایر را ملغا دانسته، باید منصرف از ق.م.ج.ن.م تلقی نمود.

به نظر می‌رسد از دو نظریه مذکور، نظریه دوم به صواب نزدیک‌تر و با اصول حقوقی سازگارتر باشد. همچنین با عنایت به ماده ۵۵ ق.ج.ر که به الحاق آن به ق.م.ا تصریح کرده است، این موضوع به راحتی قابل استناد خواهد بود.» (ترکی، غلام عباس، نگرش علمی و کاربردی به ق.ج.ر (قسمت سوم)، ماهنامه دادرسی، شماره ۷۹، س ۱۳، فروردین و اردیبهشت ۱۳۸۹، ص ۴) البته در توسل به به این استدلال باید جانب احتیاط را مراعات نمود تا از تفسیر موسع جلوگیری شده و اصل تفسیر کیفری به نفع متهم رعایت شود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، صص ۳۳-۳۱)

■ ۷۸- یکی از خلأهای این قانون در مقایسه با ماده ۱۳۱ ق.م.ج.ن.م، عدم پیش‌بینی جاسوسی اقتصادی و صنعتی است. (این نوع جاسوسی در جهان امروز رواج داشته و شامل کسب هرگونه اطلاع از طرح‌ها، برنامه‌ها، نقشه‌ها و پروژه‌هایی است که منجر به درآمدزایی و پیشرفت‌های اقتصادی، تجاری و صنعتی در عرصه ملی یا بین‌المللی می‌گردد.) هر چند در بند (ج) از شرکت یا گروه بیگانه صحبت شده، اما با توجه به این که شرکت‌ها و گروه‌ها می‌توانند نقش واسط برای دشمن داشته باشند و به ویژه به این که موضوع جرم، داده‌های سری است، این خلأ بیشتر به چشم می‌آید. (عالی پور، حسن، امنیت و ناامنی در فضای سایبر: تهدیدات رایانه‌ای علیه امنیت ملی، حقوق فناوری اطلاعات و ارتباطات (مجموعه مقالات)، به کوشش امیرحسین جلالی فراهانی، چ ۱، ۱۳۸۸، ص۳۳۳. شرح و نقل از: الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۳)

از آنجائی که در حقوق جرا، تفسیر باید مضیّق و محدود باشد، از ق.م.ج.ن.م مصوب ۱۳۸۲ نمیتوان برای جرم‌انگاری در «جاسوسی اقتصادی و صنعتی» در امور غیرنظامی، وحدت ملاک گرفت. بنابراین باید به محدوده نص اکتفا نمود و آن موارد که صرفاً مربوط به اشخاص موضوع همان قانون خاص است، به عموم افراد، تعمیم ننمود.

■ ۷۹- ماده ۱۳۱ ق.م.ج.ن.م مصوب ۱۳۸۲:

هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم افزارهای مربوط صورت گیرد و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه‌بندی شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند، افشاء غیرمجاز اطلاعات، سرقت اشیاء دارای ارزش اطلاعاتی مانند سی‌دی (CD) یا دیسکتهای حاوی اطلاعات یا معدوم کردن آنها یا سوءاستفاده‌های مالی که نظامیان به وسیله رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازاتهای مندرج در مواد مربوط به این قانون می‌باشند. (به نقل از: روزنامه رسمی شماره ۱۷۱۶۸-۱۳۸۲/۱۱/۱۲)

نقض تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری

ماده ۴ (ماده ۷۳۲ ق.م.ا) - هر کس به قصد دسترسی به داده‌های سری موضوع ماده ۳ این قانون، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از ۶ ماه تا ۲ سال یا جزای نقدی از ۱۰ میلیون ریال تا ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد.

■ ۸۰- جرم موضوع این ماده در حقیقت مقدمه جرائم مذکور در ماده قبل می‌باشد که با قصد دسترسی صورت می‌گیرد. این جرم تا زمانی است که هنوز دسترسی صورت نگرفته باشد وگرنه چنانچه نقض تدابیر امنیتی منتهی به دسترسی شود، از شمول این ماده خارج خواهد بود. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۸)

■ ۸۱- جرم موضوع این ماده با انجام فعل مثبت مادی محقق می‌شود، لذا با ترک فعل نمی‌توان وقوع آن را محرز دانست.(الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۶)

■ ۸۲- این جرم‌انگاری برای حفاظت از سامانه‌های رایانه‌ای و مخابراتی حیاتی و حساس و تامین امنیت آنها بوده و نوعی جرم بازدارنده تلقی می‌شود تا مقدمات تحقق جرم جاسوسی رایانه‌ای برچیده شود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۶)

■ ۸۳- ماده ۴ ق.ج.ر در مقایسه با ماده ۵۰۳ ق.م.ا (تعزیرات) مصوب ۱۳۷۵، حداقل کمتری را برای بزه پیش بینی کرده، همچنین در بند (ج) ماده ۳ هم با توجه به مواد ۵۰۵ و ۵۰۱ مشاهده میکنیم، مجازات شدیدتری از سوی قانونگذار در نظر گرفته شده است. (الله وردی، فرهاد، حقوق کیفری سایبری، چ ۱، ص ۶۰)

■ ۸۴- این جرم در زمره جرایم عمدی و مقیّد قرار دارد و برای تحقق و احراز آن به سوءنیت عام و نیز سوءنیت خاص نیاز است؛ لذا خواست نقض تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی با علم به وجود تدابیر مزبور به قصد دسترسی به داده‌های سری باید احرز شود. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، صص ۳۷-۳۶)

■ ۸۵- گرچه لفظ «شنود» متبادر در دریافت فایل‌های صوتی است، اما در حقیقت منظور صرف فایل‌های صوتی یا مخابراتی نبوده، شامل هر نوع داده در حال انتقالی است. این معنا در مقایسه با ماده ۳ و ۴ ق.ج.ر روشن می‌شود؛ چرا که ماده ۳ سخن از شنود و دریافت داده‌های در حال انتقال غیرعمومی (خصوصی) که مطلق بوده، شامل داده در حال انتقال است و از این روست که در این دو ماده، در حال انتقال بودن داده اشاره رفته است. در ق.ت.ا نیز در مقام حمایت از داده‌های شخصی از عبارت ذخیره، پردازش سود جسته است.

عناصر این جرم در حقیقت هر نوع پردازش، مشاهده، شنود، دریافت یا ذخیره غیرقانونی اطلاعات در حال انتقالی است که مجرم مجاز به دریافت یا شنود آن نیست، آنجایی که داده غیرعمومی و خصوصی است. در صورتی که غیر تجاری باشد، مشمول ماده ۳ ق.ج.ر می‌شود. اما اگر تجاری باشد؛ مشمول ماده ۵۸ ق.ت.ا است.

اما اگر عمومی و جزء اطلاعات سرّی باشد، مشمول ماده ۴ ق.ج.ر است.
صریح‌ترین ماده قانونی در مورد این جرم ماده ۳ ق.ج.ر است که می‌گوید: «هر کس عمداً و بدون مجوز، داده‌های در حال انتقال غیرعمومی در یک ارتباط خصوصی، یا از یک یا چند سیستم رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی شنود یا دریافت نماید، به حبس از نود و یک روز تا یک سال یا پرداخت جزای نقدی از یک میلیون ریال تا شش میلیون ریال محکوم خواهد شد.» این ماده فروع مختلف شنود و دریافت غیرمجاز، اعم از شنود داده‌های خصوصی، تجاری، عمومی سرّی و مربوط به امنیت ملی را شامل می‌شود. اما مواد خاصی، چون ماده ۵۸ ق.ت.ا و ماده ۴ ق.ج.ر موارد تجاری و مربوط به امنیت ملی را تخصیص می‌زند.
ماده ۵۸ ق.ت.ا بیان می‌دارد: «ذخیره، پردازش و یا توزیع داده پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است» و ماده ۷۱ این قانون، مجازات ناقضین حریم داده‌های پیام شخصی، که اقدام به دریافت و پردازش و... غیرمجاز و بدون رضایت صاحبان آن را به مجازات نسبتاً سنگین یک تا سه سال حبس محکوم کرده است. لازم به ذکر است که به موجب ماده ۷۲، ارتکاب این جرم توسط دفاتر خدمات صدور گواهی الکترونیکی که بیشتر در معرض این جرم هستند و سایر نهادهای مسئول، موجب تشدید مجازات به حداکثر مجازات مقرر خواهد شد.
ماده ۴ ق.ج.ر نیز به داده‌های سرّی و امنیتی اشاره دارد. کسانی که عمداً و بدون مجوز، اقدام به نفوذ، دسترسی و در نتیجه دریافت و شنود داده‌های سرّی عمومی در حال انتقال یا موجود در سیستم‌های رایانه‌ای یا مخابراتی یا حامل داده که واجد ارزش برای امنیت داخلی یا خارجی کشور باشد، می‌کنند، به مجازات حبس از یک تا سه سال و جزای نقدی از ده میلیون ریال تا صد میلیون ریال محکوم می‌شوند.
یکی از مصادیق شنود و دریافت غیرمجاز را می‌توان شنود فایل‌های صوتی و دریافت و باز کردن نامه‌های الکترونیکی افراد دانست. البته تحت نظر گرفتن رفتار، گفتار و نوشتار کاربر هنگام استفاده از گفت و گوی صوتی الکترونیکی، هنگام شرکت در تالارهای گفت وگو و گپ زنی (Chat)، هنگام ارسال نامه الکترونیکی صوتی و نوشتاری و...، مصداق کاملی از این جرم است. (پگاه حوزه، ۲۲ تیر ۱۳۸۷، ش ۲۳۵، قسمت سوم طبقه‌بندی و آسیب شناسی جرائم رایانه‌ای)
■ ۸۶- اگر تصریح این ماده نبود امکان داشت عملیات نقض تدابیر امنیتی به عنوان شروع در جرم دسترسی تلقی شود. در حال حاضر شروع به جرائم دارای مجازات حبس تعزیری درجه شش مجازات ندارد اما شروع به جرائم دارای جزای نقدی درجه شش مجازات دارد. قانون مجازات اسلامی در مورد چنین جرائمی ابهام دارد؛ اگر مجازات حبس در نظر گرفته شود شروع در آنها قابل مجازات نیست اما اگر مجازات نقدی در نظر گرفته شود شروع در آنها مجازات دارد. (زراعت، شرح مختصر ق.م.ا، ج ۲، چ ۱، ص ۳۷۸)

■ ۸۷- دسترسی غیرمجاز که عمدتاً با هک کردن امکان‌پذیر است، چه با هدف جاسوسی و چه کنجکاوی و تفریح یا جمع‌آوری اطلاعات جهت انجام فعلی مجرمانه باشد؛ یکی دیگر از جرائم امنیتی است که در اثر سوءاستفاده از رایانه به وقوع می‌پیوندد و جامعه اطلاعاتی را در گرداب هرج و مرج و ناامنی فرو می‌برد. هک کننده که فاعلی قاصد است، با صرف وقت بسیار، حرفه‌های حفاظتی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی را می‌یابد، بدان نفوذ می‌کند و امنیت اطلاعات را به باد سخره می‌گیرد. هک کنندگان گاه به عنوان تفریح و خودنمایی و گاه با هدف باج‌گیری یا تهدید صاحبان داده‌ها یا سیستم‌ها و گاه با هدف جاسوسی، اطلاعاتی را که مجاز به دسترسی بدان نیستند را مشاهده می‌کنند. دسترسی غیرمجاز از یک سو امنیت اطلاعاتی شهروندان جامعه اطلاعاتی را تهدید می‌کند و منجر به ناامنی و غیر قابل اعتماد بودن یکی از مفیدترین فناوری قرن اطلاعات؛ یعنی اطلاعات الکترونیکی می‌شود و از سوی دیگر حاکمیت، اقتدار و امنیت اطلاعات سرّی دولت‌ها را بر هم می‌زند، که منجر به جاسوسی رایانه‌ای می‌گردد (همچنان که در انتخابات مجلس هشتم نیز هکرها درصدد هک کردن و اخلال در سیستم انتخابات بودند) و از سویی موجب خدشه‌دار شدن رقابت مشروع و عادلانه در بستر مبادلات الکترونیکی اقتصادی و تجاری گشته و منجر به جرم تحصیلی غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسّسات برای خود خواهند شد.

برخورد با این جرم اقدامی پیش گیرانه در جهت امنیت اطلاعات جامعه اطلاعاتی، رقابت عادلانه و سالم تجاری و امنیت ملی و منافع راهبردی دولت‌ها است. از این رو ق.ج.ر آن را در مبحث دوم از فصل اول جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی آورده است تا مقدمه برای حفظ محرمانگی داده‌ها و سیستم‌ها باشد. این قانون در ماده ۲ در مورد دسترسی به اطلاعات غیرسرّی می‌گوید: «هر کس عمداً و بدون مجوز، با نقش تدابیر حفاظتی داده‌ها یا سیستم رایانه‌ای یا مخابراتی، به آنها دسترسی یابد، به جزای نقدی از یک میلیون ریال تا شش میلیون ریال یا به حبس از نود و یک روز تا یک سال محکوم می‌گردد». اطلاق کلمه داده‌ها، شامل همه نوع داده‌ای می‌شود. لذا ارزشمند بودن یا بی‌ارزش بودن، قابل استفاده غیرقانونی بودن یا نبودن داده‌ها، مورد نظر نبوده، دسترسی غیرمجاز و عمدی همراه با نقض تدابیر حفاظتی (که بر عنوان هک کاملاً منطبق است) به همه نوع داده‌ها، اعم از تجاری، سیاسی و جرم شمرده شده است؛ چرا که صرف ارتکاب دسترسی غیرمجاز به داده‌ها موجب نقض اصل محرمانه بودن داده‌ها و اطلاعات می‌گردد.

ماده ۶۴ ق.ت.ا مصوب ۱۳۸۲ نیز بر این اصل تأکید کرده با ناقضین این اصل برخورد شدیدتری نموده است. به موجب این ماده: «به منظور حمایت از رقابت مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسّسات برای خود... جرم محسوب و مرتکب به مجازات مقرر در این قانون (ماده ۷۵) خواهد رسید». ماده ۷۵ این قانون، مجازات شدیدتری نسبت به ماده ۲ ق.ج.ر معیّن کرده است. به موجب این ماده: «متخلّفین از ماده ۶۴ این قانون... به حبس از شش ماه تا دو سال و نیم، و جزای نقدی معادل پنجاه میلیون ریال محکوم خواهند

شد». البته شدّت برخورد ماده ۷۵، گرچه کمتر از برخورد با دسترسی به داده‌های سرّی موضوع ماده ۴ قانون مجازات جرائم رایانه است، اما با این حال با توجه به اهمیت ویژه داده‌های سرّی که مرتبط با امنیت ملی کشور است، مجازات مقرر در ماده ۴ ق.ج.ر از تناسب لازم برخوردار نبوده، شدت بیشتری را می‌طلبد.

سرقت مشخصات، که یکی از وحشتناک‌ترین جرائم رایانه‌ای است را می‌توان یکی از مصادیق دسترسی غیرمجاز دانست. امروزه اطلاعات شخصی افراد بسیاری به صورت آنلاین و رایگان قابل دسترسی است و حتی اطلاعات شخصی را می‌توان با مبلغی اندک بدست آورد. جینا دی آنجیلز در مقاله‌ای درباره جرائم رایانه‌ای در مورد خطر این جرم می‌گوید: «آیا می‌دانید اگر نام خانوادگی شما در کتاب راهنمای تلفن باشد، بدون توجه به اینکه شما رایانه دارید یا نه، احتمالاً تلفن و آدرس شما در شبکه جهان گستر قابل دسترسی خواهد بود؟ شاید تعجب کنید که چگونه تمام این اطلاعات شخصی به شبکه رایانه‌ها راه یافته است. یادآور می‌شویم که اولین شبکه‌های رایانه‌ای، دولتی بودند. با افزایش میزان دسترسی به رایانه‌ها و آسانتر شدن استفاده از آنها، شرکت‌های خصوصی، همانند دولت، شروع به استفاده از رایانه‌ها برای نگهداری اطلاعات کردند». روزنامه نگاری به نام پیتر مک گراد (Peter Mcgrath) درباره رایانه‌ها می‌گوید: «رایانه‌ها تبدیل به انبارهای نگهداری محرمانه‌ترین جزئیات زندگی مردم شدند. هر کسی که یک حساب در بانک باز می‌کرد، ردپایی الکترونیکی از خود به صورت مخارج خانه، خریداری اشیاء مورد علاقه و ملاقات با دکتر بجا می‌گذاشت. سرویس تلفن، ردپایی ایجاد می‌کرد که منجر به شناسایی اقوام و دوستان شخص می‌شد. حتی یک شماره امنیت ملی که دارای قابلیت اتکاء بالقوه‌ای بود، به وسیله آن یک دنبال کننده ردپا می‌توانست از رایانه‌های دولتی، عدم بازپرداخت مالیات صاحب آن شماره را در یابد. امروزه که شماره گواهینامه رانندگی افراد نیز در رایانه‌های شبکه‌ای بزرگ، ذخیره می‌شود، مشخصات فیزیکی اشخاص- رنگ چشم، قد و امثال آن- نیز قابل دسترسی می‌باشد».

در واقع سرقت مشخصات می‌تواند مقدمه‌ای برای جرائمی، چون سرقت اموال الکترونیکی، افترا و افشای اسرار شخصی افراد، کلاهبرداری و... باشد. به عنوان نمونه، گزارشگری به نام تی. ترنت گگاکس (T.Trent Gegax) در شماره ۱۹ جولای ۱۹۹۷ مجله نیوزویک، گزارشی درباره پرونده کاترین رمبو (Kathryn Rembo) نوشت. کاترین یکی از قربانیان سرقت مشخصات بود. یک نفر اطلاعات شخصی کاترین را در یک فرم استخدام یافته و آن را در بانک داده‌های اینترنت و موتورهای جستجو قرار داده بود و سپس با استفاده از این اطلاعات، اقدام به درخواست کارت اعتباری کرده بود. در این گزارش قید شده است که این شخص «یک اتومبیل جیپ به قیمت ۲۲/۰۰۰ دلار، پنج کارت اعتباری، یک آپارتمان و یک وام ۳/۰۰۰ دلاری را با استفاده از اطلاعات شخصی کاترین رمبو و سوابق اعتباری خوب او به چنگ آورده بود». چارلز پاپاس (Charles PaPPas) نویسنده ستونی به نام «شبکه ایمن» در تحقیقات خود بریافتن این نکته متمرکز شد، که اطلاعات شخصی تا چه حد از طریق اینترنت قابل دسترسی است. او شروع به جستجو برای

یافتن یک دوست قدیمی در اینترنت کرد و دریافت که بعضی از این اطلاعات به صورت رایگان قابل دسترسی است و با پرداخت مبلغ بسیار اندکی، امکان دسترسی بسیار بیشتری فراهم می‌آید. پاپاس نوشت: «در حدود دو روز وقت و ۵۰ دلار پول صرف کردم و مطالبی را درباره او فهمیدم که احتمالاً همسرش نیز از آنها خبر ندارد. با صرف مقداری پول بیشتر، من به سادگی توانستم سابقه رانندگی، سابقه کیفری و ادّعانامه‌های جبران کارکنان دوستم و مطالب بیشتری در مورد او را بدست آورم.» (پگاه حوزه، ۲۲ تیر ۱۳۸۷، ش ۲۳۵، قسمت سوم طبقه‌بندی و آسیب شناسی جرائم رایانه‌ای)

■ ۸۸- در یک نتیجه گیری منطقی به نظر می‌رسد، منظور قانونگذار از داده‌های سری، داده‌های غیر عمومی باشد که مطابق با ماده ۳ ق.ج.ر (ماده ۷۳۱ ق.م.ا)، افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند. (الهی منش، محمدرضا؛ سدره نشین، ابوالفضل؛ محشّای ق.ج.ر، چ ۲، ص ۳۶)

■ ۸۹- با در نظر گرفتن ق.م.ا و ق.ج.ر می‌توان، جاسوسی اینترنتی را در حقوق ایران به طور کلّی به سه بخش تقسیم کرد:

الف- دسترسی به اطلاعات و داده‌های سرّی و امنیتی:

منظور از اطلاعات و داده‌های سرّی-همچنان که در تبصره ۱، ماده ۴، ق.ج.ر آمده- اطلاعاتی است که افشای آن به منافع ملی و امنیت ملی صدمه وارد کند. این اطلاعات؛ اعم از اسرار نظامی، سیاست‌ها و تصمیمات سیاسی سرّی است. در تبصره ۲ این ماده، دولت موظّف به تهیه آیین‌نامه اجرایی تعریف و طبقه‌بندی اطلاعات و داده‌های سرّی شده است: «آیین‌نامه طرز تعیین و تشخیص داده‌های سرّی و نحوه طبقه‌بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت دادگستری و با همکاری وزارتخانه‌های کشور، اطلاعات، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت وزیران خواهد رسید».

دسترسی؛ اعم از سرقت و هک و دیگر اقدامات مجرمانه است، لذا با هر روشی که به این اطلاعات دست یابند به مجازات این جرم محکوم خواهند شد. البته به نظر می‌رسد که چون شیوه‌هایی مثل جعل و شنود و دریافت غیرمجاز-که خود جرم جداگانه‌ای هستند- اگر به عنوان مقدمه این دسترسی باشند مجازات جداگانه خواهند داشت.

نکته دیگر اینکه جرم دسترسی، موضوع این بند، جدای از جرم مذکور در بند بعدی است، لذا چه پس از دسترسی این اطلاعات را در اختیار افراد فاقد صلاحیت قرار دهد یا خیر، مجازات مذکور در این بند شامل وی خواهد شد.

ب- مطلع کردن یا قرار دادن اطلاعات در اختیار افراد فاقد صلاحیّت: برای مطلع کردن افراد فاقد صلاحیت فرقی نمی‌کند که آنها را به چه شیوه‌ای از مضمون اطلاعات سرّی آگاه کند، لذا ممکن است در قالب چت نوشتاری یا گفتاری یا تصویری باشد و یا با استفاده از ایمیل یا هر ابزار الکترونیکی و غیر الکترونیکی. البته اگر عین اطلاعات را برای شخص فاقد صلاحیتی بفرستد، «در اختیار قرار دادن» صدق خواهد کرد.

ج- افشای اطلاعات سرّی برای بیگانگان: خطر افشای اطلاعات سرّی برای بیگانگان به ویژه دول و گروه‌های متخاصم به مراتب بیشتر است، لذا مجازات آن نیز بسیار سنگین‌تر است. درواقع