



مقدمه ای بر سیاست جنایی ایران در باب جرایم سایبری



محمد حسن زولفانی، استاد ارجمند جرایم سایبری معاونت آموزش دادگستری استان تهران که بسیاری از ساجدهای قضایی استان با چهره او آشنایتند، دارفانی را در سن جوانی وداع کردند. تا کنون مقالات بسیاری از ایشان در ماهنامه قضاوت منتشر شده و خوانندگان محترم نیز با قلم وی آشنا هستند. آن چه می آید قسمت اول مقاله ای دیگر از اوست که به سیاست جنایی ایران در باب جرایم سایبری می پردازد.

■ مقدمه:

جرایم سایبری جزء جرایمی هستند که جدید و ناشی از تکنولوژی مدرن هستند. توجه به این دو نکته یعنی جدید بودن و ناشی از تکنولوژی مدرن بودن، در هر گونه آنالیز جنایی اثر فراوان دارد. این دو نکته زمانی مؤثرتر می شود که بحث از محدوده کلی به جزئی یعنی از سطح بین المللی به سطح ملی، منحصر شود. پدیده مجرمانه سایبری حدود نیم قرن پیش پیدایش یافته و کشورها به تدریج به آن پرداخته اند، اما آهنگ پرداختش به این پدیده مجرمانه جدید یکسان نیست. برخی کشورها خیلی زود (مانند آلمان، آمریکا، انگلستان و...) و برخی خیلی دیر (کشورهای آسیای میانه و برخی از کشورهای خاورمیانه و...) به این پدیده مجرمانه پرداخته اند حاصل این امر نیز به صورت تدوین، عدم تدوین سیاست جنایی جرایم سایبری، بسته به کشور مورد نظر، قابل مشاهده است. شاید اگر بتوان در سایر زمینه های جزئی به راحتی از سیاست جنایی و انواع آن سخن به میان آورد و جرایم سایبری این کار راحت و حتی میسر نیست.

در این متن که به درستی مقدمه ای بر سیاست

جنایی جرایم سایبر است فارغ از ایران یا کشور دیگر، مؤلف قصد پرداختش به مباحث به گونه تفضیلی را ندارد.

■ بخش اول: کلیات

همانگونه که در قبل آمد، هدف بررسی مقدماتی و اختصاری مقوله سیاست جنایی جرایم سایبری در ایران است. اما در این راه نکاتی را باید متذکر شد. اولاً رویکرد بحث بیشتر سیاست جنایی کلی است و نه سیاست جنایی ملی یک کشور خاص اما گاه به وضع کشورمان نیز اشاراتی خواهم داشت. ثانیاً سیاست جنایی خاص مدنظر است و نه عام. یعنی سیاست جنایی در جرایم سایبری مطرح است و سیاست جنایی به صورت عام با ارجاعات کلی و فراوان مدنظر نیست.

ثالثاً از حیث واژگانی تفاوتی بین کشورها و نیز بین جرایم سایبری با سایر مباحث وجود دارد. توضیح مختصر اینکه گاه سخنی از سیاست جنایی در مفهوم کلیات این رشته، تئوریهها، سیر تحول و... است همانند آثار خانم کریستین لازرژ و دیگران.

گاه این بحث ظهور و بروز در جرم یا جرایم

خاصی پیدا می کند. طبعاً این دو گونه روش بحث، تفاوتهایی دارند. اما اینکه چرا بدو سیاست جنایی جرایم سایبری به صورت کلی و فارغ از کشور ایران ذکر و بعد به وضعیت کشورمان اشاره ای خواهد شد. دارای دلایل متعدد است. یکی از مهم ترین این دلایل نوپایی این بحث البته در سطح جامعه علمی است. مطالعات انجام شده غالباً محدود و معدود است که خیلی کم چاپ می شود. در کنار مطالعات برنامه های IT کشورها مبنای مهم بررسی سیاست جنایی است که در کشور به دلایلی که بعداً ذکر می شود و این امر تحقق نیافته است. ادبیات قانونی که اصلاً این قدر سم است که جایی برای هرگونه چالش جدی طرح سیاست جنایی نمی گذارد.

اما نکته دیگر جستجوی واژگانی است. جرایم سایبری در سیر تحول خود، نه تنها چالش مفهومی و مصداقی برای حقوق جزای سنتی ایجاد کرده بلکه ادبیات تخصصی خاص خود را نیز دارا است. برای مثال برای مجرم، در جرایم سایر از اصطلاح هکر استفاده می شود. هکر به معنای مجرم سایبری مجرم کامپیوتری است فارغ از اینکه فصل ارتكابی او، واجد چه وصف کیفی است.

خرده فرهنگ بزهکاری سخنی به میان می آید، در جرمشناسی سایبری سخنی از زمینه سیاست جنایی نیز این ویژگی وجود دارد. در جستجوی واژگانی اگر عین عبارت سیاست جنایی جرایم سایبر، جستجو شود، با عناوین محدودی روبرو می شویم، اما اگر با ادبیات تخصصی جرایم سایبری آشنا باشیم این مشکل حل می شود. در آمریکا و برخی کشورها از

عبارت استراتژی جرایم سایبری به جای سیاست جنایی جرایم سایبر استفاده می شود. در چین، اکوادور، برزیل و برخی کشورهای دیگر از بررسی رهنمود و برنامه های IT در زمینه حقوق و... می باشد. در نتیجه اگر با این واژگان برخورد کردیم باید نگاهی به سیاست جنایی داشته باشیم. علت اینکه تفاوت واژگانی فوق وجود دارد نیز مشخص و طبیعی است. جرایم سایبری ماهیتکار جرایم فنی هستند، طبیعی است که حجم زیاد ادبیات آن فنی باشد.

در ضمن اصطلاحی که به ندرت به جای سیاست جنایی بکار رفته برنامه ملی پیشگیری سایبری و برنامه ملی امنیت سایبری، استراتژی امنیت سایبری و... است. در پاراگرافه مقدونیه و برخی کشورها این عبارت به کار رفته است.

اما نکته سهم دیگر، عبارت سیاست جنایی جرایم سایبری است. به یاد داشته باشیم جرایم سایبری در ادامه سیر تحول جرایم رایانه ای به وجود آمده اند و عام تر از آن هستند یعنی جرایم سایبری اشل بزرگ شده و مضموماً و مصداقاً جرایم کامپیوتری هستند. از این رو در بررسی سیاست جنایی جرایم سایبری فقط به بحث کامپیوتر اکتفا نمی شود بلکه مخایرات، پخش گسترده و تکنولوژیایی از این نوع در محدوده بررسی جای می گیرند و لحاظ می شود. با این کلیات می توان به بحث سیاست جنایی از حیث نوع پرداخت. همانگونه که در ادبیات سیاست جنایی در کشورمان خواه به صورت کتاب یا مقاله و با پایان نامه مشهود است، سیاست جنایی به روش واحدی تقسیم بندی نمی شود. گاه افرادی مانند خانم لازرژ یک بخش کلیات و یک بخش انواع (سیاست جنایی، قضایی، سیاست جنایی تقنینی و سیاست جنایی مشارکتی) را ذکر می کنند.

برخی با استفاده از اصل تفکیک فقط، سیاست جنایی را به سه نوع قضایی، تقنینی و اجرایی تقسیم می کنند. برخی نیز از الگوهای سیاست جنایی تبعیت، نوع سیاست جنایی را حسب آن نوع نامگذاری و بحث می کنند مانند سیاست جنایی خترافی و...

در این مش، چون قصد ورود به جزئیات وجود ندارد و فقط به عنوان یک مطالعه مقدماتی و اولیه، قصد پرداخت به سیاست جنایی داریم، سیاست جنایی را فارغ از تئوریا و مفاهیم کلی، در سه نوع قضایی، اجرایی و تقنینی بحث می کنیم.

۱- رجوع کنید به خیرنامه انفورماتیک، ش ۸۷ - مقدمه ای بر ماهیت و تقسیم بندی تئوریک جرایم سایبری، محمد حسن دزبانی و یا به: جلد اول جزوه آموزش جرایم سایبری و حقوق سایبر همین مؤلف. ۲- رجوع کنید به: جرایم کامپیوتری، جلد اول، دبیرخانه شورای عالی انفورماتیک و نیز جزوه مذکور در پانویس شماره ۱، بحث شروع جرایم سایبری و همچنین خیرنامه انفورماتیک، ش ۹۲، از همین مؤلف.

۳- در سالهای اخیر آثار تقریباً متنوعی در زمینه سیاست جنایی در ایران چاپ شده و نشر یافته است. برخی از این آثار ناظر جرایم خاصی مثلاً مواد مخدر و برخی یکی از انواع سیاست جنایی و برخی کلی و برخی ملی هستند. مثلاً:

- سیاست جنایی، کریستین لازرژ، ترجمه دکتر نجفی ایرند آبادی، چاپ اول ۱۳۷۵، نشر یلدا، ۱۴۶ ص (کلی در بخش اول و ملی در بخش دوم این کتاب)

- نظامهای بزرگ سیاست جنایی، جلد نخست، مهدی دلماس مارتی، ترجمه دکتر نجفی ایرند آبادی، نشر میزان، ۳۴۳ ص (کلی)

- شکنجه در سیاست جنایی ایران، سازمان ملل و شورای اروپا، سید عباس موسوی ۲۸۰ ص (خاص)

- سیاست جنایی در اسلام

و در جمهوری اسلامی

ایران، سید محمد

حسینی، انتشارات سمت

(دانشگاه تهران)، ۲۵۶

ص (کلی)

- سیاست جنایی

قضایی، گودرزی

بروجردی، مرکز مطالعات

توسعه قضایی معاونت

حقوقی و توسعه قضایی

قوه قضائیه، انتشارات سلسبیل ۲۰۰ ص (انواع)

و...

سیاست جنایی تقنینی

فارغ از کلیات و مباحث تئوری که پیرامون سیاست جنایی تقنینی مطرح می شود، در این بخش سخن از سیاست جنایی تقنینی در باب جرایم سایبری است. طبق روشی که در بخش اول مقاله گفته شد، گاه می توان بصورت کلی و فارغ از یک کشور بحث را مطرح کردگاه بحث یک کشور خاصی را می توان مطرح کرد. مشکل جرایم سایبری از اینجا ناشی می شود که این جرایم ماهیتی جهانی دارند و قواعد مرسوم جزایی حاکم بر زمان و مکان بر آنها قابل اعمال نیست. از این رو ناگزیر سیاست جنایی تقنینی جرایم سایبری بدو به گونه کلی و با نگاهی به سیر تحول تقنینی این جرایم مطرح بعد قوانین موجود و لوايح در دست بررسی در کشورمان است اشاراتی خواهم داشت!

از آنجا که جرایم سایبری از اوایل دهه ۶۰ پیدایش یافت و به تدریج تکامل یافت بدو پیشنهادات شکل توسعه نامه داشت. البته وضعیت اروپا و آمریکا یا به تعبیری آمریکا از یک سو و سایر کشورها از سوی دیگر قدری تفاوت می کند. اما با رویکردی حکمی و عام باید بدو به این توصیه نامه ها اشاره کرد. ابتدائاً OECD^(۱) حسب سفارش کاری که اهمیت کرد پدیده جدید را که جرم کامپیوتری به آن می گفتند، بررسی کرد و ۵ دسته مختلف را قابل شد. این دستجات ناظر به کلاهبرداری کامپیوتری، جعل

تخریب کامپیوتری، سابوتاژ کامپیوتری و... بود. مشکل این متن عدم لحاظ ظرایف بین جرایم کامپیوتری موجود و به عبارتی لحاظ نکردن اصل قانونی بودن جرم و مجازات است.

متن پیشنهادی OECD

OECD در سال ۱۹۸۶، ضمن ارائه تجزیه و تحلیل خود، متن زیر را به عنوان خطوط مشترک بین قانون گذاران ملی پیشنهاد کرده است:

الف) ورود، تغییر، پاک کردن و یا متوقف سازی داده های کامپیوتری و یا برنامه هایی که به طور ارادی یا قصد انتقال غیرقانونی وجوه یا هر چیز با ارزش دیگر صورت گرفته باشد؛

ب) ورود، تغییر، پاک کردن یا متوقف سازی داده های کامپیوتری و یا برنامه های کامپیوتری که به صورت عمدی و با قصد

ارتکاب جعل صورت

گرفته باشد؛

ج) ورود، تغییر، پاک

کردن و یا متوقف سازی

داده های کامپیوتری و یا

برنامه های کامپیوتری یا

هر گونه مداخله دیگر در

سیستم های کامپیوتری که

به عمد و با قصد جلوگیری

از عملکرد سیستم

کامپیوتری و یا ارتباطات صورت گرفته باشد؛

د) تجاوز به حقوق انحصاری مالک یک برنامه

کامپیوتری حفاظت شده، با قصد بهره برداری تجاری

از آن برنامه ها و ارائه آن به بازار؛

ه) دستیابی یا استراق سمع در یک سیستم کامپیوتری

و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد

مسئول سیستم مزبور چه (۱) یا تخطی از تدابیر

امنیتی و چه (۲) با هدف غیر شرافتمندانه و یا مضر

صورت گرفته باشد.

توضیح پیرامون متن

متن پیشنهادی OECD در پنج بند ارائه شده است که در فوق آن را از نظر گذرانیدیم. این متن توضیحاتی چند را می طلبد؛

اولاً - به عنوان اولین گام در تقسیم بندی، کاری در خور تقدیر است، اما چون هر کار ابتدایی خصایص اولین گام ها را نیز دارا خواهد بود، از جمله این خصایص جامع و مانع نبودن فهرست است، چون پهنه و گستره جرم مشخص نیست و یا این که تنظیم کنندگان متن بدان اقبالی نداشته اند، بسیاری موارد از قلم افتاده است. معمولاً در اولین گام ها محدوده و وسعت پدیده مشخص نیست.

ثانیاً فهرست حاوی تعبیری است که بسیار کلی است و نمی تواند مورد عمل قرار گیرد، زیرا عمل بدان مساوی با نقض اصل قانونی بودن است.

شاخص برخی از جرایم مندرج در فهرست، سوء نیت مرتکب جرم است که احراز این سوء نیت بدو امر ساده ای نیست. بنابراین OECD باید مرز بین جرایم

راه گونه ای دقیقتر و مطابق اصل قانونی بودن جرایم و مجازات ها و شیوه جزئی گرایبی در جزائیات تبیین می کرد.

ثالثاً- بند اول ناظر به جرایم علیه اموال است. همانگونه که ذکر شد، ماده و بند مربوط بسیار کلی است و ذکر قصد انتقال وجوه یا هر چیز با ارزش، اگر چه مرز جرایم علیه اموال را از دیگر جرایم جدا می کند، اما خود جرایم علیه اموال چندین عمل مجرمانه را در بر می گیرد و گاهی باید مقنن ملی چند جرم علیه اموال در ردیف جرایم کامپیوتری تقنین کند. در یک طرح جهانی یا حتی منطقه ای ذکر این گونه موارد با این کلیت، اثری جز اختلاف در تقنین ها و ایجاد معضلات فراملی ندارد. رابعاً در توضیح متن

ماده مربوط به جعل، اگر چه روش های ارتکاب ذکر شده است، اما دیگر شاخص های جرم جعل ذکر نشده است، از این رو، ماده کلی در این حال مبهم است. بندهای دیگر نیز هر یک به نوع خاصی از جرم کامپیوتری پرداخته است، اما این بندها جامع نیست، زیرا مرز بین

دستیابی غیرمجاز، سوءاستفاده یا استفاده غیرمجاز و... را مشخص نکرده است و با توجه به گستردگی جرایم کامپیوتری، باید بندهای بیشتری بدان اختصاص می یافت.

بدین ترتیب، این فهرست با کلیت و ابهام خود نمی توانست مورد توجه مراجع قانونگذاری ملی قرار گیرد.

■ توصیه نامه شورای اروپا

بعد از این که OECD گزارش خود را که مشتمل بر توصیه مجرمانه تلقی کردن برخی اعمال مذکور در گزارش بود، ارائه کرد، شورای اروپا ابتکار عمل را به دست گرفت و از دید فنی - حقوقی به قضیه نگریتست. آنچه ضرورت پی گیری بعد حقوقی در کنار دیدگاه فنی را بیشتر روشن می ساخت، مسأله آزادی های مدنی، حقوقی فردی و حمایت های قانونی از منافع و مصالح قضایی مختلف بود که از طریق فهرست OECD تأمین نمی شد. شورای اروپا دارای بخش های مختلفی است و یکی از این بخش ها کمیته اروپایی مشکلات ناشی از جرم است. در سال های ۸۶-۱۹۸۵، مسأله جرم کامپیوتری در برنامه کار کمیته اروپایی مشکلات ناشی از جرم قرار گرفت. این کمیته خود کمیته ای تخصصی را برای مطالعه این موضوع ایجاد کرد. این کمیته، کار خود را در سال ۱۹۸۵، شروع کرد و در سال ۱۹۸۹، به پایان برد. کمیته مزبور در آخرین نشست، یک گزارش و یک توصیه نامه (پیش نویس) به کمیته اروپایی مشکلات ناشی از جرم ارائه کرد و این کمیته در ژوئن ۱۹۸۹، آن را بررسی کرد و پس از

تأیید، در تاریخ ۱۳ سپتامبر ۱۹۸۹، به کمیته وزرای شورای اروپا فرستاد. مبنای کار کمیته پاسخ هایی بود که به پرسش نامه های ارسالی از سوی دولت های عضو داده شده متخصصان و مشاوران طراحی شد.

اشکال متنوع جرایم کامپیوتری تعریف و توضیحاتی پیرامون آن ارائه شد. معضلات موجود بر سر راه آیین دادرسی کیفری و حقوق جزایی بین الملل نیز بررسی شده است. در مورد وضعیت بزه دیدگان، ابزارهای امنیتی و بازدارنده و دیگر مطالب نیز نکاتی ذکر شده است. در طبقه بندی شورای اروپا، دو فهرست حداقل و اختیاری به چشم می خورد و در هر فهرست نیز جرایمی ذکر شده است. می توان طبقه بندی شورای اروپا را تا حد زیادی جامع و مانع دانست.

البته به دلیل پیشرفت سریع فناوری کامپیوتری و فناوری اطلاعاتی، صور جدید ارتکاب جرم نیز پدید آمده است و همین امر انجمن بین المللی حقوق جزا (AIDP) را وادار کرد که در گردهمایی خود پیشنهادهای جدیدی در کنار تأیید فهرست های دوگانه شورای اروپا

ارائه کند. در این بخش مفاد این دو فهرست ذکر می شود.

فهرست حداقل جرایم ضروری برای یکپارچه کردن سیاست جنایی مربوط به تقنین جرم کامپیوتری

الف- کلاهبرداری کامپیوتری: وارد کردن، تغییر یا ایجاد وقفه در داده های کامپیوتری یا برنامه های کامپیوتری یا دیگر مداخلات مربوط به پردازش داده ها که نتیجه پردازش داده ها را تحت تأثیر قرار می دهد، خواه موجب ضرر اقتصادی و خواه موجب دست دادن اموال و تصرف آن اموال متعلق به غیر یا قصد کسب منفعت و امتیاز اقتصادی غیرقانونی برای خود یا دیگری شود (طرح جایگزین: با قصد محروم کردن غیرقانونی آن شخص از اموالش).

ب- جعل کامپیوتری: وارد کردن، تغییر، محو یا موقوف سازی داده های کامپیوتری یا برنامه های کامپیوتری یا دیگر مداخلات در زمینه پردازش داده ها، به گونه ای یا تحت شرایطی طبق حقوق ملی تشکیل دهنده جرم جعل است که با همان قصد و موضوع مرسوم چنین جرمی (در جزای کلاسیک) ارتکاب یافته باشد.

ج- خسارت زدن به داده های کامپیوتری یا برنامه های کامپیوتری: محو، خسارت زدن، موقوف سازی یا کم ارزش کردن داده های کامپیوتری یا برنامه های کامپیوتری بدون حق.

د- سابوتاژ کامپیوتری: وارد کردن، تغییر، محو یا موقوف سازی داده های کامپیوتری یا برنامه های کامپیوتری یا مداخله در سیستم های کامپیوتری با قصد ایجاد وقفه در عملکرد کامپیوتر یا سیستم

ارتباطی مخابراتی.

ه- دستیابی غیرمجاز: قطع و استراق بدون حق و یا ابزارها تکنیکی ارتباطات، از و در حدود سیستم یا شبکه کامپیوتری.

ز- تکثیر غیرمجاز یک برنامه کامپیوتری حمایت شده: تکثیر، توزیع یا ارتباط با عامه بدون حق از طریق برنامه کامپیوتری که به وسیله قانون حمایت شده است.

ح- تکثیر غیرمجاز یک توپوگرافی: تکثیر بدون حق یک توپوگرافی که مورد حمایت قانون قرار گرفته است، یا یک محصول نیمه هادی، یا اختراع تجاری یا خارج کردن بدون حق برای این منظور و یک توپوگرافی یا محصول نیمه هادی که برای استفاده به عنوان توپوگرافی ساخته شده است.

■ فهرست اختیاری

الف- تغییر داده های کامپیوتری یا برنامه های کامپیوتری: تغییر داده های کامپیوتری یا برنامه های کامپیوتری بدون حق.

ب- جاسوسی کامپیوتری: بازرسی و تفتیش به وسیله ابزارهای مربوط به افشا، انتقال یا استفاده از اسرار تجاری و بازرگانی بدون حق یا بدون هیچ توجیه قانونی، خواه با قصد صدمه اقتصادی به شخص محق اسرار و خواه با قصد اکتساب امتیاز اقتصادی غیرقانونی برای خود یا شخص ثالث.

ج- استفاده غیرمجاز از کامپیوتر: استفاده از سیستم کامپیوتری یا شبکه، بدون حق، بدین ترتیب که:

۱- ابتکار با پذیرش خطری که موجب ضرر برای شخص محق در استفاده از سیستم است یا صدمه به سیستم یا عملکرد آن انجام شده باشد.

۲- با این قصد که موجب ضرر شخص محق در استفاده از سیستم یا عملکرد آن انجام شده باشد، یا

۳- سبب ضرر به شخص محق در استفاده از سیستم و یا صدمه به سیستم یا عملکرد آن شود.

د- استفاده غیرمجاز از برنامه کامپیوتری حمایت شده: استفاده بدون حق از برنامه کامپیوتری که به وسیله قانون مورد حمایت قرار گرفته است و همچنین تکثیر آن بدون حق، خواه با قصد کسب امتیاز اقتصادی برای خود یا دیگری و خواه به قصد ایجاد صدمه ای برای دارنده حق باشد.

■ توضیح پیرامون متن

تقسیم بندی شورای اروپا از جامعیت بیشتری برخوردار است و به گونه ای سودمند بین انواع مختلف جرایم کامپیوتری تفاوت قایل شده است. در فهرست حداقل که شامل هشت عنوان مجرمانه است، بین جرایم کامپیوتری علیه اموال، جرایم کامپیوتری علیه آسایش عمومی و جرایم خاص فناوری کامپیوتری تفاوت قایل شده است. در توضیح کلاهبرداری کامپیوتری علاوه بر نحوه فعل مرتکب، رکن معنوی را نیز تشریح کرده و در بخش نهایی متن ماده که به صورت بخش جایگزین ذکر شده است، به تفاوت سیستماتیک بین حقوق «کامن لا» و سیستم «حقوق نوشته» توجه کرده است. در جرم جعل نیز

عناصر تشکیل دهنده جرم جعل در حقوق ملی هر کشور را مدنظر قرار داده است. جرایم بعدی که به خود فناوری کامپیوتری مربوط است، مسائلی از قبیل ایجاد خسارت و صدمه اقتصادی. تخریب و . . . مورد توجه قرار گرفته است. از سویی عمده مشکل جرایم کامپیوتری بر سر نحوه دستیابی به داده‌ها، برنامه‌ها و اطلاعات و نحوه استفاده از این داده‌ها و

اطلاعات است، برای این که مرز این اعمال جدا و اصل قانونی بودن رعایت شود، عنصر مادی هر جرم به گونه ای تدوین و تبیین شده است که بتوان با ملاک قرار دادن آنها نوع جرم را تشخیص داد. زیرا مثلاً مرز صرف دستیابی غیر مجاز و ارائه داده‌ها به

شکل غیر مجاز و برای دستیابی به هدف مالی یا غیرمالی، در همین نیت و قصد مجرمانه مرتکب است. گاه مجرم قصد نفوذ در سیستم را دارد تا مهارت خود را به اثبات برساند. اما گاه مجرم از این کار هدف مالی یا غیرمالی نیز دارد. به علاوه در فهرست اختیاری، فهرست جرایمی که برای تکمیل روال قانونگذاری لازم است، ارائه شده است. از جمله کارهای مثبت در ارائه این دو فهرست ذکر توضیحی پیرامون این توضیحات به صورت خلاصه ترجمه از کتاب *Computer related crime*، فصل دو نقل می شود و برای توضیحات کامل می توان به فصل دو کتاب مذکور رجوع کرد:

۱- کلاهبرداری کامپیوتری

پدیده شناسی و وضعیت قضایی

تجارب به اثبات رسانده سیستم های کامپیوتری به دلیل ماهیت خاصشان تبدیل به وسیله ای شده اند که از سویی اشکال مرسوم به واسطه این ابزار مورد استفاده قرار بگیرند و از دیگر سو همانند جرایم مرسوم، اموال را در مقیاس وسیع تر مورد تعدی قرار دهند. ابزارها و روش های معمولی بازدارنده، توانایی برخورد با خسارات ناشی از جرایم کامپیوتری را ندارند. هنوز آمار کلاهبرداری کامپیوتری به جز در زمینه سوء استفاده از صندوق های پرداخت خودکار، سطح بالایی از حیث کمیت را دارا نیست، اما از حیث کیفی، ارقام زیادی را در بر می گیرد. اشکال جدید مجرمانه در مراحل مختلف قابل مشاهده است. مثلاً مرحله ورودی، ارائه داده های غیرصحیح، سوء استفاده از برنامه ها و . . . رویه تبار نشانگر این است که این جرایم از حیث تعقیب و جلوگیری با مشکل مواجهند، زیرا تدابیر معمولی حقوق جزا پاسخگو نیست. کلاهبرداری و برخی جرایم مربوط، نیازمند فریب انسان زنده اند (به استثنای کانادا، فرانسه، هلند و اسکاتلند) جرایمی همچون سرقت، اختلاس، کلاهبرداری در مقررات سرقت و اختلاس بسیاری از کشورها، وجود

یک هدف و شیء فیزیکی لازم است. در اختلاس و برخی جرایم برخلاف اراده و میل، مالک بودن شرط است. کمیته به واسطه این ملاحظات، پیشنهاد کرد متن ماه بدین گونه تنظیم شود: وارد کردن، تغییر، محو یا موقوف سازی داده های کامپیوتری یا برنامه های کامپیوتری، یا دیگر مداخلات در پردازش داده ها که بر نتیجه پردازش ها اثر گذارد و موجب

ضررهای اقتصادی یا

تعرض در اموال شخصی دیگر به قصد تحصیل منفعت اقتصادی غیرقانونی برای خود یا دیگری شود (راه حل جایگزین: با قصد محروم کردن غیرقانونی آن شخص از اموالش).

شرح ماده: هدف اصلی

ماده جرم، شناختن هرگونه سوء استفاده در زمینه پردازش داده ها به خاطر تأثیرگذاری بر نتایج و انتقال غیرقانونی اموال و ایجاد خسارت است. داده ها و برنامه های کامپیوتری هدف این جرم قرار می گیرند. در متن ماده، داده ها و برنامه های کامپیوتری منحصرأ ذکر شده است که هدف این است ابتدا سوء استفاده از داده ها طرح شود و بعد به طور فرعی جرم کلاهبرداری مطرح شود. در متن ماده، نحوه عمل مرتکب بیان شده است. وارد کردن، تغییر، محو و متوقف سازی، عناصر تشکیل دهنده جرمند. همچنین مداخله در پردازش داده ها ذکر شده است که دامنه ماده را از ذکر مصادیق حصری به مصادیق تمثیلی رهنمون می شود. منظور از ورود، وارد کردن داده ها به کامپیوتر است. این کار موجب تأثیر بر داده پردازش می شود. این ورود می تواند مشتمل بر داده های صحیح یا داده های کذب باشد. در نهایت، نتیجه عمل مهم است. متن ماده، سوء استفاده به هر شکل را شامل می شود، از این رو از چک ها و کارت های اعتباری مسروقه در یک بانک خودکار تا کارت شخصی و تجاوز از حدود اعتبار کارت را شامل می شود. در کنار «ورود» دیگر اشکال یعنی تغییر، محو کردن و متوقف سازی داده ها یا برنامه ها ذکر شده است تا بتواند عام الشمول باشد. تغییر شامل اصلاح، تغییر جزئی یا کلی است. محو شامل حرکت و انتقال داده ها از محل اصلی مثلاً از نوار است. متوقف سازی شامل: نگه داشتن و اختفای داده ها است باید این اعمال منجر به کسب منفعت یا مالی اقتصادی و یا تصرف اموال دیگری شود و نیز قصد مرتکب باید کسب چنین منفعت یا مالی باشد.

۲- جعل کامپیوتری

پدیده شناسی و وضعیت قانونی

گاه سوء استفاده به این دلیل انجام می شود که بتوان دلیلی گمراه کننده برای انجام اعمال حقوقی و قضایی کسب کرد. از سویی با ورود یا تغییر غیرمجاز داده های کامپیوتری، می توان ادله موجود و مثبت یک

عمل حقوقی یا پدیده کیفی را از بین برد. در برخی کشورها، اگر چه این نوع سوء استفاده نوعی تقلب است، اما آن را در داخل مفهوم جعل بررسی می کنند. نکته مهم این است که داده ها به واسطه ابزارهای تکنیکی قابل خواندن و استفاده اند، از این رو «سند» محسوب می شوند. اما در بیشتر کشورها هنوز شرط کتبی و قابل رؤیت بودن سند، جزو لازم مفهوم سند است. اگر داده های ذخیره شده به طور الکترونیکی را واجد را واجد ارزش اثباتی و مفهوم سند ندانیم، حقوق جزا را با خلایی روبرو ساخته ایم. اسناد الکترونیک گاهی واجد امضاهای الکترونیکی است که این نیز خود بر دامنه مباحثات می افزاید. متن پیشنهادی کمیته از این قرار است:

«وارد کردن، تغییر، محو یا موقوف سازی داده های کامپیوتری یا برنامه های کامپیوتری یا دیگر مداخلات در زمینه داده پردازش، از طریق یا تحت شرایطی برابر آنچه در قوانین ملی تشریح شده و تشکیل دهنده جرم جعل است، اگر به خاطر هدف های مرسوم چنین جرمی ارتکاب یافته باشد».

تفسیر متن ماده:

هدف ماده ممنوع شمردن جعل داده ها و برنامه هاست و به طور کلی همان هدف جرم جعل که ایجاد عدم اعتماد نسبت به اسناد است، در اینجا نیز هست. فرض ماده این است که بر داده ها بتوان



عنوان سند اطلاق کرد. نحوه فعل مرتکب، به یکی از صور یاد شده در ماده صورت می پذیرد. همان گونه که در جرم جعل در حالت کلاسیک، مصادیقی که ذکر می کنند، بیان گر نحوه عمل مرتکب است. در مورد سند، عناصر تشکیل دهنده سند و سازنده سند، مباحثاتی بین سیستم های حقوقی کشورها مطرح است.

۳- تخریب داده ها یا برنامه های کامپیوتری پدیده شناسی و وضعیت قانونی

داده ها و برنامه های کامپیوتری واجد ارزش اقتصادی است و شرکت ها و مقامات اداری تا حد زیادی به داده پردازی وابسته اند و نیز با توجه به حجم داده های ذخیره شده در ابزارهای الکترونیک، هرگونه تخریب و خسارت زدن به داده ها موجب خطر بسیار و تبعات منفی بعدی است. تخریب و خسارت زدن

به داده ها گاه بدینصورت ارتکاب می یابد که با برب یا مواد مخرب دیگر به خود تأسیسات کامپیوتری تعرض می شود. در اینجا، عمل تحت پوشش قوانین عادی آنگاه که تخریب و ایجاد خسارت از طریق کامپیوتر مثلاً ویروس ها یا بمب های منطقی زمانی انجام

می شود، باید جرم تخریب و ایجاد خسارت را در عداد جرایم کامپیوتری وضع و بررسی کنیم وگرنه این اعمال بدون مجازات خواهند ماند. هدف مرتکب در این جرم صرفاً صدمه وارد کردن است. کسب منفعت غیرقانونی شرط نیست. بیشتر این افراد برای اعتراض به قطع رابطه استخدامیشان به چنین اعمال دست زده اند. متن پیشنهادی کمیته بدین قرار است: «محو، خسارت زدن، کم ارزش کردن یا موقوف سازی داده ها یا برنامه های کامپیوتری بدون داشتن حق» آنچه در این جرم مورد حمایت قرار گرفته است، تمامیت و نحوه عملکرد یا استفاده از برنامه ها و داده های کامپیوتری است.

تغییر متن پیشنهادی

هدف ماده برقراری حمایت از داده ها و برنامه های کامپیوتری است. همانطور که در قوانین مرسوم کیفری، اشیاء گاهی مورد حمایت (در برابر خسارت) قرار می گیرند، البته اگر برخی همچون کشور آلمان هر چیز با ارزش را مال بدانند، با مختصر اصلاحی در قوانین مرسوم خود، می توانند پوشش حمایتی کافی را ایجاد کنند. ماده نحوه عمل مرتکب و مشخص کرده است. محو داده ها همانند تخریب اشیای فیزیکی است و موجب تخریب و نابودی و غیرقابل شناخت شدن داده ها می شود. عبارت ماده کلی است و چه خود داده ها و چه حامل داده ها، خسارت ببینند و یا تخریب شوند، تحت شمول ماده قرار می گیرند. عنصر مادی جرم به

صورت محو کردن، خسارت زدن، کم ارزش کردن و متوقف سازی مقصود شده است. هر یک از این اجزا تعریف و توضیح خاص خود را داراست. در پایان ماده، با ذکر عنوان بدون داشتن حق شرط، استحقاق کیفر بیان شده است و در صورتی که چنین حقی موجود باشد، عمل جرم نیست و به طبع مورد مجازات قرار نمی گیرد. شرط، نداشتن حق، مانند همسان شرط تعلق به دیگری در جزائیات مرسوم است. برخی کشورها داده ها را قابل تعلق به کسی نمی دانند، از این رو، در متن ماده، این گونه شرط شده است تا بحث های سیستماتیک نظام ها موجب بروز اختلاف نشود.

۴- سابتاژ کامپیوتری

پدیده شناسی و وضعیت قانونی

ایجاد اختلال و تخریب در سیستم های کامپیوتری و ارتباطی گاه از صرف تغییر داده ها یا برنامه فراتر می رود و اثر بیتری می کند. چون روز به روز جامعه به این سیستم ها بیشتر وابسته می شود. از این رو حمایت مخصوصاً از کامپیوترهای نظامی، پزشکی یا کنترل ترافیک و بانک ها واجد اهمیت بیشتری است. خطرهای ناشی از سابتاژ کامپیوتری بسیار زیاد است، از این رو چند کشور اروپایی مقرراتی در این زمینه وضع کرده اند. کمیته، اعمال زیر را مجرمانه تلقی کرده است:

«وارد کردن، تغییر، محو یا موقوف سازی داده ها یا برنامه های کامپیوتری یا مداخله در سیستم های کامپیوتری با قصد اختلال و جلوگیری از عملکرد کامپیوتر یا سیستم ارتباطات».

تفسیر متن ماده: در متن ماده جزو بسیار مهم، سابتاژ کامپیوتری، یعنی قصد اختلال و جلوگیری از عمل کرد سیستم ارتباطی یا کامپیوتری است. در جرم سابتاژ، هدف ارتکاب و طریق ارتکاب مشخصه جرم است. طریق ارتکاب، هر نوع مداخله در سیستم کامپیوتری است. برخی طرق ذکر شده در متن ماده، کلی اما وافی به مقصود است. موضوعات مورد حمایت در این جرم موجب تمایز آن با دیگر جرایم است. جرم، ناظر به گونه های مختلف فعل است. از اینرو اگر چه ممکن است ترک فعل موجب همین آثار شود، اما نباید جرم تلقی شود، متن ماده در خصوص ذکر کلمه سیستم های کامپیوتری کلی است تا محصور و محدود به برخی مصادیق نشود.

۵- دستیابی غیرمجاز

پدیده شناسی و وضعیت قضایی

داده های کامپیوتری به دلیل افزایش ارزش اقتصادی، اداری، حکومتی و... مورد توجه مجرمان قرار گرفته است. Hackers یا نفوذ

یابندگان (خدشه زندگان به سیستم) به طور غیرمجاز به سیستم ها دست یابی، مخاطرات و صدماتی را به دنبال خواهد داشت. از این رو دخالت قانون امری ناگزیر است. این دستیابی غیرمجاز است و مرتکب درصدد ورود به سیستم کامپیوتری است. انگیزه مرتکب در انجام این دستیابی متفاوت است. متن پیشنهادی کمیته از این قرار است:

«دستیابی بدون حق به سیستم یا شبکه کامپیوتری» به وسیله تجاوز به تدابیر و ابزارهای امنیتی، آنچه در این جرم مورد حمایت قرار می گیرد همانا امنیت کامپیوتر و مصون ماندن از دستیابی است.

تفسیر متن ماده: هدف از این جرم، جلوگیری از نفوذ به شبکه هایی سیستم های کامپیوتری است. صرف دستیابی کافی است. وصف این دستیابی غیرمجاز بودن است. ماده، محدود به سیستم کامپیوتری خاصی نشده است. موضوع جرم، شبکه ها یا سیستم های کامپیوتری است. دستیابی زمانی غیرمجاز است که نفوذکننده محق در دستیابی نباشد.

۶- شنود غیرمجاز

پدیده شناسی و وضعیت قضایی

درواقع این نوع فعل مجرمانه شکل جدیدی از جاسوسی است. در این جرم، شنود و استراق سمع داده ها و ارتباطات، در حین انتقال آن ارتکاب می یابد (البته به کارگیری و شنود از باب مسامحه است وگرنه لازمه استراق سمع شنود مکالمات و... است). تاکنون شنود مکالمات مطرح بود حالا ممکن است این کار بر روی سیستم های ارتباطی و کامپیوتری صورت پذیرد. برخی سعی کرده اند این اعمال را در زمره رایبش اطلاعات جای دهند، اما رایبش بر روی اموال عینی و مادی قابل تصور است. متن ماده پیشنهادی کمیته از این قرار است:

«شنود انجام شده بدون حق و به وسیله ابزارهای تکنیکی بر روی ارتباطات، از طریق یا در حدود یک سیستم یا شبکه کامپیوتری».

شرح ماده: متن ماده، حمایت از سیستم های شبکه های کامپیوتری را مدنظر قرار داده است. هدف جرم ارتباطات و انتقال داده ها است. نحوه انتقال مهم نیست، چه در یک سیستم کامپیوتری باشد، چه بین دو سیستم کامپیوتری و... شرط است عمل بدون داشتن حق انجام شود. نوع جرم نیز از جرایم عمدی است.

۷- تکثیر غیرمجاز برنامه کامپیوتری حمایت شده پدیده شناسی و وضعیت قانونی

برنامه های کامپیوتری از جهات مختلف اهمیت دارند، زیرا سخت افزار هر چند پیشرفته باشد، بدون نرم افزار کارایی ندارد. برای ایجاد یک برنامه کامپیوتری هزینه زیادی صرف می شود. وقتی این برنامه ها مطمح نظر مجرمان قرار گیرند، هزینه ها افزوده خواهد شد.

در سال های اخیر سرقت نرم افزار افزایش یافته

است. حجم تخلفات به گونه ای است که تضمین های حقوقی مدنی و اداری کافی نیست و حمایت جزایی را می طلبد. متن ماده از این قرار است: «تکثیر، توزیع یا ارتباط با عامه و بدون حق از یک برنامه کامپیوتری که به وسیله قانون حمایت شده است.»

تفسیر متن ماده: حمایت جزایی از برنامه کامپیوتری را هنگامی برقرار می کند که قبلاً به وسیله حقوق مدنی حمایت شده باشد. هدف ماده حمایت از برنامه های کامپیوتری است. برنامه های کامپیوتری را WIPO تعریف کرده است. می توان حمایت ماده را تسری داد و ساختار و پیامدهای برنامه را نیز تحت سیطره قانون قرار داد. نحوه ارتکاب جرم بیان شده است. تعریف این عناصر به عهده مقنن ملی و حقوق دانان است. شرط است انجام این اعمال بدون داشتن حق باشد. جرم نیز از نوع جرایم عمدی است.

۷- تکثیر غیرمجاز برنامه کامپیوتری حمایت شده

پدیده شناسی و وضعیت قضائی

برنامه های کامپیوتری از جهات مختلف اهمیت دارند، زیرا ساخت افزار هر چند پیشرفته باشد، بدون سرمایه کاری نداشت. برای ایجاد یک برنامه کامپیوتری هزینه زیادی صرف می شود. وقتی این برنامه ها مطمع نظر مجرمان قرار گیرند، هزینه ها افزوده خواهد شد.

در سال های اخیر سرعت نرم افزار افزایش یافته است. حجم تخلفات به گونه ای است که تضمین های حقوقی مدنی و اداری کافی نیست و حمایت جزایی را می طلبد. متن ماده از این قرار است: «تکثیر، توزیع یا ارتباط با عامه و بدون حق از یک برنامه کامپیوتری که به وسیله قانون حمایت شده است.»

تفسیر متن ماده: حمایت جزایی از برنامه کامپیوتری را هنگامی برقرار می کند که قبلاً به وسیله حقوق مدنی حمایت شده باشد. هدف ماده حمایت از برنامه های کامپیوتری است. برنامه های کامپیوتری را WIPO تعریف کرده است.

می توان حمایت ماده را تسری داد و ساختار و پیامدهای برنامه را نیز تحت سیطره قانون قرار داد. نحوه ارتکاب جرم بیان شده است. تعریف این عناصر به عهده مقنن ملی و حقوق دانان است. شرط است انجام این اعمال بدون داشتن حق باشد. جرم نیز از نوع جرایم عمدی است.

۸- تکثیر یک توپوگرافی

پدیده شناسی و وضعیت قضائی

فناوری نیمه هادی ها در پیشرفت صنایع نقش بسزایی دارد. خود این محصولات وابسته به ابزارهای دیگری هستند. این فناوری بر منابع اقتصادی انسانی، مالی و تکنیکی اثر قابل توجهی دارد. مبارزه با اعمال خلاف قانون و علیه این نوع فناوری، جز با قانون میسر نیست. در سطح بین المللی این طرز تفکر قوت یافته است که باید حمایتی خاص از توپوگرافی انجام شود.

متن ماده از این قرار است:

«تکثیر بدون حق یک توپوگرافی از محصولات نیمه هادی یا اختراع تجاری یا خارج کردن برای این منظور، بدون داشتن حق، تا آن توپوگرافی یا محصول نیمه هادی مورد استفاده قرار گیرد.»

تفسیر متن ماده: هدف ماده حمایت از خالق توپوگرافی است. موضوع جرم توپوگرافی محصولات نیمه هادی است. توپوگرافی به وسیله WIPO تعریف شده است. حمایت از توپوگرافی در برابر هر نوع کپی کردن، فروش، اجاره غیرمجاز و هر شکل دیگر توزیع انجام می شود. شرط است این اعمال بدون حق انجام شود. این جرم نیز از جرایم عمدی است.

آنچه تاکنون دیدیم مربوط به فهرست حداقل (اجباری) بود حال به مفاد فهرست اختیاری می پردازیم.

۱- تغییر داده های کامپیوتری یا برنامه های کامپیوتری

پدیده شناسی و وضعیت قضائی

گاه محو کردن، ایجاد خسارت یا متوقف سازی، در مورد عمل صدق نمی کند، بلکه عمل، تغییر داده ها یا برنامه ها است. اما این عمل به نحوی مورد بحث و نظر است که نمی توان زیر عنوان مجرمانه دیگر گنجانند. در آلمان این وضع رخ داده بود. آنچه تحت پوشش قانون بود همانا محو غیرقانونی

داده های شخصی بود، اما نسبت به تغییر غیرقانونی داده های شخصی، قانون ساکت بود. گاه شخص محق برای داده ها هیچ خسارتی نمی بیند یا داده ها در اثر تغییر دادن با کاهش ارزش مواجه نمی شود، اما عمل فی حد ذاته چون نوعی تعدی به کامپیوتر است، باید مجرمانه تلقی شود. متن ماده پیشنهادی برای این عنوان مجرمانه عبارت است از: «تغییر داده های کامپیوتری یا برنامه های کامپیوتری بدون داشتن حق.»

تفسیر ماده: نوعی گرایش بین المللی برای مبارزه با تغییر داده یا برنامه های کامپیوتری وجود دارد و ماده اساساً همین را دنبال کرده است. نحوه عمل مرتکب باید در داخل عنوان تغییر بگنجد. تغییر باید غیرقانونی یعنی بدون حق انجام شود. تغییر در کیفیت اطلاعات برنامه ها یا داده ها روی می دهد.

۲- جاسوسی کامپیوتری

پدیده شناسی و وضعیت قضائی

چون از کامپیوتر در همه شئون زندگی استفاده می شود، اسرار ارزشمندی در آن نگهداری می شود. این اسرار اعم از تجاری، اقتصادی و اجتماعی است. ارزش بسیار زیاد این اسرار موجب شده است که مجرمان با به کارگیری تکنیک های جدید، سعی در دستیابی بر این اسرار داشته باشند.

امروزه جاسوسی صنعتی و تجاوز به اسرار تجاری، شکل جاسوسی کامپیوتری را به خود گرفته است. هدف جاسوسی کامپیوتری می تواند سخت افزار، نرم افزار یا داده های کامپیوتری باشد. چون مرز جاسوسی و سرقت نرم افزار... نیز باید مورد توجه قرار گیرد، توجه به نحوه عمل و هدف مرتکب لازم است. متن ماده پیشنهادی برای جاسوسی کامپیوتری از این قرار است:

«تفتیش هررسی به وسیله ابزارهای لازم یا افشای انتقال یا استفاده از اسرار تجاری یا بازرگانی، بدون داشتن حق یا بدون هیچ توجیه قانونی دیگر، خواه با قصد ایجاد ضرر اقتصادی برای شخص محقق اسرار و خواه با قصد کسب امتیاز اقتصادی غیرقانونی برای خود یا دیگری.»

تفسیر متن ماده: هدف این جرم، حمایت از اسرار تجاری یا بازرگانی است. اسرار، طبع خاصی دارند، از این رو در متن ماده به کار رفته اند. هدف مرتکب، طریق تحصیل و نحوه عمل مرتکب، در متن ماده مشخص شده است. به خاطر افتادن ارزش اقتصادی این اسرار شرط است. در متن، افشا در کنار انتقال و استفاده ذکر شده است تا این سه واژه بتوانند هر یک از عمل مجرم را پوشانند. بدون داشتن حق، عمل کردن مجرم شرط است. ممکن است در اسرار، تلقی شدن و محقق تلقی شدن مرتکب مسایلی را پیش آورد که مباحثات بعدی را بطلبد، قصد مرتکب در ماده ذکر شده و از عناصر اصلی جرم است.

۳- استفاده غیرمجاز از کامپیوتر

پدیده شناسی و وضعیت قضائی

گاه از سیستم داده پرداز استفاده غیرمجاز

می شود که به آن سرقت خدمات می گویند (در حالت عادی نیز دیده ایم که اتومبیل یا سایر امکانات دولتی و خصوصی که برای مصارف معین مشخص شده اند، ممکن است جهت استفاده خصوصی و شخصی به کار روند). چون در اینجا استفاده گر خلاف هدف پیش بینی شده برای آن وسیله یا نهاد عمل می کند، بنابراین متخلف محسوب می شود. مستخدمان شرکت ها، کادر اداری، استادان دانشگاه ها، دانشجویان و... مجرمان اصلی این جرمند هدف از این ارتکاب این جرم استفاده از خدمات پردازشی کامپیوتر، ذخیره سازی یا انتقال داده هاست. به طور معمول این گونه رفتار مجرمانه صدمه ای در بر ندارد، اما از آنجا که این گونه استفاده، غیرقانونی است، ممکن است گاه صدمات اقتصادی جدی به دنبال داشته باشد. در متن ماده چنین آمده است: «استفاده از سیستم یا شبکه کامپیوتری، بدون حق، که یا ۱- موجب خطر

امروزه جاسوسی صنعتی و تجاوز به اسرار تجاری شکل جاسوسی کامپیوتری را به خود گرفته است هدف جاسوسی کامپیوتری می تواند سخت افزار، نرم افزار یا داده های کامپیوتری باشد

و صدمه به شخص محق در استفاده از سیستم شود، یا صدمه به سیستم وارد آید یا عملکرد آن مختل شود یا ۲- موجب ضرر به شخص محق در استفاده از سیستم یا صدمه به سیستم یا عملکرد آن شود.

تفسیر متن ماده: در متن ماده دو نوع منافع مورد حمایت قرار گرفته است: حمایت از منافع اقتصادی فرد و حمایت از امنیت و عملکرد سیستم. برای جامعیت در متن ماده، سه آلتزایو ذکر شده است تا بتواند بسته به سیستم کشورها و نیز بسته به مورد، مورد تقنین قرار گیرند، شرط است، عمل بدون داشتن حق انجام شود. صرف استفاده غیرقانونی در متن ماده با افزودن قید و بندهای بعدی تحدید شده است.

۴- استفاده غیرمجاز از برنامه های کامپیوتری حمایت شده

پدیده شناسی و وضعیت قانونی - استفاده از برنامه های کامپیوتری حمایت شده در جایی که مؤلف آن رضایت ندارد، همانند جرم اختفا و نگهداری اموال مسروقه است. استفاده غیرمجاز از برنامه های کامپیوتری یادآور تخلفات علیه

کپی رایت کامپیوتری است. متن ماده پیشنهادی از این قرار است: «استفاده بدون حق از برنامه کامپیوتری که به وسیله قانون حمایت شده و بدون حق تکثیر شده است خواه با قصد تحصیل منفعت اقتصادی غیرقانونی برای خود یا دیگری، خواه با قصد ایجاد صدمه برای مالک (دارنده) حق».

تفسیر متن ماده: در این جرم، هدف، حمایت از عدم تکثیر غیرمجاز برنامه کامپیوتری است. برنامه هایی که تحت پوشش کپی رایت قرار می گیرند، در این ماده می گنجد. جرم از جمله جرایم عمدی است و ذکر بدون داشتن حق، مفسر متن ماده است.

۴- پیشنهاد سازمان ملل

سازمان ملل در نشریه بین المللی سیاست جنایی شماره های ۴۳-۴۴ خود، در عین حال که تقسیم بندی های موجود را مورد اشاره قرار داده است، در مقام توضیح و شرح پدیده جرم کامپیوتری، برخی از اعمال مجرمانه را احصا کرده است. البته بحث بر سر این است که آیا می توان نام تقسیم بندی در مفهوم دقیق خود بدان داد یا خیر.

به هر حال چون در ابتدا قابل به وجود انواع مشترک و عمومی جرایم کامپیوتری شده است و آنگاه در مقام احصای مشکلات ایجاد شده برای حقوق خصوصی و فردی، برخی دیگر از اعمال مجرمانه را مطرح می کند، می توان این کار را نوعی تقسیم بندی محسوب کرد.

البته این نهاد و ارگان بین المللی تأکید بر تقسیم بندی های شورای اروپا و OECD دارد و در درجه

اول آنها را مهم می شمرد. فهرست انواع مشترک و عام جرم کامپیوتری از دید سازمان ملل چنین است: الف- کلاهبرداری کامپیوتری- کلاهبرداری کامپیوتری با سوءاستفاده از ورودی کامپیوتر، دست یازیدن به آنچه حقه بازی اطلاعاتی می توان نام نهاد، سوءاستفاده از برنامه سوءاستفاده از خروجی و...

ب- جعل کامپیوتری: تغییر شکل داده های مربوط به اسناد ذخیره شده در کامپیوتر و...

ج- تخریب داده ها یا برنامه های کامپیوتری- دستیابی مستقیم یا مخفیانه غیرمجاز به سیستم های کامپیوتری با استفاده از برنامه های جدید به نام ویروس، کرم یا بمب منطقی، اصلاح، موقوف سازی، پاک کردن غیرمجاز داده ها یا عملیات کامپیوتر و...

د- دستیابی غیرمجاز به سیستم ها و خدمات کامپیوتری: دستیابی غیرموجه فرد به سیستم های کامپیوتری، دستیابی از طریق یافتن راه های گریز سیستم امنیتی، معرفی خود به جای کاربر مجاز سیستم، کشف رمز و دستیابی به سیستم و...

ه- تکثیر غیرمجاز برنامه های کامپیوتری قانوناً حمایت شده - تکثیر برنامه هایی که تحت حمایت کپی رایت قرار دارند و...

پیشنهاد AIDP

انجمن بین المللی حقوق جزا در طول سالهای ۱۹۹۲ و ۱۹۹۴، در نشست های خود در ورتسبورگ آلمان و ریودوژانیرو، در عین حال که برکار شورای اروپا صحنه گذاشته و تقسیم بندی آنها را پذیرفته است، به دلیل پیشرفت های حاصل و نیز به دلیل افزایش حساسیت در برخی زمینه ها خواستار توجه به برخی زمینه های خاص شده است. از این رو، جرایم را می توان نوعاً جرایمی مستقل و در ادامه فهرست های حداقل و اختیاری شورای اروپا ذکر کرد. از نظر AIDP، این اعمال باید به طور مستقل ذکر شوند:

الف- قاچاق کلمات رمز

ب- انتشار ویروس یا برنامه های مشابه

ج- دستیابی به اسرار برخلاف قانون

د- به کارگیری، انتقال و دگرگونی غیرقانونی داده های شخصی.

ذکر این نکته لازم است که برخی صاحب نظران از جرایم کامپیوتری، تقسیم بندی هایی ارائه کرده اند که اگرچه بین المللی نیست، اما حایز نکات مهمی است. از جمله می توان به کار ارزشمند پروفیسور اولریش زیبر اشاره کرد. این حقوقدان برجسته در سری شش مجلدی کتبی که تحت عنوان Ius

Informations به چاپ رسیده است و مجلد اول آن مربوط به حقوق کیفری اطلاعاتی است، در بخش مربوط به حقوق جزای ماهوی، به جرایم کامپیوتری اشاره کرده است. در این بخش موفق نشدم بحث سیاست جنایی تقنینی جرایم سایبری را به سرانجامی برسانم زیرا در این بخش گفتنی زیاد است اما در مقاله بعدی این بحث ادامه خواهد یافت در شماره آینده بحث تقسیم بندیها و قوانین در فضای کنونی یعنی نسل سوم جرایم ذکر خواهد شد سپس به قوانین و مقررات سایبری ایران خواهم پرداخت. ادامه دارد

پانویس ها:

۱- جرایم سایبری یا به تعبیر دهه های ۶۰ و ۷۰، جرایم کامپیوتری، بدو به صورت توصیه نامه و رهنمود ارائه شد و این توصیه نامه ها و رهنمودها هم از حیث تاریخ جرایم سایبری یا به تعبیر برخی اهل فن، سیر تحول جرایم سایبری اهمیت زیادی دارد و هم از حیث ادبیات تقنینی. از این رو اگر چه توصیه نامه OECD و رهنمود شورای اروپا عنوان قانونی ندارد اما باید به عنوان مبنای قانونگذاری سایر کشورها مدنظر قرار گیرد.

۲- در سال ۱۹۸۳ OECD، مطالعه امکان پذیری اعمال بین المللی و هماهنگی قوانین کیفری را به منظور حل مسأله جرم یا سوءاستفاده های کامپیوتری متعهد شد.

این سازمان در ۱۹۸۶ گزارشی تحت عنوان «حرم کامپیوتری، تحلیل سیاستگاه قانونی» منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوءاستفاده هایی را پیشنهاد کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند. از جمله آنها کلاهبرداری و جعل کامپیوتری، حق تکثیر و شنود ارتباطات یا دیگر عملیات کامپیوتری و یا سیستم های ارتباط راه دور است.

اکثریت اعضای کمیته سیاست گذاری اطلاعات، کامپیوتر و ارتباطات نیز پیشنهاد کرده اند که حمایت های کیفری برای دیگر انواع سوءاستفاده، از جمله سرقت اسرار تجاری و دست یابی یا استفاده غیرمجاز از سیستم های کامپیوتری نیز باید مستمری یابد. بدین گونه اولین تقسیم بندی و اولین متن جرایم کامپیوتری در سال ۱۹۸۳ ارائه شد و طی آن پنج دسته اعمال را مجرمانه تلقی و پیشنهاد کرد که در قوانین ماهوی ذکر شوند. در این پرسش نامه ها، خطوط اصلی سیاست قضایی در واکنش نسبت به جرم کامپیوتری، بررسی قابلیت اجرا یا عدم قابلیت اجرای حقوق کیفری موجود و یکسری اطلاعات دیگر ذکر شده بود و در پایان نیز فهرستی را به عنوان خطوط وحد مشترک متشکل بین هیأت های مختلف ارائه کردند. نکته مهم در این فهرست، ره یافت فنی صرف تدوین کنندگان آن است.