بسم الله الرحمن الرحیم

جزوه حقوق فناوری های نوین

دانشکده حقوق دانشگاه آزاد اسلامی واحد تهران شمال

استاد:دکتر مصطفی پیرعلی

مقدمه:

با توسعه وپیشرفت تکنولوژی و فناوری های نوین و نقش پر رنگ آن در جوامع امروزی ، این حوزه به صورت یک موضوع جدید و پر چالش تبدیل شده است . امروزه نمی توان تاثیر استفاده از فناوری های نوین از جمله اینترنت و وسایل الکترونیکی از جمله رایانه ها و تلفن همراه را بر زندگی افراد نادیده گرفت . حضور افراد در فضای مجازی ، ایجاد کسب و کار در این فضا ، شکل گیری روابط اجتماعی در آن و همچنین انجام معاملات تجاری از طریق آن باعث شده است این فضا به عنوان یک محیط مجازی درآید که متاسفانه برخی از افراد نیز از آن سود جویی می کنند . از این رو شناخت حقوق فناوری های نوین برای استفاده هر چه بهتر از این فناوری ها به عنوان یک شاخه جدید از حقوق می تواند ما را در استفاده از این فناوری ها در زندگی پیچیده امروزی راهنمایی و مساعدت نماید.عبارت حقوق فناوری های نوین، در ادبیات حقوقی ایران و جهان، واژه نسبتا تازه ای است. حقوق فناوری های نوین، می تواند تعاریف و معانی متعددی داشته باشد. در واقع معنای اراده شده از حقوق فناوری های نوین بسته به مکان و نحوه کاربرد آن، متفاوت است. در بعضی از موارد، عبارت حقوق فناوری های نوین، به معنای حقوق کامپیوتر به کار می رود. در این مفهوم، کلیه مسائل مرتبط با کامپیوتر که به حقوق افراد، ارتباط دارد مورد نظر است. حقوق فناوری های نوین گاهی به معنای حقوق ارتباطات، به کار گرفته می شود. در این عبارت مسائل حقوقی پیرامون ارتباطات افراد از طریق ابزار فناوری های نوین، بررسی می شود. در نهایت، حقوق فناوری های نوین، گاهی به مفهوم حقوق مالکیت معنوی است. یعنی حمایت از حق اختراع و امثال آن.زیست فناوری و استفاده از ان نیز به عنوان یکی دیگر از فناوری های نوین نیز دارای قواعد و حقوق مخصوص به خود است که آن نیز در شررایط خودش باید مورد بررسی قرار گیرد.

مسائل مهم حقوق فناوری های نوین: حقوق فناوری های نوین در معنای عام آن، مسائل گوناگونی رو پوشش می دهد. در حقیقیت، حقوق فناوری های نوین به دنبال آن است تا مانند سایر جنبه های حقوق، زوایای قانونی مربوط به فناوری های نوین را با تعیین حدود مشخص شده در قوانین، بررسی کرده و از این طریق حقوق افراد را مورد حمایت قرار دهد. در این راستا، حقوق فناوری های نوین، به طور مشخص به موضوعاتی مانند:- حقوق هوافضا-حقوق نانوفناوری های نوین- حقوق ارتباطات از راه دور -حقوق سایبر-حقوق انتقال فناوری-حقوق مالکیت معنوی در فناوری های نوین-حقوق ارتباطات از راه دور و مانند اینها می پردازد که هر کدام از آنها موضوع بحث جداگانه ای را می طلبد.

قوانین ایران در خصوص حقوق فناوری های نوین: با توجه به رشد فناوری های نوین، در سراسر جهان، قوانینی در خصوص جنبه های مختلف فناوری های نوین، نگاشته و تصویب شد. در حال حاضر ایران، نظام

حقوقی ایران نیز در خصوص فناوری های نوین قوانینی دارد، من جمله قانون تجارت الکترونیک و قانون مجازات جرایم رایانه ای. هم چنین در خصوص ما لکیت معنوی، قوانینی در جهت حمایت از آن به تصویب رسیده است. با این مفهوم، حقوق فناوری های نوین در ایران شناخته شده و مورد حمایت است با این حال، قوانین موجود در زمینه حقوق فناوری های نوین، هنوز کافی به نظر نمی رسند.

جنبه نوین حقوق فناوری های نوین: یکی از جنبه های نوین حقوق فناوری های نوین که در جهان تازگی دارد و در ایران، به دلیل ضعف فناوری و عدم موضوعیت، هنوز مورد بررسی قرار نگرفته است، هوش مصنوعی است. مسئولیت ناشی از استفاده از هوش مصنوعی در هر دو حالت آن، یعنی هدایت شده توسط انسان و هوش مصنوعی خودمختار، موضوعی است که به دلیل برخی مسائل مانند تصادف ماشینهای خودران گوگل و تسلا، مورد بحث قرار گرفته است. مسئولیت مدنی ناشی از استفاده از به کارگیری فناوری های نوین های پیشرفته، به زودی مورد بررسی قرار خواهد گرفت.

بنابراینحقوق فناوری های نوین، به عنوان بخش نسبتا تازه ای از حقوق، می تواند شامل موضوعات متنوعی باشد. موضوعات اساسی که فعالان عرصه فناوری های نوین از منظر حقوقی در ایران درگیر آن هستند، بیشتر شامل مسائل مرتبط با حقوق ماکیت معنوی، جرائم رایانه ای و فضای مجازی و جرایم مرتبط با بهره گیری از فناوری های نوین است. لذا ما در این جزوه و در حد یک درس یک واحدی با عنوان «**حقوق فناوری های نوین**»فقط به مساله حقوق جرائم رایانه ای به عنوان بخشی از حقوق فناوری های نوین خواهیم پرداخت.

تعاریف و مفاهیم

فناوری:فناوری تعریف بسیار گسترده ای دارد که برخی از این تعاریف در ذیل آورده شده است

فناوری روش به کار بردن امکانات، دستگاه ها و ابزار هاست به طوریکه در حوزه تخصصی خود استفاده آسان تر و مفید تری را برای انسان فراهم آورد.

فناوری و یا همان تکنولوژی دانش استفاده از مواد اولیه و خام است

فناوری توانایی و مهارت انجام کار در همه ی زمینه هاست

فناوری یعنی مطالعه منظم و هدفدار و استفاده کاربردی از نتایج به دست آمده برای علومی نظیر صنایع و ...

در تمامی اعصار از ابتدای خلقت انسان، نیروی گرایش به اختراع همواره همراه آدمی بوده است. میل به زندگی راحت تر و انجام سریع تر امور، انسان را وادار به تولید تکنولوژی های جدید و اختراعات نوین نموده و این گرایش هیچ گاه در وجود انسان از حرکت باز نخواهد ایستاد. به همین منظور امروزه شاهد پژوهشگاه های

بسیاری در سرتاسر جهان هستیم که در آن دانشمندان در حوزه های مختلف مشغول بررسی و یافتن فناوری .های نوین هستند

شیوه زندگی امروز ما چنان با فناوری ها ی نوین مختلف در آمیخته که لحظه ای نبود آنها را نمیتوان متصور شد. دایره این فناوری ها آنقدر گسترده و رو به رشد است که ما قطعا از تمامی آنها اطلاعات کافی نداریم ارتباط پایه و اساس تشکیل تمدن ها و فرهنگ ها است. در زمان های دور انسان ها از طریق برقراری ارتباط با یکدیگر به تبادل افکار و اندیشه های خود اقدام کرده و بدین ترتیب پایه های فرهنگ و تمدن جوامع بشری را ایجاد کردند. در تداوم این روند انسان ها برای برقراری ارتباط با یکدیگر به راه های گوناگونی متوسل شدند و وسایل ارتباطی گوناگون را ابداع کردند. با پیشرفت جوامع و تمدن ها، راه های برقراری ارتباط بین انسان ها و ابزارهای ارتباطی نیز تحولات بسیاری یافت. اختراع زبان، خط، چاپ، تلگراف، تلفن و وسایل ارتباط جمعی همانند مطبوعات، سینما، رادیو و تلویزیون سیر تحول راه ها و ابزارهای برقراری ارتباط بین انسان ها را نشان می دهد. راه ها و امکانات برقراری ارتباط بین انسان ها در هر مرحله نسبت به مرحله ماقبل خود تکامل یافته تر شده است. اما امکانات ارتباطی عصر حاضر قابل قیاس با هیچکدام از ابزارهای ارتباطی گذشته نیست. در این گفتار نگاهی به ویژگی ها و خصوصیات فناوری های نوین می اندازیم:

-ویژگی های فناوری های نوین

فناوری های نوین ؛ترکیبی از چندین تکنولوژی شامل وسایل ارتباط جمعی، انفورماتیک و ابزارهای نوین ارتباطات دور است. این مثلث فناوری، انسان ها را در ضبط، ذخیره سازی، پردازش، بازیابی، انتقال و دریافت اطلاعات در هر زمان و مکانی یاری می نماید. فناوری های نوین تکمیل کننده امکاناتی است که وسایل سنتی گذشته ارائه کرده اند.این فناوری ها ویژگی های منحصر به فردی دارند که آنان را از وسایل قدیمی متمایز می سازد. نگاهی می اندازیم به ویژگی ها و خصوصیات فناوری های نوین در عصر حاضر.

تعاملی بودن: یکی از نقایص ابزارها در گذشته، وجود یک رابطه یک سویه و از بالا به پائین بود. به این معنی که اطلاعات در یک جریان یک طرفه ، از بالا به پائین و بدون بازگشت به سوی مخاطبان سرازیر می شد. در این حالت مخاطبان امکان اظهارنظر درخصوص اطلاعات ارائه شده را نداشتند. در عصر گذشته ارتباطات در حد بسیار اندک و ناچیز وجود داشت. اما امروزه به مدد فناوری های نوین، امکان برقراری همزمان ارتباط بین فرستنده اطلاعات و مخاطب فراهم گشته است. در این حالت مخاطبان می توانند بلافاصله پس از دریافت پیام، نظرات خود را به فرستنده پیام منعکس نمایند. تعامل بین فرستنده و مخاطب منجر به فعال شدن مخاطب در جریان ارتباط می شود. در سیستم های ارتباطی نوین، مخاطب از وضعیت انفعالی و کنش پذیری خارج شده و به طور فعال در فرآیند ارتباط مشارکت می نماید

ناهمزمانی: امروزه فناوری های نوین همیشه و در هر لحظه از شبانه روز در اختیار مخاطبان است. برخلاف ابزارهای سنتی گذشته که در یک محدوده زمانی خاص امکان برقراری ارتباط بین فرستنده و گیرنده را

فراهم می ساخت، فناوری های نوین ارتباطی با از بین بردن محدودیت های زمانی، دسترسی به اطلاعات و پیام ها را همیشگی و دائمی نموده اند. بدین ترتیب این فناوری ها اختیار و آزادی عمل بیشتری به مخاطبان داده اند تا اینکه در زمان دلخواه و مورد نظر به دریافت اطلاعات مورد نیاز اقدام نمایند.ناهمزمانی در فناوری های ارتباطی جدید، زمان را در اختیار انسان ها قرار داده است. به عنوان مثال افراد در هر زمان که بخواهند می توانند پیام الکترونیکی خود را دریافت نموده و مشاهده نمایند و یا اینکه پیامی را برای سایرین ارسال نمایند. در هم هستند، در یک زمان خاص حضور ارتباط با سیستم های جدید ارتباطی دیگر لازم نیست تا افرادی که در داشته و در جریان ارتباط قرار گیرند. در واقع ناهمزمانی بخشی از انتقال کنترل از منبع گیرنده در سیستم .ارتباطی است که در آن شرایط کنترل زمان در دست های گیرنده وجود دارد

ظرفیت بالای اطلاع رسانی: امروزه محدودیت هایی که در گذشته درخصوص اطلاع رسانی توسط وسایل ارتباطی وجود داشت از قبیل محدودیت جا در نشریات و محدودیت زمان در رادیو و تلویزیون از بین رفته است. در حال حاضر فناوری های نوین ارتباطی حجم بالایی از اطلاعات را در کمترین فضای ممکن ذخیره و نگهداری می کنند و در هر زمان که نیاز باشد، آن را به مخاطبان ارائه می کنند. حافظه های بسیار بالای رایانه ها امکان نگهداری و پردازش اطلاعات را فراهم می سازند و از طریق «بزرگراه های اطلاعاتی» و با استفاده از فناوری های نوینی همچون «فیبرنوری» آنها را به مخاطبان انتقال می دهند. حجم اطلاعات ارائه شده در فناوری های نوین ارتباطی تا حدی است که امروزه شاهد «اضافه بار اطلاعاتی» هستیم. به این معنا که میزان داده ها و اطلاعات به حدی است که شخص یا سیستم قادر نیست تا از تمامی آنها استفاده کند و یا آن را به جریان بیندازد. یک نمونه از پیشرفت های اخیر در زمینه انتقال اطلاعات، شامل تکنولوژی افزایش پهنای باند امواج (مانند استفاده از الیاف نوری) برای ارسال و دریافت همزمان حجم عظیمی از اطلاعات گوناگون شنیداری، نوشتاری، داده ای و تصاویر است

فردی شدن: در عصر حاضر شاهد تفرق و پراکندگی مخاطبان انبوه هستیم، به طوری که مخاطبانی که در گذشته جهت کسب اطلاعات در یک جا جمع می شدند، امروزه هر کدام به طور جداگانه اقدام می نمایند. فناوری های نوین ارتباطی اطلاعات را برای تک تک مخاطبان ارسال می نمایند و مخاطبان خود را نه به صورت جمع بلکه به صورت فرد در نظر می گیرند.

کنترل از سوی مخاطبان: تا مدت ها، امکان برقراری و قطع ارتباط صرفاً دراختیار فرستنده پیام بود، به طوری که هرگاه فرستنده اطلاعات اقدام به برقراری ارتباط می نمود مخاطبان قادر به دریافت اطلاعات بودند. اما امروزه به مدد فناوری های نوین مخاطبان نیز فارغ از محدودیت های زمانی و مکانی به اطلاعات مورد نظر .دسترسی دارند

تکثر و فراوانی: امروزه ابزارهای ارتباطی به طرزی گسترده در سطح جامعه پراکنده شده و هر کس می .تواند اقدام به ارسال و دریافت اطلاعات نماید

پایگاه های اینترنتی و وبلاگ ها نمونه هایی از این فناوری ها هستند که در دسترس همگان هستند. در حالی که در گذشته ابزارهای ارتباطی و اطلاع رسانی در دست عده ای خاص شامل صاحبان قدرت و نخبگان بود. امروزه همه افراد قادرند به انتشار دیدگاه ها و عقاید خود بپردازند. در واقع تک صدایی در عصر رسانه های سنتی به چند صدایی در «عصر اطلاعات» تبدیل شده است.

نفوذ: فناوری های نوین ارتباطی باعث شده اند تا افراد جامعه تا حد زیادی حریم خصوصی خود را از دست بدهند. حریم و مرزهای ملی و خصوصی کشورها معنی خود را از دست داده اند و اطلاعات با درنوردیدن مرزهای جغرافیایی به گوشه و کنار جهان رسوخ کرده و در خصوصی ترین حریم های افراد وارد می شوند.

تحرک: در گذشته افراد جهت استفاده از ابزارهای ارتباطی از محدودیت مکانی برخوردار بودند به این معنی که در یک مکان مشخص و ثابت می توانستند از ابزارهای ارتباطی بهره مند شوند. اما امروزه فناوری های نوین ارتباطی این امکان را فراهم ساخته اند تا افراد از هرجا حتی در حال حرکت و رانندگی ارتباط برقرار می کنند. گوشی های موبایل، لپ تاپ ها و رایانه های جیبی اطلاعات را در حالت ها و مکان های گوناگون در اختیار افراد قرار می دهند.

تمرکز زدایی: تمرکز زدایی یکی از پیامدهای فناوری های نوین است که بیش از همه مورد اشاره قرار گرفته است.از جمله خرید از راه دور،انجام امور بانکی از راه دور،کنفرانس از راه دور و...

جهان گرایی: فناوری های نوین برخلاف وسایل ارتباط سنتی بعدی فراگیر و جهانشمول دارند. انواع مختلف این فناوری ها از قبیل شبکه های ماهواره ای و اینترنت امروزه ابعادی جهانی یافته اند و تمامی کره زمین را دربرگرفته اند. دیدگاه جهانی فناوری های نوین ، باعث شده تا اطلاعات به راحتی و با سرعت زیاد از مرزهای به شدت حفاظت شده عبور کند. امروزه فناوری های ارتباطی، نظامی غول آسا و بسیار پرقدرت از وسایل ارتباطی گوناگون پدید آورده اند که تحت کنترل کشور خاصی نیست و نظارت، تصحیح مسیر و مداخله در فرآیند سیاستگزاری و برنامه ریزی آن کار بسیار دشواری است.

تبدیل پذیری: خصوصیت دیگرفناوری های نوین ، تبدیل پذیری است. امروزه به راحتی می توان پیام ها را از شکلی به شکل دیگر تبدیل کرد. به عنوان مثال می توان کلام را تبدیل به متن یا تبدیل به تصویر کرد. با استفاده از این خصوصیت، پیام در اشکال گوناگون از قبیل متن، صدا، تصویر و فیلم و یا ترکیبی از آنها تولید می شود.

اتصال پذیری:یکی دیگر از ویژگی های فناوری های نوین اتصال پذیری آنها است. به این معنی که یک فناوری ارتباطی به سادگی قابل اتصال به سایر فناوری های ارتباطی است. در این حالت قابلیت های فناوری

های گوناگون به کمک همدیگر آمده و کار ذخیره، تولید و توزیع اطلاعات را آسان تر می سازد. از نمونه های .اتصال پذیری می توان به اتصال دوربین های هندی کم به رایانه و تلویزیون و انتقال تصاویر به آنها اشاره کرد

جایگاه حقوق فناوری های نوین

استفاده از فناوری های نوین مسائل حقوقی جدیدی را با خود به همراه دارد.این حقوق و مقررات از نیمه دوم قرن بیستم تحت تاثیرفناوری های نوین ابتدا در کشورهای غربی و سپس در کشورهای دیگر جهان مورد توجه قرار گرفته است. در واقع ضرورت مقررات‌گذاری برای تمام فعالیت‌های اجتماعی در جوامع معاصر سبب شده است که در مورد فناوری های نوین نیز مقررات حقوقی ویژه‌ای تهیه و تدوین شود به همین لحاظ برای شناخت .موضوع و قلمرو حقوق فناوری های نوین باید سه نکته را در نظر داشت:

حقوق فناوری های نوین از لحاظ موضوع و قلمرو دارای سه شاخه اصلی است:

حقوق فناوری های نوین جمعی : شامل حقوق مطبوعات ،سینما و رادیو تلویزیون می باشد

حقوق فناوری های نوین دور : حقوق پست ، تلگراف و تلفن وتلفن همراه و ماهواره.

حقوق فناوری های نوین ارتباطی: حقوق ارتباطات الکترونیکی، حقوق انفورماتیک حقوق رایانه ای ، و حقوق اینترنت و فضای مجازی

که ما در این فرصت کوتاه به «**حقوق و قوانین رایانه ای**» به عنوان یکی ازحقوق فناوری های نوین خواهیم پرداخت که به عنوان یک درس یک واحدی در دانشکده های حقوق مورد تدریس اساتید محترم قرار می گیرد.

تعریف حقوق:

واژه حقوق با توجه به کاربردهای متعدد آن دارای معانی خاصی می‌باشد حقوق گاهی در یک معنای وسیع فلسفی مانند اخلاق و عدالت به کار می‌رود از این لحاظ حقوق شامل اصول خاصی است که در روابط افراد حاکم است مانند قواعد مذهبی، قواعد اخلاقی و غیره که هر کدام ضابطه و قانونی بر آن مستقر می‌باشد.حقوق

همچنین شامل مجموع قواعد و مقررات حاکم بر روابط اجتماعی است که از طرف قدرت عمومی وضع و اعمال می‌گردد و دارای ضمانت اجرا هستند این قواعد و مقررات حقوق موضوعه نامیده می‌شود و در هر کشور وضعیت و کیفیت خاص دارد.

طبقه‌بندی حقوق:

1-حقوق طبیعی و حقوق موضوعه

2-حقوق عمومی و خصوصی

3-حقوق داخلی یا ملی و حقوق خارجی یا بین‌المللی

حقوق طبیعی

حقوق طبیعی اصولی است که به عقیده فلاسفه غربی، بطور طبیعی در ذات انسانی سرشته است و جزء لاینفک وجود فرد بشمار می‌رود به همین علت قانونگذار ناچار است به آن احترام بگذارد و از طریق حقوق موضوعه حفظ و حراست آن را تضمین کند. بسیاری از متفکران حقوق طبیعی را براساس نظریات الهی و ماورالطبیعی حقوق مافوق فرمانروایان معرفی می‌کنند و معتقدند که اصول حقوق طبیعی باید بر حقوق موضوعه حاکم باشد و تمام مقرراتی که از طرف قدرت سیاسی برای جامعه وضع می‌شود از آنها الهام بگیرد. مفاهیمی مانند عدالت، ارزش و مقام عالی انسان، تنظیم اجتماعی و منافع عمومی در این قبیل نظریات اهمیت فراوان دارد

حقوق موضوعه

مجموعه قواعد و مقرراتی است که در زمان معین در یک جامعه مشخص و توسط انسانها وضع و اعمال می‌شود این قواعد و مقررات شامل رسوم ، عرف‌ها، قوانین، رویه‌های قضائی و قراردادهای عمومی و شخصی و امثال آنها هستند. تمام این قواعد الزامی و اجباری است. هدف مشترک آنها ایجاد نظم و محدود کردند آزادی مطلق فرد در زندگی جمعی است.

حقوق عمومی، حقوق خصوصی

حقوق موضوعه از قرن‌ها پیش تاکنون به حقوق عمومی و حقوق خصوصی تقسیم می‌گردد. این تقسیم‌بندی که نخستین بار توسط رومیان در قرن سوم میلادی صورت گرفت هنوز با وجودگذشت زمان در

اغلب ممالک رعایت می‌شود. حقوق عمومی شامل قواعد و مقرراتی است که به تشکیلات قدرت سیاسی و منافع عمومی و روابط دولت و افراد حاکم است در صورتی که حقوق خصوصی عبارت است از قواعد و مقرراتی که به روابط و منافع خصوصی افراد در برابر یکدیگر مربوط می‌شود.

حقوق داخلی یا ملی و حقوق خارجی یا بین‌المللی

حقوق عمومی و خارجی عبارت است از قواعد و مقرراتی که بر روابط متقابل کشورها حکومت می‌کند و حقوق بین‌المللی عمومی نامیده می‌شود و در کنار آن چند سالی است که حقوق بین‌المللی ارتباطات نیز اهمیت پیدا کرده است حقوق خصوصی داخلی روابط شخصی افراد در داخل یک کشور را تنظیم می‌کند و شاخه‌های مهم آن حقوق مدنی و حقوق تجارت است. حقوق ارتباطات هم در بعضی از جنبه‌های جزء حقوق خصوصی داخلی است.

بخش اول‌ن؟ نو؟ ها؟ در حقوق فناور؟انه ا؟جرائم را

مقدمه

پیشرفت‌های حاصل در عرصه‌های مختلف علوم و فناوری اگرچه موجب ارتقای سطح زندگی و آسایش بشر است و ظهور رایانه و فناوری اطلاعاتی، زمینه‌های جدیدی را برای تحقیقات جنایی و مجریان قانون فراهم ساخته؛ اما همین پیشرفت‌های سودمند مطمح نظر مجرمان قرار گرفته و آنان نیز از رهگذر فناوری مدرن و علوم نوین، بهره خود را می‌جویند.

امروزه در عصر رایانه و اینترنت، پیشرفت‌های تکنیکی موجب پیدایش اشکال متنوع و جدید مجرمیت شده است و سوءاستفاده از فناوری مدرن اطلاعاتی در سرتاسر جهان اشاعه یافته است. در مقابل، فناوری رایانه و اطلاعات موجب پیدایش و تکوین رشته‌ها و دکترین‌هایی همچون حقوق رایانه، حقوق اطلاعات و حقوق اطلاعاتی کیفری شده است که چند سالی بیشتر از عمرشان نمی‌گذرد و برای اینکه از بنیاد مستحکمی برخوردار گردند باید راه طولانی را طی کنند.

سیستم‌های رایانه‌ای فرصت‌های تازه و بسیار پیشرفته‌ای برای قانون‌شکنی در اختیار مجرمان می‌گذارد و توان بالقوهٔ ارتکاب گونه‌های مرسوم جرایم را به شیوه‌های غیر مرسوم به‌وجود می‌آورد و علاوه بر تحمیل پیامدهای اقتصادی، زندگی انسان‌ها را نیز به مخاطره می‌افکند. توسعهٔ فراملی شبکه‌های بزرگ رایانه‌ای و توانایی دستیابی به بسیاری از سیستم‌ها از

طریق خطوط تلفن معمولی باعث افزایش میزان آسیب‌پذیری این سیستم‌ها و ایجاد فرصت برای سوءاستفاده یا فعالیت‌های مجرمانه می‌شود و عواقب این جرایم می‌تواند موجب خسارت‌های اقتصادی خطرناک و خسارت‌های جدیِ امنیتی برای بشر باشد.

حقوق جزا، علمی است که به بررسی پدیدهٔ جرم از نظر حقوقی و قضایی می‌پردازد و حاوی قواعد و قوانینی است که از جرم و مجازات و کلیهٔ مسائلی که به آنها مربوط می‌شود صحبت می‌کند و جرم‌ها و کیفرهایی را که مناسب آنهاست مشخص ساخته و اجرای این کیفرها را در کشور تنظیم و تنسیق می‌نماید.

تشخیص جرایم و طبقه‌بندی آنها یکی از کمک‌های حقوق جزا به جرم‌شناسی است؛ زیرا برای مطالعه جرایم باید آنها را شناخت و برای آگاه‌شدن از شدت و ضعف اعمال ضد اجتماعی باید آنها را طبقه‌بندی کرد. اولین پدیده ناخوشایندی که با تجمع افراد و شکل‌دادن به یک جامعه، تظاهر پیدا کرد جرم یا بزه بود؛ زیرا گردهم آمدن آنان، سرپیچی و برخوردهای گوناگون را به‌وجود آورد که به نفع افراد و اجتماع نبود؛ جوامع برای ادامه حیات ناچار به گسترش قوانین و مقرراتی در جهت محدودکردن آزادی افراد به نفع اجتماع گردیدند.

با توجه به تحول همه‌جانبهٔ جوامع، به‌خصوص از قرن هیجدهم به بعد، جرایم نیز حالت گسترده‌تری یافتند و با پدیدآمدن هر اختراع جدید بعضی از افراد ناهمگون و نامتناسب با نظام اجتماعی انسان‌ها به استفادهٔ نامطلوب از آن پدیده و درست در جهت عکس حالت سودمندی آن می‌پردازند؛ به عنوان مثال می‌توان از دینامیت که *نوبل* آن را برای کمک به معدنچیان در حفاری‌ها اختراع نمود نام برد که اکنون در جهت کشتار جمعی مورد استفاده قرار می‌گیرد. رایانه نیز از این قاعده مستثنی نیست، مجرمان از این پدیده به‌عنوان وسیله‌ای برای تسهیل ارتکاب جرم استفاده می‌نمایند؛ لذا علمای حقوق جزا باید با هماهنگی علما و متخصصان رایانه تمهیداتی اساسی درخصوص راه‌های بازدارنده از جرم صورت دهند.

1- شناسایی رایانه و اینترنت

1-1- شناسایی رایانه

انسان یک موجود اجتماعی است و همیشه با استفاده از قدرت تفکر و تعقل که مزیت او بر حیوانات بوده در راه پیشرفت و تکامل و توسعه و آسان‌ترکردن کارها گام برداشته است و هیچگاه به امکانات محدود خود اکتفا نکرده و نمی‌کند. از آثار این تفکر می‌توان به اختراع چرتکه و ماشین حساب اشاره کرد که این زمینهٔ فکری به‌تدریج باعث اختراع رایانه گردید. در سال 1833 *چارلز بابیج* طرح ساخت دو ماشین را ارائه داد، یکی برای حل معادلات چند جمله‌ای و دیگری یک دستگاه محاسباتی همه‌منظوره؛ ولی هیچ‌یک از دستگاه‌های مذکور به مرحلهٔ تولید نرسید؛ زیرا فناوری دوران بابیج هنوز به آن مرحله از پیشرفت نرسیده بود که به طرح‌های مدرن او جامهٔ عمل بپوشاند.

در سال1937 *هوارد آیکن*پروفسور دانشگاه هاروارد ماشین خودکار «مارک1» را ارائه دادکه در سال 1944 تکمیل شد؛

اما نخستین محاسبه‌گر الکترونیکی در سال‌های 1939-1946 ساخته شد. این ماشین «انیاک»[1] نام گرفت. وزن این رایانه 30 تن بود و 135 متر مکعب فضا اشغال می‌کرد. با این همه این دستگاه تنها قادر بود 300 عمل ضرب را در یک ثانیه انجام دهد. رایانه‌های نسل نخست از دهۀ 1940 وارد بازار شدند و شمار این نوع رایانه اندک، حجم آن بسیار، قیمت آن گران و شمار افرادی که چگونگی کار با آن را می‌دانستند اندک و دارای امنیت بودند. در سال 1952 ساخت رایانه‌ای به نام «ادواک»[2] به پایان رسید که در آن از پایه 2 به جای پایه 10 استفاده شده بود. همزمان با تکمیل «ادواک» نخستین شرکت‌های رایانه‌ای تجاری پا به عرصۀ وجود نهادند و نخستین رایانۀ تجاری، «یونیواک»[3] نامیده شد.

رایانه‌های نسل دوم که در آنها به جای لامپ خلأ از ترانزیستور استفاده می‌شد از دهۀ 1950 وارد بازار شدند. این نسل از رایانه‌ها از نسل نخست کوچک‌تر، ارزان‌تر و سریع‌تر بودند. نسل سوم رایانه‌ها که به جای ترانزیستور از مدار مجتمع (IC) در ساخت آن استفاده شده بود از اوایل دهۀ 1960 میلادی وارد بازار شد. این رایانه‌ها دارای حجم و قیمت کمتر و قدرت پردازش و ذخیره بیشتری نسبت به نسل‌های پیش بودند.

دهۀ 50 و 60 میلادی دورۀ رواج رایانه و ارائۀ ماشین‌های جدید توسط شرکت‌های مختلف نظیر IBM بود. اوایل دهۀ 60 به خاطر تقاضای بسیار برای رایانه، سازندگان تجهیزات اداری نظیر IBM وNCP و Burroughs شروع به ساخت انواع رایانه نمودند، پیشرفت‌ها و اکتشافات در این زمینه به حدی بود که در اوایل دهۀ 70 شرکت‌های مختلف، رایانه‌هایی کم‌حجم‌تر، ارزان‌تر و با سرعتی چند برابر نسبت به رایانه‌های گذشته ساختند. رایانه‌های شخصی (PC) که نسل چهارم رایانه‌ها به‌شمار می‌روند از اوایل دهۀ 1970 میلادی وارد بازار شدند. از خصیصه‌های ویژۀ این نسل، به‌کارگیری مدارهای مجتمع الکترونیکی در تراکم بسیار کم بود که موجب کاهش فوق‌العادۀ حجم و افزایش قدرت و پردازش آنها شد. رایانه‌های شخصی اولیه، فاقد برنامه بودند. رایانه‌های نسل پنجم از نظر حجم، تفاوتی با رایانه‌های نسل چهارم ندارند. از ویژگی‌های این نسل هوشمندبودن آنهاست. این رایانه‌ها به هوش مصنوعی مجهز می‌باشند، یعنی رایانه می‌تواند فکر کند، میزان و گسترۀ فکر رایانه به برنامه‌ای بستگی دارد که به آن داده‌اند. نسل ششم، رایانه‌هایی خواهد بود که مدارهای داخلی‌شان کپی‌برداری از مغز انسان است‌به‌گونه‌ای که بتوان رایانه را به انجام کارهایی مانند آن وادار کرد. این روند همچنان ادامه دارد و هر روز شاهد ساخت انواع جدیدی از رایانه‌ها با توانایی‌ها و قابلیت‌های خیلی فراوان در بازار هستیم. در رایانه‌های نسل آینده، از فناوری نانو استفاده خواهد شو نانو رایانه‌ها و نانو روبات‌ها در بسیاری از علوم، انقلابی جدید ایجاد خواهند کرد.

تعریف رایانه

1- ENIAC, Electronic Numerical Intogrator and Computer
2- EDVAC, Electronic Diseret Variable automatic Colulator
3- UNIVAC, Universal Automatic Computer

رایانه یک دستگاه الکترونیکی قابل برنامه‌ریزی است که قادر است اطلاعات را ذخیره، بازسازی و تجزیه و تحلیل کند.[۴] رایانه یک دستگاه الکترومغناطیسی، نوری، الکتروشیمیایی، متشکل از سایر تجزیه و تحلیل گرهای اطلاعاتی با سرعت بالاست که عملیات منطقی، ریاضی و ذخیره‌سازی اطلاعات را انجام داده و هرگونه تجهیزات دیگر ذخیره‌سازی اطلاعات و ارتباطی که مستقیماً به آن وابسته‌اند یا در رابطه با آن کار می‌کنند را دربر می‌گیرد. این عنوان شامل ماشین تحریرهای اتوماتیک یا حروفچینی، ماشین‌حساب‌های دستی یا دستگاه‌های مشابه آن نمی‌شود.[۵]

رایانه مجموعه‌ای از سخت‌افزارها و نرم‌افزارها می‌باشد.

الف) سخت‌افزار[۶]

به مجموعه عناصر و مدارهای الکتریکی و الکترونیکی و اجزای مکانیکی و مغناطیسی رایانه، سخت افزار گفته می شو د. به‌عبارتی دیگر کلیهٔ اجزای فیزیکی و قابل لمس رایانه نظیر مدارهای مجتمع (آی سی ها) ترانزیستورها و سایر قطعات الکترونیکی، سیم‌ها، صفحه کلید و سایر وسایل جانبی سخت‌افزار نامیده می‌شود.

ب) نرم‌افزار[۷]

به کلیهٔ برنامه‌های رایانه‌ای، نرم‌افزار گفته می‌شود. یک برنامه، مجموعه‌ای از فرامین (دستورالعمل‌ها) است که به منظور انجام وظیفه‌ی خاص به‌طورمنظم در پی یکدیگر آمدند. برخی از این برنامه‌ها مسئول کنترل و ادامه کا ر رایانه هستند و سیستم‌عامل نامیده می‌شوند، برخی دیگر مسئول ترجمهٔ دستورالعمل‌ها ی زبان های مختلف برنامه نویسی به زبان قابل فهم رایانه هستند و مترجم نام دارند.

گروهی از برنامه‌ها، کمکی هستند که برای افزایش قابلیت و سهولت هر چه بیشتر کار با رایانه طراحی شده اند و برنامه‌های سودمند نامیده می‌شوند. برنامه‌های کاربردی هم گروه دیگری از برنامه‌ها هستند که هر کدام برای انجام وظیفه‌ای خاص طراحی شده و به کمک یک زبان برنامه‌نویسی نوشته شده‌اند.

1- 2- شناسایی اینترنت

الف) تعریف اینترنت

تعدادی رایانه که با رعایت قراردادهای مشترک بتوانند روی خطوط مواصلاتی تبادل اطلاعات نمایند، تشکیل یک شبکه رایانه‌ای را می‌دهند. گاهی شبکهٔ رایانه‌ای می‌تواند رایانه‌های موجود در یک دانشکده یا مرکز پژوهشی را دربر گیر د، به چنین شبکه‌ای که فاصلهٔ بین رایانه‌های مختلف در آن از چند صدمتر تجاوز نمی‌کند، اصطلاحاً شبکهٔ محلی[۸] یا به اختصار LAN می‌گوییم و زمانی که رایانه‌های شبکه در شهرها، کشورها یا حتی قاره‌ها ی مختلف پراکنده اند ، اصطلاحاً شبکهٔ

1- فرهنگ لغات جدید وبستر، به نقل از مجله دادرسی (سازمان قضایی نیروهای مسلح)، ش 2: 47

2- قانون مقابله با روش‌های متقلبانهٔ دسترسی، کلاهبرداری و سوء استفاده از کامپیوتر مصوب 1984 به نقل از مجلهٔ دادرسی (سازمان قضایی نیروهای مسلح) شماره2: 47

3- Hard Ware

4- Soft Ware

1- LAN: Local Area Network

2- WAN: Wide Area Network

گسترده یا WAN[9] گفته می‌شود. هر شبکهٔ گسترده معمولاً نام خاصی دارد که آن را از سایر شبکه‌ها متمایز می سازد؛ مثلاً بیت نت (BITNET) اینترنت (INTERNET)[10] یا ارن (EARN).تفاوت شبکه‌ها ی گسترد ۀ گوناگون اغلب در قراردادهای تبادل اطلاعات، شیوه‌های نشان‌دهی، فناوری مواصلاتی، تسهیلات عرضه‌شده و ح‌وۀ ادارۀ آنهاست.

ب) تاریخچه اینترنت

شبکه‌های رایانه‌ای پس از ساخت رایانه‌های نسل چهارم که قابلیت ارتباط با رایانه‌های دیگر را داشتند به وجود آمدند. استفاده از فناوری شبکه‌های رایانه‌ای و ارتباط میان شبکه‌ها (اینترنت)، موجب انقلاب بزرگی در فناوری اطلاعات و ارتباطات شد.

سابقۀ راه اندازی شبک ۀ اینترنت به شبک ۀ دیگری به نام آرپانت (Arpanet) باز می‌گردد. آرپانت یک شبکهٔ آزمایشی بود که به‌عنوان پروژه‌ای از طرف اتحادیهٔ پروژه‌های تحقیقاتی پیشرفته وابسته به وزارت دفاع آمریکا در سال 1972 میلادی آغاز به کار کرد. این شبکه طی دههٔ 70 از شکل یک پروژهٔ آزمایشی به یک پروژهٔ فراگیر تبدیل شد و ضمن به‌کارگیری ارتباطات ماهواره‌ای رفته‌رفته به‌شکل یک شبکهٔ گسترده درآمد و شبکه‌های بی‌شماری به فکر اتصال به آرپانت افتادند تا بتوانند از امکانات و اطلاعات و احیاناً قدرت و توانایی آن استفاده کنند. به این طریق، اجتماعی از شبکه‌های مختلف با اصول کاری متفاوت به‌وجود آمد که این اجتماع اینترنت خوانده شد.

ویژگی‌های خاص اینترنت عبارتند از:

1- گستردگی طیف اطلاعات موجود؛

2- تنوع خدمات موجود؛

3- بهره‌گیری از تصویر و صدا و متن به‌طور همزمان؛

4- نداشتن انحصار؛

5- روزآمدبودن اطلاعات (up to date).

پ) خدمات موجود در اینترنت

1- اتصال از راه دور Telnet: این امکان کمکی؛ دستیابی ماهواره‌ای به رایانه‌هایی که از لحاظ مکانی دور از یکدیگر هستند

3- Internet: international network
4- Personal Computer

را عملی می‌سازد.

2- پروتکل انتقال‌دهنده پرونده: این امکان کمکی، روشی برای انتقال پرونده به یک رایانه یا از یک رایانه است.

3- پیام‌دهی الکترونیک E.mail: با استفاده از این امکان می‌توان در هر نقطه از دنیا با هر فرد که دارای نشانی پست الکترونیکی باشد به راحتی تماس گرفت. در این تماس می‌توان به همراه انتقال پیام فایل و برنامه را نیز به اشکال مختلف ارسال یا دریافت کرد، دانشمندان از این رسانه جهت تبادل اندیشه و ارسال آثار علمی خود بهره می‌جویند.

4- اخبار News: این امکان کمکی وسیله‌ای جهت توزیع خودکار مقالات بحث‌انگیز (اخبار،گزارش‌ها، اطلاعات و...) برای همهٔ افرادی که خواستار خواندن چنین نکاتی هستند می‌باشد.

5- وب یا جهان‌گستر: شرکت‌ها با اداره چنین خادم‌هایی؛ اطلاعاتی در مورد محصولات خویش ارائه می‌کنند یا محصولات مهیاشده را توزیع می‌کنند. دانشگاه‌ها از این راه فهرست درس‌های خود، اعلان جلسه‌های بحث علمی ، آگهی استخدام ، موضوعات پایان‌نامه کارشناسی ارشد یا موضوع پژوهش‌نامه تحصیلی را در شبکه عرضه می کنند ، این امکان کمکی ، دانشگاه‌ها را در کاستن بار کارهای اداریِشان از طریق کاهش میزان مراجعه به دفترهای اداری دانشگاه یاری می‌کند.

1- 3- کاربردهای رایانه و اینترنت

رایانه و اینترنت با توانایی‌ها و قابلیت‌های فراوانی که دارد دارای کاربردهای متفاوتی است ، امروزه رشته‌ای از امور صنعتی و اداری، نظامی، علمی و... یافت نمی‌شود که رایانه و اینترنت در آن جایی برای خود باز نکرده باشد . استفاده از رایانه و اینترنت، انقلابی در اجتماع امروزی پدید آورده است که برخی اهمیت آن را به مراتب بیشتر از انقلاب صنعتی که در قرن 18 میلادی در اروپا آغاز گردید می‌دانند. رایانه جزئی از زندگی انسان‌ها به‌شمار می‌رود و ادامهٔ روند اجتماعی و رفع نیازمندی‌های جوامع انسانی بدون رایانه تقریباً غیرممکن است. حجم فراوانی از اطلاعات مورد نیاز جامعهٔ امروز با استفاده از رایانه‌ها و شبکه‌های مرتبط به آن تولید، ذخیره، ارسال و توسعه می‌یابد. صنایع تجاری جهان، در روز به تنهایی میلیاردها دلار معامله‌های خود را از طریق رایانه و شبکهٔ جهانی اینترنت انجام می‌دهند. اطلاعات مرتبط با طرح محصولات صنعتی، دارویی، بیمه، پژوهش‌های علمی، آداب اجتماعی، قوانین جاری، دفاع ملی از طریق رایانه‌های شخصی محل‌های کار مجازی و فایل‌های اطلاعاتی، در شبکهٔ عظیم رایانه‌ای در حال استفاده و در گردش می‌باشد.

الف) در مؤسسات و کارخانه‌ها

می‌دانیم که مدیر یک مؤسسه یا مسئول بخشی از یک کارخانه برای تصمیم گیری‌های خود به اطلاعات مختلفی نیاز دارد؛ به‌عنوان مثال، این اطلاعات ممکن است به اقلام بودجهای که وی در اختیار دارد یا مشخصات افرادی که با نظارت او کار می‌کنند مربوط‌شوند این‌گونه اطلاعات معمولاً در یک بانک اطلاعاتی رایانه‌ای که مجموعه ای از اطلاعات سازمان یافتهٔ مربوط به هم است، نگهداری می‌شود. دستیابی به بخشی از این اطلاعات برای پاسخگویی به سؤال مورد نظر به کمک

نرم‌افزارهای مخصوص صورت می‌گیرد و مجموعهٔ این نرم‌افزارها و تسهیلات ذخیرهٔ اطلاعات را سیستم بانک اطلاعاتی می‌گویند. یک سیستم اطلاعات مدیریت در واقع نوع خاصی از سیستم بانک اطلاعاتی است که در آن اطلاعات لازم برای تصمیم‌گیری‌های مدیران یک مؤسسه گردآوری شده‌است. سیستم اطلاعات مدیریت می تواند پاسخگوی سؤال‌های گوناگون مدیران باشد، مثلاً یک مدیر می‌تواند با وارد کردن شرایط احراز یک شغل (مدارج تحصیلی، سوابق کار ، سن و ...) به سیستم، فهرستی از کارمندان واجد شرایط را برای احراز آن شغل به‌دست آورد.

یک انباردار نیز می‌تواند در کار خود از یک سیستم اطلاعاتی مشابهی که در آن مشخصات کالا و میزان موجودی هر کدام ثبت شده‌اند کمک بگیرد هر گاه کالایی از انبار درخواست شود انباردار به کمک رایانه‌ای که در اختیار دارد از کافی بودن موجودی کالا و محل قرار گرفتن آن در قفسه‌های انبار مطلع می‌شود، سپس با فشار دادن کلید خاصی روی رایانه ، خروج کالای درخواستی از انبار را به سی س تم اطلاعاتی اعلام می نماید ، این عمل موجب می‌شود که میزان موجودی آن کالا در حافظهٔ سیستم روزآمد شود.

4- 1- ارتباط حقوق با فناوری رایانه و اینترنت

مصنوعات بشری گاهی دارای آثار عمیق و گسترده در زندگی اجتماعی و اقتصادی انسان بوده و در نتیجه حقوق خاص خود را نیز به‌وجود آورده‌اند. از باب نمونه می‌توان به هواپیما و کشتی اشاره کرد که به‌علت آثار ذکر شده (حقوق هوایی، حقوق حمل و نقل هوایی، حقوق دریاها، حقوق حمل و نقل دریایی و برخی دیگر از مسائل حقوقی و رشته‌های تحقیقاتی در این زمینه) موجب شده‌اند حقوق دولت‌ها و اشخاص خصوصی در ارتباط با دو مصنوع فوق مورد بررسی قرار گیرد.
رایانه نیز از این قاعده مستثنی نیست؛ بلکه به لحاظ اهمیت و تأثیر آن بر زندگی مردم در مرتبه بالاتری
قرار دارد و پیدایش رایانه را بالاتر از انقلاب صنعتی که در قرن هجدهم در اروپا
به وقوع پیوست دانسته‌اند؛ بنابراین باید از دیدگاه حقوقی به مسائل مربوط به آن پرداخت.

این موضوع که پیشرفت رایانه و اینترنت باعث درنوردیده شدن مرزها و مطرح شدن مسائل سیاسی- اقتصادی بین‌المللی می‌گردد، قابل پیش‌بینی است و دولت‌ها را وادار می‌نماید که مبادرت به تنظیم توافق‌های بین‌المللی در این زمینه نموده و حقوق و تعهدات فی‌مابین را معین کنند؛ از این رو با توجه به پیشرفت سریع رایانه و کاربرد آن کلیهٔ حوزه‌ها، بدون تردید باید به تقویت و توسعهٔ حقوق آن نیز توجه کرد تا ضمن حل و فصل مسائل موجود در آینده با حجم بسیار زیادی از مسائل حقوقی در سطوح داخلی و بین‌المللی مواجه نشویم که به دلیل بغرنج و فنی بودن مسئله نتوان از عهدهٔ حل آنها برآمد، بنابراین لازم است همراه با پیشرفت‌های جهانی، در این زمینه نیز گام‌های اساسی برداشته‌شود.
با توجه به قابلیت‌های بسیار بالای اینترنت که مجموعهٔ جهان را به یک شهر کوچک تبدیل نموده دستیابی به اطلاعات مورد نیاز در جای‌جای دنیا با فشاردادن یک کلید، امکان‌پذیر شده است امکان ارتکاب جرایم متعدد و مختلف، چه از دستهٔ جرایم سنتی و چه جرایم مدرن را برای مجرمان فراهم آورده است. به این ترتیب جرایم اینترنتی را می‌توان مکمل

جرایم رایانه‌ای دانست، به‌خصوص اینکه جرایم نسل سوم رایانه‌ای که به جرایم در محیط مجازی (Cyber Crime) [11] معروف است بیشتر از طریق این شبکهٔ جهانی به وقوع می‌پیوندد. هر روز شاهد افزایش قابلیت‌های اینترنت در تمامی زمینه‌ها هستیم؛ که از آن جمله می‌توان به تجارت الکترونیک، تبادل اطلاعات، تبادل فرهنگ‌ها، دستیابی به اطلاعات، قابلیت ایجاد محیط مجازی، گنجینهٔ اطلاعات و ... اشاره نمود. وقوع افعال مجرمانه اشکال گوناگون و سوءاستفاده در هریک از قابلیت‌های فوق متصور می‌باشد.

امروزه به لحاظ استفادهٔ وسیع از رایانه و اینترنت در فعالیت‌های گوناگون بخش‌های مختلف کشور و گسترش قابل پیش‌بینی آن در آینده، به جهت آنکه بهره‌گیری نامناسب از این فناوری در توسعهٔ کشور و روابط با دیگر کشورها و جوامع، امری اجتناب‌ناپذیر می‌باشد؛ لازم است نظام حقوق و قضایی کشور نسبت به مسائل و آثار مختلف حقوقی و جزایی و کاربرد رایانه موضع‌گیری نموده و راه‌حل‌های مناسبی را برای آنها ارائه دهد.

در حال حاضر موضوعات ذیل در رابطه با رایانه در سطح جهان مطرح است:

1- نحوهٔ حمایت از حقوق نرم‌افزار نویسان: این عنوان نیز به نوبهٔ خود به حق تألیف و حق تکثیر [12]، حق اختراع [13] علامت تجاری[14]، اسرار تجاری[15] حقوق استخدام‌کننده و استخدام‌شونده و ... تقسیم می‌شود.

2- خسارت ناشی از کاربرد رایانه: این موضوع در ارتباط با حقوق قراردادها و نیز مسئولیت مدنی (اتلاف و تسبیب و به‌عبارتی دیگر Tort) قابل بررسی است.

3- **اسناد صادره توسط رایانه:** این اسناد به‌وسیلهٔ رایانه تنظیم شده و توسط دستگاه‌های مخابراتی سریعاً به نقاط مختلف جهان ارسال می‌گردند. میزان اعتبار و قابلیت استناد به این‌گونه اسناد با توجه به شدت مواضعی که قوانین کشورها برای هرچه بیشتر اصالت‌بخشیدن به اسناد به‌منظور حفظ نظم عمومی و جلوگیری از تخلفات و اختلافات اتخاذ کرده‌اند قابل بررسی و حائز اهمیت است.

4- جرایم رایانه‌ای و اینترنتی: تحقیق در جرایمی که به این عنوان خوانده شده‌اند از دیدگاه جرم‌شناسی و مجازات‌ها، خود محل بحث جداگانه‌ای دارد.

با توجه به مطالب فوق و همچنین این موضوع که جرایم و مجازات‌ها موضوع بحث حقوق جزا هستند و با در نظر داشتن تحولات به‌وجود آمده در چند دههٔ اخیر و گستردگی استفاده از رایانه و اینترنت در تمامی صنایع و امور روزمره و نیز جنبه‌های مختلف استفادهٔ نامطلوب و غیرقانونی از این پدیده؛ ارتباط حقوق جزا و تبعات آن با فناوری مدرن مشخص می‌شود. امروزه در عصر رایانه و اینترنت، پیشرفت‌های تکنیکی موجب پیدایش اشکال متنوع و جدید مجرمیت شده‌اند؛

1- برای اطلاع بیشتر- ر.ک گاتچالک، پیتر، سامانه‌های مدیریت دانش در خدمت پلیس- مترجمان صدیقه نظری و دکتر مهدی نوروزی خیابانی: 172-169 و 221.

2- Copyright
3- Patent Ability
4- Trade mark
5- Trade secretly

لذا وظیفهٔ علمای جزا این است که راه‌هایی برای قانونگذاری ارائه نمایند که هم حقوق این پدیده جدید رعایت گردد و نیز مانعی برای ارتکاب جرم به‌وسیلهٔ این صنعت جدید توسط مجرمان باشد.

2- تعاریف و تحولات قوانین جرایم رایانه‌ای و اینترنتی (سایبری)

2- 1- تعریف جرم رایانه‌ای

تاکنون بحثهای بسیاری در میان کارشناسان در زمینهٔ اعمال تشکیل‌دهندهٔ جرایم رایانه‌ای یا جرایم مرتبط با رایانه در جریان بوده، حتی پس از گذشت سال‌ها هنوز هم یک تعریف به رسمیت شناخته شده بین‌المللی برای این اصطلاحات وجود ندارد. تعاریف ارائه شده از سوی بعضی متخصصان گاهی رهیافت تکنیکی و گاهی رهیافت حقوقی دارند. تعاریف ارائه شده کارکردی بوده و با توجه به محدودهٔ زمانی و تحولات فناوری اطلاعات و رایانه بیانگر پیشرفت و تحول فناوری و جرم رایانه‌ای است. در اینجا به ذکر چند نمونه می‌پردازیم:

سازمان همکاری و پیشرفت اقتصادی (OECD) جرم رایانه‌ای را چنین تعریف کرده است: «سوءاستفاده از رایانه شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار و انتقال داده می‌شود.[۱۶]

یکی از متخصصان شورای اروپا جرم رایانه‌ای را چنین تعریف نموده است: هر فعل مثبت غیرقانونی که در آن رایانه، ابزار یا هدف ارتکاب جرم است.[۱۷] پلیس ملی ژاپن نیز بیان داشته؛ جرایم متضمنِ اعمال توأم با بی مبالاتی یا حوادثی که موجب تخریب عملکرد سیستم رایانه یا استفادهٔ غیرقانونی از آن باشد، جرم رایانه‌ای است.[۱۸]

پروفسور شیک از اتریش جرم رایانه‌ای را چنین تعریف می‌کند: به‌طور کلی جرم رایانه‌ای عبارت است از هر عمل مجرمانه‌ای که رایانه وسیلهٔ ارتکاب یا راه ارتکاب باشد.[۱۹]

در حالی که مجادلات پیرامون جرایم رایانه‌ای در میان صاحب‌نظران ادامه داشت نوع جدیدی از جرایم رایانه‌ای تحت‌عنوان Cyber Crime در حال شکل‌گیری بود. پیدایش و شیوع این نوع جدید برپیچیدگی و دشواری تعریف کامل از جرم رایانه‌ای افزود و خود به شکلی نو تبدیل شد.

2- 2- تعریف جرم سایبر

برای درک مفهوم جرم سایبر و تفاوت آنها با سایر جرایم رایانه‌ای، درک تعریف محیط سایبر[۲۰] و ویژگی‌های آن ضروری است. Cyber از لحاظ لغوی در فرهنگ‌های مختلف به‌معنی مجازی و غیرملموس می‌باشد. از محیط سایبر تعاریف گوناگونی به‌عمل آمده که به ذکر چندنمونه از آنها اکتفا می‌شود:

1- محیط سایبر، اجتماعی شکل‌گرفته از رایانه‌های شبکه‌های رایانه‌ای و کاربران است؛ بنابراین یک دنیای مجازی است که کاربران

1- خبرنامه انفورماتیک (نشریه تخصصی- خبری شورای‌عالی انفورماتیک کشور) ش 58، 157

2- مجموعه سخنرانی‌های حقوق کامپیوتر، آذر 75

3- همان

4- خبرنامه انفورماتیک ش 58، 158

5- Cyber Space

آن وقتی که آنلاین[۲۱] هستند، موجودیت پیدا می‌کنند.

2- محیط سایبر، جایی است که شما هنگامی که با تلفن صحبت می‌کنید هستید.

3- محیط سایبر، توهم و تصور باطل توافقی است که انسان‌ها خلق کرده‌اند.

در این محیط اشیا و اطلاعات به‌صورت فیزیکی و ملموس وجود ندارند و در واقع آنچه در صفحه مانیتور مشاهده می‌شود موضوعات مجازی می‌باشد که به‌صورت دیجیتالی وارد شبکه شده است. برای آنکه شخصِ کاربر وارد فضای سایبر از طریق شبکهٔ اینترنتی شود باید پس از فراهم‌نمودن تجهیزات اولیه و رایانه، مودم و خطوط مخابراتی به شبکه وصل شده (Online) و پس از آن آدرس و سایت موردنظر خود را انتخاب نموده و با توجه به نوع و موضوع و هدف خود به بررسی و یا انجام اقداماتی در آن بپردازد.

با توجه به تعاریف فوق می‌توان در مجموع محیط سایبر را چنین تعریف نمود: «محیطی است مجازی و غیرملموس موجود در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاهراه‌های اینترنت به هم وصل هستند) که در آن تمام اطلاعات راجع به افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هر آنچه که در کرهٔ خاکی به‌صورت ملموس و فیزیکی وجود دارد در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل‌استفاده و دسترس استفاده‌کنندگان و کاربران می‌باشد و از طریق رایانه، اجزای آن و شبکه‌های بین‌المللی به هم مرتبط می‌باشند.»

به‌تدریج افراد بشر دریافتند برای ادامهٔ حیات اجتماعی خود باید از دنیای فیزیکی؛ به دنیای نو پدید و هم ارز آن، یعنی فضای سایبر کوچ کنند؛ زیرا کارآیی و اثربخشی امور آن با دنیای فیزیکی به هیچ وجه قابل مقایسه نیست. در این میان پدیدآورندگان فناوری دنیای جدید سایبر، بحث همگرایی و یکپارچگی[۲۲] تمام ابزارهای اطلاعاتی و ارتباطی را مطرح کردند، گرچه مدت زمان زیادی از ابراز این دیدگاه نمی‌گذرد؛ اما به آن جامه عمل پوشاندند به ویژه در کشورهای توسعه‌یافته، «با هر وسیلهٔ سادهٔ ارتباطی- الکترونیکی می‌توان به دنیای بیکران سایبر متصل شد و از امکانات بی‌پایان آن بهره گردید.»[۲۳] بدون وجود تعریفی از جرم سایبر در فرهنگ لغت ها، قانونگذاران و مجریان قانون در سراسر جهان جرم سایبر را درک کرده‌اند وقتی آن را می‌بینند می‌شناسند. انتشار ویروس‌ها و کرم‌های رایانه‌ای انجام حملات الکترونیکی و به‌طور کلی هرگونه فعالیتی که سبب ایجاد اخلال در شبکه‌های رایانه‌ای، امور مبتنی بر آن شود، جرایم الکترونیکی یا در بیان کلی‌تر، جرایم سایبری[۲۴] نامیده می‌شوند. جرایم سایبری را در معنی جامع می‌توان به هر گونه فعالیتی که به‌منظور انجام تبهکاری شبکه‌های رایانه‌ای به خدمت می‌گیرد، اطلاق نمود.

بر اساس تعریف فوق، اقداماتی چون حمله الکترونیکی به زیر ساخت‌های حیاتی و ملی کشورها، کلاهبرداری، پولشویی الکترونیکی، استفادهٔ جنایتکارانه از اینترنت، جعل ID و حتی استفاده از رایانه و مفاهیم فناوری اطلاعات در جریان

6- On line

1- Convergenee

2- به تدریج با فراگیرشدن نسخه ششم پروتکل اینترنت (IPV6)، محدودیت‌های فنی پیش‌روی این همگرایی برچیده خواهد شد این پروتکل با وجود برخورداری از بی‌نهایت آدرس، با شماره شبکه‌ای، می‌تواند به هر شی و موجودی در دنیای خاکی هویتی مجازی اعطا کند که به این ترتیب زیربنای لازم برای حضور همگانی در فضای سایبر مهیا خواهد شد. (برای مطالعه بیشتر در این‌باره ر.ک کاشیان، علیرضا و دیگران (مترجم) 1382- راهبری اینترنت، مشارکت فراگیر، دبیرخانه شورای عالی اطلاع‌رسانی: 318).

1- کشتر، نیر، مترجم بهروز حاجیان- نگاهی به جنایات و تبهکاری الکترونیکی این گروه خشن- منبع روزنامه شرق 85/6/14

جنایات غیر سایبری مصداق‌هایی از جرایم سایبری است. در کل می‌توان گفت که جرم سایبری زیرمجموعهٔ جرم رایانه‌ای است.

1- گستره جرایم سایبری

از لحاظ تاریخی می‌توان گفت در اواسط دههٔ90 با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای نسل سوم، جرایم رایانه‌ای تحت عنوان جرایم سایبر مجازی یا جرایم در محیط سایبر شکل گرفته است. با گسترش فناوری اطلاعات در بخش‌های مختلف امور اجتماعی و توجه بیشتر به مفاهیمی چون دولت و تجارت الکترونیکی و به‌طور کلی توسعه دنیای مبتنی بر رایانه‌ها در تعاملات اداری، جرایم سایبری نیز گسترش یافته و با افزایش بهرهٔ مالی و اقتصادی آنها از پیچیدگی بیشتری برخوردار می‌شوند. طبق گزارشFBI در ژوئن سال 2002 میلادی در هر لحظه به‌طور متوسط 500 کمپانی مورد حملهٔ جنایتکاران سایبری قرار گرفته‌اند. در گزارشی دیگر به نقل از وال استریت ژورنال در شمارهٔ ژولای گذشته میلادی، 53٪ از دادخواهی ملی مالی ارائه‌شده به کمیسیون بازرگانی ایالت متحده در سال 2004 میلادی مربوط به جرایم الکترونیکی بوده‌اند. افزایش جرایم سایبری و حملات انجام‌شده علیه شرکت‌ها و مؤسسات آمریکایی به حدی است‌که دولت آن کشور و FBI مسئلهٔ مبارزه و مقابله با آن را به‌عنوان یکی از اولویت‌های اصلی خود پس از ضد تروریسم و ضد جاسوسی قرار داده است.[۲۵]

جرایم سایبری وابسته به مکان نبوده و از درجهٔ جهانی بودن بالاتری نسبت به سایر گونه‌های جرم و جنایت برخوردارند. یکی از مشخصه‌های جرایم سایبری در مقایسه با روش‌های جاری تبهکاری، عدم وابستگی آنها به محل و منطقه بومی مجرمان است. مرزهای جغرافیایی برای جانیان محدودیتی محسوب نمی شود و همان طور که فناوری اطلاعات، ارتباطات را آسان‌تر، فواصل را کوتاه‌تر و تعاملات را بیشتر می‌کند، فعالیت مجرمان نیز در این دنیای جدید آسان می‌شود. گمنامی موجود در این فضا در کنار عدم وابستگی به مکان، کشف جرم و جنایت در دنیای سایبری را بسیار پیچیده کرده و هرگونه کوشش باز دارنده و پیشگیرانه را در این حوزه مشکل و باعث عدم تشخیص بموقع و تسهیل در باج‌خواهی و درخواست نامشروع مجرمان این جرایم می‌شود.

در بسیاری از موارد، هدف تبهکاران الکترونیکی، نفوذ و دسترسی به اسناد محرمانه پایگاه اطلاعاتی شرکت خاص نیست؛ بلکه تنها جلوگیری از دسترسی کاربران و مشتریان برای مدتی محدود نیز ممکن است خسارت قابل‌توجهی را به قربانی تحمیل کند. حملاتی از این نوع‌که بیشترین حملات رایانه‌ای انجام‌شده طی سال‌های اخیر است Dos Attack یا حملات جلوگیری از دسترسی نام دارند[۲۶].

در محیط سایبر، افراد با هوشیاری غیرواقعی و تنها براساس تخیلات شخصی در محیط رسانه‌ای اینترنت حاضر می‌شوند و در هر قالب و عنوانی خود را معرفی و با دیگران ارتباط برقرار می‌کنند. حضور پررنگ و بی‌شمار افراد مختلف از قشرهای گوناگون جامعه در شبکه‌های بین‌المللی «اینترنت» باعث شده است انواع جدیدی از جرایم رایانه‌ای وارد فرهنگ حقوق جزا شود که این جرایم هم شامل جرایم کلاسیک و جرایم نسل اول رایانه‌ای و هم یکسری جرایم بسیار

1- کشتر، نیر، مترجم بهروز حاجیان- نگاهی به جنایات و تبهکاری الکترونیکی این گروه خشن

2- شورای عالی انفورماتیک کشور، مجموعه سخنرانی‌های حقوق کامپیوتر، آذر 75

جدید و منحصر به جرایم واقع شده‌در محیط سایبر است که می‌توان به تطهیر نامشروع پول (پولشویی الکترونیکی)[۲۷]، پورنوگرافی کودکان و خرید و فروش مواد مخدر اشاره نمود. انواع دیگر جرایم سایبری را می‌توان به شرح ذیل احصا نمود:

1- جرایم سنتی در محیط دیجیتال شامل: جاسوسی، جعل، کلاهبرداری، تخریب، افترا؛

2- جرایم ناظر به کپی رایت برنامه‌ها؛

3- جرایم علیه حمایت از داده‌ها؛

4- جرایم در تجارت الکترونیک (پرداخت‌های الکترونیکی)؛

5- جرایم بانکداری الکترونیک؛

6- جرایم مخابراتی (ماهواره‌ای)؛

7- جرایم علیه محتوا؛

8- سایبر ترور (جرایم علیه امنیت ملی و بین‌المللی).

در اینجا به چند نمونه از جرایم در محیط سایبر می‌پردازیم:

1) افترا و نشر اطلاعات از طریق پست الکترونیک: هر کاربر می‌تواند به‌وسیلهٔ شبکه‌های بین‌المللی از طریق یک آدرس مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به آسانی در آن تقلب کرد. این قابلیتِ پست الکترونیک می‌تواند ابزاری برای نشر و اطلاعات مجرمانه یا نشر اکاذیب و افترا به اشخاص باشد و احتمال کنترل اطلاعاتی برای تهیه‌کننده خیلی مشکل است.

2) پولشویی رایانه‌ای: مصادیق این جرم جدید در فضای سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد و نحوهٔ ارتکاب به این نحو است که باندهای بزرگ نامشروع توسط پست الکترونیک یا اینترنت بدون هیچ‌گونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخصی معینی را می‌نمایند و در تقاضای خود نحوهٔ ارسال پول و دستمزد و مدت استرداد را بیان و در صورت قبول طرف، نوع و نحوهٔ تضمینات لازم را اعلام می‌دارند و اصولاً در زمان استرداد پول، یک عنوان مشروع در تجارت الکترونیک را با منشأ تجاری انتخاب و با هدف خود هماهنگ می‌نماید.

3) سایبر ترور: امروزه برخی اقدامات تروریستی توسط دسترسی به اطلاعات حفاظت‌شده صورت می‌پذیرد و تروریست‌های اطلاعاتی فقط با استفاده از یک صفحه کلید و یک موس رایانه می‌توانند به صورت غیرمجاز وارد سیستم‌های رایانه‌ای

3- Cyber Laundering

امنیتی شوند؛ به‌عنوان مثال، با تداخل در سیستم ناوبری هوایی باعث سقوط هواپیما شده یا باعث قطع برق سراسری یا مسموم‌کردن منابع غذایی می‌شوند.[۲۸]

4) قاچاق مواد مخدر: با توجه به گسترش ارتباطات در محیط سایبر و دسترسی آسان افراد به هم از طریق پست الکترونیکی و اینترنت، هرگونه قاچاق موادمخدر اعم از خرید، فروش، پخش، توزیع، یافتن واسطه‌ها و مصرف‌کنندگان از طریق شبکه‌های رایانه‌ای انجام می‌شود. از ویژگی‌های آن حذف و کمتر نمودن واسطه و توزیع کنندگان و گسترش دامنهٔ فعالیت قاچاقچیان تا سطح بین‌المللی و جذب مشتریان بیشتر می‌باشدضریب اطمینان قاچاق مواد مخدر از طریق ارتباطات رایانه‌ای و شبکه‌ای بالاتر از نوع سنتی آن است.

5) سوءاستفاده از کودکان: بزهکاران اینترنتی از موقعیت و سادگی کودکان استفاده و سعی می‌کنند آنها را از طریق اتاق‌های چت (Chat)[۲۹] و پست الکترونیک به انحراف کشانده و در نهایت از آنان سوءاستفادهٔ جنسی به صورت پورنوگرافی کنند و تصاویر آنها را روی سایت‌های مستجهن منتشر سازند. طبق آمارهای ارائه شده از هر 5 کودک در آمریکا، یک کودک با موضوعات جنسی در اینترنت برخورد مستقیم داشته است،
از طرف دیگر 77٪ قربانیان جرایم اینترنتی سنی زیر14 سال دارند و 22٪ قربانیان نیز 10 تا 13 سال سن داشته‌اند.

2- تمایز بین جرایم رایانه‌ای و اینترنتی

استفادهٔ عمودی از فناوری برتر، زمانی رخ می‌دهد که رایانه یا شبکهٔ رایانه‌ای، خود هدف فعالیت‌های جنایی قرار گیرد. ارسال پیام‌ها و ایمیل‌های مزاحم، رخنه‌گری و پخش کدهای مخرب در اینترنت فقط نمونه‌های اندکی هستند که در آنها وجود رایانه برای وقوع جرم از اهمیت بالایی برخوردار است . استفاد ۀ افقی از فناوری‌های برتر همگانی، زمانی اتفاق می‌افتدکه رایانه به‌عنوان یک ابزار برای تسهیل اهداف جنایی به‌کار گرفته می‌شود. به این ترتیب، جرایم اینترنتی را می‌توان مکمل جرایم رایانه‌ای دانست، به‌خصوص اینکه جرایم نسل سوم رایانه‌ای که به جرایم در محیط مجازی (Cyber Crima) معروف است اغلب از طریق این شبکهٔ جهانی به‌وقوع می‌پیوندد.

2- 3- تحولات جرایم رایانه‌ای و اینترنتی

الف) تاریخچه

به‌طور کلی تحول تاریخی جرایم رایانه‌ای را از زمان پیدایش رایانه تا اوایل هزاره سوم می‌توان به سه نسل طبقه‌بندی نمود. نسل اول این‌گونه جرایم که تا اواخر دههٔ 80 میلادی مصداق داشت، تحت‌عنوان جرایم رایانه‌ای بیان گردید که بیشتر شامل سرقت و کپی‌برداری از برنامه‌ها و جرایم علیه حریم خصوصی در رایانه بوده که با گسترش فناوری تبادل

1- سلمانی‌زاده، دکتر محمود، جنگ اطلاعات و امنیت- خبرنامه انفورماتیک ش 80: 20

2- مکالمه نوشتاری که در دههٔ اخیربصورت تصویری و صوتی از طریق رایانه و شبکه‌های بین‌المللی ارتباطی می‌باشد.

اطلاعات و ارتباطات بین‌المللی در دهۀ 90، جرایم نسل دوم تحت‌عنوان جرایم علیه داده‌ها، جلوۀ بیشتری پیدا نمود؛ به‌طوری که در این دهه تمامی جرایم علیه فناوری اطلاعاتی، ارتباطاتی رایانه‌ای، ماهواره‌ای و شبکه‌های بین‌المللی تحت‌عنوان جرایم علیه داده اطلاق می‌شود. در اواسط دهۀ 90 با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرایم رایانه‌ای، تحت‌عنوان جرایم سایبر (مجازی) یا جرایم در محیط سایبر شکل گرفته است که با توجه به ماهیت خاص خود بیش از هر زمانی نظامات حقوقی را به‌خصوص در حقوق جزای ماهوی و حقوق جزای بین‌الملل و آیین‌دادرسی دچار چالش‌های جدی نموده است.

فناوری رایانه را باید بستر و زیربنای تخلفات و جرایم رایانه ای و جرایم مرتبط با رایانه دانست و جرایم در اینترنت (شبکۀ بین‌المللی)، جرایم علیه دیتا (داده‌ها) در محیط سایبر، جرایم مولتی مدیا (چندرسانه‌ای) و انواع مشابه آن توسط فناوری رایانه قابل تحقق است. پس در شبکۀ جهانی اینترنت به عنوان یکی از مظاهر فناوری اطلاعات رایانه زیربنا و شاهراه بسیاری از تخلفات و جرایم رایانه‌ای می‌باشد.

ب) موارد پیدایش

1- در ایران: وقوع جرم رایانه‌ای در ایران را نمی‌توان همزمان با ورود رایانه به ایران دانست (یعنی سال 1340)؛ زیرا کاربرد آن در سال‌های اولیه بسیار محدود بود. در دهه‌های 50 و60 کم‌کم بر تعداد رایانه و نیز بر وسعت برنامه‌های رایانه‌ای افزوده شد.

با توجه به پیشرفته‌نبودن نوع کارکرد و عدم کاربرد رایانه در اکثر بخش‌ها نمی‌توان برای جرم رایانه‌ای عمر زیادی قائل بود. هر چند در نبود تعریفی مشخص از جرم رایانه‌ای نمی‌توان گفت نخستین جرم در چه زمانی اتفاق افتاد. سوءاستفاده از رایانه برای ارتکاب جرایم سنتی، به‌کارگیری ویروس از طریق توزیع حامل‌های داده آلوده به ویروس، سوءاستفاده‌های مالی و تکثیر و غیرمجاز نرم‌افزارهای رایانه‌ای از جمله جرایم رایانه‌ای که در مقیاس بسیار اندک در دهۀ 70 واقع شده و با قوانین کیفری مرسوم مورد رسیدگی قرار گرفتند.[۳۰] از نیمۀ دوم دهۀ 70 ارتکاب جرایم رایانه‌ای رشد نسبتاً سریعی داشته است؛ به‌عنوان نمونه در روز 26 خرداد ماه 1378 یک دانشجوی رایانه و یک کارگر چاپخانه در کرمان، چک‌های تضمینی را جعل کرد. بعد از آن موارد دیگری نیز در این رابطه بعنوان جرم رایانه‌ای به ثبت رسیده که مهم‌ترین آنها اختلاس بوده است‌جعل اسکناس، اسناد و بلیط‌های شرکت اتوبوسرانی، جعل اسناد دولتی از قبیل گواهینامه رانندگی، کارت پایان خدمت، مدرک تحصیلی، اوراق خرید و فروش موتورسیکلت، جعل چک های مسافرتی و عادی نمونه‌هایی از جرایم رایانه‌ای در ایران است.در حال حاضر بیشترین فراوانی جرایم رایانه‌ای مربوط به موضوعاتِ دسترسی غیرمجاز؛ هتک حیثیت و افترا و نشر اکاذیب و کلاهبرداری اینترنتی می‌باشد که با انگیزه‌های کسب منافع

1- دادنامه مورخ 1372/4/3 شعبه 65 دادگاه کیفری تهران یکی از آرایی است که بیانگر به‌کارگیری قوانین کیفری سنتی در خصوص جرایم رایانه‌ای است (برای اطلاع بیشتر ر.ک: خبرنامه انفورماتیک ش53: 27 و 28)

مالی، مسائل ضداخلاقی، انتقام‌جویی و تسویه‌حساب‌های فردی و گروهی و نیز کنجکاوی و سرگرمی و اثبات توانایی مرتکبین صورت می‌گیرد.

2- در سایر کشورها: دربارهٔ پیدایش اولین جرم رایانه‌ای نظرات مختلفی ابراز شده است. به نظر اغلب مؤلفان، دههٔ 1960، دههٔ بروز اولین موارد جرم رایانه‌ای است؛ چون فناوری رایانه رشد سریع خود را از دههٔ 50 شروع کرده و بر اساس همین عقیده کشف و پیدایش قضیه *الدون رویس* نقطهٔ شروع بحث پیرامون جرم رایانه‌ای تلقی می‌شود. رویس در سال 1961 به‌دنبال بروز اختلاف با مسئولان شرکتی که در آن کار می‌کرد تصمیم به انتقام گرفت و با تغییر در برنامه محاسباتی صورت هزینهٔ شرکت درصدی از درآمد حاصله را برای خود برداشت و اینجا بود که خبر وقوع اولین جرم رایانه‌ای به‌طور رسمی انعکاس یافت و خود واقعه نیز تحت تعقیب مراجع قضایی قرار گرفت.

در اتریش، دههٔ 1980 با ازدیاد کاربرد رایانه، به تبع آن با افزایش تعداد جرم رایانه‌ای همراه بوده است. در این کشور در خلال سال‌های 1970 تا 1979 پنج مورد جرم رایانه‌ای کشف شد؛ ولی در دههٔ 80 تعداد ارتکاب جرایم چندین برابر شد؛ به‌طوری که در سال 1982، 32 فقره جرم رایانه‌ای گزارش شده‌است.

گزارش اولین جرم رایانه‌ای در برزیل در سال 1988 بود. در کانادا سال 1970 را سال بروز اولین موارد یاد می‌کنند؛ اما از نظر قضایی و از دیدگاه رسمی این کشور، سال 1980 که دعوی *مک‌لاگین* مطرح و رأی آن صادرشد، اولین سنگ بنای جرم رایانه‌ای محسوب می‌شود.

در چین نیز اولین جرم رایانه‌ای در سال 1986 بروز کرد. هلند در سال 1971 با چندین مورد از گزارش‌های جرایم رایانه‌ای مواجه گردید و از آن پس با این معضل روبه‌رو شد[۳۱].

2-4- بررسی تحولات قوانین کشورها

پس از پیدایش اولین جرم رایانه‌ای با به خطر افتادن حقوق فردی، مباحث نظری تحت عنوان حمایت از داده‌ها آغاز گردید؛ اما در دههٔ 1970 شاهد بروز اولین مطالعات جرم‌شناسی پیرامون جرایم رایانه‌ای هستیم اگر چه محدودهٔ مطالعات گسترده نبود؛ ولی در همان زمان نحوهٔ ارتکاب جرم رایانه‌ای تنوع یافت. در همین دهه تحقیقات علمی بر جرایم اقتصادی مرتبط با رایانه به‌خصوص سوءاستفادهٔ رایانه‌ای، تخریب رایانه‌ای، جاسوسی رایانه‌ای و سرقت نرم‌افزار متمرکز شد.

در دههٔ 1980 شاهد تغییرات بنیادین در دیدگاه‌های عمومی و علمی بودیم. موج وسیع سرقت برنامه‌ها، تخلفات صندوق‌داران و سوءاستفاده‌ای ارتباطات مخابراتی و ... آسیب‌پذیری جامعهٔ اطلاعاتی را آشکار کرد و نیاز تدوین راهبردی جدید برای مبارزه با جرم رایانه‌ای را به اثبات رساند[۳۲]. در همین راستا اولین موجِ اصلاح حقوق در بیشتر نظام های

1- خبرنامه انفورماتیک، منبع پیشین: 155

1- مجموعه سخنرانی‌های حقوق کامپیوتر، آذر 75

قضایی در زمینهٔ حمایت از اطلاعات خصوصی در دههٔ 1970 و 1980 بر حمایت از حقوق شخصیت ظهور کرد.

دومین موج عمدهٔ اصلاح قوانین مربوط به جلوگیری از جرایم رایانه‌ای اقتصادی بود. این قانونگذاری جدید از آن جهت ضروری بود که جرایم اقتصادی مربوط به رایانه نه تنها شامل موارد مرسومی بود که توسط حقوق کیفری در برگرفته می‌شد؛ بلکه مربوط به اشیای غیرملموس (مانند برنامه‌های رایانه‌ای) یا روش‌های جدید ارتکاب جرم (مثلاً دستکاری رایانه) می‌شد. خیلی از کشورها به‌جای بسط جملات قوانین پیش‌بینی‌شدهٔ قبلی به وضع قوانین جدید دربارهٔ جرایم رایانه‌ای اقتصادی (شامل دستیابی غیرقانونی به سیستم‌های رایانه‌ای) پرداختند.

در دههٔ 1980 موج سوم اصلاح قوانین بوقوع پیوست و به صراحت برای برنامه‌های رایانه‌ای، حق تألیف (کپی رایت) قائل شدند. در همین زمان، بسیاری از دولت‌ها دست به اصلاح حقوق کیفری زدند و قوانینی برای حق تألیف تصویب شد. علاوه بر این در این دهه، انواع جرایم جدید رایانه‌ای و به تبع آن گسترش مباحث بروز کرد، به این صورت کهٔا قبل از این دهه، جرایم اهداف مالی را دنبال می‌کرد؛ اما در این دهه مسائلی مربوط به اشخاص و امنیت و آسایش عمومی نیز بدان افزوده شد. دههٔ 90 را می‌توان دهه شکل‌گیری چارچوب و عناوین و محتوای حقوق اطلاعاتی، کیفری دانست. در این دههٔ دکترین‌های مسئولیت کیفری، جرایم در شبکه‌های پیوسته، مسائل خاص اینترنت و... سیر تکاملی خود را طی می‌کنند.

موج چهارم اصلاح قوانین دربارهٔ سری جدید مقررات آیین دادرسی است.

موج پنجم در خصوص وضع قوانین در رابطه با اقدامات پیشگیرانهٔ غیرکیفری برای کنترل جرایم رایانه‌ای و اینترنتی می‌باشد که می‌توان به توصیه‌های کنفرانس انجمن بین‌المللی حقوق کیفری (AIDP) در مورد جرایم رایانه‌ای و دیگر جرایم فناوری اطلاعات (1994) و قطعنامهٔ سازمان ملل متحد در کنگرهٔ هشتم (1990) و کنگرهٔ دهم (1997) اشاره کرد.

در ایران از اواخر دههٔ 1360 مواردی از تخلفات رایانه‌ای به‌صورت کپی و تکثیر غیرمجاز نرم‌افزارها نمود پیدا کرد که تا اواسط دههٔ 70 نیز اکثر تخلفات رایانه‌ای به‌صورت عدم ایفای تعهد توسط شرکت‌های طرف قرارداد بود که خود نیز ممکن است ناشی از سوءنیت و قصور متعهد و یا عدم تبیین دقیق موضوع تعهد در قرارداد باشد. در این ایام قانون حاکم به رفع اختلاف، قانون حمایت از حقوق مؤلفان و محققان و هنرمندان مصوب 1348 بود.

با توجه به گسترش رایانه و فناوری اطلاعات در ایران با گسترش تخلفات مرتبط با کپی و تکثیر غیرمجاز نرم‌افزارها و برنامه‌های رایانه‌ای سرانجام پس از سال‌ها بحث و بررسی، قانون «حمایت از پدید آورندگان نرم‌افزارها و رایانه» در دی‌ماه 1379 به تصویب رسیده از طرف دیگر با شیوع و وقوع جرایم مرتبط با رایانه و شبکهٔ جهانی اینترنت مقامات قضایی را بر آن داشت که قانون جرایم رایانه‌ای را تدوین و برای تصویب در اختیار مجلس شورای اسلامی قرار دهند که بالاخره پس از گذشت 15 سال این قانون به تصویب رسید، مقامات قضایی و انتظامی در جهت مبارزه و پیشگیری از جرایم رایانه‌ای اقداماتی در خصوص آموزش نیروی متخصص به‌عمل آوردند که به‌عنوان مثال می‌توان به برگزاری همایش‌های تخصصی بررسی جرایم رایانه‌ای و بررسی جنبه‌های حقوقی و فناوری آن در سال‌های 1380 و 1383 اشاره نمود.

مسئله‌ای که در اینجا ممکن است در بررسی مباحث جرایم رایانه‌ای و اینترنتی مانند سایر جرایم مورد سؤال واقع

شود این است که موضوع جرم رایانه‌ای چیست و موضع قوانین جزایی کشورها در این زمینه به چه صورت است؛ لذا اکنون برای روشن‌تر شدن موضوع به بحث در این رابطه می‌پردازیم:

2- 5- موضوع جرم و موضع قوانین جزایی

الف) موضوع جرم

همان‌گونه که قبلاً بیان شد رایانه از دو قسمت تشکیل شده است، سخت‌افزار و نرم‌افزار، سخت‌افزار به قسمت‌های فیزیکی رایانه گفته می‌شود که جرایم علیه آن وجه مشخصه خاصی ندارند؛ لذا نمی تواند موضوع جرم رایانه‌ای قرار گیرد؛ اما نرم‌افزارها به برنامه‌های رایانه‌ای و فرامین و دستورالعمل هایی که به‌منظور خاص گردهم آمده‌اند گفته می‌شود که می‌توانند موضوع جرم قرار گیرند و محتوای برنامه‌ها، داده‌ها و اطلاعات هستند که از اهمیت و ارزش خاصی برخوردارند و نیز همین اطلاعات و داده‌ها هستند که به برنامه‌ها ارزش و اعتبار می‌بخشند؛ مثلاً در کارت های اعتباری، اطلاعات موجود در آن دارای اهمیت خاصی است، نه خود کارت، به همین لحاظ است که اطلاعات کارت های اعتباری و نیز اطلاعات شخصی و مالی مربوط به مشتریان دارای کارت اعتباری به دفعات هدف حمله جامعه سازمان یافته مجرمان واقع شده و می‌شود؛ بنابراین اطلاعات و داده موضوع ارتکاب جرم رایانه‌ای است.

1- تعریف داده رایانه‌ای

داده را می‌توان هرگونه مفهوم، علامت و اطلاعاتی دانست که سیستم رایانه‌ای می‌تواند آن را پردازش کند، به گونه‌ای که سیستم رایانه‌ای با دریافت آن اطلاعات و تجزیه و تحلیل منطقی، اطلاعات را درک کرده و به اصطلاح «پردازش» می‌کند. داده‌ها می تواند به شکل‌های مختلفی وجود داشته باشد؛ از جمله، داده‌های قیاسی موجود در نوارهای صوتی و تصویری، داده‌های موجود در دیسک‌های نوری (CD) که به شکل سوراخ‌های بسیار ریزی است که بر سطح دیسکت ایجاد شده‌اند، بار کدهای موجود روی یک کارت با داده‌های رقمی که در یک تراشه ذخیره شده و برای سیستم رایانه‌ای دارای مفهوم خاصی است و سیستم می‌تواند آنها را پردازش کند. داده ممکن است در سیستم رایانه‌ای بوده یا در حامل‌های داده ذخیره شده باشد. داده ممکن است به شکل ذخیره شدن یا در حال جریان باشد ویژگی‌های عمده داده رایانه‌ای عبارت است از:

- داده رایانه‌ای لزوماً متضمن بیان مفهوم یا اطلاعات درک شدنی نیست و ایجاد یک خط یا نقطه یا حرف به معنای ایجاد و یا ارائه داده خواهد بود.

- داده رایانه‌ای همواره دارای ارزش مالی نیست؛ بلکه بسیاری از آنها ارزش اقتصادی نداشته و قابلیت داد و ستد را ندارند.

- داده رایانه‌ای همیشه در مرئی و منظر کاربر سیستم رایانه‌ای یا استفاده کننده از آن قرار نمی‌گیرد. داده‌های رایانه‌ای آشکار و پنهان، عمل پردازش یا سایر فعالیت‌های مربوط را انجام می‌دهد. بسیاری از این فعالیت‌ها هرگز به صحنه رایانه

آشکار نمی‌شوند.

2- اطلاعات رایانه‌ای

اطلاعات رایانه‌ای عبارت از داده، متن، تصویر، صدا، کد، پایگاه داده‌ای، هرگونه نرم‌افزار ایجاد شده یا انتقال دادنی یا ذخیره‌شدنی که بیانگر واقعیتی درک‌شدنی باشد.

3- وجوه تمایز اطلاعات و داده‌ها رایانه‌ای

باتوجه به تعاریف فوق می‌توان گفت که اصطلاح اطلاعات رایانه‌ای از داده رایانه‌ای عام‌تر است؛ ولی باید گفت که در تفکیک این دو اصطلاح اختلاف‌نظر وجود دارد، از یک سو می‌توان گفت که داده‌های ناکارآمد و نامفهوم، متضمنِ هیچ اطلاعاتی نیستند و در نتیجه اطلاعات محسوب نمی‌شوند. از سوی دیگر می‌توان ادعا کرد که صدا یا امواج مغناطیسی یا حتی پایگاه داده در زمره اطلاعات محسوب می‌شود، حال آنکه اطلاق داده بر آنها بی‌اشکال نیست.

ب) موضع قوانین جزایی

مجموعه قوانین کیفری تمام کشورها تاکنون به‌طور عمده موضوعات مادی و ملموس و قابل رؤیت را مورد حمایت قرار داده‌اند. اما چند دهه گذشته شاهد تغییرات قابل ملاحظه‌ای در این زمینه بوده‌ایم، از جمله تبدیل جامعه صنعتی به جامعه فراصنعتی، افزایش ارزش اطلاعات در اقتصاد، فرهنگ و سیاست و اهمیت روبه رشد فناوری رایانه که این تغییرات موجب رویارویی حقوق اطلاعاتی با چالش‌ها و واکنش‌های قضایی شده است؛ اما اکنون در زمینه علوم قضایی، دکترین تازه‌ای برای اطلاعات کیفری در حال ظهور است و آن این است که اطلاعات را پس از ماده و انرژی به عنوان عامل بنیادی سوم می‌شناسند؛ بنابراین اطلاعات به‌صورت یک دارایی اقتصادی، فرهنگی و سیاسی و همچنین آسیب‌پذیر در برابر شکل های منحصر به فرد جرم ارزیابی می‌شود.

تا دهۀ 1980 در اکثر سیستم‌های حقوقی، تمامیت داده‌های ذخیره شده در رایانه تحت پوشش مقررات کلی مربوط به خسارت‌زدن به اموال (تخریب) خرابکاری قرار می‌گرفت؛ اما این مقررات به‌منظور حمایت از حقوق مربوط به اشیای مادی تدوین شده بود؛ بنابراین کاربرد آنها در حیطه اطلاعات، مسائل جدیدی را مطرح کرده است.

در تعداد معدودی از مجموعه قوانین کیفری، صرفِ پاک کردن داده‌ها بدون خسارت به محیط فیزیکی، مشمول مقررات مربوط به خسارت‌زدن به اموال (تخریب) واقع نمی‌شود؛ زیرا ضربه‌های الکترونیکی جزء اموال مادی محسوب نمی‌شود و ایجاد اختلال در استفاده از محیط فیزیکی نیز نابود کردن داده‌ها به‌شمار نمی‌آید؛ اما بر اساس عقیده اغلب کشورها، خسارت واردکردن یا نابودی عمدی داده‌های روی نوار یا دیسک معادل خسارت واردکردن (تخریب) یا ایجاد

اختلال در استفاده از اموال (خرابکاری) به‌صورت de lege data[۳۳] قلمداد می‌شود؛ زیرا در این عمل، استفاده از نوار دیسک تحت تأثیر قرار می‌گیرد.

برای روشن ساختن وضعیت موجود، در بسیاری از کشورها قوانین جدیدی وضع شده است. برخی از کشورها قوانین مرسوم خود را در مورد سوءاستفاده، خرابکاری یا خسارت‌زدن به اموال مادی (تخریب) اصلاح کردند. برخی دیگر نیز قوانین تازه و ویژه‌ای ایجاد کرده‌اند. قوانین تعداد کمی از کشورها، نه تنها داده‌های ذخیره شده در رایانه، بلکه تمامی اسناد را تحت‌پوشش قرار می‌دهند. قوانین دیگر کشورها صرفاً تمامیت داده‌های ذخیره شده در رایانه را مورد حمایت قرار می‌دهند.

حقوق کیفری به لحاظ مضیق بودن خود برای تضمین صحت کلی داده‌ها به ویژه محتوای اطلاعاتی آنها، ابزار بسیار ضعیفی است. این حقوق تنها در موارد خاصی مانند گزارش‌های پزشکی و یا اسناد خاص دیگر قادر به تضمین، حفظ و نگهداری صحیح داده‌ها است. برخی از مهم‌ترین مقررات حقوق کیفری تمامیت و صحت داده‌های خاص را دربرمی‌گیرند مقررات مربوط به جعل اسناد که صرفاً اصالت سند را از لحاظ مندرجات تضمین می‌کنند.

در برخی کشورها، مقررات مربوط به جعل اسناد به قابلیت خوانده شدن ظاهری اظهارات مندرج در سند متکی است و به همین دلیل شامل داده‌های ذخیره‌شده به‌صورت الکترونیکی نمی‌شوند. برای اینکه اسناد الکترونیکی نیز از همان حمایت قانونی اسناد کاغذی برخوردار شوند، در برخی از کشورها قوانین جدیدی در مورد جعل اسناد وضع یا پیشنهاد شده که از شرط قابلیت مشاهدهٔ ظاهری آن چشم‌پوشی شده است و به‌صورت de lege data دادگاه‌های دیگر کشورها نیز به همین نتیجه رسیده‌اند.

بخش دوم:جرایم رایانه‌ای و اینترنتی در حقوق فناوری های نوین

1- مشخصات و ارکان جرایم رایانه‌ای و اینترنتی

1-1- مشخصات جرایم رایانه‌ای و اینترنتی

آنچه باعث می‌شود قوانین موجود و مرسوم پاسخگوی مسائل مربوط به جرایم رایانه‌ای و اینترنتی نباشند، ویژگی‌ها و مشخصات خاص این‌گونه جرایم است که آنها را از دیگر جرایم متمایز ساخته و موجب دشواری عمل قانونگذار و سختی رسیدگی به آنها می‌شود. این ویژگی‌ها عبارتند از:

1- تنوع جرایم رایانه‌ای و اینترنتیجرایم رایانه‌ای شامل انواع متعدد و متنوعی است بعضی از آنها مانند جعل رایانه‌ای،

1- تخریب اطلاعات

تخریب رایانه‌ای و جاسوسی رایانه‌ای را می‌توان جزء جرایم علیه امنیت و آسایش عمومی دانست. جرایمی چون کلاهبرداری رایانه‌ای و سرقت رایانه‌ای و سرقت هویت را مربوط به جرایم علیه اموال و جرایمی مانند نفوذکردن، پخش کدهای مخرب و ... را ناشی از فناوری رایانه‌ای؛ لذا برای این قبیل جرایم نمی‌توان یک قانون کلی درنظر گرفت؛ زیرا در عمل با اشکالات زیادی مواجه خواهد شد.

2- جرایم فاقد محدودیت: جرایم رایانه‌ای محدودیت‌های بسیار کمی دارند (چه از نظر زمانی و چه از نظر مکانی) به‌عنوان مثال: چند جوان اهل آلمان علاقه‌مند به رایانه موفق شدند با شبکهٔ فوق سری که آژانس فضایی آمریکا (NASA) را به مراکز تحقیقاتی علمی در انگلیس، آلمان، سوئیس و ژاپن متصل می‌کرد ارتباط برقرار کرده و به اطلاعات فضایی فوق العاده محرمانه‌ای دست یابند. محدودیت مکانی نیز در جرایم رایانه‌ای وجود ندارد. رایانه‌هایی که فقط با یک خط تلفن به سایر مراکز رایانه‌ای متصل می‌شوند خیلی راحت می‌توانند مورد هرگونه سوءاستفاده قرار گیرند. نه تنها سرقت، بلکه بسیاری از خرابکاری‌های رایانه‌ای از همین طریق صورت می‌گیرد. به‌عنوان مثال یک دانشجوی فوق لیسانس دانشگاه کورنل آمریکا توانسته بود با واردکردن یک ویروس رایانه‌ای به رایانه‌های مرکز تحقیقات و اطلاعات دانشگاه‌های کشور، اطلاعات زیادی را از بین ببرد (رایانه‌های این مراکز به‌وسیلهٔ خطوط تلفن به یکدیگر مرتبط هستند).

3- عدم حضور فاعل در صحنه جرم: در بیشتر جرایم حضور فاعل در صحنهٔ جرم از ملزومات وقوع حادثه یا حداقل انتساب جرم به اوست؛ ولی این امر در جرم رایانه‌ای هیچ الزامی ندارد؛ بلکه معمولاً مجرم رایانه‌ای در زمان تحقق جرم اصلاً در محل وقوع حاضر نیست؛ مثالِ ارتباطِ چند جوان با شبکه فوق‌سری ناسا مبین همین مطلب است.

4- وجود مهارت خاص: در برخی از جرایم، ارتکاب جرم مستلزم آشنایی با تکنیک یا فناوری خاصی است. در بیشتر جرایم رایانه‌ای، مجرم باید تا حد زیادی مهارت و تخصص لازم را دارا باشد (بسته به نوع جرم)؛ اما بعضی از این دسته جرایم مستلزم دانش بالا و تخصص فنی و تکنیکی لازم نیستند. مجرمان رایانه‌ای اغلب از قشر روشنفکر و تحصیلکرده می‌باشند.[۳۴]

5- نبود ادله اثبات جرم: مجرمان رایانه‌ای در محیط‌های پردازش داده‌ها، اثرات و مدارکی که دال بر مجرمیت آنها باشد از خود برجای نمی‌گذارند؛ لذا این امر دسترسی به مدارک کلاسیک را غیرممکن می‌سازد. واحد ملی مبارزه با جرایم رایانه‌ای FBI برآورد می‌کند 85 تا 89٪ از تهاجمات رایانه‌ای حتی کشف نشده‌اند.[۳۵]

6- سرعت وقوع جرم: به‌عنوان مثال سرقت یا تخریب اطلاعات یک رایانه ظرف چند ثانیه صورت می‌پذیرد.

7- حجم صدمات و خسارات وارده: در جرم رایانه‌ای به‌دلیل سهولت ارتکاب جرم، حجم صدمات و خسارات وارده چند

1- جنایتکار یقه سفید

2- The FBI's National Computer Crime Squad

صدبرابر جرایم معمولی است. در این خصوص مثال‌های فراوانی از کشورهای مختلف وجود دارد که به چند نمونه از آنها اشاره می‌کنیم:

کانون وکلای آمریکا در سال 1987 میلادی با انجام مطالعاتی در شرکت‌ها و ادارات دولتی (حدود 300 شرکت و اداره) خسارت جرایم رایانه‌ای را در این سال بین 145 تا 730 میلیون دلار برآورد می‌کنند.[۳۶] صنعت نرم‌افزاری ایالات متحده به‌علت نسخه برداری غیرمجاز توسط شرکت‌ها و افراد، سالانه بیش از 12میلیارد دلار زیان می‌بینند.[۳۷] میزان زیان شرکت‌های نرم‌افزاری از بابت سرقت نرم‌افزار، سالانه بالغ بر 25 میلیون دلار تخمین زده می‌شود. به عقیده آگاهان، نقض انحصاری آثار (کپی‌رایت) آمریکایی در تایوان در سال 1992 بالغ بر 700 میلیون دلار ضرر را متوجه تولیدکنندگان آمریکایی کرده است. آنچه مشخص است آمار ثبت‌شده در مراکز پلیس در خصوص جرایم رایانه‌ای بیانگر شمار واقعی جرایم نیست؛ زیرا آمار جرایم گزارش نشده یا به اصطلاح رقم سیاه خیلی زیاد است.

انجمن بین‌المللی حقوق جزا در گردهمایی اکتبر 1992 میلادی در وتسبورگ گزارشی ارائه داد که تنها 5٪ جرایم رایانه‌ای به مقامات مجری قانون گزارش شده است.[۳۸]

8- ارزش‌های مورد حمله: در جرایم رایانه‌ای یکی از ارزش‌های مهم مورد حمله اطلاعات است؛ بنابراین در کنار حمایت از اشخاص، امنیت، اموال (به‌طور مرسوم) باید از فاکتورهای جدیدی چون اطلاعات، داده‌ها، سیستم‌های رایانه‌ای و ... سخن گفت.

9- جرایم ناشی از فناوری مدرن: برخی جرایم مانند جرایم علیه محیط زیست، جرایم هواپیمایی، جرایم رایانه‌ای و ... جزء جرایم ناشی از پیشرفت فناوری هستند یعنی جزء جرایم مصنوعی‌شبه‌ار می‌آیند.

10- پیچیدگی روزافزون فعالیت‌های مجرمانه در فضای سایبر: روزآمدشدن از ویژگی‌های ذاتی فضای اینترنت است. این ویژگی در کلیهٔ فعالیت‌های تخریبی و مجرمانه هم صدق می‌کند. فعالیت‌های مجرمان روی شبکه‌ها روز به روز پیچیده‌تر می‌شود.

1- 2- ارکان جرایم رایانه‌ای و اینترنتی

جرایم رایانه‌ای نیز مانند هر جرم دیگری دارای سه رکن می‌باشد:

1- رکن قانونی؛

2- رکن مادی؛

3- نشریه بررسی ابعاد جزایی کاربرد کامپیوتر (دبیرخانه شورای انفورماتیک) جلد اول: 22

4- خبرنامه انفورماتیک ش 53: 16

1- نشریه بررسی ابعاد جزایی کاربرد کامپیوتر، ج اول: 22.

3- رکن معنوی.

1- رکن قانونی

رکن قانونی یعنی اینکه قانون، فعل یا ترک فعل آن را تحتوان جرم، قانونگذاری و برای آن مجازات بیان کرده باشد و تا هنگامی که قانون دربارۀ فعل یا ترک فعلی چنین نکرده باشد رکن قانونی تحقق نیافته است. یک عمل، هر قدر که به ظاهر زشت و زیانبخش باشد تا وقتی که بعنوان جرم قانونگذاری نشده باشد جرم محسوب نمی‌شود و کیفر قانونی نخواهد داشت. در جرایم رایانه‌ای و اینترنتی در بیان رکن قانونی باید نکات زیر رعایت گردد:

الف: توصیف قانونی عمل مجرمانه صورت پذیرد؛ به‌گونه‌ای که از دیگر اوصاف مجرمانه متمایز شود.

ب: به‌طور دقیق در قوانین جزایی ذکر شود.

پ: اجزای عمل مجرمانه به‌طور دقیق بیان شود تا مقامات درگیر تشریفات دادرسی از جمله قاضی و وکیل با انطباق قانون با عمل ارتکابی متجاوز را مورد تعقیب قرار دهند.

ت: نحوۀ ارتکاب و مسائل مربوط به آن بیان گردد.

کشورهای مختلف برای تعیین جرایم رایانه‌ای و اینترنتی، روش‌ها و رویه‌های مختلفی در پیش گرفته‌اند که می‌توان آنها را به‌عنوان رکن قانونی جرایم رایانه‌ای قلمداد نمود. چون جرایم رایانه‌ای طیف وسیعی از اعمال مجرمانه را شامل می‌شوند، گاهی ناظر به جرایم علیه اموال است و گاهی علیه امنیت و آسایش عمومی و حتی گاهی این‌گونه جرایم علیه اشخاص است؛ لذا باید به نحوۀ درج مواد مربوطه توجه کرد. طرق مختلفی که کشورها در قوانین خود در نظر گرفته اند عبارتند از:

1- ذکر جرایم در فصلی جداگانه مانند فرانسه؛

2- ذیل مواد قبلی (نحوۀ رایج متداول آن) مانند کانادا و آلمان؛

3- قانون مستقل: مانند هلند و آمریکا و انگلستان.

در اینجا از هر نمونه، رویۀ قانونی یک کشور را توضیح می‌دهیم:

- **فرانسه**

کد کیفری فرانسه Lecade penal در فصل 3 عنوان برخی جرایم علیه موضوعات انفورماتیک را مورد بررسی قرار داده و به درج مواد آن پرداخته است. در برخی از فصل های دیگر کد نیز که ناظر به محرمانگی اشخاص و ... است، موادی درج شده است. مجازات‌ها گاهی در همان طبقۀ قبلی مانده است؛ یعنی اگر جرم جنایی یا جنحه‌ای بود مجازات جرایم رایانه‌ای نیز به همان‌گونه مقرر شده است، حتی در میزان مجازات نیز این حد و مرز رعایت شده است.

• **آلمان**

در این کشور، قانون فدرال حمایت از داها و قوانین ایالتی به ذکر برخی مقررات مربوط به جرایم رایانه‌ای پرداخته‌است؛ به‌عنوان نمونه فصل22 ناظر به کلاهبرداری و خیانت در امانت است. در این فصل مادۀ263 جرم کلاهبرداری را تبیین و مجازات آن را تا5 سال زندان یا مجازات نقدی اعلام می‌کند و در موارد خطرناک و جدی مجازات از یک تا ده سال زندان است؛در فصل مربوط به جعل، مواد260 و 270 نیز جرم جدید را تحت‌عنوان تقلب در داده‌های مربوط به امور قانونی و تقلب در روابط حقوقی از طریق داده‌پردازی پیش‌بینی کرده است.

• **انگلستان**

در انگلستان قانون سوءاستفاده رایانه‌ای مصوب 1990 میلادی، سه جرم کیفری جدید را وضع کرده است که عبارتند از:

الف: دستیابی غیرمجاز به برنامه‌های رایانه‌ای؛

ب: نفوذ یافتگی و محو یا خدشه‌زدن به برنامه‌ها یا داده‌های رایانه‌ای؛

ج: ایراد هرگونه تخریب در برنامه‌ها یا داده‌های رایانه‌ای.

جرم نفوذ یافتن مستوجب مجازات نقدی یا زندان تا 6 ماه است، جرم محو یا خدشه‌زدن و تخریب برنامه‌ها و داده‌ها بسته به شکل ارتکابی گاهی تا 6 ماه و گاهی تا 5 سال زندان دارد.

• **جمهوری اسلامی ایران**

با توجه به پیشرفت سریع رایانه و کاربردهای متعدد و متنوع در بخش‌های مختلف و امکان سوءاستفاده و استفادۀ نامطلوب از این صنعت و عدم پاسخگویی قوانین مرسوم کیفری به مسائل جرم رایانه‌ای، در جریان بازنگری بخشی از قانون مجازات اسلامی (تعزیرات) هیئت محترم وزیران مقرر ساخت تا در خصوص جرایم رایانه‌ای نیز بررسی های لازم صورت گرفته و چنانچه پیشنهادهای مشخصی وجود دارد به متن لایحۀ جدید تعزیرات افزوده شود. دو متن پیشنهاد گردید، یکی توسط دبیرخانه شورای عالی انفورماتیک و دیگری به‌وسیلۀ بانک مرکزی که متون پیشنهادی در کمیسیون لوایح دولت بررسی گردید و درنهایت یک لایحه، تحت عنوان «چگونگی برخورد با جرایم رایانه‌ای» در جلسه هیئت وزیران مورخه 73/6/6 به تصویب رسید که بر طبق آن فصلی با 2 ماده به قانون مجازات اسلامی افزوده می‌شود (مانند بند اول). متأسفانه این لایحه در مجلس شورای اسلامی به تصویب نرسید. با وجود تلاش متخصصان و حقوقدانان کشور، فصل یا قانونی تحت این عنوان به قانون مجازات اسلامی افزوده نشد.[۳۹]

تقریباً از اواخر دهۀ 70 و ابتدای 1380 تدابیر گوناگونی در رده‌های حاکمیتی کشور در خصوص ضرورت مقابله با سوءاستفاده‌های مجرمانۀ سایبری اتخاذ شده که مهم‌ترین آن ابلاغیۀ 7 ماده‌ای مقام معظم رهبری دربارۀ شبکه‌های اطلاع‌رسانی رایانه‌ای در سال 1380 است که می‌توان از آن به‌عنوان منشور سیاست جنایی ملی جرایم رایانه‌ای یاد کرد.

1- لازم به توضیح است فقط در مادۀ 131 قانون مجازات جرایم نیروهای مسلح مصوب 1382 به جرایم ناشی از تخلفات رایانه‌ای به‌طور ناقص اشاره شد.

این سیاست‌نامه، علاوه بر جنبه‌های کیفری موضوع، حاوی تدابیر پیشگیرانهٔ ارزشمندی است که توجه و پایبندی به آن می‌تواند مشکلات این حوزه را تا حد زیادی برطرف کند.

از سال 1381 فعالیت مجدد حوزه جرایم رایانه‌ای آغاز گردید که منجر به تنظیم پیش‌نویس سند جرایم رایانه‌ای در شورای عالی توسعهٔ قضایی قوهٔ قضائیه شد و در نهایت لایحهٔ جرایم رایانه‌ای بعد از گذشت 15 سال (از زمان تصویب آن در هیئت وزیران آن زمان) توسط شورای عالی توسعه قضایی تهیه و پیشنهاد گردید که در خردادماه 1388 به تصویب مجلس شورای اسلامی و تأیید شورای نگهبان رسید.

با توجه به تقسیم‌بندی انجام‌شده از آنجا که قانون جرایم رایانه‌ای در ادامهٔ قانون تعزیرات بیان گردیده می‌توان جمهوری اسلامی ایران را جزء کشورهای دستهٔ اول این تقسیم‌بندی قلمداد کرد.

2- رکن مادی (شیوه‌ها و مراحل ارتکاب)

در حالت کلی، عنصر مادی هر جرم عبارت است از فعل، ترک فعل، فعل ناشی از ترک فعل و داشتن و نگه داری که به‌موجب قانون جرم باشند؛ اما در جرایم رایانه‌ای ترک فعل و داشتن و نگه‌داری تاکنون مصداق عینی نداشته است؛ از این رو باید گفت در حال حاضر جرایم رایانه‌ای از جرایم عمدی است و هرگونه بی‌احتیاطی، بی‌مبالاتی و عدم مهارت و ... که جزء مصادیق خطا هستند باید به‌عنوان تخلفات مدنی یا اداری مورد بررسی قرار گیرند و نباید جزء موارد کیفری به‌حساب آید؛ بنابراین فعلاً جرایم رایانه‌ای را باید از مصادیق فعل قلمداد کرد؛ اما در مورد تحقق نتیجه باید گفت برخی از جرایم رایانه‌ای جزء اعمال مجرمانه کلاسیک هستند که به‌واسطهٔ تغییر و تحول در عنصر مادی، تبدیل به جرم رایانه‌ای شده‌اند؛ از این رو بحث تحقق نتیجه در این‌گونه جرایم همانند جرایم کلاسیک در همان دسته است؛ اما در تبیین جرایم نوخاسته که بر اثر پیشرفت فناوری اطلاعاتی ایجاد شده‌اند و سابقه‌ای در قوانین جزایی ندارند؛ به عبارت دیگر برخی از جرایم مقیدند و برخی مطلق؛ مثلاً جرم نفوذ یافتن (خدشه زدن)
به داده‌ها یا برنامه‌های رایانه‌ای جرمی مطلق است، صرفِ دستیابی کفایت می‌کند،
اگر بر اثر دستیابی نتیجه‌ای نیز حاصل شود، جرم داخل در توصیف مجرمانه دیگری
قرار می‌گیرد.

در مورد مسئلهٔ رابطهٔ علیت نیز باید گفت اولاً بین حقوقدانان در خود مسئلهٔ رابطهٔ علیت بحث و تنازع فراوان دیده می‌شود، ثانیاً اگر قول برخی از حقوقدانان را ملاک قرار دهیم و در جرایم مقید، رابطهٔ علیت را لازم بشماریم، آنگاه در جرایم رایانه‌ای مقید نیز چنین حالتی حکمفرماست. نکته‌ای دیگر اینکه تصور جرم محال یا عقیم یا شروع به جرم در جرایم رایانه‌ای از لحاظ شکلی وجود ندارد؛ اما باید قاعدهٔ جزایی در این مورد رعایت شود. از آنجایی که ارتکاب هر نوع جرم رایانه‌ای و اینترنتی با نفوذ و دستیابی غیرمجاز شروع می‌شود، در اینجا به تشریح این دو شیوه که مقدمه و مادر سایر جرایم رایانه‌ای است می‌پردازیم:

الف) دسترسی غیرمجاز

شیوه‌های دسترسی غیرمجاز را می‌توان به شیوه‌های فنی (از جمله؛ دسترسی برگذر واژه‌ها [۴۰]، دسترسی از رهگذر درهای پشتی [۴۱]، دسترسی از رهگذر اسب‌های تروا [۴۲]، دسترسی از طریق مودم، دسترسی به داده‌های رمزگذاری شده یا مخفی) و شیوه‌های غیرفنی، (شامل شیوه‌های مبتنی بر دانش مهندسی اجتماعی [۴۳]، اشغال‌گردی [۴۴]، برقراری ارتباط دوستانه با مدیر سیستم [۴۵]، جعل عنوان، نشان‌دادن خود به‌جای کاربر مجاز، ...) تقسیم کرد. مرحله‌های ارتکاب را می‌توان به منزلهٔ یک فرایند از لحظهٔ شروع تا پایان از نظر فنی و حقوقی تقسیم نمود. از نظر فنی، این مراحل دربرگیرندهٔ گزینش هدف، گردآوری اطلاعات و سازماندهی آنها و طرح‌ریزی، اجرا و پاکسازی حمله است. از نظر حقوقی نیز این مراحل عبارتند از قصد ارتکاب، اجرای عملیات مقدماتی، شروع به جرم و اجرای آن. از لحاظ فنی. مرتکبین این جرم به «هکرها» معروف می‌باشند. هکرها را می‌توان از نظر فنی به انواع زیر دسته‌بندی نمود:

1- نفوذگرهای کلاه سیاه: این نفوذ سبب بروز اشکال در ارائهٔ برخی سرویس‌ها، به خطر افتادن داده‌ها و از دست دادن صدها هزار دلار در سال می‌شود.

2- نفوذگرهای کلاه سفید: این افراد سعی در بی‌اعتبار کردن و نابودی سیستم‌های رایانه‌ای دارند. اینها به‌صورت غیرقانونی به سیستم‌ها نفوذ می‌کنند. در صورت موفقیت یک حفره امنیتی و یک نقطه آسیب پذیر سیستم را تشخیص می‌دهند و از این راه از مدیران سیستم‌ها پول می‌گیرند تا در رفع آن به مدیر سیستم کمک کنند.

3- نفوذگرهای کلاه خاکستری: این افراد سیستم‌ها را به قصد دستیابی به نقاط ضعف و حفره‌های امنیتی مورد کنکاش قرار می‌دهند و از این راه شروع به اخاذی می‌نمایند.

4- کدنویسان متقلب: این افراد بیشترین وقت خود را گشت‌زنی در اینترنت و دانلود کردن نسخه‌های نهایی برنامه‌های ویژه نفوذ می‌کنند.

5- هکتیویسم‌ها [۴۶]: این دسته از نفوذ و ورود به وب سایت‌ها برای اهداف شوم سیاسی تا ناتوان کردن نرم‌افزارهای سانسور در رایانه‌های دولتی استفاده می‌کنند.

1- Passwards
2- Horses Backdoors
3- Trojan
4- مهندس اجتماعی علمی است که از دانش روابط اجتماعی و شیوه‌های برقراری ارتباط گروهی و شاخه‌های مختلف دانش فنی و مهندسی به ویژه فناوری اطلاعات و ارتباطات برای هدف‌های خاص استفاده می‌کنند.
5- Danpster diving
6- Admine

1- Hactivism
2- Cyberterroiasm

6- سایبر تروریسم[۴۷]: این نوع تروریسم با نفوذ باعث مکمل‌کردن رایانه‌ها و شبکه‌های رایانه‌ای، شبکه‌های تلفنی و شبکه‌های ارتباطات می‌شود و برای اهداف تروریستی از آن استفاده می‌کند. دسترسی غیرمجاز عاملی محرک در ارتکاب سایر جرم‌های رایانه‌ای است. اغلب دست‌یابندگان غیرمجاز پس از دسترسی به صرف دسترسی بسنده نمی‌کنند و اقدامات مجرمانهٔ دیگری نیز مانند نسخه‌برداری از داده‌ها، اختلال در سیستم انتشار برنامه‌های ویرانگر و ... انجام می‌دهند. این جرم مقدمه ارتکاب جرایمی مانند شنود غیرمجاز، جاسوسی و سرقت رایانه‌ای می‌باشد.

ب) تخریب و اختلال در داده‌ها و سیستم‌های رایانه‌ای

از میان بردن، مختل‌کردن و استفاده ناپذیرکردن داده‌ها به سه شیوهٔ کلی زیر انجام می‌شود:

1- اعمال فیزیکی: مانند شکستن یا تخریب دیسک حاوی داده در رایانه یا تخریب بخشی از سیستم رایانه‌ای با وارد کردن چیزهایی مانند برادهٔ آهن یا گیره‌های کاغذی یا دمیدن و دود سیگار یا وارد کردن تکه‌هایی از آلومینیم داخل وسایل رایانه‌های و .... که موجب می‌شود داده‌ها از میان رفته یا استفاده ناپذیر شوند.

2- سیستم رایانه‌ای: مانند اینکه با دادن فرمان حذفِ داده به سیستم رایانه‌ای، سیستم رایانه‌ای داده‌های وارد شده را پردازش و براساس آن، داده‌های موجود را حذف کند.

3- امواج: که با فرستادن آنها، داده‌ها حذف، مختل یا استفاده ناپذیر می‌شوند.
ایجاد اختلال در کارکرد سیستم رایانه‌ای با استفاده از برنامه ویروس یا کرم رایانه‌ای یا تروای رایانه و حملات DOS و DDOS به‌منظور محروم‌کردن افراد از دسترسی درست و پیوسته به سیستم رایانه‌ای ارتکاب می‌شود.

3- رکن معنوی

رکن معنوی عبارت است از
قصد مجرمانه یا خطایی که مجرم بر اثر آن مرتکب جرم شده باشد و با شرایطی مسئولیت جزایی متوجه او خواهد بود.
جرایم رایانه‌ای نیز مانند دیگر جرایم نیازمند رکن معنوی است. مسلماً اراده و خواست مجرمانه بر ارتکاب جرم باید موجود باشد. جزء دوم، قصد یا سوءنیت است؛ اما در این جزء از خطا یا تقصیر جزایی سخنی به میان نمی‌آید. پس برای تحقق رکن معنوی جرم رایانه‌ای وجود اراده بر ارتکاب و قصد یا سوء نیت امری اجتناب‌ناپذیراست. کسی که به قصد کلاهبرداری مرتکب جرم رایانه‌ای شود و بدین منظور داده‌های بانکی را تغییر می‌دهد و وجوهی را به نفع خود تحصیل می‌کند، مرتکب جرم کلاهبرداری شده است.
اقتضای سیاست جنایی این است که جرایم رایانه‌ای در زمره جرایم عمدی باشند. خطا یا تقصیر که لازمهٔ تحقق جرایم غیرعمدی است به‌عنوان رکن معنوی جرایم رایانه‌ای مطرح نیست، کوتاهی و قصوری که منجر به خسارت یا صدمه می‌شود در چارچوب تخلفات اداری یا مدنی قرار می‌گیرند و ضمانت اجرایی این رشته را خواهند داشت.

از واژۀ «قصد» چنین بر می‌آید که عمل عمومی است و حصول نتیجه را نیز دربر می‌گیرد، در مورد کلاهبرداری، نتیجه‌ای را که فاعل از فعلِ تغییر داده‌های رایانه‌ای می‌خواهد همان کسب منفعت و تحصیل وجوه است . در جعل رایانه‌ای نیز همین وضعیت وجود دارد. داعی مجرمانه اصولاً در ماهیت عمل مجرمانه جز در موارد معدود تأثیری ندارد.

سوء نیت عام یعنی آگاهی از ارتکاب عمل مجرمانه و سوء نیت خاص یعنی نتیجه‌ای که فاعل از ارتکاب عمل خود دنبال می‌کند. در جرایم رایانه‌ای برخی جرایم دارای سوء نیت عام و برخی سوء نیت خاص در کنار سوء نیت عام هستند، ذکر این نکته ضروری است که جرم ممکن است فاقد سوء نیت خاص باشد؛ ولی به‌هیچ عنوان نمی‌تواند فاقد سوء نیت عام باشد. در جرم نفوذ یافتن، فرد فقط قصد دستیابی به یک سیستم رایانه‌ای را دارد. بنابراین سوء نیت خاص مطرح نیست؛ اما در مورد جرم کلاهبرداری رایانه‌ای مجرم علاوه بر خواست ارتکاب جرم، قصد ضرر به دیگری و تصاحب اموال دیگری را نیز دارد، از این رو جرم محتاج تحقق سوء نیت عام و سوء نیت خاص است. در جرایم رایانه‌ای هر نوع بی‌احتیاطی، بی‌مبالاتی و ... که مبین خطا و تقصیر است را در زمره تخلفات مدنی و اداری قرار می‌دهند و ضمانت اجرای آنها را نیز در ضمانت اجراهای مدنی یا اداری جستجو می‌کنند و این به دو دلیل است، یکی اجتناب از تورم کیفری و دیگری فرعی‌بودن حقوق جزا. از آنجایی که جرایم رایانه‌ای و اینترنتی جزء جرایم عمدی به شمار می‌روند، انگیزه تأثیری بر مجرمیت مجرمان رایانه‌ای ندارد. انگیزۀ مجرمان رایانه‌ای مختلف و متنوع است. این انگیزه‌ها عبارتند از: انگیزه‌های شرافتمندانه (از جمله بالابردن امنیت سیستم‌ها، مراقبت از سیستم‌ها در برابر آسیب، کمک به پیشرفت دانش فنی و مهندسی) انگیزه‌های غیرشرافتمندانه (از جمله، غرض ورزی و انتقام‌جویی، کسب شهرت، انگیزه‌های مالی، حسادت).

1- 3- مجازات جرایم رایانه‌ای

مجازات جرایم رایانه‌ای باید از پارامترهای سیاست جنایی درون هر کشور تبعیت کند و در ایران بر طبق اصول حاکم بر مجازات‌ها و موارد قانونی تشدید و تخفیف و تعلیق مجازات صورت می‌پذیرد. به نظر نگارندگان جزای نقدی به تنهایی صورت صرف، مجازات مطلوبی نیست؛ زیرا نه تنها فاقد جنبۀ ارعابی و عبرت آموزی است؛ بلکه مشوق اشخاص به ارتکاب جرایم گوناگون نیز می‌گردد. این موضوع به ویژه در خصوص جرایمی که جنبۀ مالی داشته، نباید اعمال گردد، هرچند نظر برخی بر این است که جزای نقدی، مجازات مطلوبی است و می تواند رضایت مجنی‌علیه را کسب نماید.

برای مجازات‌ها سه هدف ارعابی، سزادهی و اصلاحی ذکر نموده‌اند که به نظر نگارندگان مجازات نقدی واجد و تأمین‌کنندۀ هیچ یک از اهداف فوق نیست؛ البته باید به این نکته توجه نمود که در مورد جرایم مختلفی که به بزه دیده خساراتی وارد می‌آورد باید این خسارت جبران شود و این مبین جزای نقدی نیست.

در مجازات جرایم رایانه‌ای همانند سایر جرایم باید اصول حاکم بر مجازات‌ها در نظر گرفته شود. یکی از این اصول، اصل قانونی بودن مجازات است که به همراه اصل‌قانونی بودن جرم در حقوق جزا به‌صورت اصل قانونی‌بودن جرایم و مجازات‌ها مطرح است

2- طبقه‌بندی جرایم رایانه‌ای

در تقسیم‌بندی جرایم رایانه‌ای تاکنون چندین طبقه بندی و تقسیم‌بندی توسط محققان و متخصصان و حقوقدانان و علمای حقوق جزا مطرح گردیده است. نوع اول این تقسیم‌بندی توسط یکی از محققان داخلی [۴۸] ارائه شده و تقسیم‌بندی‌های دیگر مربوط به کمیسیون حقوقی اسکاتلند، سازمان همکاری و پیشرفت اقتصادی (OECD)، شورای اروپا، سازمان ملل، انجمن بین‌المللی حقوق جزا، اینترپل، کنوانسیون بوداپست (2001) و قانون جرایم رایانه‌ای (1388) صورت گرفته است که به ترتیب به توضیح آنها می‌پردازیم:

الف) تقسیم‌بندی نوع اول

این محقق جرایم رایانه‌ای را به سه دسته تقسیم می‌کند:

1- جرایمی که خود رایانه مرتکب می‌شود: این فرض در مورد رایانه‌های محاسب است که به علل مختلف از جمله خرابی در بخش حافظه، ممکن است دچار اختلال شوند، به‌عنوان مثال شرکت‌های برق که صورت‌حساب‌های خود را به‌وسیلهٔ رایانه تهیه می‌کنند و توسط پست برای مشترکان ارسال می‌نمایند، بسیار دیده شده است که این رایانه‌ها در برآورد وجوه آب و برق و ... دچار اشتباهاتی شده‌اند و باعث زیادی پرداخت بعضی از مشترکان یا پرداخت کم آنها می‌شود. جرایم ارتکابی توسط خود رایانه شاید امروزه به اندازهٔ دیگر مسائل به چشم نخورد؛ ولی با پیشرفت سریع رایانه بعید به نظر نمی‌رسد، روزی فرا رسد که خود رایانه‌ها مباشرتاً مرتکب جرایمی شوند، به‌خصوص رایانه‌های نسل پنجم که قادر به تفکر هستند و گاهی طوری اعمال می‌کنند که از تفکر خودشان حاصل شده است.

2- جرایمی که به‌وسیلهٔ رایانه ارتکاب می‌شوند: این نوع جرایم به دو دسته تقسیم می‌شود:

2-1- خروج غیرمجاز اطلاعات و داده‌های رایانه‌ای: دریافت غیرمجاز اطلاعات از یک رایانه هنگامی عنوان جرم به خود می‌گیرد که این اطلاعات سری باشد؛ به‌عنوان مثال می‌توان به فعالیت چند جوان که چند سال پیش از مرکز اطلاعات نظامی فرانسه مقداری اسرار نظامی را به سرقت برده و به کشورهای بلوک شرق فروخته بودند[۴۹] اشاره کرد.

2-2- ورود اطلاعات غلط و داده‌های خلاف واقع به رایانه: از آنجا که مبنای کار رایانه اطلاعات و داده‌های اولیه است، پس می‌توانیم با دادن اطلاعات غلط و داده‌های خلاف واقع به رایانه عمل صحیحی را غلط و یا عمل غلطی را صحیح جلوه دهیم. این نمونه در دادگستری‌هایی که از رایانه برای بایگانی سوابق مجرمان استفاده می‌نمایند کاربرد بیشتری دارد. البته ممکن است اهداف دیگری نیز از دادن اطلاعات اشتباه به رایانه دنبال شود، مثل بی اعتبار کردن یک اداره،

1- طاهری جیلی، محسن- جرم و کامپیوتر- مجله قضایی و حقوقی دادگستری- سال سوم – شماره دهم- زمستان 1372: 123

1- مجله قضایی حقوقی دادگستری، سال سوم شماره نهم، زمستان 1372: 125 به نقل از خبرگزاری جمهوری اسلامی

نتیجه‌دهی غلط رایانه ممکن است علل مختلفی داشته باشد از جمله:

- اشتباه در اطلاعات ورودی؛

- اشتباه در برنامه‌های کاربردی؛

- اشتباه عملیاتی از سوی متصدی رایانه؛

- اشتباه کشف نشده در نرم‌افزار سیستم؛

- اشتباه بر اثر خرابی نرم‌افزار[۵۰] که مسئول هر قسمت در صورت سوء نیت یا بی‌مبالاتی ممکن است مجرم شناخته شود.

3- جرایم علیه رایانه: چون اساس کار هر رایانه نرم‌افزارهایی است که درآن استفاده می‌شود، از این رو نرم‌افزارها دارای ارزش خاصی هستند و به همین علت همواره جرایم مربوط به نرم‌افزارها رو به افزایش است. این‌گونه جرایم عبارتند از: سرقت نرم‌افزار، تخریب اطلاعات نرم‌افزار، تخریب نرم‌افزار، کپی‌برداری غیرقانونی از برنامه‌ها و تقلب در نرم‌افزارها.

ب) تقسیم‌بندی کمیسیون حقوقی اسکاتلند

کمیسیون حقوقی اسکاتلند هشت شکل از رفتارهای مرتبط با رایانه را که دارای مفاهیم جزایی هستند به شرح زیر مورد شناسایی قرار داده است:

1- پاک‌شدگی یا تحریف داده‌ها یا برنامه‌ها برای به‌دست آوردن مقادیر نقدی یا دیگر پیشرفت‌ها؛

2- تحصیل دستیابی غیرمجاز به رایانه؛

3- استراق سمع در رایانه؛

4- گرفتن اطلاعات بدون برداشت فیزیکی؛

5- اقتباس غیرمجاز (تکثیر و کپی‌برداری غیرمجاز) از دیسکت‌ها یا نوارهای رایانه؛

6- استفاده غیرمجاز از زمان یا تجهیزات؛

7- کینه‌جویی یا بی‌اعتنایی به انحراف یا پاک‌کردن داده‌ها یا برنامه‌ها؛

8- انکار دستیابی غیرمجاز کاربران.

پ) تقسیم‌بندی سازمان همکاری و پیشرفت اقتصادی (OECD)

این سازمان در سال 1986 در گزارشی تحت‌عنوان جرم رایانه‌ای و تحلیل سیاست‌های قانونی، به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوءاستفاده‌هایی را پیشنهاد کرد که در کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار گیرد، این سوءاستفاده‌ها عبارتند از:

1- ورود، تغییر، پاککردن، موقوف‌سازی داده‌ها یا برنامه‌های رایانه‌ای که به‌طور ارادی با قطنتقال غیرقانونی وجوه یا هر چیز

2- پرهامی، دکتر بهروز- آشنایی با کامپیوتر- تهران، انتشارات علم و صنعت، 1372: 180

با ارزش دیگر صورت گرفته باشد (کلاهبرداری رایانه‌ای)؛

2- ورود، تغییر، پاک‌کردن، موقوف‌سازی داده‌ها و یا برنامه‌های رایانه‌ای که به‌صورت عمدی با قصد ارتکاب جعل صورت گرفته باشد. (جعل رایانه‌ای)؛

3- ورود، تغییر، پاککردن، موقوفسازی داده‌ها و یا برنامه‌های رایانه‌ای یا هرگونه مداخله دیگر در سیستم‌های رایانه‌ای که به‌صورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه یا ارتباطات صورت گرفته باشد (تغییر «جابه‌جایی» برنامه‌ها و داده‌های رایانه‌ای)؛

4- تجاوز به حقوق انحصاری مالک با برنامه رایانه‌ای حفاظت‌شده با قصد بهره‌برداری تجاری از آن برنامه و ارائهٔ آن به بازار (نقض حق تألیف)؛

5- دستیابی یا استراق سمع در یک سیستم رایانه‌ای و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور، هر چند به‌منظور تخطی از تدابیر امنیتی و یا با هدف‌های غیرشرافتمندانه یا مضر صورت گرفته باشد (استراق سمع یا دستیابی به سیستم بدون کسب مجوز).[۵۱]

ت) تقسیم‌بندی شورای اروپا

پس از گزارش OECD شورای اروپا ابتکار عمل را به‌دست گرفت و از دید فنی، حقوقی به قضیه نگریست. در طبقه بندی شورای اروپا دو فهرست حداقل و اختیاری به چشم می‌خورد و در هر فهرست نیز جرایمی ذکر شده است.

فهرست حداقل ارائه‌شده از سوی کمیتهٔ نشانگر اجماع و توافق اعضای کمیته بر ارزیابی برخی رفتارهای خطرناک و مضر و جرم تلقی‌نمودن آنها است. جرایم فهرست حداقل عبارتند از:

1- کلاهبرداری رایانه‌ای؛

2- جعل رایانه‌ای؛

3- خسارت‌زدن به داده‌ها یا برنامه‌های رایانه‌ای؛

4- تخریب رایانه‌ای؛

5- دستیابی غیرمجاز؛

6- قطع و استراق سمع غیرمجاز؛

7- ارائه و ایجاد مجدد و غیرمجاز یک برنامهٔ رایانه‌ای حمایت‌شده؛

8- ارائه و ایجاد مجدد یک توپوگرافی.

1- مجموعه قوانین ایالات متحده، مجلد17، فصل9، اقتباس از نشریه بررسی ابعاد جزایی کاربرد کامپیوتر (اسناد موجود در سازمان برنامه و بودجه) جلد اول: 46

جرایم فهرست اختیاری عبارتند از:

1- تغییر داده‌ها یا برنامه‌های رایانه‌ای؛

2- جاسوسی رایانه‌ای

3- استفادهٔ غیرمجاز از رایانه؛

4- استفادهٔ غیرمجاز از برنامه‌های رایانه‌ای؛

جرم شناختن جرایم فهرست اختیاری بستگی به ارزش‌ها و ملاحظات هر کشور دارد.

ث)تقسیم‌بندی سازمان ملل متحد

این سازمان طی کنگره‌های مختلف به بررسی جرایم رایانه‌ای پرداخت. در سال 1990 در اجلاس دوازدهم، سازمان، نمایندهٔ دولت کانادا پیش‌نویس قطعنامه‌ای را در مورد جرم رایانه‌ای تسلیم کنگره کرد که در اجلاس سیزدهم پذیرفته و تصویب شد. سازمان ملل در نشریه بین‌المللی سیاست جنایی شماره 43-44 خود علاوه بر اینکه تقسیم‌بندی‌های موجود را مورد اشاره قرار داد، انواع مشترک و عمومی جرایم رایانه‌ای را برمی‌شمرد که عبارتند از:

1- کلاهبرداری رایانه‌ای؛

2- جعل رایانه‌ای؛

3- ایجاد خسارت یا تغییر در داده‌ها یا برنامه‌های رایانه‌ای؛

4- دستیابی غیرمجاز به سیستم‌ها و خدمات رایانه‌ای؛

5- تکثیر غیرمجاز برنامه‌های رایانه‌ای حمایت‌شده.

این سازمان تقسیم‌بندی‌های شورای اروپا و OECD را مهم و درجه اول می‌شمارد.

ج) تقسیم‌بندی انجمن بین‌المللی حقوق جزا

انجمن بین‌المللی حقوق جزا سازمانی غیردولتی است که همکاری فعالی با سازمان ملل دارد و مشاور شورای اقتصادی اجتماعی سازمان است.[۵۲] سال 1990 این انجمن چهار موضوع از جمله موضوع جرایم رایانه‌ای و دیگر جرایم علیه فناوری اطلاعات را مطرح کرد. طراح این برنامه و پرسشنامه پروفسور زیبر است.[۵۳] نتیجهٔ کار انجمن، چاپ کتابی ویژه تحت‌عنوان جرایم رایانه‌ای (جلد 64 شماره 1/2 نشریه انجمن) و همچنین صدور قطعنامه ای حاوی فهرست جرایم رایانه‌ای است.

1- ر.ک. مجله قانون وکلا شماره 154، سخنرانی پروفسور اتانف

2- ر.ک. مجله گزارش کامپیوتر- ش 22 (متن نامه و پرسشنامه به چاپ رسیده است.)

انجمن معتقد است که علاوه بر جرایمی که در تقسیم‌بندی شورای اروپا قرار گرفته‌اند جرایم ذیل به دلیل افزایش حساسیت در این زمینه‌ها باید به‌طور مستقل ذکر شوند:

1- قاچاق کلمات رمز؛

2- انتشار ویروس یا برنامه‌های مشابه؛

3- دستیابی به اسرار برخلاف قانون؛

4- به‌کارگیری، انتقال و دگرگونی غیرقانونی داده‌های شخصی.

چ) تقسیم‌بندی سازمان جنایی بین‌المللی (اینترپل)

این سازمان که سال‌هاست در زمینهٔ مبارزه با جرایم رایانه‌ای فعالیت می‌کند، جرایم رایانه‌ای را به‌شرح زیر طبقه‌بندی کرده است:

1- دستیابی غیرمجاز:

1-1- نفوذ غیرمجاز (هک)؛
1-2- شنود غیرمجاز؛

1-3- سرقت زمان رایانه.

2- تغییر داده‌های رایانه‌ای:

2-1- تغییر داده‌ها به‌وسیلهٔ بمب منطقی؛
2-2- تغییر داده‌ها به‌وسیلهٔ اسب‌تروا؛
2-3- تغییر داده‌ها به‌وسیلهٔ ویروس رایانه‌ای؛

2-4- تغییر داده‌های رایانه‌ای کرم رایانه‌ای.

3- کلاهبرداری رایانه‌ای:

3-1- سوءاستفاده از صندوق‌های پرداخت خودکار پول (ATM)؛
3-2- جعل رایانه‌ای؛
3-3- سوءاستفاده از ماشین‌های بازی و ... ؛

3-4- دستکاری در مرحلهٔ ورودی و خروجی؛

3-5- سوءاستفاده از ابزار پرداخت مستقر در فروشگاه‌ها؛

3-6- سوءاستفاده تلفنی (برای شنود یا استفاده از خدمات مخابرات).

4- تکثیر غیرمجاز:

4-1- تکثیر بازی‌های رایانه‌ای؛

4-2- تکثیر نیمه‌هادی؛

4-3- تکثیر نرم‌افزارهای دیگر.

5- خرابکاری:

5-1- خراب‌کردن سخت‌افزار؛

5-2- خراب‌کردن نرم‌افزار.

6- سایر جرایم رایانه‌ای:

6-1- سرقت اسرار تجاری (فاش، انتقال و استفاده)؛

6-2- ذخیره‌سازی هرزه‌نگاری کودک و سایر نرم‌افزارهای غیرمجاز؛

6-3- سایر موضوعات تعقیب‌شدنی.

ح) تقسیم‌بندی کنوانسیون جرم سایبر (بوداپست 2001)

این کنوانسیون جرایم رایانه‌ای را به چهار طبقه به‌شرح زیر تقسیم می‌کند:

1- جرایم علیه محرمانگی یا تمامیت و دسترسی داده‌ها و سیستم‌های رایانه‌ای:

1-1- دستیابی عمدی و غیرمجاز به سیستم رایانه‌ای؛

1-2- شنود عمدی و غیرمجاز داده‌های رایانه‌ای؛

1-3- ایجاد اختلال عمدی و غیرمجاز در رایانه‌ای؛

1-4- ایجاد اختلال عمدی و غیرمجاز در داده‌های رایانه‌ای؛

1-5- سوءاستفاده از وسایل، رمز عبور، کد دستیابی یا داده‌ها یا برنامه‌های رایانه‌ای.

2- جرایم مرتبط با رایانه:

2-1- جعل مرتبط با رایانه؛

2-2- کلاهبرداری مرتبط با رایانه.

3- جرایم مرتبط با محتوا:

3-1- تولید هرزه‌نگاری کودک به قصد انتشار در سیستم رایانه؛

3-2- ارائهٔ هرزه‌نگاری کودک از طریق سیستم رایانه؛

3-3- توزیع هرزه‌نگاری کودکان از طریق سیستم رایانه؛

3-4- تهیه هرزه نگاری کودکان از طریق سیستم رایانه؛

3-5- در اختیارگذاشتن هرزه‌نگاری کودک به قصد انتشار در سیستم رایانه.

4- جرایم مرتبط با نقض حق مؤلف و حقوق مربوط به آن شامل:

4-1- جرایم مرتبط با حق مؤلف؛

4-2- جرایم مرتبط با حقوق مربوط به حق مؤلف.

استفاده از برنامه‌های رایانه‌ای حمایت‌شده زمانی که مؤلف آن رضایت ندارد، تخلف علیه کپی‌رایت رایانه‌ای است.

خ) تقسیم‌بندی قانون جرایم رایانه‌ای (1388)

این قانون، جرایم رایانه‌ای را در 5 فصل به‌شرح ذیل تقسیم نموده است:

1- جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی:

1-1- دسترسی غیرمجاز؛

1-2- شنود غیرمجاز؛

1-3- جاسوسی رایانه‌ای.

2- جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی:

2-1- جعل رایانه‌ای؛

2-2- تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی؛

3- سرقت و کلاهبرداری مرتبط با رایانه؛

4- جرایم علیه عفت و اخلاق عمومی؛

5- هتک حیثیت و نشر اکاذیب.

آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی

در اجرای ماده ۵۴ قانون جرایم رایانه ای مصوب ۵/۳/۱۳۸۸ مجلس شورای اسلامی و بـنا به پیشنهاد وزیر دادگستری، آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی به شرح مواد آتی است:

فصل اول: تعاریف

ماده ۱ـ واژه ها و اصطلاحات بکار برده شده در این آیین نامه در معانی زیر بکار می رود:

الف ـ ارائه دهندگان خدمات دسترسی: اشخاصی هستند که امکان ارتباط کاربران را با شبکه های رایانه ای یا مخابراتی و ارتباطی داخلی یا بین المللی یا هر شبکه مستقل دیگر فراهم می آورند از قبیل تأمین کنندگان، توزیع کنندگان، عرضه کنندگان خدمات دسترسی به شبکه های رایانه ای یا مخابراتی.

ب ـ ارائه دهندگان خدمات میزبانی: اشخاصی هستند که امکان دسترسی کاربران به فضای ایجاد شده توسط سامانه های رایانه ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می کنند تا رأساً یا توسط کاربر متقاضی، داده های رایانه ای را جهت نگهداری، انتشار، توزیع یا ارائه در شبکه های داخلی یا بین المللی یا هر منظور دیگر ذخیره یا پردازش کنند.

ج ـ ارائه داده های الکترونیکی: عبارت است از در اختیار قرار دادن تمام یا بخشی از داده های حفظ یا نگهداری شده توسط ارائه دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده ها را تحت تصرف یا کنترل دارند.

د ـ جمع آوری ادله الکترونیکی: فرآیندی است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه های رایانه ای یا مخابراتی یا حامل های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می شوند.

هـ ـ زنجیره حفاظتی: مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذیصلاح به منظور حفظ صحت، تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی با بکارگیری ابزارها و روش های استاندارد در مراحل

شناسایی، کشف، جمع آوری، مستندسازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجرا درآورده و ثبت می کنند؛ به نحوی که امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد.

و ـ شنود: عبارت است از هر گونه دستیابی به محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه ها و تجهیزات سخت افزاری و نرم افزاری مربوط.

زـ مجری حفاظت: شخصی است که به نحوی داده های رایانه ای ذخیره شده را تحت تصرف یا کنترل دارد و مطابق ماده ۳۴ قانون و سایر قوانین و مقررات جهت حفاظت آنها تعیین می شود.

ح ـ متصرف قانونی: در مورد اشخاص حقیقی، شخص مالک یا شخصی است که به نحوی داده یا سامانه را به صورت مشروع در اختیار دارد یا نماینده یا ولی یا سرپرست قانونی وی. در مورد اشخاص حقوقی دولتی یا عمومی غیردولتی، بالاترین مقام آنها یا نماینده قانونی آنها طبق مقررات مربوط و در مورد سایر اشخاص حقوقی، مدیر یا نماینده قانونی آنهاست.

ط ـ قانون: منظور از قانون در این آیین نامه، قانون جرایم رایانه ای مصوب ۵/۳/۱۳۸۸ می باشد.

تبصره ـ سایر اصطلاحات به شرح تعریف ارائه شده در قوانین دیگر می باشد.

فصل دوم: جمع آوری ادله الکترونیکی

الف: نگهداری داده ها

ماده ۲ـ ارائه دهندگان خدمات دسترسی و میزبانی موظفند از سامانه هایی استفاده نمایند که قابلیت نگهداری داده های ترافیک و اطلاعات کاربران را مطابق مواد ۳۲ و ۳۳ قانون داشته باشد.

ماده ۳ـ ارائه دهندگان خدمات دسترسی موظفند سامانه های خود را به نحوی تنظیم کنند که کلیه ارتباطات رایانه ای را که از طریق آنها انجام می شود ثبت کنند و کلیه داده های ترافیک مربوط به خود و کاربران مربوط را تا شش ماه پس از ایجاد نگهداری کنند.

تبصره ـ عرضه کنندگان خدمات دسترسی حضوری اینترنت (کافی نت ها) موظفند مشخصات هویتی، آدرس، تخصیصی را در دفتر روزانه ثبت نمایند (IP) ساعت شروع و خاتمه کار کاربر و نشانی اینترنتی.

ماده ۴ـ ارائه دهندگان خدمت دسترسی موظفند اطلاعات کاربران را حداقل ۶ ماه پس از خاتمه اشتراک یا لغو قرارداد کاربر نگهداری کنند. هویت و نشانی کاربر باید در قرارداد منعقده درج شود.

ماده ۵ـ ارائه دهندگان خدمات میزبانی داخلی و نمایندگان داخلی ارائه دهندگان خدمات میزبانی خارجی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند. برگه اشتراک باید به نحوی تنظیم شود که هویت و نشانی آنان مشخص باشد.

تبصره ۱ـ ارائه دهندگان خدمات میزبانی موظفند سامانه های رایانه ای خود را به نحوی تنظیم کنند که هر گونه تغییر اعم از اصلاح یا حذف محتوا و داده ترافیک حاصل از آن را ذخیره نماید.

تبصره ۲ـ اشخاصی که نسبت به انباشت یا ذخیره موقت اطلاعات در راستای ارائه خدمات دسترسی اقدام می کنند، ارائه دهنده خدمات میزبانی محسوب نمی شوند.

ماده ۶ـ ارائه دهندگان خدمات دسترسی و میزبانی و مجریان حفاظت موظفند امنیت داده های ترافیکی و محتوای نگهداری و حفاظت شده را مطابق با ضوابط و دستورالعمل هایی که به تصویب رئیس قوه قضاییه می رسد، تأمین نمایند.

ماده ۷ـ داده های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آیین نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکارناپذیری آنها محفوظ بماند.

ماده ۸ـ در مواردی که برابر قانون نگهداری و حفاظت داده ها الزامی است، نگهداری و حفاظت باید به گونه ای انجام شود که مدیریت جستجو و گزارش دهی آنها امکان پذیر باشد.

ماده ۹ـ وزارت ارتباطات و فناوری اطلاعات هماهنگی های لازم برای تنظیم زمان سامانه های جمع آوری داده های محتوا، ترافیک و اطلاعات کاربران را مطابق با ساعت رسمی کشور به عمل می آورد.

ماده ۱۰ـ مرکز آمار و فناوری اطلاعات با همکاری وزارت ارتباطات و فناوری اطلاعات سالانه رویه های فنی نحوه نگهداری، حفاظت، توقیف و ارائه داده ها و اطلاعات کاربران و همچنین راهنماهای عملی حفظ امنیت و استنادپذیری داده ها را تصویب و به ارائه دهندگان خدمات دسترسی و میزبانی و بهره برداران ابلاغ می نماید.

ب: حفاظت از ادله رایانه ای

ماده ۱۱ـ مقام قضایی در جریان تحقیق و فرآیند رسیدگی می تواند دستور حفاظت هر نوع داده رایانه ای ذخیره شده را از جمله داده های رمزنگاری شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده هایی که نوع و نام آنها موقتاً تغییر یافته و یا داده هایی که برای بررسی آنها نیاز به سخت افزار مخصوصی می باشد، صادر نماید.

تبصره ۱ـ ضابطان قضایی فقط در موارد مندرج در ماده ۳۴ قانون می توانند رأساً دستور حفاظت داده های ذخیره شده را صادر کنند.

تبصره ۲ـ قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تأیید یا رد دستور حفاظت صادره توسط ضابط اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می باشد.

ماده ۱۲ـ دستور حفاظت باید به طور صریح و دقیق مشتمل بر نوع داده ها، موضوع و مدت زمان با رعایت تبصره ۲ ماده ۳۴ قانون، باشد.

ماده ۱۳ـ در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبره مورد وثوق به نمایندگی از طرف مرجع قضایی انجام می شود.

ماده ۱۴ـ مجری حفاظت موظف است بلافاصله پس از ابلاغ، دستور حفاظت را اجرا و صورت جلسه ای را مشتمل بر زمان اجرای دستور، نحوه حفاظت، حجم و نوع داده های حفاظت شده در دو نسخه تنظیم و یک نسخه از آن را به مرجع صادرکننده دستور ارسال کند و نسخه دیگر را نزد خود نگه دارد.

ماده ۱۵ـ دستور حفاظت باید فوری و با روش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشخاص ذینفع نیز ابلاغ می شود؛ مگر آن که ابلاغ به آنها مخلّ رسیدگی باشد که در این صورت تشخیص زمان ابلاغ حسب مورد با مقام قضایی می باشد.

تبصره ـ روش مطمئن روشی است که با توجه به نوع داده ها و طول مدت زمان حفاظت، امکان بهره برداری از داده های حفاظت شده را در مراحل بعدی دادرسی ممکن سازد.

ماده ۱۶ـ حفاظت از داده ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده ها رعایت شود.

ج: ارائه ادله رایانه ای

ماده ۱۷ـ دستور ارائه توسط مقام قضایی صادر می شود و باید به طور صریح و شفاف و مشتمل بر شخص ارائه دهنده، موضوع و نوع داده ها، شیوه و زمان تحویل داده ها و مرجع تحویل گیرنده باشد.

ماده ۱۸ـ ارائه داده ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده ها رعایت شده و حتی الامکان بدون ایجاد مانع برای فعالیت سامانه و با روش متعارف و کم هزینه به یکی از شیوه های ذیل باشد:

الف ـ تحویل یک نسخه چاپ شده از داده.

ب ـ تحویل یک نسخه رایانه ای از داده.

ج ـ ایجاد دسترسی به داده.

د ـ انتقال تجهیزات رایانه ای و مخابراتی.

ماده ۱۹ـ هنگام ارائه داده ها صورت جلسه ای در سه نسخه تنظیم و حداقل موارد ذیل در آن ذکر و به امضای ارائه دهنده و تحویل گیرنده می رسد:

الف ـ شماره و تاریخ دستور قضایی ارائه داده ها

ب ـ مشخصات ارائه دهنده

ج ـ مشخصات تحویل گیرنده

د ـ زمان و مکان ارائه

هـ ـ نوع و حجم داده ها

و- اطلاعات مربوط به نحوه حفظ یا نگهداری داده ها

ز - روش های امنیتی بکاررفته در زمان ارائه

ح - مشخصات سخت افزاری و نرم افزاری تجهیزات

. ط - شیوه ارائه و مشخصات داده

.تبصره ۱- در هنگام انتقال تجهیزات، احتیاط لازم برای حفظ آنها به عمل می آید

تبصره ۲- یک نسخه از صورت جلسه به مرجع قضایی ارسال می شود و نسخه ای در اختیار ارائه دهنده و نسخه .دیگر در اختیار تحویل گیرنده قرار می گیرد

ماده ۲۰- از زمان ارائه داده ها به ضابطان قضایی یا دیگر اشخاص ذیربط، مسئولیت حفظ داده های مذکور با .شخص یا اشخاص تحویل گیرنده خواهد بود

ماده ۲۱- ارائه داده هایی که افشا یا دسترسی به آنها مطابق قوانین خاص دارای محدودیت یا توأم با تشریفات .می باشد، تابع مقررات مربوط است

ماده ۲۲- دستور ارائه داده، مجوز افشای آن نمی باشد و پس از دستور ارائه هر گونه دسترسی به مفاد داده .مستلزم صدور دستور قضایی است

ماده ۲۳- اشخاصی که مسئول اجرای هر یک از دستورات قضایی اعم از نگهداری، حفاظت، ارائه، تفتیش و توقیف سامانه و داده یا شنود آن می باشند یا دستور به آنها ابلاغ می شود یا به نوعی مرتبط با دستورات یاد .شده هستند، حق افشای مفاد دستور و یا داده ها و اطلاعات مربوط را ندارند

د: تفتیش و توقیف ادله رایانه ای

ماده ۲۴- ضابطان قضایی باید کلیه اطلاعاتی که ضرورت تفتیش و توقیف را ایجاب می نماید در درخواست خود :اعلام نمایند. همچنین، موارد زیر را حسب مورد در درخواست تفتیش یا توقیف ذکر نمایند

الف - دلایل ضرورت تفتیش و توقیف

ب - حتی الامکان نوع و میزان داده ها و سخت افزارها

ج - محل تفتیش یا توقیف

د - دلایل لازم برای تصویربرداری و بررسی در خارج از محل

.هـ - زمان تقریبی لازم برای تفتیش و توقیف

ماده ۲۵- در دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی الامکان در محل .استقرار سامانه انجام پذیرد

ماده ۲۶- مدت توقیف و فرصت اجرای تفتیش باید در دستور قضایی تصریح و کمترین فرصت ممکن منظور شود. در صورت نیاز به زمان بیشتر، به درخواست مجری تفتیش یا توقیف و ذکر علت آن، این مدت قابل تمدید .می باشد

ماده ۲۷ـ تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود.

ماده ۲۸ـ در مواردی که تفتیش یا توقیف طبق دستور قضایی بدون حضور متصرف قانونی یا شخصی که داده یا سامانه را تحت اختیار دارد، انجام پذیرد، مراتب پس از انجام فوراً به ذینفع ابلاغ خواهد شد.

ماده ۲۹ـ چنانچه پس از اجرای دستور توقیف و یا در زمان اجرای دستور توقیف داده ها یا سامانه های رایانه ای یا مخابراتی بیم لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی برود مراتب از مرجع قضایی صادرکننده دستور توقیف کسب تکلیف شده و در صورت تشخیص قاضی حسب مفاد ماده ۴۴ قانون عمل می گردد.

ماده ۳۰ـ قوه قضاییه تمهیدات لازم از جمله بسترسازی و ایجاد زیرساخت های ارتباط رایانه ای و الکترونیکی و همچنین راه اندازی سامانه ها و درگاه های مبتنی بر فناوری اطلاعات را جهت تسهیل در عملیاتی کردن فرایندها و روش های موضوع این آیین نامه فراهم می آورد.

ماده ۳۱ـ اشخاصی که داده ها یا سامانه های رایانه ای یا مخابراتی را تحت کنترل و یا تصرف دارند، موظف به همکاری در اجرای دستور تفتیش و توقیف می باشند. در صورتی که به واسطه عدم همکاری یا عدم دسترسی به این اشخاص، تفتیش یا توقیف امکان پذیر نباشد، نحوه دسترسی به داده ها یا سامانه ها از قبیل ورود به محل، رفع موانع استفاده از سخت افزار و نرم افزار، رمزگشایی و امثال آن با دستور مقام قضایی تعیین خواهد شد.

ماده ۳۲ـ رضایت متصرف قانونی سامانه موضوع بند ج ماده ۴۱ قانون، باید کتبی و با امضای وی باشد.

ماده ۳۳ـ در مواردی که توقیف داده ها به روش چاپ یا کپی یا تصویربرداری داده ها انجام می شود، اصل داده ها در صورتی توقیف و غیرقابل دسترس می شود که در دستور قضایی تصریح شده باشد.

ماده ۳۴ـ ضابطان صرفاً مجاز به تفتیش و توقیف داده ها و سامانه هایی هستند که به طور صریح در دستور قضایی ذکر گردیده و چنانچه حین اجرای دستور، داده های مرتبط با جرم ارتکابی در سایر سامانه های رایانه ای یا مخابراتی تحت کنترل یا تصرف متهم کشف شود، در صورت بیم امحا نسبت به حفظ فوری داده ها اقدام و مراتب را حداکثر ظرف ۲۴ ساعت کتباً به مقام قضایی مربوط گزارش می دهند.

ماده ۳۵ـ تفتیش داده ها یا سامانه ها در محل استقرار یا از طریق شبکه یا در آزمایشگاه یا در محل مناسب با دستور و تشخیص مقام قضایی با رعایت صحت، تمامیت، محرمانگی، و انکارناپذیری ادله انجام می پذیرد.

ماده ۳۶ـ ضابطان و اشخاصی که حسب قانون مأمور جمع آوری، تفتیش، نگهداری، حفظ و انتقال داده ها و سامانه های رایانه ای یا مخابراتی می شوند باید علاوه بر داشتن شرایط لازم از قبیل تخصص و توانایی فنی و آموزش کافی، تجهیزات و وسایل لازم را در اختیار داشته باشند.

ماده ۳۷ـ هنگام تفتیش رعایت موارد زیر ضروری است:

الف ـ شیوه اقدام نباید موجب تغییر، امحا یا جابجایی داده های مورد نظر در سامانه های رایانه ای باشد.

.ب ـ تفتیش صرفاً در محدوده دستور قضایی و داده های مرتبط با جرم موضوع دستور، انجام می پذیرد
ج ـ کلیه فرایندهای انجام شده بر روی داده های مورد تفتیش یا توقیف باید با استفاده از روش های قابل
.تشخیص، ثبت و محافظت شود
ماده ۳۸ـ توقیف با رعایت تناسب، نوع، اهمیت و نقش داده یا سامانه رایانه ای یا مخابراتی به روش های زیر
:انجام می شود
الف ـ در تـوقیف داده ها از طریـق چاپ داده ها، غیرقابـل دسترس کردن داده ها به روش هایی از قبیل تغییر
.گذر واژه یا رمزنگاری و ضبط حامل های داده
ب ـ در توقیف سامانه های رایانه ای یا مخابراتی از طریق تغییر گذر واژه، پلمپ سامانه در محل استقرار یا ضبط
.سامانه
تبصره ـ توقیف باید حتی الامکان بدون ایجاد مانع برای فعالیت سامانه و به روش ساده و کم هزینه به شیوه
هایی از قبیل ذخیره در حامل های داده، ذخیره در سامانه با گذاشتن گذرواژه، تهیه نسخه پشتیبان،
.تصویربرداری، تهیه رونوشت و چاپ انجام شود
ماده ۳۹ـ دستور توقیف سامانه شامل سایر سخت افزارها یا حامل های داده متصل به آن نمی شود، مگر آن که
در دستور قضایی تصریح گردد. در صورت نیاز به حفظ فوری سخت افزارها یا حامل های داده، ضابطان یا سایر
مأموران در حدود وظایف قانونی می توانند نسبت به حفظ فوری آن مطابق ماده ۳۴ قانون و رعایت مقررات این
.آیین نامه اقدام نمایند
.ماده ۴۰ـ در صورت پلمپ سامانه چنانچه نیاز به گماردن حافظ باشد با دستور مقام قضایی اقدام می شود
ماده ۴۱ـ به منظور حفظ وضعیت اصلی ادله رایانه ای و جلوگیری از هرگونه تغییر، تحریف یا آسیب آن، مرجع
.قضایی مدت زمان نگهداری و مراقبت از آنها را تا مدت ۵ روز تعیین می کند
تبصره ـ چنانچه برای نگهداری و مراقبت مدت بیشتری مورد نیاز باشد، مدت مذکور به صورت مستدل توسط
.مقام قضایی تمدید می شود
ماده ۴۲ـ اجرای دستور توقیف باید طی صورت جلسه ای با قید دقیق جزییات و مشخصات داده یا سامانه، محل،
تاریخ و زمان دقیق، مشخصات حاضران و مجری دستور، مشخصات حافظ در صورت وجود، شماره و تاریخ
دستور قضایی مبنی بر توقیف، شیوه توقیف و مشخصات مالک یا متصرف داده یا سامانه و موارد ضروری دیگر
.تنظیم و ضمن اعلام به مقام قضایی رسیدگی کننده، در سابقه ضبط گردد
ماده ۴۳ـ ضابطان قضایی و سایر مأموران در حدود وظایف قانونی در شروع تفتیش و توقیف باید صورت وضعیت
اولیه ای از سامانه رایانه ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت افزارها و
حامل های داده متصل به آن که علامت گذاری و ثبت می شوند را تنظیم و به امضای تفتیش کننده یا توقیف

کننده و متصرف قانونی که سامانه تحت کنترل اوست یا قائم مقام قانونی وی برسانند. برای ضبط دقیق مشخصات ابزار و اجزای آن تصویربرداری بلامانع است.

ماده ۴۴ـ مرجع قضایی صالح، ضمن صدور رأی باید نسبت به داده یا سامانه توقیف شده تعیین تکلیف نماید.

فصل سوم: امور متفرقه

ماده ۴۵ـ دستورالعمل حقوقی و فنی جمع آوری ادله و توقیف سامانه های رایانه ای و مخابراتی توسط دادستانی کل کشور با همکاری نیروی انتظامی تهیه و به تصویب دادستان کل کشور می رسد. این دستورالعمل باید دربردارنده چگونگی حفظ صحنه جرم و جمع آوری ادله از سامانه در حال اجرا، خاموش و روشن کردن سامانه، بسته بندی و انتقال اطلاعات و نیز نمونه درخواست های مرتبط با این موارد باشد.

ماده ۴۶ـ در مورد جمع آوری ادله الکترونیکی از جمله نگهداری، حفظ فوری، تفتیش و توقیف و شنود چنانچه موضوع مربوط به افراد و اماکن وابسته به قوه قضاییه و سازمان های تابعه مراکز مرتبط با قوه قضاییه باشد، با دستور مقام قضایی توسط مرکز حفاظت و اطلاعات قوه قضاییه انجام خواهد شد.

ماده ۴۷ـ نسخه های تهیه شده از داده های رایانه ای قابل استناد به صورت متن، صوت یا تصویر در حکم اصل داده می باشند.

ماده ۴۸ـ این آیین نامه توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و در ۴۸ ماده و ۱۱ تبصره در تاریخ ۱۲/۵/۱۳۹۳ به تصویب رئیس قوه قضاییه رسید.

قانون تجارت الکترونیکی

قانون تجارت الکترونیکی مصوب 1382

باب اول – مقررات عمومی

مبحث اول- در کلیات

فصل اول- قلمرو و شمول قانون

ماده ۱- این قانون مجموعه اصول و قواعدی است که برای مبادله آسان و ایمن اطلاعات در واسطهای الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به کار می‌رود.

فصل دوم – تعریف

-ماده ۲

«الف - «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.

«ب- «اصل‌ساز» (Originator): منشأ اصلی «داده‌پیام» است که «داده‌پیام» به وسیله او یا از طرف او تولید یا ارسال می‌شود اما شامل شخصی که در خصوص «داده‌پیام» به عنوان واسطه عمل می‌کند نخواهد شد.

«ج- «مخاطب» (Addressee): شخصی است که اصل‌ساز قصد دارد وی «داده‌پیام» را دریافت کند، اما شامل شخصی که در ارتباط با «داده‌پیام» به عنوان واسطه عمل می‌کند نخواهد شد.

«د- «ارجاع در داده‌پیام» (By Reference Incorporation): یعنی به منابعی خارج از «داده‌پیام» عطف شود که در صورت مطابقت با ماده (۱۸) این قانون جزئی از «داده‌پیام» محسوب می‌شود.

«ه- «تمامیت داده‌پیام» (Integrity): عبارت است از موجودیت کامل و بدون تغییر «داده‌پیام». اعمال ناشی از تصدی سیستم از قبیل ارسال، ذخیره یا نمایش اطلاعات که به طور معمول انجام می‌شود خدشه‌ای به تمامیت «داده‌پیام» وارد نمی‌کند.

«و- «سیستم رایانه‌ای» (System :(Computer هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری- نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خود کار «داده‌پیام» عمل می‌کند.

«ز- «سیستم اطلاعاتی» (System Information): سیستمی برای تولید (اصل‌سازی)، ارسال، دریافت، ذخیره یا پردازش «داده‌پیام» است.

«ح- «سیستم اطلاعاتی مطمئن» (System Secure Information): سیستم اطلاعاتی است که:

۱- به نحوی معقول در برابر سوء استفاده و نفوذ محفوظ باشد.

۲- سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد.

۳- به نحوی معقول متناسب با اهمیت کاری که انجام می‌دهد پیکربندی و سازماندهی شده باشد.

۴- موافق با رویه ایمن باشد.

ط- «رویه ایمن (Secure Method): رویه‌ای است برای تطبیق صحت ثبت «داده‌پیام» منشأ و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا و یا ذخیره سازی «داده‌پیام» از یک زمان خاص. یک رویه ایمن ممکن است با استفاده از الگوریتم‌ها یا کدها، کلمات یا ارقام شناسائی، رمزنگاری، روش‌های تصدیق یا پاسخ برگشت و یا طرق ایمنی مشابه انجام شود.

ی- «امضای الکترونیکی (Electronic Signature): عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده‌پیام» است که برای شناسائی امضا کننده «داده‌پیام» است که برای شناسائی امضا کننده «داده‌پیام» مورد استفاده قرار می‌گیرد.

ک- «امضای الکترونیکی مطمئن (Secure/Enhanced/Advanced Electronic Signature) هر امضای الکترونیکی است که مطابق با ماده (۱۰) این قانون باشد.

ل- «امضاء کننده (Signatory): هر شخص یا قائم مقام وی که امضای الکترونیکی تولید می‌کند.

م- «شخص (Person): اعم است از شخص حقیقی و حقوقی و یا سیستم‌های رایانه‌ای تحت کنترل آنان.

ن- «معقول» (سنجش عقلانی (Reasonableness Test): با توجه به اوضاع و احوال مبادله «داده‌پیام» از جمله : طبیعت مبادله، مهارت و موقعیت طرفین، حجم مبادلات طرفین در موارد مشابه، در دسترس بودن گزینه‌های پیشنهادی و در آن گزینه‌ها از جانب هر یک از طرفین، هزینه گزینه‌های پیشنهادی، عرف و روش‌های معمول و مورد استفاده در این نوع مبادلات، ارزیابی می‌شود.

س- «مصرف کننده (Consumer): هر شخصی است که به منظوری جز تجارت یا شغل حرفه‌ای اقدام می‌کند.

ع- «تأمین کننده (Supplier): عبارت از شخصی است که بنا به اهلیت تجاری، صنفی یا حرفه‌ای فعالیت می‌کند.

ف- «وسایل ارتباط از راه دور (Means Of Distance Communication): عبارت از هر نوع وسیله‌ای است که بدون حضور فیزیکی همزمان تأمین کننده و مصرف کننده جهت فروش کالا و خدمات استفاده می‌شود.

ایجاب و قبول راجع به کالاها و خدمات بین تأمین کننده و :(Distance Contract)«ص- «عقد از راه دور مصرف کننده با استفاده از وسایل ارتباط از راه دور است.

یعنی وسائلی که به موجب آن مصرف کننده شخصا :(Durable Medium) «ق- «واسط بادوام «داده‌پیام»های مربوطه را بر روی آن ذخیره کند از جمله شامل فلاپی دیسک، دیسک فشرده، دیسک سخت و یا پست الکترونیکی مصرف کننده.

یعنی «داده‌پیام»های مربوطه به یک شخص حقیقی (موضوع :(Private Data) «ز- «داده‌پیام‌های شخصی مشخص و معین (Data Subject) «داده».

فصل سوم – تفسیر قانون

ماده ۳- در تفسیر این قانون همیشه باید به خصوصیت بین‌المللی، ضرورت توسعه هماهنگی بین کشورها در کاربرد آن و رعایت لزوم حسن نیت توجه کرد.

ماده ۴- در مواقع سکوت و یا ابهام باب اول این قانون، محاکم قضایی باید بر اساس سایر قوانین موضوعه و رعایت چهارچوب فصول و مواد مندرج در این قانون، قضاوت نمایند.

فصل چهارم – اعتبار قراردادهای خصوصی

ماده ۵- هرگونه تغییر در تولید، ارسال، دریافت، ذخیره و یا پردازش داده‌پیام با توافق و قرارداد خاص طرفین معتبر است.

«مبحث دوم- در احکام «داده‌پیام

نوشته، امضاء اصل-

ماده ۶- هرگاه وجود یک نوشته از نظر قانون لازم باشد، «داده‌پیام» در حکم نوشته است مگر در موارد زیر:

الف- اسناد مالکیت اموال غیرمنقول.

ب- فروش مواد داروئی به مصرف‌کنندگان نهایی.

ج- اعلام، اخطار، هشدار و یا عبارات مشابهی که دستور خاصی برای استفاده کالا صادر می‌کند و یا از بکارگیری روش‌های خاصی به صورت فعلی یا ترک فعل منع می‌کند.

ماده ۷- هر گاه قانون، وجود امضاء را لازم بداند امضای الکترونیکی مکفی است.

ماده ۸- هرگاه قانون لازم بداند که اطلاعات به صورت اصل ارائه یا نگهداری شود، این امر یا نگهداری و ارائه اطلاعات به صورت داده‌پیام نیز در صورت وجود شرایط زیر امکان پذیر می‌باشد:

الف- اطلاعات موردنظر قابل دسترسی بوده و امکان استفاده در صورت رجوع بعدی فراهم باشد.

ب- داده‌پیام به همان قالبی(فرمتی) که تولید، ارسال و یا دریافت شده و یا به قالبی که دقیقاً نمایشگر اطلاعاتی باشد که تولید، ارسال و یا دریافت شده، نگهداری شود.

ج- اطلاعاتی که مشخص کننده مبدأ، مقصد، زمان ارسال و زمان دریافت داده‌پیام می‌باشند نیز در صورت وجود نگهداری شوند.

د- شرایط دیگری که هر نهاد، سازمان، دستگاه دولتی و یا وزارتخانه در خصوص نگهداری داده‌پیام مرتبط با حوزه مسؤولیت خود مقرر نموده فراهم شده باشد.

ماده ۹- هرگاه شرایطی به وجود آید که از مقطعی معین ارسال «داده‌پیام» خاتمه یافته و استفاده از اسناد کاغذی جایگزین آن شود سند کاغذی که تحت این شرایط صادر می‌شود باید به طور صریح ختم تبادل «داده‌پیام» را اعلام کند. جایگزینی اسناد کاغذی به جای «داده‌پیام» اثری بر حقوق و تعهدات قبلی طرفین نخواهد داشت.

مبحث سوم- «داده‌پیام» مطمئن

فصل اول- امضاء و سابقه الکترونیکی مطمئن

ماده۱۰- امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف- نسبت به امضاء کننده منحصر به فرد باشد.

ب- هویت امضاء کننده «داده‌پیام» را معلوم نماید.

.ج- به وسیله امضاءکننده و یا تحت اراده انحصاری وی صادر شده باشد

.د- به نحوی به یک «داده‌پیام» متصل شود که هر تغییری در آن «داده‌پیام» قابل تشخیص و کشف باشد

ماده ۱۱- سابقه الکترونیکی مطمئن عبارت از «داده‌پیام»ی است که با رعایت شرایط یک سیستم اطلاعاتی .مطمئن ذخیره شده و به هنگام لزوم در دسترس و قابل درک است

فصل دوم – پذیرش، ارزش اثباتی و آثار سابقه و امضای الکترونیکی مطمئن

ماده ۱۲- اسناد و ادله اثبات دعوی ممکن است به صورت داده‌پیام بوده و در هیچ محکمه یا اداره دولتی نمی .توان براساس قواعد ادله موجود، ارزش اثباتی «داده‌پیام» را صرفاً به دلیل شکل و قالب آن رد کرد

ماده ۱۳- به طور کلی، ارزش اثباتی «داده‌پیام»ها با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به .کار گرفته شده با موضوع و منظور مبادله «داده‌پیام» تعیین می‌شود

ماده ۱۴- کلیه «داده‌پیام»هائی که به طریق مطمئن ایجاد و نگهداری شده‌اند از حیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده و کلیه اشخاصی که قائم مقام قانونی آنان محسوب می‌شوند، .اجرای مفاد آن و سایر آثار در حکم اسناد معتبر و قابل استناد در مراجع قضائی و حقوقی است

ماده ۱۵- نسبت به «داده‌پیام» مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به «داده‌پیام» مزبور وارد و با ثابت نمود که «داده‌پیام» مزبور به .جهتی از جهات قانونی از اعتبار افتاده است

ماده ۱۶- هر «داده‌پیام»ی که توسط شخص ثالث مطابق با شرایط ماده (۱۱) این قانون ثبت و نگهداری میشود، .مقرون به صحت است

«مبحث چهارم- مبادله «داده‌پیام

فصل اول- اعتبار قانونی ارجاع در «داده‌پیام»، عقد و اراده طرفین

:ماده ۱۷- «ارجاع در داده‌پیام» با رعایت موارد زیر معتبر است

.الف- مورد ارجاع به طور صریح در «داده‌پیام» معین شود

.ب- مورد ارجاع برای طرف مقابل که به آن تکیه میکند روشن و مشخص باشد

.ج- «داده‌پیام» موضوع ارجاع مورد قبول طرف باشد

«فصل دوم- انتساب «داده‌پیام

:ماده ۱۸- در موارد زیر «داده‌پیام» منسوب به اصل‌ساز است

.الف- اگر توسط اصل‌ساز ویا به وسیله شخصی ارسال شده باشد که از جانب اصل‌ساز مجاز به این کار بوده است

.ب- اگر به وسیله سیستم اطلاعاتی برنامه‌ریزی شده یا تصدی خودکار از جانب اصل‌ساز ارسال شود

ماده ۱۹- «داده‌پیام»ی که بر اساس یکی از شروط زیر ارسال میشود مخاطب حق دارد آن را ارسال شده :محسوب کرده، و مطابق چنین فرضی (ارسال شده) عمل نماید

الف- قبلاً به وسیله اصل‌ساز روشی معرفی و یا توافق شده باشد که معلوم کند آیا «داده‌پیام» همان است که .اصل‌ساز ارسال کرده است

ب- «داده‌پیام» دریافت شده توسط مخاطب از اقدامات شخصی ناشی شده که رابطه‌اش با اصلساز، یا نمایندگان وی باعث شده تا شخص مذکور به روش مورد استفاده اصل‌ساز دسترسی یافته و «داده‌پیام» را به مثابه .«داده‌پیام» خود بشناسد

ماده ۲۰- ماده (۱۹)این قانون شامل مواردی نیست که پیام از اصل‌ساز صادر نشده باشد و یا به طور اشتباه صادر .شده باشد

ماده ۲۱- هر «داده‌پیام» یک «داده‌پیام» مجزا و مستقل محسوب میگردد، مگر آن که معلوم باشد که آن .«داده‌پیام» نسخه مجددی از «داده‌پیام» اولیه است

فصل سوم- تصدیق دریافت

ماده ۲۲- هرگاه قبل یا به هنگام ارسال «داده‌پیام» اصل‌ساز از مخاطب بخواهد یا توافق کنند که دریافت «داده‌پیام» تصدیق شود، اگر به شکل یا روش تصدیق توافق نشده باشد، هر نوع ارتباط خوکار یا مکاتبه یا اتخاذ هر نوع تدبیر مناسب از سوی مخاطب که اصل‌ساز را به نحو معقول از دریافت «داده‌پیام» مطمئن کند تصدیق .دریافت «داده‌پیام» محسوب میگردد

ماده ۲۳- اگر اصل‌ساز به طور صریح هر گونه اثر حقوقی «داده‌پیام» را مشروط به تصدیق دریافت «داده‌پیام» کرده باشد، «داده‌پیام» ارسال نشده تلقی می‌شود، مگرآن که تصدیق آن دریافت شود.

ماده ۲۴- اماره دریافت «داده‌پیام» راجع به محتوای «داده‌پیام» صادق نیست.

ماده ۲۵- هنگامی که در تصدیق قید میشود، «داده‌پیام» مطابق با الزامات فنی استاندارد یا روش مورد توافق طرفین دریافت شده، فرض براین است که آن الزامات رعایت شده اند.

«فصل چهارم- زمان و مکان ارسال و دریافت «داده‌پیام

ماده ۲۶- ارسال «داده‌پیام» زمانی تحقق می یابد که به یک سیستم اطلاعاتی خارج از کنترل اصل‌ساز یا قائم مقام وی وارد شود.

ماده ۲۷- زمان دریافت «داده‌پیام» مطابق شرایط زیر خواهد بود:

الف- اگر سیستم اطلاعاتی مخاطب برای دریافت «داده‌پیام» معین شده باشد دریافت، زمانی محقق میشود که:

۱- «داده‌پیام» به سیستم اطلاعاتی معین شده وارد شود؛ یا

۲- چنانچه «داده‌پیام» به سیستم اطلاعاتی مخاطب غیر از سیستمی که منحصراً برای این کار معین شده وارد شود «داده‌پیام» بازیافت شود.

ب- اگر مخاطب، یک سیستم اطلاعاتی برای دریافت معین نکرده باشد، دریافت زمانی محقق میشود که «داده‌پیام» وارد سیستم اطلاعاتی مخاطب شود.

ماده ۲۸- مفاد ماده (۲۷) این قانون بدون توجه به محل استقرار سیستم اطلاعاتی جاری است.

ماده ۲۹- اگر محل استقرار سیستم اطلاعاتی با محل استقرار دریافت «داده‌پیام» مختلف باشد مطابق قاعده زیر عمل میشود:

الف- محل تجاری، یا کاری اصلساز محل ارسال «داده‌پیام» است و محل تجاری یا کاری مخاطب محل دریافت «داده‌پیام» است مگر آن که خلاف آن توافق شده باشد.

ب- اگر اصل‌ساز بیش از یک محل تجاری یا کاری داشته باشد، نزدیکترین محل به اصل معامله، محل تجاری یا کاری خواهد بود در غیر این صورت محل اصلی شرکت، محل تجاری یا کاری است.

ج- اگر اصل‌ساز یا مخاطب فاقد محل تجاری یا کاری باشند، اقامتگاه قانونی آنان ملاک خواهد بود.

ماده ۳۰- آثار حقوقی پس از انتساب، دریافت تصدیق و زمان و مکان ارسال و دریافت «داده‌پیام» موضوع فصول دوم تا چهارم مبحث چهارم این قانون و همچنین محتوی «داده‌پیام» تابع قواعد عمومی است.

باب دوم – دفاتر خدمات صدور گواهی الکترونیکی

(Certification Service Provider)

ماده ۳۱- دفاتر خدمات صدور گواهی الکترونیکی واحدهائی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس میشوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی‌های اصالت (امضای)الکترونیکی میباشد.

ماده ۳۲- آیین‌نامه و ضوابط نظام تأسیس و شرح وظایف این دفاتر توسط سازمان مدیریت و برنامه ریزی کشور و وزارتخانه های بازرگانی، ارتباطات و فناوری اطلاعات، امور اقتصادی و دارایی و دادگستری تهیه و به تصویب هیأت وزیران خواهد رسید.

باب سوم- در قواعد مختلف

مبحث اول- حمایت‌های انحصاری در بستر مبادلات الکترونیکی

(Consumer Protection) فصل اول- حمایت از مصرف کننده

ماده ۳۳- فروشندگان کالا و ارائه دهندگان خدمات بایستی اطلاعات مؤثر در تصمیم گیری مصرف کنندگان جهت خرید و یا قبول شرایط را از زمان مناسبی قبل از عقد در اختیار مصرف کنندگان قرار دهند. حداقل اطلاعات لازم، شامل موارد زیر می‌باشد:

الف- مشخصات فنی و ویژگی‌های کاربردی کالا و یا خدمات.

.ب- هویت تأمین کننده، نام تجاری که تحت آن نام به فعالیت مشغول می‌باشد و نشانی وی

ج- آدرس پست الکترونیکی، شماره تلفن و یا هر روشی که مشتری در صورت نیاز بایستی از آن طریق با .فروشنده ارتباط برقرار کند

د- کلیه هزینه هائی که برای خرید کالا بر عهده مشتری خواهد بود (از جمله قیمت کالا و یا خدمات، میزان .(مالیات، هزینه حمل، هزینه تماس

.ه- مدت زمانی که پیشنهاد ارائه شده معتبر می‌باشد

.و- شرایط و فرایند عقد از جمله ترتیب و نحوه پرداخت، تحویل و یا اجرا، فسخ، ارجاع، خدمات پس از فروش

:ماده ۳۴- تأمین کننده باید به طور جداگانه ضمن تأیید اطلاعات مقدماتی، اطلاعات زیر را ارسال نماید

.الف- آدرس محل تجاری یا کاری تأمین کننده برای شکایت احتمالی

.ب- اطلاعات راجع به ضمانت و پشتیبانی پس از فروش

.ج- شرایط و فراگرد فسخ معامله به موجب مواد (۳۷) و (۳۸) این قانون

.د- شرایط فسخ در قراردادهای انجام خدمات

ماده ۳۵- اطلاعات اعلامی و تأییدیه اطلاعات اعلامی به مصرف کننده باید در واسطی با دوام، روشن و صریح بوده و در زمان مناسب و با وسایل مناسب ارتباطی در مدت معین و براساس لزوم حسن نیت در معاملات و از .جمله ضرورت رعایت افراد ناتوان و کودکان ارائه شود

ماده ۳۶- در صورت استفاده از ارتباط صوتی، هویت تأمین کننده و قصد وی از ایجادتماس با مصرف کننده باید .به طور روشن و صریح در شروع هر مکالمه بیان شود

ماده ۳۷- در هر معامله از راه دور مصرف کننده باید حداقل هفت روز کاری، وقت برای انصراف (حق انصراف) از قبول خود بدون تحمل جریمه و یا ارائه دلیل داشته باشد. تنها هزینه تحمیلی بر مصرف کننده هزینه باز پس .فرستادن کالاخواهد بود

:ماده ۳۸- شروع اعمال حق انصراف به ترتیب زیر خواهد بود

.الف- در صورت فروش کالا، از تاریخ تسلیم کالا به مصرف کننده و در صورت فروش خدمات، از روز انعقاد

ب- در هر حال آغاز اعمال حق انصراف مصرف کننده پس از ارائه اطلاعاتی خواهد بود که تأمین کننده طبق .مواد(۳۳) و (۳۴) این قانون موظف به ارائه آن است

ج- به محض استفاده مصرف کننده از حق انصراف،تأمین کننده مکلف است بدون مطالبه هیچ گونه وجهی عین .مبلغ دریافتی را در اسرع وقت به مصرف کننده مسترد نماید

د- حق انصراف مصرف کننده در مواردی که شرایط خاصی بر نوع کالا و خدمات حاکم است اجرا نخواهد شد. .موارد آن به موجب آیین‌نامه‌ای است که در ماده (۷۹) این قانون خواهد آمد

ماده ۳۹- در صورتی که تأمین کننده در حین معامله به دلیل عدم موجودی کالا و یا عدم امکان اجرای خدمات، نتواند تعهدات خود را انجام دهد، باید مبلغ دریافتی را فوراً به مخاطب برگرداند، مگر دربیع کلی و تعهداتی که برای همیشه وفای به تعهد غیر ممکن نباشد و مخاطب آماده صبر کردن تا امکان تحویل کالا و یا ایفای تعهد باشد. در صورتی که معلوم شود تأمین کننده از ابتدا عدم امکان ایفای تعهد خود را می‌دانسته، علاوه بر لزوم .استرداد مبلغ دریافتی، به حداکثر مجازات مقرر در این قانون نیز محکوم خواهد شد

ماده ۴۰- تأمین کننده می‌تواند کالا یا خدمات مشابه آنچه را که به مصرف کننده وعده کرده تحویل یا ارائه .نماید مشروط برآن که قبل از معامله یا در حین انجام معامله آن را اعلام کرده باشد

ماده ۴۱- در صورتی که تأمین کننده، کالا یا خدمات دیگری غیر از موضوع معامله یا تعهد را برای مخاطب ارسال نماید، کالا و یا خدمات ارجاع داده میشود و هزینه ارجاع به عهده تأمین کننده است. کالا یا خدمات ارسالی مذکور چنانچه به عنوان یک معامله یا تعهد دیگر از سوی تأمین کننده مورد ایجاب قرار گیرد، مخاطب .می تواند آن را قبول کند

:ماده ۴۲- حمایت‌های این فصل در موارد زیر اجرا نخواهد شد

.الف- خدمات مالی که فهرست آن به موجب آیین‌نامه‌ای است که در ماده (۷۹) این قانون خواهد آمد

.ب- معاملات راجع به فروش اموال غیر منقول و یا حقوق مالکیت ناشی از اموال غیرمنقول به جز اجاره

.ج- خرید از ماشین‌هایی فروش مستقیم کالا و خدمات

.د- معاملاتی که با استفاده از تلفن عمومی (همگانی) انجام می‌شود

.ه- معاملات راجع به حراجی ها

.ماده ۴۳- تأمین کننده نباید سکوت مصرف کننده را حمل بر رضایت وی کند

.ماده ۴۴- در موارد اختلاف و یا تردید مراجع قضائی رسیدگی خواهند کرد

ماده ۴۵- اجرای حقوق مصرف کننده به موجب این قانون نباید بر اساس سایر قوانین که حمایت ضعیفتری .اعمال میکنند متوقف شود

ماده ۴۶- استفاده از شروط قراردادی خلاف مقررات این فصل و همچنین اعمال شروط غیرمنصفانه به ضرر .مصرف کننده، مؤثر نیست

ماده ۴۷- در معاملات از راه دور آن بخش از موضوع معامله که به روشی غیر از وسائل ارتباط از راه دور انجام .میشود مشمول مقررات این قانون نخواهد بود

ماده ۴۸- سازمان‌های قانونی و مدنی حمایت از حقوق مصرف کننده می‌توانند به عنوان شاکی اقامه دعوی نمایند. ترتیب آن به موجب آیین‌نامه‌ای خواهد بود که به پیشنهاد وزارت بازرگانی و تصویب هیأت وزیران .میباشد

ماده ۴۹- حقوق مصرف کننده در زمان استفاده از وسایل پرداخت الکترونیکی به موجب قوانین و مقرراتی است .که توسط مراجع قانونی ذیربط تصویب شده و یا خواهد شد

(M arketing) -فصل دوم- در قواعد تبلیغ

ماده ۵۰- تأمین کنندگان در تبلیغ کالا و خدمات خود نباید مرتکب فعل یا ترک فعلی شوند که سبب مشتبه .شدن و یا فریب مخاطب از حیث کمیت و کیفیت شود

ماده ۵۱- تأمین کنندگانی که برای فروش کالا و خدمات خود تبلیغ میکنند نباید سلامتی افراد را به .خطراندازند

ماده ۵۲- تأمین کننده باید به نحوی تبلیغ کند که مصرف کننده به طور دقیق، صحیح و روشن اطلاعات مربوط .به کالا و خدمات را درک کند

.ماده ۵۳- در تبلیغات و بازاریابی باید هویت شخص یا بنگاهی که تبلیغات به نفع اوست روشن و صریح باشد

ماده ۵۴- تأمین کنندگان نباید از خصوصیات ویژه معاملات به روش الکترونیکی جهت مخفی نمودن حقایق .مربوط به هویت یا محل کسب خود سوء استفاده کنند

ماده ۵۵- تأمین کنندگان باید تمهیداتی را برای مصرف کنندگان درنظر بگیرند تا آنان راجع به دریافت تبلیغات .به نشانی پستی و یا پست الکترونیکی خود تصمیم بگیرند

ماده ۵۶- تأمین کنندگان در تبلیغات باید مطابق با رویه حرفه‌ای عمل نمایند. ضوابط آن به موجب آیین‌نامه‌ای .است که در ماده (۷۹) این قانون خواهد آمد

ماده ۵۷- تبلیغ و بازاریابی برای کودکان و نوجوانان زیر سن قانونی به موجب آیین‌نامه‌ای است که در ماده (۷۹) .این قانون خواهد آمد

فصل سوم- حمایت از «داده‌پیام»های شخصی

(Data Protection -حمایت از داده)

ماده ۵۸- ذخیره، پردازش و یا توزیع «داده‌پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص .بدون رضایت صریح آنها به هر عنوان غیر قانونی است

ماده ۵۹- در صورت رضایت شخص موضوع «داده‌پیام» نیز به شرط آن که محتوای داده‌پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع «داده‌پیام»های شخصی در بستر مبادلات الکترونیکی باید :با لحاظ شرایط زیر صورت پذیرد

.الف- اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند

ب- «داده‌پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع .«داده‌پیام» شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد

.ج- «داده‌پیام» باید صحیح و روزآمد باشد

د- شخص موضوع «داده‌پیام» باید به پرونده‌های رایان‌های حاوی «داده‌پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده‌پیام»هایی ناقص و یا نادرست را محو یا اصلاح کند.

ه- شخص موضوع «داده‌پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه در خواست محو کامل پرونده رایانه‌ای «داده‌پیام»های شخصی مربوط به خود را بنماید.

ماده ۶۰- ذخیره، پردازش و یا توزیع «داده‌پیام»های مربوطه به سوابق پزشکی و بهداشتی تابع آیین‌نامه‌ای است که در ماده (۷۹) این قانون خواهد آمد.

ماده ۶۱- سایر موارد راجع به دسترسی موضوع «داده‌پیام» از قبیل استثنائات، افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسؤول دیدبانی و کنترل جریان «داده‌پیام»های شخصی به موجب مواد مندرج در باب چهارم این قانون و آیین‌نامه مربوطه خواهد بود.

مبحث دوم – حفاظت از «داده‌پیام» در بستر مبادلات الکترونیکی

فصل اول- حمایت از حقوق مؤلف در بستر مبادلات الکترونیکی (Author's Right/ Copyright)

ماده ۶۲- حق تکثیر، اجراء و توزیع (عرصه و نشر) آثار تحت حمایت قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۳/۹/۱۳۴۸ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی مصوب ۲۶/۹/۱۳۵۲ و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۴/۱۰/۱۳۷۹ ، به صورت«داده‌پیام» می‌باشند، از جمله اطلاعات، نرم‌افزارها و برنامه‌های رایانه‌ای، ابزار و روش‌های رایانه‌ای و پایگاه‌های داده و همچنین حمایت از حقوق مالکیت‌های فکری در بستر مبادلات الکترونیکی شامل حق اختراع، حق طراحی، حق مؤلف، حقوق مرتبط (Integrated Circuits & Chips) با حق مؤلف، حمایت از پایگاه‌های داده، حمایت از نقشه مدارهای یکپارچه قطعات الکترونیکی و حمایت از اسرار تجاری، مشمول قوانین مذکور در این ماده و قانون ثبت علائم و اختراعات مصوبت ۱/۴/۱۳۱۰ و آیین‌نامه اصلاحی اجرای قانون ثبت علائم تجارتی و اختراعات مصوب ۱۴/۴/۱۳۳۷ خواهد بود، منوط بر آن که امور مذکور در آن دو قانون موافق مصوبات مجلس شورای اسلامیباشد.

تبصره ۱- حقوق مرتبط با مالکیت ادبی و هنری (Related Rights) که پیش از این به عنوان حقوق جانبی شناخته می‌شدند شامل حقوق مادی و معنوی برای عناصر (Neighboring Rights) مالکیت ادبی و هنری دیگری علاوه بر مؤلف، از جمله حقوق هنرمندان مجری آثار، تولید کنندگان صفحات صوتی و تصویری و

سازمان‌ها و مؤسسات ضبط و پخش می‌باشند که مشمول قوانین مصوب ۳/۹/۱۳۴۸ و ۲۶/۹/۱۳۵۲ مورد اشاره در این ماده می‌باشند.

تبصره ۲- مدار یکپاچه (Integrated Circuit) یک جزء الکترونیکی با نقشه و منطقی خاص است که عملکرد و کارائی آن قابلیت جایگزینی با تعداد بسیار زیادیی از اجزاء الکترونیکی متعارف را داراست. طراحی‌های نقشه، جانمائی و منطق این مدارها بر اساس قانون ثبت علائم و اختراعات مصوب ۱/۴/۱۳۱۰ و آیین‌نامه اصلاحی اجرای قانون ثبت علائم تجارتی و اختراعات مصوب ۱۴/۴/۱۳۳۷ مورد حمایت میباشد.

ماده ۶۳- اعمال موقت تکثیر، اجراء و توزیع اثر که جزء لاینفک فراگرد فنی پردازش «داده‌پیام» در شبکه‌ها است از شمول مقرر فوق خارج است.

فصل دوم- حمایت از اسرار تجاری (Trade Secrets)

ماده ۶۴- به منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید.

ماده ۶۵- اسرار تجاری الکترونیکی «داده‌پیام»ی است که شامل اطلاعات، فرمول‌ها، الگوها، نرم‌افزارها و برنامه‌ها، ابزار و روش‌ها، تکنیک‌ها و فرایندها، تألیفات منتشر نشده، روش‌های انجام تجارت و داد و ستد، فنون، نقشه‌ها و فراگردها، اطلاعات مالی، فهرست مشتریان، طرح‌های تجاری و امثال اینها است، که به طور مستقل دارای ارزش اقتصادی بوده و در دسترس عموم قرار ندارد و تلاش‌های معقولانه‌ای برای حفظ و حراست از آنها انجام شده است.

فصل سوم- حمایت از علائم تجاری (Trade Names)

ماده ۶۶- به منظور حمایت از حقوق مصرف کنندگان و تشویق رقابت‌های مشروع در بستر مبادلات الکترونیکی علائم (Online) و یا هر نوع نمایش برخط (Domain Name) استفاده از علائم تجاری به صورت نام دامنه تجاری که موجب فریب یا مشتبه شدن طرف به اصالت کالا و خدمات شود ممنوع و متخلف به مجازات مقرر در این قانون خواهد رسید.

باب چهارم – جرایم و مجازات‌ها

مبحث اول- کلاهبرداری کامپیوتری

ماده ۶۷- هر کس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده غیر مجاز از «داده‌پیام» برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف «داده‌پیام» مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیر 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.

تبصره- شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده میباشد.

مبحث دوم- جعل کامپیوتری

ماده ۶۸- هر کس در بستر مبادلات الکترونیکی، از طریق ورود، تغییر، محو و توقف «داده‌پیام» و مداخله در پردازش «داده‌پیام» و مداخله در پردازش «داده‌پیام» و سیستم‌های رایانه‌ای، و یا استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء- مثل کلید اختصاصی- بدون مجوز امضاء کننده و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی ویا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل «داده‌پیام» دارای ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان «داده‌پیام»های معتبر استفاده نماید جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون (۰۰۰/۰۰۰/۵۰) ریال محکوم میشود.

تبصره- مجازات شروع به این جرم حداقل مجازات در این ماده می‌باشد.

مبحث سوم- نقض حقوق انحصاری در بستر مبادلات الکترونیک

فصل اول- نقض حقوق مصرف کننده و قواعد تبلیغ

ماده ۶۹- تأمین کننده متخلف از مواد (۳۳)، (۳۴)،(۳۵)،(۳۶) و (۳۷) این قانون به مجازات از ده میلیون (۰۰۰/۰۰۰/۱۰) ریال تا پنجاه میلیون (۰۰۰/۰۰۰/۵۰) ریال محکوم خواهد شد.

.تبصره- تأمین کننده متخلف از ماده (۳۷) به حداکثر مجازات محکوم خواهد شد

ماده ۷۰- تأمین کننده متخلف ازمواد (۳۹)،(۵۰)،(۵۱)،(۵۲)،(۵۳)،(۵۴)،(۵۵) این قانون به مجازات از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا یکصد میلیون(۱۰/۰۰۰/۰۰۰) ریال محکوم خواهد شد.

.تبصره ۱- تأمین کننده متخلف از ماده (۵۱) این قانون به حداکثر مجازات در این ماده محکوم خواهد شد

.تبصره ۲- تأمین کننده متخلف از ماده (۵۵) این قانون به حداقل مجازات در این ماده محکوم خواهد شد

فصل دوم- نقض حمایت از «داده‌پیام»های شخصی/ حمایت از داده

ماده ۷۱- هر کس در بستر مبادلات الکترونیکی شرایط مقرر در مواد (۵۸) و (۵۹) این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود.

ماده ۷۲- هر گاه جرایم راجع به «داده‌پیام» های شخصی توسط دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسؤول ارتکاب یابد، مرتکب به حداکثر مجازات مقرر در ماده (۷۱) این قانون محکوم خواهد شد.

ماده ۷۳- اگر به واسطه بی‌مبالاتی و بی احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرایم راجع به «داده‌پیام»های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل پنجاه میلیون (۵۰/۰۰۰/۰۰۰) ریال محکوم می‌شود.

مبحث چهارم- نقض حفاظت از «داده‌پیام» در بسترمبادلات الکترونیکی

فصل اول-نقض حق مؤلف

ماده ۷۴- هر کس در بستر مبادلات الکترونیکی با تکثیر، اجرا و توزیع (عرضه و نشر) مواردی که در قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۳/۹/۱۳۴۸ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی مصوب ۲۶/۹/۱۳۵۲ و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹/۴/۱۰ منوط بر آنکه امور مذکور طبق مصوبات مجلس شورای اسلامی مجاز شمرده شود، در صورتی که حق تصریح شده مؤلفان را نقض نماید به مجازات سه ماه تا یک سال حبس و جزای نقدی به میزان پنجاه میلیون (۵۰/۰۰۰/۰۰۰) ریال محکوم خواهد شد.

فصل دوم- نقض اسرار تجاری

ماده ۷۵- متخلفین از ماده (۶۴) این قانون و هر کس در بستر مبادلات الکترونیکی به منظور رقابت، منفعت و یا ورود خسارت به بنگاه‌های تجاری، صنعتی، اقتصادی و خدماتی، با نقض حقوق قراردادهای استخدام مبنی برعدم افشای اسرار شغلی و یا دستیابی غیرمجاز، اسرار تجاری آنان را برای خود تحصیل نموده و یا برای اشخاص ثالث افشا نماید به حبس ازشش ماه تا دو سال و نیم، و جزای نقدی معادل پنجاه میلیون (۵۰/۰۰۰/۰۰۰) ریال محکوم خواهد شد.

فصل سوم- نقض علایم تجاری

ماده ۷۶- متخلفان از ماده (۶۶) این قانون به یک تا سه سال حبس و جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا یکصد میلیون (۱۰/۰۰۰/۰۰۰) ریال محکوم خواهند شد.

فصل چهارم- سایر

ماده ۷۷- سایر جرایم، آیین دادرسی و مقررات مربوطه به صلاحیت جزایی و روش‌های همکاری بین‌المللی قضایی جزایی مرتبط با بسترمبادلات الکترونیکی به موجب قانون خواهد بود.

باب پنجم- جبران خسارت

ماده ۷۸- هرگاه در بستر مبادلات الکترونیکی در اثر نقص یا ضعف سیستم مؤسسات خصوصی و دولتی، به جز در نتیجه قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود، مؤسسات مزبور مسؤول جبران خسارت وارده میباشند مگر اینکه خسارات وارده ناشی ازفعل شخصی افراد باشد که در این صورت جبران خسارات بر عهده این اشخاص خواهد بود.

باب ششم- متفرقه

ماده ۷۹- وزارت بازرگانی موظف است زمینه‌های مرتبط با تجارت الکترونیکی را که در اجرای این قانون مؤثر میباشند شناسائی کرده و با ارائه پیشنهاد و تأیید شورای عالی فناوری اطلاعات، خواستار تدوین مقررات مربوطه و آئین‌نامه‌های این قانون توسط نهادهای ذی‌ربط شود. این آیین‌نامه‌ها مقررات پس از تصویب هیأت وزیران به مرحله اجرا در خواهند آمد.سایر آیین‌نامه‌های مورد اشاره دراین قانون به ترتیب ذیل تهیه خواهند شد:

الف- آیین‌نامه مربوطه به مواد(۳۸) و (۴۲) این قانون به پیشنهاد وزارتخانه‌های بازرگانی، امور اقتصادی و دارائی، سازمان مدیریت و برنامه‌ریزی کشور و بانک مرکزی جمهوری اسلامی ایران تهیه و به تصویب هیأت وزیران خواهد رسید.

ب- آیین‌نامه مربوط به مواد (۵۶) و (۵۷) این قانون به پیشنهاد وزارتخانه‌های بازرگانی و فرهنگ و ارشاد اسلامی و سازمان مدیریت و برنامه ریزی کشور تهیه و به تصویب هیأت وزیران خواهد رسید.

ج- آیین‌نامه مربوط به ماده (۶۰) این قانون به پیشنهاد وزارت بهداشت، درمان و آموزش پزشکی و سازمان مدیریت و برنامه‌ریزی کشور تهیه و به تصویب هیأت وزیران خواهد رسید

حضرت امام حسین(ع):

«هر کس گره از کار مسلمانی بگشاید خداوند در دنیا و آخرت گره از کارش می گشاید»

التماس دعا-دکتر مصطفی پیرعلی25-6-1397