

# مباحث حقوقی و اخلاقی فناوری اطلاعات

امین چاروسه

[Charoosheh@ce.aut.ac.ir](mailto:Charoosheh@ce.aut.ac.ir)

## 1. مقدمه

همچنان که کامپیوتر و اینترنت دارای مزایا و منافع هستند در مقابل افعال ناشایستی را نیز می‌توان از طریق کامپیوتر انجام داد که شاید تا قبل از بروز این پدیده تصور آن محال بود. در گذشته تنوع جرایم بسیار کم بود و پیچیدگی چندان هم نداشت اما با ورود تکنولوژی کامپیوتر و به تبع اینترنت به عرصه جامعه چنان تحولی در ارتکاب جرایم رخ داده که متصدیان امر را با سردرگمی عجیبی روبه‌رو ساخت و با این که قریب به دو دهه از رسیدگی و اظهارنظر درباره آن می‌گذرد، حتی در کشورهایی که از یک نظام قضایی قوی و قانونگذاری منسجم برخوردارند، تصحیح یا تغییر قوانین در این زمینه ادامه دارد. پیشرفت سریع و نو شدن هر روز و عنان و اختیار را از کف تدوین‌کنندگان قانون، دادگاه‌ها و مجریان قانون ربوده است و به آنها مجال تطبیق و همسان‌سازی نیروها و سیستم‌هایشان را با این پدیده نمی‌دهد. از این رو توجه به مباحث اخلاقی و حقوقی در فناوری اطلاعات از اهمیت بسیاری برخوردار است.

## 2. اصول اخلاقی

معیار های اخلاقی<sup>۱</sup> هستند که انتظار می‌رود مردم از آن‌ها پیروی کنند. بحث اصول اخلاقی هنگامی مطرح می‌شود که نتوان در مورد انجام (یا خودداری از انجام) عملی در جامعه یا در سطح بین‌المللی قانونی وضع کرد. در آن صورت، برای توصیه و تأکید به انجام آن عمل، آن را به صورت یک اصل اخلاقی مطرح می‌کنند و از مردم انتظار انجام آن را دارند. در یک تقسیم‌بندی اصول اخلاقی را به دو دسته تقسیم می‌کنند:

- اخلاق فردی<sup>۲</sup> که مربوط به اعمال مردم در زندگی روزمره شان و در ارتباط با هم می‌شود.
  - اخلاق تجاری<sup>۳</sup> که مربوط به برخورد ها و رفتار مردم در دنیای تجارت و شغلی می‌باشد، مثل طرز برخورد با همکاران، مشتریان، و به طور کلی هر فردی که به نحوی در ارتباط تجاری با شخص دیگری است.
- یک تفاوت عمده بین برخورد قانونی<sup>۴</sup> و برخورد اخلاقی<sup>۵</sup> وجود دارد و آن‌هم این است که برخورد ها و رفتارهای قانونی لازم و ضروری و اجرا و اطاعت از آن‌ها واجب است، اما رفتارهای اخلاقی واجب‌الاجرا نیستند و بیشتر به صورت مواردی هستند که انتظار می‌رود همه آن‌ها را انجام دهند.

## 3. محرمانگی

محرمانگی<sup>۶</sup> اطلاعات به معنی مصون ماندن اطلاعات شخصی افراد از سوء استفاده می‌باشد. رفاه و تسهیلات زایدالوصفی که اینترنت به ارمغان آورده، در همه شئون زندگی از جمله امور بانکی و خریداری کتاب به قیمت قربانی شدن حریم خصوصی کاربران اینترنتی است به ویژه در شرایطی که هنگام سفارش دادن و یا حتی فقط بازدید از یک پایگاه اینترنتی، اطلاعاتی هرچند پیش پا افتاده و

<sup>1</sup> Ethics

<sup>2</sup> Personal ethics

<sup>3</sup> Business ethics

<sup>4</sup> Legal behavior

<sup>5</sup> Ethical behavior

<sup>6</sup> Privacy

بی اهمیت در اختیار قرار داده می شود. اگرچه در دنیای امروز نمی توان از لو دادن اطلاعات شخصی به طور کامل اجتناب کرد اما امکان به حداقل رساندن آن وجود دارد. ابزارها و فنون حفظ حریم خصوصی در اینترنت گسترش چشمگیری پیدا کرده است و دامنه ای وسیع را در بر می گیرد و برای این کار راه های گوناگونی وجود دارد از پنهان سازی هویت کامپیوترتان در فضای اینترنت گرفته تا استفاده از نرم افزارهای کنترل کننده کوکی ها<sup>1</sup> تا بهره گرفتن از خدمات فراهم کنندگان سرویس های اینترنتی به عنوان مثال مخفی کردن مبدأ فرستنده نامه الکترونیکی.

اکثر سازمان ها سیاست هایی در زمینه حفظ حریم خصوصی افراد دنبال می کنند و در اختیار گذاشتن اطلاعات کاربران را منوط به حکم دادگستری یا دلایل امنیت ملی کرده اند.

#### 4. مالکیت فکری و معنوی

مالکیت معنوی به خلاقیت های فکری و ذهنی انسان، شامل ابداعات، آثار ادبی و هنری و نمایه های اسامی و تصاویر مورد استفاده در تجارت اشاره دارد. مالکیت فکری به دو گروه تقسیم می شود:

مالکیت صنعتی شامل ابداعات و اختراعات طرح های صنعتی، مدارهای مجتمع، علائم تجاری و علائم جغرافیایی است.

حق نسخه برداری شامل آثار ادبی، رمان ها، اشعار، نمایشنامه ها، فیلم ها و آثار موسیقی و کارهای هنری از قبیل طراحی ها و نقاشی ها، عکس ها و تندیس ها و طراحی های معماری است.

حقوق مالکیت فکری مانند سایر حقوق مالکیت ها هستند به طوری که به مخترع یا مالک حق ثبت، علامت تجاری یا حق نسخه برداری اجازه می دهند از اثر یا سرمایه گذاری خود بهره برداری کنند و منفعت ببرند. این حقوق در ماده 27 اعلامیه جهانی حقوق بشر تصریح شده است. در این اعلامیه حق بهره برداری از منافع مادی و معنوی حاصل از تالیف هرگونه اثر علمی، ادبی یا هنری در نظر گرفته شده است.

سازمان جهانی مالکیت فکری به عنوان بخشی از سازمان ملل متحد محلی است که در آن کشور های عضو می توانند در خصوص هماهنگی و وضع قوانین و مقررات و رویه های حمایت از حقوق مالکیت فکری به بحث و تبادل نظر بنشینند. در طول دهه اخیر همراه با جهانی شدن سریع تجارت، سازمان جهانی مالکیت فکری از طریق مذاکرات و عقد پیمان، ثبت و تقویت کمک های فنی و حقوقی و دادن آموزش به شکل های مختلف نقش مهمی را در این سیستم های جدید ایفا می کند. علاوه بر این سازمان مذکور سیستم های جهانی ثبت ابداعات، علائم تجاری و طرح های صنعتی را نیز ارائه می کند.

سازمان جهانی مالکیت فکری طرح جدید و گسترده ای به نام WIPO Digital Agenda شروع کرده است که ظرف چند سال آینده مشخص کننده و پاسخ گوی تاثیرات اینترنت و فناوری های دیجیتالی بر روی نظام مالکیت فکری خواهد بود. این سازمان متعهد است تا راه کارهایی تشویقی را برای بهره برداری و پخش ابداعات و دانش جدید ارائه نماید و نیز از منافع ابداع کنندگان این آثار حمایت کند.

#### 5. سرقت نرم افزار

واژه سرقت نرم افزار<sup>2</sup> به ساختن کپی غیر قانونی از نرم افزار را گویند. یکی از موضوعات اساسی مطرح در فناوری اطلاعات است که امروزه خیلی شایع است و ضربه عظیمی به موسسات نرم افزاری وارد می کند. گروه های نرم افزاری تخمین زده اند به ازای هر کپی قانونی از یک نرم افزار، 7 کپی غیر قانونی ساخته می شود.

جهت محافظت در برابر سرقت از سه روش استفاده می شود: حق نسخه برداری، قفل نرم افزاری و تکثیر در تیراژ معین.

حق نسخه برداری<sup>3</sup> به محافظت قانونی اصل نرم افزار در برابر استفاده غیر مجاز، شامل نسخه برداری دوباره اطلاق می شود. مجوز کپی رایت روی نرم افزار به صورت تذکر درج می شود که الگوی آن در بسیاری از کشور ها یکسان است. در پی همایش جهانی کپی رایت که بیشتر ملل آن را پذیرفته اند، اعلان کپی رایت شامل سه جزء است:

نماد © (در آمریکا کلمه سابق Copyright یا مختصر Copr. نیز استفاده می شود)

سال اولین انتشار کار

نام دارنده حق نسخه برداری

<sup>1</sup> cookies

<sup>2</sup> Software Piracy

<sup>3</sup> Copyright

کپی رایت سال ها است که در مورد کتاب ها ، مجلات ، موسیقی ، ... به کار می رود. همینطور در مورد سخت افزار کامپیوتر، بانک های اطلاعاتی RAM ، ROM ، ... به هر نرم افزار بدون کپی رایتی که همگان بتوانند از آن استفاده کنند، Public domain software می گویند.

**قفل نرم افزاری<sup>۱</sup>** یک طرح محافظت نرم افزار که تلاش برای کپی کردن برنامه را بیهوده می کند یا کپی ها را غیر قابل اطمینان می کند . در این طرح از نرم افزار یا سخت افزار یا هردوی آن ها کمک می گیرند .

تکثیر در تیراژ معین<sup>۲</sup> یک موافقت نامه است که طی آن خریدار نرم افزار مبلغی به سازنده می پردازد تا تعداد مشخصی کپی از یک برنامه درست کند .

به نرم افزاری است که آزادانه توزیع می شود در حالیکه صاحب آن مالکیت نرم افزار را حفظ می کند و از کاربران می خواهد با پرداخت مبلغ کمی برنامه را رجیستر کنند یا آنرا update کنند نیز Shareware software گفته می شود.

## 6. جرایم کامپیوتری

جرم کامپیوتری<sup>۳</sup> از نظر مفهومی هر استفاده غیر مجاز از یک سیستم را شامل می شود. ( که شامل دزدی نرم افزار هم هست ) برای توضیح بیشتر جرایم کامپیوتری مثالهایی را ذکر می کنیم که جزو معمول ترین و رایج ترین اصطلاحاتی هستند که در زمینه جرایم کامپیوتری قرار می گیرند. هدف از ذکر این مثال ها تحقیق و بررسی نحوه کار و یا جزییات آنها نیست بلکه پیدا کردن دید خوب و واضح نسبت به مفهوم جرم کامپیوتری است .

### ■ کلاهبرداری کامپیوتری

هر کس با برنامه سازی کذب، سوءاستفاده از داده های ناقص و کذب، استفاده غیرمجاز از داده ها، برنامه ها یا سیستم کامپیوتری، سوءاستفاده از ارتباطات راه دور، سوءاستفاده از در مرحله ورودی، پردازش و خروجی و امثال این موارد، وجوه، اموال یا امتیازات مالی را تحصیل کند و از این راه اموال دیگران را ببرد، کلاهبردار کامپیوتری محسوب می شود.

کلاهبرداری کامپیوتری بدو به صورت تقلب در مرحله برنامه نویسی و دادن دستورعملهای اضافی خلاصه می شد. این دستورعملها و برنامه های تقلبی یا مستقیم هدف مالی داشت یا دادن صورت واقع به یک امر کذب بود و همین موجب تسلیم و تسلیم ناروای مالی می شد. بعداً با پیشرفت برنامه نویسی و ارتقای نحوه دستیابی، کلاهبرداری کامپیوتری شکل جدیدی به خود گرفت. با بحث به روز شدن داده ها، دور جدیدی از نحوه ارتکاب و در نهایت مصادیق کلاهبرداری کامپیوتری آغاز شد. در کنار آن بسته های نرم افزاری، ویروسها، کرمها، بمبهای زمانی منطقی و ... موجب شد بتوان هم به سهولت به شماره های محرمانه اشخاص دست یافت و هم بتوان اموال آنان را ربود و به خود اختصاص داد.

### ■ جعل کامپیوتری

هر کس از طریق ورود، تغییر، محو، متوقف سازی داده ها یا اطلاعات دیجیتالی و ارتباطات راه دور هرگونه مداخله در امر داده پردازی و نظیر آن داده ها یا اطلاعات دارای ارزش مالی و قابل اثبات و استناد در مراجع قضایی را جعل کند، مرتکب جعل کامپیوتری شده است. جعل مرسوم و کلاسیک ناظر به جعل چیزی است که قابلیت استناد داشته باشد و بتوان آن را ارائه کرد و اثر حقوقی بر آن مترتب باشد. موضوع این جرم ساختن نوشته، سند، چیز دیگر بر خلاف حقیقت است و ساختن به شکل به وجود آوردن سند، ایجاد نوشته و سند، خراشیدن، تراشیدن، محو، اثبات و ... دیگر مصادیق جرم صورت می گیرد.

با توجه به تحول کاربرد سند و شکل آن و گسترش تدریجی کاربرد اسناد الکترونیکی و تفاوت این اسناد با اسناد کاغذی از حیث فیزیکی و تشابه از حیث اصول اثباتی و استنادی، با توجه به تحول مصادیق جعل در محیط دیجیتالی از شکل مادر و عمده مذکور در ماده قانونی پیشنهادی و ظهور مصادیق جدید در کارت اعتباری، بانکداری الکترونیکی، پرداخت الکترونیکی و تجارت الکترونیک،

### ■ جاسوسی کامپیوتری

هر کس اطلاعات و داده های نظامی ، سیاسی و ملی موجود در سیستمهای کامپیوتری و مخابراتی، پایگاههای داده و غیره را با سوءاستفاده از ابزارهای فنی یا به واسطه شغل و موقعیت خود کسب و به افراد یا ارگانهای خارجی و غیرمجاز افشا کند جاسوس محسوب می شود.

<sup>1</sup> Copy Protection

<sup>2</sup> Site licensing

<sup>3</sup> Computer Crime

علاوه بر این هر کس با استفاده غیرمجاز، سوءاستفاده یا مداخله در سیستمهای کامپیوتری یا مخابراتی اسرار صنعتی، تجاری، اقتصادی و مالی و نیز اسرار شغلی دیگران را کسب و به اشخاص یا ارگانهای غیرمجاز افشا کند، یا در اختیار شخص، سازمان، نهاد، مؤسسات و ... غیرمجاز و بیگانه نسبت به این اسرار و اطلاعات بگذارد، نیز جاسوس محسوب می شود.

#### ▪ سابوتاژ کامپیوتری

هرگونه ورود، تغییر، محو، متوقف سازی و مداخله در خطوط ارتباطی، دادهها یا اطلاعات، برنامهها و سیستمهای کامپیوتری و مخابراتی سازمانها، ارگانهای حکومتی و وزارتخانهها به قصد مبارزه با حکومت جمهوری اسلامی ایران که موجب اختلال در عملکرد سیستمهای مزبور شود جرم سابوتاژ کامپیوتری محسوب می شود.

در سابوتاژ کامپیوتری ورود، تغییر محو، متوقفسازی و مداخله در دادهها و اطلاعات و سیستم کامپیوتری و مخابراتی ارگانهای دولتی صورت می گیرد تا با اختلال در روند کار آن ارگان نوعاً اختلال در نظام سیاسی پیش آید.

#### ▪ تخریب کامپیوتری

هرگونه تغییر، محو، متوقف سازی، مداخله و اختلال در دادهها و اطلاعات، برنامهها و سیستمهای کامپیوتری و مخابراتی، به قصد ایجاد ضرر مالی برای دیگری تخریب کامپیوتری محسوب می شود.

مرتکب تخریب کامپیوتری هیچ فعل فیزیکی در عالم واقع انجام نمی دهد بلکه در محیط دیجیتال با ورود، محو، تغییر، اثبات و ... دادهها یا اطلاعات به دیگری ضرر می رساند. دادههایی که برای دیگران ارزشمند محسوب و بروز مسائل یادشده در آنها موجب ضرر مالی می شود.

وجه تمایز تخریب و سابوتاژ اولاً در نیت مرتکب (سابوتاژ مبارزه با نظام سیاسی / تخریب = نابودی اموال دیگری و ایجاد ضرر مالی) و ثانیاً در موضوع جرم (سابوتاژ = ارگانها، نهادها و وزارتخانههای دولتی / تخریب دادههای شخص دیگر) می باشد.

#### ▪ دستیابی غیرمجاز

هرکس عمداً و بهطور غیرمجاز به دادهها، اطلاعات، برنامهها و سیستمهای کامپیوتری و مخابراتی بایا بدون نقض تدابیر ایمنی و حفاظتی دستیابی پیدا کند، مرتکب دستیابی غیرمجاز شده است. این جرم، جرم صرف دستیابی است و با مفاهیم مجرمانه دیگر یعنی نفوذیابندگی، شنود، افشاء (از جرایم ناقض حمایت از دادهها) و ... تفاوت دارد.

#### ▪ شنود غیرقانونی

شنود بدون حق و غیرمجاز ارتباطات خصوصی، ارتباطات دادهای، مخابراتی و کامپیوتری، پیامهای الکترونیکی، محتوای پیامها و دادههای موجود در برنامهها و سیستمهای کامپیوتری و مخابراتی دیگران، از طریق ابزارهای تکنیکی، شنود غیرقانونی محسوب می شود.