اخلاق حرفه ای، حریم خصوصی و حق دسترسی به اطلاعات

نوشتهٔ دکترحسن نمک دوست تهرانی

مقدمه

از جمله اصول بنیادین اخلاقی در حرفه روزنامه نگاری الزام رسانه ها به رعایت حریم خصوصی شهروندان است. از همین رو پرداختن به زندگی خصوصی افراد یکی از معیارهای تمایز میان روزنامه‌نگاری حرفه‌ای و «روزنامه نگاری جنجالی» به شمار می آید.

همزمان، برخورداری روزنامه نگاران از حق دسترسی آزادانه به اطلاعات، از جمله حقوق مسلم آنان شناخته می شود.

در این مقاله کوشش شده است تا ضمن توضیح مفهوم «حریم خصوصی» و تحول تاریخی آن، همسازی و یکپارچگی این حق با حق دسترسی آزادانه، تبیین و در عین حال عوامل نقض‌کنندهٔ آن بررسی شود. تأمل در استدلال کسانی که نقض حریم خصوصی افراد را از سوی روزنامه نگاران موجه می دانند، بخش پایانی این مقاله را تشکیل می دهد.

حق دسترسی آزادانه به اطلاعات و حریم خصوصی

همچون آزادی اطلاعات و حق دسترسی آزادانه به اطلاعات، حریم خصوصی نیز یک حق بنیادین بشری، سنگ بنای منزلت انسانی و ارزشهای دیگر همچون آزادی اجتماعات و آزادی بیان و از جمله مهم‌ترین حقوق انسانی در دوران مدرن به شمار می‌رود. از همین‌رو حریم خصوصی در سراسر دنیا و در بسیاری مناطق و فرهنگهای گوناگون، به‌رسمیت شناخته شده است. در اعلامیه جهانی حقوق بشر، میثاق بین‌المللی حقوق سیاسی و مدنی و در بسیاری دیگر از معاهدات بین‌المللی و منطقه‌ای حقوق‌بشر، بر حمایت از حریم خصوصی تأکید شده است. تقریباً تمامی کشورهای جهان در ماده‌ای از قانون اساسی خود به این حق توجه کرده‌اند. دست‌کم، این قوانین، حق مصون بودن محل زندگی و امنیتِ ارتباطات را مورد توجه قرار داده‌اند.

بسیاری از قوانین اساسی که به تازگی نگاشته شده‌اند، حقوق اختصاصی فرد را در دسترسی و کنترل اطلاعات شخصی خود به رسمیت شناخته‌اند. البته در بسیاری از کشورها نیز که در قانون اساسی‌شان، حریم خصوصی به صراحت مورد توجه قرار نگرفته است، دادگاهها برای محافظت از این حق، به قوانین عادی دیگر استناد می‌کنند. در شماری از کشورها نیز، که حق حریم خصوصی را به رسمیت می‌شناسند، توافقهای بین‌المللی، همچون میثاق بین‌المللی حقوق سیاسی و مدنی یا کنوانسیون اروپایی حقوق بشر، صورتی قانونی به خود گرفته‌اند.

در تعابیر چهارگانه‌ای که معمولا در تبیین حریم خصوصی به‌کار می‌رود و ما در جای خود به تشریح آن خواهیم پرداخت، دو تعبیر به‌طور خاص به موضوع اطلاعات شخصی، به عنوان مصداقهای حریم خصوصی، دلالت دارند: نخست «حریم اطلاعات»، که شامل تصویب قوانینی است که چگونگی دسترسی به اطلاعات شخصی نظیر اطلاعات مالی، پزشکی و دولتی افراد را تعیین می‌کند. دیگری «حریم ارتباطات» که به موضوع امنیت پست‌های الکترونی، تلفنها، پست و سایر اشکال ارتباطات توجه دارد.

مقصود آن‌که در رویکردهای متعارف، اطلاعات درباره زندگی خصوصی و شخصی افراد، و به ویژه وجوهی که تأثیری بر روندهای حیات اجتماعی جامعه ندارند، قلمروی دانسته می‌شود که باید از تعرض هر گونه نظارت مداخله‌گرانه، از جمله گسترهٔ حق دسترسی آزادانه به اطلاعات، مصون بماند. به بیان دقیق‌تر، رعایت حریم خصوصی افراد و آزادی شهروندان در دسترسی به اطلاعات، که هر دو از موازین بنیادین حقوق بشر شناخته می‌شوند، در تخالف و تزاحم با یکدیگر نیستند. تأکید آغازین بر تبیین آزادی اطلاعات به مثابه دسترسی شهروندان به اطلاعاتی که نزد دولت است، از همین روست. در حقیقت آزادی اطلاعات به طور طبیعی دسترسی شهروندان به اطلاعات پیرامون زندگی خصوصی افراد را شامل نمی‌شود. این قاعدهٔ کلی، از منظر برخی صاحب‌نظران، هنگام بحث دربارهٔ زندگی خصوصی برخی کسان، به‌ویژه آنانی که در دموکراسیها به نمایندگی از مردم سرنوشت آنان را در دست گرفته‌اند، قابل تأمل می‌شود. پرسش اصلی آنان این است که وقتی تصمیم‌گیریهای سرنوشت‌ساز از سوی جامعه، بنا بر معیار اعتماد، به دست کسانی سپرده می‌شود، که در زندگی خصوصی خود روش و منشی در مغایر با آنچه شهروندان از آنها انتظار دارند، انجام می دهند، آیا همچنان معیارهای عام حریم خصوصی، باید مراعات شوند؟

برای مثال «فرد ایچ کیت»، استاد حقوق دانشگاه ایندیانا، در مقاله خود با عنوان «معضل حریم خصوصی: نگاهی گسترده‌تر به حریم خصوصی، اطلاعات، هزینه‌ها و پیامدهای مراقبت از آن» به طرح این موضوع می‌پردازد:

«یکی از مهم ترین ارزشهایی که با تصویب قوانین جدید حریم خصوصی به خطر افتاده است، جریان اطلاعاتی است که برای دموکراسی و فعالیت مطبوعات آزاد ضروری است. اعطای آزادی به افراد برای احاطه بر اطلاعات پیرامون شان لاجرم به این معناست که به آنان اجازه می دهیم دسترسی و کاربرد آن اطلاعات از سوی عموم و مطبوعات محدود شود. از همین روست که در سالهای اخیر توجیه محرمانه کردن اسناد عمومی که به‌طور سنتی اسنادی «باز» شمرده می‌شدند و تلاش برای مخفی نگاه داشتن آنها و یا اعمال مجازات بر انتشار اطلاعات دقیق، نگرانیهایی را برانگیخته است.

اینکه [در جامعه] ارزشهای متعارض وجود دارند و پذیرش هریک متضمن پرداخت هزینه‌هایی است، به آن‌معنا نیست که قانون نباید از حریم خصوصی محافظت کند، بلکه موضوع توزین و تعیین دقیق ارزش‌ها و هزینه‌ها قبل از اتخاذ تصمیم‌هایی است که محدودیتهای تازه‌ای را بر جریان اطلاعات تحمیل می‌کنند، و این توجه حتی هنگامی که محدودیتها برای خدمت به هدفی ارزشمند طراحی شده اند، ضروری است.

«مارک روتن‌برگ»، مدیر مرکز اطلاعات الکترونی حریم خصوصی ایالات متحده‌آمریکا، نیز هنگامی که به تدقیق شیوه‌های تعرض به حریم خصوصی افراد در جوامع معاصر می‌پردازد، در عباراتی از دسترسی حکومتها و نهادهای تجاری خصوصی به اطلاعات خصوصی شهروندان و در مقابل ناتوانی شهروندان در دسترسی به اطلاعات پیرامون کارگزاران حکومت و صاحبان شرکتهای خصوصی به‌مثابه «آیینه‌ای» یک سویه تعبیر می‌کند. مقصود او از آیینهٔ یک سویه، شبه آیینه‌ای است که برای زیر نظر گرفتن دیگران تعبیه می‌شود. در حالی که افراد، همچون آیینه معمولی، چهره خود را در آن می‌بینند، مراقبان از پس آیینه رفتار آنان را نظاره می‌کنند.

اشاره آغازین به این مثالها از آن روست که نسبت میان پاسداشت حریم خصوصی شهروندان و دسترسی آزادانه به اطلاعات، در برخی جزئیات نیاز به تأمل دارد. همچنان که خواهیم دید به عنوان یک اصل کلی، برخورداری شهروندان از این دو حق، به گونه‌ای توأمان، قاعده تحقق حکومت مردم سالار است، و نقض هر یک از این دو حق، به نقض دموکراسی می‌انجامد. در پاره‌ای مصداقها و جزئیات اما، باید موضوع را از نزدیک مورد بررسی قرار داد.

در این مقاله، نخست به تعریف حریم خصوصی، تطور آن، به ویژه در دو قرن گذشته، تدقیق قلمرو حریم خصوصی و نیز جایگاه این حق در مباحث امروزی حقوق بشر خواهیم پرداخت. سپس از منظر مارک روتن‌برگ، مهم‌ترین تهدیدهای معاصر علیه حریم خصوصی را مورد توجه قرار می‌دهیم و سرانجام بر پایه مباحث دیوید آرکارد، متخصص صاحب نام اخلاق رسانه‌ای، به کندوکاو در استدلالها و ادله کسانی

خواهیم پرداخت که بر سه پایه شهرت، منفعت شهروندان و علاقه مردم، دسترسی عموم را به اطلاعات پیرامون زندگی خصوصی افراد مجاز می دانند.

۱. تعریف حریم خصوصی

از میان فهرست بین‌المللی موضوعات پیرامون حقوق بشر، شاید دشوارتر از همه تعریف «حریم خصوصی» باشد. درحقیقت تعریف حریم خصوصی بستگی تام به فرهنگ و زمینه‌های اجتماعی و محیطی دارد. در بسیاری کشورها، این مفهوم با مقوله حفظ اطلاعات، که حریم خصوصی را در معنای مدیریت اطلاعات شخصی تفسیر می‌کند، پیوند خورده و در هم ادغام شده است.

در عین حال محافظت از حریم خصوصی معمولاً به عنوان ابزاری برای ترسیم محدوده خطوطی که جامعه می‌تواند در امور افراد دخالت کند، تلقی می‌شود. نبود یک تعریف خاص، به معنای کم‌اهمیتی این مفهوم نیست؛ به یک معنا، تمامی موارد حقوق بشر، جنبه‌ها و ابعادی از حق حریم خصوصی هستند.

در دهه ۱۸۹۰، دوتن از قضات دادگاه عالی ایالات متحده آمریکا به نامهای «ساموئل وارن» و «لوئیس براندیس» در مقاله‌ای با عنوان «حق حریم خصوصی» برای اولین بار این مسأله را به عنوان یک بحث جدی و صریح حقوقی مطرح و حریم خصوصی را «حق افراد برای تنها بودن» تعریف کردند. به نظر آنان، حریم خصوصی، از جمله ارجمندترین حقوق در یک دموکراسی است و حمایت از آن، باید در قانون اساسی بازتاب بیابد.۸

«رابرت الیس اسمیت»، سردبیر مجله حریم خصوصی، حریم خصوصی را چنین تعریف کرده است:

تمایل هر یک از ما به داشتن فضای فیزیکی که می‌توانیم در آن از مداخله، مزاحمت، اضطراب و آشفتگی یا پاسخ‌گویی رها باشیم و تلاش برای کنترل زمان و شیوه افشای اطلاعات شخصی در باره خودمان.۹

«ادوارد بلوشتاین»، رئیس پیشین دانشگاه نیوجرسی (راتگرز)، حریم خصوصی را علاقه به شخصیت انسانی می‌داند. به اعتقاد او حریم خصوصی از شخصیتِ محترم شمرده شده حمایت می‌کند، از استقلال فردی، منزلت و استحکام شخصیت.۱۰

بر اساس یک تعریف دیگر:

حریم خصوصی، حق افراد برای برخورداری از حمایت شدن در برابر مداخله بی‌اجازه دیگران در امور و زندگی خود و خانواده‌شان است؛ خواه این عمل با ابزار مستقیم فیزیکی صورت پذیرد یا به وسیله نشر اطلاعات. ۱۱

در مقدمه منشور حریم خصوصی استرالیا آمده است که یک جامعه آزاد و دموکراتیک به استقلال فردی احترام می‌گذارد و هرگونه تعدی دولت و بخش خصوصی را محدود می‌کند.۱۲

همچنان که از مجموع این تعاریف برمی‌آید، حریم خصوصی یک ارزش کلیدی وزیربنای توجه به شأن و منزلت انسانی و سایر ارزشها نظیر آزادی اجتماعات و آزادی بیان است. حریم‌خصوصی یک حق اساسی بشر و خواسته منطقی هر فردی است. ۱۳

۲. حوزه‌های حریم خصوصی

حریم خصوصی را می‌توان به چهار حوزه مجزا، اما مرتبط به یکدیگر تقسیم کرد:

«حریم اطلاعات» که شامل قوانینی است که اطلاعات شخصی نظیر اطلاعات مالی، پزشکی و دولتی افراد را تحت کنترل قرار می‌دهد. این حوزه به «حفظ اطلاعات» هم معروف است.

«حریم جسمانی» که به حفاظت از جسم افراد در مقابل آزمایشهای ژنتیکی، دارویی و نظایر آن‌مربوط می‌شود.

«حریم ارتباطات» که به امنیت پستهای الکترونی، تلفنها، پست و سایر اشکال ارتباطات توجه دارد.

«حریم مکانی» که به اِعمال مجموعه‌ای از محدودیتها و نظارتها در محیط کار و زندگی افراد وهمچنین اماکن عمومی مربوط می‌شود. حریم مکانی معمولا توسط نظارت ویدئویی و یا چک کردن‌هویت افراد، مورد تجاوز قرار می‌گیرد. ۱۴

۳. الگوهای مختلف حمایت از حریم خصوصی

به منظور حمایت از حریم خصوصی، چهار الگوی حمایتی در کشورهای مختلف جهان، رایج است. دربسیاری از کشورها، چند الگو و در کشورهایی که به این مفهوم توجه خاص دارند، تمام الگوها به طورهمزمان مورد استفاده قرار می‌گیرند.

الف) قوانین جامع

در بسیاری از کشورهای دنیا جمع‌آوری، استفاده و نشر اطلاعات شخصی، چه به وسیله دولت و چه به‌وسیله بخش خصوصی و هم‌چنین دفاع از سایر حوزه‌های حریم خصوصی، تابع یک قانون عمومی است. دستگاهی خاص نیز ناظر بر حسن اجرای این قانون است. الگوی قوانین جامع توسط اتحادیه اروپا و نوع دیگری از آن هم در کانادا و استرالیا پذیرفته شده و در حال اجراست.

ب) قوانین موردی

در بعضی از کشورهای جهان، مثل ایالات متحده آمریکا از اعمال قوانین کلی امتناع و به قوانین‌موردی بسنده کرده‌اند؛ به این معنی که بر حسب مورد و نیاز به وضع قوانین دست می‌زنند. در این موردها، به ساز و کارهایی برای حفظ حریم خصوصی نیاز است. نقطه‌ضعف اساسی این رویکرد آن است که با ورود هر فناوری جدید، مدتی زمان لازم است تا قانون مربوط به آن تصویب شود و در این فاصله آنچه می‌تواند آسیب ببیند، حریم خصوصی است. نبود قوانین حمایت کننده از حریم خصوصی افراد در برابر اینترنت یکی از مثالهای بارز این ضعف است. در بسیاری از کشورها، از قوانین موردی در جهت تکمیل قوانین جامع برای هر مقوله‌بندی خاص اطلاعات استفاده می‌شود؛ همچون ارتباطات دور، پرونده‌های پلیس، کارتهای اعتباری و ...

۴. تاریخچه توجه به حق حریم خصوصی

الف. حریم خصوصی در دوران باستان

به رسمیت شناختن حریم خصوصی ریشه‌ای عمیق در تاریخ دارد. در قرآن مجید، در سوره‌های نور و الحجرات و در کلام حضرت محمد(ص) بر ضرورت احترام به حریم خصوصی تأکید شده است. در انجیل نیز اشاره‌های فراوانی به حریم‌خصوصی شده است. در احکام یهودیان نیز از دیرباز مفهوم رهایی از مراقبت به رسمیت شناخته شده است. در یونان باستان و چین کهن نیز حمایتهایی از این حریم وجود داشته‌اند. ۱۵

حمایتهای حقوقی از این حریم صدها سال است که در کشورهای غربی وجود دارند. در سال ۱۳۶۱ میلادی، در انگلستان مأمورانی به کار گمارده شدند تا کسانی را که چشم‌چرانی می‌کنند یا فالگوش می‌ایستند دستگیر کنند. در سال ۱۷۶۵ میلادی، لرد کامدن بریتانیا، در رد یک حکم ورود به خانه و توقیف

اوراق، نوشت: «به راحتی می‌توان گفت در این کشور هیچ قانونی وجود ندارد که آنچه را مدعیان انجام داده‌اند توجیه کند؛ اگر چنین قانونی وجود داشت، همه آرامش را از جامعه می‌ربود، زیرا اوراق آدمها معمولاً عزیزترین مایملکی است که یک آدم می‌تواند داشته باشد». ویلیام پیت نماینده مجلس نوشت: «تنگدست‌ترین مردمان حق دارد در کلبه خود با تمام نیروهای شاه مخالفت کند. شاید کلبه او سست باشد، شاید سقف آن بلرزد، شاید باد آن را از جا بکند، شاید توفان وارد آن شود- شاید باران وارد آن شود ـ اما شاه انگلستان حق ندارد به آن وارد شود؛ هیچ‌کدام از نیروهای او نیز جرأت ندارند از آستانهٔ در ویرانهٔ آن گامی فراتر نهند».

کشورهای مختلف در طول قرنهای بعد، هر یک حمایت‌خاصی از حریم خصوصی را شکل دادند. در سال ۱۷۷۶ میلادی، مجلس سوئد قانون «دسترسی به اسناد عمومی» را تصویب کرد که براساس آن همه اطلاعاتی که در اختیار دولت است، باید برای مقاصد مشروع به کار گرفته شود. فرانسه نیز در سال ۱۸۵۸ انتشار اطلاعات خصوصی را ممنوع اعلام و برای تخطی‌کنندگان از این قانون جریمه‌های سختی وضع کرد. طبق قوانین نروژ در سال ۱۸۸۹، انتشار اطلاعات مربوط به «امور شخصی یا خانوادگی» ممنوع اعلام شد.
همچنان که اشاره شد در سال ۱۸۹۰، ساموئل وارن و لوئیس براندیس، حقوق‌دانان آمریکایی، نوشته‌ای مقدماتی درباره حق حریم خصوصی نوشتند و حق حریم خصوصی را همچون «حق رهایی از مزاحمت» تلقی کردند. در پی انتشار این نوشته، این تلقی از حریم خصوصی به تدریج در سراسر ایالات متحده به عنوان بخشی از حقوق عرفی پذیرفته شد. ۱۶
محک امروزین بین‌المللی برای حق حریم خصوصی را می‌توان در اعلامیه جهانی حقوق‌بشر یافت، که در آن به‌طور خاص حریم خصوصیِ مکانی و ارتباطاتی مورد حمایت قرار گرفته است. در ماده ۱۲ این اعلامیه آمده است:

حریم‌خصوصی، خانواده، خانه یا مکاتبات هیچکس نباید خودسرانه مورد تعرض قرار بگیرد و به شهرت و آبروی هیچکس نباید تعرض شود. همه حق دارند از حمایت قانونی در مقابل چنین مداخلات یا تعرضهایی برخوردار باشند. ۱۷

در بسیاری از معاهدات بین‌المللی در باره حقوق بشر، حریم خصوصی به‌طور خاص به عنوان یک حق به رسمیت شناخته شده است. ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی۱۸، ماده ۱۴ کنوانسیون ملل

متحد درباره کارگران مهاجر۱۹، و ماده ۱۶ کنوانسیون ملل متحد در حمایت از کودکان۲۰، از همین مضمون برخوردارند.

در سطح منطقه‌ای نیز برپایه معاهدات مختلف، این حقوق ضمانت اجرای قانونی یافته‌اند. در ماده هشت کنوانسیون اروپایی حمایت از حقوق بشر و آزادیهای اساسی سال ۱۹۵۰، آمده است:

۱. همه حق دارند که به حریم خصوصی و زندگی خانوادگی، خانه و مکاتبات آنها احترام گذاشته شود. ۲. هیچ مقام دولتی نباید به استفاده از این حق تعرض کند، مگر مطابق قانون و در صورتی که این کار برای مصالح امنیت ملی، امنیت جامعه، رفاه اقتصادی کشور، پیشگیری از بی‌نظمی یا تبهکاری، حفظ سلامت اخلاقی، یا برای حمایت از حقوق و آزادی‌های دیگران، در یک جامعه دموکراتیک ضروری باشد.۲۱

بر پایه این معاهده، شورای اروپایی حقوق‌بشر، و دیوان اروپایی حقوق‌بشر تشکیل شدند تا بر اجرای این معاهده نظارت کنند. هر دوی این نهادها در به اجرا گذاشتن حقوق حریم‌خصوصی فعال بوده‌اند و پیوسته در تفسیر ماده هشت، حمایت‌های گسترده از این حق را در نظرگرفته‌اند و محدودیتهای این حق را کم‌دامنه‌تر تفسیر کرده‌اند.۲۲ شورا در سال ۱۹۷۶ اعلام کرد:

«ازنظر بسیاری نویسندگان انگلوساکسون و فرانسوی، حق احترام به «زندگی خصوصی» عبارت است از حق برخورداری از حریم خصوصی، حق زندگی کردن دور از انظار عمومی تا آنجا که شخص می‌خواهد... اما از دیدگاه شورا، حق احترام به زندگی خصوصی به اینجا ختم نمی‌شود. این حق همچنین تا اندازه‌ای شامل حق ایجاد و گسترش روابط با دیگر انسان‌ها، بخصوص از لحاظ عاطفی و در جهت شکوفایی و ارضای شخصیت خویش نیز می‌شود.» ۲۳

دیوان اروپایی حقوق بشر نیز قوانین کشورهای عضو را مورد بررسی قرار داده و برای بسیاری از کشورهایی که نتوانسته‌اند استراق‌سمع و شنودگذاری توسط دولتها یا اشخاص را تحت ضابطه‌ای درآورند، مجازاتهایی در نظر گرفته است. این دیوان همچنین مواردی از دسترسی افراد به اطلاعات شخصی‌شان را در پرونده‌های دولتی بررسی کرده است تا مطمئن شود که روال مناسب برقرار است. دیوان، حمایتهای مندرج در ماده هشت را فراتر برده و آن را شامل اقداماتی کرده است که دولتها ظاهراً از آنها منع شده‌اند، اما به آن ممنوعیت توجهی ندارند.

استفاده از معاهدات منطقه‌ای دیگر برای حفاظت از حریم‌خصوصی نیز شروع شده است. در ماده ۱۱ کنوانسیون آمریکایی حقوق بشر، حق حریم‌خصوصی با تعاریفی مشابه اعلامیه جهانی حقوق بشر وضع

شده است. در سال ۱۹۶۵، سازمان کشورهای آمریکایی، بیانیه آمریکایی حقوق و وظایف انسان را صادرکرد که در آن حفاظت از بسیاری حقوق انسانی، از جمله حریم خصوصی، خواسته شده بود. دیوان حقوق‌بشر قاره آمریکا، رسیدگی به مسائل حریم‌خصوصی را در پرونده‌های خود آغاز کرده است. ۲۴

ب. حریم خصوصی در قوانین اساسی ایران

ضرورت رعایت حریم خصوصی افراد در اصول ۹، ۱، ۲۲ و ۲۳ متمم قانون اساسی مشروطیت (۲۹ شعبان ۱۳۲۵ هجری قمری) چنین مورد توجه قرار گرفته است:

اصل نهم

افراد مردم از حیث جان و مال و مسکن و شرف محفوظ و مصون از هر نوع تعرض هستند و متعرض احدی نمی‌توان شد مگر به حکم و ترتیبی که قوانین مملکت معین می‌نمایند.

اصل سیزدهم

منزل و خانه هر کس در حفظ و امان است، در هیچ مسکنی قهرا نمی‌توان داخل شد مگر به حکم و ترتیبی که قانون مقرر نموده.

اصل بیست و دوم

مراسلات پستی کلیه محفوظ و از ضبط و کشف مصون است مگر در مواردی که قانون استثناء می‌کند.

اصل بیست و سوم

افشاء یا توقیف مخابرات تلگرافی بدون اجازه صاحب تلگراف ممنوع است مگر در مواردی که قانون معین می‌کند. ۲۵

در اصول ۲۲ و ۲۵ قانون اساسی جمهوری اسلامی نیز ضرورت رعایت حریم خصوصی افراد چنین مورد تأکید قرار گرفته است:

اصل بیست و چهارم

حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند.

اصل بیست و پنجم

بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون. ۲۶

پ. تحول در حفاظت داده‌ها

با ظهور فنآوری اطلاعاتی، توجه به حق حریم‌خصوصی در دهه‌های ۱۹۶۰ و ۱۹۷۰ میلادی افزایش یافت. توان بالقوه سیستمهای نیرومند کامپیوتری در پاییدن، لزوم تدوین قواعد خاصی برای نظارت بر جمع‌آوری و رفتار با اطلاعات شخصی را مطرح کرد. در سیر تکوین قانون‌گذاری مدرن در این عرصه، نخستین قانون حفاظت داده‌ها در جهان را می‌توان قانونی دانست که در سال ۱۹۷۰ میلادی در استان هس آلمان [استانی در غرب آلمان که مرکز آن ویسبادن است] به اجرا گذاشته شد. این سیر قانون‌گذاری سپس در کشورهای دیگر پی گرفته شد؛ در سوئد(۱۹۷۳)، ایالات متحده(۱۹۷۴)، آلمان(۱۹۷۷)، و فرانسه(۱۹۷۸). ۲۷

دو سند مهم بین‌المللی از این قوانین پدید آمد. در معاهده سال ۱۹۸۱ شورای اروپا برای حفاظت از افراد در برابر پردازش خودکار داده‌های شخصی۲۸ و در رهنمودهای سازمان همکاری و توسعه اقتصادی ناظر بر حفظ حریم خصوصی و جریان فرامرزی داده‌های شخصی۲۹ قواعد خاصی برای رفتار با داده‌های الکترونی وضع شد. در این قواعد، اطلاعات شخصی، داده‌هایی شمرده می‌شوند که باید در همه مراحل، از جمع‌آوری تا نگهداری و تا انتشار تحت حفاظت باشند.

عبارت حفاظت داده‌ها در بیانیه‌ها و قوانین مختلف متفاوت است. اما همه آنها متضمن آن است که اطلاعات شخصی باید:

ـ منصفانه و قانونی به دست آیند؛

ـ تنها به همان مقصودی که از ابتدا مشخص شده استفاده شوند؛

ـ به اندازه متناسب و مربوط جمع‌آوری شوند، نه بیش از حد مقصود؛

ـ صحیح و به‌هنگام باشند؛

ـ برای خود شخص قابل دسترس باشند؛

ـ محرمانه نگه‌داشته شوند؛ و

ـ پس از تکمیل مقصود، نابود شوند. ۳۰

این دو توافقنامه اثری عمیق بر اجرای قوانین در سراسر جهان داشته است. حدود ۳۰ کشور کنوانسیون شورای اروپا را امضا کرده‌اند. رهنمودهای سازمان همکاری و توسعه اقتصادی نیز به‌طور وسیعی در قوانین ملی کشورها، حتی کشورهای غیرعضو این سازمان، به کار بسته شده است. ۳۱

ت. رهنمودهای اتحادیه اروپا در حفاظت داده‌ها

در سال ۱۹۹۵، اتحادیه اروپا رهنمود حفاظت از داده‌ها را وضع کرد تا قوانین کشورهای عضو را در فراهم آوردن سطح مناسبی از حفاظتها برای شهروندان و تضمین جریان آزاد اطلاعات شخصی در درون اتحادیه اروپا هماهنگ کند. این رهنمود یک پایه مشترک در مورد حریم‌خصوصی وضع می‌کند که نه فقط قانون

حفاظت داده‌های کنونی را تقویت می‌کند، بلکه یک رشته حقوق جدید را نیز مطرح می‌سازد. این حقوق جدید مربوط به پردازش اطلاعات شخصی در پرونده‌های الکترونی و دستی است. ۳۲

یک مفهوم اصلی در مدل حفاظت داده‌ها در اروپا، «قابلیت اجرا» است. کسانی که داده‌ها مربوط به آنهاست حقوقی دارند که در قواعد و مقررات به روشنی تصریح شده است. در هر کشور عضو اتحادیه اروپا، یک مقام بلندپایه یا یک نهاد حفاظت داده‌ها وجود دارد که این قواعد را به اجرا می‌گذارد. انتظار می‌رود کشورهایی هم که با اروپاییان تجارت دارند، ناچار باشند کنترلی در همین سطح فراهم آورند.

اصول بنیادی که در رهنمود آمده عبارتند از: حق دانستن این که داده‌ها از کجا آمده‌اند؛ حق این که داده‌های نادرست تصحیح شوند؛ حق مطالبه خسارت در صورت پردازش غیرقانونی؛ و حق منع اجازه استفاده از داده‌ها در برخی شرایط. به عنوان مثال، افراد حق دارند خود را از قرار گرفتن تحت تبلیغات بازرگانی مستقیم [ارسال اوراق و مطالب تبلیغاتی به نشانی شخصی] در امان بدارند. این رهنمود شامل حفاظتهای نیرومندی ازحریم‌خصوصی در قبال بهره‌برداری از داده‌های حساس شخصی نظیر داده‌های مربوط به تندرستی، زندگی جنسی یا عقاید مذهبی و فلسفی است. در آینده، استفاده تجاری و دولتی از چنین داده‌هایی عموماً مستلزم جلب رضایت «صریح و غیرمبهم» کسی است که داده‌ها مربوط به اوست.۳۳

رهنمود سال ۱۹۹۵، کشورهای عضو را موظف می‌کند تا تضمین کنند که اطلاعات شخصی مربوط به شهروندان اروپا هنگامی که به خارج صادر می‌شود، و در کشورهای بیرون از اتحادیه اروپا پردازش می‌گردد، از همان سطح حفاظت در داخل اروپا برخوردار باشد. این الزام باعث شده است که کشورهای بیرون اروپا زیر فشار فزاینده‌ای برای تصویب قوانین حریم‌خصوصی قرار گیرند. کشورهایی که از وضع قوانین حریم‌خصوصی مناسب خودداری ورزند ممکن است دیگر نتوانند در جریان برخی تبادلات اطلاعاتی با اروپا قرار گیرند؛ به‌خصوص اگر این اطلاعات شامل داده‌های حساس باشد.۳۴

در سال ۱۹۹۷، اتحادیه اروپا رهنمود ۱۹۹۵ را با ابلاغ رهنمود حریم‌خصوصی ارتباطات دور، کامل کرد. در این رهنمود، حفاظتهای خاصی تأمین شد که تلفن، تلویزیون دیجیتال، شبکه‌های موبایل، و دیگر سیستمهای ارتباطات‌دور را شامل می‌شد. تکالیف گسترده‌ای بر عهده ارائه‌دهندگان خطوط و ارائه‌دهندگان خدمات گذاشته شد تا ضامن حریم خصوصی کاربران ارتباطی، از جمله فعالیتهای مربوط به اینترنت باشد. این بخشنامه، عرصه‌های مختلفی را تحت پوشش قرار داد که تا آن زمان در شکاف‌های میان قوانین حفاظت‌داده‌ها قرار می‌گرفتند. دسترسی به داده‌های صورت‌حسابی و همچنین فعالیتهای تبلیغاتی و بازاریابی به شدت محدود شد. الزامی شد که در فناوری «تشخیص شماره تلفن فرستنده» (کالر آی‌دی) گزینه‌ای

برای مسدود کردن ارسال شماره تلفن گنجانده شود. الزامی شد اطلاعاتی که برای برقراری یک تماس جمع‌آوری می‌شود، به محض برقراری تماس، پاک شود.۳۵

در ژوئیه ۲۰۰۰، شورای اروپا پیشنهاد یک رهنمود جدید را برای حریم‌خصوصی در بخش ارتباطات الکترونی صادر کرد. ۳۶ این پیشنهاد به عنوان بخشی از یک مجموعه بزرگتر رهنمودهای ارتباطات‌دور مطرح شد که هدف آن قوت بخشیدن به رقابت در بازار ارتباطات الکترونی اروپا بود. این بخشنامهٔ جدید، در شکل اولیه پیشنهادی، با گسترده‌تر کردن حفاظتهایی که تا آن موقع برای ارتباطات‌دور وجود داشت به مقوله‌ای وسیع‌تر و غیروابسته‌تر به فناوری «ارتباطات الکترونی»، باعث قوت حقوق حریم‌خصوصی می‌شد. اما در جریان بحث‌های پیرامون این پیشنهاد، وزیران شورای اروپا شروع کردند به فشار آوردن برای کنارگذاشتن موارد مربوط به نگهداری داده‌ها، که بر اساس آن ارائه‌دهندگان خدمات اینترنتی و گردانندگان ارتباطات‌دور باید سابقه همه تماسهای تلفنی، نامه‌های الکترونی، فاکسها، و فعالیتهای اینترنتی را به منظور استفاده‌های نیروهای انتظامی ذخیره می‌کردند. این پیشنهادها به شدت از سوی اکثر اعضای پارلمان اروپا مورد مخالفت قرار گرفت. در ژوئیه ۲۰۰۱، کمیته آزادیهای مدنی پارلمان اروپا پیش‌نویس رهنمود را بدون قسمت مربوط به نگهداری داده‌ها تصویب کرد:

«کمیته آزادیهای مدنی حمایت خود را از نظارت دقیق بر دسترسی مقامات انتظامی به داده‌های شخصی شهروندان، نظیر ترافیک ارتباط و محل داده‌ها ابراز می‌دارد. این تصمیم بنیادی است؛ زیرا به این ترتیب پارلمان اروپا مانع تلاشهای دولتهای اتحادیه اروپا در داخل شورا می‌شود که می‌خواهند با پیروی از مدل اشلون[شبکه گسترده استراق‌سمع ایالات متحده در سراسر جهان]، شهروندان خود را به‌طور عام‌وگسترده زیرنظر بگیرند.» ۳۷

اما در پی حوادث یازدهم سپتامبر، جو سیاسی تغییر کرد و پارلمان اروپا زیر فشار فزاینده دولت‌های عضو قرار گرفت تا پیشنهاد شورا برای ردگیری داده‌ها را تصویب کند. به‌خصوص، بریتانیا و هلند این پرسش را به میان کشیدند که در قواعد پیشنهاد شده برای حریم‌خصوصی آیا هنوز «با توجه به نبرد بر ضد تروریسم، توازن صحیحی میان حریم‌خصوصی و الزامهای مؤسسات انتظامی برقرار است». پارلمان اروپا ایستادگی کرد و تا چند هفته قبل از رأی‌گیری نهایی(یعنی تا ۳۰ مه ۲۰۰۲)، اکثریت اعضای پارلمان مخالف هرگونه ردگیری داده‌ها بودند. اما سرانجام پس از فشارهای زیاد از ناحیه شورای اروپا و دولتهای عضو اتحادیه اروپایی، و لابی سازمان‌یافته دو نماینده اسپانیایی، دو جناح عمده سیاسی پارلمان (احزاب چپ‌میانه و راست‌میانه) به توافق رسیدند تا به نفع موضع شورا رأی بدهند. ۳

در ۲۵ ژوئن ۲۰۰۲، شورای اتحادیه اروپایی بخشنامه جدید حریم خصوصی و ارتباطات الکترونی را که در مجلس به آن رأی داده شده بود تصویب کرد. بر اساس بخشنامه جدید، اکنون دولتهای عضو اتحادیه اروپایی می‌توانند قوانینی وضع کنند که حفظ داده‌های ترافیکی و محل همه نوع ارتباطات را مجاز بدارد؛ ارتباطات از طریق تلفنهای موبایل، اس‌ام‌اس، تلفنهای زمینی، فاکس، پست الکترونیکی، چت‌رومها، اینترنت، یا هر وسیله ارتباطی الکترونی دیگر. چنین الزاماتی می‌تواند برای مقاصد مختلف به کار بسته شود، از امنیت ملی گرفته تا جلوگیری، تحقیق و پیگرد اقدامات تبهکارانه.

در دیگر عرصه‌ها، بخش‌نامه حریم‌خصوصی و ارتباطات الکترونی نتیجه مطلوب‌تری داشت. برای مثال، در این بخشنامه تعاریف و حمایتهای جدیدی برای «تماسها»، «ارتباطات»، «داده‌های ترافیک»، و «محل داده‌ها»، ارائه شد که حق حریم خصوصی مصرف‌کننده و کنترل او بر همه انواع پردازش داده‌ها را قوت می‌بخشد. این مواد جدید حفاظت از همه نوع، انتقال اطلاعات از طریق اینترنت، ممنوعیت تبلیغات تجاری ناخواسته و بدون رضایت توسط پست‌الکترونی، ارسال «هرزنامه»، و حفاظت کاربران تلفن‌های موبایل از ردگیری و تحت نظر بودن، را تضمین می‌کند. این بخش‌نامه همچنین به مشترکان همه خدمات ارتباطات الکترونی(همچون مکان‌یابی ماهواره‌ای ـ GSM و پست الکترونی) این حق را می‌دهد که خود انتخاب کنند که در فهرست‌های عمومی قرار بگیرند یا نه. ۳۹

ث. مقامات ناظر بر رعایت حریم خصوصی و حفاظت داده‌ها

در اکثر کشورهای دارای قانون حریم‌خصوصی یا حفاظت داده‌ها، یک مقام مسئول یا یک نهاد وجود دارد که بر اجرای قانون نظارت می‌کند. قدرت این مقامات، که «عضو کمیسیون»، «مأمور رسیدگی»، یا «مسؤول دفتر» نامیده می‌شوند، از کشوری به کشور دیگر بسیار متفاوت است. در برخی کشورها همچون آلمان و کانادا، مقامات یا اداراتی در سطح استانی یا ایالتی هم برای این منظور وجود دارد. ۴۰

طبق ماده ۲۸ بخشنامه حفاظت داده‌ها اتحادیه اروپا، همه کشورهای عضو اتحادیه اروپا باید یک نهاد مستقل برای اجرای این قانون داشته باشند. طبق بخشنامه، این نهادها دارای قدرت چشمگیری هستند: دولتها هنگام تنظیم قوانین مربوط به پردازش اطلاعات شخصی باید با این نهاد مشورت کنند؛ این نهادها همچنین اختیار دارند که دست به تحقیق و تفحص بزنند و حق دسترسی به اطلاعات مربوط به تحقیقات خود را دارند؛ این نهادها می‌توانند دستوراتی برای از بین بردن اطلاعات یا ممنوعیت پردازش، و شروع مراحل حقوقی، استماع شکایتها و انتشار گزارشها صادر کنند. آنان معمولاً مسئول آموزش همگانی و پیوند بین‌المللی در حفاظت داده‌ها و انتقال داده‌ها نیز هستند.

از جمله وظایف دیگر این نهادها جلب توجه همگانی به عرصه‌های مسأله‌ساز است. آنان می‌توانند این کار را از طریق ترویج نظام‌نامه‌های عملی و تشویق اتحادیه‌های صنعتی به پذیرش این نظام‌نامه‌ها انجام دهند. آنها همچنین می‌توانند با گزارشهای سالانه‌ای که منتشر می‌کنند، مشکلات را یادآور شوند. به طور مثال، در کانادا، مقام مسئول حریم خصوصی، در گزارش سال ۲۰۰۰ خود از وجود یک بانک اطلاعاتی گسترده که در اختیار دولت فدرال است خبر داد. به محض انتشار این گزارش، وزارت مربوطه بانک اطلاعاتی را منحل کرد. ۴۱

البته چنان که در گزارش جهانی حریم خصوصی در سال ۲۰۰۲ آمده است، این نهادها با دشواریهایی نیز مواجهند. افزون بر کمبود منابع مالی و انسانی برای انجام امور، معضل عدم استقلال نیز در میان است. در بسیاری کشورها، این نهادها تحت کنترل بازوی سیاسی دولت یا بخشی از وزارت دادگستری هستند و اختیار یا اراده‌ای برای پیشبرد حریم‌خصوصی یا انتقاد از پیشنهادهای لطمه‌زننده به حریم‌خصوصی ندارند. در ژاپن و تایلند، نهاد نظارتی تحت کنترل دفتر نخست‌وزیری است. در تایلند، در سال ۲۰۰۰ پس از کشمکشهای میان دفتر نخست‌وزیر و این نهاد، مدیر این نهاد تغییر داده شد. در سال ۲۰۰۱، اسلونی در قانون حفاظت داده‌ها اصلاحاتی انجام داد تا یک نهاد مستقل نظارتی برپا شود و سازگاری این قانون با بخشنامه حفاظت داده‌ها تضمین گردد. این کار پیشتر بر عهده وزارت دادگستری بود. در برخی کشورها نیز که اداره مجزایی برای این کار وجود ندارد، نقش تحقیق و تفحص و به اجرا گذاشتن قانون را یک مقام مسئول حقوق‌بشر یا یک مقام پارلمانی ایفا می‌کند. ۴۲

ج. جریان فرا مرزی داده‌ها و مناطق‌بدون محدودیت قانونی

راحتی جریان یافتن داده‌های الکترونی به فراسوی مرزها، باعث این نگرانی شده است که قانون حفظ داده‌ها به سادگی با انتقال اطلاعات شخصی به کشورهای ثالث که در آنجا قانون ملی کشور اصلی کاربرد ندارد، دور زده شود. این داده‌ها می‌تواند سپس در آن کشورها که به «بهشت‌های داده‌ها» معروفند، بدون هیچ محدودیتی پردازش شود. ۴۳

به همین دلیل، اکثر قوانین حفاظت داده‌ها شامل محدودیتهایی نیز برای انتقال اطلاعات به کشورهای ثالث می‌شود؛ مگر این که اطلاعات در کشور مقصد نیز حفاظت شود. به‌طور مثال، طبق ماده ۱۲ کنوانسیون ۱۹۸۱ شورای اروپا محدودیتهایی برای جریان فرامرزی داده‌های شخصی وجود دارد. ۴۴ همچنین، طبق ماده ۲۵ رهنمود اروپا، این تکلیف بر عهده کشورهای عضو گذاشته شده است که تضمین کنند هر گونه اطلاعات مربوط به شهروندان اروپایی هنگام صدور به خارج و پردازش در کشورهای بیرون از اروپا حفاظت می‌شود. در این ماده آمده است:

«کشورهای عضو باید ترتیبی بدهند که انتقال داده‌های شخصی به یک کشور ثالث، تنها در صورتی انجام شود که کشور مربوطه تضمین کند که در پردازشی که انجام می‌دهد یا در پردازشی که قصد دارد پس از انتقال انجام دهد، حفاظت مقتضی از داده‌ها به عمل می‌آید.» ۴۵

این الزام باعث فشارهای فزاینده‌ای در خارج از اروپا برای تصویب قوانین نیرومند حفاظت داده‌ها شده است. آن کشورهایی که از تصویب قوانین مناسب حریم‌خصوصی‌خودداری ورزند، قادر نخواهند بود در تبادل برخی اطلاعات با اروپا قرار گیرند؛ به‌خصوص اگر این اطلاعات شامل داده‌های حساس باشد. تعیین این که وضعیت حفاظت از حریم‌خصوصی در یک کشور ثالث به چه اندازه است، با شورای اروپاست. ۴۶

چ. توافقنامه «بندر امن» اتحادیه اروپا ـ ایالات متحده

در سال ۱۹۹۸، ایالات متحده مذاکراتی را با اتحادیه اروپایی برای آنچه از آن پس توافقنامه «بندر امن» نامیده شد، آغاز کرد. آنچه به طور رسمی به عنوان هدف این مذاکرات بیان شد، دستیابی به یک تضمین برای تداوم جریان فرامرزی داده‌های شخصی بود. در پی این توافق شرکتهای ایالات متحده داوطلبانه متعهد شدند که به مجموعه‌ای از اصول حریم خصوصی تدوین شده از سوی وزارت بازرگانی ایالات متحده و هیئت‌مدیره بازار داخلی کمیسیون اروپا پای‌بند بمانند. به این ترتیب، فرض بر این قرار گرفت که این شرکتها دارای استاندارد مقتضی هستند و می‌توانند به دریافت داده‌های شخصی از اتحادیه اروپا ادامه دهند. مذاکرات در مورد پیش‌نویس اصول «بندر امن» حدود دو سال به‌طول انجامید و مورد انتقادهای شدید از سوی طرفداران حریم‌خصوصی و گروههای حمایت از مصرف‌کننده قرار گرفت. در اوایل ژوئیه همان سال، پارلمان اروپا قاطعانه تصویب کرد که بار دیگر در باره توافقنامه «بندر امن» مذاکراتی صورت بگیرد تا حفاظت مقتضی داده‌ها تأمین شود. ۴۷

در ۲۶ ژوئیه ۲۰۰۰، کمیسیون موافقت‌نامه را تصویب کرد و در عین حال قول داد که اگر غرامتهایی که به شهروندان اروپایی تعلق می‌گیرد ناکافی از آب دربیاید، مذکرات بر سرتوافق‌نامه را از سر بگیرد. به کشورهای عضو اتحادیه اروپا ۹۰ روز فرصت داده شد تا تصمیم کمیسیون را به اجرا بگذارند. شرکتهای ایالات متحده از نوامبر ۲۰۰۰ پیوستن به توافقنامه «بندر امن» را آغاز کردند. برای شرکت‌های آمریکایی امضاءکننده قرارداد یک دوره بدون محدودیت برای به اجرا گذاشتن اصول در نظر گرفته شده است.

طبق اصول این توافق‌نامه تمام سازمانهای امضاکننده ملزم هستند به طور «روشن و آشکار» به اطلاع افراد برسانند که چه نوع اطلاعاتی جمع‌آوری می‌کنند، این اطلاعات برای چه مقاصدی ممکن است مورد استفاده قرار گیرد و نزد چه اشخاص ثالثی ممکن است فاش شود. این آگاهی‌دادن باید در همان زمان

جمع‌آوری اطلاعات شخصی یا «بلافاصله پس از عملی شدن» صورت بگیرد. به افراد باید این قدرت داده شود که با جمع‌آوری داده‌ها مخالفت کنند، چه در جایی که این اطلاعات قرار است نزد اشخاص ثالث فاش شود و چه در جایی که برای مقصود نامناسبی مورد استفاده قرار گیرد. در خصوص اطلاعات حساس، باید رضایت صریح افراد به دست آید. سازمانهایی که مایل به انتقال داده‌ها به اشخاص ثالث هستند، تنها در صورتی می‌توانند این کار را انجام دهند که آن شخص ثالث یا مشترک «بندر امن» شود یا توافق‌نامه‌ای برای حفاظت داده‌ها امضا کند. سازمانها باید احتیاطهای لازم برای حفاظت از اطلاعات امنیتی به عمل آوردند تا این اطلاعات گم نشوند، مورد سوءاستفاده قرار نگیرند، نتوان به آنها دسترسی غیرمجاز داشت، آنها را فاش کرد، تغییر داد و یا از بین برد. سازمانها باید دسترسی افراد را به هر گونه اطلاعات شخصی مربوط به خود آنها تأمین کنند و فرصت تصحیح، اصلاح، یا حذف اطلاعات نادرست را برای آنها فراهم آورند. این حق تنها در مواردی داده می‌شود که هزینه یا بار تأمین دسترسی بی‌تناسب، با خطراتی که حریم‌خصوصی فرد را تهدید می‌کند، همراه نباشد یا در شرایطی که حقوق اشخاصی غیر از فرد مورد تخطی قرار نگیرد. در مورد اجرای قانون، سازمانها باید امکان برخورداری از سازوکارهای مستقل اعاده حقوق را که به راحتی در دسترس و در استطاعت باشد برای افراد فراهم کنند؛ سازوکارهایی که از طریق آن بتوان شکایتها را مورد بررسی قرار داد و خسارتها را جبران کرد. سازمانها باید روال رسیدگی به شکایات را سرعت بخشند و مجازاتهایی را که بابت عدم رعایت اصول تجویز می‌شود، رعایت کنند.

گروه‌های حمایت از مصرف‌کننده و طرفدار حریم‌خصوصی هم در ایالات متحده و هم در اروپا به شدت نسبت به تصویب این موافقت‌نامه از سوی کمیسیون اروپا انتقاد دارند. آنها می‌گویند با این موافقت‌نامه حفاظت مقتضی از داده‌های شخصی شهروندان اروپایی تأمین نمی‌شود. توافق‌نامه بر پایه یک سیستم خودگردان قرار دارد که در آن شرکتها فقط قول می‌دهند که از رویه‌های حفظ حریم‌خصوصی که اعلام کرده‌اند تخطی نکنند. ضمانت اجرایی یا بررسی منظمی از شکایات وجود ندارد. کافی است یک شرکت خود گواهی بدهد تا به عضویت «بندر امن» درآید. هیچ حق فردی برای دادخواهی یا حق مطالبه خسارت برای تجاوز به حریم‌خصوصی وجود ندارد. برای اجرای اصول یک دوره نامحدود در اختیار شرکتهای امضاکننده آمریکایی قرار داده شده است. قرارداد فقط برای شرکتهایی که تحت نظارت کمیسیون تجارت فدرال و وزارت راه‌وترابری قرار دارند (به غیر از بخشهای مالی و ارتباطات‌دور) کاربرد خواهد داشت و استثناهای خاصی نیز وجود دارد که برای سوابق اطلاعاتی عمومی تحت حفاظت قانون اتحادیه اروپایی در نظر گرفته شده است. ۴۸

در فوریه ۲۰۰۲، کمیسیون اروپا گزارشی در مورد کارکرد عملی توافقنامه «بندر امن» اتحادیه اروپا و ایالات متحده منتشر کرد.۴۹ این نخستین گزارشی بود که در آن توفیق این توافقنامه بررسی شده بود. در این گزارش نتیجه گیری شد که همه عناصر اساسی موافقت‌نامه به مورد اجرا گذاشته شده و اگر افراد احساس کنند به حقوق آنها تجاوز شده، ساختاری برای طرح شکایتها موجود است. اما در این گزارش معلوم شد که نه شفافیت کافی در میان سازمانهایی که درخواست عضویت در «بندر امن» را امضا کرده‌اند وجود دارد و نه همه راه‌حلهایی که برای اختلافات با اتکا به اجرای اصول بندر امن ارائه می‌شود، عملاً با اصول حریم‌خصوصی مندرج در خود توافق‌نامه همخوان است. ۵۰

۵. تهدیدها علیه حریم خصوصی

حال که به جنبه‌های گوناگون مفهومی حریم خصوصی پرداختیم، مناسب است به منابع اصلی تهدیدکننده حریم خصوصی در جامعه معاصر نیز نگاهی هرچند گذرا داشته باشیم.

به اعتقاد مارک روتن‌برگ تهدید علیه حریم خصوصی در دوران معاصر سه منشأ اصلی دارد: فناوری، حکومت و بخش خصوصی.

الف. فناوری

روتن‌برگ گرچه فناوری را منبع بسیاری از نگرانیها در بارهٔ حریم خصوصی می‌داند، اما اعتقاد دارد که تبیین ارتباط میان فناوری و نظارت بر حریم خصوصی شهروندان چندان آسان نیست.

فناوری شکلهای خاصی به خود می گیرد و چه بسا از طریق فرایندی که به مثابه دیالکتیک ایجاد هدفمند نظام خاص نظارت فهم می شود، به اتخاذ نظامهای تازه نظارت منجر شود. مقصود آن‌که پیشرفت ابزارهای نظارت به ایجاد نظام هدفمند نظارت می‌انجامد. آدمی وسوسه می شود که این فرایند را به مثابه فرایندی بالنسبه خودمختار ملاحظه کند، لیکن پاسخ‌گو بودن انسان نباید در هیچ نظام نظارتی نادیده انگاشته شود.۵۱

روتن‌برگ سه ویژگی فناوری در قلمرو نظارت را چنین بر می شمارد:

۱. تقویت مقصود روتن‌برگ از «تقویت»، توانایی فناوری در افزایش قدرت گردآوری اطلاعات و دخالت در زندگی خصوصی است. مثالهایی که او برای بیان مقصود خود ارائه می دهد، معطوف به تواناییهای حسی هستند.

لنز زوم روی دوربین به گزارشگر امکان می‌دهد، فاصله‌ای دورتر را مشاهده و رویدادهایی را ثبت کند که به گونه‌ای دیگر امکان‌پذیر نیست. ابزار شنود به مأمور پلیس امکان می‌دهد که یک ارتباط شخصی را استراق سمع کند و یا برحسب اتفاق بشنود. فنون جدید تصویرپردازی حرارتی به پلیس امکان می‌دهند تا دریابد آیا در خانه ای لامپهای مخصوص کشت ماری‌جوانا روشن هستند یا نه.۵۲

اما به اعتقاد روتن‌برگ این تمامی ماجرا نیست. امکان تقویت، اطلاعات به مراتب بیشتری از آنچه در آغاز مقصود بوده است، فراهم می‌کنند:

لنزهای پاپاراتزی [روزنامه نگار زرد] که برای عکسبرداری از یک چهره سرشناس به کار می‌رود، چه بسا لحظه‌ای شخصی و خصوصی را ثبت کنند. وسیله شنودی که پلیس برای پیگیری فعالیتهای یک جنایتکار نصب کرده، چه بسا گفت‌وگوی بی گناهان را نیز ضبط کند. ممکن است ابزار تصویرپردازی حرارتی، از پس دیوار آپارتمانی که مظنون به کشت ماری جواناست، به نمایش عشق بازی دو نفر در طبقه بالای آن آپارتمان بپردازد. ۵۳

۲. عادی سازی. روتن‌برگ ویژگی دوم تهدیدآمیز فناوری علیه حریم خصوصی را «عادی‌سازی» نام می‌نهد. مقصود او از این اصطلاح، توجه به فرایند ورود فناوری نظارت به زندگی به مثابه فرایندی جاری و طبیعی است. در حقیقت از این منظر، فناوری برای استقرار الگو یا شیوه نظارت مورد استفاده قرار می‌گیرد. مثالی که او برای روشن شدن بحث ارائه می‌دهد، هر دو جنبه مثبت و منفی این ویژگی را بیان می‌کند:

دوربینی که برای ضبط تصویر صندوق بانک روشن است، احتمالا مثال مثبتی از استفاده مناسب از فناوری نظارت است، زیرا از بانک در برابر سرقت و از مشتری یا به هنگام بروز یک نزاع ساده مراقبت می‌کند. اما دوربینی که در اتاق پروو یک فروشگاه بزرگ نصب شده چه بسا بسیار مشکل ساز شود. می توان استدلال کرد که هدف از نصب این دوربین جلوگیری از سرقت در فروشگاه است و به این ترتیب از هزینه‌های غیر ضروری صاحب فروشگاه می‌کاهد، اما این احتمال نیز وجود دارد که مشتریان در اتاق پروو دوربین را بسیار مزاحم بدانند.۵۴

روتن‌برگ در این فراز از بحث خود به یک موضوع فنی دیگر نیز اشاره می‌کند: فناوریهای عادی شده به‌طور فزاینده‌ای از امکان ضبط برخوردار شده اند. مثال بارز این ویژگی ضبط تمام صحنه‌های در دسترس توسط دوربینهای راهنمایی و رانندگی است که در چهارراه‌ها نصب شده اند. به اعتقاد روتن‌برگ، این هنوز مرحله نخست حضور فناوریهای نظارت عادی شده در زندگی ماست. مرحله دوم، کاربرد روشهایی برای پردازش اطلاعات ضبط شده است. مثال او هول‌انگیز است: به کمک یک دوربین می‌توان از درون هواپیما، چهره مسافران منتظر در ترمینال فرودگاه را دید، تصویر هر چهره را به پایگاه اطلاعات تصاویر چهره‌ها منتقل و پردازش کرد و به این ترتیب هویت واقعی هر مسافر را شناسایی نمود.

۳. تصعید. تصعید به ناممکن شدن روزافزون کشف فناوری تهاجم به حریم خصوصی از سوی شهروندان اشاره دارد. بنا بر توضیح روتن‌برگ، دوربینهای مخفی، ابزارهای شنود و فناوریهای گردآوری داده و اطلاعات چنان گسترده و فراگیرند که مجالی برای گریز شهروندان از پیگیری باقی نگذاشته اند؛ به ویژه از آن رو که کلیت این گونه مراقبت‌ها را قانون نیز تجویز و حمایت می‌کند.

ب. حکومت

به اعتقاد روتن‌برگ جدی ترین تهدیدها علیه حریم خصوصی از جانب دولتهاست.

در افراطی‌ترین نوع رفتار، هنگامی‌که حکومت، فردی را دستگیر و روانه زندان می‌نماید، منزلت حریم خصوصی وی را تقریباً به‌طور کامل نفی می‌کند. حکومت همچنین می‌تواند حریم خصوصی را از طریق برنامه‌هایی برای تعیین اجباری هویت، آزمایش مواد مخدر، تجسس بدنی یک فرد یا جست‌وجودرخانه‌اش، حفظ و پردازش مشخصات افراد در پایگاههای داده‌ها، انجام آزمایشهای ژنتیک و دروغ سنج از بین ببرد. اینها تنها شمار اندکی از وسایل هستند. ۵۵

بنا بر توضیح روتن‌برگ، ویژگی تهدیدهای حکومت علیه حریم خصوصی آن است که به محض استقرار، شهروندان دیگر نمی‌توانند از انجام خواستهای حاکمیت سر باز بزنند و لاجرم باید اطلاعات مورد نظر را در اختیار حکومت قرار دهند. وی با توجه به اقتدار حکومت برای ورود به حوزه حریم خصوصی شهروندان به نکته‌ای در خور تأمل اشاره می‌کند:

شفافیت، که هدف بسیار ستودنی کارکرد جامعه دموکراتیک است، در بافت نظارت حکومتی معنای متفاوتی به‌خود می‌گیرد. حکومت، به‌طورمعمول، خواستار «شهروندی شفاف» است؛ مردمی‌که کنشهایشان به سادگی قابل تشخیص و به آسانی قابل نظارت است. ۵۶

پ. بخش خصوصی

حریم خصوصی شهروندان با ابزارهای گوناگونی که بخش خصوصی امروزه برای گسترش فعالیتهای اقتصادی خود به کار می‌گیرد نیز در معرض تهدید است. این تهدید از نظر روتن‌برگ جنبه‌های گوناگونی دارد:

در محیط کار، شرکتها در تلاش برای اعمال کنترل بیشتر بر کارکنان خود از طریق مجموعه‌ای از شیوه‌های نظارت و کنترل هستند. این شیوه‌ها شامل شنود مکالمات تلفنی، بررسی اطلاعات درون رایانه‌هایی که کارکنان از آنها استفاده می‌نمایند و نیز کنترل وب‌سایتهایی که کارکنان به آنها مراجعه می‌کنند، نظارت ویدئویی در اتاقهای تعویض لباس و حمامها، آزمایش مواد مخدر و دروغ سنجی است. ۵۷

در سطح عمومی نیز شرکتها با استخراج اطلاعات پیرامون رفتار اقتصادی مشتریان، حریم خصوصی آنان را نقض می کنند. موکول کردن ارائه خدمات در ازای دریافت اطلاعات از مشتریان، وجه دیگری از تعرض شرکتها به حریم خصوصی شهروندان است. آنچنان که روتن‌برگ دقت کرده است، بسیاری از اطلاعات درخواست شده، اساساً با خدمتی که قرار است ارائه شود، بی‌ارتباط هستند. حتی در مواردی که دریافت اطلاعات از مشتریان ضروری است ـ مثلاً نشانی مشتری برای ارسال کالای مورد نظرـ هیچ تضمینی برای استفاده نکردن از این نشانی در موارد نامربوط وجود ندارد.

تعبیری که روتن‌برگ در این زمینه به کار می برد نیز جالب است:

تهدید شرکتها [علیه حریم خصوصی] ظهور «کارگر شفاف» یا «مصرف‌کننده شفاف» است؛ یعنی کسانی که به دلیل روابط اقتصادی‌شان با شرکتهای خصوصی ناچارند که وجوهی از زندگی خصوصی خود را فاش کنند. حال آن‌که اگر قدرت انتخاب داشتند آن جنبه‌ها را خصوصی نگاه می داشتند. این نوع شفافیت، همانند رابطه‌ای که در بافت نظارت شهروندان با حاکمیت دارند، یکجانبه است؛ نه شفافیت یک پنجره، بلکه شفافیت آیینه ای یک طرفه. ۵۸

۶. دسترسی شهروندان به اطلاعات و گفتمان ابطال ناپذیری حریم خصوصی

همچنان که در مقدمه این بخش اشاره شد، مفهوم آزادی اطلاعات، به طور طبیعی، متضمن دسترسی شهروندان به اطلاعات پیرامون زندگی خصوصی افراد نیست. این قاعده کلی، از منظر برخی صاحب‌نظران، به‌هنگام بحث پیرامون زندگی خصوصی برخی افراد، از جمله آنانی که در دموکراسیها به نمایندگی از مردم سرنوشت آنان را در دست گرفته‌اند، قابل تأمل می‌شود. پرسش اصلی آنان این است که وقتی تصمیم‌گیریهای سرنوشت‌ساز از سوی جامعه، بنا بر معیار اعتماد، به دست کسانی سپرده می‌شود، اما آنان

در زندگی خصوصی خود روش و منشی مغایر با آنچه شهروندان از آنان انتظار دارند، انجام می دهند، آیا همچنان باید به همان معیارهای عام در رعایت حریم خصوصی، پای‌بند ماند.
حتی عده‌ای، گستره بحث را وسیع‌تر انگاشته، بر این اعتقادند کسانی که به هر دلیل، شخصیتی عمومی می‌یابند، حریم خصوصی خود را از دست می‌دهند. «دیوید آرکارد» از صاحب‌نظران انگلیسی اخلاق رسانه‌ای، در مقالات خود به بررسی این دو رویکرد پرداخته است و ما نیز برای کامل شدن بحث، به بررسی نظرات او در این باره می‌پردازیم.
آرکارد با این توضیح بحث خود را آغاز می‌کند که شهروندان یک نظام مردم‌سالار هر چه اطلاعات بیشتری پیرامون واقعیتهای مرتبط داشته باشند، توانایی بهتری در قضاوت منطقی ــ هم در تشخیص خیر خود و هم در تشخیص خیر عمومی ــ خواهند داشت، و همین توانایی است که نتایج سیاسی مطلوب را در روندهای دموکراتیک تضمین می‌کند. اما بلافاصله با ارائه مثالهایی قابل تأمل به پیچیدگیهای نهفته در نزدیک شدن به اطلاعات پیرامون زندگی خصوصی افراد توجه می‌کند. ۵۹

الف. رویکرد عمومی به موضوع حریم خصوصی؛ مثال اول
آرکارد برای این‌که رویکرد خود را پیرامون رعایت حریم خصوصی بیان کند از یک مثال آغاز می‌کند:

روزنامه‌ای با تیراژ انبوه، عکسی را منتشر می‌سازد که از شخصیتی مشهور به‌دست آورده است؛ در این عکس، آن شخصیت در حال گفت‌وگوی صمیمانه با زنی قابل شناسایی تصویر شده است. عکس رُک است، اما وقیح نیست و در کنار آن گزارشی خبری درج شده است که اهمیت تصویر را توضیح می‌دهد. فرض کنیم که روزنامه دلیل قانع‌کننده‌ای برای ارائهٔ این روایت دارد؛ هر دلیلی که ارائه شود در جای خود بررسی خواهد شد. روزنامه تصویر را فقط به‌خاطر وجه تحریکی آن منتشر نساخته است. بیاییم بپذیریم که تصویر تنها چیزی است که گزارش خبری همراه خود را تأیید می‌کند. خلاصه آن که انتشار تصویر بی‌جهت نبوده است. کجای انتشار تصویر و گزارش اشتباه است؟ ۶۰

او در توضیح اشتباه بودن انتشار عکس و گزارش مورد نظر به چهار موضوع اشاره می‌کند:
اول، اگر تصویر با روشی غیرمعمول و بدون اجازه به دست آمده است، انتشار گزارش اشتباه است. اگر عکس به روشی مخفیانه و بدون آگاهی افراد گرفته شده باشد، دریافت نکردن مجوز برای عکس گرفتن نیز به موضوع پیش گفته اضافه می‌شود.

دومین وجه اشتباه‌آمیز بودن کار، هنگامی نمایان می‌شود که گرفتن عکس بخشی از مزاحمتهای آشکار، مداوم و نسنجیده‌ای باشد که اغلب روزنامه‌های زرد برای افراد مشهور ایجاد می‌کنند.

عکاسی که شکار خود را شب و روز دنبال می‌کند و او را برای لحظه‌ای از دید خود رها نمی‌کند و از همهٔ حرکات او عکس می‌گیرد، رفتاری غیرمنطقی و غیرعقلانی دارد ... استفاده از یک عکس انتشار یافته به‌خودی خود ایرادی ندارد. هر چه باشد، آن عکس می‌تواند تنها عکسی باشد که در مناسب‌ترین فرصت گرفته شده باشد. آن چیزی که غیرقابل قبول است، الگوی مزاحمتی است که به تهیهٔ عکس انجامیده است.۶۱

سومین اشتباه هنگامی آشکار می‌شود که تهیه و انتشار عکس باعث برملا شدن رازی شود.

اگر کسی از طریق رابطه دوستانه به اسرار فردی دیگر وارد شود و تنها از طریق همین دوستی به رازهایی دسترسی یابد و بعد آنها را فاش سازد، می‌توان گفت و اصل رازداری را نقض کرده است. ۶۲

چهارمین وجه اشتباه آمیز کار نیز هنگامی رخ می‌نماید که چاپ عکس نگرانیهای اخلاقی را برانگیزد، به‌ویژه اگر تصویر و زبان همراه با آن آشکارا به قصد تمسخر، استهزاء و تحقیر انتخاب شده باشد یا بخشی از طرحی برای این مقصود باشد.

در این صورت معقول است اگر بگوییم که گزارش از توصیف یک رخداد قابل توجه و نظر دادن پیرامون آن خارج شده است. واقعیت این است که شادی دشمنانه بر ضعف دیگران، که پشیمانی و ملامت را در پی دارد، می‌تواند به آزارهای کینه‌جویانه تبدیل شود. ۶۳

آرکارد پس از بیان این چهار وجه، نکته غایی را نیز به بحث خود اضافه می‌کند:

بیایید فرض کنیم که عکس مورد نظر ما هیچ‌یک از این نگرانیها را برنمی‌انگیزد. اگر احساس می‌شود جایی از کار انتشار ایراد دارد، این نگرانی را باید بیشتر در این بیان یافت که روابط آزاد و شخصی فردی با

دیگری از روی رضایت، ربطی به مطبوعات ندارد. مفهوم تجاوز غیرقانونی به حریم خصوصی، تلاش دارد این نگرانی را ثبت و ضبط کند. ۶۴

ب. عمومی کردن یک امر خصوصی باید تنها راه نیل به غایتی ارزشمند باشد و نه یکی از راه‌های نیل به آن غایت؛ مثال دوم
به اعتقاد آرکارد هر فرد علاقه وافری به حریم خصوصی خود دارد و هر نقضی در حریم خصوصی باید با دلائل مطمئن و متقن در علت نقض همراه باشد.

این دلایل باید برآورندهٔ این شرط باشد که عمومی کردن یک امر خصوصی باید تنها راه نیل به غایتی ارزشمند و نه یکی از راههای نیل به آن غایت باشد. کشف اشتباهات جنسی یک عضو کابینه می‌تواند دورویی او و عدم تناسب او برای مقامی خاص را نشان دهد. اما اگر همین نکته را بتوان با توجه به رفتار عمومی او نشان داد، افشای رفتار خصوصی او بیهوده است. ۶۵

آرکارد در توضیح این نظرخود به این نکته نیز توجه دارد که که روزنامه‌نگاران و کارکنان رسانه‌ها قادرند کنشهای خود را توجیه کنند. برای مثال در بیان مفید بودن افشای روابط جنسی یک سیاستمدار به این توضیح متوسل می‌شوند که با افشاگری خود، دروغها و غیرقابل اعتماد بودن وی را نشان داده‌اند. اما همین افشاء، بخشی از عموم را که از مشاهده رفتار جنسی دیگران لذت می‌برند ارضا می‌کند. به همین دلیل به اعتقاد آرکارد اگر ادعا شود که غایتی شریف در پی افشای مطلبی قرار دارد اما در اصل قصد ارضای امیال پست خوانندگان مطرح باشد، ریاکاری شده است و باید از آن دوری گزید.

پ. تمایز میان انتشار چیزی که باید خصوصی باشد و راه انجام آن؛ مثال سوم
آرکارد، در بحث خود، میان دو اشتباه نقض حریم خصوصی و راه انجام آن نقض نیز تمایز قائل می‌شود. به اعتقاد وی، انتشار چیزی که باید خصوصی باشد، یکی از اشتباهات ممکن است و کشف موضوعی خصوصی با استفاده از ابزارهای غیرقانونی، صورت دیگری از اشتباه است.

بنابراین، اشتباه شنود گذاشتن برای تلفن دیوید ملور و معشوقه‌اش و ضبط مکالمات تلفنی آنان و دزدیدن نامه‌ای از مشاور حقوقی پدی اشداون در خصوص جزئیات روابط خارج از زناشویی او را می‌توان از اشتباه برملا کردن هر یک از این جزئیات جدا کرد.۶۶

با این رویکرد، آرکارد به کالبدشکافی استدلال‌هایی می‌پردازد که در پی توجیه تهاجم به حریم خصوصی هستند.

۷. واکاوی سه استدلال در امکان‌پذیری نقض حریم خصوصی

آرکارد با توجه به مقاله کلاسیک و معروفی که ساموئل وارن و لوئیس براندیس با عنوان «حق حریم خصوصی»۶۷ در دسامبر ۱۸۹۰ پیرامون حریم خصوصی نگاشته‌اند، و نیز بیان این موضوع که آنانی نیز که از حق حریم خصوصی دفاع می‌کنند، آن را حقی مطلق نمی‌دانند، به سه دلیل که معمولا برای نقض یک حریم خصوصی ارائه می‌شود، می‌پردازد:

۱. وقتی کسی شخصیتی عمومی یافت، طبیعی است که حریم خصوصی خود را از دست دهد؛

۲. وقتی منافع معین عمومی را می‌توان با افشای منافع خصوصی برآورده ساخت؛

۳. وقتی عموم نسبت به دانستن امور خصوصی علاقه داشته باشند.

دو مورد اول شناخته شده هستند و اغلب به عنوان دلایل خوب مطرح می‌شوند. آخرین مورد تنها در مقایسه با مورد دوم مطرح می‌شود و اغلب به عنوان دلیل بد مطرح است.۶۸

الف. وقتی کسی شخصیتی عمومی یافت، طبیعی است که حریم خصوصی خود را از دست دهد؛

مثالی که آرکارد برای روشن شدن فراز نخست از سه گزاره مورد اشاره ارائه می‌دهد، تمثیلی است که وارن و براندیس در مقاله خود به کار می‌گیرند:

انتشار خبر پیرامون لکنت گفتاری یا ضعف املایی یک فرد عادی و در حال بازنشستگی، تجاوزی به حریم خصوصی است که اگر بی‌سابقه نباشد، غیرقابل توجیه است؛ در حالی‌که بیان همین مشخصات برای یکی از کاندیداهای کنگره چیزی خارج از عرف و نزاکت نیست. ۶۹

توضیح وارن و براندیس در باره این عبارت چنین است:

با این فرض که هر دوی این افراد سعی در پنهان نگه‌داشتن این ناتوانایی‌ها دارند، دو راه برای فهم این موضوع وجود دارد که سیاستمدار داوطلب دلایل کمتری برای اعتراض نسبت به انتشار خبر ناتوانایی خود دارد. راه اول با این استدلال قرین است که اختلال گفتاری یا ضعف در نوشتار، کارآمدی او برای خدمت را زیر سئوال می‌برد. او ضعیف‌ترین عضو کنگره خواهد بود و رأی‌دهندگان باید همهٔ واقعیتهایی را که یک کاندید را بر دیگری برتری می‌بخشد بدانند. ۷۰

آرکارد از جنبه دیگری نیز به توضیح گزاره نخست وارن و براندیس می‌پردازد:

راه دوم فهم نظر وارن و براندیس، در نظر گرفتن این فکر است که هر که وارد زندگی عمومی می‌شود، بخشی از حریم خصوصی خود را از دست می‌دهد. عمومی شدن مساوی است با تغییر در پایگاه، که با درجهٔ پایین‌تری از حریم خصوصی همراه است. در فهم اول از مورد ادعا، گفته می‌شود که هر چیزی که با نقش عمومی شما ارتباط دارد، دیگر در حریم خصوصی قرار ندارد؛ در فهم دوم گفته می‌شود که افراد عمومی به خاطر پایگاه و جایگاهی که دارند، حریم خصوصی کوچکتری دارند. ۷۱

آرکارد در عین حال که اذعان می‌کند حفظ حریم خصوصی برای افرادی که دارای شخصیتی عمومی هستند، از دیگران دشوارتر است، به بررسی دو توجیهی که در هنگام نقض حریم خصوصی افراد مشهور مطرح می‌شود، می‌پردازد.
وی توجیه نخست را بر اساس رأی یکی از دادگاههای استیناف انگلستان چنین صورت‌بندی می‌کند: «آنها که در جست‌وجوی شهرت هستند و از جلوه‌های مناسب از خویش استقبال می‌کنند، نمی‌توانند نسبت به نقض حریم خصوصی و آشکار شدن جلوه‌های نامناسب از خود اعتراض کنند». و در رد این صورت‌بندی چنین‌می نویسد:

استدلال عمومی آن است که از دست دادن حریم خصوصی هزینهٔ به‌حقی است که افراد مشهور برای شهرت خود می‌پردازند. شهرت، پاداشهای فراوانی در پی دارد ــ ثروت، شأن اجتماعی، قدرت، نفوذ و غیره ــ بنابراین می‌توان مطرح کرد که چرا چنین چیزی هزینه‌ای در بر نداشته باشد و آن هزینه کوچکتر شدن حریم خصوصی نسبت به دیگران نباشد؟ این دلیل موجه نیست. بر اساس اصل معقول انصاف می‌توان

اقامهٔ برهان کرد که شأن عمومی و اجتماعی فرد، حق مطلق و تمام‌عیار اوست و اخلاقاً نیازی به هزینه و غرامت ندارد. برخلاف شغل، رتبه دانشگاهی یا پیروزی در انتخابات، شأن اجتماعی را نباید به‌عنوان چیزی که به‌ناحق کسب می‌شود و دیگران را از دور خارج می‌کند پنداشت. اگر عموم مردم باعث شهرت فرد بی‌استعدادی می‌شوند، اتفاقی است و نمی‌توان آن را ناشایست و ناسزاوار دانست. اصل اصلاح و تصحیح در چنین موردی مناسبت ندارد. فرض کنید به برندهٔ خوش‌شانس یک بخت‌آزمایی گفته شود که جایزه او بسیار بزرگ است و خود باید بخشی از هزینه‌های تهیه آن را بپردازد، پاسخ او را خود در نظر آورید. ۷۲

او البته خود با این صورت بندی مخالف است، اما برای روشن شدن موضوع در توضیح استدلال موافقان این‌چنین می نویسد:

به این استدلال توجه کنید: کسی که لباسی می‌پوشد که او را خوب بازنمایی کند، اگر لباسی پوشید که بازنمایی بدی از او ایجاد می‌کند، نباید گله و شکایت داشته باشد. یا: کسی که برای نشان دادن تواناییهای جسمی خود ورزش می‌کند، اگر وادار به ورزشی شد که ناتواناییهای او را نشان می‌دهد، نباید گله کند. این استدلالها قانع‌کننده نیستند. استدلالی که شهرت خوب را سزاوار شهرت بد می‌داند هم قانع‌کننده نیست.۷۳

آخرین رابطه مورد توجه آرکارد در این باب، ارتباط مستقیم میان شأن اجتماعی و از دست رفتن حریم خصوصی است. وی چنین ضرورتی را نیز نمی پذیرد و در این باره می‌نویسد:

آیا برسر این‌که شأن اجتماعی قرین و همراه ناگزیرِ از دست دادن حریم خصوصی است، توافقی حاصل خواهد شد؟ همهٔ آنها که چنان شأنی را آرزو می‌کنند چنین «قرارداد»ی را رد خواهند کرد و کسانی که نفعی در این قضیه ندارند، آنها که مشهور به‌دنیا آمده‌اند یا نسبت به آن بی‌علاقه هستند، آن را بسیار شاق و طاقت‌فرسا خواهند دانست. فرض کنید که بر خلاف میل خود به فرد مشهوری تبدیل شوید: برای مثال نسبتی با نخست وزیر پیدا کنید، شاهد ارتکاب جرم بزرگی شوید یا از یک فاجعه جان سالم به‌در برید. مجبور به پرداخت هزینه‌های ناخواسته‌ای خواهید شد. به شما می‌گویند که به خاطر این شهرت باید بخشی از حریم خصوصی خود را هم از دست بدهید. اگر اصول انصاف در فهم عمومی جا افتاده باشد، پرسیده خواهد شد چه کسی چنین تلقی‌ای را قبول دارد؟۷۴

ب. نقض حریم خصوصی در مقام خدمت به منافع عمومی

اما به گزاره دوم از سه استدلال مطرح شده در امکان پذیر بودن نقض حریم خصوصی بپردازیم. یعنی این اندیشه که حریم خصوصی را می‌توان در صورت کسب منافع عمومی نقض کرد. شک نیست که این استدلال، قوی تر از استدلال نخست است.

مهم ترین مثالهایی که معمولا برای روشن شدن مفهوم «نفع عمومی» ارائه می‌شوند، مواردی همچون کشف و معرفی جرم و جنایت، حفظ سلامت عمومی و جلوگیری از انحراف مردم است. همگان بر این باورند که معرفی مقامهای دولتی به عنوان فاسد، بسیار ناکارآمد، تقصیرکار یا فریب‌کار، در جهت منافع عمومی است، اما آرکارد در تدقیق این اجماع عمومی، پیش شرطی را مطرح می‌کند:

به‌شرط آن که این خطاها نسبت مستقیمی با امور محوله به این اشخاص داشته باشند. بدین‌ترتیب، به‌عنوان مثال، کشف این حقیقت که یک وزیر، مدیر غیراجرایی شرکتی خصوصی است و همیشه در پی انعقاد قرارداد با بخش دولتی است، به نفع عموم است. اما، در بسیاری از موارد نقض حریم خصوصی، بیشتر به مسائل اخلاق جنسی استناد می‌شود و نمی‌توان به‌سادگی دریافت که این‌گونه افشاگریها، چه منافعی برای عمومی در پی دارند. ۷۵

برای روشن شدن مفهوم اخلاق جنسی، آرکارد در وهله نخست «سوء رفتار غیرقانونی جنسی» را از جمله جرایمی می شمارد که افشای آنها در بردارنده نفع عموم هست. برای مثال برقراری رابطه جنسی با افراد پایین‌تر از سن تعریف شده در عرف، که می تواند یک سیاستمدار را بی‌اعتبار کند. وی سپس به موضوع «رابطه نامشروع و رفتار ناشایست جنسی» توجه و این پرسش را مطرح می‌کند: برای این فکر که افشای رفتاری ناشایست در خدمت منافع عمومی قرار دارد، چه دلیلی قابل طرح است؟۷۶

در پی طرح این پرسش، آرکارد چند مورد از استدلالهای مشخصی را که در این ارتباط در باره یک وزیر مطرح می‌شود مورد توجه قرار می دهد و به توضیح در باره هر یک می پردازد:

استدلال اول: هر شکلی از کار غیراخلاقی در عرصه خصوصی، باعث سلب صلاحیت فاعل آن برای مناصب عمومی می‌شود. کسی که دست به عملی غیراخلاقی می زند برای پست وزارت دربار مناسب نیست، فقط به این دلیل که رفتارش نامشروع است و پستهای عمومی نیاز به شخصیتهای سالمی دارد.

پاسخ آرکارد:
این نظر جلوه ویکتوریایی قشنگی دارد و به همان اندازه که آن دوره با ما فاصله دارد، با واقعیت فاصله دارد. باید ضوابط معیار برای کسب پستهای عمومی را در سطحی بالا تعریف کنیم، اما نه آنقدر بالا که فقط فرشتگان صلاحیت احراز [مقامهای عمومی] داشته باشند. ۷۷

استدلال دوم: در منظر عموم خود را مرد خانواده معرفی کردن و دفاع از ارزشهای خانواده در مانورهای تبلیغاتی، و در خفا رفتار دیگری داشتن، ریاکاری است.

پاسخ آرکارد:
دانستن این که وزیر ما [در رابطه با مسائل خانوادگی اش] ریاکار است چه اهمیتی دارد؟ [این دلیل] برای اثبات این که او در همه کارها، به‌ویژه در امور محوله، ریاکار است، دلیل کافی نیست. به‌علاوه، اهمیت ریاکاری در این مورد خاص با این فکر که افراد کمی توان زندگی برحسب آرمانها را دارند، کاهش می‌یابد. ۷۸

استدلال سوم: مردی که به زنش دروغ بگوید ممکن است به وطنش هم خیانت کند، مردی که قسم ازدواج را می‌شکند، می‌تواند قسم خدمت را هم بشکند.

پاسخ آرکارد:
هیچ چیزی در الگوی رفتار انسانی وجود ندارد که بتواند ثابت کند مردی که به همسرش دروغ می گوید صرفا به این خاطر از قابلیت اعتماد و وفاداری کمتری برخوردار است. بیشتر مردم ــ در اثرشمّ یا انگیزه اخلاقی ــ می‌توانند تفاوت میان خطای فردی و خیانت عمومی را تشخیص دهند. توجه به این نکته از آن رو حائز اهمیت است که یک انسان می‌تواند در کار، دوستی، و بسیار حوزه‌های دیگر بی‌اعتبار و رسوا باشد و در عشق شرافت داشته باشد. ۷۹

چهارمین استدلال: وزیر خطاکار، بیشتر وقت خود را ممکن است به ارتکاب خطا بگذراند و در نتیجه توانایی کمتری برای انجام امور محوله و وظیفه‌های خود داشته باشد.

پاسخ آرکارد:
چنین چیزی ممکن است. اما اگر او مرد خانواده‌داری باشد هم چنین چیزی ممکن است؛ اگر ورزشکار، کتاب‌خوان، یا هزار و یک علاقه شخصی داشته باشد هم چنین چیزی ممکن است. اعلام چنین برهان‌هایی برای توجیه انتشار امور غیراخلاقی شخصی به نحو آشکار و خطرناکی همراه با توجیهات خودبینانه است.۸۰

پ. نقض حریم خصوصی آن گاه که عموم نسبت به دانستن امور خصوصی علاقه داشته باشند
اما در باره گزاره سوم، نمی‌توان به‌سادگی گفت که دانستن جزئیات زندگی افراد، منافع عمومی را برآورده می‌سازد، گرچه بیشتر مردم دوست دارند از این مسائل خبر داشته باشند و از این اخبار لذت می‌برند.
آرکارد در تبیین این استدلال، علاقه جامعه به دانستن وجوه کاملا شخصی زندگی شخصیتهای عمومی را از نوع انگیزه‌هایی می داند که به عمل مذموم «غیبت کردن» می انجامد.

عرضه و افشای زندگی خصوصی در روزنامه، شکلی از غیبت است و به‌همین خاطر ناپسند است. می‌توان با موشکافی بیشتر پدیدهٔ غیبت به آثار اخلاقی آن بیشتر پی‌برد. اول، دو نوع دلیلی که برای ناپسندی غیبت ارائه می‌شود را در نظر آورید: انگیزهٔ آنها که غیبت می‌کنند و اثری که بر قربانیان غیبت دارد.
خود غیبت «بیهوده» است، بی‌هدف و بی‌زحمت است، و با هیچ هدفی به‌جز لذتِ خودش به‌انجام نمی‌رسد. غیبت می‌تواند به خود بالنده، سرشار از شادی دشمنانه یا پر از فساد باشد؛ غیبت می‌تواند در راه دستکاری در وجههٔ قربانیان خود، لکه‌دار کردن آبروی آنان و باج‌خواهی از آنان به‌کار رود. اما هر شکلی از سخنی که پیرامون دیگران است، چنین کاری می‌کند، و همین مشخصه‌های خاص غیبت است که آن را در معرض نقد قرار داده است، نه این واقعیت ساده که نام این عمل غیبت است. غیبت کارهای خصوصی افراد را در معرض تفحص عمومی قرار می‌دهد و از این راه به آنان صدمه می‌زند. ۸۱

حاصل بحث مفصلی که در این بخش بدان پرداختیم را می توان چنین جمع‌بندی کرد: حریم خصوصی، همچون آزادی بیان و اطلاعات یکی از سنگ بناهای تحقق حقوق بشر و نظام مردم سالار است. جامعه به همان میزان که حق شهروندان را در مصون ماندن حریم شخصی‌شان به رسمیت می‌شناسد، از حاکمیت نظام‌های تمامیت خواه و اقتدارگرا فاصله می گیرد.

آزادی اطلاعات و حق شهروندان در دسترسی آزادانه به اطلاعات، به هیچ روی در تخالف و تزاحم با حق برخورداری از حریم خصوصی نیست. چه به طورکلی قلمرو آزادی اطلاعات در معنای امروزین آن، اساساً اطلاعات پیرامون زندگی خصوصی افراد را شامل نمی‌شود. و تضمین‌کننده دسترسی شهروندان به اطلاعاتی است که در اختیار دولت است؛ اطلاعاتی که آگاهی شهروندان از آنها بر روندهای سرنوشت ساز تصمیم‌گیری‌شان تأثیری قطعی دارد. به‌طور خاص نیز حتی در مواردی که دسترسی به اطلاعات مربوط به زندگی خصوصی افراد، به عنوان یک ضرورت اجتماعی مطرح می شود، دست کم باید دو ملاک قطعی مورد توجه تأکید قرار بگیرد:

نخست، اطلاعات پیرامون زندگی شخصی فرد، ارتباط و تأثیری مستقیم، قطعی و مستحکم در واگذاری نقش اجتماعی به او و کارکردهای او در یک نظام مردم سالار داشته باشد؛

و دوم، عمومی کردن یک امر خصوصی باید تنها راه نیل به غایتی ارزشمند باشد و نه یکی از راه‌های نیل به آن غایت.

منابع:

" .۱Privacy and Human Rights", Privacy International, 2002, p. 1

http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf

.۲Ibid, p. 1.

.۳Ibid, p. 3.

.۴Fred H Cate, “The Privacy Problem: An Broder View of Information

Privacy and Costs and Consequences of Protecting” http:

www.law.indiana.edu/directory/ publications/fcate/privacyproblem.pdf

.۵Marc Rotenberg, Preserving Privacy in the Information Society,

http://www.unesco.org/webword/infoethics_2/eng/papers_10.htm

.۶Privacy and Human Rights, 2004 ,

http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589&als[theme]=Privacy%20and%20Human%20Rights&headline=PHR2004

.۷Ibid.

۸Samuel Warren and Louis Brandies, “The Right to Privacy ”
http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html
“ .۹Privacy and Human Rights”, Privacy International 2004 ,
.۱۰Ibid.
.۱۱ibid.
.۲ Ibid.
“ .۳ Privacy and Human Rights”, Privacy International, 2002, p.2
.۴ Ibid, p.3.
.۵ Ibid, p.5.
“ .۶ Privacy and Human Rights”, Privacy International 2004 ,
.۷ Ibid.
“ ۸ International Covenant on Civil and Political Rights UN General Assembly resolution 2200 A (XXI)”, December 16, 1966 ,
http://www.unhchr.ch/html/menu3/b/a_ccpr.htm
“ .۹ International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, UN General Assembly resolution 45/158”, December 18, 1990
http://www.unhchr.ch/html/menu3/b/m_mwctoc.htm.
“ .۲۰Convention on the Rights of the Child, UN General Assembly resolution 45/25 of November 20”, 1989 ,
http://www.unhchr.ch/html/menu3/b/k2crc.htm.
“ .۲۱Convention for the Protection of Human Rights and Fundamental Freedoms”, Council of Europe, 1950,
http://conventions.coe.int/Treaty/EN/cadreprincipal.htm
“ .۲۲Privacy and Human Rights”, Privacy International 2004 ,
http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589&als[theme]=Privacy%20and%20Human%20Rights&headline=PHR2004
“ .۲۳Privacy and Human Rights”, Privacy International, 2002, p.7
.۲۴Ibid, pp. 8-9

۲۵ – مرتضی راوندی، سیر قانون وداد گستری در ایران)تهران، نشر چشمه، کتابسرای آمل، ۱۳۶۸)، صفحه ۳۴۴.

۲۶ – همان، صفحه ۳۷۰

۲۷.Ibid, p. 8

۲۸.Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981, http://www.coe.fr/eng/legaltxt/108e.htm

۲۹. “Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data”, OECD, Paris, 1981 , http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

۳۰.Privacy and Human Rights, Privacy International, 2002, pdf, p.9.

۳۱.Ibid, p.9

۳۲. “Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Directive 95/46/EC of the European Parliament and of the Council” , 24 October 1995 http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm

۳۳.Ibid

۳۴. “Privacy and Human Rights”, Privacy International, 2002,p.10

۳۵. “Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, Directive 97/66/EC of the European Parliament and of the Council” ,15 December 1997 http://www.ispo.cec.be/legal/en/dataprot/protection.html

۳۶. “Proposal for a directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector” ,European Commission, http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000385_en.pdf

۳۷. “Privacy and Human Rights”, Privacy International, 2002 , pp.10-11.

۳۸.Ibid, p.11.

.۳۹Ibid, pp. 44 – 45.

.۴۰Ibid, p. 13.

.۴۱Ibid, p. 13 – 14.

.۴۲Ibid, p. 14.

.۴۳Ibid, p. 14.

“ .۴۴Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data”, Council of Europe, 1981 http://www.coe.fr/eng/legaltxt/108e.htm

“ .۴۵Data protection: Commission adopts decisions recognising adequacy of regimes in United States, Switzerland and Hungary,” July 27, 2000 http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm.

“ .۴۶Privacy and Human Rights”, Privacy International, 2004

.۴۷Ibid.

.۴۸Ibid.

“ .۴۹European Commission Staff Working Paper”, February 2002 http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf.

“ .۵۰Privacy and Human Rights”, 2002, Privacy International, pdf,p.p.18 – 19.

.۵۱Rotenberg, Marc, “Preserving Privacy in the Information Society”

.۵۲Ibid.

.۵۳Ibid.

.۵۴Ibid.

.۵۵Ibid.

.۵۶Ibid.

.۵۷Ibid.

.۵۸Ibid.

۵۹. David Archard, Privacy, “the Public Interest and a Purient Public”, in Media Ethics, (Ed. by Matthew Kiern, London, Routledge, 2000), 2000, pp. 82 -96.

۶۰. Ibid, p.p. 82 - 83

۶۱. Ibid, p. 83

۶۲. Ibid.

۶۳. Ibid.

۶۴. Ibid.

۶۵. Ibid, p.p. 84 - 85

۶۶. Ibid, p. 85

۶۷. Samuel Warren and Louis Brandeis, “The Right To Privacy

۶۸. David Archard, Privacy, “the Public Interest and a Purient Public”, in Media Ethics, p.p. 86 -87.

۶۹. Ibid, p. 86.

۷۰. Ibid.

۷۱. Ibid, p. 87.

۷۲. Ibid.

۷۳. Ibid, p. 88.

۷۴. Ibid.

۷۵. Ibid, p. 88.

۷۶. Ibid, p.p. 88 – 89.

۷۷. Ibid, p. 89.

۷۸. Ibid.

۷۹. Ibid, p.p. 89 – 90.

۸۰. Ibid, p. 90.

۸۱. Ibid, p. 91.