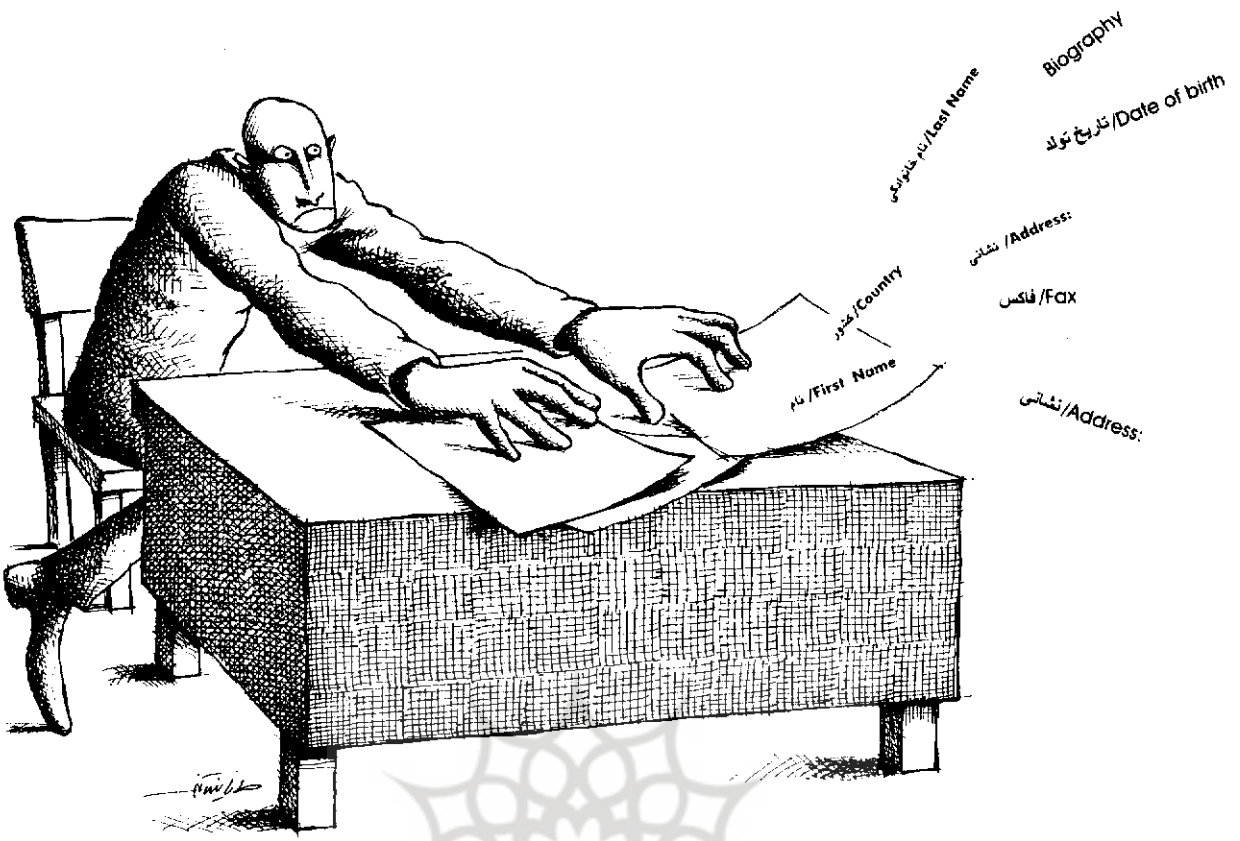


حریم خصوصی افراد در جریان بین‌المللی داده‌ها

ترجمه: حسن نورائی‌بیدخت

۱. فضای پردازش اطلاعات

با کارت اعتباری خود یک دیسک (CD) جدید موسیقی خریده‌اید. سه هفته بعد و از طریق پست، فروش کالاهایی به شما پیشنهاد می‌گردد که با ذائقه و پسندتان انطباق دارد؛ موسیقی، نوشیدنی، اتومبیل و به‌طور کلی انواع کالاهایی که مورد سلیقه شماست. بعد از مدتی درمی‌یابید که شرکت صادرکننده کارت اعتباری شما، گزارش کلیه خریدهایی را که با این کارت انجام داده‌اید به شرکت دیگری که دست‌اندرکار فروش کالا از راه دور است، فروخته است. این شرکت سایر اطلاعاتی را که درباره شما به دست آورده است با سابقه مربوط به عملکرد کارت اعتباری‌تان تلفیق نموده و تمامی اطلاعات مربوط به شما را از طریق یک رشته برنامه‌های کامپیوتری خاص یک‌کاسه کرده و شما را به عنوان فردی که به فلان نوع موسیقی، فلان نوع نوشیدنی و فلان نوع اتومبیل علاقه‌مند است، طبقه‌بندی می‌کند. این کار خوب است یا بد؟ بدون شک، این که انسان بتواند از طریق پست، کالاهای مورد علاقه‌اش را تهیه کند، کار جالبی است.

بعد از چندی متوجه می‌شوید که آنها سابقه پزشکی‌تان را نیز به مجموعه اطلاعاتی که درباره شما دارند، اضافه کرده و همراه با سابقه یا گزارش مربوط به کارت اعتباری‌تان در اختیار کارفرمای شما قرار داده و به عنوان یک خدمت، آن را برای کلیه کارفرمایان بالقوه نیز دست‌یافتنی می‌نمایند. کارفرما نیز با صرف مقداری هزینه، می‌تواند راجع به کمردرد، سابقه بیماری قند (دیابت) در میان اعضای خانوادهٔ شما، و افسردگی‌هایی که در دوره تحصیلات دانشگاهی داشته‌اید، اطلاعاتی به دست آورد. و این ویژگیِ دوره‌ای است که در آن زیست می‌کنیم.

طی ده سال گذشته، قدرت کامپیوتر به‌طور تصاعدی افزایش یافته و یکی از پایدارترین دوره‌های رشد اقتصادی قرن حاضر را رقم زده است. در اکثر موارد، این انقلاب اطلاع‌رسانی جنبه‌ای مثبت داشته است. شبکه‌های ارتباطی نیز همانند تجارت و بازرگانی، به‌طرز فزاینده‌ای

■ ایالات متحده امریکا، بزرگترین کشوری است که با توجه به استانداردهای تعیین شده توسط دستور کار اتحادیه اروپا، سیاست مناسبی در ارتباط با حریم زندگی خصوصی ندارد.

■ اگر سیاستی جهانی در زمینه جابه‌جایی اطلاعات اتخاذ نگردد، حمایت و حفاظت از اطلاعات مربوط به حریم زندگی خصوصی افراد تقریباً غیرممکن خواهد شد.

جهانی شده‌اند. در حال حاضر می‌توان گفت که اخبار و اطلاعات تقریباً در یک آن از یک طرف کره زمین به طرف دیگر آن جریان می‌یابد. محدودیت‌های رسانه‌های چاپی، رفته رفته جای خود را به انفجار شیوه تازه‌ای از انتشار اخبار و اطلاعات بر روی اینترنت می‌دهند. مع‌ذلک، این انقلاب کاملاً مثبت نبوده است. اکنون، اطلاعات و داده‌ها را می‌توان در مقیاس‌هایی حیرت‌انگیز گردآوری کرد، مورد سازماندهی و پردازش قرار داد و به صورت‌های باز هم پیچیده‌تر، به فروش یا فروش مجدد رساند. کامپیوتر جایگزین مجموعه‌ای از بایگان‌ها، ماشین‌نویس‌ها و نظایر آنها گردیده است زیرا قدرت آن در زمینه پردازش هر نوع اطلاعاتی، به مراتب از میزان کاری که گروهی از انسانها می‌توانند انجام دهند، فراتر رفته است. این اطلاعات جدیداً سازمان یافته را می‌توان مورد تحلیل و پردازش قرار داد تا درک و شناخت تازه‌تری درباره داده‌های مزبور حاصل شود، شناختی که ممکن است بعداً مورد خریدوفروش مجدد قرار گیرد. بنابراین می‌توان گفت اطلاعات، امروزه به کالای جدیدی تبدیل شده که دنیا را تکان می‌دهد.

البته این امر پیامدهایی جدی برای آزادی و دموکراسی به دنبال دارد. سازمان‌ها، (ارائه‌دهندگان خدمات اطلاعاتی) غالباً بدون رضایت و شناخت کامل کسانی که اطلاعات به ایشان مربوط می‌گردد، اطلاعات مربوط به زندگی خصوصی‌شان را گردآوری می‌کنند.

همین سازمان‌ها ممکن است پرونده‌های پیچیده‌ای درباره اشخاص مختلف تهیه کرده و اطلاعات خود را در اختیار سازمان‌هایی دیگر قرار دهند که این سازمان‌ها نیز ممکن است به نوبهٔ خود به تشکیل پرونده‌هایی برای آن اشخاص مبادرت ورزند. اگر اطلاعات مزبور به دست افراد و یا سازمان‌های ناباب بیفتد، احتمالاً در جهت اعمال نفوذ درخواسته‌های مشتریان، نابود ساختن بازارهای آزاد و ایجاد یک مرکز جاذبه یا گرانشی برای کسب قدرت مورد استفاده قرار خواهند گرفت. همین چند دهه پیش بود که رایش سوم از این قبیل پرونده‌ها برای ایجاد رعب و وحشت در قارهٔ اروپا استفاده کرد. و البته این کار در عصری انجام می‌گرفت که کارها هنوز ماشینی نشده بود و در نوشتن مطالب از خودنویس استفاده می‌شد. اکنون بیم آن می‌رود که مبادا با استفاده از قدرت کامپیوتر، آزادی‌های به مراتب بیشتری در مخاطره قرار گیرد.

مسأله‌ای که «*سوایر*» (Swire) و «*لیتان*» (Litan) در سال ۱۹۹۸ بدان اشاره کردند به «افشاگری بیش از حد» درباره مشتریان مربوط می‌گردد. بدین معنی که برخی شرکت‌ها ممکن است اطلاعات شخصی یا محرمانه مشتریان را، در مواردی فراتر از آن چه مورد توافق آنان قرار گرفته است، به‌کار گیرند. در حال حاضر، اقدامات یک سازمان در ارتباط با به‌کارگیری اطلاعات شخصی چیزی نیست که اکثر مردم از آن خبردار باشند. میزان پولی که می‌توان از طریق گردآوری و فروش اطلاعات شخصی کسب کرد، انگیزه بزرگی به دست شرکت‌ها و مؤسسات می‌دهد که تا آنجا که مقدورشان باشد، از آن اطلاعات استفاده نمایند. اطلاعات مزبور، غالباً بدون آن که خطر چندانی شرکت‌ها یا مؤسسات ارائه‌کنندهٔ خدمات اطلاعاتی را تهدید کند، مورد استفاده قرار می‌گیرد زیرا برای یک مشتری اغلب دشوار و یا تقریباً غیرممکن است که از سیاست یک شرکت در زمینه اطلاعات شخصی افراد سردر بیاورد.

حتی اگر چنین شرکتی، سیاست خود در زمینه اطلاعات مربوط به حریم شخصی افراد را نیز برملا سازد، باز هم خطر چندانی آن را تهدید نمی‌کند تا مجبور شود سیاست عنوان شده‌اش را دگرگون نماید. به‌طور مثال، چندی پیش یک تأمین‌کننده عمدهٔ اطلاعات اینترنتی، برآن شد تا فهرست مشترکانش را به طرف‌های ثالثی بفروشد که در زمینه بازاریابی از راه دور فعالیت داشتند و این درحالی بود که تأمین‌کننده مزبور اعلام کرده بود؛ دست به چنین کاری نخواهد زد. اگر این قضیه در مطبوعات برملا نشده بود، احتمالاً تنها عده بسیار معدودی از آن باخبر می‌گشتند.

در داخل و خارج دانشکده، درباره آنچه که می‌تواند پاسخ مناسبی به این مسایل باشد، بحث داغی در گرفته است. بسیاری از محققان و پژوهشگران، از قبیل هربرت برکرت (Herbert Burkert) [۱۹۹۸] از راه حلی تکنولوژیک برای مسایل مربوط به حریم زندگی خصوصی افراد طرفداری می‌نماید. از نظر «برکرت» قوانین و مقررات صرفاً حاصل مصالحه‌های سیاسی یک دوره بخصوص است که سپس به صورت قانون در می‌آید. حال آن که فن‌آوری یا تکنولوژی تجسم ارزش‌های جامعه و رویاهای مربوط به چگونگی جهان است. پس فن‌آوری قدرت فرد و نیز قدرت سازمان را تقویت می‌نماید تا حقوق خود را تضمین نمایند. دیگران، از قبیل پیتر *سوایر و رابرت لیتان* (۱۹۹۸) از «خود دیده‌بانی» از طریق تنظیم قراردادهای مطلوب به عنوان یک راه‌حل جانبداری می‌کنند. *سوایر* (۱۹۹۶)

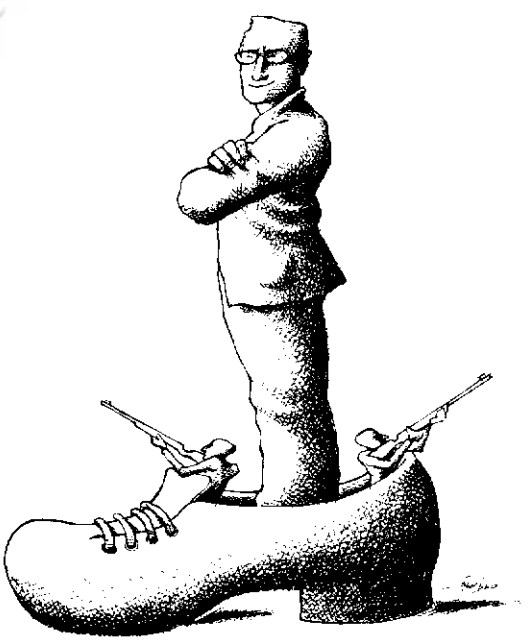
استدلال می‌کند که سه بخش از «خود دیده‌بانی» با تفکیک و جدایی قدرت همطراز است.

در نخستین بخش، یعنی وضع قانون، امر «خود دیده‌بانی» را می‌توان از طریق اعلام قوانین مربوط به حریم زندگی خصوصی و امثال آن برقرار ساخت.

بخش دوم یعنی اجرای قانون را می‌توان از طریق سازمان‌های تخصصی از قبیل انجمن حقوقدانان امریکا و انجمن ملی حقوقدانان، معمول نمود. این انجمن‌ها به عنوان قسمتی از مقررات و فرایندهای خود تا حد گسترده‌ای برکسانی که قانون را به کار می‌بندند و یا بدان عمل نمی‌کنند، نفوذ دارند.

بخش سوم، داوری و حکمیت است که آن را نیز می‌توان به همین ترتیب دراقدامات قانونی این قبیل انجمن‌ها مشاهده کرد. بنابراین، «خود دیده‌بانی» همواره اختیاری نیست بلکه ممکن است از طریق تصمیمات اتخاذ شده در بخش صنایع نیز برای تشکیل نهادهای قانونی انجام پذیرد.

راه حل دیگر، مقررات دولتی است که محققان و کارشناسانی چون سوزان گیندلین (Susan Gindlin، ۱۹۹۷) از آن جانبداری می‌نمایند. *گیندلین* معتقد است که دولت می‌تواند با تصویب یک رشته قوانین و مقررات خاص از حقوق افراد عادی جامعه در محفوظ نگاه داشتن حریم زندگانی خصوصی‌شان، حمایت کند. استدلال گیندلین بیش از همه به مقصود و هدف برنامه کار اتحادیه اروپا نزدیک است.



در این گزارش خلاصه‌ای از برنامه کار اتحادیه اروپا و تحلیلی از مفاهیم آن ارائه شده و در آن، این سیاست تازه با سیاست‌هایی که مناسب برنامه مزبور تشخیص داده نمی‌شود، مورد مقایسه قرار می‌گیرد. بنابراین در یکی از ضمیمه‌های آن گزارشی اجمالی از برخی سیاست‌های ملی در زمینه مسایل مربوط به حریم شخصی افراد وجود خواهد داشت تا نشان دهد که آنها تا چه اندازه با آرمان‌های تعیین شده از سوی اتحادیه اروپا همخوانی و انطباق دارند. به علاوه، در این گزارش اجمالی، تحقیقاتی نیز که اخیراً در خصوص این برنامه کار صورت گرفته است به اختصار مورد بررسی قرار خواهد گرفت.

با توجه به افزایش تقریباً تصاعدی قدرت کامپیوتر در سالهای اخیر، مسأله اصلی که در این برنامه، مطرح شده، نگرانی از شیوه‌های به‌کارگیری اطلاعات کامپیوتری شده است.

سهولت کار گردآوری و نگهداری اطلاعات و داده‌های کامپیوتری، نشانگر تحولی چشمگیر در اهمیت مدیریت اطلاعات شخصی است. علاوه برآن، قابلیت پیوند سیستم‌های کامپیوتری و رشد انفجارآمیز آن، این مسائل را تشدید نیز کرده است.

رشد شبکه‌های جهانی از قبیل اینترنت، راه‌های بسیار متعددی پیش روی انسان قرار می‌دهد که از طریق آن می‌توان اطلاعات را جابه‌جا کرد. بدین‌ترتیب اگر سیاستی جهانی در زمینه جابه‌جایی اطلاعات اتخاذ نگردد، حمایت و حفاظت از اطلاعات مربوط به حریم زندگی خصوصی افراد تقریباً غیرممکن خواهد شد. بنابراین، قابلیت پیوند جهانی سیستم‌های کامپیوتری، نگرانی عمده‌ای در مورد راه‌های انتقال و جابه‌جایی اطلاعات به وجود آورده است که به عنوان محصول جانبی اقدام یک فرد، گردآوری شده و در شبکه جهانی مورد استفاده قرار می‌گیرد.

به علاوه، نگرانی‌های دیگری از بابت بازرگانی ناخواسته الکترونیکی و راه‌هایی که به کمک آن، خصوصی بودن پست الکترونیک و امنیت اطلاعاتی حفاظت می‌گردد، در هسته مرکزی برنامه کار اتحادیه اروپا قرار دارد.

یکی از دلایلی که اتحادیه اروپا باید به منظور حفاظت از قلمرو یا حریم زندگی خصوصی به چنین اقدام یک جانبه‌ای دست بزند آن است که در غیاب سیاستی جهانی برای مدیریت داده‌ها، تعدی و دست‌اندازی به حریم زندگی خصوصی به گونه‌ای عارضی در چند سال آینده افزایش خواهد یافت.

در سطح بین‌المللی به حصول اتفاق‌نظر در مورد اصول بنیادین، نیاز شدیدی احساس می‌شود تا بتوان برمبنای آن، سیاست خاصی برای حفاظت از حریم شخصی افراد اندیشید. چنین اتفاق‌نظری احتمالاً در برداشتن گام دیگری در زمینهٔ حصول توافقنامه‌ها و پیمان‌های بین‌المللی پایدارتر مؤثر خواهد افتاد.

۲. دستورکار اتحادیه اروپا

پارلمان و شورای اروپایی اتحادیه اروپا، روز ۲۳ نوامبر ۱۹۹۵، دستور کار شماره EC-۴۶-۹۵ در مورد حفاظت از افراد در زمینه مالکیت داده‌های شخصی و در زمینهٔ جابه‌جایی این قبیل داده‌ها را به تصویب رساند. این دستور کار کشورهای عضو اتحادیه را مکلف می‌دارد که گردآوری و انتقال داده‌های شخصی نه تنها در درون کشورهای خود بلکه انتقال آنها به دیگر کشورهای عضو اتحادیه اروپا را نیز قانونمند کنند. بدین‌ترتیب، دستور مزبور آتش مجادله‌ای بین‌المللی را برافروخت. مجادله اصلی روی ماده‌های ۲۵ و ۲۶ آن

متمرکز بود که به انتقال داده‌های شخصی به کشورهای غیرعضو اتحادیه مربوط می‌گردید. این اقدام حساب شده‌ای بود که تحولات عظیمی در مقررات و ضوابط مربوط به تجارت بین‌المللی پدید می‌آورد. ماده ۲۵ سابقه تازه‌ای در بازار اطلاع‌رسانی بین‌المللی ایجاد می‌نماید. ماده مزبور تحدید انتقال اطلاعات شخصی به هر کشوری خارج از چارچوب اتحادیه اروپا را، که سیاست مناسبی در مورد حفاظت از حقوق حریم شخصی افراد ندارند، خواستار می‌گردد، ولو این که این درخواست به تجارت بین‌المللی لطمه وارد سازد.

اتحادیه اروپا اعلام داشت که احتمالاً محدودیت‌ها را در روابط تجاری با کشورهایی که معیارها و ضوابط حفاظت از اطلاعات شخصی را رعایت نکنند، اعمال خواهد کرد. این اقدامی است که احتمالاً به منظور واداشتن دیگر کشورهای جهان به پذیرش سیاست واحدی در زمینهٔ امور مربوط به زندگی خصوصی صورت گرفته است. به گفته سیمون دیویس (Simon Davies) [۱۹۹۸]: «اگر حریم شخصی حافظت نشود، تجارت هم از بین خواهد رفت.» این یک قانون قابل توجه و در عین حال هشداری بود به کشورهایی که هنوز سیاستی کلی در راستای حفاظت از اطلاعات شخصی تدوین نکرده بودند. برخلاف آنچه که ممکن است در نگاه اول برداشت شود، هدف از دستورکار مزبور نه متوقف ساختن جریان اطلاعات بلکه تقویت آن از طریق اتخاذ سیاستی یکسان در زمینه رفتار با اطلاعات شخصی در میان تمامی کشورهای عضو اتحادیه اروپا بود. تک تک کشورهای این اتحادیه دیگر نمی‌توانند جریان اطلاعات به سایر کشورهای عضو آن را با شیوه‌های غیرمدون متوقف سازند. با وجود این، اتحادیهٔ اروپا به منظور حفاظت از تلاش‌های آزاداندیشانهٔ خود، ناگزیر از برداشتن گام‌هایی در جهت جلوگیری از ایجاد «پناهگاه‌های اطلاعات» (*سوایر و لیتان*) [۱۹۹۸] در کشورهای غیر عضو اتحادیه اروپاست. این پناهگاهها ممکن است به صورت منابع نقل‌وانتقال غیرقانونی اطلاعات اعضای این اتحادیه در آیند و مواد ۲۵ و ۲۶ به همین دلیل تنظیم شد. در این راستا، اتحادیه اروپا، دست‌اندرکاران تجارت و امور بازرگانی را ناگزیر ساخت تا حقوق شهروندان خود را برتجارت مقدم بدانند.

ولی باهمهٔ آنچه که گفته شد، دستورکار مزبور، موضعی واقعی در برابر تجارت اتخاذ نکرد. دستور مزبور، نظامی به وجود آورد که احتمالاً جریان آزادتر اطلاعات میان کشورهای عضو اتحادیه را باعث خواهد گردید، ولی این کار قبل از هرچیز باید از طریق تضمین حقوق صاحبان آن اطلاعات انجام گیرد. بنابراین دستورکار اتحادیه اروپا دو مفهوم ارزشی را بسط داد:

۱. جریان آزاد اطلاعات؛
۲. حقوق تک تک شهروندان.

کشورها، اغلب از برداشتن گام‌هایی جدی در زمینه حقوق شهروندان ـ به ویژه اگر این امر به جریان آزاد اطلاعات و در نتیجه به عملکرد بازار آزاد لطمه وارد سازد ـ اکراه داشته‌اند. اما دستورکار مزبور برای شرکای تجاری عمدهٔ اروپا، به‌ویژه ایالات متحده امریکا، ژاپن، کانادا و استرالیا ـ که هیچ‌کدام، دارای سیاستی کلی در زمینه حفظ حریم شخصی اشخاص نیستند ـ حاوی این پیام بود که روند موردنظر را دگرگون ساخته است. پیام ارسال شده این بود که حفاظت از حقوق افراد نباید فدای پیشبرد تجارت و امور بازرگانی شود. دستورکار مزبور حاوی این پیام نیز بود که اتحادیه اروپا حاضر است به منظور تضمین این حقوق، اقداماتی معمول دارد (*گیندلین*، ۱۹۹۷). اگرچه تجارت در زمینه هرنوع اطلاعات، از جمله اطلاعات و داده‌های شخصی، روز به روز افزایش یافته و اهمیت بیشتری می‌یابد، اما تحولی از این نوع در زمینهٔ سیاست و خط مشی‌ها، پیامدهایی جدی نیز دربر دارد. این که یک نهاد بین‌المللی معیارهایی برای دیگر نهادها تعیین کند و اعلام نماید که در مورد نهادهایی که از این معیارها متابعت نکنند، اقداماتی را به عمل خواهد آورد، امر بی‌سابقه‌ای است.

همان‌گونه که انتظار می‌رفت، اقدام اتحادیه اروپا واکنش کشورهای خارج از اتحادیه اروپایی را (در اروپا و امریکا) به دنبال داشت. (*سوایر و لیتان*، ۱۹۹۸). اردوگاه اروپا استدلال کرده است که نمی‌تواند در مورد حقوق بشرِ شهروندان خود مصالحه کند. از نظر اروپایی‌ها، حریم شخصی یک حقِ انسانی است نه حق مدنی، و لذا مورد خواستهٔ آنها [که در قالب دستورکار مزبور ارائه شده است] به یکی از اصول بنیادین بدل گردیده است. آنها همچنین استدلال می‌کنند که شرکت‌های مشمولِ دستور کار یادشده، معاملات گسترده‌ای با شرکت‌های اروپایی دارند و پیش از این نیز از انواع مختلف قوانین محلی پیروی و متابعت می‌کرده‌اند. این قوانین و ضوابط از مواردی چون تنظیم قیمت‌ها و دستمزدها تا حفاظت از محیط زیست و امثال آن را شامل می‌شده است.

اروپایی‌ها استدلال می‌کنند که هیچکس، شرکت‌ها را از ارسال اطلاعات

■ اردوگاه ایالات متحده استدلال می‌کند که ضوابط و مقررات اروپا در مورد حریم زندگی خصوصی نباید سد راه دادوستدهای تجاری شرکت‌های امریکایی بشود.

■ اردوگاه اروپا استدلال کرده است که نمی‌تواند در مورد حقوق بشرِ شهروندان خود مصالحه کند. از نظر اروپایی‌ها، حریم شخصی یک حقِ انسانی است نه حق مدنی.

به خارج از اتحادیه اروپا باز نمی‌دارد. تنها چیزی که آنها می‌خواهند، قدری محافظت کافی از امور مربوط به حریم شخصی است. به گفته *سوایر و لیتان* (۱۹۹۸)، ماده ۲۶ دستور کار اتحادیه اروپا، راه‌های ممکن برای انتقال اطلاعات به کشورهای ثالث را ـ هرچند این کشورهای یادشده ضوابط کافی برای حفاظت از آنها را نداشته باشند ـ تشریح کرده است. در همین ماده آمده است که انتقال اطلاعات به کشورهای فاقد ضوابط مشخص و کافی برای حفاظت از امور مربوط به حریم شخصی تا زمانی امکان‌پذیر است که تدوین‌کنندگان قوانین اروپا، مکانیسم‌های «خود دیده‌بانی»ای را که آن شرکت‌ها برقرار نموده‌اند، تأیید کنند. ولی اردوگاه ایالات متحده، استدلال می‌کند که ضوابط و مقررات اروپا در مورد حریم زندگی خصوصی، نباید سد راه دادوستدهای تجاری شرکت‌های امریکایی بشود. طرفداران سیاست امریکا از برتری رویکرد بخشی مشخص شده طبق قانون امریکا سخن می‌رانند زیرا رویکرد [امریکایی] مزبور با عدم ایجاد یک سیاست جهانی بوروکراتیزه شدهٔ دست‌وپاگیر، که الزاماً برای هرکاربردی بیش از حد انعطاف‌پذیر خواهد بود، از بازار آزاد پشتیبانی می‌نماید.

نوع محدودیت‌های فراگیر در مورد انتقال داده‌ها توسط کشورهای عضو اتحادیه اروپا می‌تواند تأثیری بنیادین برصنعت اطلاع‌رسانی داشته باشد. این تأثیر ممکن است به یکی از صورت‌های مطرح شدهٔ زیر عملی گردد:

۱. این دستور کار باعث خواهد شد از لحاظ اطلاعات شخصی، بازار اروپا کاملاً از بازار جهانی منفک گردد؛ یا

۲. تهدید، مؤثر خواهد افتاد و سایر کشورهای جهان، از ترس از دست دادن چنین بازار پر رونقی، سر به راه شده و سیاستی جهانی در مورد امور مربوط به حریم زندگی خصوصی اتخاذ خواهند کرد؛ یا

۳. شورا و پارلمان اروپا اجباراً و به منظور اجتناب از انزوا، از تعهد و پای‌بندی خود به قانون مربوط به اطلاعات شخصی دست برخواهند داشت؛ یا

۴. جنگ تجاری نسبتاً کریهی درخواهد گرفت؛ یا

۵. همه کشورها به توافق رسیده و گفت‌وگو در مورد جزئیات امر را آغاز خواهند کرد. کشورهای فاقد ضوابط کافی برای حفاظت از اطلاعات شخصی، خواهند کوشید تا خواه از طریق یک راه‌حل تکنولوژیکی، خواه از طریق تماس و یا به هردو صورت، شکاف موجود را پر کنند.

این که کدام یک از موارد پنج‌گانه فوق محتمل‌تر باشد، هنوز معلوم نیست. در حال حاضر، به علت ابهامات موجود، اردوگاه‌های مختلف، مقرراتی و سخت‌گیر شده‌اند. این رویه، سرانجام می‌تواند به برخی نتایج اقتصادی جدی منجر گردد. از آنجا که اطلاعات شخصی بر گزارش‌های ارائه شده از سوی مؤسسات اعتباری، اطلاعات گردآوری و ارزیابی شده توسط صنعت بازاریابی مستقیم، صنعت خدمات مالی، و شمار بسیاری از دیگر شرکت‌ها و کمپانی‌هایی که با انتقال داده‌ها و اطلاعات سروکار دارند مشتمل است، حاصل کار نیز عمدتاً به این بستگی خواهد داشت که آیا صنایع یادشده باور دارند که می‌توانند طبق ضوابط و مقررات تازه، عملکرد مؤثری داشته باشند یا خیر؟

دستور کار اتحادیه اروپا در مورد ضرورت حفظ حریم شخصی افراد در اکتبر ۱۹۹۸ به تصویب رسید و بسیاری از کشورها (ایالات متحده، استرالیا، کانادا و ژاپن) که به طرز قابل توجهی فاقد سیاست‌های منسجم در زمینه امور شخصی هستند، مایلند ببینند که بخش‌های مختلف جوامع تجاری و بازرگانی‌شان تا چه اندازه فاقد تدابیر حفاظتی کافی تلقی می‌شوند. امریکایی‌ها مجبور خواهند شد که یا تحولاتی جدی در شیوه فعالیت خود صورت دهند و یا کارآیی و توان انجام مبادلات داده‌های شخصی با کشورهای اتحادیه اروپا را از دست بدهند. این بدان معنی نیست که گفته شود در این کشورها از حریم زندگی خصوصی شهروندان حفاظت به عمل نمی‌آید. بلکه برعکس، آنها از دیرباز از هرگونه تلاشی برای تهیه و تدوین سیاست‌هایی کلی اجتناب ورزیده و یک رویکرد «بخشی» را، که اغلب صرفاً در واکنش به بحران‌های درک شده ایجاد می‌شد، ترجیح داده‌اند. برخی از محققان از قبیل *گلمن* (Gellman، ۱۹۹۷) و *ریگان* (Regan، ۱۹۹۵) شکوه کرده‌اند که این رویکرد بخشی به واکنشی ضعیف در برابر تعدی به اطلاعات خصوصی و اجرای حتی ضعیف‌تر سیاست‌هایی که پیش از این وجود داشته است، منجر گردیده است.

در این مورد می‌توان بالاخص به ایالات متحده اشاره کرد که مجموعه

■ گردآوری اطلاعات شخصی باید حدومرزی داشته باشد و این بدان معناست که پردازش این اطلاعات نباید بدون حساب و کتاب انجام پذیرد.

■ نهاد نگهدارنده گزارش یا سابقه، [دربارهٔ اطلاعات شخصی]، باید فقط در داخل همان نهاد از آن استفاده کند. این بدان معنی است که سوابق و گزارش‌های موجود را نمی‌توان به‌طور دلبخواه، هر موقع و برای هر منظور، استفاده کرد.

وسیعی از قوانین و مقررات مربوط به حفاظت از اطلاعات شخصی دارد ولی در آن از وجود یک سیاست کلی در این زمینه، خبری نیست، و لذا هیچ روند یکپارچه و منسجمی نیز در خصوص اجرای آن وجود ندارد.

بنابراین منازعه و اختلاف‌نظری که وجود دارد صرفاً بر سراین است که یک سیاست مناسب در مورد حریم زندگی خصوصی را چه چیزی تشکیل می‌دهد. کاربری این اصطلاح در چارچوب دستورکار اتحادیه اروپا، توانش به کار بستن یک استاندارد جهانی را دارد، استانداردی که ضمن نشأت گرفتن از همین دستور کار، همچنان در اصول کاربردهای قانونی اطلاعات ریشه دارد. این اصول در سیاست‌های معمول و جاری برخی کشورها- اعم از داخل و خارج اتحادیه اروپا - متجلی است.

به‌طور مثال، ایالات متحده امریکا، بزرگترین کشوری که با توجه به استانداردهای تعیین شده توسط دستور کار اتحادیه اروپا، سیاست مناسبی در ارتباط با حریم زندگی خصوصی ندارد، مقررات و ضوابط خوبی درباره گردآوری و پردازش اطلاعات شخصی در سازمان‌های دولتی خود وضع کرده است. قانون حفاظت از اطلاعات شخصی [در سازمان‌های دولتی] مصوب ۱۹۷۴ در ایالات متحده امریکا یکی از نخستین استانداردهای قانونی اطلاعات را به دست می‌دهد. با وجود این، همین کشور امریکا، در تدوین سیاست فراگیری که بتواند همان ضوابط و مقررات را در بخش خصوصی و یا در دولت‌های محلی یا ایالتی نیز اعمال کند، آن‌طور که باید و شاید کار نکرده است. بلکه برعکس، امریکا [در زمینه حفاظت از حریم شخصی] دچار یک سیاست «خوددیده‌بانی» شده است که اکثر ناظران به شکست و عدم موفقیت آن معتقدند. به علاوه، بعید می‌نماید که ایالات متحده یا هریک از دیگر کشورهای فاقد یک سیاست مناسب در این زمینه، قادر باشد قوانین و مقررات مناسبی برای برآوردن خواسته‌های دستور کار فوق‌الذکر، تا موقعی که این دستور کار به اجرا در آید، تدوین نماید.

■ جریان آزاد اطلاعات را نمی‌توان به بهای از دست رفتن حقوق کسانی برقرار ساخت که هدف از این جریان، خدمت به آنان بوده است. این دو معیار را نمی‌توان از هم تفکیک نمود.

■ ماده ششم دستورکار اتحادیه اروپا متذکر شده است که اطلاعات باید (۱) به‌طور منصفانه و قانونی پردازش شود (۲) به منظور اهداف و مقاصد روشن، مشخص و با دلایل موجه گردآوری شود و (۳) در ارتباط با دلایل مزبور، کافی و مرتبط بوده و پرهزینه نباشد.

گذشته از آن، بسیاری از دیگر کشورها (که در فهرست بالا بدانها اشاره نشده است) در خصوص سیاست‌های مرتبط با اطلاعات شخصی از این هم سازمان نایافته‌تر بوده‌اند. کاربری کارت‌های شناسایی ملی، ظاهراً در بسیاری از کشورها رو به افزایش دارد. بنابراین، در غیاب هرگونه ضابطه و قانون، یا تهیه هرگونه مکانیسم اجرایی مناسب در این خصوص -که از لحاظ پردازش اطلاعات، هم در بخش دولتی کاربرد داشته باشد هم در بخش خصوصی - اتحادیه اروپا ممکن است ناگزیر از آن شود که انتقال داده‌های شخصی به آن کشورها را ممنوع سازد.

۳. مفاد دستورکار اتحادیه اروپا

دستور کار شماره ۹۵/۴۶/EC پارلمان و شورای اروپا، که در ۲۴ اکتبر ۱۹۹۵ تهیه گردید و به حفاظت از افراد در ارتباط با پردازش داده‌های شخصی‌شان مربوط می‌شود، در شرایط جریان آزاد داده‌های مزبور تنظیم شده است. دستور کار مزبور از بسیاری جهات تجسم بخش اصول قانونی اطلاعات بوده و مفهومی است که به‌کار وزارت بهداشت، آموزش و رفاه ایالات متحده به عنوان بخشی از قانون حریم زندگی خصوصی مصوب ۱۹۷۴ مربوط می‌گردد. البته، این اصول در قالب یک متن اروپایی و در درون دستورکار مزبور تبیین گردیده است و نمی‌توان گفت قالب همان قوانین و ضوابطی را دارد که توسط وزارت بهداشت، آموزش و رفاه [امریکا] تهیه و تنظیم گردیده است. معذلک، قوانین مزبور در قالب همان سنت کلی قرار دارند.

این اصول‌را، قدری بیشتر یا کمتر، می‌توان به صورت زیر (گلمن، ۱۹۹۷) خلاصه کرد:

۱. اصل شفافیت: گردآوری و پردازش اطلاعات نباید به صورت پنهانی انجام گردد.

۲. اصل مشارکت افراد: سوژهٔ گزارش باید به گزارشی که از او تهیه شده دسترسی داشته باشد و بتواند اطلاعات نادرست موجود در آن را تصحیح نماید.

۳. اصل حدود و ثغور: گردآوری اطلاعات شخصی باید حدومرزی داشته باشد. و این بدان معناست که پردازش این اطلاعات نباید بدون حساب‌وکتاب انجام پذیرد.

۴. اصل ارتباط: گردآوری اطلاعات شخصی باید در ارتباط با هدفی صورت گیرد که این اطلاعات به‌خاطر آن گردآوری شده است؛ این اطلاعات بایستی صحیح، کامل و به موقع باشد.

۵. اصل حدومرز کاربری داخلی: نهاد نگهدارنده این گزارش یا سابقه، [دربارهٔ اطلاعات شخصی] باید فقط در داخل همان نهاد از آن استفاده کند. این بدان معنی است که سوابق و گزارش‌های موجود را نمی‌توان به‌طور دلبخواه، هر موقع و برای هر منظور، استفاده کرد. این

اصل، گردآوری اطلاعات با اهداف و مقاصد سیاسی اعلام نشده را ممنوع می‌سازد.

۶. اصل افشای خارجی: این اصل افشای اطلاعات شخصی در خارج از نهاد مربوطه، بدون اجازه صاحب اطلاعات و یا اجازه یک مرجع قانونی و در شرایط مشخص را ممنوع می‌سازد.

۷. اصل امنیت منطقی: این اصل وجود قدری امنیت را ضروری می‌داند طوری که سوابق و پرونده‌های گردآوری شده به یک طرف ثالث داده نشده و یا توسط چنین طرف ثالثی به سرقت نرفته و یا در جهت اهداف اعلام نشده‌ای مورد استفاده قرار نگیرد.

■ مأمور کنترل موظف است هرگونه اطلاعات و داده‌ای را که با دستورکار همخوانی و سازگاری ندارد اصلاح و یا حذف نماید، به‌ویژه در صورتی که اطلاعات مزبور نادرست بوده باشد.

■ مأمور کنترل باید جریان اصلاح یا حذف اطلاعات را به هر طرف ثالثی که در این خصوص ذی‌ربط باشد، اطلاع دهد.

■ ماده ۱۴ دستورکار، حق صاحب اطلاعات به اعتراض و مخالفت با هرگونه سوءاستفاده از داده‌های شخصی را مشخص می‌نماید.

۸. اصل رعایت اصول: نگهدارنده پرونده‌ها بایستی تمام اصول مربوط به قوانین حفظ اطلاعات شخصی را رعایت نماید.

هشت اصل مذکور در متن دستورکار اتحادیه اروپا، به ویژه در خصوص حق دسترسی صاحب پرونده به آن و نیز حق صاحب پرونده به تصحیح اطلاعات نادرست، بازتاب یافته است. ولی همهٔ این اصول توسط دستورکار موردنظر در زمینه گسترده‌تری ـ مثلاً رابطهٔ مناسبی که میان انسانها و سیستم‌های داده‌پردازی‌ای ایجاد نموده‌اند ـ قرارداده شده است.

از ۷۲ بند (پاراگراف) مجزای موجود در گزارش‌ها، که دلایلی کلی برای این دستور کار ارائه می‌دهند، این نظریه کلی در دومین بند تشریح شده است:

درحالی که سیستم‌های داده‌پردازی برای خدمت به بشر طراحی شده‌اند، در حالی که این سیستم‌ها صرف‌نظر از ملیت یا محل اقامت افراد عادی، باید به حقوق و آزادی‌های بنیادین این افراد، به‌ویژه حق آنان به داشتن حریم خصوصی زندگی، احترام بگذارند و به پیشبرد اقتصادی و اجتماعی، گسترش تجارت و بازرگانی و رفاه همگان کمک نمایند؛ ... (قسمت دوم، بند اول).

این دستور کار بدان سبب نگارش یافت تا بار دیگر رابطه بین سیستم‌های داده‌پردازی و انسانهایی که سیستم‌های مزبور قصد خدمت به آنها را دارند، مورد تأکید قرار دهد. شرایط و ملزومات تجارت اطلاعات، درحالی که بخشی از این نظم اساسی به حساب می‌آیند، در درجه دوم اهمیت قرار می‌گیرند.

اهمیت یک بازار منسجم و یک‌پارچه در بند سوم به عنوان چیزی شناخته شده است که صرفاً می‌تواند از طریق جریان آزاد اطلاعات رخ دهد. این نظم تصحیح شده، در بند سوم مورد تقویت مجدد قرار می‌گیرد. معذلک، در ادامهٔ بند مزبور، این شناخت در زمینهٔ گسترده‌تری از حقوق افراد جای داده می‌شود. جریان آزاد اطلاعات را نمی‌توان به بهای از دست رفتن حقوق کسانی برقرار ساخت که هدف از این جریان، خدمت به آنان بوده است. این دو معیار را نمی‌توان از هم تفکیک نمود.

درحالی که ایجاد و به کاراندازی بازار منسجم و یک‌پارچه‌ای که در آن، مطابق اصل ۷-الف این پیمان، جابه‌جایی آزاد کالاها، افراد، خدمات و سرمایه تضمین شده مستلزم آن است که اطلاعات و داده‌ها، آزادانه از یک کشور عضو به کشور دیگر انتقال یابد، این حقوق اساسی بایستی مورد محافظت نیز قرار داده شود؛ ... (قسمت سوم، بند اول).

زمینه اقتصادی و سیاسی گستردهٔ این دستورکار، و این که چرا این دستورکار در این زمان تهیه شده است، در بند هفتم تشریح گشته و در بند هشتم ادامه می‌یابد. این دو بند موقعیت ویژه‌ای را تشریح می‌کنند که اتحادیه اروپا خود را، از لحاظ انتقال و جابه‌جایی اطلاعات، در آن می‌یابد. هنگامی که اتحادیه اروپا تشکیل گردید، تفاوت‌های موجود در قوانین ملی مربوط به اطلاعات شخصی و حریم زندگی خصوصی عملاً مانع جریان آزاد اطلاعات شد. بنابراین، به منظور پیشبرد همان جریان آزاد اطلاعات و به‌منظور ایجاد محیط مثبت و مساعدی برای تجارت اطلاعات بین کشورهای عضو این اتحادیه، اتخاذ سیاستی بین‌المللی درباره حقوق مربوط به حریم شخصی و انتقال اطلاعات شخصی، الزامی گردید.

ولی با توجه به آنچه که در سه بند نخستین ارائه گردید، تنها راه حل این مشکل همانا حفاظت مساوی از حقوق مربوط به حریم شخصی همه شهروندان کشورهای عضو اتحادیه اروپا بود. تنها راه‌حل مسأله قوانین مختلف و متعدد مربوط به جریان اطلاعات و داده‌ها عبارت بود از گذاردن تأکید مجدد بر عمومیت و جهان شمولی حقوق بشر.

درحالی که تفاوت در میزان حفاظت از حقوق و آزادی‌های افراد، به‌ویژه حق زندگی خصوصی، با توجه به پردازش داده‌های شخصی ارائه شده در کشورهای عضو ممکن است از انتقال این قبیل اطلاعات از خاک یک کشور عضو به خاک کشور عضو دیگر جلوگیری نماید؛ در حالی که این تفاوت

ممکن است مانعی فراراه پی‌گیری شماری از اقدامات اقتصادی در سطح جامعه قرار داده، رقابت را مختل نموده و مسؤولان را از اجرای مسؤولیت‌های خویش طبق قانون جامعه باز دارد؛ در حالی که این تفاوت در میزان حفاظت منوط است به وجود تنوع گسترده‌ای از قوانین و مقررات ملی در زمینه‌های اداری... (قسمت هفتم، بند ۲).

در حالی که، به منظور برداشتن موانع از سرراه جریان اطلاعات شخصی، میزان حفاظت از حقوق و آزادی‌های افراد در ارتباط با پردازش این قبیل اطلاعات بایستی در تمامی کشورهای عضو اتحادیه [اروپا] یکسان باشد؛ در حالی که این هدف برای بازار داخلی جنبهٔ حیاتی دارد ولی حصول آن برای کشورهای عضو، به تنهایی مقدور نیست، مخصوصاً با توجه به میزان اختلافاتی که هم‌اکنون میان قوانین مربوطه در کشورهای عضو وجود دارد و نیز نظر به نیاز موجود به هماهنگی قوانین این کشورها طوری که جریان فرامرزی اطلاعات شخصی به گونه‌ای پایدار تضمین گردیده و با هدف بازار داخلی بدان‌سان که در مادهٔ ۷ـ الف پیمان موردنظر انطباق داشته باشد؛ در حالی که اقدام جامعه اروپا برای متناسب کردن قوانین مربوط به جریان اطلاعات ضرورت دارد... (قسمت هشتم، بند ۲).

دستورکار

خود این دستورکار به هفت فصل و یک مؤخرهٔ متشکل از ۳۴ ماده تقسیم شده است. پنج مادهٔ اول آن هدف مورد نظر را تشریح کرده و درآن ضمن تعریف واژه‌ها، قلمرو دستورکار مشخص گردیده و قابلیت اعمال قانون کشور، مورد بحث و بررسی قرار گرفته است. ماده ششم، اصول مربوط به استفاده قانونی از اطلاعات را مشخص کرده و متذکر می‌گردد که اطلاعات باید ۱. به‌طور منصفانه و قانونی پردازش شود، ۲. به‌منظور اهداف و مقاصد روشن، مشخص و به دلایل موجه گردآوری شود، ۳. در ارتباط با دلایل مزبور، کافی و مرتبط بوده و پرهزینه نباشد. مادهٔ بعد از آن به مجموعه‌ای از استثناها، از جمله کاربری مناسب توسط مقامات مسؤول، اشاره دارد و آن هنگامی است که از اطلاعات به نفع صاحب آن استفاده می‌شود.

مادّه‌های ۱۰، ۱۱ و ۱۲ نیز با کاربردهای قانونی داده‌ها سروکار داشته و حقوق صاحبان اطلاعات را مشخص می‌نماید. براساس ماده‌های مزبور، هنگام گردآوری اطلاعات باید صاحب آن در جریان امر گذارده شود. ماده ۱۰ به گردآوری اطلاعاتی مربوط می‌گردد که از صاحب آن اخذ می‌شود. این ماده اشعار می‌دارد که کشورهای عضو اتحادیه اروپا بایستی ترتیبی اتخاذ کنند که مسؤول کنترل یا نماینده وی، آگاهی‌های مشروحه زیر را در اختیار صاحب اطلاعات قرار دهد:

الف. هویت مسؤول کنترل؛

ب. هدف و مقصود از گردآوری و پردازش اطلاعات؛

ج. آگاهی‌های دیگری از قبیل این که چه کسان یا نهادهایی دریافت‌کننده اطلاعات هستند، و نیز این که در صورت اجباری بودن پاسخ به سؤالات، پیامدهای احتمالی عدم پاسخگویی وی چه خواهد بود؛

د. وجود حق دسترسی به اطلاعات و در صورت لزوم، تصحیح اشتباهات احتمالی.

ماده ۱۱ به همان مسأله مربوط گردیده و حقوق مربوط به مواردی را تشریح می‌نماید که در آن داده‌ها از سوژهٔ اطلاعاتی اخذ نمی‌گردد. ماده ۱۲ نیز به مشخص نمودن حق دسترسی به اطلاعات پرداخته و اشعار می‌دارد که مأمور کنترل، بدون هیچ وقفه یا هزینه‌ای باید صاحب اطلاعات را در جریان مسایل مشروحهٔ زیر قرار دهد:

الف. تأیید این که آیا اطلاعاتی که پردازش می‌گردد واقعاً مربوط به شخص موردنظر است؛

ب. ارائه اطلاعات به‌گونه‌ای روشن و قابل درک درباره ماهیت داده‌هایی که پردازش می‌شود؛

ج. آگاهی از منطق به‌کارگرفته شده در پردازش خودکار داده‌ها.

همچنین این ماده اشعار می‌دارد که در هنگام مقتضی، مأمور کنترل موظف است هرگونه اطلاعات و داده‌ای را که با دستورکار همخوانی و سازگاری ندارد اصلاح و یا حذف نماید، به‌ویژه در صورتی که اطلاعات مزبور نادرست بوده باشد. مأمور کنترل باید جریان اصلاح یا

حذف اطلاعات را به هر طرف ثالثی که در این خصوص ذی‌ربط باشد، اطلاع دهد.

ماده ۱۴ به بسط این حقِ دستیابی پرداخته و حق صاحب اطلاعات به اعتراض و مخالفت با هرگونه سوءاستفاده از داده‌های شخصی را مشخص می‌نماید.

مادهٔ ۱۵ این حقوق را باز هم گسترش می‌دهد و برای این منظور این حق را به افراد می‌دهد که دستخوش اثرات سوءتصمیماتی که در رابطه با داده‌های مزبور گرفته می‌شود (مثلاً تصمیماتی درباره اجرای کار، داشتن لیاقت و شرایط برخورداری از کارت اعتباری و امثال آن) قرار نگیرند.

طبق ماده مزبور، این‌گونه تصمیمات

■ ماده ۲۵، بیشترین مخالفت‌ها را علیه دستورکار موردنظر موجب گردیده و اتحادیه اروپا را در موقعیتی معترض نسبت به برخی از شرکای تجاری آن قرار داده است.

■ دستورکار اتحادیه اروپا در مورد برخی از شرکای این اتحادیه، به‌ویژه آنهایی که در زمینه‌های تجاری سرمایه‌گذاری‌های چشمگیری کرده‌اند، تهدیدآمیز تلقی می‌گردد.

■ در مورد حفاظت از سوابق و پرونده‌های پزشکی و اطلاعات مالی هیچ قانونی در سطح کشور [امریکا] وجود ندارد.

دارای وجههٔ قانونی و حقوقی نخواهد بود. ماده‌های ۱۶ و ۱۷ امنیت لازم برای داده‌ها و اطلاعات شخصی را تضمین می‌نماید و این درحالی است که ماده‌های ۲۲، ۲۳ و ۲۴ اصلاحات قانونی، مسؤولیت‌پذیری و مجازات‌های مربوط به عدم سازگاری با مفاد دستورکار را تشریح می‌نماید.

ماده معروف ۲۵ اصلی‌ترین بخش این دستورکار به حساب می‌آید زیرا به انتقال داده‌های شخصی به کشورهای ثالث یعنی کشورهای غیرعضو اتحادیه اروپا مربوط می‌گردد.

کشورهای عضو اتحادیه مقید خواهند شد که اطلاعات شخصی در دست پردازش یا اطلاعاتی که قرار است بعد از انتقال پردازش شوند، تنها در صورتی به یک کشور ثالث انتقال داده خواهند شد که این کشور حفاظت کافی از اطلاعات موردنظر را تضمین نماید. علاوه برآن، هدف از این انتقال نیز بایستی با قوانین و ضوابط ملی پذیرفته شده براساس مفاد مندرج در این دستور کار انطباق و سازگاری داشته باشد.

کفایت و مناسب بودن میزان حفاظت تضمین شده توسط کشور ثالث با توجه به تمامی شرایط موجود پیرامون عملیات انتقال داده‌ها و اطلاعات شخصی ارزیابی می‌گردد. ماهیت این داده‌ها، هدف و مدت زمان عملیات پردازش داده‌ها، کشورهای مبدأ و مقصد، قوانین و مقررات موجود در کشور ثالث موردنظر اعم از کلی و جزئی و ضوابط حرفه‌ای و تدابیر امنیتی‌ای که در آن کشورها به کار بسته می‌شود نیز بایستی موردتوجه خاص قرار گیرد.

ماده ۲۵، بیشترین مخالفت‌ها را علیه دستورکار موردنظر موجب گردیده و اتحادیه اروپا را در موقعیتی معترض نسبت به برخی از شرکای تجاری آن قرار داده است. می‌توان گفت که دستورکار اتحادیه اروپا در مورد برخی از شرکای این اتحادیه، به‌ویژه آنهایی که در زمینه‌های تجاری سرمایه‌گذاری‌های چشمگیری کرده‌اند، تهدیدآمیز تلقی می‌گردد.

و سرانجام باید گفت که ماده ۲۶ مجموعه‌ای از موارد خاص یا استثناهایی را مشخص می‌کند که ممکن است به‌رغم تأکیدات ماده ۲۵، جریان فرامرزی اطلاعات در میان کشورهای اتحادیه اروپا را ممکن سازد. این استثناها احتمالاً شامل مواردی خواهد شد که طی آن صاحب اطلاعات موافقت صریح خویش با انتقال داده‌ها را اعلام می‌دارد، یا انتقال این داده‌ها برای اجرای یک قرارداد ضرورت داشته و یا انتقال آنها در جهت منافع عمومی باشد و نظایر آن. استثنای قانونی که بسیاری از شرکت‌های امریکایی روی آن حساب می‌کنند، در بند دوم ماده ۲۶، دیده می‌شود و به موجب آن کشورهای عضو اختیار می‌یابند در مواقعی که مأمور کنترل وجود ضمانت کافی در مورد حفاظت از اطلاعات شخصی و آزادی‌ها و حقوق اساسی افراد را تشخیص دهد، با انتقال داده‌های شخصی موافقت نمایند. این شرط نسبتاً مبهم به کشورهای غیرعضو اتحادیه اروپا امکان می‌دهد تا بنا به تشخیص خود ترفندهایی به کار بندند که احتمالاً به نوبهٔ خود با دستورکار اصلی انطباق خواهد داشت.

ماده ۲۷ به شیوه انجام کار مربوط می‌گردد؛ ماده ۲۸ به ایجاد مرجعیتی برای نظارت و بازبینی و ماده‌های ۲۹ و ۳۰ به تشکیل گروه کارآمدی از متخصصان و کارشناسان جهت انجام کارهای روزمره مرتبط با دستورکار.

۴. اثرات احتمالی دستورکار اتحادیه اروپا برتجارت بین‌المللی

در این مطلب، نخستین مناظره جهانی درباره مسأله حریم زندگی خصوصی رفته رفته اوج می‌گیرد. ضرب‌الاجل دستورکار، یعنی بیست‌وچهارم اکتبر، به احتمال بسیار تا موقعی که این مطلب انتشار یابد، سپری شده است. دو طرف اصلی درگیری، اروپا و ایالات متحده هستند و نخستین گلوله به طرف ماده‌های ۲۵ و ۲۶ دستورکار شلیک خواهد شد. هر شرکتی که با شرکت‌های دیگری در اتحادیه اروپا

دادوستد تجاری داشته و مابین کشورهای عضو این اتحادیه به مبادله اطلاعات می‌پردازد، خواه این اطلاعات درباره مشتریان باشد خواه در خصوص کارکنان، مشمول آن قرار خواهد گرفت. به علاوه، هر شرکتی که در سطح جهانی دارای یک شبکه اطلاعاتی از آن خود باشد که به کمک آن، اطلاعات و داده‌هایی را با کشورهای دیگر مبادله نماید، نیز مشمول اثرات این مناظره قرار خواهد گرفت. به‌طور مثال، به گفته دکلان مک کالاف (Declan Mc Cullaugh، ۱۹۹۸)، شرکت هواپیمایی امریکن ایرلاینز پیش از این در یک دعوای حقوقی محکوم شده است و دیگر نمی‌تواند در چارچوب سیستم نگهدارندهٔ SABRE خود اطلاعات را در اختیار مشتریان خود از سوئد گرفته تا ایالات متحده، قرار دهد، زیرا استدلال می‌شد که ایالات متحده آن‌طور که باید و شاید از اطلاعات خصوصی محافظت به عمل نمی‌آورد. مسأله صرفاً این است که شرکت‌ها با صرف چه هزینه‌ای خواهند توانست این ضوابط و مقررات تازه را به‌کار بندند. دیوید بانیسار (David Banisar، ۱۹۹۸) می‌گوید:

دستور کار اتحادیه اروپا بزرگترین چالش را فراروی ایالات متحده قرار می‌دهد. معدود قوانین موجود در امریکا در مورد حریم زندگی خصوصی و اطلاعات شخصی به درستی به عنوان یک چیز وصله پینه شده و سوراخ سوراخ توصیف شده است. در مورد حفاظت از سوابق و پرونده‌های پزشکی و اطلاعات مالی، هیچ قانونی در سطح کشور [امریکا] وجود ندارد. به‌طور بالقوه، جریان کلیه اطلاعات شخصی را می‌توان از بروکسل قطع کرد. چنین کاری، دست‌کم موجب خواهد شد روابط در سطوح مختلف مختل و دچار ابهام و سردرگمی گردد. این ابهام احتمالاً در زمینه فروش و کارمزدهای قانونی میلیاردها دلار زیان به بار خواهد آورد. (رجوع شود به مقدمه)

به گفت مک کالاف (۱۹۹۸) و به نقل از جان کالفی (John Calfee) که در «انستیتو کاتو» سخن می‌گفت، اگر قرار باشد جلو پیشرفت‌های موجود در بازاریابی هدفمند را بگیریم، رفاه مشتریان راکاهش خواهیم داد. اصل استدلال *کالفی* این است که دستور کار اتحادیه اروپا به یک مانع تجاری مبتنی بر حمایت از تولیدات داخلی شباهت دارد. پیتر *سوایر* و *رابرت لیتان* (۱۹۹۸)، طی گزارش کوتاهی در مورد این سیاست که توسط مؤسسه بروکینگز انتشار یافت، ادعا می‌کند که دستور کار اتحادیه اروپا به احتمال زیاد ممکن است جنگی تجاری میان اروپا و ایالات متحده به راه اندازد. آنان می‌گویند اتحادیه اروپا احتمالاً مطالبی انتشار نخواهد داد که در آن تدابیر حفاظتی امریکا درباره اطلاعات و داده‌های خصوصی ناکافی تلقی شده باشد. مع‌ذلک، اتحادیه اروپا احتمالاً از این طریق جدی بودن خود را نشان نخواهد داد که یک یا چند بخش یا شرکت امریکایی فاقد تدابیر حفاظتی کافی را برشمرده و با توجه به آن، ممنوعیت انتقال اطلاعات طبق دستورکار اتحادیه اروپا را در مورد آن اعمال نماید. (اتحادیه اروپا چه تصمیمی خواهد گرفت؟)

معلوم نیست این منازعه تا کجا پیش خواهد رفت. در اینجا مخاطرات بسیاری وجود دارد. به گفته (*سایمون دیویس* ۱۹۹۸)، «آینده بانکداری، مسافرت، معاملات از طریق کارت‌اعتباری، بازرگانی الکترونیک، و تجارت و بازرگانی دولتی، جملگی ممکن است تحت‌تأثیر واقع گردند. آینده عمدتاً بستگی به این خواهد داشت که سایر کشورها، مخصوصاً کشورهای فاقد مقررات حفاظتی کافی در مورد اطلاعات شخصی، چگونه به این دستورکار واکنش نشان دهند. در حال حاضر، چشم‌انداز مربوطه چندان خوش‌بینانه به‌نظر نمی‌رسد. به گفتهٔ (دیویس، ۱۹۹۸)، واشنگتن برآن شده است که از هرگونه انطباق و سازگاری با نظریات اروپا در قبال حریم زندگی خصوصی جلوگیری نموده و در عین حال نگذارد که دستورکار مزبور برمناسبات بازرگانی تأثیر بگذارد. با وجود این، اگر اروپایی‌ها همچنان در مورد این سیاست، سرسخت و انعطاف‌ناپذیر بمانند، ایالات متحده ممکن است خود را در یک جنگ تجاری نامطلوب، درگیر ببیند.»

■ استثنای قانونی که بسیاری از شرکت‌های امریکایی روی آن حساب می‌کنند، در بند دوم ماده ۲۶ دیده می‌شود و به موجب آن کشورهای عضو اختیار می‌یابند در مواقعی که مأمور کنترل وجود ضمانت کافی در مورد حفاظت از اطلاعات شخصی و آزادی‌ها و حقوق اساسی افراد را تشخیص دهد، با انتقال داده‌های شخصی موافقت نمایند.

■ واشنگتن برآن شده است که از هرگونه انطباق و سازگاری با نظریات اروپا در قبال حریم زندگی خصوصی، جلوگیری نموده و در عین حال نگذارد که دستورکار مزبور برمناسبات بازرگانی تأثیر بگذارد.

۵. واکنش‌های بالقوه به مسأله کفایت

درحال حاضر در بحث و مناظره برسر دستورکار اتحادیه اروپا، انواع مختلفی از طرح‌های «خود دیده‌بانی» جایگزین وجود دارد. مسأله «خود دیده‌بانی» در خصوص رفتار یک شرکت، هسته اصلی این مناظره را تشکیل می‌دهد. هنوز معلوم نیست که آیا این طرف ثالث (که با نیروها و عوامل ناب بازار یا نظارت دولت در تضاد است) مؤثر خواهد افتاد یا خیر. نخستین تلاش در زمینه «خود دیده‌بانی» بازار، یعنی

«تراست‌ای» (TrustE) کاملاً به شکست انجامیده است و دومین تلاش یعنی «تریبون اولویت‌های حریم زندگی خصوصی» رفته رفته زیرآتش انتقاد قرار می‌گیرد [*کراداک* (Craddock) ۱۹۹۸؛ *اوکس* (Oakes) ۱۹۹۸؛ مرکز الکترونیک اطلاعات مربوط به حریم زندگی خصوصی ۱۹۹۸؛ *وارنی* (Varney) ۱۹۹۸.]

یکی از استدلالات اصلی در مخالفت با هرگونه طرح قانونی این است که قوانین، که همواره در مقایسه با سیل سریع توسعه تکنولوژیکی بسیار سرد و بی‌روح می‌باشند، به واسطه مسؤولیت‌های محدود از لحاظ مکانی آن برای تنظیم و

از طریق یک شبکه اطلاع‌رسانی از قبیل Amazon- Com و امثال آن.

در «تریبون اولویت‌های حریم زندگی خصوصی» و نیز در «تراست‌ای» این طرح به سیاست اعلام شده یک سایت شبکه در مورد حریم زندگی خصوصی بستگی دارد. تراست‌ای ـ که تلاشی در زمینه «خود دیده‌بانی» در صنعت است که به عقیده اکثر ناظران کاملاً به شکست انجامیده است ـ در صدد آن بود که معیاری برای سیاست‌های مربوط به حریم زندگی خصوصی در اینترنت به دست دهد تا شرکت‌ها آن را بپذیرند و لذا مهر «تراست‌ای» بر سایت‌های شبکه‌شان بخورد. چیزی بسیار شبیه [به آنچه که به]

جهانی (WWW) ایجاد گردید و این پروتکلی است که امکان گزینش را به استفاده‌کنندگان می‌دهد تا هر اطلاعاتی را که بخواهند از سایت این شبکه دریافت دارند (*راین*، ۱۹۹۸). براساس مقاله کریس *اوکس* در «*وایرد نیوز*» (Wired News، ۱۹۹۸) تحت عنوان حریم زندگی خصوصی به عنوان زبان کامپیوتر، یک جست‌وجوگر سازگار با تریبون اولویت‌های حریم زندگی خصوصی به‌طور خودکار می‌تواند به سیاست یک سایت شبکه پیرامون این حریم پی‌برده و با توجه به آن، امکان دستیابی به اطلاعات شخصی را بدهد یا ندهد. اگر تریبون اولویت‌های حریم زندگی خصوصی در جایی با مانعی برخورد کند در محدودهٔ آموزش استفاده کننده خواهد بود. کریس *اوکس* در «اشکالات تریبون اولویت‌های حریم زندگی خصوصی» (۱۹۹۸) خاطرنشان می‌سازد که بخش دشوار و بغرنج ایجاد نرم‌افزار [حفظ] حریم شخصی این است که کاری کنیم تا بدون آن که این نرم‌افزار استفاده‌کنندگان را گیج کند و آنها را از کاربری شبکه دلخور سازد، استفاده‌کنندگان [امکانات] آن را درک کنند.

اشکالی که در این دو راه‌حل وجود دارد این است که هنگامی که اطلاعات شخصی انتشار یافته و در غیاب نظارت دولت ـ از نوعی که دستور کار اتحادیه اروپا سعی در ایجاد آن داشته است ـ احتمالاً هیچ چیزی مانع افشای بیش از حد این اطلاعات در یک سایت شبکه‌ای نمی‌شود. به بیان دیگر، چه چیزی می‌تواند یک شرکت را از نقض قراردادها و تعهداتش باز دارد؟ یک فرد به دلیل اعتماد به یک شرکت خاص، اطلاعات شخصی خود را به آن شرکت ارائه می‌کند ولی همین شرکت به‌طور مخفیانه اطلاعات مربوطه را به یک طرف ثالث می‌فروشد. چنانچه نقض مقررات مربوط به حفاظت حریم زندگی خصوصی نوعی پیامد قانونی نداشته باشد، انگیزه‌های مالی و اقتصادی شرکت‌ها را وادار به افشای

■ چنانچه نقض مقررات مربوط به حفاظت حریم زندگی خصوصی نوعی پیامد قانونی نداشته باشد، انگیزه‌های مالی و اقتصادی شرکت‌ها را وادار به افشای اطلاعات مزبور می‌کند.

■ تنها درصد اندکی از شرکت‌های متمرد و سرکش ممکن است حتی با وجود مکانیسمی چون تریبون اولویت‌های حریم زندگی خصوصی به نقض این مقررات مبادرت ورزند چرا که تمامی تجارت الکترونیک براعتماد و اطمینانی مبتنی است که انسان می‌تواند نسبت به این موجودات نامرئی پیدا کند.

ایجاد یک زیرساخت جهانی اطلاعات الکترونیکی، چندان مجهز نیستند [*رایدنبرگ* (Reidenberg) ۱۹۹۷]. یک راه‌حل جایگزین که به‌طور قابل درکی طرفدار جامعهٔ دست‌اندرکار بازرگانی الکترونیک است، همانا ایجاد چیزی است که هربرت برکرت (۱۹۹۷) آن را فرآوری‌های تقویت حریم زندگی خصوصی یعنی مکانیسم‌های «خود دیده‌بانی» مبتنی بر تکنولوژی می‌خواند، مثل: تریبون اولویت‌های حریم زندگی خصوصی.

یادآوری می‌شود که منظور از بازرگانی الکترونیک، مبادله پول از طریق یک شبکه الکترونیک است، مثلاً خرید کتاب

«مهر تأیید خانه‌داری خوب برای اینترنت [معروف است]» ولی تنها معدودی از شرکت‌ها آن را پذیرفتند و در سطح وسیعی اذعان شده که فرایندهای اجرایی تراست‌ای نامناسب و غیرکافی است.

دومین تلاش در زمینه «خود دیده‌بانی» تکنولوژیکی، بلافاصله بعد از نخستین تلاش صورت گرفت و آن تدارک پروتکل مضمون و مبادله اطلاعات بود که با استفاده از زبان قابل اشاعهٔ افزایش بها و به منظور ایجاد معیار تازه‌ای از مبادله در خصوص کاربری تجاری از داده‌های شخصی انجام پذیرفت. به دنبال آن، تریبون اولویت‌های حریم زندگی خصوصی توسط کنسرسیوم شبکه سراسر

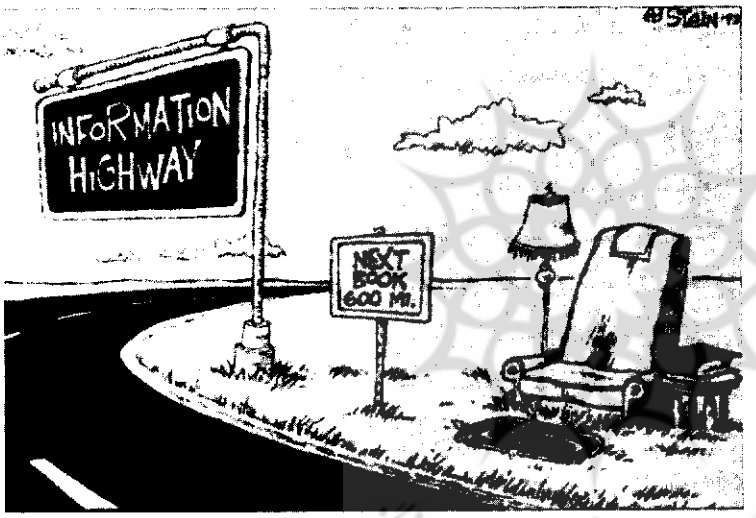
اطلاعات مزبور می‌کند. شاید گفته شود که تنها معدودی از شرکت‌ها ممکن است به چنین کارهای نامعقولی دست بزنند، زیرا عدم پای‌بندی به حفظ اطلاعات شخصی، به اعتبار و حیثیت شرکت لطمه وارد می‌سازد. به علاوه، کاملاً به نفع یک شرکت خواهد بود که بتواند سیاست سفت و سخت خود در زمینه حفاظت از حریم زندگی خصوصی افراد را تبلیغ نموده و همانند بانک‌های سوئیس، سابقه بسیار خوبی از خود در اذهان به وجود آورد. (*سوایر و لیتان، ۱۹۹۸ ـ الف*).

از سوی دیگر، تنها درصد اندکی از شرکت‌های متمرد و سرکش ممکن است حتی با وجود مکانیسمی چون تریبون اولویت‌های حریم زندگی خصوصی به نقض این مقررات مبادرت ورزند چرا که تمامی تجارت الکترونیک براعتماد و اطمینانی مبتنی است که انسان می‌تواند نسبت به این موجودیت‌های نامرئی پیدا کند. ایجاد اعتماد و اطمینان در میان کسانی که در یک بلوک زندگی می‌کنند دشوار است اما در امور تجاری و بازرگانی، ایجاد این اعتماد و اطمینان چندان دشوار نیست. مع‌ذلک، اعتمادکردن به سازمان‌های نامرئی بسیار دشوار می‌باشد، چرا که درصد اعتماد موردنیاز آنها افزایش می‌یابد.

به‌طور قطع، اکثر مردم به استفاده از کارت اعتباری عادت کرده‌اند؛ عده‌ای حتی از طریق شبکه (Web) خرید کرده‌اند، اما این امر تا حدودی بدان سبب است که شرکت‌های صادرکننده کارت‌های اعتباری، تدابیر حفاظتی شدیدی در برابر سرقت به‌کار می‌بندند، اگر قرار باشد اطلاعات شخصی بده بستان شود، در آن صورت مردم خواستار وضع تدابیر کنترلی شدیدی در خصوص چگونگی این مبادلات خواهند شد. برای ایجاد اعتماد و اطمینانی در این سطح، بازار ناگزیر خواهد شد به سطح بسیار بالایی از اطاعت و پیروی دست یابد. در غیراین صورت، بعد از آن که تنها چند شرکت متخلف، پایشان گیر بیفتد، این اعتماد نیز ممکن است همانند مه صبحگاهی، به سرعت از میان رفته و بخش اعظم تجارت الکترونیک را با خود ببرد.

۶. تحقیقات تازه

همان‌گونه که در بالا اشاره شد، دستورکار اتحادیه اروپا آن قدر تازگی دارد که نشریات آکادمیک هنوز فرصت آن را نیافته‌اند که به آن پردازند. بخش اعظم تحقیقات و مطالعات موجود را می‌توان از طریق شبکه سراسری جهانی (WWW) به دست آورد. این تحقیقات عمدتاً به حقوقدانان و پژوهشگران سیاست عمومی محدود است. به عقیدهٔ من، پژوهشگران در زمینه ارتباطات، به‌زودی متوجه رویدادهای مزبور خواهند شد زیرا این رویدادها می‌تواند تحولی تاریخی در شیوه به‌کارگیری اطلاعات و در نتیجه در شیوه ارتباط سازمان‌ها با یکدیگر، صورت دهد.



بدون شک، این دستورکار بخشی است از محیط تازه‌ای برای بحث و گفت‌وگو پیرامون حفاظت از حریم زندگی خصوصی. به عقیدهٔ نویسنده، یکی از بهترین آثاری که درباره این محیط جدید به بحث و بررسی می‌پردازد «تکنولوژی و حریم زندگی خصوصی: چشم‌انداز تازه» نوشته *فیلیپ ای ایگر* (Philip E. Agre) و *مارک روتنبرگ* (Mark Rotenberg) است. یک ویژگی این چشم‌انداز جدید این است که قانون و تکنولوژی ممکن است به جای تخاصم و مقابله، دست همکاری به یکدیگر بدهند. به‌طور مثال، یکی از ایده‌های جالب برخاسته از این منازعه ـ که ممکن است به کمک آن پاسخ دادن به دستورکار اتحادیه اروپا آسانتر گردد ـ همانا ایدهٔ تکنولوژی‌های تقویت‌کننده حریم زندگی خصوصی است. در واقع، این اندیشه مدتی مطرح بود، مخصوصاً در اثر نظری دیوید چاوم (David Chaun؛ ۱۹۸۵، ۱۹۸۶، ۱۹۹۰، ۱۹۹۲) که تداوم داده‌پردازی بدون مشخص کردن هویت صاحب اطلاعات را امکان‌پذیر می‌سازد. بدین معنی که بدون استفاده از مشخصه‌های عمومی هویت یا معلوم کردن این که مشخصه‌های مزبور در چه فایل‌های کاملاً رمزگذاری شده‌ای نگهداری می‌شوند، اطلاعات را می‌توان گردآوری، پردازش و مورد ارزیابی قرار داد، طوری که هویت افراد را نمی‌شود به داده‌های درحال پردازش، مرتبط ساخت. البته استثناهایی وجود دارد. اما این استثناها ممکن است تحت شرایط روند مربوطه صورت گیرد.

هربرت برکرت

از جمله پیش‌کسوتان این رویکرد تکنولوژیک می‌توان به هربرت برکرت سوئیسی اشاره کرد (۱۹۹۷، ۱۹۹۸) که از

حقوقدانان و پژوهشگران در زمینه سیاست عمومی است. از نظر برکرت، راه حفاظت از حریم زندگی خصوصی در آینده همانا پیوند دادن اندیشه حریم زندگی خصوصی با اندیشهٔ ناشناختگی و گمنام باقی ماندن است. در دنیای رسانه‌ای شدهٔ کامپیوتری، حریم زندگی خصوصی الزاماً این نیست که انسان بتواند برخی از اطلاعات مربوط به خودش را حفظ و برخی دیگر را برملا سازد، بلکه حریم مزبور عبارت است از داشتن حق حفظ یا اشاعه این واقعیت که اطلاعات موردنظر در واقع به شما ارجاع دارد.

لذا، از برخی جهات، دستورکار اتحادیه اروپا شاید به خوبی راه تازه‌ای به ما نشان دهد که به کمک آن به مسأله حفاظت از حریم زندگی خصوصی بپردازیم؛ راهی که قانون را با تکنولوژی پیوند دهد. برخی از اندیشه‌های تازه‌تری که رفته رفته پدیدار می‌گردد، ظاهراً مؤید این نظریه است.

پیتر سوایر و رابرت لیتان

پیتر *سوایر* (۱۹۹۶، ۱۹۹۷)، استاد رشته حقوق دانشگاه ایالتی اوهایو، مدتی، به‌ویژه در مقاله انتقادآمیز سال ۱۹۹۷ خود تحت‌عنوان «کاربری‌ها و حدومرزهای رمزشناسی مالی: نظر یک استاد حقوق» پیرامون مسایل مربوط به حریم زندگی خصوصی به نگارش مشغول بود. در مقاله مزبور اثرات طرح‌های تکنولوژیکی مربوط به حریم زندگی خصوصی، یعنی طرح‌های مبتنی بر ناشناختگی صاحب اطلاعات، مورد انتقاد قرار گرفته است.

کتاب تازه وی با همکاری *رابرت ای لیتان*، اقتصاددان، و تحت‌عنوان «به شما مربوط نیست: جریان اطلاعات در جهان، تجارت الکترونیک و دستورکار اروپا در مورد حریم زندگی خصوصی». (۱۹۹۸) نگاشته و توسط مؤسسه بروکینگز انتشار یافته است. این کتاب دستورکار مزبور را از نقطه‌نظر قانون و تأثیر بالقوه آن برتجارت مورد تحلیل قرارداده و سپس ایجاد مکانیسم‌های «خود دیده‌بانی» مبتنی بر قانونِ قرارداد را ارائه داده است که از دیدگاه مؤلفان آن جایگزین منطقی و معقولی برای نظارت جهانی تلقی می‌شود. از نظر *سوایر و لیتان*، این رویکرد بهترین‌های دنیاهای متعدد ممکن را در طرح قابل اجرایی برای حفاظت مبتنی بر «خود دیده‌بانی» از حریم زندگی خصوصی تلفیق می‌نماید و این خصوصیتی از چشم‌انداز اجتماعی‌ای می‌باشد که از دیدگاه آنان به مراتب برتر از قیمومت‌ها و نظارت‌های دولتی است.

سوزان گیندلین

سوزان گیندلین دو مقاله جالب درباره مسأله جریان بین‌المللی اطلاعات نوشته است. یکی با عنوان «پیدا و پنهان در فضای سیبرنتیک (Cyberspace) اطلاعات مربوط به زندگی خصوصی در عصر اینترنت» (۱۹۹۷) و دیگری با عنوان «دستورکار اتحادیه اروپا در مورد حفاظت از داده‌ها؛ در شرایطی که جهان ماهواره‌ای تحول می‌یابد» (۱۹۹۷). در این مقاله‌ها مسایل مزبور به اختصار تشریح گشته و استدلال‌هایی برای یک پاسخ تندتر از جانب سازمان‌های دولتی ارائه گردیده است. نویسنده همچنین خلاصه‌ای از سیاست‌های مرتبط با حریم زندگی خصوصی در خارج از دالان امریکا ـ اروپا عرضه می‌دارد.

۷. ضمیمه: سیاست‌های ملی خارج از اتحادیه اروپا

واکنش بین‌المللی نسبت به دستورکار اتحادیه اروپا متفاوت بوده است. بسیاری از کشورها، به‌ویژه آن دسته از کشورهای فاقد امکاناتِ لازم برای گردآوری و، مهمتر از همه، پردازش اطلاعات شخصی از طریق سیستم‌های کامپیوتری، در این منازعه و کشمکش خود را درگیر نکردند. براساس گزارش اخیر مؤسسه جهانی آزادی اینترنت (Global Internet Liberty Campaign) با عنوان «حریم زندگی خصوصی وحقوق بشر: مطالعه‌ای بین‌المللی در خصوص فعالیت‌ها و قوانین مربوط به حریم زندگی خصوصی» (۱۹۹۸)، تقریباً تمام کشورهای جهان خواه به صراحت و خواه به گونه‌ای تلویحی، حریم زندگی خصوصی را یک حق مسلم بشری می‌دانند و در اکثر قوانین اساسی اخیراً تدوین شده، حقوق ویژه‌ای برای دسترسی به اطلاعات شخصی و کنترل آنها در نظر گرفته شده است.

از نظر بسیاری از کشورها، مسایل مربوط به حریم زندگی خصوصی در

■ برخی معتقدند که دستور کار اتحادیه اروپا به یک مانع تجاری مبتنی بر حمایت از تولیدات داخلی شباهت دارد.

■ در دنیای رسانه‌ای شدهٔ کامپیوتری، حریم زندگی خصوصی الزاماً این نیست که انسان بتواند برخی از اطلاعات مربوط به خودش را حفظ و برخی دیگر را برملا سازد، بلکه حریم مزبور عبارت است از داشتن حق حفظ یا اشاعه این واقعیت که اطلاعات موردنظر در واقع به شما ارجاع دارد.

■ از برخی جهات، دستورکار اتحادیه اروپا شاید به خوبی راه تازه‌ای به ما نشان دهد که به کمک آن به مسأله حفاظت از حریم زندگی خصوصی بپردازیم؛ راهی که قانون را با تکنولوژی پیوند دهد.

سطح اساسی‌تری مطرح می‌گردد. در آن دسته از کشورهایی که در آنها قوانین ضبط و تفحص اطلاعات معمولاً از سوی دولت نقض می‌گردد و یا در آنها حقوق افراد به رسمیت شناخته نمی‌شود، مسأله عملکرد قانونی اطلاعات به ندرت مطرح می‌گردد. آن دسته از کشورهایی که در آن تجارت الکترونیک هم‌اکنون به عنوان یک عامل مسلط مطرح است و یا همانند امریکا، در آن رفته رفته به یک عامل برتر بدل می‌شود، در سطوح متفاوتی نسبت به آن واکنش نشان داده‌اند. برای آن دسته از کشورهایی که وجود یک سیاست کلی در مورد حریم زندگی خصوصی را مغایر تجارت آزاد می‌دانند، دستورکار اتحادیه اروپا به یک مسأله دردآور بدل گردیده است.

جمهوری آرژانتین

براساس گزارش مؤسسه جهانی آزادی اینترنت، مورخ دسامبر ۱۹۹۶، کنگره آرژانتین قانونی از تصویب گذراند که اطلاعات شخصی ضبط شده در فایل‌های اطلاعاتی، دفاتر ثبت، بانک‌هایا دیگر ابزارهای تکنیکی الکترونیک و غیرالکترونیک مرتبط با داده‌ها را مورد حفاظت قرار دهد تا حیثیت و حریم شخصی افراد و نیز دسترسی آنان به اطلاعاتی که ممکن است دربارهٔ این اشخاص ثبت شود را تضمین نماید. (جمهوری آرژانتین). این قانون به موقع تصویب گردید اما سپس با مداخله بانک مرکزی، از سوی رئیس‌جمهور وتو شد.

به‌طور کلی، جمهوری آرژانتین درطول دوره انتقال به حکومت دموکراتیک به انبوهی از رسوائی‌های مرتبط با استراق سمع تلفنی دچار بود. تلفن‌های دفتر رئیس‌جمهوری آن به شدت تحت‌کنترل قرار داشت. سیاست‌های داخلی آکنده از اتهامات و ضداتهامات مربوط به استراق‌سمع غیرقانونی تلفن بود.

استرالیا

استرالیا از دیرباز سیاستی بینابینی در پیش گرفته است که چیزی است میان سیاست مورد حمایت ایالات متحده و سیاست موردنظر اتحادیه اروپا. در اواسط دهه ۱۹۹۰، اکثر طرف‌های ذی‌نفع اعم از طرفداران حریم شخصی و نمایندگان صنایع، سیاستی را دنبال نمودند که آن را «نظارت مشترک» می‌خواندند و آن آمیزه‌ای بود از نظارت دولت و «خوددیده‌بانی». هنوز معلوم نیست که آیا این سیاست بینابینی با دستورکار اتحادیه اروپا هماهنگی خواهد داشت یا خیر. اکثر طرف‌های ذی‌نفع در این زمان معتقد بودند که قواعد و مقررات مربوط به حریم شخصی باید از قوانین مربوط به سوءاستفاده‌های احتمالی دولت فراتر رفته و بخش خصوصی را نیز دربرگیرد.

طرح آنها برای تحقق این امر یعنی درپیش گرفتن سیاستی که *راجر کلارک* (Roger Clarke، ۱۹۹۸) آن را سیاست مشترک خواند، با ضوابط کاری معمول در این صنعت آغاز شد که خود با مشورت و همفکری کمیساریای حریم زندگی خصوصی تدوین گردیده، توسط این صنایع به اجرا درآمده، مورد نظارت کمیساریای مزبور قرار گرفته و مورد حمایت قانونی واقع بوده است.

به گفته کلارک، این رویکرد از پشتیبانی هردو حزب عمده، که آن را به عنوان تریبون‌های خاص خود پذیرفته‌اند، برخوردار بود. در سپتامبر ۱۹۹۶، دادستان کل با انتشار یک گزارش به تشریح این ابتکار پرداخت. سپس در تاریخ اول مارس ۱۹۹۷، نخست‌وزیر طی یک گزارش مطبوعاتی مختصر چهار پاراگرافی، سیاست مزبور را دگرگون ساخت و اعلام داشت که در آینده نزدیک هیچ نظارتی در مورد بخش خصوصی اعمال نخواهد گشت. وی دلیل این تغییر در سیاست را بالابودن هزینه اجرایی آن ذکر کرد. اعلام این خبر بدون رایزنی با اعضای هیأت دولت یا دادستان کل و یا کمیساریای حریم زندگی خصوصی انجام گرفت. به گفته کلارک، «چنین می‌نمود که نخست‌وزیر از سوی یک گروه فشار کوتاه بین و ناآگاه، که احتمالاً بانک‌های عمده بودند، تحت‌فشار قرار گرفته است.»

درحال حاضر، گروه‌های طرفدار حفاظت از حریم شخصی با برگزاری یک نشست درصدد به اجرا درآمدن مجدد قانون مزبور برآمده‌اند.

برزیل

در سال ۱۹۹۶، سنای برزیل لایحه‌ای در مورد داده‌های مرتبط با حریم زندگی خصوصی تسلیم داشت که در صورت تصویب، از رهنمودهای سازمان عمران و همکاری اروپا و اصول اتحادیه اروپا پیروی خواهد کرد. در این لایحه می‌خوانیم: «داده‌ها و اطلاعات به هیچ‌وجه بدون اجازه صاحب آن در جهت اهداف و مقاصدی غیراز آنچه به ایجاد پایگاه‌های اطلاعاتی یا مراکز ثبت و ضبط اطلاعات انجامید، فاش نساخته، انتقال نیافته و یا مبادله نخواهند گردید. به علاوه، گردآوری، ثبت، بایگانی، پردازش

■ به موجب لایحه‌ای که سنای برزیل در ۱۹۹۶ ارائه داد «هر شهروندی حق دارد بدون هیچ‌گونه هزینه‌ای به اطلاعات مربوط به خودش که در پایگاه‌های اطلاعاتی یا مراکز ثبت و ضبط داده‌ها نگهداری می‌شود دسترسی داشته و این اطلاعات را تصحیح کرده یا چیزی بدانها بیفزاید و یا از آن حذف نماید».

و انتقال داده‌های مربوط به قومیت، اعتقادات و باورهای سیاسی و مذهبی، بهداشت جسم و روان، مسایل جنسی، سوابق کیفری، مسایل خانوادگی، به جز رابطه خانوادگی، منزلت و موقعیت اداری و وضعیت تأهل، ممنوع می‌باشد.»

بار دیگر تأکید می‌گردد که، «هر شهروندی حق دارد بدون هیچ‌گونه هزینه‌ای به اطلاعات مربوط به خودش که در پایگاه‌های اطلاعاتی یا مراکز ثبت و ضبط داده‌ها نگهداری می‌شود دسترسی داشته و این اطلاعات را تصحیح کرده یا چیزی بدانها بیفزاید و یا از آن حذف نماید.

همچنین مسؤولان پایگاه‌های اطلاعاتی بایستی وی را در جریان اطلاعات و داده‌هایی که درباره او نگهداری می‌کنند، قرار دهند.» (مؤسسه جهانی آزادی اینترنت، ۱۹۹۸). این قانون اگر به تصویب برسد هم بخش دولتی و هم بخش خصوصی را شامل خواهد گردید، ولی هنوز خیلی مانده است که چنین قانونی مورد تصویب قرار بگیرد.

برزیل در سال ۱۹۹۰ قانون حمایت و دفاع از مصرف‌کننده را به تصویب رسانده است. این قانون هنوز هم در این کشور اجرا می‌گردد و بسیاری از حقوق مندرج در قانون جدید را مورد تأیید قرار می‌دهد. برزیل در سال ۱۹۹۶ نیز قانونی در ارتباط با استراق سمع تلفنی وضع کرده است که به موجب آن ضبط مکالمات تلفنی رسمی را به مدت پانزده روز مجاز می‌شمارد ولیکن تا به حال تعدادی رسوایی مرتبط با استراق سمع برسر کاربری غیرقانونی این تکنولوژی نیز وجود داشته است.

کانادا

همان‌طور که در مورد ایالات متحده امریکا عنوان شد، قانون اساسی کانادا در مورد حریم شخصی حق صریحی قایل نشده است جز این که در آن آمده است حریم مزبور از تفحص و ضبط و ثبت غیرموجه، مصون است. با وجود این، از سال ۱۹۸۳، پارلمان کانادا قانون حریم شخصی و قانون دسترسی به اطلاعات را از تصویب گذراند که قانون اول به گردآوری، تصحیح، افشا، ضبط، و کاربری اطلاعات شخصی و دومین آن به حق دسترسی افراد به اطلاعات شخصی و غیرشخصی مربوط می‌گردد. این قوانین در مورد بخش عمومی رعایت می‌شود ولی دولت قول داده است قانون تازه‌ای درباره حریم شخصی تصویب نماید که تا سال ۲۰۰۰ مسایل بخش خصوصی را نیز دربر خواهد گرفت.

انتظار می‌رفت لایحه این قانون تا اکتبر ۱۹۹۸ تسلیم پارلمان گردد یعنی در همان تاریخی که دستورکار اتحادیه اروپا به تصویب رسید.

چین

براساس «گزارش کشوری در مورد حقوق بشر» (۱۹۹۷) ـ که توسط وزارت خارجه ایالات متحده انتشار یافت و سازمان بین‌المللی حریم شخصی نیز گزیده‌ای از آن را انتشار داد ـ تلاش‌های چین در زمینه آزادسازی اقتصاد، تضادها و تناقضاتی برای خود آن نیز پدید آورده است. اگر چه دولت فعالانه میزان دسترسی به اینترنت را افزایش می‌دهد (حدود ده‌هزار استفاده‌کننده از اینترنت در پکن وجود دارند) ولی دستیابی شهروندان به برخی از «سایت»های خاص راکه مغایر با منافع امنیتی کشور تشخیص داده است، محدود می‌سازد. این سایت‌ها ممکن است عمدتاً سایت‌های مربوط به سازمان‌های خبری غربی و گروه‌های طرفدار اندیشه‌های مختلف باشند.

قانون اساسی مصوب سال ۱۹۸۲ چین آزادی و حق مکاتبات شخصی و خصوصی را برای شهروندان کشور قایل شده است ولی با وجود این، دولت مرتباً تلفن‌ها، دورنگارها، پست الکترونیک، و ارتباطات اینترنتی خارجی‌ها، از جمله دیپلمات‌ها، روزنامه‌نگاران و دست‌اندرکاران تجارت و بازرگانی را کنترل می‌کند. به‌طور قطع، در چنین وضعیتی کاربرد امور اطلاع‌رسانی قانونی به هر طریق عملی، و نه صرفاً برروی کاغذ، در سطح مطلوبی قرار ندارد.

هند

در قانون اساسی مصوب ۱۹۵۰ هند، صراحتاً حقی برای حریم شخصی شهروندان قید نشده است، هرچند دیوان عالی این کشور در سال ۱۹۶۶ اعلام داشته است که این حق به‌طور ضمنی وجود دارد. براساس گزارش مؤسسه جهانی آزادی اینترنت، از قوانین کلی درباره حریم زندگی خصوصی مردم نیز در هند اثری به چشم نمی‌خورد.

از سوی دیگر، یک نیروی ضربت ملی در مورد تکنولوژی اطلاع‌رسانی و توسعه نرم‌افزار نیز که در مه ۱۹۹۸ تشکیل گردید، به‌منظور اتخاذ سیاست ملی تازه‌ای درباره

■ قانون اساسی مصوب سال ۱۹۸۲ چین، آزادی و حق مکاتبات شخصی و خصوصی را برای شهروندان کشور قایل شده است ولی با وجود این، دولت مرتباً تلفن‌ها، دورنگارها، پست الکترونیک، و ارتباطات اینترنتی خارجی‌ها، از جمله دیپلمات‌ها، روزنامه‌نگاران و دست‌اندرکاران تجارت و بازرگانی را کنترل می‌کند.

■ در جریان تظاهرات میدان تیان آن‌من، دولت چین با مراجعه به کامپیوتر و اخذ مشخصات صاحبان ۳۰هزار دستگاه فاکس موجود در پکن، ارسال‌کنندگان اخبار از طریق فاکس را دستگیر کرد.

■ دولت کانادا قول داده است قانون تازه‌ای درباره حریم شخصی تصویب نماید که تا سال ۲۰۰۰ مسایل بخش خصوصی را نیز دربر خواهد گرفت.

■ دولت ژاپن در سال ۱۹۸۸ قانون حفاظت از داده‌های شخصی پردازش شده کامپیوتری که توسط سازمان‌های اداری نگهداری می‌شوند را تصویب کرد.

امنیت اطلاعات و حفاظت از داده‌ها، خواستار ارائه یک طرح کاربردی شده است. قرار است تا اواخر سال ۱۹۹۸ پیش‌نویس قانون تازه‌ای در این خصوص تهیه شود.

ژاپن

دولت ژاپن در سال ۱۹۸۸ قانون حفاظت از داده‌های شخصی پردازش شده کامپیوتری که توسط سازمان‌های اداری نگهداری می‌شوند را تصویب کرد. این قانون بر کاربری اطلاعات شخصی نگهداری شده در بانک‌های اطلاعاتی دولتی نظارت داشته و مطابق رهنمودهای سازمان عمران و همکاری اروپا تنظیم گردیده است.

در ژوئن ۱۹۹۸، نخست‌وزیر ژاپن در مورد ایجاد مکانیسم‌های «خود دیده‌بانی» برای حفاظت از حریم شخصی در بخش خصوصی، قراردادی با ایالات متحده به امضا رساند. بدین‌ترتیب، دولت ژاپن الگوی چند بخشی امریکا را به جز در مورد صنایعی که با اطلاعات بسیار محرمانه سروکار دارند، برگزید.

زلاندنو

زلاندنو موضعی انتخاب کرده است که شباهت بسیار به مواضع ایالات متحده و استرالیا دارد. می‌توان گفت که تلاش‌های این کشور جهت ایجاد یک سیاست کلی در مورد حریم شخصی به سان آنچه اتحادیه اروپا در پیش گرفته است، در نهایت ناهمگون بوده است. گزارش باری ویلسون (Barry Wilson، ۱۹۹۲) درباره قانون مربوط به حریم زندگی خصوصی در زلاندنو، مجادله و کشمکشی را به راه انداخت که در درجه اول برسر کارت‌های اجباری ملی «کی‌وی» (Kiwi) بود که هدف از آن تا حدودی به مراقبت‌های پزشکی مربوط می‌شد.

نگرانی موجود در زلاندنو از بابت کاربری اطلاعات و انتقال و جابه‌جایی آنها از یک سازمان دولتی به سازمان دولتی دیگر در داخل کشور بود. در واقع، بخش اعظم این نگرانی به واسطه وجود برخی رسوائی‌ها مورد تأیید قرار گرفته و آن هنگامی بوده است که اقدام یک مقام مسؤول دولتی به هنگام فروش اطلاعات لو رفت.

ایالات متحده امریکا

شاید قدرتمندترین مخالفت‌ها با دستورکار اتحادیه اروپا، از جانب ایالات متحده صورت گرفته باشد. به گفته دیوید *بانیار* (۱۹۹۸)، از سالهای ۱۹۷۰، سیاست ایالات متحده در مورد حریم شخصی در حالت اغما قرار گرفته است. از یک لحاظ، ایالات متحده از مبلغان اندیشهٔ «خود دیده‌بانی» در صنعت اطلاع‌رسانی بوده است.

مع‌ذلک، تا به حال فقط ۱۱۲ شرکت مجوز «تراست‌ای»، را که از سازمان‌های بسیار پیشرفته در زمینه خود دیده‌بانی در شبکه «وب» می‌باشد، به دست آورده است. از سوی دیگر رسوائی‌های اطلاعاتی یکی پس از دیگری به وقوع می‌پیوست. شرکت‌های کارت اعتباری تی ار دبلیو (TRW) و اکیفاکس (Equifax) به خاطر انتشار داده‌های نادرست تحت تعقیب قرار گرفته‌اند. مچ فروشگاه‌های زنجیره‌ای دارویی بارها در هنگام فروش سوابق پزشکی به شرکت‌های دارویی گرفته شده است. شرکت کارت اعتباری امریکن اکسپرس درحال فروش فهرست‌هایی از مشتریان خود به دست‌اندرکاران تجارت از راه دور، مشاهده شده است.

در تمام این مدت، دولت ایالات متحده با مبارزه‌ای که علیه مقامات اتحادیه اروپا آغاز کرده کوشیده است تا آنان را به عقب‌نشینی از موضع عنوان شدهٔ دستورکار این اتحادیه وادار نماید.

بنا به گفته دیوید *بانیار* (۱۹۹۸)، «کاخ سفید نمایندگانی به نقاط مختلف جهان گسیل داشته است تا کشورهای دیگر، از جمله ژاپن، را به عدم تصویب قوانین مربوط به حریم شخصی وادار سازند. آنها تهدید کرده‌اند که [مشکل] اتحادیه اروپا را به سازمان تجارت جهانی ببرند ولو این‌که قرارداد کلی تعرفه و تجارت (گات) قوانین مربوط به حریم شخصی را قابل اجرا ندانند.»

در پایان باید گفت که مخالفت ایالات متحده ممکن است اثرات زیانباری بر تجارت الکترونیک داشته باشد، و این چیزی است که ایالات متحده در سیاست «خود دیده‌بانی»اش، همواره تلاش کرده است از آن بپرهیزد. عجیب اینجاست که هرچه این منازعه تأثیر بیشتری بر تجارت بگذارد، احتمال این که سیاست اطلاع‌رسانی جهانی، سرانجام مورد قبول کشورها قرار گیرد، نیز بیشتر خواهد شد، زیرا برهمگان روشن خواهد شد که تفاوت‌های موجود در سیاست مربوط به حفظ حریم زندگی خصوصی در واقع ممکن است بیش از هرچیز برای تجارت و بازرگانی زیانبار باشد.□

منبع:
Communication Research Trends, Vol. 18 (1998) No. 1, pp. 3-18.