

# تأثیر اجتماعی تکنولوژیهای ارتباطی و اطلاعاتی

نویسنده: ویلیام جی. مارتین  
مترجم: نیلوفر نامدار قشقایی

برای یک سازمان بسیار ارزشمندتر از خود سخت‌افزار کامپیوتری است. از کارهای عملیاتی روزبه‌روز گرفته تا منابع سود رقابتی، باید در مقابل از بین رفتن، آسیب دیدن، بهره‌برداری ناصحیح یا دسترسی غیرمجاز حفاظت شوند. تمام سیستمهای کامپیوتری در مقابل از دست رفتن تصادفی داده‌ها در جریان حوادث طبیعی مانند: آتش‌سوزی، سیل، اشتباهات نرم‌افزاری و سخت‌افزاری، قطع ارتباطات راه‌دور، قطع یا نوسانات برق، آسیب‌پذیرند. در واقع، براساس یک گزارش، ۶۰ تا ۷۰ درصد سوانح ناگوار ناشی از قطع برق بوده است و تعداد زیادی از سازمانها به سیستمهای برق غیرقابل قطع و مولدهای برق با سوخت فسیلی پشتیبان مجهز شده‌اند، تا اطلاعاتشان را حفظ کنند.<sup>۱</sup> بدیهی است که هرچه تکنولوژیهای اطلاعاتی و ارتباطی

یکی از دل‌مشغولیهای اساسی در مطالعه جوامع اطلاعاتی، ایجاد مسائل ناشی از تأثیر و پیامدهای اجتماعی تکنولوژیهای ارتباطی و اطلاعاتی است. این امر در نهایت خود می‌تواند بر تمام جوانب زندگی تأثیر گذارد، که مطالعه آن ممکن است به آسانی به ابعادی جامع و دایره‌المعارفی برسد. در اینجا، فقط به ارزیابی این تأثیر در حوزه‌های مهمی چون امنیت و حفاظت داده‌ها، جرائم کامپیوتری، امور خصوصی، دارایی‌های هوشمند، سانسور و آزادی بیان، مشاغل وابسته به کامپیوتر و شبکه‌ای شدن جامعه خواهیم پرداخت.

## امنیت اطلاعات

اطلاعات ذخیره شده در سیستمهای کامپیوتری در اکثر موارد



به نحو فزاینده‌ای شالوده جامعه قرار می‌گیرند، خود جامعه نسبت به این پدیده‌ها (سوانح) آسیب‌پذیرتر می‌شود. متأسفانه، یکی از تهدیدهای جدی‌تر برای امنیت سیستم‌های اطلاعاتی و ارتباطی ناشی از خلاف‌کارهای روبه‌رشدی است که دستیابی به سودهای بادآورده در جامعه‌ای اطلاعات بسیار گسترده است.<sup>۲</sup>

### تکنیک‌های ارتکاب جرم

متداولترین روش ارتکاب جرم کامپیوتری عملی به نام سرقت اطلاعات (یا مزاحمت کامپیوتری) است، که اساساً مستلزم استفاده از سیستم تلفن برای دسترسی غیرمجاز به سیستم‌های کامپیوتری یا داده‌های آنهاست. سرقت اطلاعات، بنابر تعریف، عبارت است از جستجو برای پیدا کردن رمزهای دستیابی؛ این جستجو می‌تواند به صورت تصادفی یا با استفاده از تکنیک‌های پیشرفته برای فرار از ردیابی صورت گیرد. سرقت اطلاعات دستی<sup>۳</sup>، عبارت است از استفاده از تلفن و تکنیکی که در آن

### جرایم کامپیوتری

جرم کامپیوتری عبارت است از عملی مجرمانه که هدف آن کامپیوتر و اطلاعات ذخیره شده در آن باشد یا انجام جرم به کمک کامپیوتر باشد. این عمل شامل استفاده غیرمجاز، یا دسترسی غیرمجاز، به سیستم‌های اطلاعاتی یا تغییر دادن برنامه‌ها به منظور دستیابی به منابع مالی یا به نیتی مغرضانه است. شایعترین شکل جرم کامپیوتری سرقت است. سرقت کامپیوتری می‌تواند شامل سرقت پول، مثل انتقال غیرقانونی پول

شماره بعد از شماره امتحان می شود تا به یک رمز دسترسی ارزشمند برسند.

سرقت اطلاعات کامپیوتری، یعنی استفاده از کامپیوترهای برنامه ریزی شده برای گرفتن شماره های هدف، و جستجو برای کدهای دستیابی از طریق پلکانی، تصادفی یا لگاریتمی<sup>۳</sup>. در سال ۱۹۸۶ در استرالیا، در پاسخ به تهدید فزاینده سرقت اطلاعات، در کمپانیهای بزرگ، دولت ایالتی گروه ویژه ای از دایره آگاهی پلیس و یکتوریا (BCI) تشکیل داد. این تحقیق تحت عنوان «عملیات مانا»<sup>۴</sup> نشان داد که میزان فعالیت های مجرمانه سرقت اطلاعات بسیار بالاتر از آن چیزی است که تصور می شد. در واقع، این مشکل از بیم کاهش اعتماد مردم، عملاً توسط بانکها و مؤسسات مشابه دیگر، کوچک جلوه داده شده بود.<sup>۵</sup>

یکی از صورتهای دیگر مربوط به جرم الکترونیکی از این دسته، که شامل سرقت اطلاعات هم می شود، ورود غیرمجاز به PBX و سیستمهای پست صوتی است. در این حالت، فرد سارق اطلاعات سیستم را در جهت ختشی کردن اقدامات امنیتی آن دستکاری می کند تا رمزهای دستیابی، کلمات عبور، و شماره های تلفن را برای فروش به بهترین خریدار، به دست آورد. در بریتانیا، شرکت تلفن BT<sup>(۶)</sup> «آژانس کارآگاهی» داخلی مخصوص به خود را دارد که هدفش یافتن و تحت پیگرد قرار دادن افرادی است که از شبکه تلفن سوء استفاده قرار

می کنند. تعداد زیادی از سیستمهای PBX مدرن چنان طراحی شده اند که نمایندگان فروش می توانند با گرفتن یک شماره تلفن چهار رقمی به مرکز تلفن شرکت وصل شوند، و از این طریق به برقراری ارتباط تلفنی برای مقاصد شغلیشان اقدام کنند. سارقان اطلاعات با سوء استفاده از این عمل و ابداع برنامه های کامپیوتری، با به دام انداختن شماره های ۰۸۰۰ (رایگان) برای یافتن رمزهای چهاررقمی، قادرند ارتباط تلفنی رایگان برقرار کنند. سارقان اطلاعات نه تنها از این طریق می توانند با هر جای دنیا که بخواهند تماس تلفنی برقرار کنند، بلکه چون از مرکز تلفن یک شرکت، و نه تلفن شخصی خودشان، استفاده می کنند، عملاً غیرقابل ردیابی اند. حتی در صورتی که سارق اطلاعات دستگیر شود، اثبات جرم آنها دشوار است، زیرا اگر یک سارق اطلاعات با یک شماره ۰۸۰۰ در لندن با نیویورک و از آن طریق با هلند ارتباط تلفنی برقرار کند، کدامیک از شرکتهای تلفن در کدام یک از این سه کشور عملاً مورد سوء استفاده قرار گرفته است؟ در واقع، فقط شماره ۰۸۰۰ ثبت شده است و بنابراین بدون یک صورت حساب تفکیک شده به عنوان شاهد، اصلاً چه جرمی را می توان ثابت کرد<sup>۷</sup>؟

افرادی که در چنین عملیاتی درگیرند، یعنی سارقان اطلاعات، از دانشجویان باهوش و زیرک تا افرادی با نیت های ویرانگر را در برمی گیرند و انگیزه آنان می تواند کنجکاوی، بلندپروازی، حرص پول یا حس انتقام نسبت به مالک سیستم باشد. اما، در مورد جرم کامپیوتری، مجرمان انواع وسیله های ورود غیرقانونی، گاهی از پایگاهی از مکانی دوردست، را ابداع کرده اند.

از میان روشهای به کار گرفته شده برای تجاوز به سیستمهای از راه دور، می توان بارزتر از همه ویروسها، کرمها، و اسپهای تروا را برشمرد.

### ویروسها

ویروسهای کامپیوتری عبارتند از برنامه هایی که برنامه های دیگر را تغییر می دهند به نحو نامحدودی تکثیر می شوند. برنامه های دیگر را آلوده کرده و تحت تأثیر قرار می دهند. این ویروس، با شباهت بسیار زیادش با آنچه که در ویروسهای زیستی پیش می آید، از طریق برنامه آلوده به سیستم کامپیوتر حمله می کند،

## یکی از تهدیدهای جدی برای

## امنیت سیستمهای اطلاعاتی و

## ارتباطی ناشی از خلاف کاریهای

## رو به رشدی است که هدف آنها

## دستیابی به سودهای باد آورده در

## جامعه ای است که اطلاعات در

## آن بسیار گسترده است.

آنگاه با واداشتن ساختن برنامه میزبان به گنجاندن قطعه‌هایی ریز (با رمز) برنامه‌های دیگر، تکثیر پیدا می‌کند. برنامه‌های آلوده به انتشار ویروس ادامه می‌دهند تا جایی که آلودگی به نحو مؤثری گسترش پیدا می‌کند، ویروسها فعال می‌شوند و تمام نرم‌افزارهای روی سیستم را نابود می‌کنند.

### کرم‌ها

کرم برنامه‌ای است که خود را تکثیر و از یک کامپیوتر به کامپیوتر دیگر انتشار پیدا می‌کند. کرم برنامه‌ای متکی به خود است که به‌طور مخفیانه از یک پایگاه کامپیوتری به پایگاه کامپیوتری دیگری منتقل می‌شود. به محض اینکه کرم به داخل کامپیوتر هدف وارد شد، می‌تواند اطلاعات را به دنیای خارج نشر دهد، سیستم را نابود کند یا صرفاً به یک عنصر مزاحم تبدیل شود و سرعت کامپیوتر را تا حد حرکت حلزونی پایین بیاورد. کرم پیشرفته‌ترین نوع تکنیک حمله به سیستم است؛ احتمال آشکارسازی آن بسیار اندک و در اثر نشت اطلاعات حساس، فوق‌العاده کارساز است.

### اسب‌های تروا

اسب تروا مجموعه‌ای از رویه‌های برنامه‌ای است که گاهی عملیات غیرمجاز اجرا می‌کنند اما معمولاً به برنامه‌ها اجازه می‌دهند که کار اصلی خود را انجام دهند. مثلاً، اگر کسی بخواهد یک پایگاه داده‌ها را نابود کند، ممکن است برای صاحب آن فایلی ارسال کند که وقتی اجرا شود، زیرکانه و به آرامی پایگاه داده‌ها را نابود کند

دو روش شناخته شده برای حمله به کامپیوترها در پایگاهها، عبارتند از تکنیکهای کالباسی و بمبهای منطقی در تکنیکهای کالباسی، معمولاً کارمند بانکی برنامه‌ای می‌نویسد که اعداد را در تمام حسابها تا نزدیکترین صدم آنها گرد می‌کند، و باقیمانده آن را به حساب شخصی خودش منتقل می‌کند. نهایتاً این برشها روی هم جمع می‌شوند و کالباس بزرگی تشکیل می‌دهند. خلاف انجام شده نیز تا زمانی که فرد مجرم تصمیم به متوقف کردن آن نگیرد، نامکشوف باقی می‌ماند.

بمب منطقی عبارت است از برنامه‌ای که توسط کارمندی نوشته و طوری طراحی می‌شود که عملیات مخرب یا خلافی

هر چند که تعدی به یک پایگاه داده‌ها، ضرورتاً در چارچوب تعریف قانون عرفی سرقت قرار نمی‌گیرد، ولی معنی آن محروم کردن مالکان یا کاربران مجاز از به کارگیری آن، و دزدی، و استفاده غیر مجاز غیر قابل قبول است.

انجام دهد. برنامه‌ریز ممکن است برنامه‌ای به سیستم وارد کند به‌طور مرتب و ارسی کند آیا اسم فرد برنامه‌ریز در فهرست حقوقی الکترونیکی هست یا خیر، اگر اسم فرد مورد نظر در این فهرست نباشد، برنامه مورد نظر اطلاعات حیاتی و مهم را نابود خواهد کرد و به این ترتیب اگر این کارمند اخراج شود، سیستم کامپیوتری کمپانی در عملیات انتقامی چنین اقدامی، نابود خواهد شد.

حدود دو سال پیش، تهدیدهای متوجه امنیت کامپیوتری به هفت «E» طبقه‌بندی شد که عبارتند از: اشتباه (Error)؛ اختلاس (Embezzlement)؛ بلسندپروازی (Ego)؛ استراق سمع (Eavesdropping)؛ جاسوسی (Espionage)؛ دشمنی (Emnity) و اخاذی (Extortion).

تخمین زده شده است که در امریکا دست کم دو میلیارد دلار به صورت مخارج مستقیم سالانه ناشی از جرائم کامپیوتری از دست می‌رود، و این مبلغ حتی می‌تواند فقط قله پیدای یک کوه یخ باشد!

### بالا بردن امنیت کامپیوتری

امنیت کامپیوتری طیف وسیعی از مسئولیتها، از ایجاد مانع برای دسترسهای غیرمجاز تا ایجاد امکانات کامپیوتری برای حفاظت شبکه‌ها و داده‌هایشان، را دربرمی‌گیرد. این کار مداوم است و

تضمینی برای رسیدن به موفقیت کامل نیز در آن وجود ندارد. در این مسیر، گروهی از روشهای امنیتی برای حفاظت داده‌ها و تجهیزات ارائه شده‌اند عبارتند از:

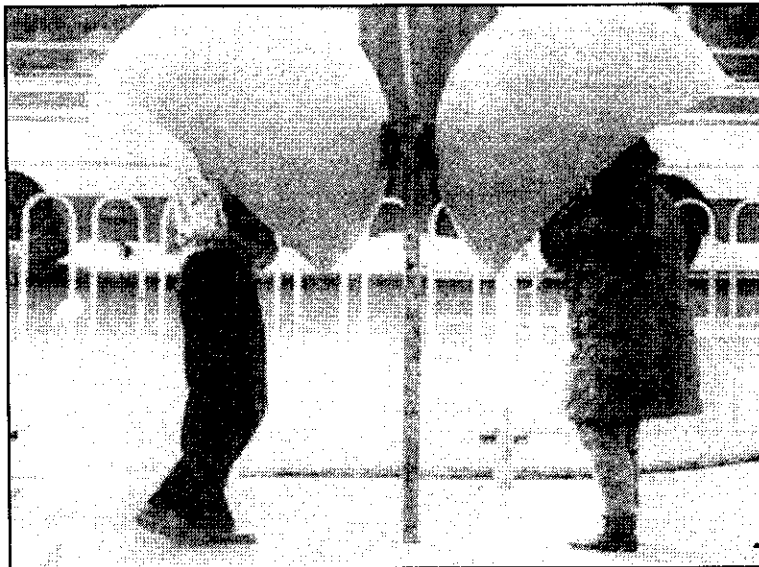
**کنترل‌های دستیابی فیزیکی:** جایی که دسترسی فقط به کاربران مجاز محدود می‌شود. این کار به کمک سنجاق سینه‌های امنیتی، کارت‌خوانهای مغناطیسی، و روشهای شناسایی بیولوژیکی صورت می‌گیرد.

**کنترل‌های رویه‌ای:** شامل استفاده از نگهبانان امنیتی و برکه‌های امضاء هنگام ورود و خروج.

**کنترل‌های تکنیکی:** شامل استفاده از کلمات عبور (کلمات رمز)، وسیله‌های قفل کردن و تلویزیونهای مدار بسته.

با استفاده از ترفند ساده و مناسب کنترل به وسیله کلمات عبور، می‌توان امنیت کامپیوتری را به‌نحو چشمگیری بهبود بخشید. امروزه نرم‌افزارهای کنترل دسترسی مخصوصی یافت می‌شود که کارسرها و میزان مجاز بودن آنها به دسترسی را تشخیص داده و آنها را به انجام مأموریت مجازشان محدود می‌کنند. متأسفانه، چنین نرم‌افزارهایی سازمانها را در مقابل سوء استفاده‌های کارمندان در زمان انجام وظایفشان ایمن نمی‌سازد.

اقدامات درجا برای جلوگیری از سوء استفاده از سیستمها توسط تلفن‌کنندگان از خارج، شامل سیستم برگردان تلفن<sup>۷</sup> که ارتباط تمام استفاده‌کنندگان خارج را قطع کرده و پس از شناسایی کلمه رمز عبور آنها مجدداً با آنها تماس برقرار می‌کند، و کارتهای هوشمند شبیه به آنهايي که در ماشینهای عابربانک به‌کار می‌روند، با تراشه‌ای در داخل پایانه برنامه داده شده راه دور، تشخیص می‌دهد که آیا فرد تماس‌گیرنده کاربر مجازی است یا خیر. همچنین، ابزارهایی برای تکنیک درهم‌سازی به‌منظور رمزی کردن اطلاعات و وسیله‌های رمزی‌سازی به کار گرفته می‌شوند؛ از جمله اینها می‌توان پردازنده‌های سیگنالهای دیجیتال را نام برد که سیگنالهای ارتباط از راه دور یا کامپیوتری را طوری ترجمه می‌کنند که برای کاربران غیرمجاز بی‌معنی باشند. این سیستمها گرانند و حتی بهترین رمزهای رمزسازی هم در برابر شکسته شدن آسیب‌پذیرند و بنابراین به‌طور مکرر عوض می‌شوند<sup>۸</sup>. نیز، می‌توان برنامه‌هایی نرم‌افزاری به کار گرفت که اپراتورها و زمان دستیابی آنها به سیستم را مشخص و ثبت کنند. این بسته‌ها می‌توانند دفعات غیرعادی مداخله‌های تصحیح را نیز مشخص کنند که اغلب می‌تواند به مشخص شدن تلاشهای آزمون و خطای مجرمان کامپیوتری منجر شوند<sup>۹</sup>.



آنها نهفته است.

## تمهیدات قانونی در مقابل رفتارهای خلاف

در نوامبر سال ۱۹۹۱، یکی از دانشجویان تحصیلات تکمیلی دانشگاه کرنل به نام ناپن مورس، یک برنامه کرم را به داخل اینترنت فرستاد. این بزرگترین حمله به امنیت کامپیوتری تا آن زمان بود و باعث از کارافتادن هزاران کامپیوتر در دانشگاهها، آزمایشگاههای دولتی و مشتریان در سرتاسر دنیا شد.

سرانجام مورس دستگیر و به ۱۰۰۰۰ دلار جریمه نقدی و ۴۰۰ ساعت انجام خدمات اجتماعی محکوم شد. با توجه به اهمیت تأثیر این حمله بر کامپیوترهای جهان، افراد زیادی عقیده دارند که این جریمه برای چنین جرمی بسیار ناچیز بوده است.

در واقع، با کمی توجه به میزان تعدی، آسیب و تقلب متضمن حمله به سیستمهای کامپیوتری، مشکل می توان فهمید که چرا گروه زیادی از مردم سعی دارند به نحوی این رفتار ذاتاً ضد اجتماعی را تبرئه کنند. هرچند که تعدی به یک پایگاه داده ها، ضرورتاً در چارچوب تعریف قانونی عرفی سرفت قرار نمی گیرد، ولی معنی آن محروم کردن مالکان یا کاربران مجاز از به کارگیری آن، و دزدی، و استفاده غیرمجاز غیرقابل قبول است. به علاوه، سعی بر توجیه چنین اقداماتی با یادکردن از آن در حکم جرم بدون قربانی، در صورتی که هدفهای اصلیش نه تک تک افراد بلکه گروههای عظیمی از مشتریانند، عملی غیرمسئولانه و خطرناک است. علاوه براین، در حالی که در گذشته یک سازمان مشکل می توانست ثابت کند جرمی اتفاق افتاده، زیرا ورود غیرقانونی به پایگاه داده ها علی الاصول تجاوزی فیزیکی تلقی نمی شد، امروزه قوانینی تدوین شده که دزدی الکترونیکی را شبیه به دزدی فیزیکی می دانند.

بر طبق قانونی در مورد مبارزه با سرقت اطلاعات در بریتانیا در سال ۱۹۹۱، ورود غیرمجاز، تخطی از قانون و ورود با امیال ناثواب و خلاف، تبهکاری و جنایت قلمداد شده است. در امریکا، ایالتهای متعددی قوانین ویژه ای را وضع و تصویب کرده اند که جرائم کامپیوتری مثل تزریق ویروس و برنامه های مزاحم دیگر به نرم افزار یا سیستمهای شبکه ای را نیز دربر می گیرند<sup>۱</sup>. در ایالت ویکتوریای استرالیا، قانون جرائم (کامپیوتری) مصوب سال ۱۹۸۸، در ازای ارتکاب اینگونه

پیشگام این تکنولوژی تعدادی تکنیک امنیت زیست سنجی است که عملاً فقط برای موارد مستلزم امنیت بالا و سازمانهای دفاعی به کار می روند و طوری طراحی شده اند که مشخصات فیزیکی انحصاری هر فرد را شناسایی کنند؛ در حال حاضر این سیستمها مشتمل اند بر:

● **انگشت نگاری الکترونیکی:** در جایی که پیشگراها آثار انگشت کاربران را، هر بار که دکمه ای را با شست خود فشار می دهند، می خوانند و آن را با فایل های دیجیتالی جمع آوری شده از اثر انگشت کاربران مجاز مقایسه کنند.

● **پویش شبکه چشم:** جایی که پیشگر الگوی عروق خونی پشت کره چشم افراد را می خوانند.

● **پویایی امضاء:** که نه بر روی ظاهر دست خط، که قابل تقلید است، بلکه بر روی تغییرات ظریف در حرکت و فشار امضاء، که قابل نسخه برداری نیستند، تأکید می کند. و دوباره نتیجه با موارد ثبت شده قبلی جمع آوری شده از امضاهای افراد مجاز مقایسه می شوند.

● **پویایی ضربه روی کلیدها:** که همان تکنیک بالا را در پویایی و حرکت نحوه استفاده از صفحه کلید اجرا می کند.

● **هندسه کف دست:** جایی که طول انگشتان، ضخامت کف دست و شکل کلی دست اندازه گیری و نتیجه به صورت دیجیتالی برای مصارف بعدی ذخیره می شود.

● **تشخیص صدا:** جایی که تکنولوژی چندان پیشرفته است که نه تنها قادر به تمایز صدای آدمی است، بلکه می تواند فیزیولوژی دقیق نحوه صحبت کردن را دنبال کند.

● **بازشناسی شبکه عصبی:** جایی که سوابق به شیوه ای بسیار پیشرفته بر پایه الگوی اعصاب صورت انسان گردآوری می شوند.

● **اثر انگشت DNA:** جایی که تصویر ژنتیکی اثر انگشت DNA نگهداری می شود، تا بعداً با پیشینه افرادی که می خواهند به امکانات دسترسی پیدا کنند، مقایسه شود<sup>۲</sup>.

● بدون در نظر گرفتن هزینه ها و منافع چنین اقداماتی در راه بالا بردن امنیت کامپیوتری، در تحلیل نهایی می توان گفت که این یک مشکل اجرایی است نه مشکل تکنیکی. افراد، منابع اصلی مشکلات مربوط به جرائم کامپیوتری و شناس نهایی به زانو در آوردن این مشکل، در کنترل و اداره صحیح و به جای

عمومی و خصوصی می‌پردازد و می‌تواند مکمل اقدامات و عملیات تکمیلی در راه امنیت سیستمهای اطلاعاتی باشد.<sup>۱۱</sup>

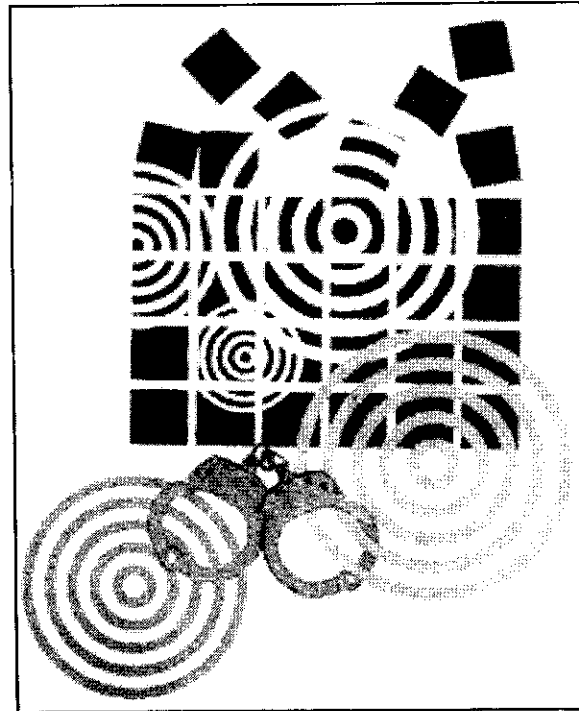
### امور خصوصی

توسعه سیستمهای کامپیوتری، مستقل از هزینه‌ای که دارند، مشکل تعادل بین نیاز به امنیت و اهمیت جلوگیری از آسیب به رکوردها را پیش می‌آورد و بنابراین، تجاوز به امور خصوصی داده‌ها از اهمیت برخوردار می‌شود. امور خصوصی (خصوصی بودن اطلاعات یا داده‌ها) اصطلاح جامعی است که استفاده و گاهی حتی استثمار اطلاعات در مورد افراد برای منظورهایی مختلف را در برمی‌گیرد. این فرضیه به استفاده از اطلاعات ربط دارد، اگرچه خود این معنا گاهی با محرمانه بودن یا حتی رازداری مترادف به‌کار می‌رود.<sup>۱۱</sup> در آینده نزدیک، امور خصوصی باید به مفهوم وسیعتر شبکه‌ای اطلاق شود. مثلاً «کاربر» اطلاعات شخصی یا سیستم، نه تنها باید به عنوان شخص بلکه حرکت پردازش در شبکه از جانب یک انسان کاربر یا از جانب سیستم یا سازمان دیگر، معنی پیدا کند.<sup>۱۲</sup>

به تدریج که شبکه‌های کامپیوتری بیشتری به هم وصل می‌شوند، اطلاعات ناشی از تغییرات درباره تک تک شهروندان می‌تواند با داده‌های سرشماری، کدهای پستی و سایر اطلاعات همگانی قابل دسترسی تطبیق داده شوند. مردم از بابت ماهیت و میزان جمع‌آوری چنین داده‌هایی نگران می‌شوند و هنوز هم داده‌های دیجیتالی تقریباً به کلی تنظیم نشده‌اند، چراکه در داخل هیچ چهارچوب قانونی‌ای که در گذشته وجود داشته نمی‌گنجند. اساساً قوانین وضع شده فقط به‌طور مشخص برای پست، روزنامه، تلویزیون کابلی و برنامه‌های رادیویی وجود داشته است. سیگنالهای جاری در یک محیط دیجیتالی بین صدا و ویدیو و داده فرقی قائل نمی‌شوند.<sup>۱۳</sup>

اطلاعات شخصی فراوانی که در سیستمهای اطلاعاتی مدرن نگهداری می‌شوند، احتمال استفاده ناصحیح از این اطلاعات را بسیار بالا می‌برد. تهدید نسبت به خصوصی بودن اطلاعات می‌تواند در نتیجه شرایط ناخواسته ناشی از تصمیمات دولت یا مجریان امر یا در نتیجه مستقیم معاملات بازرگانی، بالا گیرد.

مثلاً در ایالات متحده درباره گسترش بهره‌گیری از شماره‌های مربوط به امنیت ملی افراد از سوی مراجع مسئول



جرائم، ۸۴۰۰۰ دلار جریمه یا ده سال زندان جریمه قائل شده است.<sup>۱۴</sup>

در راه غلبه بر معضل امنیت اطلاعاتی در سطح بین‌المللی، سازمان همکاری و توسعه اقتصادی (OECD) در نوامبر ۱۹۹۲ خط‌مشی ویژه‌ای در راه تأمین امنیت سیستمهای اطلاعاتی ارائه داد و با توجه به افزایش اهمیت سیستمهای اطلاعاتی در تمام جوانب زندگی ملی و بین‌المللی،<sup>(۸)</sup> توجه همگان را به میزان آسیب‌پذیری اطلاعات الکترونیکی نسبت به دستیابی، بهره‌گیری، سوءاستفاده، تغییر و تخریب غیرمجاز جلب کرد. این خط‌مشی به تمام انواع سیستمهای اطلاعاتی در هر دو بخش

مالیاتی، مراجع مربوط به گواهینامه رانندگی و مؤسسات رفاه برای پی گیری شیوه پرداخت حقوق والدین، نگرانیهایی ابراز شده است. همیشه این احتمال وجود دارد که این اطلاعات برای سوءاستفاده مناسب‌اند. اگر قرار باشد اطلاعات شخصی برای مقاصد مناسب استفاده شوند، و تعادل مناسبی بین نگهدارنده‌های این رکوردها و مباحث داده‌ها و بین سازمانها و افراد برقرار باشد، پس، ضرورتاً حفاظت‌های اداری و قانونی باید بایه‌گذاری شوند. اگر، مثلاً، قرار است فایل‌های شماره‌های مالیاتی برای کمک به فعالیتهای دیگر، مثلاً برای شناسایی متخلفان در سازمان رفاه مورد استفاده قرار گیرد، پس باید سیستم قنادر باشد که نه تنها اشتباهات را شناسایی و تصحیح کند، بلکه بتواند به اصلاح کامل موضوعات داده‌ای صدمه دیده از طریق بهره‌گیری پرغلط یا نادرست از اطلاعات اقدام کند.<sup>۱۳</sup>

هرچند که این گزاره‌ها منطقی به نظر می‌رسند، اما تحقق عملی آنها به هیچ وجه آسان نیست. با توجه به گستره و مقیاس صرف گردآمدن داده‌ها به تنهایی توسط دولتهای مرکزی یا محلی و نامحدود بودن قابلیت تکنولوژی تکثیر چنین داده‌هایی، گفته شده است که خصوصی بودن (داده‌ها) همان‌قدر می‌تواند وجود داشته باشد که صاف بودن پوست کرگدن!<sup>۱۴</sup>

در ایرلند، اخیراً نگرانیها نسبت به تهدید شدن حقوق خصوصی به صورت پیشنهاد وارد کردن یک شماره بیمه اجتماعی درآمد (RSI)<sup>(۹)</sup>، که می‌تواند از محدوده‌های مالیات و خدمات اجتماعی فراتر رود و درهایی به نوعی سیستم هویت ملی بگشاید، بروز یافته است.<sup>۱۵</sup>

خطر بسیار واقعی از جانب ارتکاب خلاف در چارچوب تحقیقات انجام شده از سال ۱۹۹۰ تا ۱۹۹۲ در استرالیا توسط کمیسیون مستقل مبارزه با فساد (ICAC)<sup>(۱۱)</sup> نیوساوت‌ولز بروز یافت. توجه اساسی در این تحقیق معطوف به یک تجارت چند میلیون دلاری در اطلاعات محرمانه از رکوردهای دولتهای محلی، ایالتی و کشوری بود که به‌طور مشخص شامل دفاتر عمومی، شبکه‌های تحقیقاتی و شرکتهای بانکداری، خدماتی و قانونی می‌شد. اطلاعات ردوبدل شده شامل شماره تلفن‌ها، نشانیها، اطلاعات مربوط به گذرنامه و حسابهای بانکی، اطلاعات مربوط به بازنشستگی و سوابق ارتکاب جرم، و اطلاعات مربوط به مهاجرت بود. در مجموع، ۱۵۵ سازمان و

فرد در هدایت این خرابکاری دخیل بودند و ۱۰۱ نفر دیگر به اعمال و رفتار تشویق‌کننده و عامل این خرابکاری محکوم شدند.<sup>۱۶</sup>

این اتفاق درباره استاندارد اداره جامعه، حداقل در مورد آنها که به سازمانهای بیمه و دارایی بر می‌گشت، سؤالهایی پیش آورد که عمده‌اً در راه کسب اطلاعات برای مقاصدشان، نادیده گرفته شده بود. همچنین به برملا شدن کمبودهای جدی در سیاستهای جمع‌آوری و کنترل اطلاعات، به‌خصوص نیاز به محدود کردن موارد دستیابی به چنین اطلاعات و اجرای سیستمهای بازرسی مؤثر برای رسیدگی به اجرای درست چنین محدودیتهایی، انجامید. در سطوح بنیادینتر، درباره نیاز به گردآوری این میزان اطلاعات شخصی در وهله اول سؤالهایی مطرح شد. تهاجمهایی در این مقیاس عظیم به امور خصوصی که در این مثال آشکار شد هشداردهنده است و یافتن راه حل برای آنها دشوار به نظر می‌رسد، ولی نکته مهم این است که جامعه به یک راه‌حل نهایی برسد.<sup>۱۷</sup>

در کانادا، که در مدتی بیش از ده سال ماشینهایی به شهروندان کمک می‌کرد تا حقوق خصوصی خود را در رابطه با دولت مرکزی اجرا کنند، کمیسیون امور شخصی فهرست سودمندی از امور خصوصی منتشر کرده است که موارد زیر را در برمی‌گیرد.

**آشکار بودن / شفافیت:** جایی که تک‌تک افراد از این واقعیت آگاهند که رویه‌های گردآوری داده‌های جدید بهبود یافته، و نیز از حقوق شهروندی‌شان، دست‌کم حق اعتراضشان، آگاه باشند.

**توافق آگاهانه:** نیاز تک‌تک افراد به مطلع شدن و در جریان قرار گرفتن آنها نسبت به هرگونه افشای راز و نشت اطلاعاتی که علناً جمع‌آوری و پردازش می‌شوند.

**دسترسی:** تک‌تک افراد جامعه باید حق دسترسی و تصحیح اطلاعات نگهداری شده درباره خودشان که ناشی از هر داد و ستد باشد، داشته باشند.

**انطباق:** سیستمهای مشترک بین چند کاربر باید به‌طور داخلی چنان جداسازی شوند که از جداسازی احتمالی یا برهم افتادگی اطلاعات در حین مبادلات جلوگیری شود.

**دروازه‌گذاری:** باید روشهای امنیتی مناسبی برای جلوگیری از سوء استفاده یا دسترسی ناآگاهانه به اطلاعات درباره افراد



وجود داشته باشد و همراه با آن، باید برای افرادی که اطلاعات را به سیستم وارد می‌کنند، قابلیت اطمینان آن تضمین شود.

**وفاداری:** تمام کسانی که در امر جمع‌آوری اطلاعات دخالت دارند باید با قوانین مربوط به خصوصی بودن اطلاعات آشنا و نسبت به آنها وفادار باشند.<sup>۱۷</sup>

نیاز به توجه به موارد بالا، نه تنها در تکثیر پرونده‌های شخصی در گروهی از سازمانهای عمومی و خصوصی حایز اهمیت است، بلکه در توانایی سازمانها کاربرد کامپیوتر برای جستجوی فایل‌های همدیگر و هماهنگ کردن مجموعه داده‌های خصوصی آنها، دارای اهمیت است. مثلاً تطبیق دادن پرداختهای مالیاتی با فهرست عضویت در کلوپها و گروههای اجتماعی دیگر<sup>۱۷</sup>. پیشرفتهای دیگری در استفاده از برنامه‌های کامپیوتری برای آگاه‌سازی و نظارت کارمندان دست داده است. مثلاً دو مورد از جدیدترین بهسازیها روشن کرده که مسلم این است که هرچه تکنولوژی پیشرفته‌تر می‌شود تهدیدات نسبت به حوزه‌های خصوصی نیز جدی‌تر خواهند شد. اولاً برپایی یک پایگاه داده‌های شهروندی ملی در امریکا پیشنهاد شده که حامل نام هر شهروند مهاجر قانونی دارای شماره امنیت اجتماعی یا کارت سبز باشد. این پایگاه داده‌ها توسط کمیسیون اصلاح مهاجرت و در راه کمک به کارفرماهای آینده پیشنهاد شده است تا به وسیله آن بتوانند به صحت و سقم اطلاعات ارائه شده از جانب افراد جویای کار در فرمایشان پی‌بیرند. این پیشنهاد از سوی هر دو جناح در مجلس حمایت شد اما در حوزه حمایت از حقوق بشر به نگرانیهایی دامن زد<sup>۱۸</sup>. ثانیاً گروهی از افراد متخصص در اصلاح و بهره‌برداری اطلاعات از پایگاه داده‌ها، به نام کارآگاهان پایگاه داده، ظهور کردند. این افراد در قبال دریافت وجهی در پایگاه داده‌ها نفوذ می‌کنند و داده‌ها را می‌کاوند و اطلاعات بسیار حساسی را برای طرف قراردادشان مهیا می‌کنند<sup>۱۹</sup>. شاید آن چه که بیشتر از هر چیز در چنین مواردی نگران‌کننده باشد، این است که این تاخت و تازها به حریم خصوصی می‌تواند به راحتی در قالب فعالیت مفید و بهره‌وری بیان شوند. چنین پیشرفتهایی است که باعث شده تجاوز به حریم خصوصی به عنوان جدیدترین مشکل ارتباط با جوامع اطلاعاتی عنوان شود.

### قوانین محافظت داده‌ها

در ایالات متحده، قوانینی در زمینه خصوصی بودن در چارچوب

قانون محرمت، از سال ۱۹۷۴ تدوین شده است. این قوانین شهروندان را مجاز به امتحان و تصحیح رکوردهای جمع‌آوری شده توسط دولت می‌کنند. تصویب این قانون توجه عموم را به سوءاستفاده از اطلاعات جمع‌آوری شده و انباشته در سیستمهای کامپیوتری جلب کرد. کنگره نیز در سال ۱۹۸۴ قانون ابزارهای دسترسی جعلی و سوء استفاده و تقلب کامپیوتری را تصویب و دسترسی غیرمجاز به کامپیوترهای فدرال را خلاف قانون معرفی کرد<sup>۲۰</sup>.

در سال ۱۹۸۶، قانون تجاوز و تخلف کامپیوتری، قلمرو قانون فدرال را به جرائم کامپیوتری در بخشهای خصوصی بین ایالات، بسط داد. این امر در مورد تمام کامپیوترهای استفاده شده در دولت فدرال و مؤسساتی که توسط دولت فدرال بیمه شده‌اند اجرا می‌شود، سرقت کلمات رمز از پست، یا دستیابی به آنها یا نظر غیرمجاز به داده‌ها در هر کامپیوتری حاوی اطلاعات فدرال را، تخلف از قانون اعلام کرد. در همان سال، قانون خصوصی بودن ارتباطات الکترونیکی، جلوگیری از برقراری ارتباطات الکترونیکی مثل انتقال الکترونیکی سرمایه‌ها (EFTS)<sup>۲۱</sup> و پست الکترونیکی، بدون داشتن مجوز قبلی، را برای افراد غیرقانونی اعلام کرد<sup>۲۲</sup>.

در پانزدهم اکتبر ۱۹۹۲، کمیسیون اروپایی پیشنهاد تجدید نظر برای یک چارچوب اجرایی در حفاظت افراد با در نظر گرفتن پردازش داده‌های شخصی و حرکات آزادانه چنین داده‌هایی ارائه داد. امریه ارائه شده قصد داشت موانع موجود بر سر راه حرکات آزادانه داده‌های شخصی بین ایالات عضو را از میان بردارد؛ هم به دلیل نیاز به هماهنگی مقررات برای بازار متحد احتمالی اروپا، و هم برای از بین بردن ناسازگاریهای بین قوانین موجود در برخی کشورها یا فقدان هرگونه قانونی در برخی موارد دیگر<sup>۲۱</sup>.

این رهنمود از خطوط اصلی شورای پیمان اروپا درباره حفاظت داده‌ها (شماره ۱۰۸) حمایت می‌کرد که قبلاً توسط هفت کشور عضو شورای اروپا به تصویب رسیده بود. تغییرات مهم آن شامل تأکید بر داده‌های شخصی و برطرف کردن اختلاف مابین داده‌های بخشهای عمومی و خصوصی بود. جنبه مهم دیگر شکل مکمل آن است؛ یعنی این رهنمود خط‌مشی اصلی برای اجرای قوانین را ارائه می‌دهد، ولی برای کشورهای

عضو این حق را قائل می‌شود که به صلاحدید خود این اصول مشترک را اجرا کنند.

علیرغم این تغییرات، پیشنهاد تجدید نظر شده، ناشی از وسعت تعریف آن از پردازش و حجم اطلاعاتی که برای انجامش لازم است، و میزان مخارج بالای آنها هر دو، مورد انتقاد قرار گرفته است. از سوی دیگر، گفته شده است که این رهنمود به جای حفاظت حقوق افراد، ممکن است به حقوق آنها تجاوز هم کند. به خصوص اینکه گفته می‌شد که بندهای ۷ و ۸ و ۲۶ و ۲۷ آن، حقوق ارتباطات آزاد را به خطر می‌اندازند. نیز، احتمالاً سازمانهای خدماتی چون بانکداری، بیمه، هواپیمایی و حمل‌ونقل در معرض تغییر و تحولات پرهزینه‌ای قرار می‌گیرند که در واقع هیچ توجیه و دلیلی ندارند.<sup>۲۳</sup> انتقادهای به بررسی جریان برون مرزی داده‌ها تعمیم یافته است. جایی که بحث شده است که این رهنمود به جای ارتقای حفاظت تا حدنصاب مناسب، باید به بهبود انتقال داده‌ها به طرف سوم قرارداد در کشور دیگر می‌پرداخت، که استانداردهای پایتتری در این کشور سوم اجرا می‌شود و به این ترتیب پیشنهاد قانون حفاظت داده‌ای EC خدشه‌دار خواهد شد.<sup>۲۴</sup>

به نظر می‌رسد که تغییرات دیگری نیز در این رهنمود ضروری است. حتی گفته شده است که بهترین اقدام برای اعضای اتحادیه اروپا این است که صرفاً تاریخی را برای تحقق عملی شورای کمیسیون اروپا، شماره ۱۰۸، تعیین کنند.

## دارایی هوشمند

حضور همه‌جایی و ویژگی تواناساز تکنولوژیهای ارتباطی و اطلاعاتی اجتناب‌ناپذیر است، که پیامدهای آن به حوزه مفاهیم مالکیت و دارایی هم گام می‌نهد.

توانایی آنها در شکستن حد و مرزهای زمان و مکان و سهولت تکثیر و انتقال اطلاعات الکترونیکی، خصوصیت‌های ویژه‌ای‌اند که گنجاندن آنها را در مدارک قابل لمس دشوار می‌کند. در حالت خیلی ابتدایی، این امر می‌تواند به سردرگمی، مثلاً در نقش و هویت مؤلفان، ناشران و محافظان یا کاربران اطلاعات الکترونیکی منجر شود.

برای مثال، در ایالات متحده، در بازنگری قانون حق مؤلف (کپی رایت) فرض می‌شود که هر اثر اولیه و چاپ نشده‌ای تا زمانی که تکثیر نشده تحت حمایت حقوق مؤلف آثار منتشر می‌شود و حق مؤلف متوجه چه کسی است. قراردادهای متعارف بین مؤلفان، ناشران و کتابخانه‌ها دیگر برای یک محیط الکترونیکی مناسب نیستند. چرا که کاربرها می‌توانند هر وقت که بخواهند به اطلاعات الکترونیکی دسترسی یابند و آنها را پیاده کنند و اکثراً با حداقل توجه نسبت به حقوق مالکیت یا نیاز به پرداخت حق امتیاز یا حق التألیف این کار را انجام می‌دهند. به‌علاوه، با رشد شبکه‌ها نه‌تنها در سطح بین‌المللی، بلکه جهانی



حق مؤلف و مالکیت هوشمند موضوعی است که همان قدر واقعی و تحقق یافتنی به نظر می‌رسد که سایراسپیس<sup>(۱۲)</sup>

سایراسپیس عبارت است از هر منطقه‌ای که با قوه تصور و خیال انسانها و با کمک تکنولوژی الکترونیکی ایجاد می‌شود به بیانی ساده‌تر، این امر مستلزم موضوعات اساسی مثل حفاظت حق مالکیت در شبکه‌هایی است که معمولاً مشتمل بر آمیزه‌ای از اطلاعات رسانیهای تجاری و غیرتجاری می‌شوند. برطبق قانون جدید مالکیت آثار فکری در ایالات متحده در ارتباط با پایگاه داده‌ها، فقط توصیفهای اصلی می‌توانند شامل حقوق مؤلف شوند نه عقاید و ایده‌ها. بنابراین، کاربران می‌توانند هر چقدر می‌خواهند اطلاعات چاپ کنند، و تا وقتی که تمام سازمانها، یا نمای برنامه‌های نرم‌افزار به‌کاررفته برای ترتیب‌بندی این اطلاعات را تکثیر نکرده‌اند، تخلفی از حقوق مؤلف صورت نپذیرفته است<sup>(۱۳)</sup>

جوهره معضل تهدید مالکیت آثار فکری، به توان تکنولوژی حاضر در بازسازی و تدوین ایده‌ها و خارج کردن آنها از حیطه کنترل صاحبان اصلیشان برمی‌گردد. حال مسئله حساستری در حوزه نرم‌افزارها پیش می‌آید و آن نه تنها تکثیر غیرقانونی، بلکه مشکلات واقعی تفسیر و تعبیر آن چیزی است که کدام را اصل و کدام را جعلی بداند و چه چیزی خصوصی است و چه چیزی در حوزه عمومی قرار می‌گیرد. در واقع، این امر به‌طور فزاینده‌ای مشکل می‌شود که چگونه دقیقاً تشخیص دهیم که چه چیزی در واقع نرم‌افزار است در حالی که در عمل هر نرم‌افزاری می‌تواند در داخل سخت‌افزار به صورت ریزتراشه‌ها درآید<sup>(۱۴)</sup>.

تلاشهای انجام شده برای حل این مسائل از طریق حق مؤلف نمی‌تواند به موفقیت کامل برسد. در واقع، تلاشهای اجباری کردن حق مالکیت در محصولات مثل ورداستار<sup>(۱۵)</sup> با شکست کامل مواجه شد. هرچند شرکتهای نرم‌افزاری به تلاشهایشان در متوسل شدن به قوانین حق مؤلف، حق امتیاز و رمز و راز تجارتي ادامه می‌دهند، طیفی از اقدامات تخیلی دیگر به وجود آمده که همکاری مین سازنده‌ها و کاربران به شکل مشترک ابزار<sup>(۱۶)</sup> و یا باشگاههای عضویت نرم‌افزار را دربرمی‌گیرند.

در معنای وسیعتر کنترل بر استفاده از مالکیت آثار فکری،

## جرم کامپیوتری عبارت است از عملی مجرمانه که هدف آن کامپیوتر و اطلاعات ذخیره شده در آن یا انجام جرم به کمک کامپیوتر باشد.

یک رفتار سودمند می‌تواند توجه به موضوع جریان اطلاعات باشد تا انبار کردن آن. «کمسیون جرائم کامپیوتری» هلند پرداختن به جریان اطلاعات به جای انبار کردن آنها را پیشنهاد کرد. انجمن جرائم کامپیوتری آلمان پیشنهاد کرده است که کنترل در چنین مواردی می‌تواند روش نشانی‌گذاری هر قطعه از اطلاعات روی شبکه، توسط طراحان و فرستنده‌های آنها باشد. اگر پیامی برای انتقال خاص نشانی یا کدگذاری شده باشد، پس استفاده غیرمجاز می‌تواند دزدی قلمداد شود. در تمام موارد دیگر، استفاده آزاد است. به این وسیله، قانون شروع می‌کند به ساختن این که ارتباطات را بیشتر با کانالها درگیر کند نه با اشیاء. اما، به‌ناچار در دنیایی شبکهای شده و با پیوندهای درونی فزاینده، واقع‌گرایانه‌تر است اگر موفقیت در کنترل کامل بر اطلاعات را در بهترین حالت، موقت و مشروط فرض کنیم.

### سانسور و آزادی بیان

دل‌مشغولی دیگر در جامعه‌ای که هر روز فشار بیشتری از جانب تغییرات ناشی از اطلاعاتی شدن حس می‌کند، تبادل اطلاعات و ایده‌هاست. جوامع آزاد در سرتاسر جهان از دیرباز برای آزادی بیان و عقیده از سستهای جا افتاده‌ای برخوردارند، به همراه حفاظتهای عقلانی قانون برای مبارزه با سوءاستفاده‌ها. موضوع طعنه‌آمیز آن است که این آزادیها به دشواری به دست آمده‌اند و امروزه با تهدید گروهی تندرو با قدرت آزادی و توان زیادی به نام شبکه ارتباطات و کامپیوتر روبه‌رو شده‌اند. یک مثال برای

این مشکل، رفتار کاربران اینترنت است؛ شبکه وسیعی که بیش از ۷ میلیون نفر در ۱/۲ میلیون میزبان متصل به آن در ۱۱۷ کشور مختلف را به هم مربوط کرده است. هرچند که از سوی کاربران مختلف اینترنت که به دلیل محتوای سیاسی، مذهبی، یا نژادی پیامها و شکایتهایی دیده شده است، اما بیشترین شکایتها در حول موضوعهایی مربوط به وقاحت‌نگاری است

موضوع مهم در یک جامعه آزاد این نیست که آیا این موضوعات وقاحت‌نگاری‌اند یا خیر، بلکه این است که مدیران و کاربران شبکه چگونه با آن برخورد می‌کنند. بحث اصلی در خصوص برقراری تعادلی بین آزادی بیان و سانسور است. این امر در واقع صورت جدیدی از یک مسئله قدیمی است، مشکلی که قرن‌هاست دنیای نشر با آن دست به گریبان است، اما دلیل مشکل بودن آن این نیست.

در واقع، موضوعی که مدیران اینترنت با آن روبه‌رو بوده‌اند، شامل آزادی بیان، مزاحمت‌های جنسی و تنزل مقام زن، استفاده «مناسب» از منابع محدود دانشگاهی، مقاصد دانشگاهها، رابطه بین وقاحت‌نگاری و رفتار و زن بودن و وقاحت‌نگاری است

در پس این سیاهه دل‌مشغولها به آسانی می‌توان دید که بیشتر عملکرد این برنامه‌هاست که مدنظر است تا جنبه ارتباطی در یک شبکه وسیع کامپیوتری. از بیش از ۴۰۰۰ گروه خبری که در روی اینترنت یافت می‌شود، کمتر از ۲۰ واحد آنها خلافکاران مسائل مستهجن شناخته شده‌اند. میل به کنترل چنین مباحثی باید در همان قالبهای تجاوزات یادشده در بالا و حملات جاری در رسانه‌های چاپی دیده شود. واقعیت این است که در راه افشای چنین موضوعاتی، گروه‌های مخالف باید ابتدا قبول کنند که اینگونه مطالب را خوانده‌اند و سپس نظرات لازم را ارائه دهند.

این موضوع در مورد مطالب گرافیکی چشمگیرتر است چرا که تصاویر به‌شکل رمزگذاری شده منتقل می‌شود و سپس توسط نرم‌افزارهای خاصی رمزگشایی می‌شوند. ممنوع کردن تمام مطالب تصویری کاری غیرعادلانه و سخت‌گیرانه، و در حقیقت تصمیم‌گیری در این مورد که مرز بین خوب و بد کجاست. دشوار است ناچار گروه‌های موافق و مخالف چنین اقدامی در حال ازدیاد است. اقدام مناسب، قائل شدن آزادی بیان در یک چهارچوب ضوابط اخلاقی متفاوت و حتماً قوانین

مقررات رسانه‌های الکترونیکی است، ضمن تشویق گروه‌های مخالف مطالب مستهجن با توسل به اینکه رویه‌های مستهجن جنسی موجود و در حال گسترش بر علیه افراد نسردهنده آنها به‌کارگرفته شود.<sup>۲۵</sup>

در بریتانیا، در تلاشی برای رسیدگی به مشکل وسیع مطالب مستهجن کامپیوتری، لایحه‌کیفری خلافکاران و قانون انتشار وقاحت‌نگاری، هر دو، در سال ۱۹۹۴ برای دربرگیری تصاویر کامپیوتری، بازنگری و به‌روز شدند. در همان زمان قدرت پلیس در جستجو، جمع‌آوری و دستگیری تا حد دربرگیری مطالب کامپیوتری گسترش داده شد. هدف اصلی این کار تصاویر وقیح کامپیوتری است که می‌تواند از طریق لوح‌هایی فشرده (CD) یا مودم بین کامپیوترهای شخصی پخش شوند.<sup>۲۶</sup>

اگرچه نیت مقامات واضح است، به آسانی می‌توان پی‌برد که چرا گروهی از مردم به‌چنین اقداماتی بدبین‌اند. ابداع سایراسپیس مشکلی آفریده است که برای سانسور لاینحل به‌نظر می‌رسد، چرا که در واقع چیزی برای بریدن یا قطع کردن وجود ندارد، تمام آنچه که اتفاق می‌افتد در محدوده ذهن انسانهاست. با هجوم تأثیر تکنولوژی رسانه‌های گروهی و گسترش دسترسی به کامپیوترهای شخصی و وسعت کانالهای فرستنده، عمل سانسور در واقع ناممکن می‌شود. و حالا این ابزارها هستند که همانقدر مشکل آفرینند که کنترل چنین موضوعاتی. دستیابی به تمام خطوط تلفنی در کشور، قدرتی برای پلیس در جستجو و دستگیری می‌طلبد که در دموکراسی غیرقابل قبول خواهد بود.<sup>۲۷</sup>

---

حضور همه جایی و ویژگی

تواناساز تکنولوژیهای ارتباطی

و اطلاعاتی اجتناب‌ناپذیر است،

که پیامدهای آن به حوزه مالکیت

و دارایی هم گام می‌نهد.

---

## (اشتغال) کار

در طول دهه‌های هفتاد و هشتاد، توجه اصلی در تأثیر تکنولوژی جدید بر روی بازارکار این بود که اساساً آیا تأثیر کلی این تکنولوژی به سود کار است یا به زیان آن. نگرانیها با افزایش دامنه بیکاری ناشی از کاربرد تکنولوژی تا به امروز ادامه دارد. آمار نشان می‌دهد بین سال‌های ۱۹۹۰ تا ۱۹۹۴ بیش از ۳۰۰۰ تکنسین سخت‌افزار کامپیوتری در کانادا شغل خود را از دست داده‌اند، زیرا قدرت خودکفایی دستگاهها بالا رفته است، و پیش‌بینی می‌شود حدود ۲۵۰۰ شغل دیگر هم تا سال ۱۹۹۶ از دست برود<sup>۲۸</sup>.

امروزه مباحثات در جهتی است که نه تنها تغییرات تکنولوژیکی، بلکه عوامل سیاسی - اجتماعی چشمگیری مثل جنسیت، کنترل و سازماندهی کار و طراحی اجتماعی سیستمها در نظر گرفته شوند.

هیچ جنبه دیگری از مباحثات درباره تأثیر اجتماعی تکنولوژی به اندازه تأثیر آن بر روی اشتغال و شرایط کاری باعث ایجاد دو قطب کاملاً مخالف تفکر خوش‌بینانه و بدبینانه بین گروههای مختلف فکری نشده است. آنچه که مدینه فاضله تکنولوژیک گفته می‌شود، بینش انسان‌گرایانه‌ای از کارمشرک و خلاق و حساس علمی ارائه می‌دهد، درحالی که برای مخالفان این مدینه فاضله، آینده یعنی شغل تکراری و غیرانسانی در محیطی که توسط ماشینها کنترل می‌شود. به نظر کلینگ، این

دیدگاههای مختلف در یک طرز فکر در تأثیر اجتماعی پیشرفتهای تکنولوژیک توافق نظر دارند و آن این است که هر دو در نشان دادن نوعی تغییرات اجتماعی محدود تلاش می‌کنند<sup>۲۹</sup>.

در عصری که کامپیوتری شدن کماکان راه فراگیری می‌پیماید، تأثیر تغییرات تکنولوژیک ایجاد شده لزوماً به معنی تعمیم یک تفسیر روشن نیست. گروههای مختلف، مکانهای شغلی و سازمانهای متفاوت، نسبت به اجرای تکنولوژیها و سیستمهای مشابه واکنشهای متفاوت و پیش‌بینی نشده‌ای نشان خواهند داد. در واقع، برای اینکه واقعاً تأثیر اجتماعی تکنولوژی ارتباطات و اطلاعات را درک کنیم، باید ابتدا به ساختار اجتماعی و سازمانی که این تکنولوژیها در آن به کار گرفته می‌شوند، نظر کنیم. مثلاً، مباحثی مثل جنسیت و ساختار شغلی که در آن زنان کارمند باید در محیطهای بسته کار کنند، برای کنترل و سازماندهی یک کار، به خصوص در مشاغل اداری، عوامل حیاتی به شمار می‌آیند.

ابعاد مباحثه‌انگیز دیگر، به استفاده از کامپیوتر در کارهای گروهی یا در دفتر کار یا به معنی کار از راه دور، یا برای اداره و سنجش نحوه کار کارمندان ربط پیدا می‌کند. این امر، موضوع حساس تأثیر یک تکنولوژی جدید بر مهارت کارمندان را دربر می‌گیرد، موضوعی که در آن هر دو حالت زیاده از حد بودن مهارت یا نقص مهارت می‌تواند پیش آید، که به عوامل مختلفی مثل شغل، کارمند، محل کار و نوع تکنولوژی خاص مورد نظر، بستگی دارد. بی‌گمان، معرفی چنین سیستمهایی، به خصوص

آنچه که مدینه فاضله تکنولوژیک گفته می‌شود، بینش انسان‌گرایانه‌ای از کارمشرک و خلاق و حساس علمی ارائه می‌دهد، در حالی که برای مخالفان این مدینه فاضله، آینده یعنی شغلی تکراری و غیر انسانی در محیطی که توسط ماشینها کنترل می‌شود.

سیستم‌های اطلاعاتی، باید از طریق چشم‌انداز طراحی جامعه انجام شود، تا بر روی نظرات و ارزشهای استفاده‌کنندگان نهایی از سیستم تأثیرگذارد و باعث شناسایی اهمیت انسان و زیربنای جامعه برای اجرای موفق هر سیستم جدیدی شود.

قلمرو دیگری که به آن توجه زیادی می‌شود وجود نگرانی، نسبت به ارتباط، بین زمان کار و زمان فراغت است. پیشگویان زیادی عقیده دارند که بازده نهایی تغییرات تکنولوژیک حاضر کاهش سطح اشتغال در تمام بخشهای اقتصادی، چه در مشاغل اداری و چه در مشاغل کارگری، خواهد بود.<sup>۲۹</sup> هرچه که این پیشگویان پیشگوییهای خیال‌پردازانه‌تری برای سازمانهای کاری کنند، چنین جامعه‌ای می‌تواند زمان بیشتری برای فعالیتهای شخصی افراد ارائه دهد. چراکه زمان لازم برای انجام کار کاهش پیدا کرده و کارهای ضروری جامعه نیز بین تعداد زیادتری از افراد تقسیم خواهد شد.<sup>۳۰</sup> اینکه این برنامه‌ریزها چگونه خواهند بود و با چه بودجه‌ای تأمین خواهند شد معلوم نیست؛ به علاوه، اگر جوامع مدرن در حال تغییر یا دست‌کم برخوردارشان نسبت به مسئله کار را به‌طور جدی تغییر خواهند داد، بازسازیهای پردامنه اجتماعی و فرهنگی لازم خواهد بود که فقط اندکی از اشکال اولیه آن موجود است.<sup>۳۱</sup>

### کار از راه دور

قبلاً، نگرشهای خوش‌بینانه، گسترش بهره‌گیری از کار از راه دور را در جامعه پیش‌بینی کرده بودند. یعنی، به جای اینکه مردم به سر کار بروند، این اقبال را داشته باشند که از منزلشان یا از یک روستای دورافتاده یا هر مرکز مرتبط دیگری کار کنند، و این امکان‌بالقوه می‌تواند از وظایف عادی پردازش اطلاعات تا کارهای حساس علمی و پیشرفته را دربرگیرد. در نتیجه قدرت تطبیق خارق‌العاده و شتاب زیاد تکنولوژی ارتباطات و ارزان شدن روزافزون کامپیوتر، این امر را امکان‌پذیر می‌نمود. این تکنولوژیها در عمل می‌توانند سخت‌افزار و نرم‌افزار، پایگاه داده‌ها و رسانه‌های گروهی اطلاع‌رسانی را که تاکنون به‌طور عمده در دفاتری که در مرکز شهر مستقر بودند به خانه و در مناطق حومه شهر یا مناطق غیرشهری منتقل کنند.<sup>۳۲</sup>

در ایالات متحده و اتحادیه اروپا، کار از راه دور در بخشهای مختلفی به‌کار گرفته شده است. از آن جمله ارتباطات از راه

دور، سخت‌افزار و نرم‌افزاری کامپیوتری، بانکداری و بیمه، کار دولتی در سطح ملی و محلی، چاپ و انتشارات و تجارت را می‌توان برشمرد. برخلاف پیشگوییهای خوش‌بینانه در دهه‌های هفتاد و هشتاد، این امر به اندازه‌ای که انتظار می‌رفت همه‌گیر نشد؛ شاید به دلیل عدم انطباق با سلسله‌مراتب سازمانی موجود، یا ناسازگاری با عملیات لازم برای کنترل بازدهی کارمندان.

شواهد ناشی از یک مطالعه که توسط شرکت زیراکس در بریتانیا انجام شد، وجود شش‌ویژگی در سازمان را برای موفقیت در به‌کارگیری کار از راه دور ضروری دانست که عبارتند از:

- سازمان باید انطباق‌پذیر باشد نه غیرقابل انعطاف؛
- باید دارای هزینه‌های بالاسری با اصل کمتر دائمی باشد؛
- باید مشارکت فردی را افزایش دهد؛
- باید خلاقیت را شکوفا کند؛
- باید تشکل‌یافته باشد و مردم را درگیر کند؛
- باید برانگیزاننده ایجاد کار با کیفیت بالا باشد.<sup>۳۳</sup>

در استرالیا، در فوریه ۱۹۹۴، جورج اسمیت عضو شورای روابط صنعتی دستور اعلام فوری یک برنامه صنعتی برای تمام مستخدمان عمومی فدرال را صادر کرده، که این افراد را قادر به انجام سه روز کار از راه‌دور در هفته می‌کرد.<sup>۳۴</sup> اگرچه این اقدام سیل درخواستها از جانب مستخدمین عمومی برای انجام کار در منزل را به راه انداخت، ولی حداقل دوسال وقت لازم است که این تقاضاها به یک حادثه کار از راه دور در ابعاد وسیع تبدیل شود. در میان دلایل بیان شده برای این پیشگویی، نیاز به یک زیربنای تکنیکی برای پیش بردن پروژه را می‌توان عنوان کرد، که شامل اقدامات امنیتی برای صیانت اطلاعات و فقدان درخواستهای شدنی و امکان‌پذیر می‌شود. به علاوه در حالی که گردانندگان راجع به امکان بالقوه بهره‌وری بالا در نتیجه کار از راه دور صحبت می‌کنند، هنوز مسائل حل نشده‌ای در رابطه با بیمه سلامتی، غرامت کارمندان و شرایط محیط کار باقی مانده است.

تحقیقات انجام شده توسط شبکه ارتباطی استرالیا، در سال ۱۹۹۳ نشان داد افرادی که در منزلشان کار می‌کنند، معمولاً فعال‌تر، شادابتر و سالم‌ترند. اما زمان زیادی را صرف صحبت با همکارشان از طریق تلفن می‌کنند تا عنصر حذف شده ارتباط

اجتماعی را جبران کنند. میزان بازدهی و فعالیت کارمندان تا حدود ۱۸ درصد افزایش نشان داد، و میزان اضطراب در مورد زمان تحویل کار و فشارهای عمومی کار تا حدود ۱۵ درصد کاهش یافت. موارد مرخصیهای استعلاجی کمتر بود، شاید به این خاطر که افراد قادر بودند در زمانی که برایشان مناسب بود کارکنند و در روزهایی که احساس می‌کردند ناخوش‌اند می‌توانستند دیرتر کارشان را شروع کنند.

حدود ده درصد از شرکت‌کنندگان در مطالعه ارتباط از راه دور گزارش داده بودند که احساس دورافتادن از محیط کار را دارند. مطالعه یاد شده، ۳۱ نفر را که بچه‌ای در منزل نداشتند و دفتر کاری در منزلشان ایجاد کرده بودند انتخاب کرد. آنان علاقه داشتند که ساعات طولانی‌تری کارکنند، احساس می‌کردند می‌توانند بیشتر به خودشان متکی باشند و به‌طور کلی فکر می‌کردند که کنترل بهتری روی زندگی‌شان دارند. اگرچه کارشناسان اصرار دارند که روابط اجتماعی انسانها هنوز حیاتی است و هیچگاه نمی‌تواند به‌طور کامل در مکانی خارج از محل کار تحقق یابد<sup>۳۴</sup>.

اینطور نیست که کار از راه دور حتماً باید در منزل انجام شود، می‌تواند در مراکز کاری محلی یا دفاتر جانبی مجهز به منابع الکترونیکی لازم انجام شود. شواهد موجود در اروپا حاکی از این است که افسراد ترجیح می‌دهند در گروه‌های ۱۰ تا ۱۲ نفره در مراکز کار محلی کار کنند، به اضافه اینکه چنین بنیادهایی می‌توانند به ایجاد شغل‌های جدید منجر شوند. اگرچه راه‌اندازی چنین مراکزی منطقه به منطقه برحسب نیازها و شرایط محلی فرق می‌کند، ولی آنها معمولاً خدمات حمایتی برای کار و محلی برای فعالیتهای جمعی ایجاد می‌کنند.

اما همانطور که تام فوستر اشاره کرده است، امروزه تعداد قابل ملاحظه‌ای از افراد چه به‌صورت تمام وقت و چه نیمه‌وقت در منزلشان کار می‌کنند، که از این تعداد فقط تعداد کمی را می‌توان به عنوان کارمندان از راه دور یا با تکنولوژی بالا نام برد که از ابزار تکنولوژی ارتباطات برای پردازش یا انتقال محصولات هوشمند استفاده می‌کنند<sup>۳۵</sup>. با کمی دقت می‌توان دید که این مطلب زیاد تعجب‌آور نیست، با توجه به این که بیشتر خانه‌ها یا آپارتمانها برای کاربری به عنوان دفتر کار و اجرای فعالیتهای دفتر کار، کوچک‌اند و به نظر می‌رسد که کار در

منزل برای برخی مناسب است، در حالی که برای برخی دیگر چنین نیست. این که آیا واقعاً افزایش چشمگیری در نیروی کار مشغول در منزل در مقایسه با دفتر کار وجود دارد، هنوز مشخص نیست. به‌نظر می‌رسد تعداد افرادی که در منزلشان کار می‌کنند رو به افزایش است. چرا که الگوهای انعطاف‌پذیر کار گسترش بیشتری پیدا کرده و میزان قابل حمل و نقل بودن تکنولوژی ارتباطات کامپیوتری هم در حال افزایش است.

علیرغم فقدان شواهد دلگرم‌کننده برای بالا بردن موقعیتهای مناسب برای کار از راه دور، افرادی یافت می‌شوند که گسترش آن را در سطح بین‌المللی و در واقع جهانی پیشگویی می‌کنند. بنابراین، مفهوم مهاجران الکترونیکی مطرح شده است. یعنی، کسی که در کشور خودش می‌ماند اما از راه بسیار دور شاید چندین هزار کیلومتر، ارتباط برقرار می‌کند. مهاجران الکترونیکی معمولاً در یک یا دو گروه شغلی تخصصی یا تکنیکی، دفتری یا منشیگری، می‌گنجند. استفاده موفق از چنین کارمندانی، مستلزم تغییرات عمده‌ای در ساختار سازمان و مدیریت اجرایی آن و نیز عناصری مثل بازدهی و تولید مفید و طول روزهای کاراست.

در واقع، تغییرات عظیمی در شرایط کاری و روش زندگی کارمندان نیز ضروری خواهد بود. به علاوه، با نگرش به این واقعیت که اکثر قریب به اتفاق موارد، سازمانهای ارائه این مشاغل شرکتهای بزرگ بین‌المللی‌اند و دلایل کافی به وجود می‌آید که باعث ارتباط بین شرکتها و دولتهای هر دو کشور مربوطه می‌شود. این امر منجر به بروز نگرانی از بابت ایجاد یک نوع جدید استعمار الکترونیکی می‌شود که در آن، کشورهایی که کارمندان را ارائه می‌دهند، نسبت به فشارهایی که از طرف کشورهای خارجی به آنها وارد می‌آید آسیب‌پذیرند. از سوی دیگر، کشورهای مهاجردهنده از آسیب‌بهای شدن از نیروی متخصص و رفتن آنها به کشورهای خارجی در امان می‌مانند و از انتقال سرمایه به‌صورت حقوقی که به کارمندان از راه دور پرداخت می‌شود نیز سود می‌برند.

به آسانی می‌توان یک مدینه فاضله در این پیش‌بینیها ملاحظه کرد، به‌خصوص که در این پیش‌بینیها احتمال کاهش چشمگیری در الگوهای تبعیض در استخدام افراد را، مانند نژاد، جنس، سن و میزان قدرت فیزیکی که در شبکه ارتباطی جهانی

اهمیت کمتری دارند، به وجود می‌آورند. از سوی دیگر، نسبت به امکان بهره‌کشی از طریق محدود کردن کار قابل دسترس برای کسانی که سواد کمی دارند، و کمتر می‌توانند با صفحه کلید کار کنند و فاقد مهارت‌های ارتباطی لازمند، احتمال‌هایی وجود دارد. نسبت احتمال ایجاد کیت خطر شدید در سیستم مخابراتی جهانی از طریق به‌اصطلاح ترویج‌های تکنولوژیک، و تمامیت‌خواهی الکترونیکی که ممکن است از جانب کشورهای اعمال شود که می‌توانند بر تکنولوژی ارتباط و اطلاعات انحصار اعمال کنند، نیز خبرهایی به گوش می‌رسد.

با وجود فقدان شواهد کافی در مورد پذیرش فراگیر کار از راه دور، کسانی یافت می‌شوند که گسترش فراگیر آن را در مقیاس جهانی پیش‌بینی می‌کنند. بنابراین و مفهوم «مهاجر الکترونیک»، یعنی کسی که در کشور خودش زندگی می‌کند، اما با محل کارش شاید در هزاران کیلومتری رابطه مخابراتی دارد، سربرآورده است.

### سایر فعالیتهای بازرگانی در خانه

یکی از توضیحاتی که برای رشد آهسته‌تر از انتظار فعالیتهای در خانه بیان شده است، نقصان عناصر کلیدی، به اصطلاح انفورماتیک در خانه، چون بانکداری در خانه و خرید از طریق خانه است. بانکداری در خانه ظاهراً به این دلیل پا نگرفت که عملاً مفید نیست. عمدتاً به این علت که نمی‌تواند معاملات نقدی را انجام دهد و اکثر مشتریان، معاملات قابل ملاحظه‌ای که بتواند جبران مخارج این کار را بکند، انجام نمی‌دهند. تجربیات بانکداری در خانه در اروپا و آمریکا نتوانست از گامهای اولیه‌اش فراتر رود. موفق‌ترین مورد آن در دنیا بانک وربراگر در هامبورگ آلمان با مجموع ۵۰/۰۰۰ مشتری بود. بنابراین، به گفته فوستر، به بانکداری از خانه باید به عنوان یک تجربه شکست خورده نگاه کرد.<sup>۳۵</sup>

خرید از منزل هم بیشتر از مورد بالا با ناکامی مواجه شد؛ با ترکیبی از سیستم‌های پیچیده با محدودیت در انتخاب و کمبود ارتباط اجتماعی که به نظر می‌رسد باعث عدم اشتیاق و جلب نظر مشتریان برای پرداخت مبالغ گزاف شد، مانند ویوترون در ایالات متحده که ۵۰ میلیون دلار در مدت کوتاه سه سال از دست داد. ممکن است با اجرای با اصلاحات جدید، که در هر دو

تکنیک بالا رخ داده است، در آینده دور تمایلات ایجاد شده برای خرید از منزل بیشتر شود و آن را به جایی برساند که سرمایه‌های عمده‌ای که بتوان نامش را موفقیت گذاشت، به کار اندازد.

علاوه بر این، توافقیهای جدید مابین میکروسافت و چندین شرکت خدمات مالی صورت گرفته است که مشتریان را قادر می‌سازد به امکانات بانکداری خانگی از طریق بسته نرم‌افزاری پولی میکروسافت روی کامپیوترهای منزلشان دسترسی پیدا کنند، و می‌توانند به ایجاد تغییرات اساسی در موقعیت چنین فعالیتهایی منجر شود. در واقع، این امر می‌تواند به همگرایی کار با کامپیوتر و سرویس‌های ارتباط از راه دور به یک بسته‌بندی کامل نیازهای آموزشی، سرگرمی، اطلاعاتی و ارتباطی منجر شود.<sup>۳۷</sup>

### شبکه‌ای بودن جامعه

#### اینترنت

هر چند شبکه‌های گسترده‌ای برای کاربرد به وسیله سازمانهای منفرد مانند خطوط هوایی و بانکها، اجتماعات پژوهشگران یا انجمنهای تحقیقاتی در کشورهای گوناگون ظهور کرده‌اند. شبکه‌هایی با قلمرو وسیع از امکان بالقوه فراوان تأثیرگذاری اجتماعی برخوردارند.

انگیزه نیاز به چنین پیشرفتهایی از ایالات متحده و به کمک شرکتهای Arpanet و BITNET و Net Cs ناشی شد، که جملگی به قصد استفاده گروههای وسیع و پراکنده از محققان ایجاد شدند. این پیوندها با مثلاً اتصال BITNET به هم‌تای اروپایی‌اش EARN، به اتصالی در سطح جهانی ارتقا یافت. بعدها، شبکه‌های ملی مثل JANET در بریتانیا و ARNET در استرالیا، در واقع به گروههای اصلی در شبکه جهانی تبدیل شدند.

این فعالیتهای در قالب اینترنت به اوج خود رسید، که به متهورانه‌ای برمی‌گردد اقدام متهورانه‌ای که به تاریخ ۱۹۶۹ و شبکه‌ای که توسط وزارت دفاع ایالات متحده ایجاد شد، و امروزه تحت حمایت بنیاد ملی علوم ملی آمریکا کار خود را انجام می‌دهد. اینترنت در واقع شبکه‌ای از شبکه‌هاست که بیش از ۱۰۰/۰۰۰ کامپیوتر و میلیونها کاربر را در سرتاسر جهان به هم



مرتبط می‌کند. در حالی که غالباً اینترنت متوجه فعالیتهای تحقیقاتی و دانشگاهی است، ولی کاربران اینترنت برای مقاصد تجاری و صنعتی رشد زیادی کرده است. گسترش این امکانات خارق‌العاده بوده، و هرچند که استفاده از آن برای اکثر افرادی که به اینترنت دسترسی دارند رایگان است، ولی برای گردانندگان ملی مستلزم مقادیر چشمگیری هزینه، هم زمینه مسائل، اجرایی و بهسازی و به روز آوردن سیستم در میزان بالای استفاده از اینترنت، است و هم به مشکلاتی منجر شده که در زمانهای خاصی به حد اشباع خود می‌رسد.

اینترنت به انحاء گوناگونی در جوامع اطلاعاتی پایه مظهر کاربرد اجتماعی تکنولوژی به‌شمار می‌آید. یک نمونه روشن در این مورد، ظهور گروههای مباحثه تخصصی یا گروههای شبکه است که در روی اینترنت به عنوان گروههایی برای تبادل آزاد عقاید و اطلاعات، از مباحث جزئی گرفته تا موضوعات جدی، از راهپیمایی در فضا<sup>(۱۵)</sup> تا حفاظت محیط زیست، رشد کرده‌اند. یک نمونه جالب در این زمینه عبارت بود از تبادل ایده‌ها و اطلاعاتی که در طول جنگ خلیج فارس از ۱۹۹۰ تا ۱۹۹۱ بر روی اینترنت انجام شد. در همان هنگامی که محققان در چندین کشور در مورد بحران موشکهای اسکاد بحث می‌کردند، می‌توانستند نخستین اطلاعات دست اول را از همکاران اسرائیلی خود دریافت دارند، حتی در وقتی که موشکها در تل‌آویو فرود می‌آمدند. نمایش توانمند دیگر از تأثیر بالقوه اینترنت، عبارت است از پیامدهای آن در نوشته‌های پژوهشی در جایی که به جای تحمیل تأخیرهای سنتی در سیستم، مؤلفان می‌توانند صرفاً مطالب خود را به یک پژوهشنامه الکترونیکی مرکزی پست کنند که خوانندگان برای خلاصه مقاله یا مقاله کامل به آن دسترسی یابند.

در واقع، ناشران علمی السویرا<sup>(۱۶)</sup> برنامه اعطای مجوز به دانشگاهها را اعلام کردند؛ پروژه‌ای سه ساله که حدود ۱۵ دانشگاه را به دسترسی و پیاده‌کردن مجلات تحقیقاتی السویرا از طریق اینترنت قادر می‌کرد. این امر می‌تواند به ایجاد یک انقلاب واقعی در صنعت نشر انجامد.

جدای از مخارج زیاد برای ایجاد زیربنایی ضروری برای اداره سیستم، نگرانیهایی در باب امنیت داده‌ها در اینترنت رو به فزونی است. این موضوع به خاطر علاقه‌ای که سازمانهای

تجاری به استفاده از اینترنت نشان داده‌اند، به نحو چشمگیری پررنگتر شده‌است. ابعاد، تنوع و ماهیت پویای اینترنت آن را به محیط پیچیده‌ای تبدیل کرده که حل مشکلات امنیت و خصوصی نگهداشتن داده‌ها را دشوار می‌کند. اما این مسائل کمابیش قابل کنترل‌اند. تغییرات جالبتر مربوط به رشد درگیری سازمانهای تجاری و مفاهیم ساختاری و پشتیبانی است، که این امر به همراه دارد.

### ابر بزرگراههای اطلاعاتی

در سالهای اخیر، هیجان‌انگیزترین پروژه تکنولوژی رسانه‌های جمعی که نوید بخش عمیق‌ترین تأثیر بر کل جامعه است، عبارت است از «پروژه زیربنای اطلاعات ملی»<sup>(۱۷)</sup> در امریکا. اتحادی، بین دولت فدرال و طیف وسیعی از صنایع، به ابتکار ال‌گور، معاون رئیس جمهور امریکا به وجود آمد. این اتحاد به تکوین موارد مشابه و تکمیلی در سرتاسر جهان منجر شد.

ابر بزرگراه اطلاعاتی شبکه‌هایی از تارهای نوری و کابلهای هم‌محور را تشریح می‌کند که توسط کلیدهای پیچیده‌ای به هم وصل شده‌اند و می‌توانند صوت، داده، تصویر، متن و سیگنالهای ویدیویی را جملگی به زبان دیجیتالی و هماهنگ، منتقل کنند. این، یعنی همه چیز، از مکالمات تلفنی معمولی و دورنگار گرفته تا ارائه خدمات وسیعی چون دسترسی به پایگاه داده‌ها، تلفنهای ویدیویی، تلویزیونهای دوسویه، و ۵۰۰ تا ۱۰۰۰ کانال تلویزیونی پولی.

در ایالات متحده ادعا شده است که این جریان می‌تواند اساس یک انقلاب ملی به سوی جامعه‌ای اطلاعات پایه باشد و عنصری کلیدی در برداشتن گامهای ملی به سوی تداوم رهبری این کشور در دنیای اقتصادی است. دولت و صنایع در کار ایجاد زمینه جدیدی از رقابت‌اند که ارتباطات از راه دور و تلویزیون کابلی و کمپانیهای نرم‌افزاری و سخت‌افزاری کامپیوتری و شرکتیهای تفریحات و سرگرمی را به همکاری با یکدیگر در راه ایجاد و اجرای این بزرگراه اطلاعاتی قادر می‌سازد.

در راه تحقق این هدف، گروه کاری صنعتی کراس (XIWT) اتحادیه‌ای متشکل از ۲۸ کمپانی شامل AT&T، کامپیوتر، Apple، سیتی کروپ و بل ساوت، دیجیتال، IBM و هیوولت پاکارد برای سرپرستی تکنولوژیهایی که می‌توانند از مرزهای



سنتی صنعتی بگذرند و به ایجاد NII کمک کنند، تشکیل شده است. این امر دستیابی به تکنولوژی معسول و پروژه‌های آزمایشی و همایشهای تکنولوژی را در بر می‌گیرد.<sup>۳۸</sup>

طی یک ابتکار جداگانه، بل کور و تعدادی از همکارانش در تلویزیون، و تلفن و صنایع کارخانه‌ای در امر همکاری در خصوص زیربنای اطلاعات درگیرند، تا تکنولوژیهای پیش‌نمونه را برای NII ایجاد کنند و به عرصه آورند. به‌خصوص، تأکید بر نرم‌افزار پیش‌نمونه است که عامه مردم را به هدایت کردن این شبکه‌ها قادر سازد. نوید نهایی این فعالیتها گستره وسیعی از ارائه خدمات الکترونیک شامل مراکز خرید الکترونیک، آموزشهای الکترونیک مشترک و آموزش از راه دور، کتابخانه‌های الکترونیک، پیام‌گیری و اطلاع‌رسانی چندرسانه‌ای و سرگرمیهای چندرسانه‌ای متقابل است.<sup>۳۸</sup>

نظر به جدید بودن پروژه، هنوز در اینکه ابر بزرگراه اطلاعاتی در واقع چه چیزهایی را ایجاد می‌کند، عدم قطعیت چشمگیری وجود دارد. شرکت اوراکل این پروژه را مشتمل بر پنج مؤلفه اساسی معرفی کرده است که عبارتند از:

- مضمون، ذخیره‌سازی، شبکه، کاربردها و ابزارهای مصرف‌کننده،
- مضمون: اطلاعاتی چون متن، تصاویر ساکن، صدا، ویدیو و مانند آنها؛

- ذخیره‌سازی: «انبارهای اطلاعاتی» وسیع، در حقیقت خدمات رسانهای<sup>(۱۸)</sup> پر قدرت؛

- شبکه: دسته‌ای از شبکه‌های مختلف شامل همه چیز از سیم مسی تا تار نوری، صدا و سیما و ارتباطات ماهواره‌ای پالس سلولی.

- کاربردها: گسترده‌ای از کاربر و نرم‌افزار برای مشخص کردن مضمون؛

- ابزارهای مصرف‌کننده: گروهی از دستگاهها شامل کامپیوترهای شخصی، دستیاران دیجیتالی شخصی، تلویزیونهای معمولی و دو سره، و تلفنهای هوشمند (تلفن همراه) سنتی و سلولی.

پیش‌بینی می‌شود که خانه و یا کسب و کار عادی در ایالات متحده از چندین وسیله برخوردار باشند که می‌توانند به ابر بزرگراههای کامپیوتری وصل شوند.<sup>۳۹</sup>

گسترده خدمات قابل دسترس کاربران خانگی عبارتند از:

- سرگرمی: با کنترل شبانه‌روزی تماشاگر بر برنامه؛
- تندرستی: با سهیم کردن در اطلاعات و حتی تجزیه و تحلیل روشهای درمانی به کمک اتصالات ویدیویی و غیره؛
- اخبار: با توانایی بخشیدن به استفاده‌کنندگان برای مشخص کردن و نشان‌گذاری و انتخاب اطلاعات برای اطلاع از خبرهای مورد نظرشان؛

● **حراجیهای فصلی:** با ارائه خدمات شبانه‌روزی، مراکز خرید دور دنیا قابل دسترسی ویدیویی دوسره و فروشندگان دیجیتالی شده.

به استانداردها و مقررات، برای قوانین جاده‌ها به خاطر این ابربزرگراه اطلاعاتی نیاز است تا از بهره‌کشی و سوءاستفاده‌های خلافکارانه جلوگیری شود. امور خصوصی به یک مشکل عینی تبدیل می‌شود. چرا که هر مبادله‌ای در جایی ثبت خواهد شد. بنابراین، چه کسی باید به آنها دسترسی پیدا کند و چه استفاده‌ای از آنها بشود؟ این امر به نوبه خود به پرسشهایی اساسی از این دست منجر می‌شود که چه کسی باید این آیین‌نامه‌ها را تنظیم کند و چه کسی مخارج سیستم را پرداخت خواهد کرد؟

دولت فدرال در امریکا سیستمی را اختیار کرده که کسب و کار خصوصی در آن ابربزرگراه اطلاعاتی را ممکن می‌سازد و وجوه آن را پرداخت می‌کند و دولت شرایطی را برای سرمایه‌گذاری تضمین می‌کند که عمدتاً از طریق حذف نظارت دولتی بر تمام اشکال ارتباطات از راه دور انجام می‌گیرد. در عین حال، ال‌گور، معاون رئیس‌جمهور وقت، عنوان کرد که بدون تعهدات و حفاظتهای پر قدرت برای حقوق عمومی در بزرگراه اطلاعاتی، رهایی از قید و بندهای موجود امکان‌پذیر نخواهد بود

هیچ‌کس مشتاق نوآوری در ابر بزرگراه نیست و آشکارا هزینه‌های اجتماعی بالقوه به‌اضافه ابداع بزرگراه اطلاعاتی چیزی نیست که همگان را شیفته خود کرده باشد و به‌طور قطع هزینه‌های مالی گزافی برای آن ضروری است. مثلاً در استرالیا بی‌عدالتی‌هایی بالقوه تشخیص داده شده است و این احتمال که سیستمهای حامل شبکه، در تلاش برای بازیابی مخارج نصب شبکه‌های مدرن از مشتریانشان، احتمالاً درآمد بالا و نواحی پرجمعیت را به ضرر نواحی فقیر و روستایی ترجیح می‌دهند. این امر باعث توجه دقیق به مسئله اصلی خدمات عمومی در جامعه‌ای با گستردگی اطلاع‌رسانی می‌شود.<sup>۳۹</sup>

در حال حاضر بیشتر مردم فقط دارای یک تلفن هستند، اما این اوضاع در حال تغییر است. بعضی از اهالی مناطق دورافتاده که از خدمات پستی نامرتبی برخوردارند، به خدمات دورنگار به عنوان یک سرویس ضروری می‌نگرند، در حالی که افراد دارای اشکالات گفتاری و شنوایی استفاده از پست الکترونیکی

با وجود فقدان شواهد کافی در مورد پذیرش فراگیر کار از راه دور، کسانی یافت می‌شوند که گسترش فراگیر آن را در مقیاس جهانی پیش‌بینی می‌کنند. بنابراین، مفهوم «مهاجر الکترونیک» یعنی کسی که در کشور خودش زندگی می‌کند اما با محل کارش شاید در هزاران کیلومتری رابطه‌مخابراتی دارد سر بر آورده است

را ترجیح می‌دهند. به علاوه، کامپیوترهای شخصی برای مراحل دوم و سوم بسیاری از رشته‌های آموزشی و برای اتصال به کتابخانه‌های موجود روی خطوط، حیاتی به‌شمار می‌آیند.

در استرالیا گروه‌های مصرف‌کننده اصرار دارند که تعریف قانونی خدمات عمومی از آنچه که شامل فراهم آوردن خدمات استاندارد تلفن با بنیانی عادلانه و قابل دسترسی کافی است، به دربرگیری قدرت دستیابی به استاندارد جهانی، استانداردهای تکنولوژیک جهانی و ارتباط از راه دور جهانی و مشارکت در جامعه، تعمیم یابد.<sup>۴۰</sup> اما، درخواست برای دسترسی عمومی باید مشکلات تشویق شرکتهای بازرگانی به ارائه این خدمات و یافتن راههایی برای پرداخت غرامت خسارات در این راه، را در نظر بگیرند.<sup>۳۹</sup> اگرچه دولت کلینتون قول داده است که با بی‌عدالتی اجتماعی بالقوه که می‌تواند با پیشرفت ابر بزرگراههای اطلاعاتی توأم باشد، دست و پنجه نرم کند و

قوانین را در جهت دسترسی رایگان مدارس، کتابخانه‌ها و بیمارستانها تدوین کند، هنوز افرادی وجود دارند که نسبت به تأثیر چنین سیاستهایی شک دارند.

در واقع، نگرانی از این‌که اقدامات لازم برای اطمینان‌بخشی این خدمات ممکن است منجر به الزاماتی برای فراهم‌آمدن نیازهای ویدیویی و خدمات تفریحی برای فقرا و عملاً به معنی افزایش قدرت قوانین شود، به پاکسازی قوانین نظارتی دولت تا حد قانون کابل در سال ۱۹۹۲ در ایالات متحده آمریکا منجر شده است.<sup>۴۱</sup>

باید گستره وسیعی از سلیقه‌ها را سازگار کنند. مالکان مراکز سرگرمیها و اطلاع‌رسانی راههای جدیدی برای ارائه آن می‌خواهند. مالکان کانالهای ارائه اطلاعات می‌خواهند خطوط لوله‌ای بزرگتری بسازند و می‌خواهند انواع گوناگون مضامین را از طریق آن آزادانه ارسال کنند. کارخانه‌ها و تدوین‌کنندگان

## برخی نگران این تأثیر

### ضد اجتماعی

### بزرگراههای

### اطلاعاتی اند که مردم را

### از یکدیگر و از رودرویی

### با هم دور می‌کند. این

### پدیده مفهوم وارنده

### «عامه مردم» را از بین

### ممی‌برد و آن را با مفهوم

### بسیار متفاوت توده‌ای از

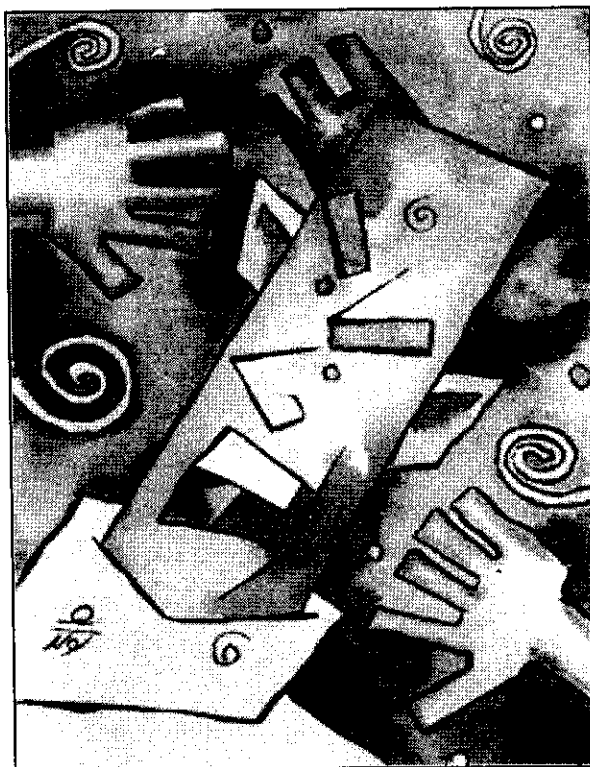
### افراد جایگزین می‌کند.

نرم‌افزارها می‌خواهند هر اطاق نشیمن یک دستگاه کامپیوتر داشته باشد و انواع جدیدی از نرم‌افزارها برای کاراندازی آن وجود داشته باشد. دولت آمریکا می‌خواهد موانع موجود سر راه تمام این اقلام را از میان بردارد و پهنه وسیعی از صنایع بعد از صنعتی شدن و قدرت تجاری آمریکا را در تکنولوژیها و رسانه‌های سرگرم‌کننده جدید ایجاد کند؛ از این‌رو گشودن راههای جدید از طریق شکستن موانع قانونی در سر راه رقابتها ایرادی ندارد چرا که این امر به موضوع بسیار جدی دموکراسی و مسئولیت عصر الکترونیک نمی‌پردازد.

برخی ابر بزرگراه اطلاعاتی را نمونه‌تهایی جبرگرایی تکنولوژیک و کمی بیش از یک اقدام بازاریابی از شرکت‌هایی تلقی می‌کنند که در فروش قطعات و ارائه خدمات ذی‌نفع‌اند. هستند. برخی دیگر، نگران یک تأثیر خاص ضد اجتماعی‌اند که به تدریج مردم را از یکدیگر و از رودر روی با هم دور می‌کند. این پدیده، مفهوم واژه عامه مردم را از بین می‌برد و آن را با مفهوم بسیار متفاوت توده‌ای از افراد جایگزین می‌کند.<sup>۴۲</sup> در میان انتقادهای صریحتر بر رهیافت دولت کلیتون به این معضلات، کسانی هم هستند که کل فشارها به سوی رقابت در ارتباطات راه دور را مثل یک نفرین نسبت به خیر عموم مردم در یک جامعه بالغ دموکراتیک می‌دانند.

چنین مفاهیمی گذراندن قوانین ابربزرگراه اطلاعاتی را نشانه‌ای از بدترین عناصر اخلاقی بازار، و به‌مثابه انتقال انبوه ثروت از طبقه متوسط به مراکز تجمع ثروت و روند چیرگی صنایع خدمات اطلاع‌رسانی توسط به اصطلاح انحصارگران کمپانی بل می‌دانند.<sup>۴۳</sup>

ضرورتاً نباید تمام و کمال چنین استدلال و مباحثه‌ای را پذیرفت تا برای بسته‌بندی کلی قوانین مربوط به بزرگراه اطلاعاتی که در حال تصویب در مجلس‌اند نگرانی به وجود آید، و یا برای مفهوم وسیع خدمات عمومی و دسترسی به اطلاعات نگران شد. اگر مثلاً حاملان ارتباط از راه دور با فاصله زیاد مجاز به ارائه خدمات مستقیم به کاربرهای شرکتهای بزرگ در شبکه‌های خصوصی، و در نتیجه انشعاب آن به شبکه‌های انتقالی محلی باشند، پس هزینه خدمات عمومی که عمدتاً از طریق وجوهی تأمین می‌شود که کاربران راه دور به گردانندگان شبکه‌های محلی برای دسترسی به شبکه پرداخت کنند، به خطر



هر چند باید دقت‌چشمگیری در ارتباط با پیش‌بینی‌های اجتماعی به جا آید، و بسط آن بدون تردید ریشه اصلی دل‌سردی‌های جاری ناشی از تأثیر تکنولوژی در جامعه است، فواید زیادی می‌تواند از مطالعه این روندهای جاری حاصل شود. بنابراین، دامنه تحولی که کامپیوتر در زندگی روزمره ایجاد کرده است می‌تواند حقیقتاً همه‌گیر و فراگیر تلقی شود و برای ایجاد یک نقطه عطف در روش زندگی ما، از کار گرفته تا تفریح، نویدبخش باشد.<sup>۴۴</sup>

هنوز پاسخ ساده‌ای برای این پرسش که آیا تکنولوژی‌های ارتباطی و اطلاع‌رسانی در الگوهای موجود در جامعه می‌گنجد، و آیا رفتارهای اجتماعی باید برای گنجد شدن در تکنولوژی تغییر کند یا خیر، وجود ندارد. با در نظر گرفتن تفاوت‌های موجود بین کشورها، پیش‌بینی شده است که تأثیر نهایی این تکنولوژی انقلابی، موج بزرگی از بدعت‌ها و نوآوری‌ها را به جوامع پیشرفته در طی سالهای نخست قرن بیست و یکم تزریق خواهد کرد. این تنها یک پیش‌بینی است. اما اگر درست از آب در آید، پیامد نهایی آن نه تنها تحول فاحش در اساس

خواهد افتاد. همچنین، ورود شرکتهای فرعی بل و زمینه‌هایی چون خدمات اطلاعاتی و انتشارات الکترونیکی می‌تواند آثار نامطلوب ایجاد مجموعه‌های غیررقابتی را پدید آورد که هر دو جنبه مضمون و کانالهای عبوری را دربر می‌گیرد.

واضح است که ورود ابر بزرگراه‌های اطلاعاتی بسیار مهمتر از یک دسترسی الکترونیکی فوری در راه زندگی مرفه شهروندی است. هنوز برای پیشگویی درباره نتیجه چنین پیشرفتهایی بسیار زود است، اما روشن است که صحنه برای نمایشی آماده است که به نظر می‌رسد مدت درازی روی پرده خواهد بود.

#### تأثیر اجتماعی تکنولوژی‌های ارتباطات و اطلاع‌رسانی

گرچه گاهی پدیده یاد شده در بالا بیشتر از آنچه در واقع قادر به ارائه چیزی بوده، وعده آن را داده است، نویدهای تکنولوژی ارتباطی و اطلاع‌رسانی به هیچ وجه از نظر تحقق مادی ناکام نبوده است. دست‌کم در حوزه اجتماعی و با در نظر گرفتن تأثیر این تکنولوژی‌ها بر روش زندگی است که اختلافات بین قابلیت و اجرای آن بیشتر از هر چیز قابل توجه بوده است.

تکنولوژی جوامع مدرن، بلکه یک انقلاب اجتماعی خواهد بود.

عمل تایپ کردن فرمانها در کامپیوتر چیزی بیش از تبادل نظر است، و در واقع به بروز اتفاقاتی از درون صحبت و عملی می‌انجامد که ساخته دنیای کامپیوتری است.<sup>۴۶</sup>

این که آیا کسی با نظر دیبل موافق باشد، یا به نظر وی تأثیر رسانه‌های دوسره هرچیزی غیر از جان سالم بدر بردن بی‌ضرر است، زمینه‌های روشنی برای این بحث پدید می‌آورد که تکنولوژیهای ارتباطات و اطلاع‌رسانی در حوزه امور انسانی و اجتماعی ژرفترین تأثیر را خواهد نهاد.

### یادداشتها

- 1- Uninterruptible power systems (UPS)
  - 2- Hacking
  - 3- Manual hacking or finger hacking
  - 4- Operations Manna
  - 5- British telecom
  - 6- Stand - alone
- سیستم یا ابزار یا دستگاهی که بدون نیاز به چیزی می‌تواند کار کند.
- 7- Dial back
  - 8- Organization for Economic Co- Operation and Development
  - 9- Revenue Social Insurance.
  - 10- Independent commission against corruption.
  - 11- Electronic Funds Transfers
  - 12- Cyberspace
  - 13- Wordstar نامی تجاری است
  - 14- Share ware
- نرم‌افزاری که فروشنده بدون دریافت پول به خریداری می‌دهد یا خریدار می‌تواند کپی آن را از هر کسی بگیرد یا بیازماید، اما در صورتی که آن را پسند کند و بخواهد به کار بگیرد، باید بهایش را به فروشنده بپردازد.
- ۱۵- Star Trek نام یک فیلم فضایی جدید.
- 16- Elsevier
  - 17- National Information Infrastructure (NII)
  - 18- Server
  - 19- Lambda Moo
  - 20- Multi-User Dimension

### منابع:

- 1- Carl B. Jackson (1992) «The need for security». In: *Managing Information Technology*. Delran, NJ: Datapro, 6010, pp. 1-12.
- 2- Tom Forester and Perry Morrison (1990) «Computer crime: new problem for the information society». *Prometheus*, 8, (2), December pp.257-7?
- 3- Ira Hertzoff (1992) «Voice network fraud». In: *Managing Information Technology*. Delran, NJ: Datapro, 1434, pp. 1-9.
- 4- Hugo Kelly (1988) «Law aims to hunt computer hackers». *The Age*, Melbourne, 7<sup>th</sup> December.
- 5- John G. Burch (1992) *Systems analysis, design and implementation*. Boston: Boyd & Freefone, pp. 451-53.

بی‌گمان، ترویج‌دهندگان و حامیان ابربزرگراه اطلاعاتی در قابلیت انقلابی آن برای ایجاد تحول در جامعه تردیدی ندارند. به نظر ال‌گور، معاون سابق رئیس جمهور امریکا، این پروژه به ارتقای آموزش، برقراری دموکراسی و نجات جان آدمی می‌انجامد. کری‌الیسون، بانی و رئیس هیئت مدیره شرکت اوراکل، مدعی است که این امر حیات و زندگی ما را نسبت به آنچه می‌پنداریم، دگرگون خواهد کرد. برطبق نظر الیسون، مانه تنها از طریق ابربزرگراه اطلاعاتی صحبت یا خرید خواهیم کرد، بلکه در فضای آن به‌زندگی خواهیم پرداخت. افرادی که چنین تعاریفی را ابراز می‌کنند، در مورد سنجش و مفهوم برخی فعالیتها در بازیهای گروهی اینترنت حق دارند. عمدتاً آنهایی که در این عملیات درگیرند، ظاهراً دچار اختلال حواس می‌شوند یا دست کم مات و گیج و بین واقعیت و خیال سردرگم‌اند.<sup>۴۹</sup>

یکی از موارد مشهود در فحواهی یک بازی به‌نام لامدامو<sup>(۴۹)</sup> روی داد: در عمارت پر از جادویی که فقط به شکل لغات روی صفحه وجود داشت، اما در نظر تعداد زیادی از بازیکنان به‌صورت یک جماعت واقعی قلمداد می‌شد. در این بازی پرکاربر یا (MUD)<sup>(۴۹)</sup> بیش از ۱۵۰۰ بازیکن در این عمارت جمع شده بودند و هرکدام شخصیتهای مخصوص به خود را خلق می‌کردند که از اطایقی به اطایق دیگر در رفت و آمد، و مشغول تبادل نظر بر طبق قوانینی صریح بودند. آرامش این محیط خیالی سال گذشته وقتی که یکی از ساکنین این خانه به فرد دیگری تجاوز کرد، از هم گسیخت. غوغای بعدی بازیگران و تقاضای کیفر از سوی قربانی، به‌سرعت به جایی رسید که به نظر می‌رسید کسانی که درگیر قضیه بودند مشکل می‌توانند بین یک حادثه خیالی و دادخواست جرم در زندگی واقعی، با آنچه در یک فضای خیالی سایبراسپیس بازسازی شده بود، فرق بگذارند.<sup>۴۵</sup>

جولیان دیبل که این داستان را در روزنامه ویلیج وِسس نیویورک نوشت، مفهوم عمیقتری از این اتفاق برداشت کرد. به نظر دیبل، این گواه دیگری بود از مرحله نهایی عبور ما به عصر اطلاعات، و نمونه‌ای از تغییراتی که ممکن است دیوار قدیمی حافظه بین قول و تعهد و عمل را از میان بردارد.

- 28- *Toronto Financial Post* (1994) 23<sup>rd</sup> August, p. 6 (taken from the Internet).
- 29- Rob Kling and Charles Dunlop (1993) «Controversies about computerization and the character of white collar worklife». *The Information Society*, 9, pp. 1-29.
- 30- Herbert Applebaum (1992) «Work and its future». *Futures*, 24, (4). May, pp. 36-50.
- 31- F.W. Newton (1993) Australia's information landscapes. *Prometheus*, 11, (1), June, pp. 3-39.
- 32- Penelope Schoeffel, Alison Loveridge and Carl Davidson (1993) «Telework: issues for New Zealand». *Prometheus*, 11, (1), June, pp. 49-60.
- 33- Philip Sim (1994) «Telecommuting, still a long way off». *Computerworld*, April, p. 29.
- 34- Ben Mitchell (1994) «Workforce of the future stays home». *The Sunday Age*, Melbourne, 20<sup>th</sup> February, p. 18.
- 35- Tom Forester (1991) «The electronic cottage revisited: towards the flexible workstyle». *Urban Futures*, 2, (1), (Special Issue, 5) pp. 27-33.
- 36- Virgil L.P. Blake and Thomas T. Suprenant (1990) «Electronic immigrants in the information age: some policy considerations». *The Information Society*, 7, pp. 233-44.
- 37- Geoff Wheelright (1993) «Homing in on a new market: Microsoft plans for PCs in the home». *Financial Times*, 21<sup>st</sup> December, p. 8.
- 38- Louise Kehoe (1993) «US moves one step nearer the 'information highway'». *Financial Times*, 14<sup>th</sup> December, p. 26.
- 39- Adam Lincoln (1994) Dawn of a new information age? *Managing Information Systems*, 3, (3), April, pp. 70-73.
- 40- Ben Potter (1994) «Waiting for directions on the technological superhighway». *The Age*, Melbourne, 11<sup>th</sup> February, p. 14.
- 41- *Wall Street Journal* (1994) 17<sup>th</sup> August, A12.
- 42- McKenzie Wark (1994) *The Australian*, Melbourne, 14<sup>th</sup> May, p. 26.
- 43- Vigidor Schreibman (1994) Closing the 'Values gap': the crisis point. *Federal Information News Syndicate*, 11, (18), 29<sup>th</sup> August (taken from the Internet).
- 44- Halal, William E. (1993) «The information technology revolution: computer hardware, software and services into the 21<sup>st</sup> century». *Technological Forecasting and Social Change*, 44 pp. 69-86.
- 45- Julian Dibbell (1994) «Data rape: a tale of torture and terrorism online». *Good Weekend, the Age Magazine*, Melbourne, 9<sup>th</sup> February, pp. 26-32.
- 46- Stephen Amidon (1994) «Lost in cyberspace». *Sunday Times, Arts & Culture*, 17<sup>th</sup> July, pp. 8-10.
- 47- Robert Schrifteen (1993) «Freefone lines set off spate of 'data rape'». *Sunday Times*, 14<sup>th</sup> November, p. 11.
- 48- Information security news (1993) *Information Management & Computer Security*, 1, (1), p. 9.
- 49- Richard H. Baker (1991) «Physical security techniques». In: *Managing Information Technology*, Delran, NJ: Datapro, 6030, pp. 1-14.
- 50- Andrew S. Tannenbaum (1992) *Modern operating systems*. Englewood Cliffs, NJ: Prentice Hall, pp. 184-86.
- 51- *Transnational Data & Communication Report* (1993) January-February, p. 30.
- 52- Willis H. Ware (1993) «The new faces of privacy». *The Information Society*, 9, pp. 195-210.
- 53- Anne W. Branscomb (1991) «Common law for the electronic frontier». *Scientific America*, September, pp. 112-116.
- 54- Jerry L. Salvaggio (1989) «Is privacy possible in an Information Society?» In: *The Information society: economic, social and structural issues*. Hillsdale, NJ: Lawrence Associates Inc., pp. 115-29.
- 55- Data Protection (1993) *Transnational Data & Communication Report*, 16, (2), March – April, pp. 39-42.
- 56- Thad Dunning (1993) *Transnational Data & Communication Report*, 16, (5), September – October, pp. 28-32.
- 57- Ian Temby (1993) «Australia exposes illegal data sales». *Transnational Data & Communication Report*, 16, (1), January – February, pp. 26-29.
- 58- Thad Dunning (1993) Data protection. *Transnational Data & Communication Report*, 16, (5), March – April, pp. 39-42.
- 59- *Information Week* (1994) 18<sup>th</sup> August, p. 20.
- 60- *New York Times* (1994) 18<sup>th</sup> August, C1.
- 61- Jay Bloombecker (1990) «US Computer crime legislation: a review». *Managing Information Technology*, Delran, NJ: Datapro, 1430, pp. 1-28.
- 62- EC Data Protection (1993) (Special Report) *Transnational Data & Communication Report*, 15, (6), November – December, p. 31.
- 63- Jan Barkvens and Marc Schauss (1992) New EC data protection era. *Transnational Data & Communication Report*, 15, (6), November – December, pp. 43-45.
- 64- Simitis sees improvement in EC data protection revision (1992) *Transnational Data & Communication Report*, 15, (5), November – December, p. 42.
- 65- Mitchell Kapor (1991) «Civil liberties in cyberspace». *Scientific American*, September, pp. 116-20.
- 66- Richard S. Rosenberg (1993) «Free speech, pornography, sexual harassment and electronic networks». *The Information Society*, 9, pp. 285-331.
- 67- Michael Prescott and Howard Foster (1994) «Police got new Powers to fight computer porn». *Sunday Times*, July.
- 68- Stephen Amidon (1994) «Lost in Cyberspace». *Sunday Times, Culture*, 17<sup>th</sup> July, pp. 9-11.