اخلاقیات سایبر

کلمات کلیدی.
اخلاق(Ethics)، جرم رایانه‌ای(Cyber Crime)، سامانه اطلاعاتی و ارتباطی(ICT System)، فضای سایبر(Cyber Space)، محرمانگی(Privacy)، مالکیت فکری(Intellectual Property)، حق نشر(Copyright)، شهروند سایبر(Netizen)

مقدمه.

همواره پیشرفت‌های بشر در طول تاریخ، علاوه بر منافعی که برای وی به ارمغان آورده است، بدلیل ایجاد امکانات جدید و نوع آفرینش جستجوگر آدمی، باعث دردسرهایی نیز شده است. این امر پس از رنسانس صنعتی و تولید روزافزون ابزارهای نو بقدری شدت گرفت که در برهه‌های زمانی خاصی، بنگاه‌های قانونی را از پایگاه‌های جرم عقب انداخت. با پیدایش رایانه‌ها و نفوذ گسترده‌ی آن‌ها در خانه‌ها، دسترسی عامه مردم در گوشه گوشه دنیا به اینترنت، گسترش شبکه‌های مخابراتی و ایجاد انواع بسترهای ارتباطی، زمینه‌های مناسبی برای انجام افعال ناشایستی که تحت نام «جرایم رایانه‌ای» شناخته می‌شوند فراهم آمد. بیشتر ما هر روزه مواردی نظیر این‌ها را در مطبوعات مرتبط و وب مشاهده کرده‌ایم:

روزانه ۶۱۱۰ مورد حمله به خدمات اینترنتی رخ می‌دهد. [۰]

جرایم رایانه‌ای جهانی ۸۱٪ افزایش یافت. [۱]

نوجوان انگلیسی به بانک اطلاعاتی ناسا نفوذ کرد. [۲]

مسلم است که در گذشته تنوع جرایم بسیار اندک بود و پیچیدگی چندانی نیز در آن‌ها مشاهده نمی‌شد اما با ورود بسترهای مذکور به عرصه جامعه، چنان تحولی در ارتکاب به جرایم رخ داد که حتی در کشورهایی با نظام‌های قانونی قوی و با گذشت بیش از دو دهه از شروع رسیدگی به موارد این چنین، تصحیح و تغییر قوانین مربوطه به آن ادامه دارد. با عنایت به رشد تجارت الکترونیک، پایه‌ریزی بسیاری از سرمایه‌گذاری‌ها بر روی بسترهای اطلاعاتی و ارتباطی و تمام مواردی که در بالا به آن‌ها اشاره شد، همگی لزوم توجه به مباحث اخلاقی و حقوقی در فناوری اطلاعات و ارتباطات را روشن می‌کند. قصد ما در این مقاله، تنها پرداختن به مسائل در سطحی کلی است و آشنایی با تعاریف مرتبط با اخلاقیات سایبر مدنظر است.

[۱AD]Comment: براساس آمار گوگل در سال ۲۰۰۵

[۲AD]Comment: براساس گزارش گروه امنیتی سیمانتک

[۳AD]Comment: خبرنامه اینترنتی شرکت مایکروسافت در سال ۲۰۰۳

اخلاق [۳]

اخلاق جمع واژه «خُلق» و به معنای سرشت، طبیعت،عادت و خوی است. عالمان اخلاق، معانی اصطلاحی متعددی برای اخلاق بیان کرده‌اند. یکی از رایج‌تری آن‌ها عبارت است از:

«صفات انسانی که در نفس انسان رسوخ کرده و پایدار باشند.»

علم اخلاق، علمی است که با آموزش صفات و ملکات پسندیده و طریقه کسب آن‌ها و نیز بیان صفات ناپسند و روش‌های اجتناب از آن‌ها، راه رسیدن به منش نیکو را به ما نشان می‌دهند و نیز شیوه صحیح رفتار ما را در ارتباط با خود، دیگران و پروردگار به منظور نیل به سعادت و کمال معرفی می‌کند.

[٤AD]Comment: فلسفه اخلاق، دفتر نشر اخلاق، چاپ یکم

جرایم رایانه‌ای.

یک جرم رایانه‌ای به فعالیت یا مجموعه‌ای از اقدانات اطلاق می‌شود که یک سامانه رایانه‌ای نظیر یک رایانه یا شبکه‌ای از رایانه‌ها ابزار یا هدف آن باشند. جرایم رایانه‌ای در فضایی رخ می‌دهند که به اصطلاح «فضای سایبر» نامیده می‌شود. همچنین این لفظ به آن دسته از جرایم سنتی چون کلاهبرداری، دزدی، تهدید و اخاذی، جعل اسناد و اختلاس نیز اطلاق می‌شود که در آن‌ها سامانه‌ی رایانه‌ای جهت تسهیل فعالیت غیرمجاز بکار می‌رود. جرایم رایانه‌ای را می‌توان بصورت گسترده در عبارت زیر تعریف کرد:

«بزه‌ای که با زیرساخت فناوری اطلاعات و ارتباطات درگیر است و شامل مواردی چون دسترسی غیرمجاز، شنود غیر قانونی(با بکارگیری ابزار فنی برای انتقال داده رایانه‌ای غیرعمومی)، مداخله داده‌ای(وارد کردن خسارت، حذف، تباه کردن،

براساس برآورد کمیته‌ی تجسس فدرال ایالات متحده آمریکا (FBI) در سال ۲۰۰۴، ۹۰٪ از ۵۰۰ شرکت مورد برآورد، رخنه‌های امنیتی را گزارش کردند و به ۸۰٪ آن‌ها از این رخنه‌ها، زیان‌های مالی تحمیل شده است. مطابق آمار ملی در سال ۲۰۰۳، همه ساله چهار میلیارد دلار در کلاهبرداری‌های مبتنی بر کارت اعتباری، مورد سرقت قرار می‌گیرد. تنها ۲٪ از تراکنش‌های مالی کارت اعتباری از طریق اینترنت صورت می‌گیرد ولی نیمی از چهار میلیارد ذکر شده در این تراکنش‌ها ردوبدل می‌شود. تمام این یافته‌ها تنها شرحی از بزه‌های رخ داده از طریق سامانه‌های رایانه‌ای هستند و دلیلی برای لزوم کند کردن این فعالیت‌ها. سؤال اینست که چگونه؟

جرایم رایانه‌ای بدلیل بکارگیری از سامانه‌های اطلاعاتی و ارتباطی، پیگیری قانونی را تا حدی برای بنگاه‌های قانونی در دنیا مشکل کردند. فعالیت‌ها برای کنترل جرایم رایانه‌ای آغاز شد ولی این اقدامات نه تنها موفق نبودند بلکه کار را به یک نبرد از پیش باخته برای پلیس تبدیل کردند. شاید عمده دلیل این امر، عدم وجود استاندارد بین‌المللی در ردگیری و قوانین آن بود.

کنوانسیون جرایم رایانه‌ای بعنوان اولین قرارداد جهانی، برای پویش جرایم سایبر با یکنواخت کردن قوانین ملی، اطلاح اسلوب‌های بازجوینده و افزایش همکاری ملت‌ها تشکیل شد و چهل و سه آن‌را پذیرفتند. تنفیذ این کنوانسیون در مجلس سنای ایالات متحده آمریکا در آگوست سال ۲۰۰۶ و به‌عنوان شانزده‌امین کشور پذیرنده کنوانسیون صورت گرفت.

«در راستای ایجاد تعادل بین آزادی مدنی و محرمانگی، این معاهده باعث به اشتراک گذاری مدارک وشواهد الکترونیک شاخص در بین ملل مختلف را تقویت می‌کند تا اقدامات قانونی بطور مؤثرتری در ستیز با جرایم صورت بگیرند.»

مثال‌هایی از جرایم سایبر.

در این قسمت با بررسی چند نمونه مهم از جرایم، اهمیت آن‌ها را بیشتر آشکار می‌کنیم. این مثال‌ها در حوزه مالکیت‌های فکری قرار دارند.

۱. نَپستر[۶](Napster): فرض کنیم که دیروقت شبی در اوایل سال ۲۰۰۱ هستیم و شما پشت رایانه شخصی خود به گشت و گذار اینترنتی مشغول هستید که در جایی نظیر e-zines به گروهی برمی‌خورید که از کارهایشان بدلیل سبک مشابه یانی –آهنگساز معروف- تعریف بسیاری شده است. شما می‌توانید سری به Napster بزنید و کارهای این گروه را جستجو کنید. مطمئناً بسیاری از کاربران آن‌ها را دارند و با کمی شانس، یکی از آنها برخط است. با چند کلیک ساده و البته پهنای باند مناسب، در عرض چند دقیقه شما آلبوم این گروه را روی هارددیسک خود دارید، میتوانید تا هر زمانی که دوست دارید آن‌را گوش دهید و اگر مناسب بود، برای دوستان خود نیز ارسال کنید.تمام این‌ها از درون اتاق شما و بدون صرف حتی یک ریال برای ارزش محتوی مذکور است. آیا این مسأله اخلاقی است؟

نپستر نام مستعار یک جوان ۱۹ساله اهل نیوجرسی بنام «Shaun Fanning» است. وی در ژانویه سال ۱۹۹۹ با نوشتن قطعات کد رایانه‌ای، امکان انتقال فایل‌های با فرمت MP3 را بین خود و دوستانش فراهم آورد. این کد به یک موفقیت بزرگ بدل شد زیرا به هر کسی و در هر کجا، اجازه مبادله موسیقی بصورت سریع و رایگان را می‌داد. چند ماه بعد او کالج را ترک کرد و با یافتن سرمایه‌گذار، شرکت نپستر را در جولای سال ۱۹۹۹ تأسیس کرد.

همان‌گونه که «Edgar Bronfman Jr.»، رئیس Universal Corporation، بزرگ‌ترین مؤسسه موسیقی در دنیا اظهار داشت:

> «چند کلیک کافی است تا شما را قادر سازد که به تمام کتب نوشته شده در تمام زبان‌های دنیا، تمام فیلم‌ها ساخته شده، تمام موسیقی‌های تهیه شده و تمام برنامه‌های ضبط شده دسترسی بیابید»

آیا این مسأله خوب است یا بد؟ یک کاربر ناشناس می‌گوید:

> «نپستر برای من یعنی رایگان. اگر آن‌ها تصمیم بگیرند که برای خدمات‌شان هزینه تصویب کنند، من از بنگاه رایگان دیگری استفاده خواهم کرد. اینترنت جای خوبی است. شما می‌توانید هر چیزی را بخواهید در آن بیابید. مهم نسیست چه چیزی، مهم اینست که رایگان!»

پروفسور حقوق از دانشگاه Temple، آقای «David Post» می‌گوید:

> «اگر هفت میلیون نفر چیزی را می‌دزدند، در نتیجه آن‌ها آن‌را نمی‌دزدند!»

[٥AD]Comment: براساس تعریف ویکی-پدیا

[٦AD]Comment: تعداد بروز شود جستجو شود Convention on Cybercrime

[٧AD]Comment: رهبر حزب اکثریت سنا، بیل فریست

[٨AD]Comme: Intellectual property and cyberspace, www.napste

درمقابل آقای «Michael Eisner»، رئیس و مدیرعامل شرکت والت دیزنی معتقد است که:

«دزدان دریایی اینترنتی امروزه در تلاش اند تا پشت استدلالات تدبیری نسل جدید فضای سایبر پنهان شوند ولی تنها کاری که در واقع انجام می‌شود، ایجاد روکشی برای سرقت‌های نسل قدیم است.»

برای آن‌هایی که دارای حقوق قانونی پرداخت برای این‌گونه محصولات –که با نام محتوی تحت مالکیت فکری شناخته می‌شوند- هستند، این اخبار دلهره‌آور است. درمقابل، کاربران اینترنت از هکرها گرفته تا معلم‌ها تا دانش‌پژوهان تا علاقه‌مندان موسیقی‌های غیرمجاز، سر دیگر این طناب را می‌کشند.

۲. دزدی هویت[۷](Phishing): هنگامی که گمان می کردید که می توانید با اطمینان به سراغ میل باکس خود بروید، نوع جدیدی از تقلب در راه بود، Phishing. حیله‌های دزدی هویت چیزی فراتر از هرزنامه های ناخواسته و مزاحم هستند. آنها می توانند منجر به دزدیده شدن شماره‌های اعتباری، کلمات عبور، اطلاعات حساب یا سایر اطلاعات شخصی شما شوند. Phishing نوعی از فریب است که برای دزدیدن هویت شما طراحی شده است. در یک حیله از نوع Phishing، یک فرد آسیب‌رسان سعی می کند تا اطلاعاتی مانند شماره‌های اعتباری و کلمات عبور یا سایر اطلاعات شخصی شما را با متقاعد کردن شما به دادن این اطلاعات تحت ادعاهای دروغین بدست آورد. این نوع حملات معمولاً از طریق هرزنامه یا پنجره‌های pop-up می‌آیند.

[۹AD]Comme: گروه امداد امنیت کامپیوتری ایران

یک فریب Phishing توسط یک کاربر بداندیش که میلیون‌ها ایمیل فریبنده ارسال می‌کند، آغاز می‌شود بطوریکه بنظر می‌رسد که از وب سایت‌های معروف یا از سایت‌هایی که مورد اعتماد شما هستند همچون شرکت کارت اعتباری یا بانک شما می‌آیند. ایمیل‌ها و وب سایت‌هایی که از طریق ایمیل‌ها برای شما ارسال می شود، آنقدر رسمی بنظر می رسند که بسیاری از مردم را به این باور می‌رسانند که قانونی هستند. با این باور که این ایمیل‌ها واقعی هستند، افراد زودباور اغلب به تقاضای این ایمیل‌ها مبنی بر شماره‌های کارت اعتباری، کلمات عبور و سایر اطلاعات شخصی پاسخ می دهند.

یک جاعل لینکی در یک ایمیل جعلی قرار می دهد که اینگونه بنظر می رسد که لینک به وب سایت واقعی است، اما در واقع شما را به سایت تقلبی یا حتی یک پنجره pop-up می برد که دقیقاً مانند سایت اصلی بنظر می رسد. این کپی‌ها اغلب وب سایت‌های Spoofed نامیده می شوند. زمانی‌که شما در یکی از این وب سایت‌ها یا pop-up های تقلبی هستید، ممکن است ناآگاهانه حتی اطلاعات شخصی بیشتری وارد کنید که مستقیماً به شخصی که این سایت تقلبی را درست کرده است، ارسال خواهد شد. حال این شخص می‌تواند از این اطلاعات برای خرید کالا یا تقاضا برای یک کارت اعتباری جدید یا سرقت هویت شما اقدام کند.

۳. کمین سایبر(Cyber Stalking): استفاده از خدمات پیام‌رسانی اینترنتی یا سایر ابزار الکترونیک برای آزار رساندن به شخص دیگری است. یک متجاوز سایبر، فعالیت‌های مختلف قربانی‌اش را به قصد جمع‌آوری اطلاعات، آغاز ارتباط، ایجاد تهدیدات متعدد و سایر گونه‌های آزار ردگیری می‌نماید. متجاوزان سایبر، قربانیان‌شان را از طریق فروم‌ها، تابلوهای اعلان الکترونیک(Bulletin Boards)، اتاق‌های گفتگو، ابزراهای جاسوسی رایانه‌ای و اسپم‌ها هدف‌گیری می‌کنند. کمین‌کاران با دریافت اولین پاسخ از سمت قربانی، ردگیری وی را آغاز نموده و بنا به نوع تجاوزشان، اطلاعات مورد نظرشان را دریافت و آزار خود را وارد می‌کنند.

کمین سایبر، یک مجموعه فعالیت دنباله‌دار است. دقیقاً مشابه کمین فیزیکی، کمین در فضای سایبر می‌تواند منجر به تجربیات وحشتناکی برای قربانی منجر شود. در این‌گونه آزارها، احتمال آسیب‌های روانی شدید و حتی آسیب‌های فیزیکی هست. در موارد فیزیکی، قربانی مواردی چون تماس‌های تلفنی فریب‌کارانه یا توهین‌آمیز، بسته‌های پستی خراب‌کارانه یا موهن، تجاوز و تهاجم‌های فیزیکی را تجربه می‌کند.

نخستین قانون ایالات متحده علیه آزار سایبر، در ۱۹۹۹ و در ایالت کالیفرنیا وضع شد. سایر ایالات، قوانین جدید را در دل قوانین کمین و آزار قدیمی افزودند. در انگلستان و به سال ۱۹۹۸، هرگونه برقراری تماس بداندیشانه در شاخه آزار سایبر قرار گرفت و به عنوان عمل تهاجمی و دارای جرم کیفری شناخته شد.

۴. پیام‌های کوتاه کلاهبردارانه(SMS Spoofing): به نسبت، یکی از جدیدترین روش‌های شرارت با فناوری پیشرفته است. امروزه این مورد تقریباً بر روی تمام دستگاه‌های تلفن همراه و PDAها برای دست انداختن یا جعل هویت قابل پیادسازی است. این اقدامات معمولاً با ارسال ویروس‌های قابل انتقال از طریق خطوط مخابراتی و با انگیزه ایجاد رفتار خرابکارانه صورت می‌پذیرد. پیام‌های کوتاه کلاهبردارانه از زمانی‌که اپراتورهای مخابراتی، شبکه‌های خود را با اینترنت بصورت یکپارچه در آوردند امکان‌پذیر شد. در این شرایط، هر کسی از درون فرم‌های درون صفحات سایت اپراتور و یا نمایندگی-های آن‌ها و یا حتی از درون ایمیل ممکن است. متأسفانه در اکثریت قریب به یقین فرم‌های طراحی شده، بدلیل وجود آسیب‌پذیری زیاد و عدم رعایت موارد امنیتی، این اجازه به هکرها داده می‌شود تا با شکستن تونل‌های پروتکلی که اتصال وب و شبکه مخابراتی را ایجاد می‌کنند، برای مقاصد خود ایجاد بستر کنند. درکنار ایم مورد، نرم‌افزارهای کدباز اختصاصی برای این کار تهیه شده است که به کاربر ناشناس اجازه استفاده از شبکه مخابراتی اپراتور مورد نظرش را برای اقدامات خرابکارانه می‌دهد. البته گونه‌های دیگری از این نوع اقدامات را در ایران هم شاهد بودیم. مسلماً همگی ما ماجرای smsهای بهزیستی را بخاطر داریم!

قوانین سایبر.

قوانین حاکم بر فضای سایبر موضوعات بسیاری را شامل می‌شوند که همگی در ارتباط با استفاده از سامانه‌های اطلاعاتی و ارتباطی هستند. این قوانین موارد زیر را دربر دارند:

- ✓ محرمانگی
- ✓ مالکیت فکری
- ✓ آزادی بیان و سانسور
- ✓ حوزه قضایی اختیارات قانونی

در قوانین سایبر، به حقوق قانونی شهروندان وب(Netizens) و قواعدفضای سایبر برای زندگی سالم، مسالمت‌آمیز و هماهنگ آنان پرداخته می‌شود. بزرگ‌ترین چالش پیش از قوانین سایبر، ایجاد یکپارچگی بین آن‌ها با سامانه‌های قانونی دنیای فیزیکی است. از آن-جایی که فضای سایبر دارای هیچ‌گونه مرز جغرافیایی نیست و شهروندان آن، دارای خصوصیات دنیای بیرون نظیر جنسیت، سن و ... نیستند، تعارضات بسیاری در بحث حقوق شهروندی از نقطه‌نظر یک شهروند دنیای فیزیکی پیش خواهد آمد. بسیاری از کشورها در دنیا، قوانینی را برای کنترل تراکنش‌های شهروندان سایبر در حوزه اختیارات قضایی خود، وضع نموده‌اند. البته موارد بحث‌انگیزی هم در این قوانین بوجود آمدند که باعث جدال‌هایی شدند. به عنوان مثال:

- ✓ محجوبیت فعالیت‌های ارتباطی(Communication Decency Act)
- ✓ آئین‌نامه‌های هرزه‌نگاری(Pornography Regulation Law)
- ✓ تعهد منابع کپی متون(Scholar Liability)
- ✓ قانون علایم تجاری و اسامی دامین

در ایران هم قانون جرایم رایانه‌ای با ارسال لایحه‌ای در انتهای دولت خاتمی، و با پافشاری قوه قضائیه به تصویب رسید. این قانون در سه بخش تعاریف، جرایم و مجازات‌ها و آئین دادرسی توسط مرکز مطالعات مجلس شورای اسلامی شکل گرفت. البته برای پیاده-سازی این قوانین توسط مجری آن یعنی دولت، زیرساخت‌هایی لازم است که با وجود تصویب قوانین، این ساختار استاندارد هنوز وجود خارجی هم ندارد.

محرمانگی[۹].

Comment[AD۱۰]: مباحث حقوقی و اخلاقی در فناوری اطلاعات، علی انگورچی/امامیان

Ethics and Privacy of Communications in the E-Polis
Gordana Dodig-Crnkovic and Virginia Horniak
Department of Computer Science and Electronics
Mälardalen University
Västerås, Sweden

پیش از ظهور فناوری اطلاعات و ارتباطات، ارتباطات نوع بشر بطور برجسته مستقیم و کلامی بود. امروزه ما برای ایجاد ارتباط از سامانه‌های اطلاعاتی و ارتباطی استفاده می‌کنیم. با درمیان بودن یک رایانه، اطلاعات با سرعت بسیار به سمت عده بسیار زیادی از گیرندگان دور و نزدیک ارسال می‌شود. این مسأله، ما را به سوی انواع جدیدی از اصول اخلاقی نظیر نفوذ به حریم خصوصی و استفاده از اطلاعات محرمانه رهنمون می‌سازد.

حریم خصوصی را می‌توان دفاع از دو حق اولیه آدمی دانست:

- ✓ اولویت در تعیین هویت فرد
- ✓ حق دارایی فضای فکری خصوصی

حریم خصوصی را می‌توان در ارتباط چهار تشکل مجزا بررسی نمود:

- ✓ فرد مورد مطالعه در زمینه حریم خصوصی.
- ✓ افرادی که تشکل اول به آن‌ها اطلاعاتی به منظور برقراری یا ادامه ارتباط شخصی یا در مقابل خدمات می‌دهد.
- ✓ افراد جامعه مورد بررسی که توانایی دسترسی به اطلاعات خصوصی تشکل اول را دارند ولی هیچ‌گونه رابطه با او نداشته و نیز صلاحیت استفاده از آن اطلاعات را هم ندارند.
- ✓ عموم مردم که هیچ‌گونه ارتباطی با تشکل اول و اطلاعات وی ندارند.

در جریان تعاملات بین این چهار تشکل، فرد منحصربفرد تقاضای درجات متفاوتی از محرمانگی را می‌کند. برتری‌های روابط نزدیک با ریسک انتشار اطلاعات و سوءاستفاده از آن‌ها در قیاس است که می‌تواند منجر به هدر رفتن فضای شخصی و یا صدمه به هوویت فرد شود.

محرمانگی اطلاعات به معنی مصون ماندن اطلاعات شخصی افراد از سوءاستفاده است. رفاه و تسهیلات بسیاری که سامانه‌های اطلاعاتی و ارتباطی برای شهروندان سایبر، در همه شئون زندگی از جمله امور بانکی و خریدها به قیمت قربانی شدن حریم خصوصی کاربران تمام می‌شود. در این راستا، سازمان‌ها موظف به دنبال کردن سیاست‌هایی در زمینه حفظ حریم خصوصی افراد هستند و دراختیار گذاشتن اطلاعات کاربران را منوط به احکام مراجع ذی‌صلاح قانونی یا اثبات وجود دلایل امنیت ملی عنوان می‌کنند.

مالکیت فکری[۹].

Comment[AD۱۱]: مباحث حقوقی و اخلاقی در فناوری اطلاعات، علی انگورچی/امامیان
www.napster.com
www.riaa.com
www.copyright.gov

مالکیت فکری به خلاقیت‌های ذهنی انسان شامل ابداعات، آثار ادبی و هنری و نمایه‌های اسامی و تصاویر مورد استفاده در تجارت اشاره دارد. این مورد با مالکیت فیزیکی معمولی در یک نقطه تفاوت اساسی دارد. اگر من صاحب یک خانه باشم، شما دیگر نمی‌توانید به عنوان مالک آن بحساب بیایید. در مقابل در فضای سایبر، مالکیت فکری امکان به اشتراک‌گذاری را دارد، آن هم بدون کاستی در ارزش‌اش.

حقوق مالکیت فکری مشابه سایر حقوق مالکیت است، بگونه‌ای که به مخترع یا مالک حق ثبت، علامت تجاری یا حق نسخه‌برداری اجازه بهره‌برداری از اثر یا سرمایه‌گذاری خود را می‌دهد. این حقوق در ماده ۲۷ اعلامیه جهانی حقوق بشر تصریح شده است. سازمان جهانی مالکیت فکری به عنوان بخشی از سازمان ملل متحد، محلی است که در آن کشورهای عضو می‌توانند درخصوص هماهنگی و وضع قوانین و مقررات و رویه‌های حمایت از حقوق مالکیت فکریبه بحث و تبادل نظر بنشینند. بعلاوه این سازمان، سامانه‌های جهانی ثبت ابداعات، علایم تجاری و طرح‌های صنعتی را نیز ارایه می‌دهد.

این سازمان طرح جدید و گسترده‌ای را به‌نام WIPO Digital Agenda آغاز کرده است که طی چند سال آینده، مشخص‌کننده و پاسخ‌گوی تأثیرات اینترنت و فناوری‌های دیجیتالی برروی نظام مالکیت فکری خواهد بود.

شاید مهم‌ترین مبحث در این مورد بحث سرقت نرم‌افزاری و کپی‌های غیرقانونی بود که در اکثر مناطق دنیا بگونه‌ای و تا حد خوبی حل شده است.

آزادی بیان.

در قیاس با رسانه‌های سنتی چاپی، قابلیت دست‌یابی و گم‌نامی نسبی فضای سایبر موانع قدیمی بین فرد و توانایی او برای انتشار را از میان برداشته است. هر شخص با دارا بودن یک اتصال اینترنتی و با هزینه پخش نزدیک به صفر، صورت بالقوه دارای میلیون‌ها شنونده برای سخنانش است. این مسأله باعث ایجاد سؤلات بسیار و بزرگ‌نمایاندن پیچیدگی‌های قانونی مرتبط با آزادی بیان می-

راه‌حل‌های بسیاری برای این مورد پیشنهاد و مورد آزمایش قرار گرفت. از جمله در چین، ایران، عربستان سعودی، سنگاپور و تونس، هزینه‌های بسیاری برای فیلترینگ و سانسور صرف شد ولی همان‌طور که در مقدمه گفته شد، بدلیل پیشرفت سریع‌تر اینترنت از قانون‌گزاران‌اش، آن‌چنان که باید و شاید جواب‌گو نبوده است.

راه‌حل دیگری که در بسیاری از نقاط دنیا مورد استفاده قرار گرفت، برنامه‌ریزی برای تولید محتوی مؤثر و فرهنگ‌سازی است. از جمله در سوئد، درکنار عدم وجود سیاست‌های فیلترینگ، از مبلغین دینی برای انتشار آموزش‌های دینی اخلاقیات استفاده شد.

اصول اخلاقی سایبر.

مبحث اصول اخلاقی وقتی مطرح می‌شود که نتوان در سطح جامعه یا بین‌المللی برای انجام یا عدم انجام عملی قانون وضع کرد. از آن‌جا که قوانین سایبر با وجود مؤثر بودن‌شان در کند کردن روال جرایم رایانه‌ای در دنیا، ریشه‌کنی آن‌ها را به دنبال نداشت، شاید تنها راه‌حل قابل برنامه‌ریزی دست به دامان اخلاقیات شدن است. معیارگزاری اخلاقیات باید با این انگیزه باشد که افراد آن را بپذیرند. اصول اخلاقی در یک دسته‌بندی کلی به دو دسته تقسیم می‌شوند[۱۰]:

Comment[۱۲AD]: مباحث حقوقی و اخلاقی در فناوری اطلاعات، علی انگورچی/امامیان

۱. اخلاق فردی که مربوط به اعمال مردم در زندگی روزمره‌شان و در ارتباط با هم است.
۲. اخلاق تجاری که مربوط به برخوردها و رفتار مردم در دنیای تجارت و شغلی می‌باشد.

هر دو نوع این اصول در موارد سایبر قابل بحث هستند. در مورد اول، اخلاق فردی درهنگام ارتکاب به جرم رایانه‌ای می‌تواند مانعی برای تبهکار باشد و تصمیم او برای ورود به حریم محرمانگی سایرین را تغییر دهد. در مورد دوم هم، مدیران شرکت‌ها برای جلوگیری از امکان استفاده خرابکاران از منابع شرکت‌شان همچون محصولات نرم‌افزاری یا خدمات مخابراتی تحت وب، با صرف هزینه و رعایت حریم‌های امنیتی، بسترهای آماده برای نفوذ را از بین برده و یا غیرقابل دسترسی نمایند. البته گاهی اوقات بدلیل عدم رعایت موارد از طرف دیگری در معاملات تجاری این امکان وجود دارد که شرکت مورد نظر لطماتی ببیند. مثلاً شرکتی هزینه‌های ارایه خدماتش را با متدهای پرداخت الکترونیک از کاربر اخذ می‌کند و مبنای شناخت کاربران را هم بر اطلاعات بانک یا مؤسسه مالی مورد استفاده قرار می‌دهد. در مقابل بنگاه مالی علی‌رغم استانداردها، هیچ‌گونه شناختی از کسانی که به آن‌ها خدمات بانکی ارایه می‌کند، ندارد. در این حالت، درصورت وجود معضلات قانونی، شرکت طرف اول است که مضر خواهد شد.

پیشنهادات.

در این بخش چند مورد برای حل مشکلات مطرح شده آورده می‌شود. البته این‌ها تنها نظرات نویسنده است و امید او برای از میان برداشتن معضلات فضای سایبر به این موارد دوخته شده است.

- ✓ تشکیل اتحادیه جهانی اخلاق سایبر
- ✓ تدوین قانون یکپارچه تجارت الکترونیک
- ✓ تشکیل اتحادیه جهانی امضای الکترونیک برای شناخت هویت‌ها
- ✓ استانداردسازی دروازه‌های انتقال مالی
- ✓ ایجاد دادگاه بین‌المللی رسیدگی به پرونده‌های جرایم رایانه‌ای
- ✓ توجه به مسایل دینی اخلاق و سرمایه‌گزاری جهانی برای تولید محتوی مؤثر مقابله با جرایم رایانه‌ای
- ✓ سیاست‌گزاری صحیح در زمینه آموزش استفاده از منابع داده‌ای جهانی

مؤخره.

با عنایت به موارد ذکر شده در این مقاله، بار دیگر یادآور می‌شویم که گزارشات این مقاله تنها برای آشنایی بیشتر با آموزه‌های مرتبط با اخلاقیات سایبر است که شاید تنها سلاح در برابر حرایم سایبر و البته با کمک قوانین حاکم بر این فضای مجازی باشد. به امید روزی که ایران در زمینه جرایم سایبر در زمره آخرین کشورهای جهان باشد، البته با ایجاد امکان استفاده از تمام زیرساخت‌های فناوری اطلاعات و ارتباطات براری شهروندان سایبر.

منابع.

Ethics and the Internet: The Cyberspace Behavior of People, Communities and Organizations, Roger Clarke, Principal, Xamax Consultancy Pty Ltd, Canberra, Sixth Annual Conference of the Australian Association for Professional and Applied Ethics, Old Parliament House, Canberra, 2 October 1999,Revised version published in Bus. & Professional Ethics J. 18, 3&4 (1999) 153-167.

Ethics and Privacy of Communications in the E-Polis, Gordana Dodig-Crnkovic and Virginia Horniak, Department of Computer Science and Electronics, Mälardalen University, Västerås, Sweden.

FALL 2005 SUPPLEMENT TO CYBERLAW PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE, Second Edition, By Patricia L. Bellia; Lilly Endowment Associate Professor of Law; Notre Dame Law School, Paul Schiff Berman; Professor of Law University of Connecticut School of Law, David G. Post; Professor of Law; Beasley School of Law, Temple University LAST UPDATED AUGUST 15, 2005.

Technology and Privacy: The New Landscape. MIT Press, Agre PE & Rotenberg M. edition (1997).

مباحث حقوقی و اخلاقی در فناوری اطلاعات، علی انگورچی، امامیان

فلسفه اخلاق با تکیه بر مباحث تربیتی، دفتر نشر معارف، نهاد نمایندگی رهبری در دانشگاه‌ها، چاپ اول، تابستان ۱۳۸۵

http://www.wikipedia.org

http://www.napster.com

http://www.riaa.com

http://www.copyright.gov

http://www.lawblog.ir

http://www.hoquq.com

درباره نویسنده.

آرمان دیدنده، دانشجوی رشته علوم‌کامپیوتر مقطع کارشناسی در دانشگاه صنعتی امیرکبیر(پلی‌تکنیک) تهران، رئیس هیأت مدیره شرکت فناوری اطلاعات و ارتباطات مهان و کارشناس مسایل فناوری اطلاعات و ارتباطات در این شرکت