

قدرت و سیاست در جامعه شبکه‌ای

نوشته جان ون دایک
ترجمه اسماعیل یزدان پور

مقدمه: شبکه‌ها و قدرت

موضوع اصلی این گفتار قدرت است. تقسیم قدرت یکی از مهم‌ترین ابعاد اجتماعی ساخت و کاربرد شبکه‌ها است و این شبکه‌ها به هیچ وجه از لحاظ فنی و سیاسی خنثی نیستند. ساختار شبکه به گونه‌ای است که هم تمرکززدایی را ممکن می‌سازد و هم ابزارهایی را برای تمرکز فراهم می‌آورد. می‌توان مرکز، پیوندها و پایانه‌ها را با آرایش‌های گوناگون چید. در آینده، وضعیت افراد در شبکه‌های رسانه‌ای، تعیین‌کننده وضعیت آنان در جامعه خواهد بود. با توجه به این نکته، فریب پنهان در گزاره‌های عامیانه‌ای از جنس "اطلاعات قدرت است" و "دانش قدرت است" آشکار می‌شود. دسترسی به دانش و اطلاعات، به تنهایی فایده‌ای ندارد، بلکه باید در موقعیت استفاده از آن قرار داشت. خالقان و پردازشگران واقعی اطلاعات و دانش در جامعه ما - اعم از دانشمندان، متخصصان اطلاعات، و روزنامه‌نگاران - کمتر به عنوان کنترل‌کنندگان واقعی آن شناخته می‌شوند. چیزی که قطعیت دارد آن است که کسی که مهارت استفاده از اطلاعات را ندارد، در زمره افراد فاقد قدرت قرار دارد. از این رو، دسترسی فرد به اطلاعات یا دانش، یکی از شرط‌های لازم و نه کافی

برای دسترسی به قدرت است.

داشتن موقعیتی که در آن بتوان درباره شرایط سازمانی و فنی ساخت و استفاده از شبکه‌ها تصمیم گرفت، اولین و مهم‌ترین عامل تعیین‌کننده موقعیت فرد در شبکه است. این نکته، در تمامی سطوح موقعیتی، صادق است. در سطح کلان، ساخت شبکه‌های دربرگیرنده تعادل قدرت میان حکومت و شهروندان، مدیریت‌های عمومی و شهروندان، کارفرمایان و کارگران، مدیران و مجریان، تولیدکنندگان و مصرف‌کنندگان است. در سطح میانی، سازمان‌ها و تغییرات قدرت ناشی از ساخت و کاربرد شبکه‌ها بیشترین نمود را دارند که در این گفتار به تفصیل تشریح خواهند شد. در سطح خرد، آثار اجتماعی و روانی ارتباطات رسانه‌ای، تعادل قدرتی میان افراد را تغییر می‌دهد که موضوع بحث مستقلی است.

به هر حال، به نظر می‌رسد بهتر است در این گفتار از عمومی‌ترین سطح آغاز کنیم. مردم بیشتر فراموش می‌کنند که کنترل (توسط همه پست‌ها و موقعیت‌های) یک سیستم، با ظهور شبکه‌ها، در عین افزایش، کاهش نیز می‌یابد. سیستم که تلاش دارد توان ارتباطی خود را افزایش دهد به رسانه‌ای فنی وابسته می‌شود. به این ترتیب، شبکه‌های رسانه‌ای، فناوری‌هایی به شدت آسیب‌پذیرند.

بخش‌هایی از این مقاله به روش‌های تقسیم قدرت میان دولت و شهروندان در واحدهای بزرگ سیاسی می‌پردازد. شبکه‌ها می‌توانند به دولت قوی‌تر (تمرکز قدرت سیاسی) و یا قدرت بیشتر شهروندان و برجسته شدن منافع اجتماعی (پراکندگی قدرت سیاسی) منجر شوند. آنها را هم می‌توان برای مراقبت و نظارت متمرکز و ثبت و ضبط مدارک و شواهد به کاربرد و هم می‌توانند در خدمت استقلال محلی و مشارکت شهروندان در تصمیم‌گیری‌های سیاسی قرار گیرند.

بخش دیگر پیرامون تأثیرات ناشی از ساخت و کاربرد شبکه‌ها بر تغییر قدرت در سازمان‌ها است. به نظر می‌رسد هر دو شکل تمرکز شدید و تمرکز زدایی و تقسیم‌بنیادی کار و افزایش کار گروهی ممکن باشد. هر صورتی که حادث شود، سطوح میانی مدیریت بیشترین تأثیر و تغییر را می‌پذیرند.

بخش‌نهایی پیرامون شهروندان منفرد، کارمندان، مشتریان، و مصرف‌کنندگان در پایانه‌ها و انتهای شبکه است. از آنجا که شبکه‌ها حوزه‌های عمومی و خصوصی را به هم مرتبط می‌سازند، استقلال فردی مصرف‌کنندگان (آزادی انتخاب) و حریم خصوصی افراد اهمیت می‌یابند.

آسیب پذیری شبکه‌ها

حالا همگان می‌دانند که شبکه‌های رایانه‌ای، می‌توانند به سرعت و آسانی متلاشی شوند. هر روز، خبرهای جدیدتری از هک، ویروس، نقض حریم خصوصی، و خرابی رایانه‌ها منتشر می‌شود. در پایان دهه ۱۹۹۰ میلادی، نگرانی‌هایی پیرامون مساله سال ۲۰۰۰ ظاهر و شایع شد. مساله از این قرار بود که در بسیاری از سیستم عامل‌ها، بانک‌های اطلاعاتی، برنامه‌های نرم‌افزاری، ریزپردازنده‌ها، و دیگر تجهیزات میکروالکترونیکی، سال ۲۰۰۰ تعریف شده نبود. در سال ۲۰۰۰ با این واقعیت آشنا شدیم که شبکه‌های اجتماعی با اتکای کامل بر نظام‌های رایانه‌ای می‌توانند آسیب پذیر باشند. در دهه اخیر، کنگره‌ها و سمینارهای بی‌شماری پیرامون اهمیت نظام‌های اطلاعاتی برپا شده است. به‌رغم -یا شاید هم در اثر- تقلیل مسائل به سطوح فنی، سازمانی، و حقوقی، هنوز باید در پی راه حل‌های اصلی و کامل تر بود.

قابل توجه آن است که مساله آسیب پذیری شبکه به امنیت فنی و حفاظت از حریم خصوصی و رازداری تقلیل یافته است. در واقع، آسیب پذیری مساله‌ای عام تر و گسترده تر است. آسیب پذیری بیشتر مربوط به ثبات کلیت نظام اجتماعی است که با فناوری‌های جدید اطلاعاتی و ارتباطی کار می‌کند. این نظام خود را وابسته به قدرت‌هایی کرده است که هیچ کنترل (کاملی) بر آن ندارد. وقتی فناوری از کار می‌افتد، نظام وابسته به آن هم نمی‌تواند عملکردی داشته باشد، یا اگر کار کند، با مسائل گاه بزرگ و مزمن و مهمی مواجه است. به علاوه، گاه نیروهایی درونی برای مقابله با استفاده از فناوری و مقاومت در برابر آثار آن و حتی تخریب آن شکل می‌گیرد. این نیروی مخرب یا مقاومت گر، هنگامی ایجاد می‌شود که برخی گروه‌ها یا طبقات اجتماعی احساس کنند به خاطر شکلی از "عدم تناسب" با جامعه شبکه‌ای، از برخی حقوق محرومند و یا به حاشیه‌های جامعه رانده شده‌اند.

به علاوه، قدرت کلیت نظام می‌تواند در معرض تهدید واحدهای خارجی و بیگانه‌ای باشند که دسترسی گسترده تری دارند. از این رو، در بیشتر کشورها، حاکمیت ملی در خطر است؛ چرا که ملت‌ها کنترل خود بر اقتصاد، فرهنگ، و سیاست را از دست می‌دهند و آنها را به شبکه‌های سخن‌پراکنی و ارتباطات رایانه‌ای، صنایع جهانی و مهم تر از همه بازار بین‌المللی واگذار می‌کنند.

ایده وسیع آسیب پذیری که در اینجا مطرح شده است، به طور کلی در مورد فناوری اطلاعات

صادق است. اما به طور خاص، در مورد شبکه‌ها کاربرد دارد. آسیب پذیری شبکه‌ها ناشی از برخی ویژگی‌های خاص شبکه‌هاست. این ویژگی‌ها عبارتند از:

"اندازه" مهم‌ترین ویژگی یک شبکه است. ریسک یک شبکه، قدرت و کاربرد آن را مشخص می‌کند. در عین حال، هر چه توان دسترسی یک شبکه افزایش می‌یابد، کنترل و مهار آن برای مدیریت شبکه دشوارتر شده و امکان خطای سیستم افزایش می‌یابد. شبکه چیزی بیش از ماشین‌ها و کاربردهای مجزا است و کیفیت سخت‌افزارها و نرم‌افزارها وابسته است.

"انسجام" منابع مرکزی و محلی یا حاملان اطلاعات و کارکردهای چندگانه آنها، از مشخصه‌های مهم شبکه‌ها هستند. به هر حال، همین ویژگی‌ها باعث می‌شوند اگر یک بخش از سیستم از کار بیفتد، اثری مستقیم یا غیرمستقیم بر کل سیستم داشته باشند. از مثال‌های بارز در این خصوص می‌توان به ویروس‌ها و هک‌های رایانه‌ای اشاره کرد که اغلب بدون مشاهده شدن، درون و میان شبکه‌ها "انتقال" می‌یابند. طراحی فنی خوب یک شبکه و توجه دقیق به دسترس پذیری، انعطاف پذیری، و کارایی، می‌تواند نقص‌ها و از کار افتادگی‌های ناشی از شبکه‌ها را به حداقل برساند.

"دسترس پذیری برای کاربران مرتبط" یکی از قوی‌ترین ویژگی‌های یک شبکه است و در عین حال یکی از نقاط ضعف آن به شمار می‌رود. امکان دسترسی افراد ناآگاه و غیرمجاز به شبکه به تناسب افزایش می‌یابد.

شبکه‌ها، در مقایسه با واحدهای منفرد و مجزا، باعث افزایش پیچیدگی نظام‌های اطلاعاتی می‌شوند. به علاوه، مسائل ارتباطی جدید و متنوعی پدید می‌آید. وقتی واحدهای محلی رایانه‌ها و پایانه‌های هوشمند قادر به انجام کار مستقل می‌شوند، این پیچیدگی افزایش می‌یابد. به همان نسبت پیچیده شدن شبکه، امکان خراب شدن و از کار افتادن شبکه هم افزایش می‌یابد و یافتن منشا و تعمیر این خرابی‌ها دشوارتر می‌شود.

پیچیدگی بیشتر به وابستگی به متخصصان معدود می‌انجامد: تکنیسین‌ها و اپراتورهای شبکه. غیبت یا عدم دسترسی به این متخصصان - چه به خاطر بیماری، اعتصاب، ناتوانی، یا شایعی - باعث آسیب پذیری بیشتر شبکه‌ها می‌شود.

یک ویژگی رایج و عمومی و در عین حال اجتناب پذیر شبکه‌ها، عدم وجود یا ضعف در امکانات پشتیبانی است. وقتی بخشی از شبکه از کار می‌افتد، تجهیزات، نرم‌افزارها و نظام‌های ذخیره‌سازی

پیشین و قدیمی به کار نمی آیند. مساله اساسی تر و اجتناب ناپذیر تر دیگر آن است که کاربران فرایندها و شیوه های سنتی و دستی و پیشین را خیلی زود به فراموشی می سپارند. برای مثال، بسیاری از طراحان و برنامه ریزان بازنشسته برای رفع مساله تاریخ سال ۲۰۰۰ به خدمت فراخوانده شدند. راه حل؟ بسیاری از راه حل های این مسائل، ویژگی های ایجابی و مثبت شبکه ها را محدود می کنند. برخی گزینه های راهبردی، پیامدهای گسترده و دامنه داری دارند: آیا باید شبکه ها را از لحاظ اندازه محدود کرد؟ یا باید میزان عملکرد و درجه انسجام آنها را کاهش داد؟ می توان با ایجاد شبکه های کوچک و برای مقاصد خاص، چنین راهبردهایی را عملی کرد. این شبکه های کوچک، بدون هیچ الزامی، می توانند به هم اتصال داشته باشند. اتصالات درونی را می توان با امنیت و پیچیدگی نسبی طراحی کرد. به علاوه، خود اتصال را می توان تا حد زیادی کنترل کرد و در حد ابتدایی و ساده تعریف کرد. در این صورت، "اطلاعات" فقط در مرکز و در تجهیزات پایانه ای ذخیره می شود.

شرکت ها برای کاهش پیچیدگی، به جای استفاده از ترکیب چند سطحی تجهیزات قدیمی و جدید یا چند دستگاه مستقل، بیشتر تمایل دارند سیستم های از پیش طراحی شده بخرند. به علاوه، همیشه در پی استاندارد کردن و مطابق شدن هستند. دسترسی برای همگان ملموس ترین ویژگی است که نیاز بیشتری به نظارت و مهارت و کنترل دارد. بخش عمده ای از امنیت سازمانی و فنی کنونی بر محدودیت و نظارت و کنترل مبتنی است. اما بسیاری از کارشناسان بر این باورند که امنیت تمام عیار شبکه ها غیر ممکن است. آنها نمی توانند با بیان این که امنیت وابسته به مردم است، این ادعا را توجیه کنند. کاربرپسندی یک شبکه - که دلخواه همه است - رابطه مستقیمی با اندازه شبکه، کارکردهای چندگانه آن، و قابلیت های اتصال و ارتباطی آن دارد و این ویژگی ها در عین مطلوبیت، امکان خرابی و دسترسی غیرمجاز را افزایش می دهند. افزون بر این، هر محدودیت در دسترسی پذیری در تضاد با توزیع دانش و قدرت قرار دارد و سبب وابستگی به جمع محدودی از متخصصان می شود.

تهیه و نصب امکانات پشتیبانی از سخت افزارها، نرم افزارها، و ظرفیت ذخیره سازی، فرایند هزینه بری است. حفظ فناوری ها، شیوه های سازماندهی، و روال های کاری قدیمی هم نیاز به هزینه های زیادی دارد. در آینده ای نزدیک تهیه نسخه های پیشین از اهمیت کمتری برخوردار خواهد بود. در بسیاری موارد، نگهداشت تجهیزات کامل و کافی در انبار، برپایی شبکه ها رابی فایده

و عبث می کند.

فهرست ذیل نشان می دهد که بسیاری از راه حل ها محدود کننده و حتی خنثی کننده اثر و کارایی شبکه ها هستند. برخی راه حل ها آسیب پذیری های دیگر و متفاوتی را برای شبکه ها ایجاد می کنند. به علاوه، می توانند اثر مخربی بر تعادل قدرت در نظام اجتماعی مورد نظر داشته باشند. مواردی از این موضوع را به تفصیل خواهیم شکافت. اما پیش از هر چیز، به مساله قدرت در نظام اجتماعی و آسیب پذیری نظام در برابر مخاطرات اجتماعی در اثر استفاده از شبکه ها می پردازیم. تصمیم به نصب و استفاده از شبکه، بیش و پیش از هر چیز، تصمیمی سیاسی است، حتی اگر تحت فشارهای خارجی افزایش رقابت و ارتقای رتبه اتخاذ شود.

پراکندگی و تمرکز سیاست

بی شک، نفوذ رسانه های ارتباطی و افزایش سطح آموزش های عمومی، مهم ترین عوامل احیای جهانی جنبش های حقوق مدنی و دموکراسی در دهه های ۱۹۸۰ و ۱۹۹۰ میلادی بوده است. گسترش شبکه های مخابرات و ارتباطات جمعی بین المللی، نقش مهمی در فروپاشی رژیم های استالینی در اروپای شرقی داشته و در کشورهای در حال توسعه، جنبش های خواهان دموکراسی را برانگیخته است. می توان چنین گفت که به علت پخش برنامه های رادیویی و تلویزیونی غربی و افزایش مکالمات تلفنی بین المللی، فروپاشی دیوار برلین و سقوط اتحاد جماهیر شوروی اجتناب ناپذیر شده بود. حتی کشورهای به نسبت "بسته تری" همچون آلبانی و جمهوری های جنوبی شوروی، و کشورهای در حال توسعه ای همچون چین، نپال، کنیا و زامبیا، نشان دادند که در برابر آثار ارتباطات بین المللی آسیب پذیرند.

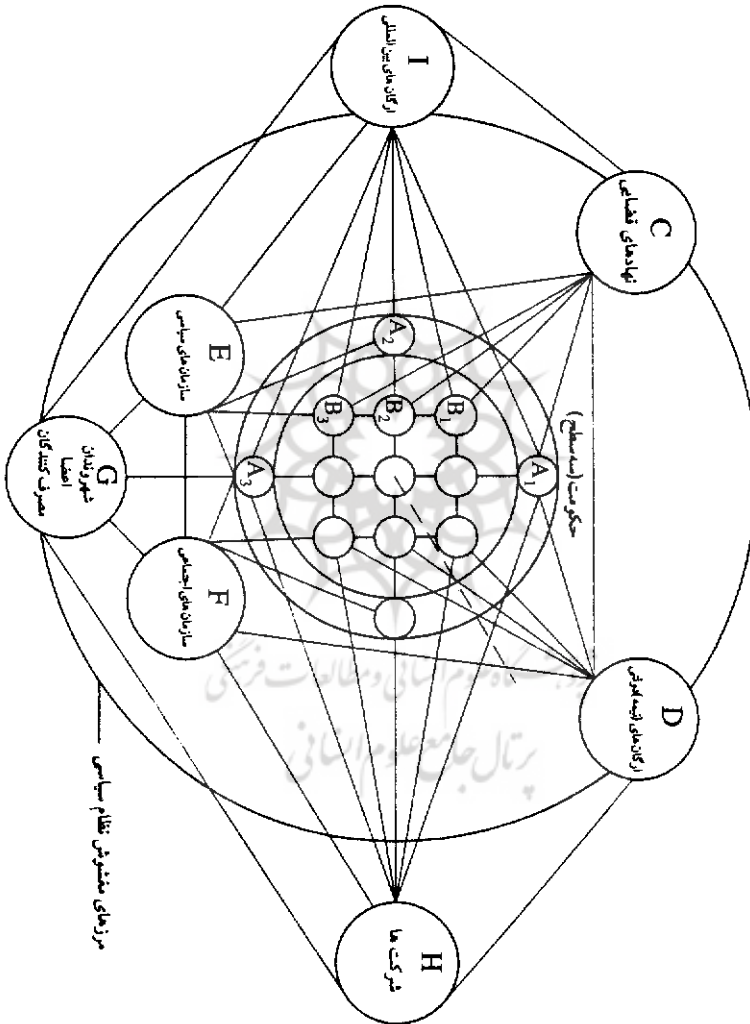
ظریه ای، که فناوری های اطلاعاتی و ارتباطی را عامل "مرگ" نظام های سیاسی سنتی تمامیت خواه (مبتنی بر تمرکز و کنترل همه اطلاعات و ارتباطات در یک قلمرو خاص) می داند را می توان به سادگی توجیه کرد. با استفاده از این فناوری های، محال است که بتوان تک تک تولیدات محلی و توزیع های گسترده در یک قلمرو خاص را به صورت متمرکز ثبت و مستند کرد. هیچ رژیم تمامیت خواهی نمی تواند پس از رواج گسترده رایانه های شخصی، دیسکت، فاکس، و دیگر تجهیزات سمعی و بصری به حیات پیشین خود ادامه دهد. از سوی دیگر، با توجه به امکاناتی که فناوری های جدید برای نظارت و مدیریت و کنترل مرکزی پدید آورده است، می توان صورت های دیگری از حاکمیت با تمایلات تمامیت خواهانه را متصور شد.^۲ برای درکی حقیقی از این صورت

های جدید حاکمیت، نباید پنداشت که آنها به نظرات مستقیم (به مفهوم جرج ارولی کلمه) یا کنترل کامل همه سطوح تولید و توزیع اطلاعات نیاز دارند. قدرت سیاسی یا اقتصادی راتنها باید هنگامی به کار برد که شهروندان، کارگران، یا مصرف کنندگان از یکی از خطوط تعیین شده - که توسط نظام های کلان و گسترده الکترونیکی ثبت و محافظت می شوند - عبور کنند. راه ها و شیوه های خاصی برای چک کردن افراد و فعالیت هایشان هست که کار آبی های بیشتری از مراقبت مستقیم الکترونیکی یا چشمی دارند فضا و آزادی زیادی وجود دارد، اما وقتی خط خاص نقض شد، در یک مرکز کنترل، زنگ خطری به صدا در می آید.

با توجه به امور متفاوت ارائه شده در بند پیشین، خیلی هم عجیب نیست که نظرات متفاوت و متعارضی پیرامون آثار فناوری های جدید اطلاعاتی و ارتباطی بر آزادی، مردم سالاری و ساختار سازمانی وجود داشته باشد. به نظر عده ای، فناوری های اطلاعاتی و ارتباطی، فناوری آزادی است، چرا که این فناوری ها آزادی انتخاب افراد را تقویت می کند و روابط افقی (پایین به پایین) را در شبکه سازمان ها و افراد تشدید می کند.^۳ برخی دیگر چنین استدلال می کنند که طراحی و معرفی فناوری های جدید اطلاعاتی و ارتباطی توسط رهبران حکومتی، مدیران بخش دولتی، بازار و دیگر سازمان های رسمی انجام می شود و به همین جهت، فناوری های جدید ابزاری برای ثبت و ضبط و مراقبت و نظارت و کنترل است. از این نگاه، به کارگیری فناوری های جدید اطلاعاتی و ارتباطی به معنای تلاش برای کنترل بیشتر سازمان ها و واحدهای تابعه است.^۴

پیش از پیچیدن در این بحث ایدئولوژیک، بیایید بر پیشرفت های واقعی حکومت ها و مدیریت های عمومی متمرکز شویم. این پیشرفت ها را می توان در یک نمودار ترسیم کرد. روابط میان همه کنشگران درگیر در فعالیت های سیاسی به مفهوم وسیع کلمه، را می توان در یک مدل جامع از نظام سیاسی گنجانند (نمودار ۱ را ببینید). در گفتارهای پیشین، تجلی زیرساخت های جامعه شبکه ای در بخش اقتصاد (درون و میان شرکت ها) را بررسی کردیم. نمودار ۱ نشان می دهد که سیاست جامعه شبکه ای در ساختاری شبکه ای سازمان می یابد. تمامی روابط میان کنش گران مختلف نظام سیاسی - حکومت، پارلمان، مدیریت عمومی در سطوح ملی، منطقه ای و محلی، احزاب سیاسی و سازمان های جامعه مدنی، سازمان های بین المللی، مراجع قانونی، نهادهای (نیمه) دولتی، شرکت ها، و شهروندان - را هم می توان به عنوان روابط سیاسی (قدرت) تفسیر کرد و هم به عنوان روابط اطلاعات و ارتباطات. شبکه های رسانه ای و کاربرد آنها، به این روابط شکل و سازمان

می دهند. نمودار ۱ را باید مدلی از یک نظام پویا دید که می تواند نشان دهد چگونه برخی از روابط و کنشگران اهمیتی مضاعف می یابند و برخی دیگر طرد می شوند یا به حاشیه رانده می شوند.



در دموکراسی دیجیتال^۵، نگارنده به این نتیجه رسیده است که فناوری‌های ارتباطی و اطلاعاتی هم می‌تواند به پراکندگی قدرت کمک کند و هم می‌تواند در خدمت تمرکز قدرت باشد. استفاده از فناوری‌های اطلاعاتی و ارتباطی، نیروهای گریز از مرکز کنونی را تقویت می‌کند، چرا که در قلب سیستم، نیروهای نهادینه سیاسی باید بخشی از قدرت خود را به سازمان‌های بین‌المللی، شرکت‌های ملی و بین‌المللی، نهادهای حقوقی، آژانس‌های خصوصی شده، و شرکت‌های خصوصی و شهروندانی تفویض کنند که بی‌گير جدي منافع خود هستند. با کمک فناوری‌های اطلاعاتی و ارتباطی، آنها می‌توانند روابط اطلاعاتی و ارتباطی خود را شکل دهند و حیطه‌های نفوذ و مدیریت خود را اداره کنند. به این ترتیب، آنها نظام سیاسی مختص خود را می‌سازند و نقش هماهنگ کننده دولت در یک قلمرو خاص را دور می‌زنند. برخلاف دولت، فناوری‌های اطلاعاتی و ارتباطی هیچ مرزی ندارد.

از سوی دیگر، شبکه‌ها امکان ثبت مطلق و کامل را برای دولت‌ها و مدیریت‌های عمومی فراهم می‌آورند، قدرت کارمندان دولت را نسبت به نمایندگان مجلس افزایش داده، اغلب احزاب سیاسی را تابع ماشین و مکانیسم‌های دولتی کرده و این احزاب را محل توزیع دستورات رسمی و متمرکز سیاسی می‌کنند. از این رو، فناوری‌های اطلاعاتی و ارتباطی امکان تمرکز سیاست و قدرت را هم تأمین می‌کنند.^۶ دولت و مدیریت عمومی از جمله اولین بخش‌هایی هستند که فناوری‌های اطلاعاتی و ارتباطی را در مقیاس وسیع به کار می‌گیرند. بدیهی است که آنها از این فناوری‌ها برای اولویت‌های حاکمیت، هماهنگی، و جمع‌آوری مالیات استفاده می‌کنند و کمتر به فکر بهبود نظام نمایندگی شهروندان و پارلمان خواهند بود.

با وجود این، تحلیل‌انتهایی که انتظار ظهور دولت مقتدری با توانایی ثبت و ضبط و کنترل فراگیر را دارند، به همان میزان یک سوپیه و غیرواقعی است که تحلیل‌انتهایی که گمان می‌برند دولت از میان خواهد رفت یا حتی در میان روابط مجازی از نوع افقی در سازمان‌های اینترنتی محو خواهد شد. فریسن^۷ ظهور دولت مجازی و ناپدید شدن سیاست سنتی در حواشی جامعه را پیش‌بینی می‌کند. در همین ادامه، گوهنو^۸ پایان سیاست و دموکراسی را پیش‌بینی کرده است. بنا به نظر او، این دو جای خود را به نظامی از روابط غیررسمی و شبکه‌ای بدون مرکز مشخص خواهند داد:

در عصر شبکه‌ها، روابط میان شهروندان و مرکز سیاست در رقابت با ارتباطات بی‌شماری قرار

دارد که هر فرد می‌تواند جدای از این مرکز ایجاد کند. سیاست دیگر سازمان دهنده اولیه زندگی مردم و جامعه نخواهد بود؛ در عوض، کار درجه دومی خواهد بود که همچون بنایی سست، نخواهد توانست مسائل عملی جهان متغیر و گذرارا حل کند.

هر دوی این نظرهای یکسویه‌اند چرا که شبکه‌ها علاوه بر اتصالات و ارتباطات افقی، از مراکز و گره‌های عمودی هم تشکیل شده‌اند. شبکه‌ها کنشگران گوشتی و خونی (مردم) و منابع مادی (در منازل و سازمان‌ها) را به هم وصل می‌کنند. در یک جامعه شبکه‌ای، شبکه‌ها جایگزین جامعه نمی‌شوند، اما اجزای سازنده آن را به هم وصل کرده و سازماندهی می‌کنند. پس هنوز دولت از قوی‌ترین (مجمع) کنشگران جامعه است. از این رو، سیاست و دموکراسی که بیش از همه در سطح جامعه کارکرد دارند، محکوم به نابودی و فنا نیستند. البته، این دو نیاز به پشتیبانی و بازاندیشی توسط نیروهای سیاسی و دموکراتیک خارج از سیاست‌های رسمی و نهادهای دارند و در این راه، فناوری‌های اطلاعاتی و ارتباطی می‌تواند به کار آید.

نویسندگان همچون گوینو و موشویز^۹ بیان داشته‌اند که توسعه فناوری‌های اطلاعاتی و ارتباطی الزاما به نفع دموکراسی نیست. قدرت می‌تواند به دست نیروهای کمتر دموکراتیک و یا حتی غیردموکراتیک بیفتد. به علاوه، اثر ایجابی فرضی فناوری‌های اطلاعاتی و ارتباطی بر دموکراسی، بستگی به این دارد که چه نگاهی به دموکراسی داشته باشیم.^{۱۰} در این خصوص حداقل شش نظر درباره دموکراسی مطرح است. پنج نظر اول را دیوید هلد به عنوان "مدل‌های دموکراسی" معرفی کرده است. مدافعان این نظریه‌ها، ترجیحات و اولویت‌های متفاوتی برای طرح و کاربرد فناوری‌های ارتباطی و اطلاعاتی در نظام سیاسی دارند.^{۱۱}

دو نظر اول درباره دموکراسی به کاربرد فناوری‌های اطلاعاتی و ارتباطی برای تقویت سیاست نهادی، یعنی مرکز نظام سیاسی می‌انجامد (نمودار ۱ را ببینید، "آ" و "ب" کنشگران حکومت و مدیریت عمومی). با پراکندگی سیاست به طور اعم و با فرسایش دولت ملی در برابر دیگر نیروهای ملی و بین‌المللی به طور اخص، سیاست نهادی در وضعیت خطرناکی قرار دارد که با روی آوردن به فناوری‌های اطلاعاتی و ارتباطی وخیم تر خواهد شد. با وجود این، غالب‌ترین نیروهای سیاسی دموکراسی‌های غربی به میدان می‌آیند و از فناوری‌های اطلاعاتی و ارتباطی برای تقویت مواضع دولت استفاده می‌کنند. نظریه کلاسیک دموکراسی غربی که از این حرکت پشتیبانی می‌کند، دموکراسی حقوقی است - نظریه به اصطلاح نظام‌نامه‌ای دموکراسی که قانون اساسی و دیگر قوانین

و مقررات را مبنای دموکراسی می‌داند. سه اصل اساسی عبارتند از: تفکیک قوا (قوه مجریه، قوه مقننه، قوه قضائیه)؛ نظامی از بازرسی و تعادل میان حکومت، مدیریت عمومی؛ و قوه قضائیه؛ و نمایندگی. بر اساس این نظر، اطلاعات ناقص گردآوری شده توسط دولت، مهم‌ترین مسأله‌ای است که می‌توان با استفاده از فناوری‌های اطلاعاتی و ارتباطی آن را حل کرد. از این رو، فناوری‌های اطلاعاتی و ارتباطی، دولتی قوی می‌آورند و حکومت را به خوبی اداره می‌کنند. به علاوه، این فناوری‌ها با ارائه اطلاعات بهتر و بیشتر و دو جانبه، می‌توانند پشتیبانی‌های عمومی از دولت را بهبود بخشند و سطح مدیریت را ارتقا دهند.

درک دوم از دموکراسی را "دموکراسی رقابتی" می‌نامند. این نظر بیشتر در کشورهای دو حزبی و نظام ریاست جمهوری مورد توجه قرار می‌گیرد. بنا به این برداشت، احزاب و رهبران برای کسب پشتیبانی و آرای مردم با هم رقابت می‌کنند. این برداشت به نسبت نخبه‌گرا از دموکراسی، بر نمایندگی و تصمیم‌گیری‌های موثر و کارآمد رهبران تأکید می‌کند. فناوری‌های اطلاعاتی و ارتباطی بیش و پیش از هر چیز در رقابت‌های اطلاعاتی و رقابت‌های ریاست جمهوری به کار می‌آیند. در امریکا، تجربه‌های زیادی درباره استفاده از فناوری‌های اطلاعاتی و ارتباطی به دست آمده است.^{۱۲} نظام‌های اطلاعاتی عمومی و نظر سنجی‌های تلفنی می‌تواند به رای دهندگان در انتخاب بهترین برنامه‌ها و رهبران کمک کند.

چهار نظر دیگر پیرامون دموکراسی، جهت‌گیری راهبردی بسیار متفاوتی دارند. مدافعان این نظریه‌ها بیشتر به دنبال "اجتماعی کردن سیاست" هستند؛ یعنی پراکندگی بیشتر سیاست در کلیت نظام (با توجه به کنشگران بیرون از مدل در نمودار شماره ۱). این نظر متضمن نقش برجسته‌تر سازمان‌های اجتماعی و به ویژه شهروندان منفرد است. این پنداشت وجود دارد که فناوری‌های اطلاعاتی و ارتباطی، آنها را قادر خواهد ساخت تأثیر بیشتر و مستقیم‌تری بر سیاست داشته باشند و حتی سیاست‌های رسمی و نهادی را دور بزنند یا روابط سیاسی خود را جایگزین آن کنند. نمودار ۱ به خوبی نشان می‌دهد که روابط آنها بیشتر به صورت دور زدن مرکز شکل می‌گیرد. اگر نظریه‌ها و چشم‌اندازهای با تقویت‌کننده سیاست‌های رسمی و نهادی را سیاستمداران و مدیران تقویت و پشتیبانی می‌کنند، این نظریه‌های بدیل مورد حمایت بسیاری از سازمان‌های اجتماعی و روشنفکران قرار دارد.

بنیادی‌ترین دیدگاه پیرامون رویه‌های سیاسی موجود "دموکراسی همه‌پرسی" است. بنا بر

این نظر، تصمیم‌های سیاسی را باید از طریق فراندوم یا همه‌پرسی اتخاذ کرد. به بیانی دیگر، دموکراسی مستقیم بر دموکراسی پارلمانی و نمایندگی برتری دارد. حامیان این نظر، فرصت‌هایی که فناوری‌های اطلاعاتی و ارتباطی برای برپایی نظرسنجی‌ها و فراندوم‌های تلفنی و از راه دور ایجاد می‌کند و نیز فناوری ایجاد گروه‌های مباحثه اینترنتی را جالب توجه می‌یابند. از این رو، اغلب گفته می‌شود فناوری‌های جدید، دموکراسی مستقیم را به همان شکلی که در آگوراهای آنتی جریان داشت، زنده می‌کنند. اصطلاح "دموکراسی از راه دور"^{۱۴} از واژه‌های برساخته مدافعان این مدل است.^{۱۵} دموکراسی از راه دور به آن معناست که شهروندان و سازمان‌های اجتماعی می‌توانند از راه دور و با استفاده از فناوری‌های اطلاعاتی و ارتباطی، رخدادهای جاری در مرکز نظام سیاسی را تعیین کنند.

نظر دیگر، "دموکراسی تکثرگرا" است. در این نظر، شکل‌گیری افکار عمومی درون و میان سازمان‌ها اهمیت دارد. دموکراسی محصول اراده اکثریت نیست، بلکه حاصل ائتلاف‌های همه در حال تغییر اقلیت است. مهم‌ترین ارزش تکثرگرایی در بحث‌های اجتماعی و سیاسی و در حوزه رسانه‌هاست. این مدل از دموکراسی ترکیبی از دموکراسی مستقیم و نمایندگی است، چرا که کار نمایندگی مختص سیاستمداران نیست و بر عهده سازمان‌های اجتماعی هم هست. فناوری‌های اطلاعاتی و ارتباطی فرصت‌های بی‌شماری را برای تکثرگرایی در بحث‌های عمومی و از جمله بحث‌های اینترنتی فراهم می‌آورد.

نظر پنجم، "دموکراسی مشارکتی" است. حامیان این نظر، در پی اجتماعی کردن امور سیاسی هستند و شهروندان را به فعالیت و کسب توانایی‌های بیشتر تشویق می‌کنند. در این نظر، شکل‌گیری بیشترین حد ممکن از آگاهی سیاسی و ترکیب خاصی از دموکراسی مستقیم و نمایندگی اهمیت دارد. مهم‌ترین ابزارهای این مدل بحث‌های عمومی و مشارکت عمومی شهروندان است. اگر رسانه‌های جدید می‌خواهند نقش مثبتی در بهینه‌سازی این ابزارها داشته باشند، باید در دسترس همگان باشند.

آخرین نظر پیرامون دموکراسی، در میان پیشگامان عرصه اینترنت، مدلی مسلط است. این بدان معنا نیست که نظرهای سیاسی پشت این مدل، همگی جدید و تازه‌اند. بسیاری از ناظران، قرابت و نزدیکی میان پیشگامان اینترنت و جنبش‌های بنیادین اجتماعی دهه‌های ۱۹۶۰ و ۱۹۷۰ کشورهای غربی را متذکر شده‌اند. این نظرها، گستره‌ای از آنارشیسم کلاسیک تا سوسیالیسم چپ‌گرا و همه

اشکال آزادی گرای ۱۶ را شامل می شود. این جریان آخر، در دهه ۱۹۹۰ میلادی بیشترین اهمیت را یافت. نظر آزادخواهان از بسیاری جهات شبیه نظرات تکثرگرایان و همه پرسیان است و در آن به فرصت های تشکیل اجتماعات (مجازی)، نظرسنجی از راه دور و مباحثات از راه دور توجه شده است. یکی از ویژگی های خاص آزادی گرای، تاکید بر سیاست مستقل شهروندان در انجمن هایشان است که با استفاده از فناوری های جدید اطلاعاتی و ارتباطی و به ویژه اینترنت بهتر شکل می گیرد. در تندترین صورت بندی از این الگو، سیاست رسمی و نهادی در نهایت منسوخ خواهد شد و جای خود را به واقعیت های سیاسی جدیدی خواهد داد که در شبکه ها ساخته می شود. بنابراین نظر، مساله مهمی که باید مورد توجه قرار گیرد آن است که مرکز گرای، دیوان سالاری، و ارتجاع سیاست رسمی در وضعیتی هستند که انتظارات را بر آورده نمی سازند و نمی توانند بسیاری از معضلات مهم جامعه مدرن را حل کنند. ترکیبی از دموکراسی اینترنتی و اقتصاد بازار آزاد می تواند به عنوان جایگزین مطرح باشد. کاتر این نکته را به خوبی خلاصه کرده است:

در تولد یک ملت دیجیتال، اجتماعی پساسیاسی را توصیف کردم که انسان گرای لیبرالیسم را با پویایی اقتصادی محافظه کاران ترکیب می کند. نوشتم که اعضای این گروه پیوسته تعصبات مداخله جویانه چپ و ایدئولوژی بی مدارای راست را رد می کنند. از سوی دیگر، نشان دادم که شهروندان دیجیتال به عقل گرای بهمی دهند، اقتصاد بازار آزاد و آزادی های مدنی را پاس می دارند و به سوی صورت میانه ای از آزادی گرای گرایش دارند.

کاربردهای رسانه های جدید در نظام های سیاسی

کاربردهای رسانه های جدید در نظام های سیاسی، آن قدر متنوع و متفاوت است که نیاز به تحلیل و مقوله بندی دقیق دارد. در جدول ۱ کاربردهای عمده رسانه های جدید در نظام سیاسی نشان داده شده است. در اینجا این کاربردها را به اختصار شرح می دهیم.

کاربردهای خطابه ای

رسانه های خطابه ای جدید، بهترین معادل رویه های سیاسی جاری را به دست می دهند. در خطابه، مرکز همان عامل تصمیم گیرنده برای اطلاعات سیاسی عرضه شده باقی می ماند، اما برخی عوامل مشورتی و دفتری و ثبتي افزوده می شوند. مرکز می تواند مجموعه ای از مدیریت های سیاسی یا دولتی، یک حزب سیاسی، یک سازمان اجتماعی، یا یک شرکت درگیر با مسائل مربوط به سیاست باشد. این مراکز، نسبت به رسانه های جمعی قدیمی، فرصت های بیشتری را برای انتخاب

و ارسال بازخورد در اختیار مردم قرار می دهند. رسانه های جدید فقط تا حد خاصی تعاملی می شوند. در نتیجه، به تدریج به صورتی به کار می روند که پخش پیام از مرکز الگویی غالب باقی می ماند.

جدول ۱. کاربرد رسانه های جدید در نظام سیاسی

<p>مطبوعات و پخش تعاملی مبارزات انتخاباتی فعالیت های اطلاعاتی حکومت</p>	<p>خطابه ای</p>
<p>نظام های اطلاعات عمومی توده ای نظام های پیشرفته اطلاعات عمومی (اینترنت و غیره) نظام های اطلاعات پارلمانی مراکز اطلاعات خدمات مدنی</p>	<p>مشاوره ای</p>
<p>نظام های ثبتي مدیریت دولتي و حکومت طرح پرسش های شهروندان با استفاده از فناوری نظرسنجی های الکترونیکی رفراندوم های الکترونیکی انتخابات الکترونیکی</p>	<p>ثبت</p>
<p>پست الکترونیک بانک های اطلاعاتی و کنفرانس های از راه دور الکترونیک مطبوعات و پخش تعاملی تصمیمات گروهی برای حمایت از سیستم ها</p>	<p>مکالمه</p>

اولین کاربردها، پخش و مطبوعات تعاملی است. در سال ۱۹۹۸ این شکل از پخش و انتقال فقط در تلویزیون کابلی دو سویه یا تلویزیون ماهواره‌ای و در انتشار روزنامه‌ها و مجلات در اینترنت وجود داشت. این رسانه‌ها دریافت کنندگان و کاربران با علاقه‌های سیاسی را قادر می‌ساخت اطلاعاتی پیرامون سیاست‌ها، احزاب، کاندیداها و غیره دریافت کنند. پخش تعاملی که هنوز دوران اولیه حیات خود را می‌گذراند، مصرف کنندگان را قادر می‌سازد اخبار و برنامه‌های خاص سیاسی را از فهرست انتخاب کنند. اینترنت امکان جست‌وجو در روزنامه‌ها و نشریات را برای مقاصد سیاسی خاصی ارائه می‌دهد و می‌تواند اخبار مورد نظر را به صورت روزانه یا هفتگی به پست الکترونیکی شخصی فرد ارسال کند. با وجود این، هنوز این ارائه‌دهنده اطلاعات است که محتوا را تعیین می‌کند.

آشکار است که این رسانه‌ها تناسب خوبی با مبارزات انتخاباتی و فعالیت‌های سیاسی دارند.^{۱۷} اثر این فعالیت‌ها و مبارزات از وقتی بیشتر شده است که مصرف کنندگان خود درخواست اطلاعات می‌کنند و نمی‌گذارند اطلاعاتی که نمی‌خواهند به آنها تحمیل شود. به علاوه، می‌توان در خصوص این که چه گروه‌های هدفی نسبت به چه تبلیغی واکنش نشان می‌دهند، پژوهشی میدانی به عمل آورد. نظام‌های تلفنی رایانه‌ای، تلویزیون کابلی دوسویه، و اینترنت، به وفور برای نظرسنجی‌های از راه دور به کار می‌روند. عکس‌العمل نسبت به سخنرانی‌ها و مباحثات میان کاندیداها به صورت فوری و همزمان منعکس می‌شود که شکلی از تشویق از راه دور است.^{۱۸}

نظرسنجی‌ها و افکارسنجی‌ها به تدریج شباهت و ارتباط بیشتر و بهتری با بازاریابی‌های مستقیم می‌یابند. یک گروه هدف انتخابی از مردم، به جای تبلیغات، مجموعه‌ای از پرسش‌ها را دریافت می‌کنند که مخصوص این گروه طراحی شده‌اند. تا به حال، این کار از طریق تلفن، نامه، و نوارهای ویدئویی انجام می‌شده است. از این به بعد، اینترنت و پست الکترونیک امکان تماس همزمان و فوری با رای‌دهندگان، اعضا و حامیان بالقوه را فراهم می‌کنند. در آینده‌ای نزدیک، پخش تعاملی یکی از راه‌های اصلی خواهد بود. نتایج بازاریابی مستقیم الکترونیکی در بانک‌های اطلاعاتی عظیم ذخیره می‌شوند. این بانک‌های اطلاعاتی نسبت به نظرسنجی‌های از راه دور، داده‌های دقیق‌تری برای پژوهش‌های قبل از تولید به دست می‌دهند. دست‌آخر، به نظر می‌رسد تبلیغ کنندگان سیاسی از این رسانه‌ها استفاده می‌کنند تا رسانه‌های جمعی را دور بزنند و کانال‌های ویژه خود را برای ارتباط با حامیان خود بسازند.

رسانه های جدید، فرصت های مشابهی برای اطلاعات دولتی فراهم می آورد. استفاده دولت از رسانه های جدید به ظاهر شبیه تبلیغات سیاسی است، اما تفاوت هایی دارد. مدیریت دولتی هم با مردمی طرف است که باید آنها را برانگیزد و بسیج کند و هم با شهروندانی مواجه است که حق دسترسی به اطلاعات خاصی را دارند. این امر را اطلاعات آموزشی حکومت می نامند. در رسانه های جدید، آموزش کلاسیک (جریانی یک سویه) در حال تبدیل به فرآیند جریان اطلاعات (دوسویه) می شود. مدیریت دیگر تنها حزبی نیست که گام اول را برمی دارد. شهروندان با پرسش های خاص خود مدیریت را مخاطب قرار می دهند. گذار به مشورت از اینجا آغاز می شود.

کاربردهای مشورتی

این گذار در نظام اطلاعات دولتی کامل می شود. شهروندان با استفاده از این نظام ها، دیگر مثل نظام های سنتی اطلاعات حکومتی، مجموعه ثابتی از پیام ها را برای جمع بزرگی برنمی گزینند، بلکه پیام های متفاوتی را برای جمع به نسبت کوچکی انتخاب می کنند. صورت دوم بیشتر در نظام های اطلاعات عمومی پیشرفته کاربرد دارد و در نظام های اطلاعات عمومی جمعی کمتر به کار می آیند. نظام های اطلاعات عمومی که اغلب توسط حاکمان شهر تهیه و ارائه می شود، شکلی از پخش برنامه های تلویزیونی و بردهای اطلاعاتی روی ساختمان های عمومی شهر است. در این رسانه ها، اطلاعات مورد علاقه عموم مردم، همچون امور محلی شهروندان، سرگرمی، اخبار، حمل و نقل، و اشتغال ارائه می شود.

نظام اطلاعات عمومی پیشرفته، اطلاعات خیلی بیشتری را نسبت به نظام های توده ای و جمعی ارائه می دهند. البته، کاربران این نظام اطلاعاتی باید پیگیری، قدرت انتخاب، و مهارت های بالایی داشته باشند. اینترنت و محیط های به اصطلاح دیجیتال، مثال های خوبی از این نظام های پیشرفته هستند. به علاوه، این نظام ها کاری بسیار بیشتر از بازیافت اطلاعات انجام می دهند. آنها بسترهای چندکاربره ای هستند که گزینه های متنوعی همچون مباحث محلی و ملی را ارائه می دهند. فقط با در اختیار داشتن برخی مهارت ها و مقداری انگیزه می توان اطلاعات پیچیده و موضوعی زیادی دریافت کرد. در عمل، این رویه، به نخبه گرایی اطلاعاتی مردم علاقه مند به سیاست، نمایندگان حرفه ای، و گروه های ذی نفع می انجامد. به هر حال، هر دو نظام اطلاعات پیشرفته و عمومی، حکومت ها و مدیریت های دولتی و عمومی را در دسترس شهروندان عادی قرار داده است.

حکومت‌ها و مدیریت‌های عمومی هم فرصت دریافت و تبادل اطلاعات را به دست می‌آورند. آنها فقط از این نظام اطلاعات عمومی استفاده نمی‌کنند، بلکه نظام‌های خیلی پیشرفته پارلمانی و مدیریتی خود را هم دارند.

از دیگر کاربردهای رسانه‌های جدید می‌توان به مراکز اطلاعاتی و خدماتی حکومتی اشاره کرد - جاهایی که حجم وسیعی از داده یا خدمات در یک میز مجازی با نظام‌های اطلاعاتی و کارمندان دولت گرد هم می‌آیند. این کاربرد، امکان ارائه خدمات بهتر و وسیع‌تری دارد که بیشتر در اجتماعات محلی نمود می‌یابد. یک شهروند، دیگر از یک نهاد به نهادی دیگر فرستاده نمی‌شود و همه خدمات اطلاعاتی و مبادلاتی دولت، به عنوان مثال در خصوص املاک، در نظام گردآوری می‌شود.

کارکردهای ثبتي

انسجام عرضه اطلاعات و خدمات دولتی نیاز به وجود نظام‌های وسیع و به هم مرتبطی از قبیل ثبت مشخصات پایه، افراد و کالاها و ثبت بخش‌ها برای اجرای امور خاص دولتی و حکومتی است. ثبت مشخصات پایه در برگیرنده مواردی همچون ثبت جمعیت، ثبت دارایی، تامین اجتماعی، و ثبت تملیکات است. ثبت بخش‌ها را می‌توان از جمله در پلیس، خدمات اجتماعی، امور مسکن، و خدمات پزشکی یافت. این ثبت‌ها اهمیت سیاسی زیادی دارند و در رابطه میان دولت و شهروندان از اهمیت بیشتری نسبت به اموری همچون اینترنت برخوردارند. اگرچه اینترنت در شکل دهی به افکار عمومی نقش خیلی برجسته‌ای دارد اما واقعیت آن است که نظام ثبت دولتی مبتنی بر فناوری‌های اطلاعاتی و ارتباطی، اهمیت خیلی بیشتری در مقوله‌هایی از جنس حقوق شهروندی دارند. بنا بر نظر یک دانشمند مدیریت دولتی:

رشد اینترنت با همه جذابیت‌های درونی خودش، در حاشیه قدرت صورت می‌گیرد. در عین حال، در مرکز قدرت، فرایند وسیع‌تر و نظام‌مندتری از پردازش و عرضه اطلاعات شکل می‌گیرد که فایل‌های رایانه‌ای را با داده‌های شخصی مرتبط می‌سازد و از انواع هوش‌های انسانی و مصنوعی برای افزایش شفافیت شهروندان استفاده می‌کند.^{۱۹}

شهروندان، به ویژه به صورت منفرد، نمی‌توانند با قدرت مجموعه‌های دولتی که شبکه‌های درونی خود را به هم وصل کرده و با شبکه‌های گروهی بیرونی هم‌گره خورده‌اند، برابری کنند. به همین خاطر، حقوق شهروندان، همچون حق حریم خصوصی و حق دریافت خدمات دولتی، همیشه در معرض خطر قرار دارد.

شاید بتوان گفت که رسانه‌های جدید، مردم را وادار به دادن اطلاعات بیشتر به دولت می‌کند و نه برعکس. تحقیق و تفحص‌ها و رفراندوم‌های الکترونیکی هم چنین وضعیتی دارند. رسانه‌های جدید روش‌های پژوهشی جدیدی همچون مطالعات پایه الکترونیک، بررسی کیفیت خدمات دولتی، و نظر سنجی را ممکن ساخته است.

انتخابات و رفراندوم الکترونیکی از مناقشه برانگیزترین کاربردهاست که اغلب در زمره ابزارهای لازم برای تحقق مدل دموکراسی مستقیم قرار می‌گیرد. البته در مواردی همچون دستگاه‌های رای‌گیری الکترونیکی و رفراندوم‌های مشورتی (و نه تصمیمی) می‌تواند در زمره امور و مسائل جاری در دموکراسی نمایندگی هم باشد. به هر حال، به علت عدم دسترسی همگان از خانه و عدم حمایت همگانی، رای‌گیری‌های رسمی الکترونیکی و رفراندوم‌های از خانه، به این زودی مورد استفاده قرار نخواهند گرفت. اما بدیهی است که همه نظر سنجی‌های الکترونیک انجام شده به صورت مستقل توسط رسانه‌ها و سازمان‌ها همچنان بر نمایندگان سیاسی و مدیران اثر خواهند داشت.

کاربردهای مکالماتی

فرصت‌هایی که رسانه‌های جدید برای ایجاد و بهبود ارتباطات میان شهروندان و دولت فراهم می‌آورد، سروصدای زیادی برپا کرده است. گفته می‌شود این رسانه‌ها فاصله فرضی میان سیاست و شهروندی را پیر کرده است. پست الکترونیک یکی از بدیهی‌ترین راه‌حل‌هاست. می‌توان از این ابزار برای ارسال نامه به سیاستمداران و مدیران استفاده کرد. به علاوه، اینترنت ابزار بسیار مناسبی برای واکنش شهروندان نسبت به نظرهای سیاسی و اسناد منتشر شده در اینترنت است. با استفاده از این رسانه، دسترس‌پذیری سیاستمداران و کارمندان دولتی افزایش می‌یابد. اما برای جلب توجه بهتر و بیشتر حاکمان نسبت به این رسانه، باید کیفیت و ضوابط اخلاقی حاکم بر آن - مثل مواردی از قبیل هرزنامه - بهبود یابد.

مباحثات الکترونیک، به عنوان جایگزین یا مکمل‌های بالقوه‌ای برای گردهم‌آیی‌های الکترونیک به حساب می‌آیند. در این مباحثات، گروه‌ها و افراد می‌توانند در فرایند شکل‌دهی به افکار عمومی در جامعه مدنی و فرایندهای تصمیم‌گیری و تصمیم‌سازی در امور دولتی شرکت کنند. مورد اخیر را تصمیم‌گیری تعاملی می‌نامند. در اواخر دهه ۱۹۹۰ صدها هزار گروه مباحثه و گروه‌های خبری در اینترنت ظاهر شد. وقتی سیاست‌های جدیدی باید اتخاذ شود، برخی مقامات

محلی و ادارات دولتی در سطح ملی، مباحثات الکترونیکی را در میان شهروندان برپا می کنند. مساله جدی آن است که این مباحثات الزاما به اجماع یا نتیجه نمی رسد. به علاوه، مشارکت صورتی ناپایدار و نامتوازن دارد؛ شدت و عمق مشارکت تغییر می کند و در عمل دسترسی به جمعی از علاقه مندان سیاسی و نخبگان اطلاعاتی و آموزشی محدود می شود. در زمان نگارش این قطعه، مورد قابل توجهی از مباحثات الکترونیکی موثر بر سیاست های رسمی مشاهده نشده است.

مطبوعات و پخش تعاملی هم می توانند مباحثات سیاسی را سازمان دهی کنند. گردهم آبی های سالن مجازی شهر در تلویزیون پخش می شوند و صفحات مباحثه در روزنامه های الکترونیکی باز می شوند و بینندگان و خوانندگان می توانند به صورت مستقیم و از طریق تلویزیون کابلی دوسویه، تلفن، یا اینترنت، به سئوال پاسخ دهند.

پیشرفته ترین کاربردهای مکالمات سیاسی، نظام هایی هستند که به کار تصمیم گیری می آیند و به آن کمک می کنند. کاربر پس از چند دور مذاکره، با پاسخ به پرسشنامه ها می تواند انتخابی خاص، تصمیمی برای رای و یا نتیجه ای متفاوت را اعلام کند. بانک های اطلاعاتی، الگوها، پرسش های طراحی شده در این سیستم، انتخاب های نهایی را هدایت می کنند.

نگارنده این اثر در دموکراسی دیجیتال به این نتیجه رسید که رسانه های جدید با استفاده از ابزارها و کاربردهایی که توصیف شد، تغییرات مهمی را در نظام های سیاسی ما ایجاد خواهد کرد، اما انقلابی را سبب نخواهد شد. این تغییرات، صورتی از گسترش و تعمیق سیاست است که پیش از این توصیف شد. به نظر نمی رسد که رسانه های جدید میزان مشارکت شهروندان در نظام سیاسی را افزایش دهند. هیچ راه حل فنی "ساده ای" برای رفع بی انگیزگی سیاسی وجود ندارد. بسیاری از صاحب نظران بر این باورند که امکان مشارکت در فرایندهای سیاسی در هر زمان و مکان، باعث شکسته شدن موانع خواهد شد. این امر در مورد افراد معلول و بیمار و کسانی که ساعات کاری نامنظمی دارند صادق است. از سوی دیگر، موانع جدیدی در برابر کسانی که به رسانه های جدید دسترسی ندارند و کسانی که نمی دانند چگونه با آن کار کنند ایجاد می شود.

قدرت در سازمان

در گفتارهای پیشین شرح داده شد که چگونه می توان از شبکه ها برای تغییر ساختار کلان سازمان های (بزرگ) تجاری استفاده کرد. آشکار شد که این شبکه ها ترکیبی از قدرت، اقتصاد و کنترل متمرکز و تولید و اجرای غیر متمرکز را تقویت می کنند. در سطحی پایین تر از ساختار کلان

سازمان‌ها، شبکه‌ها می‌توانند بر تشکیل بخش‌ها و گروه‌ها اثر بگذارند. ساختار موازی بخش‌ها در الگوی تولید "ژاپنی" پیش از این مورد بحث واقع شد. چنین ساختاری موازی یا ساختارهای مشابهی از قبیل ساختار بخشی و سازمان‌های ماتریسی به کار رفته در "گروه‌های پروژه‌ای" ۲۰ ساختار کلاسیک، بخش‌های کاری را مهجور خواهند کرد. تا همین اواخر، این ساختار ویژگی بارز همه سازمان‌های دیوان‌سالار بوده است. یعنی، سازمان‌های دیوان‌سالار کارکردهای مشابه را در یک بخش قرار می‌داده و به عبارتی بخش‌ها را وادار به استقلال و ایجاد لایه‌های کنترل درونی برای خود می‌کرده است. شبکه‌ها فرصت ارتباط و وحدت دوباره میان بخش‌ها را فراهم می‌آورد. کارها را می‌توان در ایستگاه‌های چند کاربری یا پایانه‌های متصل به یکدیگر، تلفیق کرد. هر ساختاری که فرد انتخاب کند، استفاده از شبکه به معنای نیاز به تعادل بخشیدن به کارها و کارکردهای درون و میان بخش‌هاست. این انسجام کارکردی بر ساختارهای سازمانی کنونی تاثیر خواهد داشت. در گذشته، بسیاری از مدیران این اثر را دست کم گرفتند و بر این باور بودند که فناوری شبکه‌ای تنها یک مرحله از توسعه سازمان است.

با ظهور شبکه‌ها هم ساختارهای کلان و هم ساختارهای درونی سازمان‌ها، به صورتی بنیادین تغییر می‌کنند. در اینجا بحث خود را به تغییرات مدیریتی محدود می‌کنیم. در گفتارهای قبلی نشان دادیم که دیوان‌سالاری به جای آن که منبع نوآوری باشد، مانعی بر سر راه سازمان است. فناوری‌های اطلاعاتی و ارتباطی با مدرن کردن دیوان‌سالاری می‌توانند این مانع را برطرف کنند. بنا به نظر ماکس وبر، دیوان‌سالاری پنج مشخصه دارد:

۱. سلسله مراتب اقتدار
۲. تمرکز تصمیم‌گیری
۳. صورت رسمی قوانین
۴. تخصصی شدن کارها
۵. استاندارد شدن کنش‌ها

استفاده از فناوری‌های اطلاعاتی و ارتباطی باعث محو این ویژگی‌ها نمی‌شود. برعکس، این ویژگی‌ها در این فناوری جمع شده‌اند. فریسن^{۲۱} روابط نزدیک میان دیوان‌سالاری و فناوری‌های اطلاعاتی و ارتباطی را نشان داده است. این امر در مورد سه ویژگی که در اینجا عنوان شد، آشکار است. در مقایسه با فنون قدیمی، فناوری‌های جدید فرصت‌های خیلی بهتری برای رسمی شدن

قوانین، تخصصی شدن کارها، و استاندارد شدن کنش‌ها فراهم آورده است. رویه‌های قدیمی و سنتی در برنامه‌های نرم‌افزاری و حتی سخت‌افزارهای رایانه‌ای و شبکه‌ای به صورتی رسمی به کار می‌روند. راه‌حل‌های غیررسمی تا حد امکان اجازه بروز نمی‌یابند. مردم پیش از گذشته به کارهای خاص خود محدود می‌شوند چرا که می‌دانند هر کاری که انجام دهند ثبت می‌شود. دست‌آخر، استفاده از رایانه‌ها و شبکه‌ها به استاندارد شدن وسیع کنش‌ها می‌انجامد. هر چه باشد، استفاده از آنها به معنای وجود رویه‌های ثابت و ظریف و انجام تنظیمات دقیق قبل از آغاز همکاری با شبکه است.

در مورد دو مشخصه اول، رابطه میان دیوان‌سالاری و فناوری‌های اطلاعاتی و ارتباطی وضوح کمتری دارد. بسیاری چنین می‌پندارند از آنجا که توزیع کارکردهای شبکه نیاز به سلسله‌مراتب و تمرکز کمتر در فرایندهای تصمیم‌گیری دارد، فناوری‌های اطلاعاتی و ارتباطی سازمان‌ها را در نهایت "مسطح" می‌کند. از این رو، این دو ویژگی نیاز به بررسی بیشتر دارد.

زورموند^{۲۲} پس از مطالعه تعدادی از ادارات ارائه‌دهنده خدمات دولتی و عمومی هلند به این نتیجه رسیده است که سلسله‌مراتب، تمرکز، امور صوری، و تخصص در این ادارات در حال کاهش است. از برخی جهات، این سازمان‌ها "مسطح" تر شده‌اند. در سطوح مختلف، کارهای تیمی و گروهی بیشتری انجام می‌شود. کارمندان دولت دیگر همه مراحل را ثبت و یادداشت نمی‌کنند. آنها مسئولیت‌های شغلی وسیع‌تری به دست آورده‌اند. حتی ویژگی پنجم دیوان‌سالاری که استانداردسازی باشد، انتخاب شده است. کارمندان، در حدود خاصی، اجازه دارند کارهای آزمایشی انجام دهند. البته حدود این آزادی کاری را رایانه‌ها تعیین می‌کنند. به کارکنان فرصت‌های تصمیم‌گیری کمتری نسبت به قبل داده می‌شود. زورموند با تاکید بسیار اعلام می‌کند که فناوری‌های اطلاعاتی و ارتباطی، علی‌رغم نیاز به رویه‌های دیوان‌سالاری حداقلی، کنترل (مرکزی) بر سازمان را تقویت می‌کنند:

به این ترتیب، یک سازمان می‌تواند ساختارهای افقی بیشتری بسازد، سطوح سلسله‌مراتبی را از رده خارج کند، نقاط کنترل را حذف کند و نظام‌های کاغذخور را کاهش دهد، که معماری اطلاعات می‌تواند همه این کارها را انجام دهد. به ویژه، هماهنگی برنامه‌ای و ارتباطات عادی، جای خود را به نظام‌های اطلاعاتی می‌دهند. مدیریت دیگر مجبور به کنترل این هماهنگی‌ها و ارتباطات نیست؛ رویه‌های خیلی دقیقی که برای هدایت این نظام‌ها طراحی شده‌اند، اجازه دارند

نابدید" شوند. حالا همه آنها در درون سیستم جدید هستند.

پس، بخش اصلی کارهای مدیریت سنتی در فنون اطلاعاتی انسجام یافته اند. مدیریت مدرن این فنون را انتخاب و هدایت می کند. زورموند این نوع مدیریت را "اطلاعات سالاری" می نامد و آن را جایگزین و مرحله پیشرفته دیوان سالاری می داند.

این ادعا که کنترل مرکزی بر سازمان ها در حال افزایش است و رویه های سلسله مراتبی و دیوان سالارانه در حال کاهش است، به نظر متناقض می آید. معنای آن چیست؟ برای توصیف بهتر این فرایند باید در زیر ساخت های سازمانی، میان ابعاد زیر تمایز قائل شویم:

۱. ساختار کنترل، وضع قوانین، و هماهنگی اطلاعات درون و میان لایه های سازمانی
۲. ساختار اقتدار در تعدادی از لایه های سازمانی مورد نیاز در سلسله مراتب و هماهنگی
۳. تقسیم کار برای توزیع کارکردها و کارهای درون سازمان

کنترل

کنترل تصمیمات در شبکه ها باید نیازهای زیادی را برآورده سازد. هم باتمركز و هم با تمرکز دایی می توان این نیازها را برآورده ساخت. میتمرکزگ ۳۳ میان بعد افقی (درون یک سطح سازمانی) و بعد عمودی (میان سطوح سازمانی) تمایز قائل می شود. با کاربرد این مفاهیم در اینجا، صورت های احتمالی زیر ظاهر می شود:

۱. تمرکز افقی: بالاترین سطح مدیریت کنترل کامل را در دست می گیرد و مهم ترین تصمیم ها از نظر کارکنان عضو دور نگه داشته می شوند. کار کارکنان شکل دادن به شبکه های اطلاعاتی و ایجاد گزینه های قابل مدیریت است.

۲. تمرکز دایی افقی: فرایندهای پیچیده اطلاعاتی به کارکنان، اقتدار بیشتری در امر مدیریت سازمان می دهد؛ ساختار به اصطلاح خطی (مدیریت)، بخشی از دامنه نفوذ خود را به ساختارهای جدید فنی می دهد.

۳. تمرکز عمودی: لایه های بالایی مدیریت تصمیمات را با استفاده از استاندارد سازی، صوری سازی، و روال های معمول، از سطوح پایین تر مدیریتی و حتی از کارمندان پایه می گیرند؛ در نتیجه، خط کوتاه تر شده و بخش هایی از مدیریت میانی مازاد و بی فایده می شوند.

۴. تمرکز دایی عمودی: استاندارد سازی، صوری سازی، و افزایش روال های معمولی، انتقال سریع تر قدرت تصمیم گیری به سطوح عملیاتی را ممکن می سازد. این مشخصه ها امکان واکنش

سریع تر و دقیق تری به تغییرات در محیط شرکت را فراهم می آورند.

قابل توجه است که همه چهار گرایش به لحاظ فنی می توانند در محیط های شبکه ای به کار بیفتند. این که کدام گرایش غالب شود، به تعادل قدرت درون سازمان، به نوع و اندازه سازمان، به تنوع درونی آن، و به میزان رایانه ای شدن آن بستگی دارد. در اداره هایی که تاکنون استفاده کمی از اتوماسیون داشته اند، احتمال افزایش تمرکز بیشتری وجود دارد. اما بیشتر سازمان ها با ترکیبی از چهار گرایش توصیف شده مواجه خواهند شد. امکان تحقق یافتن تمرکززایی افقی و عمودی بیشتر است.

اقتدار

رشد و توسعه ساختار سازمانی را می توان با وضوح بیشتری شاهد بود. همگان می دانند که با ظهور شبکه ها، تعداد سطوح سلسله مراتب کاهش می یابد. "خود" شبکه برخی از کارهای نظارت و هماهنگی پرسنل را انجام می دهد. بخشی از نظارت و هماهنگی جای خود را به کارکردهای شبکه می دهند. کار باقی مانده برای ناظران و هماهنگ کنندگان، به جای هماهنگی و نظارت پرسنل، مراقبت و نگهداری از شبکه است. مدیریت میانی و پایینی، بخشی از اقتدار خود را از یک سو به سطوح بالایی مدیریتی و کارکنان و از سوی دیگر به کاربران رایانه ها و شبکه می سپارند. بسیاری از مردم با مشاهده این جریان ها به این نتیجه رسیده اند که سازمان ها مسطح تر می شوند. اما با مشاهده دقیق تر به نظر می رسد که چنین چیزی کمتر رخ می دهد. شاید بهتر باشد که گفته شود خط میان بالا و مبنا کمرنگ شده است. فاصله ای که ارتباط باید بر کند در حال کاهش است، و کنترل و اقتدار تفاوتی نکرده است.

این ایده را می توان با قیاسی تمثیلی روشن کرد. سازمانی را فرض کنید که پیش از این ساختاری گلدان مانند داشت و حال ساختار آن همچون ساعتی شنی است که با همان اندازه قبلی، کمری باریک و پایه ای بزرگ تر از راس دارد. این تمثیل مربوط به بحث های مشهوری است که میان دو نگرش جریان دارد: در یک سو، آنهایی که بر ظهور گروه روزافزونی از کارشناسان نخبه اطلاعاتی تاکید دارند و آنها را توسعه دهنده کارهای جدید می دانند، و در سوی دیگر، آنهایی که بر فضای دوقطبی میان کارهای کارمندی و مدیریتی در سازمان تاکید دارند. نحوه ظهور شبکه ها در زمان نگارش این اثر - یعنی حذف مدیریت میانی، افزایش قدرت تصمیم گیری راهبردی و حقوق مدیریت عالی (شاید کوچکتر)، در ضمن کاهش قدرت و هزینه های مخزن کارکنان منعطف و روبه رشد

تولید- نشان می دهد که گرایش دوم بیشتر جریان دارد. ۳۴ این موضوع را به تفصیل بررسی خواهیم کرد.

تقسیم کار

می توان از گرایش به سوی دوقطبی سازی فضا اجتناب کرد. این نظر را می توان با این تجربه توجیه کرد که در ساخت شبکه ها، تقسیم کار درون سازمان ها، همان طور که می توانند به تلفیق کارها (توسعه کارها و حتی غنی سازی کارها) بینجامند، می توانند به تخصصی شدن کارها (تقسیم کار و حتی کاهش کارها) منتهی شوند. همان طور که پیش از این اشاره شد، استفاده از فناوری های اطلاعاتی و ارتباطی احتمال تلفیق کارها را افزایش می دهد. گشودن مجموعه متکثری از کارها در یک پایانه ممکن می شود. به علاوه، مبادلات کاری انجام می شوند: هر کسی می تواند برای مدتی جای دیگری را بگیرد. فناوری به افزایش درجه انعطاف سازمان کمک خواهد کرد. با دیدن امور از این زاویه، متوجه خواهیم شد که کارها گسترش می یابد. غنی شدن کارها بیشتر بستگی به درجه قدرت، آموزش، و آزادی عملی دارد که کارکنان مربوط در برنامه ها دارند. استانداردها سازی و برنامه ریزی رایانه ای نیروهای کاری یا فکری، بدون تغییر در سیاست های تقسیم کار درون سازمان، بیشتر به تضعیف و فرسایش کارها می انجامد. گسترش کار برای جبران این ضایعه است.

البته همین فناوری های شبکه ای می تواند در سازمان های صنعتی و مدیریتی به تقسیم کار بینجامد: در برنامه هایی که عملکردهای خاصی را برای هر کار تعیین می کنند، کارها خیلی دقیق تر از قبل استاندارد می شوند. نظام رایانه ای ثبت دسترسی به این امر را کنترل می کند. در نتیجه، خود سیستم، نظارت بر رویه های تجویزی را برعهده می گیرد.

همه اینها نشان می دهد که فنون شبکه ای خنثی نیستند. برای مثال در بحث معماری شبکه، مسائل طراحی همه چیز را تعیین می کنند. از این رو، بیابید نگاه دقیق تری به گزینه های فنی در ساخت شبکه ها بیندازیم. مهم ترین پرسش ها در این خصوص عبارتند از:

۱. ظرفیت های اصلی پردازش در موقعیت مرکزی قرار خواهد گرفت یا محلی؟
 ۲. آیا ایستگاه های کاری به صورت مستقیم به رایانه های مرکزی وصل خواهند بود؟
 ۳. در شبکه چه کسی اجازه دارد با چه کسی و پیرامون چه موضوعی ارتباط داشته باشد؟
 ۴. کدام برنامه ها و فایل ها را گروه های مختلف پرسنلی به کار خواهند برد؟
- پاسخ بیشتر این پرسش ها را نوع و وضع فنی شبکه تعیین می کند که در ساخت و سازمان

لايه های ارتباطی آن برنامه ریزی شده است.

نوع شبکه دربرگیرنده گونه های زیر است:

۱. پردازش متمرکز در برابر توزیعی
۲. نظام های چندکاربره (مثل شبکه های رایانه ای) در برابر شبکه های رایانه های شخصی
۳. ایستگاه های کاری خرفت در برابر هوشمند
۴. ایستگاه های کاری خیلی تخصصی و هوشمند در برابر ایستگاه های کاری رایانه های شخصی با تخصص پایین تر و چندکارکردی.

گزینه اول در هر مورد بهترین تناسب را با تمرکز عمودی و تقسیم دقیق کار دارد؛ گزینه دوم با تمرکززدایی عمودی و گسترش و تعمیق کارها تناسب دارد. انقلاب میکروالکترونیک "پردازش توزیعی" داده ها را ممکن ساخته است. به خاطر مینیاتوری شدن و کاهش شدید قیمت قطعات، سازمان ها می توانند از ظرفیت های پردازشی محلی استفاده کنند. حالا کنترل در سازمان را می توان خیلی بهتر از روزهای خوش رایانه های بزرگ و متمرکز مین فریم تقسیم کرد. در طول ۱۵ سال گذشته، انتقال قابل توجهی از رایانه های مین فریم به شبکه های رایانه های کوچک، شبکه های با دسترسی محلی، و شبکه رایانه های شخصی صورت گرفته است. البته، ظهور رایانه های شبکه ای می تواند شکل جدیدی از تمرکز را باعث شود.

یکی از رایج ترین گزینه ها، استفاده از نظام های چندکاربره (که در آن چندین کاربر از امکانات و برنامه های یک رایانه بزرگ استفاده می کنند) به جای استفاده از شبکه رایانه های شخصی (که در آن هر رایانه ظرفیت ها و برنامه های خاص خود را دارد) است. تمایل سازمان به قدرت را شاید بتوان در انتخابش میان شبکه رایانه ای و رایانه های شخصی، یا در گزینه سوم شبکه رایانه های شخصی دید.

با وجود این، مهم ترین گزینه انتخابی، میزان "هوش" موجود سخت افزارها و نرم افزارهای هر ایستگاه کاری است. هر ایستگاه می تواند طیف وسیعی از گزینه ها - از پایانه ای "خرفت" که به درد ورود اطلاعات می خورد تا ایستگاه با هوش بالا - برای پردازش اطلاعات علمی باشد.

دست آخر، مشخصه چندکارکردی یا تک کارکردی یک ایستگاه کاری، تقسیم کاری آن را تعیین می کند. این مساله بیشتر به نرم افزارهای موجود در ایستگاه بستگی دارد.

موقعیت شبکه هم در امور قدرت و ارتباطات سازمان ها اهمیت دارد. به آسانی می توان دریافت

که ساختاری ستاره‌ای، مثل موردی که در سیستم مین فریم به کار رفته است، قدرت را متمرکز می‌کند. ساختار حلقه‌ای و ساختار گذرگاهی که در شبکه‌های محلی رواج زیادی دارند، طرح و کارکردی ساختارزدایی شده دارند. ساختار توری که امکان ارتباط مستقیم میان همه پایانه‌ها را می‌دهد، و نمونه خوب آن را می‌توان در شبکه‌های مخابراتی و تلفنی و اینترنتی دید. ساختارزدایی شده است. اما میزان و پیچیدگی شبکه‌های توری آن قدر عظیم است که گره‌های مرکزی مجبور به تنظیم ترافیک است. دیگر آن که این پیش‌نیازهای فنی با اولویت‌ها و اقتدارهای ارتباطی بسط یابد، بیشتر به ماهیت شبکه توری بستگی دارد که محل مبادلات (سازمانی) دولتی یا خصوصی باشد. ساختارهای گذرگاهی و حلقه‌ای در شبکه‌های محلی امکان ارتباط همه ایستگاه‌ها با یکدیگر را فراهم می‌آورند. اما اینجا هم، مدیریت شبکه، توانایی توقیف دسترسی به ایستگاه‌های خاص را دارد و از این طریق اولویت‌های ارتباطی را مشخص کرده، نظام‌های خود را تحمیل می‌کند. البته این قوانین می‌توانند یک شبه تغییر کنند.

حریم خصوصی و استقلال شخصی

از اینجا به سطح فرد می‌رسیم. استفاده از شبکه‌ها می‌تواند پیامدهای عمده‌ای در میزان قدرت افراد داشته باشد. حریم خصوصی آنها و استقلال شخصی آنها می‌تواند نقض شود. البته آنها می‌توانند از همین فنون برای حفاظت از خود و افزایش دایره انتخاب خود استفاده کنند.

میان حریم خصوصی و استقلال شخصی تمایزی وجود دارد. حریم خصوصی، یک آزادی است و بیش از آن که به گروه‌ها و سازمان‌ها ربطی داشته باشد، آزادی افراد است. استقلال شخصی، مشخصه‌ای از روابط فرد با دیگران است که فرصت‌های فرد برای کسب و صیانت از آزادی را تعیین می‌کند. استقلال شخصی مترادف با قدرت فرد است. اینجا آزادی به معنای آزادی در انتخاب و کنترل، برای مثال در حوزه فناوری‌های اطلاعاتی و ارتباطی است. حریم خصوصی پیش‌نیاز استقلال شخصی است. بدون آزادی کلی فرد، هر شکلی از آزادی انتخاب محدود است. از این رو، این بخش را با بحث پیرامون حریم خصوصی آغاز می‌کنیم. اول، معنای حریم خصوصی شرح داده خواهد شد. بعد، مخاطرات و تهدیدهای ناشی از فناوری‌های اطلاعاتی و ارتباطی بررسی می‌شود. در نهایت، امکانات موجود برای حفظ حریم خصوصی مورد توجه قرار خواهد گرفت.

حریم خصوصی چیست؟

”حریم خصوصی“ مفهومی انتزاعی است که می‌تواند بر چیزهای زیادی دلالت داشته باشد.

این مفهوم آن قدر ناملموس است که بسیاری از مردم اهمیت آن را در نمی‌یابند. از جمله توصیف‌های عامه می‌توان به این موارد اشاره کرد: "حریم خصوصی، حق فرد برای تعیین میزان در معرض دید دیگران قرار گرفتن است" یا "حریم خصوصی حق تنها ماندن و خلوت گزیدن است". اما یک تعریف قابل توجیه علمی، باید بر اساس مفاهیم و مقولات موجود در نظریه‌های حقوقی، تاریخ و یا علوم اجتماعی باشد.

پژوهش‌های تاریخی و انسان‌شناختی نشان داده است که نیاز به حریم خصوصی می‌تواند عام باشد، اما ساختار و وضعیت نهایی آن بستگی به ساختار محیط زیست فرد و فرهنگ اجتماع دارد. (پاورقی) برینگتون مور در پایان یک پژوهش تاریخی تطبیقی وسیع به این نتیجه رسید که نیاز به حریم خصوصی، به معنای نیاز به جدا کردن رفتارهای فردی شخص، خلوت گزیدن‌های گه‌گاهی، و نشان ندادن برخی رفتارها و عقاید به جامعه یا گروه، نیازی عام و جهانی است. البته در رویه‌های تاریخی، این نیاز بنا به نظر مور در ذیل فناوری‌های و سازمان‌های بدوی اجتماعی تعریف شده است. در این مجال می‌خواهم این نکته را بیفزایم که در پایان قرن بیستم خود فرد در ذیل سازمان‌ها و فناوری‌های پیشرفته اجتماعی تولید می‌شوند در نظریه حقوق، حریم خصوصی حق آزادی خاصی است. حریم خصوصی حق عدم دخالت در زندگی خصوصی است. نابین و ون دولیتگاردن حتی تا آن جا پیش رفته‌اند که این حق را "آزادی نهایی" نامیده‌اند که باید به اجتماع تفویض شده یا در مقایسه با دیگر منافع قرار گیرد.

هولمز یکی از فیلسوفان اجتماعی است که از نظر مایکی از بهترین تعریف‌ها را ارائه کرده است: "آزادی راه ورود به حوزه‌هایی از زندگی فرد که به صورت ضمنی یا آشکار در برابر دیگران گشوده نیست." در این تعریف از حریم خصوصی و بسیاری تعاریف دیگر، ابعاد فضایی و اطلاعاتی مطرح است. حریم خصوصی درباره خلوت مکانی در حوزه‌های خاص است که از بدن و محیط مستقیم آن (زندگی خصوصی) آغاز می‌شود و نباید مورد مداخله قرار گیرد. علاوه بر این، مراحل پردازش اطلاعات در بیشتر تعاریف وجود دارد: درک، ثبت، و آشکار سازی ویژگی‌ها و رفتار فرد.

بنابه نظر پستین، همیشه میان حریم خصوصی رابطه‌ای و اطلاعاتی تمایزی وجود دارد. با آن که مشاهده خواهیم کرد که این دو نوع حریم خصوصی به ویژه در بستر شبکه‌ها با هم ترکیب می‌شوند، آن را جدی می‌گیریم و حتی نوع سومی هم به آن می‌افزاییم: حریم خصوصی جسمی؛ در واقع بدن و محیط فیزیکی بلافاصله آن حوزه نهایی حریم خصوصی است. این مهم‌ترین دلیلی است

که تجاوز به عنف به عنوان یکی از مهم ترین موارد نقض حریم خصوصی مطرح می شود. حریم خصوصی فیزیکی و جسمی به معنای حق صمیمیت انتخابی است. این به معنای نقض ناپذیری بدن و ارضای نیازهای انسانی است که به حضور تعداد کمی از افراد برگزیده یا عدم حضور کسی منتهی می شود و به نظر می رسد، رابطه مستقیمی با فناوری های اطلاعاتی و ارتباطی نداشته باشد. اما واقعیت آن است که فناوری های زیستی و فناوری های اطلاعاتی با هم ترکیب می شوند. مهم ترین رابطه میان این اطلاعات ژن حیات یا همان دی ان ای (DNA) است. نمودارگیری از همه ژن های انسانی و نگهداری آزمایش های دی ان ای رابطه بسیار نزدیکی با ثبت اطلاعات فردی دارد. به نظر می رسد در آینده دی ان ای مهم ترین داده های شخصی را تولید کند. این داده ها با استفاده از فناوری های اطلاعاتی و ارتباطی ثبت خواهند شد و از این ابزار برای مرتبط ساختن داده های دی ان ای و دیگر داده های شخصی استفاده خواهد شد.

یکی دیگر از تهدیدهای حریم خصوصی جسمی بیومتری است که بیش از هر چیز در تشخیص هویت (مثل تشخیص چشم، چهره، اثر انگشت، و صدا) و مبادی ورودی ها (حس گرایی که بر روی بدن نصب می شوند) به کار می روند. به عنوان مثال می توان به دوربین های آنالوگ و دیجیتال ویدئویی که به حوزه های خصوصی و فیزیکی زندگی فرد وارد می شوند، اشاره کرد. مثلاً مواردی مشاهده شده است که کارفرمایان میزان دستشویی رفتن کارکنان خود را چک می کرده اند.

در بیشتر اوقات دوربین های کنترل، بر روابط صمیمانه انتخابی اثر می گذارند. این امر بیشتر در مورد رفتارها و روابط در حوزه (نیمه) خصوصی فرد، در منزل، ماشین، محل کار است. توانایی تعیین روابط و رفتارهای شخصی بدون مشاهده یا دخالت دیگران، یکی از موارد بنیادی حق آزادی است.

حق استفاده از شبکه های ارتباطی و نظام های اطلاعاتی برای ثبت رفتارها و روابط فرد از راه دور می تواند در معرض تهدید قرار گیرد. دستگیری الکترونیکی در خانه و دوربین های موجود در مکان های نیمه عمومی مثال های خوبی از ثبت رفتار فرد است. ثبت دیجیتالی مکالمات تلفنی و پیگیری شماره های تلفن، صندوق پست های الکترونیک و آدرس های اینترنتی مثال های دیگری از ثبت روابط هستند.

آخرین شکل حریم خصوصی، حریم خصوصی اطلاعاتی است یعنی حق آشکار ساختن

انتخابی. در مفهومی بدوی، این نوع از حریم خصوصی به قدمت بشر (غیبت) یا نوشتار (اولین ثبت‌ها) است. اما با ظهور فناوری‌های جدید موضوعیت آن به شدت افزایش یافته است. حریم خصوصی اطلاعاتی پیرامون حوزه‌هایی است که فرد پیرامون داده‌های شخصی و تصمیمات مرتبط با داده‌های خود دارد. متأسفانه مفهوم داده شخصی، مفاهیم مشترک حریم خصوصی را محدود کرده است. حفظ حریم خصوصی جای خود را به حفظ داده‌های شخصی داده است و حتی گاه به مفهوم امنیت این داده‌ها محدودتر می‌شود. بدیهی است که در این گفتارها به حریم خصوصی اطلاعاتی می‌پردازیم اما در عین حال سعی می‌کنیم مهم‌ترین عناصر حریم خصوصی رابطه‌ای و جسمی را تا حد امکان در نظر داشته باشیم. جمع این سه نوع حریم خصوصی را توصیف خواهیم کرد. برای مثال واژه "تعقیب‌پذیری" و "شفافیت" که در بخش‌های آتی به کار خواهد رفت رابطه نزدیک میان حریم خصوصی رابطه‌ای، اطلاعاتی و جسمی را نشان می‌دهد.

تهدیدهای حریم خصوصی

ظهور شبکه‌های بیش و پیش از همه مراحل توسعه فناوری‌های اطلاعاتی، باعث ایجاد مخاطرات و تهدیدهایی در برابر حریم خصوصی شده است. آشکارترین تهدیدها در رابطه با حریم خصوصی اطلاعاتی هستند اما وقتی فضای مکانی و فیزیکی زندگی شخصی گشوده می‌شود، حریم خصوصی رابطه‌ای و جسمی هم به مخاطره می‌افتند. خطر تعقیب‌پذیری همه کنش‌های کاربران شبکه‌های عمومی چیزی است که بیشترین ترس را در میان مردم ایجاد کرده است. سیر رشد چنین سرویس‌هایی در تاریخ نشان می‌دهد که این خطر واقعی می‌شود. برای مثال خدمات اقتصادی و مالی از فرایندی گذشته‌اند که از ضرب و انتشار سکه آغاز شده است. از چک و اوراق بهادار گذر کرده و به پرداخت‌های الکترونیکی انجامیده است. در طول این مسیر، ارائه‌دهندگان خدمات اطلاعات روز افزونی را پیرامون مشتریان خود گردآورده‌اند. در مبادلات الکترونیکی، بانک نسبت به اطلاعات دقیق مکان، زمان و ماهیت مبادله اطلاع دارد و مشتری فهرستی از این داده‌ها را دریافت می‌کند. در خدمات مبادلاتی، تغییر مشابهی از چک به ثبت در حال رخ دادن است. ثبت‌کننده‌های هوشمند چک، پایانه‌های فروش، سفارش‌های خریدی الکترونیکی، و رزروهای مختلف اطلاعات و جزئیات خیلی بیشتری درباره مشتری ثبت می‌شود. این فرصتی طلایی برای پژوهش در بازار و تبلیغات است. در اینترنت، همه مراحل کسب اطلاعات و خدمات مکالمه‌ای را فناوری‌های موسوم به "پیگیر" ثبت می‌کنند. مدیران سایت‌ها اگر بخواهند می‌توانند همه ورودها و همه کلیک‌های زده

شده در سایت خود را چک کنند. برای هر قدم برداشته شده در اینترنت یک "فایل گزارشی" ۲۵ وجود دارد. فایل های گزارشی از مجموعه ارقام بزرگی تشکیل شده اند که اطلاعاتی پیرامون رایانه، کاوشگر اینترنت، و کشور محل استفاده را ثبت کرده اند. به تدریج، سخت افزارهایی همچون پردازشگرها و سی پی یوها و نرم افزارهایی همچون پردازشگران متن و تصویر، شماره های اختصاصی و حتی نام کاربران خود را درج می کنند. اغلب، آدرس پست الکترونیکی کاربران به این اطلاعات افزوده می شود. این اطلاعات، فایل های گزارشی را تبدیل به مجموعه ای از اطلاعات شخصی می کند. تحلیل این گزارش ها بدون برنامه های پیشرفته کار بسیار دشواری است. به همین خاطر، اغلب از ابزاری ثانویه استفاده شده و برای کاربر یک "گوکی" ۲۶ غیر مشهود ارسال می شود. یک فایل کوچک حاوی اطلاعات مراجعه کننده به سایت به صورت خودکار ایجاد شده و نسخه ای از آن خارج از نظر کاربر در رایانه او ذخیره می شود. هر بار که کاربر به یک سایت خاص مراجعه کند، آن فایل به صورت خودکار دوباره نوشته می شود. به این ترتیب، پس از مدتی، پرونده کاربر تشکیل می شود. همه این وقایع بدون اطلاع و آگاهی کاربر رخ می دهد. کاربران قبل از استفاده از یک سرویس خاص، هر شکلی از پرسش نامه را پر می کنند. اغلب کاربران بی خبرند و نمی دانند که این پرسش نامه ها پرونده آنها را کامل تر می کند.

آشکار است که خدمات مشاوره و ثبت، بیشترین خطر را در برابر حریم خصوصی ایجاد کرده است چرا که در پشت این خدمات، مراکزی هستند که گرسنه اطلاعات فردی اند. اما با ظهور شبکه های ارتباطات دیجیتال و با استفاده از نرم افزارهای ثبت، حریم خصوصی در مکالمات غیر متمرکز هم در خطر قرار دارد. برای مثال، ضبط و خواندن نامه های الکترونیکی یک نفر، به نسبت ساده است. این خطر از مردمی که به مرکز ثبت وارد می شوند (مثل هکرها) ناشی نمی شود. مسائل و خطرهای اصلی در خود مرکز تولید می شود. برای مثال، مدیران ممکن است بخواهند (بتوانند) همه نامه های الکترونیکی کارمندان خود را بخوانند - گرچه آنها فقط با چک کردن آدرس های مورد مراجعه و سرویس های مورد استفاده ارضا می شوند. همان طور که نقش مبادلات مرکزی در مکالمات غیر متمرکز رشد می کند، ظرفیت این چک کردن ها هم افزایش می یابد. در مبادلات الکترونیکی کنترل شده با نرم افزار مدت و هزینه ارتباط و تعداد ارسال کنندگان و دریافت کنندگان همیشه ثبت می شود.

ملاحظه بعدی، استفاده از شماره مشترک در شبکه های دیجیتال است. این فناوری با استفاده

از تجهیزات تلفن دیجیتال آسان شده است. در این خصوص ثبت هویت تماس گیرنده اهمیت زیادی دارد. با استفاده از فناوری های مختلف، شماره تماس گیرنده ثبت می شود. این فناوری ها، از زمان ظهور تلفن های خودکار، امکان تماس های ناخواسته و مزاحم های تلفنی را به حداقل رسانیده است. حال سرویس های اورژانس کافی است به شماره بنگرند و به آدرس بروند.

از جمله مهم ترین معایب این فناوری آن است که مشترک به صورت خودکار شماره خود را ارائه می دهد. افراد بازاریاب و بخش تجاری و سازمان های امنیتی می توانند این شماره ها را برای تهیه بانک های اطلاعاتی سفارشی مورد استفاده صحیح یا غلط قرار دهند. آنها می توانند بفهمند چه کسی در چه زمانی، برای چه مدتی و به چه منظوری تماس گرفته و همه این موارد را ثبت کنند. آنها با استفاده از نرم افزارهای پیشرفته، اطلاعات زیادی را از این داده ها استخراج می کنند. به علاوه، شرکت ها و افراد می توانند فهرستی از شماره ها را برای پذیرش یا طرد وارد کنند. حال کارفرمایان می توانند تعیین کنند کارمندان شان با چه کسانی تماس بگیرند یا نگیرند. یکی از معایب این سیستم ضرری است که متوجه تلفن های ناشناس برای کمک یا پژوهش می شود. اعتماد به تلفن های ناشناس کاهش خواهد یافت.

تا جایی که به صیانت از حریم خصوصی مربوط است، فناوری های تشخیص هویت تلفنی مزایا و معایبی دارد. امکان رد یا متوقف کردن این سرویس، اهمیتی حیاتی دارد اما وجود این گزینه ها نباید از ترس ما بکاهد. برای مثال، در بسیاری مواقع گیرندگان مجبور به توجه خود برای فرستندگان می شوند که اجازه دسترسی نداده اند، یا شماره خود را نشان نداده اند، یا در مورد تلفن های تصویری، خود را نشان نداده اند. گزینه های امتناع فنی، در صورت وجود، همیشه وابسته به روابط فردی و اجتماعی و از جمله روابط قدرت است.

از اینجا به مخاطرات حریم خصوصی رابطه ای می رسیم. در همه فناوری های ارتباطی، کششی به سوی "دسترسی در هر زمان و مکان" وجود دارد. اگر تجهیزات جدیدی از قبیل منشی های تلفنی و پیام گیرهای صوتی، این امکان را به خوبی فراهم نکرده اند، تلفن های همراه در این جهت حرکت کرده اند. تقاضاهای فراوان برای این فناوری ها نشان می دهد، مردم به ارتباطات پیوسته عادت کرده اند؛ در عین حال، این فناوری ها، افراد را در جامعه و در همه محیط ها قابل ردگیری می کند. تقریباً هر فضایی تبدیل به فضایی اجتماعی می شود. سخت است که بتواند در هر زمان و مکانی در دسترس بود. و حتی اگر فرد بتوان گزینه های بلوک کننده را فعال کند، شانسی

توجیه خود کاهش می‌یابد. این امر خطری برای استقلال فردی است (در این زمینه بحث خواهیم کرد). فضای طبیعی ما برای پس کشیدن (گرچه این فضا توزیع اجتماعی خوبی نشده است) و برای خلوت گزیدن کوچک و کوچک تر می‌شود. با وجود این، فضاهای جدید برای تاثیر و کارایی ارتباطات مفید است. در همه زمان‌ها و مکان‌ها، در دسترس بودن باعث خواهد شد کمیت ارتباطات اهمیت خود را (تقریباً) از دست بدهد.

شبکه‌های رایانه‌ای هم فضاهای زندگی شخصی در خانه و ماشین و هم فضاهای اختصاصی در محیط‌های اجتماعی را باز کرده است. این امر منحصر به مکان‌های خاصی است که افراد باید در برابر یک رایانه یا پایانه کار کنند. در این خصوص مدیر می‌تواند هم دستاوردهای کارمندان و هم رفتار و حرکت‌های او را پیگیری کند. حرکت آزاد در بخش، ساختمان، یا کوچه و خیابان پیگیری و ثبت می‌شود. از طریق کارت‌های عبور مختلف تقریباً می‌توان همه حرکات را کنترل کرد. حتی استفاده از رایانه‌ها و تلفن‌های همراه را هم می‌توان با تجهیزات راداری و ماهواره‌ای کنترل کرد. استفاده از کنفرانس‌های از راه دور از قبیل کنفرانس‌های ویدئویی رایانه‌ها و شبکه‌های رایانه‌ای مجهز به دوربین، با آنکه منافع زیادی دارد، تهدید بالقوه جدیدی برای حریم خصوصی کارمندان است. در کنفرانس‌های ویدئویی علاوه بر سخنرانی‌های رسمی، هر حرکت یا تبادل اطلاعات میان شرکت کنندگان ثبت می‌شود. گروه‌های دیگر و مخاطبان می‌توانند خیلی بیشتر از نشست‌های سنتی، اطلاعات دریافت کنند، چرا که نوار ضبط شده را می‌توان بارها و بارها دید. آنجا که رایانه‌ها و دوربین‌ها مشغولند، مدیران می‌توانند حضور و نوع کار انجام شده را کنترل کنند. البته تجهیزات فنی برای مسدود کردن این گزینه‌ها هم وجود دارد. به هر حال استفاده از این گزینه‌ها به تعادل میان کارفرمایان و کارکنان بستگی دارد. به صورت کلی، مدیریت و فناوری حق انتخاب از تباط کارمندان را تعیین می‌کنند. برخی مدیران و کارفرمایان هیچ حقی را برای حریم خصوصی، در هنگام کار به رسمیت نمی‌شناسند. به هر حال، فضاهای خصوصی در محیط کار جای خود را به فضاهای جمعی ترمی دهند.

تهدید دیگر حریم خصوصی استقرار ارتباط میان داده‌هایی است که در صورت استفاده مجزا ضرری ندارند. فناوری‌های اطلاعاتی به روش‌های گوناگون می‌توانند میان داده‌های شخصی درون و میان پرونده‌ها ارتباط برقرار کنند. اول، روابط درون پرونده‌ها و فایل‌ها را بررسی می‌کنیم. بعد به روابط میان فایل‌ها که "پیوند" یا "اتصال" نام دارد خواهیم پرداخت.

بسیاری از فایل های بانک اطلاعاتی برای استقرار ارتباط میان ثبت جدول های منفرد از مشخصه ها شکل گرفته اند. اطلاعات پیرامون افراد در اینجا تولید می شود. به عنوان مرحله بعدی، برای مطالعه اجمالی همه ثبت ها و جدول ها یا بخشی از آن، بانک های اطلاعاتی تشکیل می شود. به همین خاطر، اطلاعات راهبردی درباره گروه ها یا افراد، برای مثال از طریق تعقیب گروه های مختلف مردم در زمان های متفاوت گردآوری می شود. در بسیاری از موارد، اطلاعات را می توان تا سطح فرد پیگیری کرد. این داده ها از چندین منبع تهیه شده و در یک بانک اطلاعاتی بزرگ گردآوری می شوند. این داده های گردآوری شده "داده خانه" نام دارد. پر کردن داده خانه ها با حجم بالایی از اطلاعات و برای استفاده در زمینه های مختلف، صنعت مستقلی شده است.

مرحله بعدی کاوش در داده هاست؛ استخراج داده و اطلاعات احتمالاً موجود، ناشناخته و بالقوه کارآمد. فنون جدیدی برای جست و جو ابداع شده است که مبتنی بر ترکیبی از آمار و هوش مصنوعی است و توسط رایانه های پر قدرتی که به صورت موازی و در شبکه های عصبی به هم وصل شده اند اجرا می شود.

داده خانه ها و کاوش در داده ها، اطلاعات راهبردی مهمی را پیرامون افراد تولید می کنند. افراد درگیر اغلب نسبت به این فرآیندها آگاهی نداشته اند. آنها کارهای روزمره خود را انجام می داده اند اما آثار خود را در هر جا به جای گذاشته اند. برای مثال از کارت های اعتباری خود استفاده می کرده اند و فرم های پاسخنانه را پر می کرده اند. در مسابقات تلویزیونی شرکت می کرده اند و هیچوقت فکر نمی کرده اند که اعمال آن ها ثبت می شود. به یکباره همه این اطلاعات مثل یک بومرنگ به فرد باز می گردد. نهادهای زیادی وجود دارند که اطلاعات شگفت آور و زیادی را پیرامون افراد دارند و به نظر می رسد می توانند هر تصمیمی پیرامون افراد، کارمندان و شهروندان بگیرند. این دانش می تواند به پیشنهادات جالبی بینجامد و در عین حال می تواند عامل رد شدن مصاحبه شکلی، در دریافت وام و در دریافت تخفیف مالیات شود.

در تولید رابطه میان داده ها به روش های مختلف، امکانات بیشتری ظاهر می شود. این فرایند را "پیوند پرونده ها" می نامند و می تواند به مقایسه ساده پرونده ها، محدود مانده و یا تا استفاده از فنون جست و جوی پیشرفته گسترش یابد. ساده ترین این روش ها مقایسه اول و آخر است. برای مثال، وقتی فردی درخواست تسهیلات اقتصادی می کند، اطلاعات ارائه شده توسط این فرد در هر مورد خاص باید مورد تایید بانک های اطلاعاتی قرار گیرد. ثبت های جمعیتی چک می شود تا معلوم

شود فرد مذکور چه وضعیتی دارد و به پرونده های امنیتی مراجعه می شود تا معلوم شود که آیا فرد مذکور شغلی دارد یا خدماتی دریافت نکرده است. از این راه، اطلاعات تکمیلی را می توان درباره یک فرد به دست آورد.

تکنیک بعدی مقایسه نظام مند پرونده هاست. در فرایند تطبیق پرونده ها کلی پرونده پس از تکمیل مقایسه می شوند. موردی که با بقیه تطابق داشته یا نداشته باشد، بسته به این که منظور از مقایسه پرونده ها چیست، "هدف" نام دارد. از این روش برای پیگیری خطاهای موجود در یک پرونده یا شناسایی موارد کلاهبرداری و خطاهای فردی استفاده می شود. البته بدیهی است که از این فن هم می توان در مقاصد غیر مشروعی همچون بازاریابی تجاری یا حتی جنایی استفاده کرد.

ترکیب دو یا چند پرونده می تواند به انسجام کامل پرونده ها در یک پرونده بینجامد. انسجام می تواند به ایجاد پروفایل برای هر فرد یا "سازمان و گروه" کمک کند. این پروفایل ها با استفاده از آمار و روان شناسی رفتاری تهیه شده اند و بر اساس آن می توان تخمین زد که یک نفر با مشخصات خاص می تواند کار خاصی را انجام دهد. (پاورقی)

این پروفایل ها اهمیت بیشتر و بیشتری در نظام های اطلاعات شخصی و در نظام های اطلاعات مدیریتی و بازاریابی دارند. در همه این نظام ها، فاصله زیادی میان داده های ترکیبی و منبع وجود دارد، در واقع در ترکیب داده ها، داده های جدیدی ایجاد می شوند که اغلب هدف متفاوتی با اهداف ثبت اولیه دارد و "بلافاصله به عنوان اطلاعات تلقی و تفسیر می شوند. فرد درگیر به ندرت از این تفسیرها و کاربردهای جدید اطلاع می یابد. این اطلاعات راهبردی است. با وجود این اشتباهات و خطاهای زیادی رخ می دهد.

گنگی و ابهام نهفته در ترکیب و تفسیر پرونده ها در شبکه ها، به این معناست که فاصله میان واقعیت افراد، داده های پیرامون این افراد و تصمیمات اتخاذی پیرامون آن ها در حال افزایش است، به همین نسبت اثر افراد بر این فرآیند در حال کاهش است.

دفاع از حریم خصوصی

ظهور شبکه ها بدون اقدامات تامینی به خطرهای جدی در حوزه حریم خصوصی می انجامد. لازم نیست مبتلا به "دیگر هراسی" باشیم که به چنین نتیجه ای برسیم. کاربردهای ارائه شده توسط شبکه ها توجه افراد سیاسی و بازاری را به شدت جلب کرده است. و ما حتی درباره ظهور ناخوشایند

مدیریت توتالیتری که زیر ساخت های لازم را یافته است، صحبت نمی کنیم. برای اولین بار در تاریخ، مرحله شبکه ای در رایانه ای کردن، کم و بیش یادآور "جامعه برادر بزرگ" شده است که ویژگی بارز آن کنترل پذیری و قابلیت گسترده افراد است. تفاوت در اینجا است که ما بایک "برادر بزرگ" منفرد مواجه نیستیم و به جای آن مجموعه فراگیری از "برادرهای کوچک" داریم. به علاوه اغلب با نظارت مستقیم از طریق مانیتورها و تلویزیون های مدار بسته و دوربین های فیلم برداری مواجه نیستیم و به صورت غیر مستقیم تعقیب شده و کنترل می شویم. به هر حال این روش همان کارآیی و تاثیرات را دارد زیرا (الف) می تواند مبتنی بر داده ها و اطلاعات خلاصه شده باشد و (ب) قربانیان هیچ اطلاعی از آن ندارند و از این رو همیشه احساس می کنند که تحت تعقیبند و نسبت به آن بی تفاوت می شوند.

خوشبختانه راه های زیادی هم برای صیانت از حریم خصوصی در شبکه ها وجود دارد. این راه ها را می توان در چهار مقوله خلاصه کرد:

۱- حفاظت حقوقی

۲- حفاظت اجتماعی: امتناع یا مشارکت در عرضه فنون و خدمات جدید به وسیله

مصرف کنندگان و شیوه های ابداعی تولید کنندگان

۳- حفاظت سازمانی و فنی سیستم

۴- جایگزین های فنی

تا به حال گزینه های ۱ و ۳ بیشترین توجه را دریافت کرده اند، اما بنا به تحلیلی که در پی می آید در کوتاه مدت گزینه های ۲ و ۴ حفاظت بیشتری را تامین می کنند.

صیانت حقوقی از حریم خصوصی در شبکه های رسانه ای، یک چارچوب لازم و مبنای دیگر صورت های حفاظت از حریم خصوصی است. متأسفانه حفاظت حقوقی هنوز خیلی ابتدایی و ناکافی است. تقریباً همه کشورها در جهان حق حریم خصوصی را در قانون اساسی یا یک قانون دیگر تصریح کرده اند (پاورقی) در سال ۱۹۹۵ فقط ۱۱۰ کشور صیانت از حریم خصوصی را در قانون اساسی خود پیش بینی کرده بودند و ۵۵ کشور شکلی از قانون حریم خصوصی را داشتند (پاورقی). هر کشور می تواند در سه سطح، قانون حریم خصوصی داشته باشد: قانون اساسی، قانون خاص حریم خصوصی و قانون عمومی (قانون عمومی قانونی است که به جای مکتوب بودن بر تصمیم قضات و دادگاه ها مبتنی است). حفاظت قانونی از حریم خصوصی ناکافی است و این امر به ویژه



در حوزه شبکه‌ها شدیدتر است. دلایل این عدم کفایت را مرور می‌کنیم:

اول، قانون‌گذاری در حوزه حریم خصوصی در سطح پایینی از رشد و اثر است. قانون‌های اساسی خیلی وسیع نوشته شده‌اند و تضمین‌های اجرایی بی‌واسطه و بی‌مناقشه‌ای ندارند. در آمریکا آن بخشی از قانون اساسی که به این موضوع ارتباط دارد، یعنی اصل چهارم، هم خیلی وسیع و هم خیلی محدود است. در این قانون از فرد و حریم خصوصی او در برابر دخالت‌های دولتی حمایت شده است. از سوی دیگر قوانین حریم خصوصی خیلی محدود هستند. برای مثال، در آمریکا مجموعه جالبی از قوانین حریم خصوصی در سطوح فدرال و ایالتی تصویب شده است (پاورقی) این امر به از هم گسیختگی کامل وضع قوانین حریم خصوصی منجر شده است، که باعث تضعیف آن شده و فقط قضات با تجربه می‌توانند با آن کار کنند. در سوی دیگر، اتحادیه اروپایی، قانون جامع و خیلی دقیقی برای حریم خصوصی وضع کرده است و برای تشکیل آن از همه اصول و هدایت‌های شورای اروپا استفاده کرده است. اما اجرای قانون جامع حریم خصوصی اروپا، تلاش‌ها و پشتیبانی اجتماعی فراوانی را می‌طلبد، تا آنجا که اجرای آن دشوار شده است. به علاوه، نمی‌توان آثار قوانین حریم خصوصی را تضمین کرد چرا که داده‌های شخصی از مرزهایی گذرانده می‌شوند که هر یک قوانین خاص خود را دارند و وضع قوانین، منزلت به نسبت پایینی دارد: حریم خصوصی بیشتر در زمره حقوق مدنی و حقوق عمومی قرار می‌گیرد و کمتر به عنوان حقوق جزایی تعریف شده است. از این رو، تنبیه و مجازات به خاطر نقض حریم خصوصی کمتر رخ می‌دهد.

از اینجا به دلیل دوم می‌رسیم. حریم خصوصی به عنوان حق مطلق فرد مطرح نیست. همیشه این حق را در مناسبت با حقوق و قوانین، به ویژه آزادی اطلاعات و ارتباطات دیگران و حقوق امنیتی دولت می‌سنجند. در عمل، وضع قوانین حریم خصوصی به شدت تحت تاثیر قوانین دیگر و به ویژه مسائلی همچون امنیت ملی و قوانین اضطراری قرار دارد.

سومین ضعف حفاظت از حریم خصوصی آن است که هنوز به صورت انحصاری به حریم خصوصی اطلاعات می‌پردازد. همیشه مساله حفاظت از "اطلاعات" مطرح است. این در حالی است که فناوری‌های اطلاعاتی و ارتباطی به صورت عام و شبکه‌های رسانه‌ای به صورت خاص، هر روز به میزان بیشتری وارد حوزه‌های ارتباطی و جسمی حریم خصوصی می‌شوند. در نتیجه، کاربردهایی از قبیل پست الکترونیک، تعیین هویت تماس گیرنده تلفنی، نظارت‌های ویدیویی با

امکانات ذخیره سازی، و همه گونه های استفاده از رسانه های جدید برای نظارت، همچون استفاده از اینترنت، به خوبی مورد حفاظت واقع نشده اند. حریم خصوصی جسمی هم چنین وضعی دارد و می تواند با استفاده از فنون بیومترسی و آزمایش دی ان ای مورد تهدید واقع شود.^{۲۷}

دست آخر، مهم ترین ضعف حفاظت از حریم خصوصی آن است که مثل دیگر قوانین، خیلی بارشده و توسعه فناوری فاصله دارد. برای مثال، قانون حفاظت از اطلاعات هلند، تصویب شده به سال ۱۹۸۹ برای این طراحی شده بود که مسائل حفاظت از حریم خصوصی در رایانه های حاوی اطلاعات شخصی را حل کند. در این قانون، ثبت رایانه ای امری دانسته شده است که ثابت است و می توان به محض مشاهده نسخه ای دیگر، اصالت آن را تشخیص داد و اقامه دعوی کرد. اما در واقعیت جدید، ثبت در محیط های شبکه ای رایانه ای امری پویاست که در حال گردآوری، پردازش، ویرایش، تغییر، مشاوره، کاربری، و انتقال داده ها و اطلاعات است. اتحادیه اروپایی این فرایند پویا را نقطه عزیمت اصلی خود قرار داده و بر این مینا از دولت هلند خواسته است نسبت به تطبیق مناسب قوانین خود اقدام کند. در این ضمن، تغییرات فنی و جدیدی پدید آمده است که همین نقطه عزیمت را هم به چالش می کشد.

ضعف های موجود در وضع قوانین رسمی باعث می شود قوانین خودساخته افراد و گروه های ذی نفع جالب به نظر برسند. بدیهی است که برای جلوگیری از حاکمیت قانون جنگل و هدایت قانون های کوچک، نیاز مبرمی به وضع قوانین مناسب هست. هر چه باشد، قوانین خودساخته به نفع گروه های قدرتمند است. دو شکل از قوانین خودساخته هست: فردی و اجتماعی.

قوانین خودساخته فردی از تلاش هایی تشکیل شده است که کاربران برای حفاظت از حریم خصوصی خود و با استفاده از مهارت ها، کنش ها و ابزارهای فنی در دسترس به عمل می آورند. قوانین خودساخته اجتماعی، قوانینی هستند که در این راه و توسط سازمان های حفاظت از حقوق مصرف کنندگان، گروه های کاربری، اتحادیه های تجاری و غیره به وجود می آیند. این گروه ها فقط می توانند از سوء استفاده های پیشگیری کرده و بعد از عمل انجام شده قادر به کاری نیستند.

ایجاد بدیل های فنی می تواند یکی از بهترین راه حل های فنی برای رفع مسائل مربوط به حریم خصوصی باشد. در واقع، تعداد کمی از دانشمندان و مهندسان از اوایل دهه ۱۹۹۰ در حال کار بر روی ایجاد نظام های جایگزین هستند. آنها کار خود را بر چهار مشخصه شبکه ای زیر گذاشته اند: مقیاس کوچک تر: تمایل به ایجاد شبکه هایی با مقیاس بزرگ و واحد در حال کاهش است. این

شبکه‌ها هم آسیب پذیرند. در عوض، می‌توان تعداد زیادی از شبکه‌های کوچک اما مرتبط به هم را طراحی کرد. با این روش، می‌توان اقدامات امنیتی بیشتری اتخاذ کرد و برای هر یک قوانینی وضع کرد. به علاوه، چند نوع از شبکه‌ها با ثبت هاتی مختلف را می‌توان بدون پیوند دادن پرونده‌ها و فایل‌های موجود در آن، به هم وصل کرد. با این روش، کاربران مورد حمایت بیشتری قرار می‌گیرند.

زیرساختی خالی: یکی از مناقشات مهم در ساخت شبکه‌ها پیرامون این پرسش قرار دارد که آیا باید "هوش" را بیشتر در مرکز شبکه قرار داد یا در پایانه‌های آن؟ در این زمینه، سازندگان شبکه‌ها از نظر اول طرفداری کرده و سازندگان تجهیزات پایانه‌ای نظر دوم را برمی‌گزینند. از منظر حریم خصوصی هم نظر دوم جالب‌تر است. در این نظر امکان دسترسی فرد به اطلاعات کاربردی بیشتر است و اطلاعات به صورت متمرکز و یکجا انباشت نمی‌شود.

تجهیزات مستقل از شبکه: کارآمدترین راه حل برای مسائل مربوط به حریم خصوصی، خاموش کردن مراکز ثبت است. تندترین راه حل، استفاده هرچه بیشتر از تجهیزات مستقل از شبکه است. این راه حل، برای همه مشکلات شبکه‌ها توصیه می‌شود. در این حوزه، مجموعه‌ای از ابزارهای فنی مستقل از شبکه ایجاد شده است.

فناوری‌های تقویت حریم خصوصی: همان فنونی که حریم خصوصی را به مخاطره می‌اندازند را می‌توان برای حفاظت از آن به کار برد. این تجربه که هویت افراد در بخش عظیمی از فرایند ثبت اهمیتی ندارد، مهم‌ترین اصل در این فنون است. به افراد هویت‌های مشابهی داده می‌شود که جایگزین هویت اصلی آنها در فرایند ثبت است. در ثبت با استفاده از نظام‌های فناوری اطلاعات و ارتباطات مراحل زیر پشت سرهم قرار دارند:

۱. اعطای مجوز (اجازه ورود به سیستم)

۲. تشخیص هویت و تایید هویت

۳. کنترل دسترسی (در برخی کاربردها)

۴. حسابرسی (بررسی و توجیه استفاده از سیستم)

۵. حسابداری

مهم‌ترین نتیجه حاصل از چهار ابزار به کار گرفته شده برای حفاظت از حریم خصوصی آن است که هیچ‌یک از آنها را نمی‌توان نادیده گرفت. این ابزارها به یکدیگر نیاز دارند. تشکیل گروه‌های

ابزاری و فنی برای دفاع از حریم خصوصی بار دیگر نشان می دهد که شبکه ها ابزارهای فنی و خنثایی نیستند و به ساختارهای قدرت در جامعه، در سازمان ها و در میان افراد وابسته اند.

استقلال شخصی

وقتی که از بحث حریم خصوصی خارج می شویم و پیرامون استقلال شخصی به تامل می نشینیم، متوجه می شویم که همان نتایج در این حوزه هم صادق است و کاربرد دارد. شبکه ها شخصیتی سیستمی دارند و چند نقطه یا پایانه را به هم وصل می کنند. در این نقاط، انسان هایی کار، زندگی، یا تحصیل می کنند. این گزاره ساده، بنیادی ترین پرسش در خصوص قدرت در شبکه ها را مطرح می کند. تا چه حد افراد در مقام اعضای یک سازمان، در مقام شهروند، کارمند، مشتری، یا مصرف کننده می توانند بیان کنند که به شبکه وصل هستند و وقتی که وصل هستند، چه میزان اثری بر کاربرد شبکه دارند؟

این پرسش ها پیرامون کنترل انسان ها بر ابزارهای فنی خودشان است. به هر حال، شبکه با ماشینی که تصمیم داریم بحریم متفاوت است. شبکه ابزاری مستقل نیست که فعالیت ها و ارتباطات انسانی را جایگزین یا ساده کند. شبکه رسانه ای با مشخصه های سیستمی است و ماشین های مختلف و کاربران انسانی آنها را به هم وصل می کند و جریان کارآمدی از ارتباطات و فعالیت های آنها را به راه می اندازد. کوییک و رولف^{۲۸} نیاز به رویکرد کاملاً متفاوتی برای کار با فناوری شبکه ها را خاطر نشان ساخته اند. رویکرد سنتی به نظر می رسد مدلی "ماشینی" باشد. آثار این ماشین ها را می توان به صورت مستقیم محاسبه کرد و تغییر داد. این مدل دیگر در فناوری شبکه ای کاربرد ندارد. باید یک الگوی سیستمی را جایگزین کرد. الگوی سیستمی هم همه گره ها، ارتباط ها، پروتکل ها، پایانه ها، و برنامه ها را به صورت مجزا بازرسی می کند هم کلیت ترکیبی نظام را در نظر دارد و هم به شرایط اجرایی آنها در فرایندهای سازمانی و اجتماعی جاری نظر دارد. □

این مقاله ترجمه فصل چهارم کتاب زیر است:



بی نویس ها:

- 1.Reach
- 2.see Burnham 1983; Mulghan, 1991; Gandy, 1994; Lyon, 1995; Beniger, 1996.
- 3.Pool, 1983
- 4.Burnham, 1983; Loudon, 1968; Gandy, 1994; Zuurmond, 1994.
- 5.Hacker and van Dijk, forthcoming.
- 6.van Dijk, forthcoming
- 7.Frissen, 1999.
- 8.Guhenno, 1993.
- 9.Guhenno, 1993; Mowshowitz, 1992.
- 10.see Abrahamson et al., 1998.
- 11.van Dijk, 1996; forthcoming
- 12.Newman, 1994; Selnow, 1994.
- 13.Plebiscitary Democracy
- 14.Tele-democracy.
- 15.Arreton, 1987; Barber, 1984; Becker, 1981.
- 16.libertarianism
- 17.see Rash, 1997.
- 18.Selnow, 1994.
- 19.Zuurmond, 1996, originally Dutch.
- 20.see Khandwalla, 1977; Mintzberg, 1993.
- 21.Frissen, 1989.



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

22.Zuurmond, 1994

23.Mintzberg, 1979

24.see Harrison, 1994.

25.log file

26.cookie

27.Davies, 1994

28.Kubicek and Rolf, 1985.



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی