فهرست

فصل اول

فناوری اطلاعات

فناوری اطلاعات

فناوری اطلاعات به فرایند دانش و روش های بکارگیری آن در تولید، پردازش، انتقال و به جریان انداختن اطلاعات اطلاق میشود. فناوری اطلاعات عبارت از گردآوری، سازمان دهی، ذخیره‌سازی و نشر و استفاده از اطلاعات در قالب صوت، تصویر، گرافیک، متن، عدد و ... با استفاده از ابزار رایانه‌ای و مخابراتی و ... است. اعضای خانواده فناوری اطلاعات عبارتند از : رایانه های بزرگ ، ریز رایانه ها ، لوح های فشرده ، تلفن هاب بی سیم ، مودم ، چاپگرهای لیزری و رنگی ، تلفن های همراه ، تصاویر متحرک و رایانه ای (انیمیشن)، شبیه سازی رایانه ای ، منابع کمک آموزشی رایانه ای ، نشر الکترونیکی ، دوربین دیجیتالی، آموزش از راه دور ، دی.وی.دی، نمابر، فیبر نوری، رادیو ضبط و تلویزیون دیجیتالی، دیسکت ، نظام اطلاعات جغرافیایی ، بزرگراه های اطلاعاتی ، شبکه های رایانه ای (محلی و جهانی) ، فرا رسانه ای ها ، فرا متن ها ، اینترنت ، جاوا ، لوح فشرده لیزری، چند رسانه ای ها، نرم افزارها، شبکه، ابر رایانه ها، تلفن ویدیویی، واقعیت های مجازی، شبکه های گسترده جهانی، وب و مانند آن ها. همان گونه که در تعاریف فوق شاهد هستیم منظور از فناوری در اینجا هر گونه فرایند و روش و ابزاری است که به تولید، انتشار و انتقال بهتر و مطلوبتر اطلاعات مدد رساند.

مزایا و معایب فناوری اطلاعات

در خصوص مزایای استفاده از فناوری اطلاعات مطالب زیادی مطرح است اما نباید این موضوع را از نظر دور داشت که هم در استفاده از این فناوری ها با مشکلات و محدودیت هایی روبرو هستیم و هم استفاده از این فناوری ها آثار نامطلوب و معایبی به همراه دارد. در مورد اول کاربرد فناوری ها در آموزش مستلزم وجود امکانات سخت افزاری و نرم افزاری است که در هر دو مورد نظام آموزشی ما با شرایط مطلوب فاصله زیادی دارد . به عنوان نمونه نسبت تعداد رایانه های موجود به دانش آموز در مدارس بسیار پایین است . و حتی برخی از مراکز آموزشی فاقد حتی یک رایانه هستند. البته فناوری اطلاعات محدود به استفاده از رایانه نیست و رایانه تنها یکی از مجموعه ابزار فناوری است . از دیگر زیر ساخت ها برای آموزش های الکترونیک خطوط دیتا و امکان ارتباط اینترنتی است که در این زمینه هم با مشکلات زیادی مواجهیم . عدم پوشش کامل کشور و سرعت بسیار پایین و هزینه بالا از آن جمله اند .تعیین حد اکثر ۱۲۸کیلو بایت سرعت برای کاربران خانگی اینترنت نمونه بارز این موضوع است که آقای سلیمانی وزیر ارتباطات و فناوری اطلاعات در بخش گفتگوی ویژه خبری اخبار ۲۲:۳۰شبکه دو سیما مورخ ۸۵/۱۰/۲۰ ضمن تأیید این موضوع عدم وجود زیرساخت های لازم برای سرعت های بالاتررا دلیل این امر اعلام کردند. در حالیکه در کشور های توسعه یافته تمام منازل و مراکز آموزشی و تجاری بطور شبانه روزی به خطوط پر سرعت اینترنت متصل هستند .از سوی دیگر استفاده از فناوری های نوین نیاز به امکانات نرم افزاری دارد . صرفا وجود تعدادی رایانه نمی تواند به معنی استفاده از آن باشد. هنوز فرهنگ استفاده از فناوری های نو در جامعه ما فراگیر نشده است و شاهد نوعی واپس ماندگی فرهنگی در این عرصه هستیم. چراکه برخی ادارات با داشتن منابع مالی زیاد اقدام به خرید دستگاه های پیشرفته و از جمله رایانه می کنند ولی از آنها برای اهداف سازمانشان به نحو مطلوب استفاده نمی کنند. در ادارات در دوایر مختلف تعدادی رایانه وجود دارد ولی گویا این دوایر کاملا با هم بیگانه اند. مثلاً در صندوق بیمه محصولات کشاورزی هرسال یک کشاورز باید ساعت ها وقت خود را صرف پرکردن فرم های تکراری کند باوجود این که درختان و باغ ها از جایشان حرکت نکرده و تغییر مکان نداده اند ولی گویا در مسئولین هیچ اعتقادی به امکان استفاده از حداقل امکانات رایانه ای وجود ندارد.از دیگر معایب این روشها می تواند سطحی بار آمدن دانش آموزان و عادت به کپی برداری از کار دیگران باشد. امکان جستجوی مطلب مورد نظر دانش آموز را از مطالعه یک

کتاب یا مقاله بی نیاز کرده صرفاً به بخش مورد نظر مراجعه می کند. همچنین وجود مطالب متنوع و قابل دسترسی و چاپ این امکان را به افراد می دهد که به راحتی حاصل زحمات دیگران را کپی برداری کرده با نام خود تحویل دهد. این موضوع و سایر سوء استفاده ها از اینترنت از مواردی است که به عنوان معایب این شیوه های آموزشی مطرح می شود. ولی علیرغم این معایب و کاستی ها شکی نیست که لازمه زندگی در جهان امروزی مجهز شدن به این فناوری های نو و استفاده از آن در زندگی روزمره و از جمله در نظام آموزشی است.

اهم معایب و مزایای فناوری اطلاعات

مزایای استفاده از سیستم های اطلاعاتی	معایب استفاده از سیستم های اطلاعاتی
اجازه مهندسی مجدد را می دهد: به واسطه تغییر قوانین	مهندسی مجدد می تواند یک فرآیند بسیار پیچیده باشد، که اغلب با مقاومت کارکنان و مدیریت همراه می شود
موجب کاهش استفاده از منابع انسانی و موانع دست و پاگیر انسانی می گردد	اتوماسیون ها جایگزین عملیات کارمندان می شوند و اعتراضات بسیاری به علت بیکاری بوجود خواهند آمد
باعث کوتاهتر شدن زمان واکنش ها در یک رقابت می شود؛ ایجاد بازده بالا در بازار	کارگران در برابر این مسئولیت بیشتر و نیاز به کارایی بالاتر از خود مقاومت نشان می دهند، مرزهای بین کار، خانواده، تفریح و سرگرمی به تدریج به خطر می افتد
کمک در جمع آوری، یکپارچه سازی، مقایسه، تجزیه و تحلیل و پخش اطلاعات داخلی و خارجی به منظور سرمایه گذاری به موقع. شیوه ای موثر و کارآمد برای پشتیبانی از مدیران برای حمایت از اولویت های مدیریت	نگرانی در زمینه امنیت اطلاعات افزایش می یابد و حفظ حریم شخصی به عنوان یک تهدید بزرگ مطرح می شود
سرعت تجدید فن آوری اطلاعات را تسریع می بخشد	کسب دانش بیشتر به کارمندان اجازه می دهد تا برای خود شغل های مناسبتری پیدا نمایند
اجازه می دهد تا دسترسی آسان به اطلاعات با هزینه ای کم امکان پذیر باشد. انبوه اطلاعات کمک می کند تا تصمیم گیری هایی سودمند تر اتخاذ شود	اضافه بار اطلاعات: مردم در بین انبوه اطلاعات موجود، زمان و انرژی بیشتری را صرف بدست آوردن اطلاعات مهم می کنند
استفاده گسترده از فناوری اطلاعات را اموجب می شود، صرفه جویی در وقت و هزینه ها	کسب و کارها به راحتی ممکن است بواسطه مختل شدن سیستم های اطلاعاتی آسیب پذیر شوند، این امر بستگی به آن دارد که آن کسب و کار تا چه اندازه وابسطه به فناوری اطلاعات باشد

فصل دوم

رویکردهای فناوری اطلاعات

فناوری و رویکردهای متفاوت

مناقشه های بسیاری در مورد تعریف و سطوح فناوری وجود دارند. بی تردید، یکی از مهمترین و ابتدایی ترین مضامینی که در فلسفه فناوری مورد توجه است، همین تعریف فناوری است. یکی از مهمترین رویکردها در تعریف فناوری، مبتنی بر نگاه ویتگنشتاین به تعریف- به صورت عام- است. ویتگنشتاین بر خلاف سنت جوهراندیش تاریخ فلسفه که مفهوم یا شیئی را با جوهر و ماهیتش تعریف می کند، معتقد بود سودای تعریف جامع و مانع مبتنی بر ماهیت را باید رها کرد و به کاربرد مفاهیم نظر نمود. به همین جهت، اگر می خواهیم بدانیم فناوری یا هنر چیستند، باید به سراغ زبانهای مختلف برویم و ببینیم در این زبانها این مفاهیم چه کاربردی دارند و چگونه به کار برده می شوند.

با همه اینها، چه تعریفهای ماهیت گرا و چه تعریفهای غیرماهیت گرا در فناوری گاهی سخت افزارانه و گاهی نرم افزارانه هستند. در تلقی سخت افزارانه از فناوری، این ساحت ابزارها و وسایلی قلمداد می شود که زندگی ما را کارآمدتر و راحت تر می سازد. تعریف نرم افزارانه بیشتر به فکر و نظری توجه دارد که پشت سر این ابزارها قرار دارند. در تاریخ فلسفه فناوری، دیدگاه سخت افزارانه نسبت به دیدگاه نرم افزارانه مقدم است.

در واقع، مشکلات دیدگاه سخت افزارانه باعث شد متفکران فناوری به اندیشه و رویکردی که ابزارهای فناورانه را به وجود می آورند، توجه خاصی نشان دهند. با این حال، دیدگاه نرم افزارانه هم خالی از مشکل نیست. یکی از این مشکلات آن است که این دیدگاه نمی تواند نقش نهادها و سازوکارهای اجرایی، حقوقی و اخلاقی را که در سامان فناوری نقش دارند، در نظر بگیرد. این خلل باعث توجه به تعریفی شد که به تعریف نهادافزارانه از فناوری معروف است، یعنی مجموعه ای از نهادها که نهادهای سخت افزارانه، نرم افزارانه و دیگر نهادها هستند که در تعریف فناوری دخالت دارند. تعریف نهادافزارانه هم به دلیل کم رنگ بودن نقش انسان در آن، به تعریف دیگری منجر شد که بدان تعریف انسان افزارانه می گویند. در این رویکرد، نسبت نهادهای فناوری و انسان بسیار مورد توجه قرار گرفته است.

نگاه دیگر به تعریف فناوری، تقسیم آن به تعریفهای ریز و کلان است. تعریف کلان هر ابزار محاسباتی و عقلانی را فناوری می نامد. به عنوان مثال، در ورزش ابزارهای زیادی برای فعالیت بهتر موجودند که اینها در این تعریف کلان، فناوری نامیده می شوند. ابزارهای زیادی که در جهان قدیم برای سامان زندگی فردی و اجتماعی به کار می رفتند، اما گستردگی و پیشرفت و عمومیت فناوریهای جدید را ندارند، فناوری در نظر گرفته می شوند. در واقع، در اینجا بهتر است میان تکنیک و فناوری تمایز و تفکیک قایل شد. تکنیک می تواند به فناوری منجر شود، اما باید میان این دو تمایز قایل شد. بسیاری از تکنیکها حتی به فناوری منجر نمی شوند. به طور مثال، روشهای سخنرانی و عادتهای دیدن و آداب دوستیابی هرچند ابزارها و

تکنیکهای سودمند هستند، اما فناوری نامیدن آنها گستره ای کلان را به وجود می آورد که در برخی مواقع بر هدفهای ما تیرگی و ابهام می افکند. با این حال، یک دید کلان نسبت به فناوری، همه این موارد را فناوری در نظر می گیرد.

یک رویکرد میانه به تعریف فناوری، فناوریهای پیش از جهان مدرن را از رده فناوریها بیرون نمی اندازد و آنها را نیز فناوری قلمداد می کند. این رویکرد از جهت انسان شناسی و فلسفی به آن اندازه بزرگ است که بیشتر اشکال فرهنگ مادی را فناوری بداند. این رویکرد همچنین این گونه فرض نمی گیرد که هر فناوری حتماً باید مصنوع آدمی باشد. طبق این چشم انداز، نمی توان فرهنگی را سراغ گرفت که در آن فناوری موجود نباشد، خواه این فرهنگ قدیم یا جدید باشد. با همه اینها، فناوریهای جهان قدیم از اصول بسیار متفاوتی پیروی می کردند و پیدا کردن اصول واحد و مشترک میان فناوری قدیم و جدید، کار بسیاری سختی است.

رویکرد باریک و ریز نسبت به تعریف فناوری، تنها فناوری جهان جدید را فناوری می داند و قایل به تفاوت ماهوی میان این دو نوع فناوری است. قاعده بر این است که فناوری جدید و تأثیرات مختلفش را قابل قیاس با فناوریهای دیگر نمی بینند و معتقدند، این فناوری کاملاً باید به صورت مجزا و مستقل مورد بررسی قرار گیرد. با این فرض، تعریف زیر از فناوری برای تعریف فناوری کاملاً به تلقی مدرن و جدید تأمل می کند و بقیه ابزارها و رویکردهایی را که فناورانه هستند، از دایره منظور خود خارج می کند. البته، آنچه گفتیم تنها بخشی از مناقشات فراوانی هستند که در باب تعریف مفهوم فناوری موجودند با این همه، شاید این مجمل بتواند دورنمای کلی بخشهای زیادی را که در فلسفه فناوری موجودند، پوشش دهد.

رویکردهای چهارگانه

در میان تعاریف گوناگونی که از فناوری مطرحند، شاید تعریف و تقسیم «دون آیدی»، یکی از معروفترین آن باشد. به نظر «آیدی»، چهار نوع رابطه میان «ما- فناوری- جهان» وجود دارند که این روابط ماهیت فناوری را برای ما بهتر و بیشتر مشخص می کنند. یک گونه از رابطه انسان و فناوری، رابطه تجسد یافته است. در این رابطه، فناوری در حکم واسطه ای برای حسهای مختلف انسانی، وارد عمل می شود. هنگامی که ما با عینک شیئی را می بینیم یا با تلسکوب ماه را می ببینم، این عینک و تلسکوب جهان را به گونه ای دیگر از وقتی که ما از آنها استفاده نمی کنیم، بر ما عرضه می کنند. این رابطه که عبارت است از رابطه «من- عینک (یا تلسکوپ)- جهان» همیشه جهان را کوچکتر، بزرگتر، سنگین تر، سبک تر و... از آنچه هستند بر ما عرضه می کند. به همین دلیل، آنها نمی توانند در نقش اندامهای حسی ما وارد عمل شوند. ما به دلیل تأکید بر مؤلفه ای چون بزرگتر دیدن، حاضریم از موقعیت واقعی شیء بگذریم. هنگامی که از طریق اینترنت با کسی دیگر در ارتباط هستیم، گویی فرد نزد ما حضور دارد اما این حضور به صورت متن است. حضور وی به متن محدود است، اما می توانیم ارتباطی را با وی صورت دهیم؛ هرچند این ارتباط با ارتباط حضوری بسیار متفاوت است و حضور اینترنتی چیزی از حضور فیزیکی کم دارد.

نوع دوم رابطه ما با فناوری و رسانه، رابطه هرمنوتیکی است. در این رابطه، فناوری و رسانه را به چیزی فراتر از خود ارجاع می دهند. هنگامی که به نقشه یا متنی توجه می کنیم، آنچه می بینیم خود نقشه یا متن نیست، بلکه به معنایی توجه داریم که این نقشه و متن بدان ارجاع می دهد. این نقشه ها و متون از اینکه جهان باشند، طفره می روند و تنها به جهانی اشاره می کنند. «آیدی» این رویکرد را با عنوان «من-]نقشه- جهان[» مشخص می کند.

نسبت سوم، نسبت غیریت است که در آن، رسانه و فناوری به مثابه چیزی غیر از من فرض می شود. در این نوع رابطه، گویی فناوری و رسانه خود موجودیت دارد.آیدی، شمایلهای دینی و روباتها را نمونه هایی از این نوع فناوری قلمداد می کند. گویی در رابطه ما با آنها، خود این فناوریها یک جهان دیگر هستند و نه آنکه به جهانی دیگر اشاره کنند. در این نسبت، جهان واقعی محو می شود و آنها، ما را به یک جهان ممکن دیگر رهنمون می سازند. به همین جهت، آیدی قدرت این فناوریها را در جدا کردن ما از جهان واقعی به قدرت بازی، ورزش و هنر تشبیه کرده است. آیدی این نسبت را «من – فناوری–] جهان[» می نامد که در آن، فناوری جهان را در حاشیه قرار می دهد.

به نظر آیدی، بزرگترین نماد این نوع رابطه در نسبتی که ما با روباتها برقرار می کنیم، خود را نشان می دهد. نوع چهارم نسبت ما با فناوری، نسبتی است که فناوری به عنوان یک فرآیند آگاهانه وارد ماجرا نمی شود، بلکه فناوری به عنوان یک پیش زمینه و بستر عمل می کند.

آیدی مثالهای این نوع رسانه و فناوری را سیستم کنترل دمای مرکزی ساختمانها و سیستم کنترل ترافیک می داند. این سیستمها جعبه هایی سیاهی هستند که ما به آنها توجه نمی کنیم، اما در زندگی در حال توسعه مان، بسیار بدانها نیازمندیم. این فناوریهای زمینه، هویدا نیستند، اما زندگی ما را شکل می دهند؛ هرچند از تحلیلهای ما فرار می کنند.

رویکردهای چهارگانه آیدی به ما گوشزد می کنند که هر موضعی که ما نسبت به فناوری می گیریم، به تجارتی وارد گشته ایم که در آن سود و زیان وجود دارد. این گونه نیست که فناوریها و رسانه ها ذاتاً زیانبار یا سودمند باشند. سخن بر سر گزینشی است که مانند هر گزینش دیگر، تبعات خواسته و ناخواسته مثبت و منفی دارد. نسبتهای چهارگانه آیدی در یک سطح برای جواب به مواضع افراطی «هایدگر»، «بورگمن» و حتی «دریفوس» ارائه شده اند.

نسبتهای فناوری و اخلاق

این تعریفها و تقسیمها، فضا را برای بحث در مورد نسبت اخلاق و فناوری بهتر آماده می کنند. با توجه به این تقسیم بندی مفهومی که به وجود آمده است، ما می توانیم نسبتهای زیادی را میان فناوری و اخلاق مشخص کنیم که در اینجا به چهار نسبت از این نسبتها اشاره می کنیم:

۱)گاهی منظور از این نسبت آن است که ببینیم فناوری چه پیامدهای اخلاقی داشته باشد. معمولاً افرادی که نسبت فناوری و اخلاق را در نظر می گیرند، از این نسبت تأثیرهای فناوریهای مختلف بر اخلاق را مورد توجه قرار می دهند. برخی از پژوهشگران معتقدند، ذیل این بررسی می توان یک مکتب «تأثیرات» را هم مشخص کرد که از تأثیرات فرهنگی، اجتماعی، اقتصادی، روانی و معرفتی فناوریهای جدید سخن می گویند. در اینجا به طور مثال می توان گفت، رایانه چه با انسان می کند و چگونه روابط انسانی وی را تحت تأثیر قرار می دهد؛ اینترنت بر روابط سنتی انسان و بر شخصیت وی چه تأثیر یا تأثیراتی دارد و جهان فناوری زده ما چگونه فرهنگ را از خود متأثر کرده و روابط طبقات اجتماعی را تحت تأثیر قرار داده است. در این راستا، دو رویکرد منفی و مثبت وجود دارند. برخی بر جنبه ها و تأثیرات مثبت این فناوریها اشاره می کنند و عده ای دیگر بر نکاتی دست می گذارند که فناوری با آنها، جامعه انسانی را از اصالت و شکوفایی انداخته است. در این میان، تأثیر فناوری بر ارزشهای اخلاقی هم به دو صورت قابل ردیابی است؛ عده ای معتقدند، فناوری، ارتباطات را گسترش داده، فرصت و فراغتی برای انسان فراهم کرده که به کارهای جدی تر بپردازد و رفاه مادی وی را فراهم می سازد، اما عده ای دیگر، این نکات را در مقابل معایب و ضعفهای فناوری چندان پررنگ نمی دانند. به نظر این افراد، فناوری در مجموع، گونه ای اخلاق مصرفی را دامن زده، روابط انسانی را از حیز انتفاع ساقط کرده و به ارزشهای غنی و اصیل انسانی چون عفت، کرامت، شرافت، اصالت و... آسیب رسانده است. به نظر این افراد، فناوری و کلاً جهان مدرن،

ارزشهای معنوی خانواده را کمرنگ ساخته، انسانها را تنها و بی مبنا کرده و در نهایت مشکلات معنوی و اخلاقی بسیاری را به وجود آورده است.

۲)معنای دیگری که می توان از نسبت فناوری و اخلاق گرفت، تأثیری است که فناوری بر نظریه های علم و فلسفه اخلاق می گذارد. در اینجا از اخلاق نه هنجارها و ارزشهای اخلاقی، بلکه معرفت اخلاقی مدنظر است و این مبتنی بر تمایزی است که بدان اشاره کردیم. در اینجا سخن بر سر تأثیراتی است که فناوری بر نظریه های اخلاقی بر جای گذاشته اند. در این میان، عده ای معتقدند، این تغییرها و تأثیرها در دل سه اخلاق هنجاری موجود یعنی «فضیلت گرایی»، «تکلیف گرایی» و «فایده گرایی» قابل توسعه و گسترش هستند. در حالی که عده ای دیگر معتقدند، ما باید به دنبال مفاهیم و دیدگاههای تازه تری باشیم. به نظر این عده، به طور مثال در فضای اینترنت مفهوم عمل، خود، عاملیت و... دچار تغییرات ماهیتی شده اند و باید به دنبال دستگاههای مفهومی و تحلیلی جدیدی برای گسترش این موضوعات بود.

۳)معنای سومی که از نسبت اخلاق و فناوری برداشت می شود، ارزشهای اخلاقی است که در شکل گیری فناوری مدرن نقش داشته اند. به تعبیر دیگر، اگر در بند «۱» اشاره کردیم، هدف آن است تا مشخص شود فناوری چه تأثیری بر اخلاق دارد، در اینجا قصد آن است که بفهمیم چه ارزشهای اخلاقی در به وجود آمدن و توسعه فناوریهای جدید نقش ایفا کرده اند. با جهان جدید، چشم انداز و گفتمانی جدید فراروی بشر قد کشیدند. البته این رویکرد جدید، مبتنی بر ارزشها و هنجارهایی بود. برخی متفکران تصریح کرده اند، نشستن نقد به جای فهم، تغییر جهان به جای تفسیر، توجه به آینده به جای گذشته، توجه به حق به جای تکلیف و عاقبت توجه به فرد به جای جمع، برخی از تغییرهای ارزشی هستند که بشر جدید به خود دیده است. در این راستا، نمی توان خاستگاههای ارزشی فناوری را نیز بدون این تغییرهای ارزشی دریافت. مکتب ساختارگرایی اجتماعی حتی ارزشهای دخیل در فناوری را از اولین مرحله تصمیم گیری تا ساخت یک فناوری مورد توجه قرار می دهد. پژوهشگران این عرصه این کار را برای فناوریهایی چون دوچرخه،

اتومبیل، نیروگاهها و... به انجام رسانده اند. هرچند در اینجا هم شاهد نگاههای متفاوتی هستیم، اما یکی از نسبتهای میان اخلاق و فناوری، خاستگاههای ارزشی و اخلاقی فناوری به شمار می آید.

۴)معنای چهارمی که از نسبت اخلاق و فناوری به دست می آید، اخلاقی است که افرادی که با فناوری سر و کار دارند، باید رعایت کنند. این امر هم شامل افرادی است که فناوری را به وجود می آورند و هم کسانی که آن را به کار می برند و هم افرادی که آن را تحلیل و نقد می کنند. به طور مثال، مهندسان به عنوان افرادی که با تولید فناوری سر و کار دارند، باید اصولی چون وفاداری به شرکت متبوع خود یا تلاش برای ساخت فناوریهایی با امنیت بالا را مدنظر قرار دهند. از سوی دیگر، استفاده از فناوری هم به اخلاق خاصی نیاز دارد و در هر دوی این زمینه ها، می توان کدهای اخلاقی را مورد توجه قرار داد، چنانکه بسیاری سعی کرده اند این کدهای اخلاقی را ارائه کنند. علاوه بر این، نقد فناوری هم مانند هر نقدی دیگر به اخلاقی نیاز دارد. البته در این راستا، می توان همه مواردی را که ذیل عنوان اخلاق نقد از آنها یاد می کنند، برای اخلاق نقد فناوری نیز در نظر گرفت.

فصل سوم

اخلاق و آداب فناوری اطلاعات

تعاریف و مفاهیم

دو کلمه یا اصطلاح اخلاق و آداب در حوزه های فلسفی در زبان فارسی به کرات معادل یا به جای هم به کار رفته اند و این امر درحوزه آداب و اخلاق فناوری اطلاعات هم دشوارساز گردیده و خواهد گردید. آنچه به عنوان" آداب اطلاعاتی " مطرح می شود در حوزه اخلاق و فناوری اطلاعات بحث می شود و در مواردی این دو به یکدر تعریف Moral مفهوم به کارگرفته می شوند .اخلاق در ترجمه واژه به "قواعد و اصول تعیین کننده رفتارهای خوب و بد از منظر ارزش وناظر بر Ethics داوری "اشاره دارد در حالیکه آداب در ترجمه واژهقواعد اخلاقی پایشگر رفتار حرفه ای، کاری برای ترسیم مجموعه ایاز ضوابط توافقی " است .در تعریفی دیگر" سامانه قواعد اخلاق ورفتاری را آداب گفته اند و در همین جا آن را شاخه ای از فلسفهمبتنی بر ضوابط اخلاقی "دانسته ان .بنابراین به نظر می رسدآنچه مرسوم و مفید است سوادآموزی در

حوزه آداب فناوری اطلاعاتاست و اخلاق فناوری اطلاعات مولد این آداب، نیاز به پژوهشهای فلسفی گسترد هتری دارد که جزئی از سواد پژوهشی در این زمینه تلقی می گردد .درآموزش حرفه ای و تحصیلی، آموزش آداب فناوری حتی به عنوان ضوابط و معیارهای کاری، بر آموزش مباحث نظریاخلاق فناورانه اولویت دارد، هر چند بدون پژوهش در اخلاق فناوری نمی توان آداب فناورانه را تدوین نمود که برای آن امروزه الگوها ومعیارهای حتی شکلی هم وجود دارد.

ابعاد اخلاقی و فناوری

گزاره اخلاقی، گزاره ای است که موضوع آن یا انسان، یا حالات نفسانی انسان و یا افعال ظاهری انسان است و محمول آن یکی ازمفاهیم خوب و بد، درست یا نادرست، باید و نباید، وظیفه یا تکلیف، مسئولیت و فضیلت و رذیلت است . آنچه در فلسفه اخلاق گفته می شود، جنبه عقلی دارد .هرچند می توانیم در مورد اخلاق سخنانی بگوییم که جنبه عقلی نداشته باشد ام ا آنها در فلسفه اخلاق نمیگنجند .دشواریهای عمومی فلسفه اخلاق 5 علاوه بر مرزهاینامشخص آن با آداب که از آن زاده می شود در تقسیم بندی و وجوه فلسفه اخلاق است که به آن اشاره خواهیم کرد . فلسفه اخلاق که پیشینه ای به اندازه حیات انسانی دارد در بسیار ی موارد در قال بالگوهای سنتی تبدیل به عادات اجتماعی شده و در این جوامع به علت قلت پژوهش، دانش مستقلی نیست .نسبت اخلاق و دین که درامتزاج سترگی به سر میبرند سازگاری اخلاق دینی و اخلاق سنتی رانیازمند پژوهش مستمر کرده که در غیاب آن در جوامع مذهبی با نگرههای اغراق آمیز، می توان اخلاق را به مناسک تبدیل نمود و جامعه مذهبی غیراخلاقی مقید به مناسک را شکل داد کته پایانی دشواری علمی در تحلیل مفاهیم نادقیق توصیف شده در اخلاق عملی است که تدوین آداب اخلاقی را در حوزه های گوناگون با دشواری مواجه ساخته است .در یک تقسیم بندی اولیه، فلسفه اخلاق به سه

حوزه اخلاق توصیفی ، اخلاق دستوری یا هنجاری و اخلاق تحلیلی یا فرا اخلاق تقسیم می شود .در حوزه اخلاق تحلیلی یا فرا اخلاق به مباحثی پرداخته می شوند که مبنای اخلاقی دارند در حالیکه درتقسیم بندی اولیه انواع اخلاق با توجه به واژه معادل در فارسی، آداب عبارت مناسب تری است که مرزهای این دو را تفکیک می نماید،یعنی :آداب توصیفی، آداب هنجاری و آداب تحلیلی.در اخلاق تحلیلی یا فرا اخلاق که جنبه آدابی دارد به سه حوزه زیراعتنا می شود :معنا شناسی اخلاق ، معرفت شناسی اخلاق و وجود یاهستی شناسی اخلاق .اما مباحثی بین رشته ای وجود دارند که درآداب شناسی اخلاق بسیار به کار می آیند از جمله : روان شناسی اخلاق، جامعه شناسی اخلاق، تاریخ اخلاق و مفاهیمی نظیر اخلاق هنری اخلاق فناوری یا اخلاق رایانه ای.گرایش های امروزین و کلی فلسفه اخلاق در هر سه حوزه معناشناسی به همسانی یا ناهمسانی مفاهیم در حوزه های اخلاقی وغیراخلاقی و در معرفت شناسی به واقع گرایی و ناواقع گرایی اخلاقی از منظر استدلال پذیری و ناپذیری آن و در وجود شناسی اخلاق به موضوع کشف یا جعل اخلاق می پردازد .چهار مکتب مهم و مورداعتنا در فلسفه اخلاق، قائلان به وظیفه گروی یا اصالت وظیفه که قائل به کشف در حوزه وجودشناسی اخلاق هستند و قائلان بهنتیجه گری یا اصالت نتیجه که درستی و نادرستی را به آثار مترتبر آن بر می گردانند که قائلین به اصالت فایده هم از این دسته هستند، و طرفداران مکتب اخلاق حق محور ؛ گروه اخیر معتقدنداخلاق مبتنی بر وظیفه نیست بلکه مبتنی بر حق است و مکتب چهارمکه مسلک اخلاقی فضیلت محور است تشکیل می دهند . گروه چهارم از قائلین به مکتب اخلاق عامل تلقی می شوند که وجه دیگرآن اخلاق برای ناظر است . اشاره به طبقه بندی های ف و ق درعمل برای تنظیم کنندگان آداب حرفه ای و فنی که واجد وجوه اخلاقی انجام عمل تخصصی و پاسخ به پرسشهای است در حوزه اجتماعی به کارگیری فناوری در گستره همگانی، دغدغه فن سالارانه و جامعه شناسان و حقوق دانان است. فرانک وبستر "در تبیین دیدگاه های" امانوئل کاست لز"در مقوله اطلاعات و تغییر شهری "می نویسد : "در عین حال این گزاره که پسانوگرایی فاقد اساس، انسجام و حتی

جنبه های اخلاقی است به هیچ وجه نباید تفسیری از محکوم کردن آن داشت .کاملاً برعکس این جدی گرفتن ظواهر پدیده ها و تغییر ناپذیر دانستن شهرها می تواند نکته ای مثبت در این تفکر تلقی شود ."هر چند گروهی دیگر بازگشت مجدد به مفاهیم اخلاقی و مذهبی در عصر پسانو را در جهت عکس این تحلیل می دانند و گروهی دیگر بنیاد گرایی اخلاقی را عکس العمل آن میشمارند، که هر دو منظر به نگره هایی در مواجهه با فناوری منجر شده است که طیف قائلین به جبر فناورانه و معتقدین به ویرانگری مظاهر حیات انسانی از جمله محیط زیست به عنوان حاصل لجام گسیختگی مصرف فناوری، به مباحثه با یکدیگر کشانده است .در این میان نگاهی به آرای" پل تیلیش " واجد نکات دیگری است" :فناوری به مثابه یک شکل فرهنگی، امری غیرارزشی و خنثی نیست .بر خلاف ادعای رایج و متعارف فناورها، فناوری ابزاری نیست که کاربرد خیر یا شرش منوط به انتخاب ما باشد .هر چه انجام می دهیم هدفی دارد، رفع این یا آن نارضایی، یا تحقق امری ارزشمند؛ علاقه و نفع ما در فناوری، خود ذاتاً امری ارزشی است .علاوه بر این رشد و تحول فناوری با تخاصمات ارزشی عجین بوده است تحولات فناورانه امروزه، به گونه ای مورد بحث است که نگره هایی نظیر آنچه هایدگر گفته است مورد نقد واقع می شود امروزه مباحثی نظیر شکاف رقمی از جامعه به افراد تسری داده می شود و در این زمینه صحبت از ایجاد کاست های فناوری می شودکه گون های جامعه طبقاتی مدرن است .این گروه راجع به سود برندگان از آنچه انقلاب رقمی می نامند و ملاحظات اخلاقی آن، نظر متفاوتی دارند از جمله" :اگر این انقلاب رقمی به میز محاکمه کشانده شود، مدافع آن مدعی خواهد شد که هر فردی در سراسر پهنه جهان از آن در حال بهره برداری است، در حالی که شاکی ادعا خواهد کرد که این دفاع، میان بخشی از جامعه که در معرض فناوری قرار دارد و بخش د یگر جامعه که به راستی از منافعش منتفع می شود خلط کرده است ..... و سپس بقیه جامعه می مانند که از دور، دستی بر آتش دارند و ناظر این انقلاب هستند و صرفاً منافع آن را مشاهده می کنند ... در اینجا چیزی به نام اطلاعات رقمی آزاد وجود ندارد .... این که چه کسی اعمال مقررات اخلاقی را بازبینی کند و

آیا این نظارت می بایست در سطح ملی یا بین المللی توسط قانونگذاری یا از طرق مقررات نیمه اختیاری باشد، مسأله ای مهم است " از منظری دیگر ، فناوری اطلاعات مورد بحث فلاسفه هم قرار گرفته است . پژوهش5 میلیون دلاری پژوهشگران دانشگاه کارنگی ملون 20 نتیجه ای بسیار غافلگیر کننده داشته است : "هنگامی که به افراد امکان دسترسی به شبکه جهانی اطلاعات داده می شود، آنها در می یابند دچار احساس انزوا و افسردگی شده اند عدم تجسد که ثمره ارتباط مجازی در غیاب حضور جسمانی است نیز موضوع بحثهای جدی است" .جان پری بارلو "می نویسد" :سر حد الکترونیکی، دنیایی است که هم در همه جا هست و هم د ر هیچ کجا، اما در آن جا که بدن ما زندگی می کند، نیست . به نظر می رسد منظور این نظریه پردازان، تنها جسم ما نیست بلکه خلقیات ما نیز هست که اهمیت چیزها را برای ما تعیین می کند . موضع ما در یک زمینه معین که در آن مجبوریم با چیزها و افراد کنار بیای یم و شیوه های بسیاری که طی آنها ناگزیر از نومیدی و شکست و نیز

جراحت و مرگ می شویم .به طور خلاصه منظور آنها از تجسد ما، همه جنبه های تناهی و آسیب پذیری ماست .به این ترتیب پرسش این است که رابطه آتی ما با این جهان، رابطه یک ناظر نا متجسد بی اعتناست یا عاملی متجسد و درگیر.

آنچه" کیرکگور "به عنوان پیامد پوشش دادن نامتمایز و غیرمتعهد اخبار مجسم میکرد، اکنون بر روی شبکه جهانی اطلاعات کاملاًمحقق شده است .به یمن ابرپیوندها، تفاوت های معنی دار در واقع ، همسان شده اند و مربوط بودن و اهمیت داشتن ناپدید شده است. کیرکگور از نیهیلیسم تلویحی این رخداد انتقاد می کند و با اشاره به توجه یکسان خداوند به رستگاری یک گناهکار و سقوط یک گنجشک و این که برای خداوند نه هیچ چیز مهم است و نه هیچ چیز بی اهمیت، اشاره می کند که این اندیشه یکسان نگر شبکه ای، فرد را به آستانه نومیدی هدایت می کند اثرات اجتماعی، فردی و حقوقی به کارگیری فناوری اطلاعات که مسائل روز و مهمی هستند، در بررسی اخلاق و آداب فناوری اطلاعات باید مورد اعتنا واقع شوند. مثلا فقط

تبعات جرم از راه دور و نحوه مقابله با آن می تواند ابعاد پیچیده این دشواریها و لزوم سوادآموزی در مورد آنها را یادآوری کند.

فصل چهارم

جرائم رایانه ای

تعریف جرایم رایانه ای

جرایم سایبری، نوعی از جرایم اینترنتی می‌باشند که شامل جرم‌هایی هستند که در محیط سایبر بوجود می‌آیند، که در این مقاله ما به تعریف محیط سایبر که یک محیط مجازی می‌باشدوبه ویژگی محیط سایبر، بطوریکه کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی در سراسر دنیا دستیابی پیدا کنندوچگونگی ایجادجرایم که در فضای سایبر کپی عین اصل می‌باشدوانواع مجرمین محیط سایبرشامل هکرها، کرکرها، فریک‌های تلفن وانواع جرم‌های ممکن بانام سایبرکرایم ودرموردجرم آینده با نام تروریسم سایبر که مانند تروریست‌های معمولی دارای انگیزه‌های سیاسی برای ارتکاب جرایم هستندو همچنین بحران سازهای سایبر شامل ویروسها، عنکبوتهای موتورهای جستجووپالسهای الکترومغناطیسی، کرمهاوبمب‌های منطقی ودرمورد پلیس سایبر که مطابق با خاص بودن جرم‌های سایبر، نیاز به آموزش‌های خاص دارند و در آخر در مورد روشهای امنیت شبکه وداده‌ها می‌پردازیم.

در ایالات متحده آمریکا تعریف وسیعی از جرم رایانه‌ای به عمل آمده مبنی بر آنکه «هر اقدام غیرقانونی که با یک رایانه یا به کارگیری آن مرتبط باشد را جرم رایانه‌ای می‌گویند. یا هر اقدامی‌که به هر ترتیب با رایانه مرتبط بوده و موجب ایجاد خسارت به بزه دیده شود و مرتکب از این طریق منافعی را تحصیل کند، جرم محسوب می‌شود».

در ایران تعریف زیر میان حقوقدانان رایج است:

«آن دسته از جرایمی‌که با سوءاستفاده از یک سیستم رایانه‌ای برخلاف قانون ارتکاب می‌یابد جرایم رایانه‌ای نام دارد. البته این دست از جرایم را می‌توان شامل جرایم سنتی که به واسطه رایانه صورت می‌گیرد از قبیل کلاهبرداری و سرقت و نیز جرایم نوظهوری که با تولد رایانه پا به عرصه حیات گذاشتند دانست، مانند جرایم علیه صحت وتمامیت داده‌ها».

تاریخچه جرائم رایانه ای

با پیدایش کامپیوتر، جرائم کامپیوتری نیز بوجود آمد. تاریخچهٔ جرائم کامپیوتری را می‌توان به سه نسل طبقه بندی نمود. نسل اول که تا اواخر دههٔ ۱۹۸۰ می‌باشد شامل سرقت و کپی برداری از برنامه‌ها و جرائم علیه حریم خصوصی اشخاص مانند سرقت از آثار و تحقیقات افراد بود. نسل دوم که تحت عنوان جرائم داده‌ها نامیده می‌شود تا اواخر دهه ۱۹۹۰ ادامه داشته است.

در این دهه تمامی جرائم علیه تکنولوژی اطلاعاتی، ارتباطاتی، کامپیوتری، ماهواره ای و شبکه‌های بین المللی تحت عنوان جرائم علیه داده‌ها اطلاق می‌شود. نسل سوم که از اواسط دههٔ ۱۹۹۰ شروع می‌شود جرائم کامپیوتری تحت عنوان جرائم سایبر یا جرائم در محیط سایبر معروف گردید. پیشینهٔ تاریخی جرائم کامپیوتری به سال ۱۹۸۵ بر می‌گردد که جرائم کامپیوتری در بر گیرندهٔ جرائمی مانند جاسوسی کامپیوتری، سرقتهای آثار ادبی و سوء استفاده غیر قانونی از سیستم‌های کامپیوتری بود. در دههٔ ۱۹۷۰ مقالات زیادی پیرامون جرائم کامپیوتری در روزنامه‌ها و در بعضی از کتابها نوشته شد ولی با توجه به اینکه نوشته‌های آنها مبتنی بر تحقیقات تجربی نبوده است لذا ارزش علمی نداشته تا بتوان به آنها استناد نمود ولی در اواسط دههٔ ۱۹۷۰ مطالعات تجربی پیرامون جرائم کامپیوتری صورت پذیرفت که در این مطالعات تمامی جرائم کامپیوتری بوقوع پیوسته را شامل نمی‌گر دید.

نمونه‌هائی از تحقیقات هائی که راجع به جرائم اینترنتی صورت گرفته را بطور خلاصه بیان می‌نمائیم: اولین

تحقیقاتی که پیرامون جرائم کامپیوتری صورت گرفت در آمریکا بود که در این تحقیقات به قضیهٔ کلاهبرداری از طریق سوء استفاده از ۵۶ هزار مورد بیمه به ارزش حدوداً ۳۰ میلیون دلار اشاره نمود. مورد دیگر می‌توان به قضیه \"هراشتات\" در آلمان که مربوط به معاملات ارزی خارجی به مبلغ ۲۰۰ تا ۳۰۰ هزار مارک از حساب ارزی بانک هراشتات خارج گردیده و همین امر باعث ورشکستگی این بانک و وارد شدن خسارت به مشتریان گردید.

در دههٔ ۱۹۸۰ که بعنوان نسل دوم جرائم کامپیوتری محسوب می‌گردد. جرائم کامپیوتری فقط محدود به جرائم اقتصادی نبوده و سایر زمینه‌ها را هم که جنبهٔ اقتصادی نداشته مانند دستکاری کامپیوتر بیمارستان‌ها، جعل اسناد با استفاده از کامپیوتر و ورود به اطلاعات خارجی محرمانهٔ آمریکا، انگلستان و چند کشور دیگر دست یافته و این اطلاعات را به ک . گ . ب بفروشند. در دههٔ ۱۹۹۰ که شبکهٔ جهانی (اینترنت) فراگیر شد جرائم کامپبوتری از جنبهٔ اقتصادی وسیعتر گردیده و ابعاد جدیدتری به خود گرفته است. جرائم جدید مانند ورود کرم اینترنتی که برای اولین بار توسط یک دانشجوی آمریکائی ساخته شده بود و باعث شد تا سیستم کامپیوتری حدود ۶۲۰۰ کاربر اینترنت شامل دانشگاهها، سرویسهای نظامی و سایتهای بیمارستانها را مختل نماید. و هزینهٔ تعمیرات سیستمها حدودا\" به مبلغ ۹۸ میلیون دلار بود که بعد از مدتی این دانشجو دستگیر و پس از محاکمه محکوم به پرداخت کلیه مبالغ فوق گردید. در زمینه جرائم کامپیوتری می‌توان به اقدامات زیر اشاره نمود:

-تصویب موافقتنامهٔ جرائم کامپیوتری در سال ۱۹۸۶-۱۹۸۵ توسط شورای اروپا گامهای زیادی برای تدوین قوانین مرتبط با جرائم کامپیوتری برداشته شد.

– در سال ۱۹۸۹ کمیتهٔ تخصصی شورای اروپا برای تدوین و یکنواخت نمودن سیاست جنائی مربوط به جرائم کامپیوتری پیشنهادهائی نمود که مورد تصویب شورا نیز قرار گرفت.

-در همایشی که انجمن بین المللی حقوق جزا در سال ۱۹۹۴ داشت یکسری از مسائل را به عنوان جرائم مستقل کامپیوتری تدوین نمود.

-نهایتاً در سال ۲۰۰۱ میلادی شورای اروپا، مبادرت به وضع موافقتامه جرائم کامپیوتری نمود که این موافقتنامه شامل چهار فصل و چهل و هشت گفتار می‌باشد.

در ایران نیز با توجه به توسعهٔ تکنولوژیک وانفورماتیک با گسترش تخلفاتی از قبیل کپی و تکثیر غیر قانونی نرم افزارها و برنامه‌های رایانه‌ای در دیماه ۱۳۷۹ قانون حمایت از پدید آورندگان نرم افزارهای رایانه‌ای به تصویب رسید که آئین نامهٔ آن نیز در ۷۰ ماده به تصویب هیأت وزیران رسیده است.

انواع مجرمین سایبر

هکر: دردهه ۱۹۷۰ واژه هکر به شخصی اطلاق می‌شد که در برنامه نویسی بسیار ماهروباهوش باشد.بعدها دردهه ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم‌های جدید به صورت ناشناس تبحر داشته باشد.امروزه بیشتر با هدف ترساندن هکرها، رسانه‌ها ومقامات مسئول مانند آژانس‌های دولتی وادارات پلیس، این واژه به هرشخصی که مرتکب یک جرم مرتبط با فناوری شود، اطلاق می‌کنند.این درست است که هکرهای کنجکاو میتوتنند سهوا باعث زیان‌های قابل توجهی شوند، اما جستجو برای یافتن اطلاعات وآموزش، نه انتقام گیری یا صدمه زدن به دیگران، عاملی است که باعث می‌شود اکثرهکرها سرگرمی خود را به نحوی بیرحمانه دنبال کنند.

کرکرها: ازسوی دیگر کرکرها هکرهای بدخواهی هستند.آنها به سیستم‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها وکرمهای رایانه‌ای رامنتشر کنند، فایلها را پاک کنند یابعضی انواع دیگرویرانی راببارآورند.اختلاس، کلاهبرداری یاجاسوسی صنعتی(سرقت اطلاعات محرمانه یک شرکت)تنها بخش کوچکی از اهداف احتمالی کرکرها می‌باشد.

تفاوت هکرهاوکرکرها : هکرها دریک مورد مهم با کرکرها تفاوت دارند، کارهایی که آنها انجام می‌دهند معمولاً از روی بدخواهی نیست.انگیزه بیشتر هکرهابرای این کار، تمایل شدید به یادگیری نحوه کار سیستم رایانه، یافتن راهی برای ورود مخفیانه به آنها وپیداکردن سوراخ‌های امنیتی این سیستم هاست هیجان خواندن اطلاعاتی که می‌دانند اجازه دیدن آنهارا ندارندیا انجام کاری که می‌دانند قانونی نیست به لذت دست زدن به چنین تجاربی توسط هکرها به عنوان سرگرمی می افزاید.آنها در فعالیت‌های خود معتقد به نگرش ببین اما دست نزن هستند.

فریک‌های تلفن : شکل دیگر از جرایم رایانه‌ای را"فریک‌های تلفن " مرتکب می‌شوند.فریک‌ها به جای دسترسی به سیستم‌های رایانه ای، ازطریق خطوط تلفن دردنیای سایبر گشت می‌زنند.فریک‌ها از میان اولین هکرها دردهه۱۹۷۰ پدید آمدند.یکی از حوادثی که توسط فریک‌ها بوجود آمده بود در سال ۱۹۷۷ مربوط به اداره پلیس شهر نیویورک می‌شد، فریک‌ها به سیستم تلفن این اداره نفوذ کرده بودند ومتن ضبط شده‌ای را که به تماس گیرندگان خوشامد می‌گفت تغییر داده بودند، در متن ضبط شده جدید گفته می‌شد که افسران پلیس مشغول

خوردن نان شیرینی ونوشیدن قهوه هستند وفر صت جواب دادن به تلفن‌ها را ندارند، این پیام به تماس گیرندگان توجه می‌کرد که در موارد اورژانس با شماره ۱۱۹ تماس بگیرند.

بحران سازهای سایبر

ویروس: ویروس‌ها یا برنامه‌های خود همانندساز، برنامه‌هایی هستندکه با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند ومعمولا از طریق یک دیسکت وگاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند.بعضی ویروسها ممکن است قادر به حمله به فایل‌های سیستم وذوب کردن مادربورد یک رایانه، پاک کردن تمام داده‌های دیسک سخت وازکارانداختن رایانه باشند.

عنکبوت‌های موتورهای جستجووپالس‌های الکترومغناطیس: که می‌توانند دسک سخت یک رایانه را ذوب کنند.

کرم ها: میتوانند به یک سیستم دسترسی پیدا کنندااما نمی‌توانند در خارج از شبکه، برای مثال از طریق یک دیسکت، گسترش پیدا کنند.کرم‌ها در یک رایانه مقیم می‌شوندوفضای رایانه را اشغال می‌کنندتا آنکه رایانه کندشودیا از کار بیفتد.

بمب‌های منطقی: آنها تعمدا زیانبار ساخته می‌شوند اما مانند ویروس‌ها تکثیر نمی‌شوند.آنها طوری طراحی شده اند که طی یک دوره زمانی دررایانه غیرفعال باقی می مانندوسپس با سررسیدن تاریخی که برنامه آنها مشخص شده است منفجر می‌شوند.اهداف این بمب‌ها متفاوت است.

انواع سایبرکرایم

تنوع انواع جرایم ارتکابی در سایبرسپیس شامل جرایم نسل اول کامپیوتری (البته به شکل نوین)ویکسری جرایم بسیار جدید وبی سابقه می‌باشد.

جرایم سنتی درمحیط دیجیتال

جاسوسی رایانه‌ای : جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه ای، تجاری، اقتصادی، سیاسی، نظامی ونیزافشاءوانتقالواستفاده از اسرار است، فرد مرتکب جرم بادستیابی وفاش کردن این اسرار، ضررسیاسی، نظامی، مالی، تجاری بمیکند.این جرم امنیت ملی را با مخاطره مواجه می‌کند.

سابوتاژرایانه‌ای : این جرم باجرم تخریب شباهت بسیاری دارد، هدف مجرم اخلال در نظام سیاسی واقتصادی یک کشوروبالطبع اخلال در امرحکومت است.درواقع اصلاح، موقوف سازی، پاک کردن غیرمجازداده‌ها یا عملیات کامپیوتر به منظور مختل ساختن عملکردعادی سیستم سابوتاژرایانه‌ای گویند.

جعل کامپیوتری: واردکردن، تغییر، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور واهداف سیاسی واقتصادی صورت میگرد.جعل کامپیوتری جعل داده هاست.در جعل کامپیوتر ی عمل ارتکابی برداده‌ها اثر میگذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.

افتراونشر اطلاعات از طریق پست الکترونیک: پست الکترونیک مرسوم‌ترین وگسترده‌ترین سرویس شبکه‌های کامپیوتری وبین المللی است، هرکاربر می‌تواند در شبکه‌های بین‌المللی از طریق یک آدرس مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به آسانی درآن تقلب کرد.این قالبیت پست الکترونیک می‌تواند ابزاری جالب برای نشر اطلاعات مجرمانه یا نشر اکاذیب وافترا به اشخاص باشدواحتمال کنترل اطلاعات برای تهیه کننده کاملا مشکل است ودر عمل به خاطر تعداد بسیار زیاد پست الکترونیک ارسالی، اتخاذ تدابیر کلی وگسترده امنیتی مشکل بوده وتنها برای بخش کوچکی از داده‌ها میسر می‌باشد.

تطهیرنامشروع پول: بدست آوردن پول از طریق غیر قانونی یا پول کثیف، به نحوی که قانونی یا پاک به نظر برسد، از جرایم کلاسیک بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک وشبکه‌های بین‌المللی ارتباطی صورت می پذیرد، نحوهٔ ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط پست الکترونیک یا اینترنت بدون هیچ کونه اثرونشانی درخواست ارسال مبالغی پول به حساب شخص معینی را مینمایندودر تقاضای خود نحوهٔ ارسال پول ودستمزد ومدت استردادرا بیان ودر صورت قبول طرف نوع ونحوه تنظیمات لازم رااعلام می‌دارندواصولا درزمان استردادپول یک عنوان مشروع در تجارت الکترونیک را با منشا تجاری انتخاب وبا هدف خود هماهنگ می نمایند لازم به ذکر است غالب این درخواستها از افراد کشورهایی که از لحاظ تکنولوژی اطلاعاتی وارتباطی وهماهنگی پلیسی در سطح بین‌المللی در درجه پایین تری قراردارند انتخاب می‌شود.

قاچاق موادمخدر: باتوجه به گسترش ارتباطات شبکه‌ای ودرمحیط سایبرودسترسی آسان افرادبه هم از طریق پست الکترونیک واینترنت هرگونه قاچاق مواد مخدر اعم از خرید، فروش، پخش، توزیع یافتن واسطه هاومصرف کنندگان از طریق شبکه‌های کامپیوتری انجام می‌شود.از ویژگیهای آن حذف وکمترنمودن واسطه‌ها وتوزیع کنندگان، گسترش دامنه فعالیت قاچاق چیان تا سطح بین‌المللی، اقدامات پلیس در خصوص کشف فروشندگان وخریداران موادمخدربه سختی ودرمواردی غیر ممکن می‌باشد وضریب اطمینان قاچاق موادمخدر از طریق ارتباطات کامپیوتری وشبکه‌ای بالاتر ازنوع سنتی آن می‌باشد.

جرایم ناظر به کپی رایت وبرنامه ها: هرگونه تکثیر، ارسال، انتقال، در اختیارعامه گذاشتن، پخش گسترده، توزیع، فروش واستفاده غیر مجازاز برنامه‌های کامپیوتری سرقت نرم‌افزار گویند.

جرایم در تجارت الکترونیک : شامل کلاهبرداری در تجارت، تعریف کلی وکلاسیک کلاهبرداری عبارتست از"تحصیل مال دیگری بااستفاده از وسایل متقلبانه"شخصی در نقطه‌ای نامعلوم با واردشدن به شبکه بین‌المللی (مثل اینترنت)ومعرفی خود به عنوان تاجروصاحب یک شرکت معتبردر یک سایت تجاری وارائه "نهادی مشابه اداره ثبت اسنادکه این نهاد عهده دارثبت داده‌های تجاری وتجاراست تا بدین ترتیب تاجر مجوز ورود به عرصه تبادلات الکترونیک را کسب نماید "وهم چنین نهادی که در تجارت الکترونیک به معنای زیرساخت کلید عمومی است.اساس تجارت الکترونیک واز محورهای عمده ومهم آن داشتن این نهاد برای تجار می‌باشد "(تماما غیرواقع وکذب)، اظهار می‌دارد که کالایی را با قیمت معین، نوع وتعداد مشخص در اختیار داشته وقابل عرضه به مشتریان می‌باشد از طرفی خریدارانی که در فضای شبکه‌ها مشغول تجارت الکترونیک(خریدوفروش) می‌باشند پس از دریافت پیام، نسبت به برقراری ارتباط شبکه ای(که غالبا به صورت پست الکترونیک یا ارسال درخواست هز طریق شبکه می‌باشد قبول(خرید)خودرا اعلام ومقداری از کالای موردنظررادرخواست می‌کنند. شخص فروشنده پس از جلب اعتمادطرف مقابل، نسبت به اعلام شماره حساب یا شماره کارت اعتباری خود برای دریافت وجه اقدام مینماید.خریدار نیز پس از پرداخت وجه (غالبا به صورت پرداختهای الکترونیکی) منتظر دریافت کالا می‌باشددر صورتیکه شخص فروشنده قبلا با عملیات‌های متقلبانه ونفوذ توانسته بوده که نهادهای نامبرده را به صورت غیرواقع برای خوداختیار نماید وبدین وسیله مبلغی را من غیرحق کسب نماید.

جرم آینده، تروریسم سایبر: والتر لاکور یک متخصص تروریسم در مرکز مطالعات استراتژیک وبین المللی اشاره می‌کند که یک مقام رسمی سیا ادعا کرده است که می‌تواند "با یک میلیارد دلار و ۲۰ هکر قابل، ایالت متحده را فلج کند."لاکور یادآوری می‌کند که اگرچه هدف تروریست‌ها معمولاً قتل سران سیاسی، گروگان گیری یا بعضا حمله ناگهانی به تسهیلات دولتی یا عمومی است، اما صدمه‌ای که ممکن است به وسیله حمله الکترونیکی به شبکه‌های رایانه‌ای وارد آید می‌تواند"بسیار غم انگیزتر باشدو اثرات آن تا مدت‌ها باقی بماند."لاکور معتقد است

که تروریسم رایانه‌ای ممکن است برای تعداد کثیری از مردم بسیار ویران کننده تر از جنگ‌های بیولوژیک یا شیمیایی باشد. از اقدامات سایبر ترور ارتباط بین تروریست‌ها از طریق شبکه‌های بین‌المللی وتبادل افکار واعمال مجرمانه در سطح بسیار پیچیده است که از ویژگیهای این نوع ارتباط عدم توانایی پلیس در کنترل وشنود این ارتباطات می‌باشد. اما آیا واقعا تروریسم سایبر امکان پذیر است؟ درسال ۱۹۹۱ حین جنگ خلیج فارس که میان عراق وائتلافی از چند کشور به رهبری ایالت متحده در گرفت، یک جوان ۱۸ ساله فلسطینی، متهم به نفوذ به رایانه‌های پنتاگون شد.این مرد جوان ظاهرا به اطلاعات سری مربوط به موشک پیتریوت دسترسی پیدا کرده بود که یک سلاح کلیدی آمریکا برای دفاع در مقابل حمله موشکهای اسکاد عراق محسوب می‌شد.در نفوذ دیگری در همان جنگ چندین نوجوان هلندی به رایانه‌های نظامی، زمینی، هوایی ودریایی ایالت متحده در۳۴ سایت مختلف نفوذ کردند، نفوذکنندگان در یکی از حملات خود به داده‌های بسیار حساسی درباره پرسنل نظامی، نوع ومیزان تجهیزات نظامی فرستاده شده به خلیج فارس، اهداف موشکها و توسعه سیستم‌های تسلیحاتی دست یافتند، در واقع این نوجوانان کرکرهایی بودند که تنها به خواندن این فایلها اکتفا نکردند بلکه اطلاعات مربوط به تحرکات ارتش وتوانایی موشک‌ها را سرقت کردند ودر اختیار عراقی‌ها قراردادند.

پلیس سایبر

بعضی ازافسران پلیس از دهه۱۹۷۰ در زمینه جرایم سایبر آموزش دیده اند وتخصص پیدا کرده اند.جرایم سایبر ممکن است در هر جایی اتفاق بیفتد وغالبا قابل ردیابی نیستند.بیشترادارات پلیس محلی فاقد پرسنل ماهر یا بودجه لازم برای مبارزه با جرایم سایبر هستند به ویژه به این دلیل که این پرونده‌ها ممکن است در آن واحد به حوزه‌های قضایی متعددی مربوط شوند.بنابراین چه کسی مسئول مبارزه با جرایم سایبر خواهد بود؟علاوه برآنچه پلیس رایانه‌ای نامیده می‌شود، شهروندانی نیز وجود دارند که به صورت شخصی به جلوگیری از جرایم سایبر وشناسایی مجرمان کمک می‌کند.هنوز هم مباحثات زیادی درمورد روشهای مورد استفاده توسط مقامات رسمی، دراجرای قوانین مبارزه با جرایم سایبر وجود دارد.پلیس تا چه حد مجاز است که در تحت پیگرد قراردادن ودستگیری مجرمان سایبر به ویژه هکرها پیش رود؟ پلیس تا چه حد اجازه دارد که به حریم خصوصی الکترونیک شهروندان پا بگذارد؟چگونه باید میان حقوق افراد ونیاز مقامات دولتی برای تحقیقات وتشکیل پرونده تعادل برقرار کرد؟ولی با این وجود پلیس توانسته بسیاری از هکرهای بدخواه را شناسایی کند ودر یافتن مجرمان سایبر موفق باشد.

امنیت سایبر

با وجود تبادل عظیم اطلاعات حیاتی ویا خصوصی از طریق اینترنت باید دید اینترنت تا چه حد برای ارسال داده‌های حساس، مطمئن است.وامنیت شبکه‌ها وقتی داده‌ها درآن جریان پیدا می‌کنند چگونه است؟چرا که با وجود جریان داده‌ها روی اینترنت بسیر طبیعی است که فکر کنیم گوش دادن وگرفتن اطلاعات حساس موجود می‌تواند کار ساده‌ای باشد.اما رمزگذاری روی داده ها(غیر قابل فهم یا غیر قابل خواندن داده ها) لایه سوکت‌های امن به عنوان استاندارد ایمنی ورمز عبور معتبر، جداسازی داده‌ها روی کامپیوترهای متعدد وتفکیک پایگاه داده‌ها (جدا نگه داشتن اطلاعات مشتریان)روش‌های پیشرفته در ایمنی داده‌ها می‌باشند که می‌توانند از دستیابی هکرها به داده‌ها جلوگیری کنند.

فصل پنجم

قوانین جرائم رایانه ای در نظام مقدس جمهوری اسلامی ایران

فصل یکم ـ جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

مبحث یکم ـ دسترسی غیرمجاز

ماده (۱) هرکس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

مبحث دوم ـ شنود غیرمجاز

ماده (۲) هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سیستم‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

مبحث سوم ـ جاسوسی رایانه‌ای

ماده (۳) هرکس به طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

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

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

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

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

تبصره ۲ـ آئین‌نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت آن‌ها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارت‌خانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت دولت خواهد رسید.

ماده (۴) هرکس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۵) چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سیستم‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سیستم‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سیستم‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

فصل دوم ـ جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

مبحث یکم ـ جعل رایانه‌ای

ماده (۶) هرکس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد:

الف) تغییر داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها،

ب) تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علایم به آنها.

ماده (۷) هرکس با علم به مجعول بودن داده‌ها یا کارت‌ها یا تراشه‌ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهد شد.

مبحث دوم ـ تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی

ماده (۸) هر کس به طور غیرمجاز داده‌های دیگری را از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۹) هر کس به طور غیرمجاز با انجام اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سیستم‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آنها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۰) هرکس به طور غیرمجاز با انجام اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده(۱۱) : هرکس به قصد به خطر انداختن امنیت یا آسایش عمومی اعمال مذکور در مواد (۸و۹و۱۰) این قانون را علیه سیستم‌های رایانه‌ای و مخابراتی که برای ارائهٔ خدمات ضروری عمومی به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهد شد.

فصل سوم ـ سرقت و کلاهبرداری مرتبط با رایانه

ماده (۱۲) هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۳) هرکس به طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم ـ جرایم علیه عفت و اخلاق عمومی

ماده (۱۴) هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را تولید، ارسال، منتشر، توزیع یا معامله کند یا به قصد ارسال یا انتشار یا تجارت تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ۱ ـ ارتکاب اعمال فوق در خصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازات های فوق می شود. محتویات وآثار مبتذل به آثاری اطلاق می گردد که دارای صحنه ها وصور قبیحه باشد.

تبصره ۲ ـ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک تا پنج میلیون ریال

جزای نقدی محکوم خواهد شد.

تبصره ۳ ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفهٔ خود قرار داده باشد یا بطور سازمان‌یافته مرتکب شود چنانچه مفسد فی‌الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره ۴ ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده (۱۵) هرکس از طریق سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به منظور دستیابی افراد به محتویات مستهجن، آنها را تحریک یا ترغیب یا تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آنها را تسهیل کند یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات.ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو تا پنج میلیون ریال است.

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز تحریک یا ترغیب یا تهدید یا دعوت کند یا فریب دهد یا شیوه ارتکاب یا استعمال آنها را تسهیل کند یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات. تبصره ـ مفاد این ماده و ماده (۱۴) شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می‌شود.

فصل پنجم ـ هتک حیثیت و نشر اکاذیب

ماده (۱۶) هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ـ چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

ماده (۱۷) هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۸) هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سیستم رایانه یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی به طور صریح یا تلویحی نسبت دهد، اعم از این‌که از طریق یاد شده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل ششم ـ مسئولیت کیفری اشخاص

ماده (۱۹) در موارد زیر، چنانچه جرایم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم بوقوع پیوندد.

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

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

تبصره ۱ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره ۲ـ مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود.

ماده (۲۰) اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

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

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

تبصره ۱ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا

نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگری را نخواهد داشت.

تبصره ۲ـ خسارات شاکی خصوصی از اموال شخص حقوقی جبران خواهد شد. در صورتی که اموال شخص حقوقی به تنهایی تکافو نکند، مابه‌التفاوت از اموال مرتکب جبران خواهد شد.

ماده (۲۱) ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کمیتهٔ تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای بکار می‌رود را پالایش کنند. در صورتی که عمداً از پالایش محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینهٔ دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبهٔ نخست به جزای نقدی از بیست تا یکصد میلیون ریال و در مرتبهٔ دوم به جزای نقدی از یکصد میلیون تا یک میلیارد ریال و در مرتبهٔ سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره «۱» چنانچه محتوای مجرمانه به وب‌سایت‌های مؤسسات عمومی شامل نهادهای زیرنظر ولی فقیه و قوای سه‌گانهٔ مقننه، مجریه و قضائیه و مؤسسات عمومی غیردولتی موضوع قانون فهرست نهادها و مؤسسات عمومی غیردولتی مصوب ۱۳۷۳/۴/۱۹ و الحاقات بعدی آن یا به احزاب، جمعیت‌ها، انجمن‌های سیاسی و صنفی و انجمن‌های اسلامی یا اقلیت‌های دینی شناخته شده یا به سایر اشخاص حقیقی یا حقوقی حاضر در ایران که امکان احراز هویت و ارتباط با آنها وجود دارد تعلق داشته باشد، با دستور مقام قضایی رسیدگی‌کننده به پرونده و رفع اثر فوری محتوای مجرمانه از سوی دارندگان، وب‌سایت مزبور تا صدور حکم نهایی پالایش نخواهد شد.

تبصره «۲ «پالایش محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضایی رسیدگی‌کننده به پرونده انجام خواهد شد.

ماده (۲۲) قوهٔ قضائیه موظف است ظرف یک ماه از تاریخ تصویب این قانون کمیته تعیین مصادیق

محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. وزیر یا نمایندهٔ وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر نمایندهٔ مجلس شورای اسلامی به انتخاب کمیسیون حقوقی و قضایی و تأیید مجلس شورای اسلامی اعضای کمیته را تشکیل خواهند داد. ریاست کمیته به عهدهٔ دادستان کل کشور خواهد بود.

تبصره ۱- جلسات کمیته حداقل هر پانزده روز یک بار و با حضور هفت نفر عضو دارای حق رأی رسمیت می‌یابد و تصمیمات کمیته با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره ۲- کمیته موظف است به شکایات راجع به مصادیق پالایش شده رسیدگی و نسبت به آنها تصمیم‌گیری کند. رأی کمیته قطعی است.

تبصره ۳ -کمیته موظف است هر شش ماه گزارشی در خصوص روند پالایش محتوای مجرمانه را به رؤسای قوای سه‌گانه و شورای عالی امنیت ملی تقدیم کند .

ماده (۲۳) ارائه‌دهندگان خدمات میزبانی موظفند به محض دریافت دستور کمیته تعیین مصادیق مذکور در مادهٔ فوق یا مقام قضایی رسیدگی‌کننده به پرونده مبنی بر وجود محتوای مجرمانه در سیستم‌های رایانه‌ای خود از ادامهٔ دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دستور کمیته یا مقام قضایی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبه نخست به جزای نقدی از بیست تا یکصد میلیون ریال و در مرتبهٔ دوم به یکصد میلیون تا یک میلیارد ریال و در مرتبهٔ سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره ـ ارائه‌دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب به

کمیتهٔ تعیین مصادیق اطلاع دهند.

ماده (۲۴) هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند, به حبس از یک تا سه سال یا جزای نقدی از یکصد میلیون تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم ـ سایر جرائم

ماده (۲۵) هرکس مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد:

الف) تولید یا انتشار یا توزیع یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌روند.

ب) فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.

ج) آموزش نحوهٔ ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی.

تبصره ـ چنانچه مرتکب اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

فصل هشتم ـ تشدید مجازات‌ها

ماده (۲۶) در موارد زیر، حسب مورد مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) هر یک از کارمندان و کارکنان اداره‌ها و سازمان‌ها یا شوراها و یا شهرداری‌ها و موسسه‌ها و شرکت‌های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به طور کلی اعضا و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند.

ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد.

ج) داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارایه‌دهنده خدمات عمومی باشد.

د) جرم به صورت سازمان‌یافته ارتکاب یافته باشد .

هـ) جرم در سطح گسترده‌ای ارتکاب یافته باشد.

ماده (۲۷) در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نود و یک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال .

ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال .

ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.

منابع

1. j.harris, M.j.Rabins, C.E.Harris, "Engineering Ethics: concept & cases" , Thomson, 2004.
2. George Reynolds, :Ethics in information Technology" Thomson, 2006.

۳. **دکتر حسین آل کجباف، "جرایم رایانه ای (بزهکاری مدرن) " چاپ نامه الکترونیکی**

٤. سلمان زاده، محمود، «جنگ اطلاعات و امنیت» خبرنامه انفورماتیک، سازمان برنامه و بودجه کشور، شمارهٔ ۸۰ آذرودی ۱۳۸۰، ص ۲۰.

۵. دزیانی، محمد حسن، \"ابعاد جزائی کاربرد کامپیوتر و جرائم کامپیوتری\"، خبرنامه انفورماتیک شورای عالی انفورماتیک کشور، شماره ۵۸، دی و اسفند ۱۳۷۳، صص ۱۵۸-۱۵۷

٦. سازمان ملل، \"نشریهٔ سیاست جنایی\" ترجمهٔ دبیرخانه شورای عالی انفورماتیک – سازمان برنامه و بودجه کشور، جلد اول، مرداد ۱۳۷۶، صفحه ۳۲.

۷. کرمی پور، تکنولوژی آموزشی، شماره۲، آبان ۸۲، ص ۴۵

۸. رئیس دانا ، تکنولوژی آموزشی، ش ۲، آبان ۸۱، ص ۱۶

۹. ربابه فرهادی ؛ نقش فناوری اطلاعات در آموزش ،فصلنامه کتاب ۵۶ ص۱۴۲