جرایم اینترنتی - مشکلات و راهکارها بر پایهٔ قوانین مالزی

نویسنده: پروفسور دکتر نازورا عبدالمناپ
مترجم: وکیل حسین تاجی

چکیده :
کشور مالزی از اواسط دههٔ ۱۹۹۰ با مشکل روند فزاینده تکنولوژی اطلاعات روبرو بوده است؛ و دلیل این مشکل پیشرفت سریع تکنولوژی اینترنت در سر تا سر دنیاست. سیستم‌های کامپیوتری فرصت‌های جدید و هوشمندانه ای را برای قانون شکنی ارائه داده و امکان ارتکاب جرایم سنتی و قدیمی را به روش‌های مدرن میسر می‌کنند. یکی از واضح‌ترین مشکلاتی که به واسطهٔ استفاده از این تکنولوژی ایجاد می‌شود نوع جدیدی از جرایم است که به آن اصطلاحاً «جرایم اینترنتی» می‌گویند. جرایم سنتی در اصل نیازمند آن هستند که توسط عوامل فیزیکی باعث شوند. برعکسِ جرایم اینترنتی که مرکب و پیچیده هستند و در مورد آن‌ها اثبات عمل خلاف دشوار تر می‌شود. جرایم اینترنتی ماهیت بین‌المللی دارند و مقابله موثر در برابر این جرایم همکاری جدی بین‌المللی را می‌طلبد؛ و این مطلب تنها در صورتی امکان پذیر است که چهار چوبی یکسان برای درک این که مشکل چیست و راهکارهای

مقدمه :

در سال‌های اخیر تکنولوژی پیشرفته، به خصوص کامپیوترها با روند رو به گسترش مرکز توجه اذهان عمومی در کتاب‌ها، تلویزیون، فیلم و سایت‌های اینترنتی شده‌اند. رسانه‌ها در مورد هکرها به روش‌های گوناگون اطلاع رسانی می‌کنند. در مالزی، ما هنوز شاهد ظهور هکرهایی چون kevin mitnick و David smith هستیم که توانسته است در سیستم‌های کامپیوتری سر تا سر جهان اختلال ایجاد کنند.

(امروزه ما در جامعه ای بسیار بزرگ زندگی می‌کنیم که این همسایگی توسط شبکهٔ کاربران کامپیوتری سر تا سر جهان به واسطه وجود اینترنت حاصل آمده است). جامعه مالایی تنها محدود به شهروندان و ساکنان مالزی نیست بلکه به شکل غیر مستقیم شامل مردم کشورهای دیگر نیز می‌شود و این عامل می‌تواند عامل مشوق در ظهور جرایم اینترنتی باشد. دزدی، کلاهبرداری، خشونت، مسائل جنسی و تخریب اموال همگی جزو جرایم شناخته شده هستند. با استفاده از اینترنت تمامی این جرایم به شکلی دیگر امکان پذیر می‌شوند. دلیل اصلی اینکه چرا جرایم اینترنتی به نظر حائز اهمیت هستند این است که تنها از طریق وجود رکوردهای مالی هنگفت در کامپیوترهای انتقال مبالغ زیاد میسر می‌شود. با این وجود، این مثال تنها دیدگاه محدود شده ای از آثار جرایم اینترنتی را آشکار می‌کند. این جرایم تنها به پول محدود نشده بلکه فرزندان و زندگی خصوصی افراد را نیز تحت‌الشعاع خود قرار می‌دهد. به عبارت دیگر، این روزها جرایم اینترنتی در ارتباط با مباحث کامپیوتری از جمله، حق مالکیت معنوی و عقلی، سوء استفاده جنسی از بچه‌ها و مباحث خصوصی می‌شوند.

در این مقاله، نویسنده ابتدا توضیحی دارد در باب توضیحات و طبقه

بندی‌های جرایم اینترنتی و سپس قوانین سنتی موجود و راه های مقابله با مشکلات جهانی جرایم اینترنتی مورد بحث قرار می‌گیرد. به منظور اطمینان حاصل کردن از اینکه آیا مشکلات ایجاد شده به دلیل استفاده از قوانین قدیمی قابل حل شدن هستند یا خیر، قانون جرایم کامپیوتری ۱۹۹۷ به دقت بررسی خواهد شد.

نویسنده مقاله را با طرح پیشنهاداتی مبنی بر چگونگی حل این مشکلات، به خصوص اجرای قوانین جرایم کامپیوتری ۱۹۹۷ را برای این جرایم اینترنتی، نتیجه گیری خواهد کرد.

مردم غالباً «جرایم کامپیوتری» را با «جرایم اینترنتی» اشتباه می‌کنند. اختلاف نظرهای زیادی در بین متخصصان در مورد اینکه چه چیزی جرایم کامپیوتری را به جرایم اینترنتی و یا جرایم مربوط به کامپیوتر را تشکیل می‌دهد وجود داشته است. حتی پس از چندین سال هیچ تعریف شناخته شده بین‌المللی‌ای برای این واژه‌ها وجود ندارد. نویسنده‌ها و متخصصینی که در تلاش برای رسیدن به توصیفی از این جرایم ذکر شده بودند توضیحات خود را در ارتباط با تحقیق‌ها و مطالعات به کار برده‌اند. در نتیجه، استفاده از این توضیحات خارج از متن، خود باعث ایجاد اشتباهاتی می‌شود. بر اساس توضیح گستردهٔ این واژه، جرایم کامپیوتری شامل انواع زیادی از جرایم کیفری، فعالیت‌ها و مسائل محرمانه است. که این شامل استفاده از کامپیوتر به عنوان وسیله نیز می‌شود و شامل ارتباط مستقیم بین مجرم و دستگاه کامپیوتر می‌شود. به عنوان مثال، کارمند ناکار آمد بانک برای رسیدن به سود، بدون داشتن مجوز پول مشتری را به حسابی غیر فعال منتقل می‌کند و یا شخص که توانسته بدون اجازه به کامپیوتر شخص دیگر دسترسی پیدا کند و اطلاعاتی را دانلود کرده که سری بوده‌اند. تمامی این موفقیت‌ها مستلزم دسترسی مستقیم هکر به کامپیوتر قربانی است. هیچ خط اینترنتی و یا حتی استفاده از شبکه اینترنتی و یا حتی استفاده از شبکه اینترنتی محدودی مانند شبکه محلی (LAN) در این موارد وجود نداشته است.

در حالی که جرایم اینترنتی جرایمی هستند که اکثر از طریق خط اینترنت به وقوع می‌پیوندند، این بدان معنا است که این جرم‌ها می‌توانند به سایر کشورها که فراتر از نظام حقوقی مالزی هستند نیز گسترش پیدا کنند. به هر حال، اشاره به جرایم کامپیوتری تحت عنوان جرایم اینترنتی و یا بلعکس هیچ مشکلی را ایجاد نمی‌کند. چرا که این دو یک تأثیر را در این قانون دارند. سئوال مهمی که اینجا مطرح می‌شود این است که قوانین قدیمی تا چه حد در حل مشکلات ناشی از این گونه جرایم نسبی قبل اجرا هستند؟

ممکن آن چه می‌تواند باشد وجود داشته باشد.
از آنجایی که حقوق جزایی در مالزی برای کنترل این مشکل کافی نیست، دولت قانون جدید را به نام قانون جرایم کامپیوتری در سال ۱۹۹۷ تصویب کرده است. تا به امروز، این قانون به این دلیل که اجرا نشده است هنوز آزمایش نشده. در نتیجه، هدف از این مقاله تاکید بر انواع جدید جرم و چگونه هماهنگ کردن این قانون موجود در بین کشورها است.

طبقه بندی جرایم اینترنتی :

انواع جرایم اینترنتی توسط نویسنده‌ها به صورت‌های مختلف طبقه بندی

شده‌اند. این تفاوت در بین طبقه بندی انجام شده توسط بازرسی تا طبقه بندی دانشگاهی دیده می‌شود. با در نظر گرفتن همه این موارد جرایم اینترنتی به طور عمومی تقسیم می‌شود به:

۱- جرایم اینترنتی علیه اموال و مالکیت
۲- جرایم اینترنتی علیه اشخاص
۳- تروریسم اینترنتی

۱- جرایم مربوط به دارایی‌ها :

این مجموعه شامل جرایم اینترنتی است که در مورد تمامی شکل‌های مالکیت صحت دارد. معمول‌ترین مثال‌های مربوط به این نوع طبقه بندی در زیر توضیح داده شده است.

سرقت : دزدی در جرایم اینترنتی شامل دزدی اطلاعات، دزدی پول یا دارایی و دزدی خدمات است. این نوع دزدی با دزدی که در دنیای حقیقی رخ می‌دهد متفاوت است.

سرقت اطلاعات : اطلاعات موجود در اینترنت گاه بسیار مهم است و می‌تواند دزدیده شود. رکوردهای پزشکی، لیست مشتریان و ایمیل‌های شخصی همه می‌توانند دزدیده شوند و به اشخاصی که علاقه‌مند به این اطلاعات هستند فروخته شود. دزدی شماره کارت، دزدی از دستگاه خود پرداز، دسترسی به رمز و سرقت اطلاعات برخی از نمونه های این نوع جرم می‌باشند.

دزدی دارایی : این نوع دزدی اینترنتی شامل استفاده ناصحیح از اطلاعات ذخیره شده الکتریکی است که نشان دهندهٔ بودجه مالی است.

سرقت خدمات : شامل خدمات و سرویس‌هایی است که شخصی از طریق حقه های دغل کارانه بدست می‌آورد. به عنوان مثال به منظور دسترسی به یک سایت پرداخت، شخص بدون مجوز از رمز ثبت شده شخصی دیگر استفاده می‌کند تا از پرداخت پول اجتناب کند.

فریب /کلاهبرداری : در این نوع دسته بندی جرایم اینترنتی، مجرم برای ترغیب قربانی به تحویل راغبانهٔ اموالش از جملات دروغ استفاده می‌کند. این نوع جرم غالباً از طریق هرم‌ها و تجارت‌های طبقه ای، مجوزهای نمایندگی‌ها و فرصت‌های تجاری، مزایده‌ها، فروش کالاهای عمومی، پیشنهاد دریافت کارت اعتباری، پیشنهاد کار و وام‌های مالی آماده صورت می‌گیرد. اینترنت بهترین مکان برای مجرمان است تا بتوانند از طریق ایمیل و سایت‌های اینترنتی اظهارات دروغ خود را به قربانی خود منتقل کنند.

جعل : شامل تغییر سند به قصد سوء استفاده از سند تغییر یافته و به قصد گمراه کردن شخصی دیگر است. این نوع جرم اینترنتی زمانی انجام می‌شود که شخصی با استفاده از کامپیوتر، سندی را تغییر داده و یا اطلاعات غلطی را ضمیمه سندهای موجود در اینترنت کند.

ایجاد مزاحمت و دردسر : این نوع خلاف عمدتاً توسط ویروس‌های کامپیوتری صورت می‌گیرند. ویروسی شامل برنامه ای است که به

کامپیوتر آسیب می‌رساند. ویروسی قابل ازدیاد و گسترش است.
کامپیوتر از دو طریق ویروسی می‌شود : یکی از طریق دانلود و باز کردن برنامه‌ها و دستورات و دوم از طریق باز کردن فایلی که ضمیمه یک ایمیل است. نوعی دیگر از ایجاد مزاحمت اینترنتی تخریب اینترنتی است. در دنیای واقعی، مخرب ویژگی شخصیتی کسی است که به هیچ دلیل منطقی به اموال خصوصی و عمومی آسیب رسانده و آن‌ها را تخریب می‌کند. این نوع رفتار در جهان اینترنت به نام تخریب اینترنتی نامیده می‌شود. به عنوان مثال، شخصی که امکان ورود به سیستم کامپیوتری را دارد که دسترسی به آن به منظور از بین بردن اطلاعات آن آسان است.

۲- جرایم اینترنتی بر علیه اشخاص :

جهان اینترنت فضای به مراتب بزرگتری را نسبت به تلفن و سایبر تکنولوژی‌ها برای وقوع ناهنجاری‌های رفتاری ارائه می‌دهد. جرایم اینترنتی می‌تواند بر ضد شخصی انجام شود. حتی اگر این جرم صدمه فیزیکی را به دنبال نداشته باشد، خود نوعی آسیب به قربانی محسوب می‌شود. مثال‌های مربوط به این نوع جرم در زیر بررسی می‌شوند :
مسائل جنسی : این بخش از جرایم شامل قاچاق، پخش، نصب و اشاعه موضوعات ممنوع از جمله مطالب جنسی، پخش اطلاعات بی‌شرمانه و سود استفاده های جنسی از بچه‌ها می‌شود. کامپیوتر و جهان اینترنت تنها روشی دیگر را برای ارتکاب این جرایم در اختیار افراد می‌گذارد.
خشونت اینترنتی : شخصی می‌تواند از طریق اینترنت مورد خشونت قرار گیرد. این خشونت می‌تواند از طریق ایمیل، سایت‌های اینترنتی و برنامه های chat به قربانی منتقل شود.
تهدید اینترنتی : در این نوع از طریق فرستادن پیغام‌های الکترونیکی به قربانی جهانی تخیلی ساخته می‌شود. به عنوان مثال ایمیل‌های تهدید آمیز به رئیس شرکت ms (micro soft)، بیل گیتس فرستاده شد. در مثالی دیگر برای ۲ قاضی فدرال تهدید های مرگ از طرف شخصی کانادایی فرستاده شد.
ورود غیر قانونی به سیستم (هتک مراسلات اینترنتی) : ورود غیر قانونی موضوعی است که کاربران اینترنتی زیادی را می‌ترساند. در مورد خسارت‌هایی که از این طریق ایجاد می‌شود و اینکه چگونه هکرها فایل‌ها را سرقت می‌کنند شایعات زیادی وجود دارد. با این وجود افراد کمی عمق فاجعه را درک می‌کنند؛ و غالباً این افراد در مورد خطر های موجود اغراق می‌کنند. روش‌های متفاوتی برای ورود غیر قانونی اینترنتی وجود دارد که شامل موارد زیر می‌شود :
۱- ایمیل مشکوک : ایمیلی که تجار و دیگر افراد برای فروش کالاهایشان می‌فرستند.
۲- هک کردن صفحه وب : این جرم توسط مزاحمینی انجام می‌شود که به هر طریقی و بدون داشتن مجوز صفحهٔ اینترنتی را مسدود کرده و یا آن را تغییر می‌دهند.

۳- ورود به کامپیوتر شخصی : فرایند حمله به یک کامپیوتر شخصی شبیه مسدود کردن یک صفحهٔ اینترنتی است. تعداد روزنه های اینترنتی امنیتی در سیستم‌های اجرایی (مثل windows و یا LINUX) با زیادتر شدن تعداد مسدود گران کامپیوتر های شخصی روز به روز روبه افزایش است.

۳- تروریسم اینترنتی :

شامل حملهٔ از پیش طراحی شده سیاسی بر ضد اطلاعات، سیستم‌های کامپیوتری، برنامه های کامپیوتری و اطلاعاتی که منجر به اعمال خشونت عوامل غیر قانونی و گروهک‌های ملی به غیر نظامیان است می‌باشد.

تروریست‌های اینترنتی از آسیب پذیری سیستم کامپیوتر برای رسیدن به مقاصد خود سوء استفاده می‌کنند. در این باب توضیحات زیادی وجود دارد. یک تروریست اینترنتی به سیستم کنترل پردازشی تولید کننده غلات دسترسی پیدا می‌کند و با تغییر مقدار مکمل آهن، فرزندان یک ملت را که از آن غذا استفاده می‌کنند را بیمار می‌سازد و یا از بین می‌برد. از دیگر مثال‌های مربوط به این نوع جرم می‌توان از برج مراقبتی نام برد که منجر به سقوط هواپیمای بزرگ می‌شود، تغییر فرمول دارویی در کارخانهٔ داروسازی، تغییر فشار در لوله گاز که باعث انفجار و سوختن ساختمان‌های در خواب فرو رفته اطراف شهر می‌شود را نام برد. توضیحاتی از این نوع عملیات‌هایی هستند که تروریست‌های اینترنتی برای ایجاد آشوب در کشور به آن دست می‌زنند.

جرایم کیفری سنتی : همان‌گونه که قبلاً بحث شد، جهان اینترنت فرصت‌های جدید و زیرکانه ای را برای اعمال خلاف آمیز ایجاد می‌کند و این فرصت‌ها باعث ایجاد زمینه ای برای ارتکاب جرم‌های سنتی به روش‌های جدید می‌شوند. این روش در را به روی رفتارهای غیر قانونی باز کرده است که تا به حال غیر ممکن بوده‌اند. به رغم ظهور جرایم جدید که نتیجه پیشرفت تکنولوژی بوده‌اند و باعث ایجاد مشکلات جدیدی برای سیستم حقوقی موجود شده‌اند. قوانین موجود در قوانین سنتی هنوز برای مسائل مربوط به جرایم اینترنتی قابل استفاده هستند. قوانین مربوطی که در اینجا بحث شده بر اساس طبقه بندی‌هایی است که پیش‌تر توضیح داده شد.

سرقت : جرم دزدی بر طبق بخش ۳۷۸ قانون جزا (کیفری) قابل اجرا است. در اینجا عبارت " دارایی‌های قابل انتقال " مورد توجه است. بر طبق s.۲۲ قانون کیفری، دارایی‌های قابل انتقال شامل دارایی‌های فیزیکی از هر نوع بجز زمین و اقلام متصل به زمین می‌باشد. بر طبق این توصیف، مورد دزدیده شده می‌بایست بتوان از زمین جدا کرد؛ و از همه مهم‌تر آن که این شیء را باید بتوان از زمین برداشت و حمل کرد. بر طبق این قانون، اگر شیء سرقت شده متصل به زمین باشد و یا غیر قابل حرکت، آن شخصی مجرم شناخته نمی‌شود.

سئوالی که در اینجا مطرح می‌شود این است که این ماده چگونه در مورد

انتقال فایل‌های محتوی اطلاعات ارزشمند به کامپیوتر دیگر مصداق پیدا می‌کند؟ در حقیقت، اگر چه سندی از کامپیوتر دزدیده شد اما خود سند مفقود شده است. با اینکه چندین نسخه از این سند ایجاد شده ولی تا زمانی که سند پاک نشده و هنوز در دیسک‌های کامپیوتر ذخیره شده است، ویژگی دارایی قابل انتقال در این مورد خاصی جوابگو نیست و در نتیجه این ماده قابل اجرا نمی‌باشد. مبحث دیگر در این بخش کلمهٔ «دارایی» است دارایی در این بخش قانون به اموال قابل انتقال اشاره دارد؛ و منظور از دارایی در اینجا دارایی فیزیکی است که دارای ماهیت ملموس باشد. هر چیز به شکل دیجیتال باشد و یا به صورت مغناطیسی ذخیره شود قابل لمس نیست و در نتیجه ماهیتی ملموسی ندارد. متأسفانه، این ماده شامل حال این توصیف نمی‌شود.

فریب و کلاهبرداری : مثال‌های بالا گویای آن هستند که متخلفان با استفاده از اینترنت اظهارات غلط و بی اساس خود را به قربانیان احتمالی منتقل می‌کنند. مرتبط ترین بخش مورد استفاده توسط دادستان عمومی بخش ۴۱۵ قانون جزا است. در جرایم کامپیوتری، کلمات «گول زدن» ایجاد ابهام می‌کند. هنگامی که از کامپیوتر به منظور تغییر سند اصلی و یا انتقال پول سوء استفاده می‌شود. شخص گمراه شده در واقع کامپیوتر است و همان‌گونه که در قانون کیفری ملزم شده، کامپیوتر انسان تلقی نمی‌شود. این امر باعث ایجاد مشکل در اجرا و اعمال این بخش از قانون می‌شود.

نقشه های گول زننده در جهان اینترنتی بسیار متداول است. ۹۳ درصد قربانیان توسط این نقشه‌ها گول خورده‌اند و پول خود را از طریق چک در اختیار طراحان این نقشه‌ها قرار داده‌اند. اگر چه در جرایم اینترنتی فریب انسان مطرح است نه ماشین، برای اثبات عامل فریب هنوز مشکلاتی وجود دارد. سیستم‌های هرمی یا طبقه ای تجاری را که در اینترنت تبلیغ می‌کنند را به عنوان مثال در نظر بگیرید. برای موفقیت در این پرونده شخصی باید ثابت کند که گول خورده است. این در حالی است که در همان موقع افراد دیگری نیز بوده‌اند که از همان سایت دیدن کرده‌اند، پیغام را خوانده‌اند و گول نخورده‌اند. اثبات فریب خوردن کار آسانی نیست چرا که این امر باید فراتر از حد شک و گمان باشد.

جعل : بخش ۴۶۳ قانون کیفری به ویژگی‌های جرم جعل در مالزی می‌پردازد. اگر چه هیچ اشاره ای به عامل فریب نشده است، می‌توان آن را از عبارت زیر استنباط کرد ... «قصد به انجام جعل و یا انجام دادن عمل جعل به معنای وقوع جرم می‌باشد» در اینجا نیز قبل از اینکه شخصی متهم به انجام جعل شده باشد، ویژگی فریب خوردن باید رعایت شده باشد. همان‌گونه که قبلاً گفته شد، کلمه «فریب» در قانون جزایی مالزی تنها شامل فریب دادن انسان می‌شود. از آنجایی که عمل فریب دادن در جهان اینترنتی به فریب ماشین اشاره دارد، این قانون قابل اجرا نیست. مشکل دیگر در اجرای این قانون به منظور متهم کردن شخص اصطلاح «دارایی» است که بر طبق آن چه گفته شد به دارایی‌های فیزیکی که

ماهیتی ملموس دارند گفته می‌شود.
پرونده Rv gold بهترین مثال برای این نوع جرم است. در این پرونده، متهمان بدون مجوز به سرویس BT·S دسترسی پیدا کردند و سپس توانستند رمزهای میل باکس‌های خصوصی زیادی را به دست آوردند متهمان بر طبق قانون جعل ۱۹۸۱ به خاطر ورود غیر قانونی به سیستم مشتری از طریق کد وی مواخذه شدند. گفته شده بود که این دستگاه CIN(شماره شناسایی مشتری) و رمز ورود بوده است. با این وجود، دادگاه تجدید نظر بر این رای داد که سیگنال‌های الکترونیکی که کد شناسایی را تشکیل می‌دهند نمی‌توانند مانند دیسک و نوار ملموس باشند. همچنین شماره های مشتری‌ها و رمزهای ورود تنها به شکل موقت در سیستم کامپیوتر نگهداری شده‌اند و به نظر نمی‌آید که ضبط و یا ذخیره شده باشند.
مزاحمت : این نوع جرم در بخش ۴۲۵ قانون کیفری مطرح شده است. مشکلی که دوباره در این مطرح است دارایی‌هایی است که ملموس نیستند. هنگامی که کامپیوتری ویروسی می‌شود به دیسک اصلی صدمه وارد شده و ان را غیر فعال می‌سازد. منظور از دارایی در اینجا اطلاعاتی است که شکل جریانات الکترونیکی و مغناطیسی در دیسک کامپیوتر ذخیره می‌شود. سخت افزار کامپیوتر بدون اینکه آسیب دیده باشد هنوز فعال است. سئوال آنجاست که چگونه می‌توان ثابت کرد که دارایی در این مورد ذکر شده مورد تخریب واقع شده است؟
این مشکل در پروندهٔ V Cox Reiley که در ارتباط مستقیم با تخریب برنامه کامپیوتری بود مورد بررسی قرار گرفت. شاکی پرونده Cox استخدام شده بود تا یک اره کامپیوتری را توسط وارد کردن کارت جریان الکتریکی که شامل چندین برنامه کامپیوتری بود به کار اندازند. این وسیله شامل برنامه کنسلی نیز بود و Cox عمداً از این برنامه برای پاک کردن آن استفاده کرد. این امر باعث شد که اره بدون استفاده شود تا زمانی که دوباره برنامه ریزی بر روی آن نصب شود؛ و این کار وقت و تلاش زیادی را برای صاحبش به همراه داشت. Cox بر طبق بخش (۱) قانون خسارت‌ها ۱۹۷۱ محکوم شد. کلمه دارایی این گونه توصیف می‌شود «دارایی ملموس، چه حقیقی، چه شخصی». مشاورین متهم اظهار داشتند که عمل متهم تنها بر جریانات الکترونیکی نا ملموس تأثیر داشته‌اند. که این شامل مفهوم دارایی نمی‌شود. با این حال دادگاه متهم را به دلیل اینکه صاحب اره مستلزم صرف وقت و هزینه برای تعمیر اره شده مجرم تشخیص داد.
دادگاه ضرر مالی مالک را و نه منطبق بودن مفهوم دارایی با قانون موجود را مورد توجه قرار داد. مثال دیگری که نشانگر رفتاری خلاف در جهان اینترنت است را می‌توان در پرونده های R.V.whitely پیدا کرد. whitelyبدون مجوز به شبکه کامپیوتری JANET که با رمز کنترل می‌شد دسترسی پیدا کرد رفتار او تنها ناراحتی زیادی را ایجاد کرد بدون ایجاد کمترین جرمی برای مجرمان خدمات کامپیوتری و کاربران

سیستم بر طبق تبصره های خسارت جزایی ۲ اتهام بر این اشخاص وارد است :یکی از آن‌ها خسارت به دیسکی بود که حاوی برنامه و اطلاعات مورد استفاده در کامپیوتر بود. او بر طبق این قانون متهم شناخته شد و در طی دادگاه بررسی مجدد وی اظهار داشت که بر طبق قانون خسارت جزایی ۱۹۷۱ خسارت باید قابل مشاهده باشد. این در خواست او توسط Lord Jane CJ رد شد که در دادگاه تجدید نظر اظهار داشت «آنچه بر اساس این قانون باید ثابت شود این است که به دارایی ملموس آسیب رسیده باشد نه اینکه لزوماً خسارت ملموس باشد» تصمیم اتخاذ شده در پرونده Whitely نشان دهنده رضایت قضایی از این دادگاه است که عملی که باعث تغییر اطلاعات موجود در حافظه کامپیوتر می‌شود می‌تواند به عنوان خسارت جزایی شود. بر این اساس، تبصره مربوط به تخلف در قانون جزایی مالزی می‌تواند از استدلالی که در پرونده Whitely داده شد به منظور تفسیر «خسارت یا نابودی دارایی» در معانی فراتر استفاده کند.
مسائل جنسی:سوء استفاده های جنسی در قدیم شامل موارد جنسی است که توسط رسانه‌ها، از جمله کتاب‌ها، مجله‌ها، فیلم‌ها و نوار های ویدیویی پخش و منتشر می‌شود. قوانین مربوط به این مسئله به ۲ دسته تقسیم می‌شوند:

قوانین مربوط به مطالب و مزاحمت‌های جنسی: مهم‌ترین مشکل در باب پخش این مطالب از طریق اینترنت این است که هیچ تعریف مشترک بین‌المللی برای انواع توهین‌ها و مطالب جنسی وجود ندارد. به عنوان مثال در آمریکا توهین تنها محدود به مطالب سکسی می‌شود، مطالبی که بر طبق استاندارد جامعه می‌توانند میل جنسی را افزایش دهند و نشان دهنده رفتار جنسی باشند. اما در انگلستان، این واژه تنها به مسایل جنسی محدود نشده، بلکه شامل هر نوع مطلبی می‌شود، از جمله ایجاد فساد اخلاقی در شخص که ممکن است این مطلب را بخواند، ببیند و یا بشنود. آنچه در مالزی توهین محسوب می‌شود به احتمال زیاد در امریکا توهین نیست. در مالزی قوانین مربوط به این مورد شامل قانون کیفری، قانون چاپ و مطبوعات ۱۹۸۴ و قانون ارتباطات و رسانه‌ها ۱۹۹۸ می‌شود بخش ۲۹۲ قانون کیفری بیان می‌کند که هر شخص با اهداف تجاری که این توهین را در اختیار داشته و یا در بین عموم پخش کند مرتکب جرم شده است. علاوه بر آن، هر کسی در این جرم شریک باشد و یا از هر تجارتی که از طریق استفاده از این مطالب حاصل شود سود ببرد، مرتکب عمل خلاف شده است؛ و این شامل صاحبان سایت‌ها و یا گروهی است که در ایجاد سایت‌های جنسی و توزیع این مطالب به بینندگان مشارکت دارند. در میان موضوعات بحث شده در قانون ۱۹۸۴ مطبوعات و انتشارات، «چاپ مسائل ممنوع» به چشم می‌خورد. این عبارت به معنای انتشار مقاله‌ها، عکس، یادداشت‌ها، نوشته‌ها، صداها، موسیقی و اظهارات به هر روشی است که بتواند مخرب نظم جامعه باشد. مسائل جنسی جزو مثال‌های تحت پوشش این بخش است. وزیر حق جلوگیری از انتشار چنین مطالبی را دارد. با نگاهی اجمالی به این دو

بخش قانون به نظر می‌رسد این تبصره‌ها تنها حاکم بر انتشاراتی است که توسط ماشین چاپ و منتشر می‌شود. اما با مطالعه دقیق مفهوم «چاپ» در بخش ۲ این قانون، نتیجه گیری یکسان نخواهد بود.
این تعریف آنقدر وسیع و فرا گیر است که مطالب جنسی که به شکل دیجیتالی بر روی صفحه اینترنت منتشر می‌شود را نیز در بر دارد. به همین شکل، قانون ارتباطات و رسانه‌ها، بخش ۲۱۱ نیز انتشار مطالب غیر قانونی از طریق اینترنت را منع می‌کند که شامل مطالب توهین آمیز و تهدید کننده می‌شود. پروندهٔ RV fellows Amdd مورد مشابه است که فرستادن مطالب خلاف از طریق شبکه تلفنی عمومی جرم محسوب شد. این مطلب در سایه بخش ۴۳ قانون ارتباطات ۱۹۸۴ تصویب شد.
فعالیت‌های جنسی غیر قانونی : شامل سوء استفاده از زنان و کودکان در فعالیت‌های بی‌شرمانه است که یا با طیب خاطر و یا به هر شکل دیگر صورت می‌پذیرد. سئوال اینجاست که آیا قانون برای فایق آمدن بر این مشکل می‌تواند قابلیت اجرایی داشته باشد؟
تبصره های مربوط به قوانین حمایت از زنان و دختران، قانون مربوطه به جوانان و قانون حمایت از کودک تا حدی برای حل این مشکل قابل اجرا هستند. همانند تبصره های قانون کیفری، بخش‌های مرتبط با این موضوع یافت می‌شود. اگر فعالیت جنسی شامل آمیزش از مقعد و یا اعمال غیر طبیعی باشد، بخش ۳۷۷ تا D۳۷۷ قابل اجرا هستند. شخصی که به او تجاوز شده باشد و صفحه تجاوز بر روی اینترنت گذاشته شده باشد می‌تواند از آن به عنوان مدرکی برای متهم کردن متجاوز در دادگاه استفاده کند. بر اساس مباحث بالا قوانین موجود مرتبط به فعالیت‌های جنسی و توزیع این مطالب خلاف برای متهم کردن متخلفین کافی است. اما مشکل باقی مانده تنها در مورد کلمات و اصطلاحات استفاده شده در این تبصره است. عمدتاً عبارت‌های موجود در تبصره های ذکر شده به طور مستقیم به فعالیت‌های جنسی در اینترنت اشاره ای ندارند. برای استفاده از این تبصره‌ها باید به نتایجی دست پیدا کرد و این مترادف با شک است. به منظور رفع ابهام این اطلاعات و جرم شناختن عمل جنسی در اینترنت باید تغییرات را در زمینهٔ بخش‌های قانون کیفری اعمال کرد.

قانون جرایم کامپیوتری ۱۹۹۷ : راه حلی برای این مشکل؟

در راستای تأسیس کوریدور عالی رسانه ای (MSC) توسط نخست وزیر مالزی در سال ۱۹۹۶، دولت مالزی ۲ قانون جدید را که اصطلاحاً قوانین اینترنتی نامیده می‌شوند را معرفی کرد. این قانون شامل قانون جزای کامپیوتری ۱۹۹۷، قانون امضای دیجیتالی ۱۹۹۷، قانون پزشکی ۱۹۹۷ می‌باشد. اخیراً قانون جزای کامپیوتری ۱۹۹۷ (CCA ۹۷) از ابتدای ماه ژوئن سال ۲۰۰۰ به اجرا گذاشته شد. بر این امید هستیم که با اجرای این قانون، تا حدی بتوانیم بر مشکلاتی که فعالیت‌های خلافکارانه در جهان اینترنت ایجاد کرده‌اند فایق آییم. CCA ۹۷ تنها ۱۲ ماده دارد که همگی تا حد زیادی بر روی جرایمی که از طریق استفاده

از کامپیوتر ناشی می‌شوند تمرکز دارد و شامل جرایمی است که از طریق کامپیوترهای متصل به شبکه اینترنت انجام می‌شود.
این قانون ۳ تخلف عمده را مطرح کرده :
۱- دسترسی غیر قانونی به مطالب کامپیوتر که به آن مسدود کردن (هک کردن) نیز می‌گویند (بخش ۳ از ۹۷ **CCA**)
۲- دسترسی غیر قانونی با سو نیت به قصد ارتکاب جرم و یا سهولت بخشیدن به جرایم بعدی.
۳- ایجاد تغییرات غیر قانونی در مطالب موجود در کامپیوتر (بخش ۵ CCA ۹۷)
در توصیف تخلفات ذکر شده در بالا شفاف سازی معنای کامپیوتر ضروری به نظر می‌رسد. قانون۹۷ CCA یکی از معدودترین قوانین بین‌المللی بود که کامپیوتر را با توجه به هدفی که خود دنبال می‌کند تعریف کرد. معنای ذکر شده در بخش ۲ ۹۷ CCA چنان فرا گیر است که تمامی پیشرفت‌های تکنولوژی را در بر می‌گیرد. با وجود پوشش دهی گسترده آن، در مورد اینکه تا کجا این مفهوم عملکرد یک پردازشگر ریز را در مایکرو ویو و یا یخچال را شامل می‌شود نامفهوم و گنگ است. آیا شخصی به خاطر اینکه به سیستم پردازشگر بدون مجوز دسترسی پیدا کرده متهم می‌شود؟ این سئوال هنوز بی جواب مانده است.

تحصیل غیر قانونی مطالب و محتویات کامپیوتر :
بخش ۳ (۱) از ۹۷ CCA شخصی را زمانی بزهکار می‌داند که :
a) شخصی از کامپیوتر برای دسترسی به هر برنامه و اطلاعاتی که در آن ذخیره شده است استفاده کند.
b) دسترسی او غیر قانونی باشد.
c) در موقع استفاده از کامپیوتر بداند که دسترسی وی غیر قانونی است.
این ملزومات قابل افزایش هستند. برای بر آوردن ضرورت اول، هکر باید عملیاتی را برای دسترسی به اطلاعات ذخیره شده در کامپیوتر انجام دهد. عبارت «انجام عملیات» در این قسمت مورد سئوال است. تا چه اندازه شخصی می‌تواند عملیاتی را بر روی کامپیوتر انجام دهد؟ همان‌گونه در بخش ۲ ۹۷ CCA گفته شد، عملیاتی چون محاسبات منطقی، حذف، ذخیره و باز خوانی، ارتباطات با و یا از کامپیوتری را شامل می‌شود؛ و این به طور واضح مستلزم دوباره روشن کردن دستگاه کامپیوتر است. کلمات ارتباطات و ارتباطات رسانه ای نشان دهنده آن است که این زیر مجموعه تنها به جرم دسترسی به اطلاعات محدود نمی‌شود.
این بدان معناست که این جرم می‌تواند هم توسط شخصی که دسترسی مستقیم به کامپیوتر دارد و هم توسط هکر حرفه ای اینترنتی انجام شود. دسترسی به یک کامپیوتر خاصی لازم و ضروری نیست. غالباً گزارش می‌شود که هکرها به طور شانسی تماس تلفنی برقرار می‌کنند تا بتوانند افراد متصل به سیستم کامپیوتری را پیدا کنند. اولین لازمهٔ ارتکاب جرم بخش ۳ زمانی مثمر ثمر واقع می‌شود که حتی اگر هکر قربانی را نشناسد

ارتکاب جرم با موفقیت انجام شود. اول اینکه باید قصد و نیتی برای دزدی اطلاعات وجود داشته باشد و دوم اینکه مجرم بداند دسترسی وی غیر قانونی است. پرونده ای که نشان گر این وضعیت است پروندهٔ RV sean cropp، متهمی که به محل کار کارفرمای قبلی خود باز گشته بود تا وسایلی را خریداری کند. هنگامی که دستیار فروشنده متوجه نبوده، متهم دستورات را به کامپیوتر می‌دهد و برای خود درصد تخفیف قابل ملاحظه ای را لحاظ می‌کند.

قاضی در جلسه اول دادگاه صحبت وکیل را مبنی بر قصد داشتن مجرم به ارتکاب جرم را می‌پذیرد که «هر کامپیوتر» که در بخش ۱ ۱۹۹۰ CMA (معادل بخش ۳ ۹۷ CCA مالزی) ذکر شده مستلزم وجود کامپیوتر دومی نیز هست. اما این ادعا توسط دادگاه تجدید نظر رد شد و بیان شد که «معنای طبیعی و ساده واضح و آشکار» در AG reference ذکر شده است. دومین لازمه این بخش در ارتباط با دسترسی غیر قانونی است. اینکه آیا دسترسی پیدا کردن قانونی و غیر قانونی است در بخش (۵) ۲ ۹۷ CCA به شکل زیر آمده است.

a) خود شخص حق دسترسی به اطلاعات را نداشته.

b) وی از رضایت و یا اجازه شخصی که حق دسترسی به اطلاعات را داشته برخوردار نبوده است.

اولین مورد واضح و آشکار است. این دسته به افرادی اشاره دارد که بدون هیچ حقی، به سیستم اطلاعاتی کامپیوتر دسترسی پیداکرده اند. برای اثبات اینکه دسترسی شخصی غیر قانونی است، نیت دارنده کامپیوتر باید شفاف سازی شود. به عنوان مثال، ارائه دهنده یک سرویس اطلاعاتی ممکن است از روی رغبت به بازدید کنندگان اجازه دسترسی به یک سری اطلاعات را بدهد اما سایر اطلاعات را تنها در اختیار استفاده کنندگان محدودی بگذارد. ارائه کنندگان سرویس‌ها برای نشان دادن قصد خود مبنی بر اینکه بخش‌های خاصی از اطلاعات در اختیار بینندگان قرار دارد، ملزم می‌شوند که هر محدودیت دسترسی را به اطلاع بازدید کنندگان سایت‌ها قرار دهند. برای این کار آن‌ها می‌توانند برای ورود به سیستم از بیننده رمز و یا کد شناسایی بخواهند. شخصی که چنین اطلاعاتی را نداشته باشد متوجه می‌شود که از لحاظ قانونی اجازه پیشروی ندارد.

دومین گروه از دسترسی غیر قانونی مربوط به شخصی است که خود اجازه استفاده از رمز را دارد ولی اجازه ندارد که این حق را به شخصی دیگر بدهد مانند نوع رابطهٔ کارفرما و کارگر که در این نوع رابطه اگر چه کارگر اجازه دسترسی به سیستم کامپیوتری را دارد اما حق کنترل آن را نداشته و در نتیجه نمی‌تواند این حق را به شخصی دیگر واگذار کند. پروندهٔ Vignell Dppدر مورد دو افسر پلیس بود که هر دو به کامپیوتر ملی پلیس (prvc) برای مقاصد شخصی دسترسی داشتند. این اشخاص بر طبق بخش ۱ ۹۰ CMA مجرم شناخته شده و در دادگاه محکوم شدند آن‌ها موفق شدند از رأی صادره به دادگاه Crown در

خواست تجدید نظر کنند؛ و درخواست آن‌ها توسط دادگاه مورد تأیید قرار گرفت. سئوال اصلی اینجاست که آیا شخص که برای هدفی خاص اجازه دسترسی به سیستم کامپیوتری را دارد می‌تواند با استفاده قانونی خود به منظور انجام اهداف غیر قانونی جرم بخش ۱ را مرتکب شود؟ دادگاه تجدید نظر بر این عقیده بودند که این افسران پلیس قانونی عمل کرده‌اند.

نیت درونی ارتکاب جرم :

بخش ۴ از ۹۷ CCA به این مطلب می‌پردازد که نیت درونی در ارتکاب جرم چیست شخصی محکوم به ارتکاب جرم است اگر دسترسی غیر قانونی بر این قصد باشد که بخواهد به ارتکاب جرمی که بر اساس قانون جزا به تقلب، دروغ و یا آسیب رساندن منجر شود ادامه دهد و یا بخواهد از طریق خود و یا شخصی دیگر ارتکاب چنین جرمی را سهولت بخشد. اینکه ارتکاب جرم همزمان با دسترسی به سیستم و یا بعدها انجام شد حائز اهمیت نیست. به عنوان مثال هکری که بخواهد به قصد تهدید از طریق ایمیل به کامپیوتر و سیستم آن دسترسی پیدا کند اما نتواند وارد سیستم شود. احتمال آن ضعیف است که این شخص محکوم شود چرا که جرمی را مرتکب شده که تنها در حد برنامه ریزی بوده است اما اگر قصد و نیت وی ثابت شود احتمال محکومیت او بر اساس بخش ۴ ۹۷ CCA بیشتر است.

مورد شبیه RV. Thompsonبه راحتی به محکومیت منجر می‌شود. اگر چه که تکرار عملی که بر پایه دزدی و یا به دست آوردن دارایی از طریق حقه صورت گیرد هنوز قابل محکوم شدن نیست، نیت درونی جرم زمانی آشکار می‌شود که مجرم به اطلاعات مورد نیاز دسترسی پیدا می‌کند.

این بخش قانون ۲ نوع جرم را شامل می‌شود. اول : جرم دسترسی غیر قانونی و دوم سهولت بخشیدن به جرمی که منجر به فریب، دروغ و آسیب رساندن شود. جرم دوم به جرمی که در بخش ۳ ۹۷ CCA ذکر شد بستگی دارد. بر طبق این تبصره، متهم نمی‌تواند خلافکار اعلام شود در صورتی که مدرکی از دسترسی وی وجود نداشته باشد. به عنوان مثال، اگر شخصی به سایتی اینترنتی دسترسی پیدا کند که در آن هیچ نشانی از محدودیت در استفاده از رمز و یا کد خاص، ورود به اتاق گفتگو، تبادل نظر، گروه خبری و یا شبکه کاربری وجود نداشته باشد در این صورت استفاده شخصی قانونی است. این شخص سپس مطالب توهین آمیز یا نامناسبی را در این سایت‌ها قرار می‌دهد. در این صورت، اگر چه که این شخص مرتکب جرم‌های بعدی شده است، بر طبق بخش ۴ ۹۷ CCA به خاطر عدم وجود دسترسی غیر قانونی مجرم شناخته نمی‌شود. به منظور تعیین استفادهٔ مؤثر از این بخش، عامل دسترسی غیر قانونی نباید در این قانون لحاظ شود و در نتیجه در مورد پرونده‌هایی که به طور مثال پیش از این ذکر شد، بتوان شخصی را که مرتکب جرایم بعدی شده مجرم اعلام کرد. موارد زیر شامل موقعیت‌هایی است که بر طبق این قانون (بخش

چهار) امکان پذیر هستند.
RV pearlstone : کارگر قبلی شرکت تلفنی که از حساب این شرکت و از حساب مشتریان آن برای اختلال در سیستم تلفنی و تماس با آمریکا سو استفاده کرد.
RV Bong : تحلیلگر شرکت سرمایه گذاری که متهم به ایجاد حساب‌های جعلی در سیستم مدیریت سرمایه گذاری شد. در این جا «جرم بعدی» شامل انتقال فریبکارانه پول به حساب جعلی بوده است.
RV farquharsun : متهمی که به خاطر دسترسی به شماره‌ها و کدهایی که برای ایجاد مدل تلفنی تعقیب شد. farquharsun محکم به دسترسی غیر قانونی شد اگر چه که خود هرگز از کامپیوتر استفاده نکرد اما تنها از کارگر شرکت تلفنی خواست که به اطلاعات دسترسی پیدا کند

.

تغییرات غیر قانونی در محتوای هر کامپیوتر :

هر شخص که عملی را انجام دهد که منجر به تغییرات غیر قانونی محتویات و مطالب کامپیوتر شود بزهکار به حساب می‌آید. مفهوم اختیار به همان شکلی که در بخش ۱ بیان شده به کار می‌رود. تغییرات در صورتی غیر قانونی است که شخصی که این تغییرات را سبب شده حق ایجاد این تغییرات را نداشته و یا رضایت شخصی را که حق این تغییرات را نداشته و یا رضایت شخصی را که حق این تغییرات را دارد جلب نکرده باشد. بخش ۲ این قانون به طور مفصل در مورد تغییرات صحبت به عمل آورده است. تغییر محتویات کامپیوتر زمانی اتفاق می‌افتد که به واسطهٔ استفاده از عملکردهای کامپیوتر یا هر کامپیوتر دیگر :

a) هر برنامه و اطلاعات موجود در کامپیوتر مورد نظر تغییر کرده و پاک شود.
b) اطلاعاتی دیگر به محتویات معرفی یا اضافه شود.
c) رویدادی که باعث اخلال عملکرد عادی کامپیوتر شود اتفاق بیفتد.

بر طبق این تعریف، تغییرات غیر قانونی چنان دامنه وسیعی دارد که شامل دستورهای مخرب و تغییرات فوری می‌شود. اگر چه که به منظور بزهکار شمردن شخصی، مدرکی قوی مبنی بر تغییرات غیر قانونی باید وجود داشته باشد.

در غیر این صورت رأی بر بی گناهی صادر می‌شود. در پروندهٔ .RV Vatsal patelکه مربوط به پروژهٔ نوشتن نرم افزاری خاص بود آنچه اتفاق افتاد این بود که کابل‌های اطلاعاتی ناپدید شدند و سرانجام پیشرفت کار متوقف شد. برنامه های تخریب شده در کامپیوتر متهم پیدا شد. حکم محکومیتی بر اساس بخش ۳ قانون استفاده نادرست از کامپیوتر ۱۹۹۰(انگلستان) که معادل بخش ۵ CCA ۱۹۹۷مالزی است اعمال شد. خسارت‌های کلی ارباب رجوع بالغ بر ۹۰ پوند می‌شد و این احتمال وجود داشت که متهم جدول‌ها را به منظور طولانی کردن این قرار داد پر سود از بین برده و پاک کرده است.

هیچ مدرک حقیقی برای اثبات دست داشتن متهم در این موضوع وجود

نداشت. در نتیجه، دادگاه حکم تبرئه او را صادر کرد. دیگر مورد مربوط به تغییر اطلاعات کامپیوتر پرونده R V sinha است. وی که دکتر عمومی در کاردیف است متهم به استهزاء گرفتن و سعی بر منحرف کردن یک مورد قانونی است. او با دانستن این مطالب که نوعی دارو خطر حمله کشنده آسم را افزایش می‌دهد آن را برای یک زن حامله که قبلاً به آسم بود تجویز کرد. بعدها دکتر این مطلب را بیمار از بیماری آسم رنج می‌برده را در رکوردهای کامپیوتر خود تغییر داده این مورد به این دلیل که دکتر اجازه استفاده از کامپیوتر را داشته نتوانست بر طبق بخش ۳ قانون استفاده نامناسب از کامپیوتر ۱۹۹۰ (انگلستان) با آن برخورد شود. در بخش ۲ این قانون در مالزی تنها از آنچه تغییر غیر قانونی به حساب می‌آید صحبت شده اما متأسفانه این بخش شامل افرادی نمی‌شود که با داشتن مجوز دست به سوء استفاده و یا استفاده بیش از حد از قدرت خود برای تغییر محتویات کامپیوتر استفاده می‌کنند. این بخش قانون می‌بایست برای پاسخ به این مشکل مورد بازبینی قرار گیرد.
مثال‌های دیگر از این تبصره خاصی را می‌توان در پرونده RV Gaulden the times و RV. Whitaker مشاهده کرد. در مورد پرونده اول، Gaulden برای یک شرکت چاپ بسته های امنیتی نصب می‌کرده. بسته شامل سرویس بوده که از دسترسی بدون رمز جلوگیری می‌کرده و برای این سرویس شرکت مبلغ هنگفتی را پرداخت کرد. به علت ماهیت کامپیوتری عملیات‌های چاپ، کار در شرکت به مدت چند روز متوقف شد. دادگاه به دو سال ممنوعیت از کار و جریمه رأی داد. در مورد دوم، برنامه نویسی متهم چنین ادعا کرد که از آنجا که بر طبق قرار داد او تمامی حق مالکیت ذهنی را در نرم افزار در اختیار دارد، برای تغییر نرم افزار اختیار تام دارد. دادگاه اعلام کرد که با وجود حق چاپ نرم افزار، ماهیت قرار داد محدودیتی را بر اعمال حق تغییر دهنده ایجاد می‌کند؛ و این شخص بر طبق بخش ۳CMA(و یا بخش ۵ ۱۹۹۷ CCA مالزی) متهم شناخته شد.

۴- ارتباطات نادرست و غلط :
شخصی متهم به ارتکاب جرم می‌شود اگر شخصی به طور مستقیم و یا غیر مستقیم عدد، کد، رمز عبور و یا هر روشی دسترسی به کامپیوتر را در اختیار شخصی به غیر از کسی که اجازه انتقال اطلاعات به وی را دارد بگذارد. این حکم جرم برای جبران عمل خلاف دسترسی مستقیم و یا غیر مستقیم غیر قانونی به هر سرویس کامپیوتر وضع شد. به عنوان مثال یک کارمند اجازهٔ افشای راه دسترسی به سیستم کامپیوتر را به شخصی به جز کسی که اجازه انتقال اطلاعات را به وی دارد، نمی‌تواند داشته باشد.

۵-تشویق و شروع به ارتکاب جرم :
بر طبق بخش (۱) ۷ از ۹۷ CCA تشویق به ارتکاب جرم و یا تلاشی به

ارتکاب هر نوع عمل خلاف جرم محسوب می‌شود. علاوه بر آن، شخصی که در برنامه ریزی و یا مراحل بعدی ارتکاب جرم دست دارد بر اساس این قانون متهم شناخته می‌شود. برای این جرم خاصی، محکومیت زندان بیشتر از نیمی از حداکثر زمان تعیین شده برای جرم را شامل نمی شود بر طبق این بخش از قانون، برنامه ریزی و تلاشی برای ارتکاب جرم عمل خلاف به حساب می‌آیند. در حقوق جزا، جدا کردن مرز بین آماده سازی و تلاشی برای ارتکاب جرم بسیار سخت است اگر چه که جرم تلاش به ارتکاب جرم نیازمند آن است که برای جرم نامیده شدن از لحاظ درجه نزدیکی به انجام جرم تست شود، در حالی که آماده سازی برای ارتکاب عمل خلاف بر طبق بخش ۵۱۱ از قانون جزا جرم محسوب نمی‌شود. اما بر طبق بخش (۲) ۷ از CCA ۹۷ جرم به حساب می‌آید.

اشتباهات موضوعی: صاحب کامپیوتری که برنامه ای را در اختیار دارد که در کامپیوتری ذخیره شده و یا از کامپیوتری گرفته می‌شود و وی حق قانونی ذخیره و یا گرفتن این اطلاعات را نداشته باشد تا زمانی که خلاف آن اثبات شود مرتکب جرم بخش ۳ شده است. این بخش قانون بیان می‌کند که هر شخصی که در کامپیوتر خود اطلاعاتی را داشته باشد که غیر قانونی کسب شده باشند و چه آگاهانه از این جرم با خبر باشد یا نه مرتکب جرم دسترسی غیر قانونی به اطلاعات را شده است.

این حکم بر اساس قانون بخش ۳ قابل اجرا است. عبارت «مگر غیر از آن ثابت شود» به عنوان جرمی با مسئولیت قانونی تفسیر می‌شود. حتی اگر دارنده کامپیوتری که حاوی اطلاعات غیر مجاز است از محتویات موجود در کامپیوتر بی خبر باشد، به دلیل ماهیت بسیار بالای قانونی این جرم، وی مسئول شمرده می‌شود.

صلاحیت قضایی :

خاصیت بی مرزی کامپیوترها در انتقال و دریافت اطلاعات به وجود مرزهای ملی توجه ای ندارد. فعالیت‌های خلافکارانه در حالی به صورت on – line انجام می‌شوند که افراد خلافکار از کشورهای مختلف در آن سهیم هستند. این سئوال مطرح می‌شود که کدام سیستم قانونی دارای اختیار است؟ CCA ۹۷ جواب این سئوال را در بخش ۹ این قانون آورده است. این تبصره توضیحی است بر استفاده از این بخش قانون که از طریق آن هر شخصی که خارج از کشور مالزی در هر نقطه از جهان و با هر ملیت و یا نوع شهروندی مرتکب جرمی شود در حوضه ی اختیارات قضایی مالزی قرار می‌گیرد اگر اطلاعات و یا برنامه کامپیوتری در مالزی واقع شده باشد و یا امکان اتصال، فرستادن و استفاده کردن توسط کامپیوتری در مالزی وجود داشته باشد. واضحاً این بخش قانون اختیارات زیادی را در اختیار واحد اجرای قانون قرار داده است. اما مشکل در اجرای قانون برای متخلفین اینترنتی است که در خارج از مالزی سکونت دارند؛ و این با اختیارات قضایی کشور دیگر تداخل دارد. بهترین مثال از مواردی که به هنگام محکوم کردن فعالیت‌های خلاف بین‌المللی

ایجاد می‌شوند را می‌توان در پروندهٔ RV Governcr of Britxon Prcson & Anor exparte leorn (Levin's case) یافت.

در سال ۱۹۹۴، بانک شهر دچار نا امنی زیادی در سیستم برنامه ریزی پولی خود شد دلیل این ناامنی انتقال مبالغ موجود در حساب‌های مشتریان به حساب متهم و همدستانش بود. پس از همکاری همه جانبه ی آژانس‌های اجرای قانون و بقیه سازمان‌ها، من جمله شرکت تلفنی St. Petersburg، متهم پیدا و شناسایی شد. ولادیمرلوین در انگلستان دستگیر شد و پس از درخواست تجدید نظر به کشور آمریکا تحویل داده شد.

دو مورد مهم در این پرونده وجود دارد :

۱- قانون تحویل مجرم به مرجع قضایی کشور دیگر (استرداد) :

در هنگام تحویل مجرم، متقاضی موظف است ثابت کند که عمل مجرم فراتر از کمترین حد جرایم سنگین در دو حوضه ی قضایی است، یعنی هم در کشوری که مجرم از آن بازستانی می‌شود و هم کشوری که مجرم به آن تحویل داده می‌شود.

۲- محل وقوع جرم :

در پرونده levin، مشاور متهم ادعا کرد که عمل خلاف در سنت پطرزبورگ زمانی اتفاق افتاده که levin برای انتقال غیر قانونی پول از بانک شهر کلیدهای خاصی از صفحه کلید کامپیوتر را فشار داده و در نتیجه قانون روسیه قابل اجرا است. مشاور متهم اظهار داشت که مکانی که در آن تغییرات اطلاعات صورت گرفته، یعنی کامپیوتر بانک شهر در Paris penny آمریکا جایی است که جرم به وقوع پیوسته. رأی دادگاه به نفع متهم صادر شد؛ و دلیل آن این بود که زمان حقیقی که levin با سیستم کامپیوتری بانک در ارتباط بوده همان تماس با کلیدهای کامپیوتر بوده است.

هماهنگی بین‌المللی :

گام‌های مهمی توسط برخی سازمان‌ها برای هماهنگ سازی محافظت قانونی در برابر ارتباطات اینترنتی در سطح بین‌المللی برداشته شده است. اجرای قوانین داخلی بدون همکاری همهٔ کشورهایی که از طریق سیستم اینترنتی به هم متصل هستند آسان نخواهد بود. تلاش‌های زیر توسط تعداد کمی از سازمان‌ها انجام شده است :

۱- **OECD** : پس از کاری مشترک با مجمع فعال در زمینه اطلاعات، (خط مشی) سیاست ارتباطاتی و کامپیوتر (ICCP)، گزارشی نهایی در سال ۱۹۸۶ منتشر شد که شامل ۵ دسته جرایم اینترنتی است که یک شیوهٔ مشترک را در مورد جرایم کامپیوتری تشکیل می‌دهند.

۲- شورای اروپا : کمیته اروپایی با عنوان مشکلات مربوط به جرایم به منظور رسیدگی به مسائل حقوقی که به واسطه جرایم کامپیوتری ایجاد شده‌اند. گزارشی نهایی در سال ۱۹۸۹ منتشر شد.

کنوانسیون جرایم اینترنتی : شورای اروپا در حال حاضر مشغول ایجاد

توافقنامه ای است که مسائلی از جمله همکاری دو جانبه، تحویل مجرم به مراجع کشور دیگر، منع و رمز گشایی ارتباطات اینترنتی را شامل خواهد شد.
کنوانسیون همکاری‌های چند جانبه حقوقی : اجرای قوانین جرایم اینترنتی

نتیجه گیری:
اجرای قانون CCA ۹۷ از ابتدای ماه ژوئن سال ۲۰۰۰ راهکار مفیدی است برای مقابله با مشکلات جدی جرایم اینترنتی. همان‌گونه که قبلاً گفته شد، مشکلاتی که در ارتباط با جرایم سنتی ایجاد می‌شوند دیگر وجود ندارند چرا که قانون جدید از مواردی که «سخت قابل اثبات هستند» و قانون را غیر قابل اجرا می‌کنند رهایی پیدا کرده. به عنوان مثال جرم دسترسی غیر مجاز، مستلزم عامل دارایی قابل انتقال و فیزیکی که با ماهیت دیجیتالی هم خوانی ندارد نیست.
سه جرم اصلی در CCA ۹۷ ممکن است بر مشکلات قوانین سنتی فایق آیند. با این وجود تبصره های CCA ۹۷ به نوبهٔ خود مشکل ساز هستند. همان طور که ذکر شد، فائق آمدن بر قسمت‌های مشکل ساز این تبصره‌ها بهترین راه حل است.

Cyber-crimes: Problems And Solutions Under Malaysian Law.

By:
Associate Prof. Dr. Nazura Abdul Manap
Lecturer in Information Technology Law
Universiti Kebangsaan Malaysia (The National University Of Malaysia)
۴۳۶۰۰ Bangi ,Selangor, Malaysia.
Email: nazura@pkrisc.cc.ukm.my

ABSTRACT.

Malaysia has been burdened with the explosion of information technology since middle of ۱۹۹۰s. This is due to the rapid development of internet technology all over the world. Computer systems offer some new and highly sophisticated opportunities for law breaking and they create the potential to commit traditional type of crime in non-traditional ways. One of the obvious problems occurred by the usage of this technology is the new version of crimes, so-called "cyber-crimes". Basically traditional crimes require the proof of physical elements, unlike this cyber-crime which is committed virtually , the task of proving the criminal act is increasingly difficult. The cyber-crime is transnational in nature which requires concerted international cooperation to address it effectively. This can only happen , however, if there is a common framework for understanding what the problem is and what solutions there may be. Since criminal law in Malaysia is inadequate to curb this problem , the government has come up with the new legislation namely Computer Crime Act ۱۹۹۷. Till date, this particular act has not yet been tested since it is still not enforced. Thus, this paper is aimed at highlighting this new version of crime and how to harmonize the existing law amongst the countries.