ARTICLE 19

ایران: لایحه صیانت و حفاظت از داده‌های شخصی

تیر ۱۳۹۸

تحلیل قانونی

خلاصه

سازمان آرتیکل ۱۹ نگرانی های خود را پیرامون لایحه «صیانت و حفاظت از داده‌های شخصی» که در حال حاضر در مجلس شورای اسلامی تحت بررسی است در این تحلیل ابراز می کند. این تحلیل تطبیق‌پذیری این لایحه را نسبت به تعهدات بین المللی ایران بمنظور حمایت از حق آزادی بیان و اطلاعات و همچنین حق داشتن حریم خصوصی بررسی می کند و سپس وارد جزئیات چارچوب قانونی داخلی می شود .در نهایت تطبیق‌پذیری این لایحه را نسبت به حقوق بین الملل مرور کرده و پیشنهاداتی ارایه می دهد تا این لایحه را با موازین آزادی بیان و حریم خصوصی بین الملل و منطقه سازگار کند. این لایحه بطور کل در چندین بخش فاقد وضوح است. این لایحه به طرز قابل ملاحظه ای با وظایف حقوقی بین‌المللی ایران مغایرت دارد و به اندازه کافی از حقوق شهروندان برای داشتن حریم خصوصی حفاظت نمی‌کند و از موازین بین‌المللی در زمینه حفاظت از داده‌ها تا حدود زیادی عدول می‌کند. این لایحه در ضمن تهدیدی برای حق آزادی بیان است. سازمان «آرتیکل ۱۹» در ضمن به شدت نگران استقلال نهاد مسئول نظارت بر اجرای این قانون و همچنین فقدان راه‌های مناسب جبران مافات برای افراد جهت مقابله با نقض حقوق‌شان و تقاضای دریافت غرامت برای خرابی‌های به بار آمده است.

<u>پیشنهادات:</u>

۱- لایحه باید از نو نوشته شود، سازمانی مجدد بیابد و منظم‌تر شود و تمام اصول حفاظت از داده‌ها که در قانون بین‌المللی آمده‌اند در بخش مشخصی بعد از بخش دو لایحه که در آن «تعاریف» ارائه شده‌اند گنجانده شوند.

۲. لایحه باید شامل مفاد مشخصی باشد که نشان دهد در چه مواردی و در چه محدوده قلمرویی به کاربسته می‌شود. این مفاد باید به روشنی اعلام کنند که این قانون در مورد تمام نهادهای دولتی و همچنین تمام نهادهای خصوصی کاربرد دارد. در حال حاضر این حقوق در سایر قوانین ایران به اندازه کافی مورد صیانت قرار نگرفته‌اند. این تغییرات در ضمن باید با قانون انتشار و دسترسی آزاد به اطلاعات ۱۳۸۸ در ایران هماهنگ شوند.

۳. ماده ۳ باید مطابق اصل عدم تبعیض بازنویسی شود تا در مورد تمام افراد به کار بسته شود و نه فقط شهروندان ایران و شهروندان خارجی که داده‌هایشان درون خاک ایران پردازش می‌شود. در شکل کنونی، تفاوت قائل شدن بین شهروندان ایران و شهروندان خارجی و همچنین عدم محسوب کردن شهروندان بی‌دولت قابل قبول نیست.

۴. لایحه باید مشخصا کاربست ضمانت‌های حریم خصوصی در رابطه با شرکت‌ها را حذف کند.

۵. مقدمه باید از نو نوشته شود تا بر حق آزادی بیان که در قانون اساسی آمده تاکید کند و به منشور حقوق شهروندی اشاره کند که چارچوب پاسداشت حق آزادی بیان، حق دسترسی به اطلاعات، حق داشتن حریم خصوصی و حفاظت داده‌ها در ایران را ارائه می‌کند. لایحه باید مسئولیت‌های ایران به عنوان دولت عضو میثاق بین‌المللی حقوق مدنی و سیاسی را در نظر بگیرد بخصوص اصل ۱۷ (حق حریم خصوصی) و اصل ۱۹ (حق آزادی بیان.)

۶. ماده ۱۲ تغییر یابد تا در مورد پردازش‌هایی که هدف‌شان مخابره اطلاعات به عموم، افکار یا نظرات مورد علاقه عمومی از جمله به دلایل روزنامه‌نگارانه یا بیان دانشگاهی، هنری یا ادبی است استثنا قائل شود. ماده ۱۲ در ضمن باید ضمانت دهد که هنگام دسترسی به داده‌ها بدون رضایت، رویه قضایی دنبال می‌شود. برای این کار باید

شفاف سازد که هدف پیشگیری از تهدیدهای موجود برای نظم، امنیت یا ایمنی عمومی یا برخورد با آن‌ها چیست. این شرایط در ضمن می‌توانند در ماده ۲ تعریف شوند که «تعاریف» را ارائه می‌کند. این‌گونه مقامات امکان نقض حقوق افراد بخصوص در زمینه سرکوب و پیگرد مدافعین حقوق بشر، اقلیت‌ها، روزنامه‌نگاران، وبلاگ‌نویس‌ها و فعالین را نخواهند داشت.

۷. لایحه باید در ضمن کسب اطمینان کند که روزنامه‌نگاران و سایر افرادی که در زمینه منفعت عمومی مشغول کار ارتباطات هستند (از جمله سازمان‌های غیردولتی که اطلاعات مربوط به منفعت عمومی منتشر می‌کنند) مجبور به افشا کردن منابع اطلاعات خود نشوند.

۸. باید کسب اطمینان شود که هرگونه قانون مربوط به حذف اطلاعات عمومی با حق آزادی و منفعت عمومی در دسترسی به اطلاعات و بایگانی تاریخی در توازن است. این از طریق گنجاندن آزمون هفت قسمتی «آرتیکل ۱۹» در رابطه با آن‌چه «حق فراموش شدن» نامیده می‌شود در ماده ۹ ممکن است.

۹. این شرط که تمام داده‌های شخصی باید تحت محلی‌سازی داده قرار بگیرند حذف شود.

۱۰. ماده ۱۲ اصلاح شود تا شامل مستثنی ساختن صریح اطلاعات شخصی در رابطه با فعالیت‌های خصوصی مقامات دولتی و یا سایر افرادی که تحت دولت عمل می‌کنند یا پول دولتی خرج می‌کنند باشد. این‌گونه حق اطلاعات که در قانون اساسی آمده و منفعت عمومی در دستیابی به این اطلاعات تامین می‌شود.

۱۱. لایحه باید مشخصا تبصره‌های مربوط به منفعت عمومی در قانون انتشار و دسترسی آزاد به اطلاعات در رابطه با نهادهای عمومی را به رسمیت بشناسد و تضمین کند که منفعت عمومی در تمام تقاضاها در نظر گرفته می‌شود.

۱۲. در ماده ۱۰ شفافیت‌سازی شود تا کسب اطمینان شود افراد، دسترسی کامل و آزاد به اطلاعات شخصی خود که در اختیار طرفین سوم است داشته باشند مگر در موارد محدودی که قانون بین‌المللی مشخص ساخته، مهم‌تر از همه مواردی که در «اظهار نظر عمومی شماره ۱۶» آمده. باید تعریف شود که «اطلاعات طبقه‌بندی‌شده عمومی» در ماده ۱۰ چه معنایی دارد.

۱۳. به افراد موضوع داده‌ها حق تصحیح داده‌هایشان داده شود.

۱۴. کمیسیون مستقل از دولت است و اختیارات الزام‌آور داشته باشد تا قادر به توقف پردازش، اصلاح، انتشار اطلاعات شخصی نزد افراد موضوع داده‌ها و سایر قدرت‌ها باشد.

۱۵. به افراد حق مشخص اعتراض در دادگاه علیه تصمیمات قضایی داده شود.

فهرست

درباره برنامه «شفافیت» و «منطقه خاورمیانه و آفریقای شمالی» سازمان «آرتیکل ۱۹»

«برنامه شفافیت» سازمان «آرتیکل ۱۹» خواهان شکل‌گیری موازین مترقی در زمینه دسترسی به اطلاعات در سطح بین‌المللی و منطقه‌ای و اعمال آن در نظام‌های حقوقی داخلی است. «برنامه شفافیت» چند گزارش منتشر کرده که موازینی تعیین کرده‌اند. این گزارش‌ها قوانین بین‌المللی و تطبیقی را ارائه می‌کنند و به بهترین تجربه‌های عملی در مواردی همچون امنیت ملی و حریم خصوصی اشاره می‌کنند.

«برنامه شفافیت» بر بنیان این گزارش‌ها و کارشناسی حقوقی عمومی «آرتیکل ۱۹» هر سال شماری تحلیل‌های حقوقی، راهنما و غیره منتشر می‌کند و در مورد پیشنهادهای تقنینی و همچنین قوانین موجود اظهار نظر می‌کند که بر حق اطلاعات، حقوق افشاگری و حقوق مرتبط با این‌ها تاثیر می‌گذارند. این کار تحلیلی اغلب منجر به بهبود چشمگیر قوانین داخلی موجود یا پیشنهادی می‌شود. تمام انتشارات ما در اینترنت به آدرس article19.org قابل دسترسی هستند.

اگر دوست دارید در مورد این تحلیل بیشتر صحبت کنید با دیوید بنی‌سر تماس بگیرید که مشاور حقوقی ارشد و رئیس بخش شفافیت در «آرتیکل ۱۹» است. اطلاعات او:banisar@article19.org و شماره تلفن ۰۰۴۴۲۰۷۳۲۴۲۵۰۰

برنامه «خاورمیانه و آفریقای شمالی» سازمان «آرتیکل ۱۹» بر چند کشور در منطقه تمرکز می‌کند که نگرانی‌هایی درباره کارنامه‌شان در زمینه آزادی بیان موجود است. بسیاری از کشورهای منطقه فاقد پاسداشت قانونی حقوق بشر هستند و حکومت قانون در آن‌ها به علت فقدان قوه قضائیه مستقل ضعیف است. اعتراضات مردمی بهار عرب ۲۰۱۱ همراه با امید بهبود بود اما جنگ‌های خانمان‌سوز، دخالت خارجی و بی‌ثباتی باعث شده منطقه محیطی بسیار خطرناک برای روزنامه‌نگاران، جامعه مدنی و مدافعین حقوق بشر شود و میلیون‌ها نفر را مجبور کرده در جستجوی امنیت کشورهای خود را ترک کنند. جنگ و تخاصم باعث ویرانی زیرساخت‌ها و عقب‌گرد عظیم در شاخص‌های توسعه در یمن، سوریه، لیبی و عراق شده. در بقیه منطقه دولت‌های سرکوبگر در عربستان، ایران، مصر و بحرین را داریم که اعمال ضدحقوق بشر خود را از نو تحکیم کرده‌اند و اغلب هم به نام امنیت ملی و مقابله با تروریسم.

فعالیت «آرتیکل ۱۹» متمرکز است بر نظارت بر قوانین، سیاست‌ها و مقرراتی که بر آزادی بیان و اطلاعات در اینترنت و خارج از آن تاثیر می‌گذارند. ما ناظر بر سیاست‌های پیچیده اینترنت در ایران هستیم و به خطرهای روزافزون متوجه اینترنت پاسخ می‌دهیم. ما در همکاری با شبکه وسیعی از کارشناسان و مدافعین حقوق بشر می‌خواهیم استفاده موثری از قانون آزادی اطلاعات به عمل بیاوریم و نقض آزادی بیان و دسترسی به اطلاعات را برجسته کنیم.

اگر دوست دارید در مورد چارچوب و تحلیل این لایحه بیشتر صحبت کنیم لطفا با مهسا علیمردانی تماس بگیرید.
نشانی: mahsa@article19.org

یک. مقدمه

حق داشتن حریم خصوصی و حق آزادی بیان و اطلاعات حقوق بشر برابر هستند. سازمان «آرتیکل ۱۹» بر این باور است که این حقوق مکمل یکدیگر هستند و در کنار هم به شهروندان امکان می‌دهند از حقوق خود پاسداری کنند و شفافیت و مسئولیت‌پذیری نهادهای عمومی و نهادهای خصوصی را که در جامعه قدرت دارند بهبود بخشند. «آرتیکل ۱۹» حامی اتخاذ قوانینی در زمینه صیانت از داده‌ها است که طراحی مناسبی داشته باشند و حقوق افراد را مورد پاسداشت قرار دهند و از شفافیت دولت و آزادی بیان کسب اطمینان کنند.

در این سند تحلیلی، «آرتیکل ۱۹» نگرانی‌های خود در مورد لایحه «صیانت و حفاظت از داده‌های شخصی» را مطرح می‌کند که در حال حاضر در مجلس ایران مورد گفتگو است. تحلیل‌گران تطبیق‌پذیری این لایحه با وظایف بین‌المللی ایران تحت قانون بین‌المللی حقوق بشر جهت پاسداشت آزادی بیان و اطلاعات و همچنین حق داشتن حریم خصوصی را بررسی می‌کنند. سند سپس جزئیات چارچوب قانونی داخلی را بیان می‌کند. سند در نهایت تطبیق این لایحه با قانون بین‌المللی را مورد بازبینی قرار می‌دهد و پیشنهادهایی ارائه می‌کند که این لایحه را همگام با موازین بین‌المللی و منطقه‌ای در زمینه آزادی بیان و حریم خصوصی خواهد ساخت.

دو. پاسداشت داده‌ها و آزادی بیان و اطلاعات

الف. حق داشتن حریم خصوصی

حق داشتن حریم خصوصی برای پاسداشت قابلیت فرد در رسیدن به افکار و روابط شخصی ضروری محسوب می‌شود. این حق در ضمن در چندین معاهده بین‌المللی حقوق بشر آمده از جمله بیانیه جهانی حقوق بشر[1]، کنوانسیون اروپایی حقوق بشر[2]، بیانیه قاره آمریکا در زمینه حقوق و وظایف انسان[3]، و کنوانسیون حقوق بشر قاره آمریکا[4].

در این قوانین حریم خصوصی مفهومی وسیع است در رابطه با پاسداشت خودمختاری افراد و رابطه بین فرد و جامعه از جمله دولت‌ها، شرکت‌ها و سایر افراد. این مفهوم عموما به عنوان یکی از حقوق محوری تامین‌کننده کرامت انسانی و سایر ارزش‌ها شناخته می‌شود. این اصل در ضمن تامین‌کننده بهره‌وری و استفاده از حقوق بشر مختلف در اینترنت و خارج از آن است، از آزادی بیان[5] و آزادی تشکل و تجمع گرفته تا ممنوعیت تبعیض.

در سطح منطقه‌ای، حق حریم خصوصی عموما توسط اسناد حقوقی غیرالتزام‌آور به رسمیت شناخته شده که مهمترینش «بیانیه قاهره درباره حقوق بشر در اسلام»[6] است. ماده ۱۸ (ب) آن می‌گوید:

---

1 بیانیه جهانی حقوق بشر، ماده ۱۲

2 ماده ۸

3 ماده ۵، ۹ و ۱۰

4 ماده ۱۱

5 گزارش گزارشگر ویژه تشویق و پاسداشت حق آزادی نظر و بیان، فرانک لاروئه، شورای حقوق بشر ۴۰/۲۳، ۱۷ آوریل ۲۰۱۳، **https://undocs.org/A/HRC/23/40**: گزارش گزارشگر ویژه تشویق و پاسداشت حق آزادی نظر و بیان، دیوید کی، شورای حقوق بشر/۳۲/۲۹، ۲۲ مه ۲۰۱۵، **https://undocs.org/A/HRC/29/32**

6 «بیانیه قاهره درباره حقوق بشر در اسلام»، ۵ اوت ۱۹۹۰، سازمان ملل، «آرشیو دفتر مجمع عمومی»، کنفرانس جهانی حقوق بشر، جلسه چهارم، موضوع شماره ۵ برنامه، سند سازمان ملل **A/CONF.157/PC/62/Add.18**، ماده ۱۸، **http://hrlibrary.umn.edu/instree/cairodeclaration.html**

« هر انسانی حق دارد که در امور زندگی خصوصی خود (در مسکن و خانواده و مال و ارتباطات) استقلال داشته باشد و جاسوسی یا نظارت بر او و مخدوش کردن حیثیت او جایز نیست و باید از او در مقابل هر گونه دخالت زورگویانه در این شؤون حمایت شود.» (از نسخه فارسی «شبکه اجتهاد»، http://ijtihad.ir/NewsDetails.aspx?itemid=11750).

۱. صیانت از داده‌ها

حق صیانت از داده‌ها ارتباط نزدیکی با حق حریم خصوصی دارد. این حق شیوه جمع‌آوری، پردازش، ذخیره و حفظ الکترونیکی اطلاعات راجع به افراد توسط نهادهای خصوصی و عمومی را تنظیم می‌کند. این حق هم به عنوان بخشی از قانون بین‌المللی در زمینه حریم خصوصی به رسمیت شناخته شده و هم هویت خودش را به عنوان حقی خودمختار دارد.

کمیته حقوق بشر سازمان ملل اعلام کرده که صیانت از داده‌ها بخشی بنیادین از حریم خصوصی است، چنان‌که در ماده ۱۷ میثاق حقوق مدنی و سیاسی آمده. کمیته در «اظهار نظر عمومی شماره ۱۶» می‌گوید:

«جمع‌آوری و نگهداری اطلاعات شخصی در کامپیوتر، بانک داده و سایر وسایل چه توسط مقامات عمومی باشد و چه توسط افراد یا نهادهای خصوصی باید تحت نظارت قانون انجام شود. دولت‌ها باید اقدامات موثری انجام دهند تا کسب اطمینان کنند که اطلاعات مربوط به زندگی خصوصی افراد به دست کسانی که قانون اجازه آن‌را نداده نمی‌رسد و آنان قادر به دریافت، پردازش و استفاده از چنین اطلاعاتی نخواهند بود و هیچ‌گونه استفاده‌ای از قوانین در جهت اهدافی که مغایر با میثاق باشد صورت نمی‌گیرد. برای اعمال موثرترین پاسداشت افراد، هر شخص باید حق این‌را داشته باشد که به شیوه‌ای قابل فهم بفهمد آیا اطلاعات شخصی او در فایل‌های خودکار داده‌ها هست و اگر هست چه اطلاعاتی و به چه علتی. هر فرد باید بتواند بفهمد کدام نهادهای عمومی یا افراد و نهادهای خصوصی پرونده‌های او را در اختیار دارند یا می‌توانند داشته باشند. اگر چنین پرونده‌هایی شامل داده‌های شخصی غلط باشد یا اطلاعاتی که مغایر با مفاد قانون جمع‌آوری یا پردازش شده باشد، هر فرد باید حق تقاضای تصحیح یا حذف این اطلاعات را داشته باشد.» [7]

تحت قانون بین‌المللی، چند اصل بنیادین مطرح شده‌اند:

— اطلاعات در مورد افراد نباید به شیوه‌های غیرمصفانه و غیرقانونی جمع‌آوری شود (اصل قانونی بودن و انصاف.) این شامل می‌شود بر دریافت اطلاعات به شیوه غیرقانونی همچون ضبط غیرقانونی، دسترسی غیرقانونی به مجموعه داده‌ها و جعل هویت.

— افراد مسئول جمع‌آوری و پردازش باید مرتبا چک کنند که داده‌های جمع‌آوری شده دقیق و مربوط هستند و به روز نگاه داشته می‌شوند؛ در ضمن تمام قدم‌های لازم باید برداشته شود تا داده‌های شخصی که نادقیق هستند (با توجه به دلیل پردازش آن‌ها) حتما بی‌تاخیر حذف یا اصلاح شوند (اصل دقت.)

— داده‌های خصوصی باید برای هدفی مشخص و مشروع جمع‌آوری شوند و باید به اطلاع موضوع داده برسند (اصل مشخص کردن هدف.) در پی اعمال این اصل، کنترل‌کنندگان و پردازش‌گران داده‌ها باید کسب اطمینان کنند که تمام داده‌های شخصی جمع‌آوری‌شده و ضبط‌شده هنوز موضوعیت دارند و همگام با مصارف مشخص‌شده

[7] اظهار نظر عمومی شماره ۱۶، همان‌جا، ماده ۱۰

هستند و در جهت مقاصدی که مغایر با این مصارف مشخص‌شده هستند مورد استفاده و انتشار قرار نمی‌گیرند و در ضمن زمان نگهداری از آن‌ها فراتر از آن‌چه برای دستیابی به اهداف مصارف مشخص‌شده نیاز است نمی‌رود.

— هر فرد موضوع داده حق دارد بداند اطلاعات مربوط به او دارد پردازش می‌شود یا نه و بتواند آن‌را به شکلی قابل فهم دریافت کند، بدون تاخیر یا مخارج بی‌رویه و با امکان ایجاد اصلاحات لازم (اصل دسترسی فرد مورد علاقه.)

— ممنوعیت جمع‌آوری داده‌هایی که منجر به تبعیض غیرقانونی و خودسرانه شود از جمله اطلاعات مربوط به ریشه‌های قومی یا نژادی، رنگ پوست، زندگی جنسی، افکار سیاسی، باورهای مذهبی، فلسفی و غیره و همچنین عضویت در انجمن‌ها یا اتحادیه‌های کارگری

— بالاخره اصل امنیت مقرر می‌دارد که پاسداشت‌های معقول و مناسب فنی و تشکیلاتی موجود باشند تا انتشار یا دسترسی غیرقانونی به داده‌ها ممکن نباشد

این اصول در سال ۱۳۶۹ مورد تصویب مجمع عمومی سازمان ملل قرار گرفتند و موضوع قطع‌نامه‌ای درباره رهنمودهای نگهداری از اطلاعات شخصی ذخیره‌شده در کامپیوترها بودند.[8] این خطوط کلی ۶ اصل بنیادین صیانت از داده‌ها را بر بنیان تجربه‌های مربوط به اطلاعات منصفانه مطرح می‌کنند، که از این قرارند: اصل قانونی بودن و انصاف، اصل دقت، اصل مشخص کردن هدف، اصل دسترسی فرد مورد علاقه، اصل عدم تبعیض و اصل امنیت.

حق حریم خصوصی در ضمن در پی انتصاب گزارشگر ویژه حق داشتن حریم خصوصی توسط شورای حقوق بشر سازمان ملل[9] در تابستان ۱۳۹۴ و اتخاذ قطع‌نامه‌هایی در مورد «حق داشتن حریم خصوصی در عصر دیجیتال» در ۲۷ آذر ۱۳۹۲[10]، ۱ بهمن ۱۳۹۲[11] و ۲۹ آذر ۱۳۹۵ [12]توسط مجمع عمومی سازمان ملل و در ۲ فروردین ۱۳۹۶[13] توسط شورای حقوق بشر و همچنین گزارش ویژه کمیسیونر عالی حقوق بشر سازمان ملل مفصل‌تر تدوین شده[14].
مجمع عمومی در این قطع‌نامه آخری می‌گوید «افزایش ظرفیت‌های شرکت‌ها برای جمع‌آوری، پردازش و استفاده از داده‌های شخصی می‌تواند خطری باشد برای بهره‌وری از حق داشتن حریم خصوصی در عصر دیجیتال» و از دولت‌ها می‌خواهد چنین کنند: «توسعه یا حفظ و اعمال قوانین مناسب با مجازات‌ها و جبران مافات‌های موثر که پاسدار افراد در مقابل نقض و پایمال شدن حق داشتن حریم خصوصی باشد، مثلا از طریق جمع‌آوری، پردازش، حفظ یا استفاده غیرقانونی و خودسرانه از داده‌های شخصی توسط افراد، دولت‌ها، شرکت‌ها و سازمان‌های خصوصی.»[15]

---

[8] رهنمودهای نگهداری از داده‌های شخصی در کامپیوترها، قطع‌نامه مجمع عمومی سازمان ملل ۹۵/۴۵، ۲۳ آذر ۱۳۶۹

[9] نگاه کنید به وب‌سایت دفتر کمیسیونر عالی حقوق بشر سازمان ملل، گزارشگر ویژه در مورد حق داشتن حریم خصوصی: **https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx**

[10] حق داشتن حریم خصوصی در عصر دیجیتال، قطع‌نامه مجمع عمومی سازمان ملل، ۱۶۷/۶۸، ۲۷ آذر ۱۳۹۲، **http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167**

[11] حق داشتن حریم خصوصی در عصر دیجیتال، قطع‌نامه مجمع عمومی سازمان ملل ۳۷/۲۷، یک بهمن ۱۳۹۲، **https://www.ohchr.org/documents/issues/digitalage/a-hrc-27-37_en.doc**

[12] حق داشتن حریم خصوصی در عصر دیجیتال، قطع‌نامه مجمع عمومی سازمان ملل ۹۹/۷۱، ۲۹ آذر ۱۳۹۵، **https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199**

[13] حق داشتن حریم خصوصی در عصر دیجیتال، قطع‌نامه شورای حقوق بشر، ۳۴/ال. ۷، ۲ فروردین ۱۳۹۶، **https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement**

[14] **The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, HRC res. 39/29, 3 August 2018, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement**

[15] حق داشتن حریم خصوصی در عصر دیجیتال، قطع‌نامه مجمع عمومی ۱۹۹/۷۱، ۲۹ آذر ۱۳۹۵

۲. صیانت از داده‌ها در اروپا و سایر نقاط

اروپا تنها منطقه‌ای است که در آن مفاد صریح قانونی حق صیانت از داده‌ها را در سطح منطقه‌ای تامین کرده که این‌را در «منشور حقوق بنیادین اتحادیه اروپا» می‌بینیم.[16]از زمان اجرایی شدن معاهده لیسبون در سال ۱۳۸۸، این منشور به جایگاهی همتراز «قانون اساسی» رسیده و مشابه معاهده‌های بنیان‌گذار اتحادیه است.[17] ماده هشت منشور نه فقط بر حق صیانت از داده‌های شخصی تاکید می‌کند که ارزش‌های محوری مربوط به این حق را نیز برمی‌شمرد. این ماده مقرر می‌دارد که پردازش داده‌های شخصی باید منصفانه، جهت مصارف مشخص‌شده و بر بنیان یا رضایت شخص مورد نظر یا بنیان مشروعی که قانون تعیین کرده باشد. افراد باید حق دسترسی به داده‌های شخصی خودشان و اصلاح آن‌ها را داشته باشند و تبعیت از این حق باید تحت سیطره اداره‌ای مستقل باشد.

«مقررات عمومی صیانت از داده‌های اتحادیه اروپا»[18] نیز مقرر می‌دارد که رضایت موضوع داده باید آزاد، مشخص، بر اساس اطلاع و بدون تردید باشد و این شرط قانونی بودن پردازش است. این سند بر اصل حداقل‌سازی داده تاکید می‌کند و مقرر می‌دارد که داده‌های شخصی باید در سطح لازم و نه بیشتر، مربوط به موضوع و محدود به آن‌چه برای موضوع پردازش ضروری‌اند باشند.[19]

کنوانسیون حفاظت از افراد در رابطه با پردازش خودکار داده‌های شخصی (که معمولا معروف به کنوانسیون شماره ۱۰۸ شورای اروپا است)[20] در سال ۱۳۶۰ تصویب شد و نسخه «جدید» آن را کمیته ورزا در ۲۸ اردیبهشت ۱۳۹۷ تصویب کرد. کنوانسیون ۱۰۸ تنها سند بین‌المللی الزام‌آور در زمینه صیانت از داده‌ها است که در کل جهان کاربست دارد. امکان امضای این سند برای کشورهای عضو و غیرعضو شورای اروپا در همه جای جهان موجود است.[21] تا بحال ۵۱ کشور عضو کنوانسیون ۱۰۸ شده‌اند. از جمله تمامی کشورهای شورای اروپا (۴۷ کشور)؛ اروگوئه، اولین کشور غیراروپایی که در تابستان ۱۳۹۲ به آن پیوست؛ و جزایر موریس، سنگال و تونس که در سال‌های ۱۳۹۵ و ۱۳۹۶ بپیوستند.
حقوق صیانت از داده‌ها در روندهای اداری و حقوقی نیز در سراسر دنیا توسط سازمان‌هایی همچون اتحادیه آفریقا، سازمان دولت‌های قاره آمریکا، سازمان همکاری و توسعه اقتصادی، سازمان همکاری اقتصادی آسیا پاسیفیک و سایر نهادهای بین‌المللی حقوق‌بشری، تجاری و تعیین استاندارد اتخاذ شده‌اند.[22]

۳. تحولات کشوری

---

[16] «اتحادیه اروپا، منشور حقوق بنیادین اتحادیه اروپا ۵ آبان ۱۳۹۱ **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT**» سی ۳۲۶/۰۲، قابل دسترسی در ۲۰۱۲/ ،

[17] منشور حقوق بنیادین اتحادیه اروپا، ماده ۸

سند «مقررات» ۶۷۹/۲۰۱۶ مجلس اروپا و شورا در روز ۸ اردیبهشت ۱۳۹۵ درباره پاسداشت شخصیت‌ها حقیقی در رابطه با پردازش داده‌های شخصی و حرکت آزاد چنین داده‌هایی و لغو فرمان ۴۶/۹۵/کمیسیون اروپا («مقررات عمومی صیانت از داده‌های اتحادیه اروپا»)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[19] «مقررات عمومی صیانت از داده‌های اتحادیه اروپا»، ماده ۵

[20] شورای اروپا، کنوانسیون جدید برای حفاظت از افراد در رابطه با پردازش داده‌های شخصی، در تصحیح پروتکل «کنوانسیون حفاظت از افراد در رابطه با پردازش داده‌های شخصی، مصوب کمیته وزرا در جلسه ۱۲۸ام آن در هلسینگور در ۲۸ اردیبهشت ۱۳۹۷
https://www.coe.int/en/web/data-protection/convention108-and-protocol

[21] شورای اروپا، کنوانسیون جدید برای حفاظت از افراد در رابطه با پردازش داده‌های شخصی، در تصحیح پروتکل «کنوانسیون حفاظت از افراد در رابطه با پردازش داده‌های شخصی، مصوب کمیته وزرا در جلسه ۱۲۸ام آن در هلسینگور در ۲۸ اردیبهشت ۱۳۹۷

[22] نگاه کنید به کنوانسیون امنیت سایبری و صیانت از داده‌های شخصی اتحادیه آفریقا، قانون تکمیلی «جامعه اقتصادی دولت‌های غرب آفریقا»، آ/ اس آ ۱ / ۰۱/ ۱۰، درباره پاسداشت داده‌های شخصی، اصول سازمان دولت‌های قاره آمریکا درباره حریم خصوصی و صیانت از داده‌های شخصی در قاره آمریکا؛ رهنمودهای سازمان توسعه و همکاری اقتصادی درباره صیانت از حریم خصوصی و جریان فرامرزی داده‌های شخصی (۱۹۵۹؛ به‌روز شده در ۱۳۹۲)؛ چارچوب حریم خصوصی سازمان همکاری اقتصادی آسیا پاسیفیک، ۱۳۸۴؛ بیانیه حریم خصوصی مادرید، موازین حریم خصوصی جهانی برای دنیای جهانی، ۱۲ آبان ۱۳۸۸

این تحولات بین‌المللی در سطح ملی نیز قویا دنبال شده‌اند. در زمان نوشتن این تحلیل بیش از ۱۲۰ کشور و حیطه قضایی مستقل قوانین جامعی در زمینه صیانت از داده‌ها تصویب کرده‌اند و ۴۰ کشور نیز دیگر در حال بررسی لوایح پیش‌نویس یا ابتکارهایی در این زمینه هستند.[23]

در منطقه خاورمیانه و آفریقای شمالی علاقه روزافزونی به صیانت از داده‌ها در جریان است و بسیاری کشورهای همسایه فی‌الحال چنین قوانینی اتخاذ کرده‌اند از جمله الجزایر، بحرین، مراکش، قطر، بازار جهانی ابوظبی، مرکز مالی بین‌المللی دوبی، لبنان، ترکیه و تونس. قوانین مشابه در حال حاضر در اردن، کویت، عمان و عربستان سعودی مورد گفتگو هستند. این قوانین همگی تا حدی مکمل اصول بین‌المللی صیانت از داده‌ها هستند.

ب. ایجاد توازن بین حریم خصوصی و آزادی بیان و اطلاعات

حق آزادی بیان از حقوق بنیادین بشر است که در قانون حقوق بشر بین‌المللی به رسمیت شناخته شده. بهره‌وری کامل از این حق در مرکز دستیابی به آزادی‌های فردی و ساختن دموکراسی قرار دارد. آزادی بیان شرط لازم تحقق اصول شفافیت و مسئولیت‌پذیری است که به نوبه خود نقشی ضروری در تشویق و پاسداشت تمامی حقوق بشر دارند.

چنان‌که در بالا گفتیم، حق داشتن حریم خصوصی و آزادی بیان در قانون حقوق بشر حقوقی درهم‌تنیده به حساب می‌آیند. در اسناد بین‌المللی، قانون اساسی کشورها و متن قوانین مشخص این دو را در کنار هم می‌بینیم. این دو حق همدیگر را تحکیم می‌کنند.

این دو در کنار هم مسئولیت‌پذیری دولت و سایر بازیگران قدرتمند نزد شهروندان را تضمین می‌کنند. آزادی بیان و آزادی اطلاعات به افراد امکان می‌دهد نقش حقوق بشر از جمله نقش اصل حریم خصوصی را مورد تحقیق و چالش قرار دهند. حق حریم خصوصی به افراد امکان می‌دهد در فضایی کار کنند که توسط قدرت محدود نباشند و به صدای خود برسند. محدود کردن حریم خصوصی در سطح عملی بر قابلیت عملکرد رسانه‌ها تاثیر می‌گذارد. روزنامه نگاران قادر به دنبال کردن موثر تحقیقات و دریافت اطلاعات از منابع محرمانه و سایر منابع نیستند.[24] قوانین صیانت از داده‌ها می‌توانند با محدود کرن جمع‌آوری غیرقانونی اطلاعات شخصی برای مصارف سیاسی پشتیبان آزادی بیان باشند. مثلا در مواردی که نهادهایی برای فشار گذاشتن بر روزنامه‌نگاران و سایرین برایشان پرونده‌سازی می‌کنند.

تفاوت‌هایی هم در کار هست. تنش بین آزادی بیان و حق داشتن حریم خصوصی در شرایطی تشدید می‌شود که جمع‌آوری و در دسترس قرار دادن اطلاعات شخصی فرا روی مرزها در سطحی بی‌سابقه و با هزینه کمی برای هم شرکت‌ها هم دولت‌ها ممکن نیست. در عین حال کاربست قوانین صیانت از داده‌ها و سایر اقدامات برای پاسداشت حق حریم خصوصی می‌تواند تاثیری نامتناسب بر استفاده مشروع از آزادی بیان داشته باشد.

---

[23] نگاه کنید به گرین‌لیف، گراهام، جدول‌های جهانی قوانین و لوایح حریم خصوصی داده‌ها (نسخه پنجم، ۲۰۱۷) (۱۲ بهمن ۱۳۹۵) (۱۳۹۵). ۱۴۵ قانون حریم خصوصی و گزارش بین‌المللی شرکت‌ها، ۱۴-۲۶. قابل دسترس در اس اس آر ان: https://ssrn.com/abstract=2992986؛ بنی‌سر، دیوید، قوانین و لوایح جامع کشوری در زمینه صیانت از داده‌ها و حریم خصوصی ۲۰۱۸ (۱۳ هریویر ۱۳۹۷). قابل دسترس در https://ssrn.com/abstract=1951416 یا http://dx.doi.org/10.2139/ssrn.1951416

[24] نگاه کنید به هشدار ایفکس، سی عضو ایفکس از دولت‌ها می‌خواهند به حقوق بنیادین بشر برای آزادی بیان و حریم خصوصی ارتباطات احترام بگذارند، ۱۵ خرداد ۱۳۸۸ http://www.ifex.org/international/2009/06/05/ja_qm/

همین است که این دو باید دو حق برابر انسانی به شمار بیایند و ضروری است که دولت‌ها و دادگاه‌ها به شیوه‌ای منصفانه بین دو ایجاد توازن کنند و یک طرف را بر طرفی دیگر ترجیح ندهد. قانون حقوق بشر بین‌الملل چنین سلسله‌مراتبی بین حقوق را نمی‌پذیرد (در چنین سلسله‌مراتبی یک حق باید از دیگری پیشی بگیرد.) چنان‌که در «بیانیه و برنامه عمل وین» که در سال ۱۳۷۲ به تصویب کنفرانس جهانی حقوق بشر رسید می‌خوانیم:

«تمام حقوق بشر جهانی، غیر قابل تفکیک و متکی و مربوط به یک‌دیگر هستند. جامعه جهانی باید در سطح جهانی برخوردی منصفانه و برابر با حقوق بشر داشته باشد و رویکردی یکسان نسبت به آن‌ها و با تاکید برابر. اهمیت مسائل مشخص ملی و قومی و پیشینه تاریخی، فرهنگی و مذهبی را باید در نظر گرفت اما این وظیفه دولت‌ها است که فرای سامانه‌های سیاسی، اقتصادی و فرهنگی خود دست به تشویق و پاسداشت تمامی حقوق بشر و آزادی‌های بنیادین بزنند.»[25]

کمیسیون حقوق بشر سازمان ملل گفته است:

«تمامی حقوق بشر از اهمیت یکسان برخوردارند. بیانیه جهانی حقوق بشر در سال ۱۹۴۸ به روشنی می‌گویند که تمام انواع حقوق بشر (اقتصادی، سیاسی، مدنی، فرهنگی و اجتماعی) ااز عتبار و اهمیت برابر برخوردارند... حقوق بشر در ضمن غیر قابل تفکیک و متکی به یکدیگرند. اصل تفکیک‌ناپذیری آن‌ها این واقعیت را به رسمیت می‌شناسد که هیچ یک از حقوق بشر ذاتا از دیگری کم‌تر نیست.»[26]

دادگاه حقوق بشر اروپا مدت‌ها است در مواردی که پای حریم خصوصی و آزادی بیان در میان است رویکرد ایجاد توازن بین حقوق را اتخاذ کرده:

«هنگام تایید این‌که آیا مقامات بین دو ارزش ضمانت‌شده در کنوانسیون که می‌توانند در این نوع موارد در تصادم با یکدیگر قرار بگیرند (آزادی بیان مورد ضمانت اصل ۱۰ و حق احترام برای زندگی خصوصی که در ماده ۸ آمده) توازنی منصفانه ایجاد کرده‌اند یا نه، دادگاه باید بین منفعت عمومی در انتشار یک عکس و نیاز به صیانت از زندگی خصوصی توازن ایجاد کند... ایجاد توازن بین منافع مجزا که می‌توانند در تناقض با یکدیگر باشند امری دشوار است و دولت‌های مورد نظر شاید حاشیه امنیت کمی در این زمینه داشته باشند چرا که مقامات کشوری نسبت به این دادگاه از جایگاه بهتری برخوردارند تا ارزیابی کنند این‌که آیا «نیاز اجتماعی فوری» که قادر به توجیه دخالت در یکی از حقوق ضمانت‌شده توسط کنوانسیون باشد موجود است یا خیر.»[27]
دادگاه حقوق بشر اروپا در پرونده‌ای که در پی آمد با شفافیت بیشتر اعلام کرد که هنگام ایجاد توازن بین حق آزادی بیان و حق داشتن حریم خصوصی اصل بر این است که هر دو حقوق باید مورد احترام یکسان قرار بگیرند.[28] دادگاه سپس شماری از عوامل دخیل در ایجاد توازن بین این حقوق را بر شمرد از جمله:

— نقش داشتن در نزاعی که مربوط به منفعت عموم باشد
— میزان شناخته‌شدن فرد مورد نظر و موضوع گزارش
— رفتار قبلی فرد مورد نظر
— محتوا، شکل و عواقب انتشار
— شرایطی که عکس در آن گرفته شده (در موارد مربوطه.)

---

25 بیانیه و برنامه عمل وین، سند سازمان ملل آ/کنف ۲۳/۱۵۷ (۲۱ تیر ۱۳۷۲)
26 دفتر کمیسیونر عالی حقوق بشر سازمان ملل، سوال‌های متداول در مورد رویکرد حقوق بشری به همکاری توسعه، ۲۰۰۶
27 نگاه کنید به فون هانوفر علیه آلمان، شماره ۰۰/۵۹۳۲۰، ۴ تیر ۱۳۸۳
28 دادگاه اروپا، فون هانوفر علیه آلمان شماره ۲، [GC]، شماره «۰۸/۴۰۶۶۰ & ۰۸/۶۰۶۴۱»، بند ۱۰۶، ۲۰۱۲

دادگاه حقوق بشر قاره آمریکا نیز از رویکردی مشابه استفاده کرده و می‌گوید:[29]

«دادگاه باید بین زندگی خصوصی و آزادی بیان ایجاد توازن کند و مقرر دارد که این‌دو حقوق بنیادین توسط کنوانسیون قاره آمریکا ضمانت شده‌اند و اهمیت مهمی در جوامع دموکراتیک دارند. دادگاه تاکید می‌کند که تمام حقوق بنیادین در رابطه با سایر حقوق بنیادین کاربرد دارند. این روندی از هماهنگ‌سازی است که در آن هر دولت نقشی کلیدی در تعیین مسئولیت‌ها و تعیین مجازات در مواردی که لازم است دارد.»

«اتحادیه آفریقا» هم در «بیانیه اصول آزادی بیان در آفریقا» به این مساله می‌پردازد و در اصل ۷ (۲) می‌گوید:
«قوانین حریم خصوصی نباید مانع انتشار اطلاعات مربوط به منفعت عمومی شوند.»[30]

صیانت از داده‌های شخصی و آزادی بیان

نیاز به ایجاد توازن بین حقوقی که در تصادم با یکدیگر هستند در اسناد بین‌المللی مربوط به صیانت از داده‌ها نیز به رسمیت شناخته شده است. در مقدمه نسخه جدید کنوانسیون ۱۰۸ شورای اروپا می‌خوانیم:

«مقرر می‌دارد که حق صیانت از داده‌های شخصی باید در رابطه با نقش آن در جامعه مورد توجه قرار بگیرد و باید با سایر حقوق بشر و آزادی‌های بنیادین از جمله آزادی بیان هماهنگ شود.»

شورای اروپا در گزارش توضیحی به نیاز به ایجاد توازن بین آزادی بیان و حقوق داشتن حریم شخصی اشاره می‌کند:

«۱۱. با توجه به حق صیانت از داده‌های شخصی در جامعه، این مقدمه بر این اصل تاکید می‌کند که منافع، حقوق و آزادی‌های بنیادین افراد باید در زمان لازم در سازش با یکدیگر قرار بگیرند. جهت برقراری توازن محتاطانه بین منافع، حقوق و آزادی‌های بنیادین این کنوانسیون شرایط و محدودیت‌های مشخصی در رابطه با پردازش اطلاعات و صیانت از داده‌های شخصی مطرح می‌کند. حق صیانت از داده‌های شخصی مثلا باید در کنار حق «آزادی بیان» که در ماده ۱۰ کنوانسیون حقوق بشر اروپا آمده مد نظر گرفته شود (مجموعه معاهده‌های اروپا، شماره ۵) که شامل است بر آزادی داشتن افکار و دریافت و ارائه اطلاعات. کنوانسیون باضافه تاکید می‌کند که استفاده از حق صیانت از داده‌ها که حقی مطلق نیست به هیچ وجه نباید به عنوان وسیله‌ای عمومی برای جلوگیری از دسترسی عموم به اسناد رسمی مورد استفاده قرار بگیرد.»[31]

این توازن در سایر اسناد نیز مورد اشاره قرار گرفته. «کمیسیون اروپا» در بررسی تاثیر «مقررات عمومی صیانت از داده‌های اتحادیه اروپا» می‌نویسد:

---

29 دادگاه حقوق بشر قاره آمریکا، پرونده فونتوکیا و دامیو علیه آرژانتین، قضاوت روز ۸ آذر ۱۳۹۰

30 بیانیه در مورد اصول آزادی بیان در آفریقا، کمیسیون حقوق بشر و مردم‌های آفریقا، فصل ۳۲ام، ۲۵ مهر تا ۱ آبان ۱۳۸۱: بانجول، گامبیا

31 گزارش توضیحی به پروتکل در ترمیم «کنوانسیون حفاظت از افراد در رابطه با پردازش خودکار داده‌های شخصی، ۱۸ مهر ۱۳۹۷، https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

«حریم خصوصی و صیانت از داده‌های شخصی... نقشی کلیدی در تحقق حقوق بنیادین به وسیع‌ترین معنای کلمه دارند. بسیاری از آزادی‌های بنیادین تنها در صورتی قابل استفاده هستند که فرد مطمئن باشد تحت نظارت و بازبینی دائمی مقامات و سایر سازمان‌های قدرتمند قرار ندارد. آزادی اندیشه، آزادی بیان، آزادی تشکل و تجمع و در ضمن آزادی عمل به کسب و کار نمی‌توانند در محیطی مورد استفاده کامل تمام شهروندان قرار بگیرد که در آن افراد احساس می‌کنند تک تک حرکات، اعمال، گفته‌ها و داد و ستدهایشان زیر نظر سایرینی انجام می‌شود که در پی کنترل آن‌ها هستند. عمل به هر یک از این آزادی‌ها برای حفظ تمام آزادی‌های بنیادین ضروری است.»[32]

بدین‌سان نمی‌بایست رابطه این دو حق را مثل بازی «برد و باخت» تعریف کرد که در آن یکی بر دیگری «پیروز» می‌شود. در عوض باید متوجه ساز و کارهای این دو باشیم که حامی یکدیگرند

سه. چارچوب قانونی در ایران

در ایران شماری از اسناد حقوقی در مورد حریم خصوصی و صیانت از داده‌ها موجود هستند که بعضی الزام‌آورند و بعضی نه. این اسناد میزانی از صیانت را ارائه می‌کنند که جامع نیست. از این موارد می‌توان به قانون اساسی جمهوری اسلامی ایران، قانون بازرگانی الکترونیک، قانون جرایم رایانه‌ای[33]، قانون مجازات اسلامی و قانون مسئولیت مدنی اشاره کرد. باضافه حق داشتن حریم خصوصی و صیانت از داده‌ها در منشور حقوق شهروندی مورد اشاره قرار گرفته که یک سند حقوقی غیرالزام‌آور برای پاسداشت حقوق بشر است. مواد و اصول مربوطه در زیر به خلاصه آمده‌اند.

اما همچنان شاهد جای خالی مواد قانونی مربوط به صیانت از داده‌ها هستیم. لایحه «حفاظت و صیانت از داده‌های شخصی» اولین تلاش برای ارائه قانونی جامع است که تعیین می‌کند اطلاعات شخصی چطور مورد استفاده سازمان‌ها، شرکت‌ها و دولت قرار می‌گیرند.

الف. انقلاب ۱۳۵۷

قانون اساسی ۱۳۵۷ شامل مواردی در زمینه آزادی بیان، دسترسی به اطلاعات و حریم خصوصی می‌شود. اصل ۲۴ بر آزادی بیان تاکید می‌کند اما به شیوه‌ای که نسبت به آن‌چه در قانون بین‌المللی آمده محدود است. در ضمن این ماده تنها بر انتشارات متمرکز است و به صراحت بر حق اطلاعات تاکید نمی‌کند. باضافه خود اصل قانون اساسی هم محدودیت‌های وسیعی بر بنیان اضرار به اسلام یا حقوق عمومی تعیین کرده است.

اصل ۲۵ ضامن حق داشتن حریم خصوصی و صیانت از داده‌های شخصی است اما این حقوق را مشروط می‌داند و اعلام می‌کند که بازرسی نامه‌ها و نرساندن آن‌ها، ضبط و پخش مذاکرات تلفنی، تلگرافی یا تلکس، سانسور یا اختلال عامدانه در آن‌ها، استراق سمع و تمامی سایر انواع نظارت مخفیانه ممنوع هستند.

---

32 کمیسیون اروپا، سند کاری خدمه کمیسیون، سند «بررسی تاثیر» همراه سند مقررات مجلس اروپا و شورا درباره پاسداشت افراد در رابطه باپردازش داده‌های شخصی و حرکت آزاد این داده‌ها (سند «مقررات عمومی صیانت از داده‌های اتحادیه اروپا»، اس ئی سی (۲۰۱۲)، ۷۲ نهایی، ۵ بهمن ۱۳۹۰

33 آرتیکل ۱۹، «جمهوری اسلامی ایران:قانون جرایم رایانه‌ای، تحلیل حقوقی (۱۳۹۱)

https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf

اصل ۳ در باره «اهداف» دولت مقرر می‌دارد که دولت وظیفه دارد از منابع خود برای دستیابی به اهداف مختلف استفاده کند از جمله کاهش فساد و «بالابردن سطح آگاهي هاي عمومي در همه زمينه ها با استفاده صحيح از مطبوعات و رسانه هاي گروهي و وسايل ديگر.»

ب. قوانین حافظ حق داشتن حریم خصوصی در ایران

قانون جرایم رایانه‌ای که در سال ۱۳۸۸ تصویب شد شامل مواد مختلفی است که ضامن حقوق افراد هستند از جمله موارد تامین‌کننده ضمانت‌های لازم در زمینه حریم خصوصی برای کاربران. تحت این قانون هر گونه انتشار شفاهی یا کتبی اطلاعات شخصی، جعل داده‌ها برای توهین عمومی به کرامت افراد یا آسیب زدن به شهرت از طریق تهمت و توهین و یا منتسب ساختن موضوعی غیرواقعی به افراد هتک حرمت محسوب می‌شود.[34] این قانون جرم جنایی ۱ تا پنج سال زندان و/یا مجازات را برای افرادی در نظر می‌گیرد که با استفاده از وسایل الکترونیکی ناقض حریم خصوصی افراد می‌شوند و برای «هرکس که به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد.»[35] باید اشاره کرد که هدف این قانون مجازات جرایم رایانه‌ای است و در نتیجه تنها در مورد جدی‌ترین تخلفات به کار می‌آید.

«قانون تجارت الکترونیکی» نیز شامل موادی مربوط به صیانت از داده‌ها هست.[36] اما در این قانون صیانت از داده‌های شخصی محدود به مشتریان اینترنتی است که با فروشندگان در تماس هستند. در قانون مدنی جایی برای حفاظت از حق حریم خصوصی در گرفته نشده و در قانون مسئولیت مدنی سال ۱۳۳۹ می‌خوانیم «هر کس بدون مجوز قانونی عمدا یا در نتیجه بی احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتی یا به هر حق دیگر که به موجب قانون برای افراد ایجاد گردیده لطمه‌ای وارد نماید که موجب ضرر مادی یا معنوی دیگری شود مسئول جبران خسارت نشای از عمل خود می‌باشد.»[37]

قانون مجازات اسلامی برای کسانی که ناقض اخلاق و کرامت عمومی هستند سه ماه تا یک سال زندان و جریمه تعیین کرده و البته این مجازات در مواردی که جرم از طریق تلفنی یا سیستم‌های ارتباطی انجام شده به ۱ تا ۶ ماه و بدون جریمه کاهش می‌یابد.[38]

قانون تجارت الکترونیکی اصلی‌ترین قانونی است که موادی در زمینه حریم خصوصی و صیانت از داده‌ها دارد. اما در این قانون حفاظت از داده‌های شخص مربوط به چارچوبی مشخص یعنی برخورد مشتریان و فروشندگان اینترنتی با یکدیگر است.[39]

ج. سایر مواد قانونی غیرالزام‌آور

---

[34] قانون جرایم رایانه‌ای ایران، فصل‌های ۴ و ۵

[35] قانون جرایم رایانه‌ای ایران، ماده ۱۲ـ در ضمن نگاه کنید به مواد ۱۳، ۱۴ و ۱۶ـ تحلیل حقوقی «آرتیکل ۱۹» را بخوانید https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf

[36] قانون تجارت الکترونیک جمهوری اسلامی ایران ـ بخصوص مواد ۵۸ تا ۶۱ـ

[37] قانون مسئولیت مدنی ایران، ماده ۱

[38] قانون مجازات اسلامی (کتاب پنجم، تعذیرات)، مواد ۶۴۰ و ۶۴۱

رئیس‌جمهور حسن روحانی در سال ۱۳۹۵ منشور حقوق شهروندی را به میان آورد. این منشور سندی غیرالزام‌آور است که از ۱۲۰ ماده تشکیل شده که بسیاری از حقوق بین‌المللی مدنی، سیاسی، اجتماعی و اقتصادی موجود از جمله حق آزادی بیان، حریم خصوصی، محیط زیست پاک و اشتغال را شامل می‌شوند.

در فصل «خ» هفت بخش مربوط به حق داشتن حریم خصوصی و صیانت از داده‌ها موجود است. مثلا در ماده ۳۷ می‌خوانیم: «تفتیش، گردآوری، پردازش، به‌کارگیری و افشای نامه‌ها اعم از الکترونیکی و غیر الکترونیکی، اطلاعات و داده‌های شخصی و نیز سایر مراسلات پستی و ارتباطات از راه دور نظیر ارتباطات تلفنی، نمابر، بی‌سیم و ارتباطات اینترنتی خصوصی و مانند این‌ها ممنوع است مگر به موجب قانون.» جمع‌آوری اطلاعات شخصی از شهروندان بدون رضایت موضوع داده یا در مواردی که در مطابقت با ماده ۳۸ تعیین شده ممنوع است. در ماده ۳۹ می‌خوانیم که «حق شهروندان است که از اطلاعات شخصی آن‌ها که نزد دستگاه‌ها و اشخاص حقیقی و حقوقی است، حفاظت و حراست شود.»[40]

د. مواد مشکل‌آفرین قوانین در زمینه آزادی بیان

در ایران مواد قانونی دیگری هم هستند که به آزادی بیان مربوط می‌شوند. نسخه اصلاح‌شده‌ای از قانون مجازات اسلامی در سال ۱۳۹۲ ارائه شد.[41] نسخه جدید شامل محدودیت‌های متعدد وسیع و مبهم در زمینه آزادی بیان است که تحت قانون بین‌المللی حقوق بشر مشروع شمرده نمی‌شوند و هدف گرفتن مدافعین حقوق بشر، روزنامه‌نگاران یا صداهای مخالف و اقلیت را تسهیل می‌کنند.[42]

از جمله مشکل‌آفرین‌ترین موادی که در دادگاه‌ها از آن‌ها برای محدود کردن آزادی بیان استفاده می‌شود موارد زیرند:
— کتاب اول، فصل نهم، ماده ۲۸۶ جرم «افساد فی‌الارض» را تعریف می‌کند که مجازات اعدام دارد. این جرم شامل اعمالی می‌شود که درست تعریف نشده‌اند مثل: «نشر اکاذیب»، «دایر کردن مراکز فساد و فحشا یا معاونت در آن‌ها»، «اخلال در نظام اقتصادی کشور» البته «به گونه‌ای که موجب اخلال شدید در نظم عمومی کشور یا ناامنی» شود.[43]

---

[40] منشور حقوق شهروندی ایران، فصل ۹ **http://epub.citizensrights.ir/CitizensRightsEN.pdf**

[41] قانون مجازات اسلامی در سال ۱۳۹۵ ترمیم شد. نسخه به‌روز شدن آن‌را در وب‌سایت مجلس ایران ببینید: **http://rc.majlis.ir/fa/law/print_version/845048**

[42] "قانونی ساختن سرکوب: بررسی قانون جدید مجازات اسلامی ایران، دیدبان حقوق بشر، ۲۹ اوت ۲۰۱۲- **https://www.hrw.org/report/2012/08/28/codifying-repression/assessment-irans-new-penal-cod**

[43] ماده ۲۸۶ - هرکس به طور گسترده، مرتکب جنایت علیه تمامیت جسمانی افراد، جرائم علیه امنیت داخلی یا خارجی کشور، نشر اکاذیب، اخلال در نظام اقتصادی کشور، احراق و تخریب، پخش مواد سمی و میکروبی و خطرناک یا دایر کردن مراکز فساد و فحشا یا معاونت در آنها گردد به گونه ای که موجب اخلال شدید در نظم عمومی کشور، ناامنی یا ورود خسارت عمده به تمامیت جسمانی افراد یا اموال عمومی و خصوصی، یا سبب اشاعه فساد یا فحشا در حد وسیع گردد مفسد فی الارض محسوب و به اعدام محکوم می گردد

https://www.ekhtebar.com/%D9%85%D8%AA%D9%86-%D9%82%D8%A7%D9%86%D9%88%D9%86-%D9%85%D8%AC%D8%A7%D8%B2%D8%A7%D8%AA-%D8%A7%D8%B3%D9%84%D8%A7%D9%85%DB%8C-%DA%A9%D8%AA%D8%A7%D8%A8-%D8%A7%D9%88%D9%84-%D8%AA%D8%A7-%DA%86%D9%87%D8%A7/

— کتاب دوم، فصل پنجم، ماده ۲۶۲ به طوری مبهم می‌گوید: «هر کس پیامبر اعظم صلی الله علیه و آله و سلم و یا هر یک از انبیا عظام الهی را دشنام دهد یا قذف کند ساب النبی است و به اعدام محکوم می‌شود.»[44]

در کتاب پنجم بعضی مواد کلیدی هستند که آن نوع استفاده از آزادی بیان را که طبق قوانین حقوق بشری بین‌المللی قانونی محسوب می‌شود جرم می‌دارند:

— ماده ۵۱۳ «اهانت» به «مقدسات اسلام» و یا رهبران مذهبی را جرم می‌دارد (از یک تا پنج سال زندان) که در صورت این‌که «سب النبی» باشد مشمول مجازات اعدام می شود.

— ماده ۵۱۴ توهین به «مقام معظم رهبری» را موجب شش تا دو سال زندان می‌دارد[45]؛

— ماده ۵۰۰ هرگونه «فعالیت تبلیغی... به نفع گروه‌ها و سازمان‌های مخالف نظام» را جرم می‌دارد و محکوم به سه ماه تا یک سال زندان. [46] از این ماده اغلب برای آزار روزنامه‌نگاران و مدافعین حقوق بشر استفاده می‌شود؛

- ماده ۶۹۸ هر کس را که از طریق هرگونه نوشته موجب «اضرار» یا «تشویش اذهان عمومی یا مقامات رسمی» شود مجرم می‌دارد و به دو ماه تا دو سال زندان و ۷۴ ضربه شلاق محکوم می‌کند[47]؛
— ماده ۶۱۸ «اخلال نظم و آسایش و آرامش عمومی» را جرم می‌دارد و موجب سه ماه تا یک سال زندان و تا ۷۴ ضربه شلاق.[48]

---

44 قذف به معنی تهمت جنسی است

45 اگر نماید اهانت **(س)**طاهره صدیقه حضرت یا **(ع)**طاهرین ائمه یا عظام انبیاء از یک هر یا و اسلام مقدسات به کس هر **–** ۵۱۳ ماده **.**شد خواهد محکوم سال پنج تا یک از حبس به صورت این غیر در و شودمی اعدام باشد النبی‌ساب حکم مشمول

نماید اهانت انحاء از نحوی به رهبری معظم مقام و علیه ...ارضوان اسلامی جمهوری بنیانگذار خمینی، امام حضرت به کس هر - ۵۱۴ ماده شد. خواهد محکوم سال دو تا ماه شش ازحبس به

قانون مجازات اسلامی، کتاب پنجم، «مرکز انساد حقوق بشر ایران»، قابل دسترسی در: « https://iranhrdc.org/islamic-penal-code-of-the-islamic-republic-of-iran-book-five/»

46 ماده ۵۰۰**: «**هر کس علیه نظام جمهوری اسلامی ایران یا به نفع گروهها و سازمانهای مخالف نظام به هر نحو فعالیت تبلیغی نماید به حبس از سه ماه تا یکسال محکوم خواهد شد**.»**

قانون مجازات اسلامی، کتاب پنجم، «مرکز انساد حقوق بشر ایران»، قابل دسترسی در: « https://iranhrdc.org/islamic-penal-code-of-the-islamic-republic-of-iran-book-five/»

47 **«**ماده ۶۹۸ **–** هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله نامه یا شکواییه یا مراسلات یا عرایض یا گزارش یاتوزیع هر گونه اوراق چاپی یا خطی با امضاء یا بدون امضاء اکاذیبی را اظهار نماید یا با همان مقاصد اعمالی را برخلاف حقیقت رأساً یا به عنوان نقل‌قول به شخص حقیقی یا حقوقی یا مقامات رسمی تصریحاً یا تلویحاً نسبت دهد اعم از اینکه از طریق مزبور به‌نحوی از انحاء ضرر مادی یا معنوی به‌غیر وارد شود یا نه علاوه بر اعاده حیثیت در صورت امکان، باید به حبس از دو ماه تا دو سال و یا شلاق تا **(**۷۴**)** ضربه محکوم شود**.»**

قانون مجازات اسلامی، کتاب پنجم، «مرکز انساد حقوق بشر ایران»، قابل دسترسی در: « https://iranhrdc.org/islamic-penal-code-of-the-islamic-republic-of-iran-book-five/»

48 ماده ۶۱۸**: «**هر کس با هیاهو و جنجال یا حرکات غیر متعارف یا تعرض به افراد موجب اخلال نظم و آسایش و آرامش عمومی گردد یا مردم را ازکسب و کار باز دارد به حبس از سه ماه تا یک سال و تا **(**۷۴**)** ضربه شلاق محکوم خواهد شد**.»**

قانون مجازات اسلامی، کتاب پنجم، **«**مرکز انساد حقوق بشر ایران**»**، قابل دسترسی در**: « https://iranhrdc.org/islamic-penal-code-of-the-islamic-republic-of-iran-book-five/»**

«لایحه صیانت و حفاظت از داده‌های شخصی» خواهان استفاده از مجازات‌های درجه ۵ و ۶ می شود. درک این نکته ضروری است که این مجازات‌ها را تحت آزمون «ضرورت و نسبیت» درک کنیم. حکم شلاق که جزو مجازات‌های درجه ۶ محسوب می‌شود هم مغایر با میثاق حقوق مدنی است و هم مغایر با کنوانسیون علیه شکنجه که هر دو «شکنجه و مجازات‌ها یا برخوردهای ظالمانه، غیرانسانی و تحقیرکننده» را ممنوع می‌دارند.
باضافه لایحه صیانت از داده‌های شخصی هم مثل قانون مجازات اسلامی هم شرکت‌ها (یا اشخاص حقوقی) را موجب مجازات می‌داند و هم افراد (یا اشخاص حقیقی) را چنان‌که در مجازات‌هایی که در زیر برای هر دو آمده می‌بینیم. ما در آن بخش از این گزارش که به کاربست ناروشن لایحه می‌پردازد به مشکلاتی که اعطای حق داشتن حریم خصوصی به شرکت‌ها پیش می‌آورد اشاره کرده‌ایم — پیشینه این اعطای حق در قانون مجازات اسلامی است.

درجه ۵:

- ۲ تا ۵ سال زندان
- هشتاد میلیون تا صد و هشتاد میلیون ریال جریمه
- محرومیت از حقوق اجتماعی از پنج تا پانزده سال
- ممنوعیت دائمی از فعالیت‌های حرفه‌ای یا اجتماعی برای اشخاص حقوقی
- ممنوعیت دائمی از دعوت عمومی برای افزایش سرمایه برای اشخاص حقوقی

درجه ۶

— زندان از شش ماه تا دو سال
— جریمه از بیست تا هشتاد میلیون ریال
— شلاق از سی و یک تا هفتاد چهار ضربه و تا سقف نود و نه ضربه در جرایم هتک عفت
— محرومیت از حقوق اجتماعی از شش ماه تا پنج سال
— انتشار حکم نهایی در رسانه‌ها
— ممنوعیت از فعالیت‌های حرفه‌ای و اجتماعی برای اشخاص حقوقی تا سقف پنج سال
— ممنوعیت تهیه بعضی اسناد تجاری برای اشخاص حقوقی تا سقف پنج سال

«قانون جرایم رایانه‌ای»[49] که در سال ۱۳۸۹ تصویب شده همچنان باعث نگرانی جدی در زمینه آزادی بیان و حفظ حریم خصوصی است. بخصوص:

— ماده ۱۴ این قانون می‌گوید «هر کس ... محتویات مستهجن را تولید، ارسال، منتشر، توزیع یا معامله کند یا به قصد ارسال یا انتشار یا تجارت تولید یا ذخیره یا نگهداری کند» مجرم است.

[49] تحلیل حقوقی آرتیکل ۱۹: **https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf**

— ماده ۱۰ می‌کوشد با ممنوعیت عملی استفاده کاربران و شرکت‌های اینترنتی از رمزگذاری یا حفاظت از داده‌ها به کار نظارت دولت بر جامعه کمک برساند. این ماده هرگونه حفاظت از داده‌ها که «مانع دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی شود» ممنوع کرده.

— ماده ۲۱ شرکت‌های ارائه خدمات دسترسی اینترنتی را موظف می‌دارد داده‌های مربوط به استفاده کاربران از اینترنت و اطلاعات شخصی این کاربران را حفظ کنند و ماه ۴۸ آن‌ها را موظف می‌دارد داده‌های مربوط به تماس‌های تلفنی در اینترنت را نگاه دارند و عملا نظارت وسیع دولت بر مردم را قانونی می‌کند.

این مواد قانونی مبهم به نیروهای انتظامی از جمله سپاه پاسدارانِ تندرو و فتا، پلیس فضای تولید و تبادل اطلاعات ناجا[50]، امکان داده‌اند دست به دستگیری خودسرانه افراد بر اساس انگیزه‌های سیاسی بزنند. از جمله مجازات‌هایی که اعمال می‌شود زندان و جریمه است.

از نمونه‌های قابل توجه را در خرداد ۱۳۹۴ دیدیم. فتا دست به دستگیری فردی زد که متهم بود به راه‌اندازی «۲۳ گروه ضدفرهنگی در نرم‌افزار لاین و واتس‌اپ» و «نشر اکذیب و مسائل غیراخلاقی» بود و بدین سان ناقض ماده ۱۴ قانون جرایم رایانه‌ای شده بود[51]. این بخشی از روند هدف گرفتن افرادی بود که در پلاتفرم‌های اینترنتی دست به اشتراک محتوا می‌زدند. این اقدامات در روزهای منتهی به انتخابات ریاست‌جمهوری و بعد از آن منتشر می‌شد و هدفش باز داشتن مردم ایران از دستیابی به اطلاعات مهم در اینترنت و انتشار آن‌ها بود.

چهار. تحلیل پیش‌نویس لایحه «حفاظت و صیانت از داده‌های شخصی»

روبهمرفته، لایحه به خوبی تنظیم نشده و شامل مواد متعدد ناسازگار و متناقض است و عموما درک آن دشوار است و این به شدت از موثر بودن آن می‌کاهد. با توجه به فقدان ضمانت‌های موثر در قانون کنونی ایران، رسیدگی به این کمبودها و تضمین این‌که این قانون سازگار با معیارهای بین‌المللی خواهد بود و حافظ تمام و کمال حقوق صیانت از داده‌های تمام مردم ایران، امری ضروری است.

باضافه، این لایحه همگام با قانون اروپا نیست (با این‌که گفته شده بود هدف اصلی آن چنین است). در خردادماه ۱۳۹۷ که «مقررات عمومی صیانت از داده‌های اتحادیه اروپا» اجرایی شد، آذری جهرمی، وزیر ارتباطات، اعلام کرد لایحه صیانت از داده‌ها ظرف چند ماه آینده تصویب می‌شود و ابراز امیدواری کرد که مذاکرات سازنده‌ای با اتحادیه اروپا درباره کمک دوجانبه و حقوقی صورت بگیرد[52]. دولت در بیانیه مطبوعاتی خودش اعلام کرد که هدف از لایحه اعمال حق حریم خصوصی است که در قانون اساسی آمده و پر کردن خلا حقوقی در این مورد[53]. ما در تحلیلی که این‌جا انجام داده‌ایم می‌کوشیم نشان دهیم که این لایحه از هر دو نظر به اهداف خود نمی‌رسد. یعنی

---

[50] پلیس فتا در سال ۱۳۹۰ به عنوان واحد جرایم سایبری نیروی انتظامی ایران ایجاد شد. تشکیل این واحد در تبعیت از قانون جرایم رایانه‌ای بود که مجلس ایران در همان سال تصویب کرد. **http://bbc.in/1VOXj2I**

http://www.iran-newspaper.com/newspaper/BlockPrint/67527[51]

[52] آذری جهرمی، وزیر ارتباطات ایران، در روز ۴ خرداد ۱۳۹۷ توئیت کرد: «تبریک به کمیسیون اتحادیه اروپا بخاطر اعمال سند «مقررات صیانت از داده‌ها»، که مجموعه قوانینی جامع است! من هم می‌خواهم در چند ماه آینده سند صیانت از داده‌ها را تصویب کنم و می‌خواهیم مذاکرات سازنده‌ای با اتحادیه اروپا درباره همکاری دوجانبه حقوقی و فنی انجام دهیم.»

https://twitter.com/azarijahromi/status/999668731852877824?s=20

[53] نگاه کنید به بیانیه مطبوعاتی که لایحه را اعلام می‌کند

https://ito.gov.ir/news/-/view/ انتشار-پیش-نویس-لایحه-حمایت-از-داده-ها-وحریم-خصوصی-در-فضای-مجازی **/1409**

نه منطبق با «مقررات عمومی صیانت از داده‌های اتحدیه اروپا» است و نه قانون جامعی در زمینه صیانت از داده‌ها به حساب می‌آید چرا که فاقد اصول عمومی است.

الف. فقدان اصول

اولین مشکل لایحه این است که اصول بنیادین ناظر بر آن به روشنی بیان نشده‌اند و در متن نیامده‌اند. چنان‌که در بالا نشان دادیم سند «رهنمودهای نگهداری از داده‌های شخصی در کامپیوترها» مصوب سازمان ملل در سال ۱۳۶۹ که به تصویب مجمع عمومی رسیده شش اصل را به عنوان حداقل ضمانت‌ها که باید در مقررات کشوری بیایند ضروری می‌دارد. این اصول از این قرارند: اصل قانونی بودن و انصاف، اصل دقت، اصل مشخص کردن هدف، اصل دسترسی فرد مورد علاقه، اصل عدم تبعیض و اصل امنیت.

تنها اصول شفافیت و امنیت هستند که به روشنی در بخش سوم لایحه مورد اشاره قرار گرفته‌اند. اصول قانونی بودن و انصاف، دقت، مشخص کردن هدف، دسترسی فرد مورد علاقه و عدم تبعیض در لایحه نیامده‌اند. تاکید این اصول بر این است که پردازش داده‌ها باید به طور قانونی و منصفانه و برای اهداف مشخص و بر بنیان اطلاع و رضایت فرد مورد نظر (یا بنیان مشروع دیگری که قانون تعیین کرده) صورت بگیرد. رویکردی که لایحه اتخاذ کرده لازم می‌دارد مدام در قانون عقب و جلو برویم و این‌گونه خطر این وجود دارد که به طور پایدار اعمال نشود.

چنین چیزی مغایر با شیوه تدوین تقریبا تمام قوانین صیانت از داده‌ها در جهان و مغایر با موازین بین‌المللی است. مثلا قانون «صیانت از داده‌های شخصی» ترکیه در ماده ۴ خود می‌گوید داده‌های شخصی در انطباق با اصول قانونی بودن و انصاف، دقت، مشخص بودن هدف، محدودیت ذخیره و حداقل‌سازی داده پردازش می‌شوند.[54] این آخری اصلی است که سند «مقررات» اروپا مقرر داشته و طبق آن داده‌های شخصی باید به حد کافی اما نه بیشتر، مربوط به موضوع و محدود به آن چه برای هدف مورد نظر ضروری است باشند.[55] به همین سان قوانین صیانت از داده‌ها در لبنان[56] و الجزایر[57] نیز شامل اصول محدود بودن هدف، حداقل سازی داده و دقت هستند.[58]

پیشنهاد

— لایحه می‌بایست از نو تنظیم شود تا نظمی دوباره بیابد، خوانا و قابل درک باشد و اصولی که در قانون بین‌المللی آمده را به کلی در متن قانون، در قسمت مشخصی پس از بخش دو که «تعاریف» را مطرح کرده بگنجاید.

ب. ناروشن بودن حیطه کاربست

۱. فقدان روشن ساختن حیطه مادی و قلمرویی کاربست

---

[54] ترکیه، قانون صیانت از داده‌های شخصی، ماده ۴

[55] سند «مقررات»، ماده ۵

[56] لبنان، قانون شماره ۸۱ در رابطه با داد و ستدهای الکترونیک و داده‌های شخصی، ماده ۸۷

[57] قانون الجزایر درباره پاسداشت افراد فیزیکی برای پردازش داده‌های شخصی، ۲۰ خرداد ۱۳۹۷، ماده ۹

[58] قانون شماره ۳۰ بحرین برای سال ۲۰۱۸ که «قانون صیانت از داده‌های شخصی» را صادر کرده است، ماده ۳

دیگر خلا چشمگیر در لایحه فقدان هرگونه ماده روشن برای تعیین حیطه مادی و قلمرویی کاربست آن است. به گفته ماده ۱(ب) لایحه ناظر است بر «فرایند پردازش داده‌های شخصی.» در این ماده هدف قانون تعیین‌شده اما لایحه ماده‌ای ندارد که حیطه مادی آن‌را توضیح بدهد. منظور از حیطه مادی معمولا تعریف آن انواعی از پردازش داده‌های شخصی است که لایحه در مورد آن‌ها کاربست دارد و آن‌ها که برعکس خارج از حیطه آن هستند. قوانین صیانت از داده‌ها معمولا حیطه قلمرویی خود را نیز تعیین می‌کنند تا معلوم شود اشخاص و سازمان‌ها در کدام قلمرو موظف به تبعیت از این قانون هستند. لایحه چنین موادی ندارد.

نگاهی داشته باشیم به سند «مقررات» اتحادیه اروپا تا تفاوت را ببینیم. این سند در زمینه حیطه مادی اعلام می‌کند که شامل است بر پردازش کامل یا بخشی که به طرق خودکار انجام شود مثلا با استفاده از کامپیوترهایی که داده‌های دیجیتال دارند. باضافه، پردازش داده‌های شخصی به هر شیوه دیگری نیز تحت ضوابط این سند محسوب می‌شود به شرط این‌که داده‌ها در سیستم ذخیره‌ای قرار داشته باشند (یا قصد استفاده از آن‌ها در چنین سیستمی موجود باشد) که در ماده ۲(۱) سند آمده. مثلا وقتی که داده‌های شخصی به طور دستی پردازش می‌شوند و در سیستم ذخیره‌ای قرار دارند یا قرار است قرار داشته باشند که مجموعه‌های ساختاریافته‌ای از داده‌های شخصی را دارد که قابل دسترسی بر طبق شرایطی مشخص هستند، مثلا پرونده‌های دستی که روی کاغذ چاپ می‌شوند.

در زمینه حیطه قلمرویی، ماده ۳(۱) سند «مقررات» اعلام می‌کند که مربوط به است به پردازش داده‌های شخصی توسط کنترل‌گرها و پردازشگرهایی که در اتحادیه اروپا حضور دارند. از این لحاظ این‌که خود کار پردازش درون اتحادیه انجام می‌شود یا خارج از آن اهمیت ندارد.

نکته مهم این‌جا است که ماده ۳(۲) سند مقررات اعلام می‌کند که وقتی کنترل‌گران و پردازشگران در اتحادیه اروپا حضور ندارند اما داده‌های شخصی افرادی را که در اتحادیه هستند پردازش می‌کنند این سند شامل آن‌ها هم می‌شود. چنین فعالیت‌های پردازشی باید مربوط به ارائه کالاها یا خدماتی در ازای پرداخت یا رایگان به این افراد باشد و یا به نظارت بر رفتار این افراد تا زمانی که این رفتار در اتحادیه اروپا صورت می گیرد، چنان‌که در مواد ۳(۲)(الف) و (ب) سند آمده. بالاخره این سند ناظر است بر پردازش داده‌های شخصی توسط کنترل‌گرهایی که در اتحادیه مستقر نیستند اما جای دیگری هستند که قوانین یکی از دولت‌های عضو اتحادیه اروپا به دلیل قانون بین‌المللی عمومی در آن‌جا کاربست دارد. مثلا در مقرهای دیپلماتیک یا کنسولی دولت‌های عضو اتحادیه اروپا.

طبق موازین بین‌المللی، ضروری است که قانون هم در مورد نهادهای خصوصی و هم در مورد نهادهای عمومی کاربست داشته باشد. کمیته حقوق بشر سازمان ملل و بیانیه مجمع عمومی سازمان ملل هر دو به روشنی گفته‌اند که حق حریم خصوصی مورد پاسداشت قوانین صیانت از داده‌ها شامل اطلاعاتی می‌شود که در اختیار نهادی خصوصی یا عمومی است. عموما مورد پذیرش است که حق داشتن حریم خصوصی وظایف مثبتی برای دولت‌ها ایجاد می‌کند که از اتخاذ قوانینی کسب اطمینان کنند که تمام افراد را علیه حملات مورد حفاظت قرار می‌دهند. کمیته حقوق بشر سازمان ملل در «اظهار نظر عمومی شماره ۱۶» می‌گوید:

«به نظر این کمیته این حق باید در مقابل تمام دخالت‌ها و حملات چه از سوی مقامات دولتی بیایند و چه از سوی اشخاص حقیقی و حقوقی مورد حفاظت قرار بگیرد. وظایفی که این ماده مقرر می‌دارد دولت را موظف می‌کند که دست به اقدامات مناسب تقنینی و غیره بزند تا ممنوعیت علیه چنین دخالت‌ها و حملاتی و همچنین حفاظت از این حق عملی شود.»[59]

[59] کمیته حقوق بشر سازمان ملل، اظهار نظر عمومی شماره ۱۶: حق احترام به حریم خصوصی، خانواده، خانه و مراسلات و پاسداشت شرف و شهرت (ماده ۱۷)، **CCPR/C/GC/16** ، ۱۳ مرداد ۱۳۶۷

مجمع عمومی سازمان ملل در سند «رهنمودهای نگهداری از داده‌های شخصی در کامپیوترها» در رابطه با «حیطه کاربست» می‌گوید:

«اصول حاضر باید در وهله اول در مورد تمام پرونده‌های کامپیوتری خصوصی و عمومی به کار بروند و همچنین، از طریق گسترش انتخابی و بسته به تمام تطبیق‌های مناسب، در مورد پرونده‌های دستی. می‌توان مواد ویژه‌ای (ایضا انتخابی) به میان آورد تا تمام یا بخشی از این اصول به پرونده‌های موجود در مورد اشخاص حقوقی گسترش یابند بخصوص وقتی که شامل اطلاعاتی در مورد افراد هستند.»[60]

تقریبا تمام قوانین صیانت از داده‌ها در جهان هم شامل پردازش اطلاعات شخصی می‌شود که در اختیار نهادهای دولتی هستند و هم خصوصی. در منطقه هم همین است. قانون صیانت از داده‌های الجزایر که در سال ۱۳۹۷ تصویب شد ماده‌ای دارد که به صراحت می‌گوید هم در مورد بخش خصوصی کاربست دارد و هم در مورد نهادهای عمومی.[61] در قطر، «قانون صیانت از حریم خصوصی داده‌های شخصی» مقرر می‌دارد که این قانون در مورد «داده‌های شخصی که مورد پردازش الکترونیکی قرار می‌گیرند [کاربست دارد] هنگام دریافت، جمع‌آوری و ذخیره به هر شیوه دیگری که منجر به پردازش الکترونیکی شود.»[62] همین‌طور قوانین موجود صیانت از داده‌ها در مراکش[63] و تونس که سابقه‌ای طولانی دارند نیز به روشنی هم در مورد نهادهای خصوصی کاربست دارند و هم در مورد نهادهای عمومی.[64]

تعریف روشن حیطه کاربست قطعیت حقوقی و مسئولیت‌پذیری ایجاد می‌کند بخصوص در رابطه با نهادهای عمومی که داده‌های شخصی را پردازش می‌کنند. بدین‌سان این مواد قانونی باید طوری تنظیم شوند که به روشنی اعلام کنند این قانون راجع به هر دو بخش دولتی و خصوصی می‌شود.

۲. کاربست تبعیض‌آمیز بر بنیان شهروندی

ماده ۳ لایحه می‌گوید: «اشخاص مشمول این قانون عبارت‌اند از: الف) اتباع ایرانی حقیقی یا حقوقی عمومی یا خصوصی، اعم از آن‌که داده‌های شخصی آن‌ها درون یا بیرون از ایران پرداز شود. ب) اتباع خارجی حقیقی یا حقوقی عمومی یا خصوصی که داده‌های شخصی آن‌ها از سوی کنترل‌گر یا پردازشگر ایرانی پردازش می‌شود.»

این ماده ناقض اصل عدم تبعیض است چرا که بین افراد موضوع داده بر اساس شهروندی‌شان تمایز قائل می‌شود. کمیته حقوق بشر سازمان ملل در «اظهار نظر عمومی شماره ۱۶ می‌نویسد:

«ماده ۱۷ حقوق تمام اشخاص را در مقابل دخالت خودسرانه یا غیرقانونی در مورد حریم خصوصی، خانواده، خانه یا مراسلات و همچنان حملات غیرقانونی علیه شهرت و کرامت مورد حفاظت قرار می‌دهد.»[65]

---

[60] رهنمودهای نگهداری از داده‌های شخصی در کامپیوترها، قطعنامه مجمع عمومی سازمان ملل ۹۵/۴۵، ۲۳ آذر ۱۳۶۹ http://www.un.org/documents/ga/res/45/a45r095.htm.

[61] قانون الجزایر درباره پاسداشت افراد فیزیکی برای پردازش داده‌های شخصی، ۲۰ خرداد ۱۳۹۷ ، ماده چهار

[62] قطر، قانون شماره ۱۳ سال ۲۰۱۶، اعلام «قانون صیانت از حریم خصوصی داده‌های شخصی، ماده ۲

[63] مراکش، قانون ۰۹-۰۸ درباره صیانت از افراد در رابطه با پردازش داده‌های شخصی ماده ۲

[64] تونس، قانون شماره ۲۰۰۴-۴۳ مورخ ۶ مرداد ۱۳۸۳ درباره صیانت از داده‌های شخصی، ماده ۲

[65] کمیته حقوق بشر سازمان ملل، اظهار نظر عمومی شماره ۱۶: حق احترام به حریم خصوصی، خانواده، خانه و مراسلات و پاسداشت شرف و شهرت (ماده ۱۷)، CCPR/C/GC/16، ۱۳ مرداد ۱۳۶۷

کنوانسیون جدید ۱۰۸ شورای اروپا درباره صیانت از داده‌ها نیز می‌گوید:

«هدف از این کنوانسیون حفاظت از تمام افراد، مستقل از ملیت و محل سکونت، در رابطه با پردازش داده‌های شخصی آن‌ها است و بدین‌سان مشارکت در ایجاد احترام برای حقوق بشر و آزادی‌های بنیادین فرد و بخصوص حق داشتن حریم خصوصی.»[66]

سند «مقررات» اتحادیه اروپا نیز اعلام می‌کند که در مورد «پردازش داده‌های شخصی افرادی که در اتحادیه اروپا هستند» کاربست دارد.[67] قانون صیانت از داده‌ها که اخیرا در بحرین تصویب شده نیز در مورد اشخاص حقیقی کاربست دارد که مشغول کسب و کار در کشور یا بیرون آن هستند به شرط این‌که «از وسایلی استفاده کنند که در بحرین قابل دسترسی باشد.»[68]

۳. لایحه به شرکت‌ها حق داشتن حریم خصوصی می‌دهد

دیگر مشکل لایحه این است که حقوق صیانت از داده‌های افراد را شامل شرکت‌ها نیز می‌کند. این جنبه‌ای مشکل‌آفرین از قانون است که علیه موازین بین‌المللی است. باید بخاطر داشت که حق داشتن حریم خصوصی و صیانت از داده‌ها جزو حقوق بشرند و در نتیجه فقط در مورد افراد به کار می‌روند. شرکت‌ها که شخصیت‌های حقوقی هستند شاید ضمانت‌های قانونی مشخصی در رابطه با اسرار تجاری، مالکیت فکری و محرمانه بودن تجاری داشته باشند و همچنین مسئولیت‌هایی در قبال پاسداشت حق کارمندان و مشتریان برای داشتن حریم خصوصی اما نمی‌توان به شرکت‌ها حق حفاظت از حریم خصوصی‌شان را داد چون شخصیت حقوقی اصلا نمی‌تواند چنین حریمی داشته باشد.

این اصل در عمل می‌تواند بسیار مشکل‌آفرین باشد و می‌تواند منجر شود روزنامه‌نگاران مجبور به حذف ارجاع به شرکت‌ها در مقالات خبری خود شوند و یا مجبور به ارائه اطلاعات در مورد منابع‌شان؛ می‌تواند شرکت‌های اینترنتی را وادار کند مقالاتی که فساد یا اعمال غیراخلاقی را افشا می‌کند سانسور کنند؛ و یا می‌تواند نهادهای عمومی را از افشای شرکت‌هایی که بخاطر الغای قوانین مورد تحقیق هستند منع کند.

چنان‌که در بالا گفتیم، کمیته حقوق بشر سازمان ملل اعلام کرده که آن ماده «حق تمام افراد» و نه شخصیت‌های حقوقی را مورد حفاظت دارد. قطعنامه‌ای که مجمع عمومی سازمان ملل در روز ۲۹ آذر ۱۳۹۵ تصویب کرد تاکید می‌کند که «همان حقوقی که مردم در خارج از اینترنت دارند باید در اینترنت نیز مورد حفاظت قرار بگیرد از جمله حق داشتن حریم خصوصی.» [69]

مورد جدیدتر سند «مقررات» اتحادیه اروپا است که می‌گوید:

---

66 شورای اروپا، کنوانسیون جدید برای حفاظت از افراد در رابطه با پردازش داده‌های شخصی، در تصحیح پروتکل «کنوانسیون حفاظت از افراد در رابطه با پردازش داده‌های شخصی»، ماده ۱۱، مصوب کمیته وزرا در جلسه ۱۲۸ام آن در هلسینگور در ۲۸ اردیبهشت ۱۳۹۷
https://www.coe.int/en/web/data-protection/convention108-and-protocol

67 سند «مقررات» اتحادیه اروپا، ماده ۲ـ۳

68 قانون شماره ۳۰ بحرین برای سال ۲۰۱۸ که «قانون صیانت از داده‌های شخصی» را صادر کرده است، ماده ۲

69 حق داشتن حریم خصوصی در عصر دیجیتال، قطعنامه مجمع عمومی ۱۹۹/۷۱، ۲۹ آذر ۱۳۹۵، بند ۳

«آن ضمانت حقوقی که این سند ارائه می‌کند باید در مورد اشخاص حقیقی به کار بسته شود مستقل از ملیت یا مکان سکونت‌شان، در رابطه با پردازش داده‌های شخصی‌شان. این سند شامل پردازش داده‌های شخصی مربوط به شخصیت‌های حقوقی نمی‌شود، بخصوص در مورد اقدامات برپایی شخصیت‌های حقوقی از جمله نام و شکل شخص حقوقی و اطلاعات تماس شخص حقوقی.»[70]

باضافه این سند داده‌های شخصی را چنین تعریف می‌کند

«هرگونه اطلاعات مربوط به شخص حقیقی شناسایی‌شده یا قابل شناسایی («موضوع داده»)؛ شخص حقیقی قابل شناسایی فردی است که قابل شناسایی مستقیم یا غیرمستقیم باشد بخصوص با ارجاع به شناسه‌ای همچون اسم، شماره شناسایی، داده‌های محل، شناسه اینترنتی یا یک یا چند عامل که مختص به هویت جسمی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی یا اجتماعی آن فرد طبیعی باشد.»[71]

پیشنهادها

— لایحه می‌بایست شامل ماده مشخصی باشد که حیطه مادی و قلمرویی آن‌را تعیین کند. این ماده باید به روشنی اعلام کند که در مورد تمامی نهادهای دولتی و همچنین نهادهای خصوصی کاربست دارد. در حال حاضر این حقوق در سایر قوانین ایران مورد پاسداشت کافی نیستند. این تغییرات باید با قانون انتشار و دسترسی آزاد به اطلاعات ۱۳۸۸ ایران هماهنگ شوند.

— ماده ۳ باید از نو نوشته شود تا با اصل عدم تبعیض همگام گردد و شامل تمام افراد شود و نه فقط شهروندان ایرانی و شهروندان خارجی که داده‌هایشان درون خاک ایران پردازش می‌شود. قانون در شکل کنونی‌اش بین شهروندان ایرانی و خارجی فرق می‌گذارد و در ضمن شهروندان بدون دولت را محسوب نمی‌کند و این مشکل‌آفرین است.

— لایحه می‌بایست مشخصا اعلام کند که در مورد حریم خصوصی و صیانت از داده‌های شرکت‌ها کاربست ندارد.

ج. تاثیر بر آزادی بیان و اطلاعات

دیگر مشکل چشمگیر لایحه رابطه آن با آزادی بیان است. چنان‌که در بالا گفتیم، تحت قانون بین‌الملل دولت‌ها می‌بایست کاری کنند که اعمال حقوق صیانت از داده‌ها شامل استثناها یا محدودیت‌های وسیع بشود تا استفاده از آزادی بیان تضمین شود.

دفتر کمیسیونر عالی حقوق بشر سازمان ملل در گزارش خود با عنوان «حق حریم خصوصی در عصر دیجیتال» که در تابستان ۱۳۹۷ به شورای حقوق بشر ارائه شد تاکید کرد:
«مهم است که چارچوب قانونی تضمین کند که این حقوق (یعنی حقوق داشتن حریم خصوصی و صیانت از داده‌ها) حق آزادی بیان را محدود نمی‌کنند، از جمله حق پردازش داده‌های شخصی برای مصارف روزنامه‌نگارانه، هنرمندانه و دانشگاهی.»[72]

---

[70] سند «مقررات»، ماده متمم ۱۴، در ضمن نگاه کنید به ماده ۱ و ۲

[71] سند «مقررات»، ماده متمم ۱۴، در ضمن نگاه کنید به ماده ۴

[72] گزارش سالیانه کمیسیونر عالی حقوق بشر سازمان ملل و گزارش‌های دفتر کمیسیونر عالی و دبیر کل، **A/HRC/39/29** در ۱۲ مرداد ۱۳۹۷

دیوان دادگستری اروپا رای داده که دولت‌ها می‌بایست «توازن منصفانه» بین حق حریم خصوصی و آزادی بیان بر بنیان اصل تناسب برقرار کنند. چنان‌که این دیوان در پرونده‌ای در سال ۱۳۸۷ اشاره کرد:

«برای درک اهمیت حق آزادی بیان در هر جامعه دموکراتیک اول باید مفاهیم مربوط به آن آزادی، مثل روزنامه‌نگاری، را وسیعا تفسیر کرد. دوم، برای رسیدن به توازن بین این دو حق بنیادین، ضمانتِ حق بنیادین داشتن حریم خصوصی نیازمند این است که محدودیت‌هایی که در رابطه با صیانت از داده‌ها در فصل‌های سندی که در بالا به آن اشاره شده آمده تنها تا جایی به کار بسته شوند که اکیدا ضروری است.»

لایحه در مقدمه خود چند اصل قانون اساسی را یادآوری می‌کند از جمله فصل سوم به طور کلی و بعضی مواد به طور مشخص. نکته نگران‌کننده این‌جا است کهحق آزادی بیان که در اصل ۲۴ قانون اساسی آمده در کنار سایر حقوق مثل حق داشتن حریم خصوصی مورد اشاره قرار نمی‌گیرد. چنان‌که در بالا توضیح دادیم این دو حق پشتیبان یکدیگر هستند. باید بین آن دو به شیوه‌ای منصفانه ایجاد توازن کرد بدون این‌که یکی بر دیگری برتر شمرده شود. قانون بین‌المللی حقوق بشر بین حقوق مختلف سلسله‌مراتب به رسمیت نمی‌شناسد. در ضمن ضروری است که اهمیت آزادی بیان به رسمیت شناخته شود چرا که جمع‌آوری و پردازش غیرقانونی داده‌های شخصی بخصوص اگر در مورد روزنامه‌نگاران باشد بر قابلیت رسانه‌ها برای فعالیت و برای دنبال کردن پیگیر تحقیقات و دریافت اطلاعات از منابع محرمانه و غیره تاثیر خواهد گذاشت.

۱. عدم شمول استثنا در موارد روزنامه‌نگارانه، هنری، ادبی و سایر موارد فرهنگی

ماده ۱۲ لایحه می‌گوید که پردازش داده‌های شخصی درون چارچوب قوانین مربوطه بدون اجازه افراد در بعضی موارد مجاز است. هیچ اشاره‌ای به استثنا برای مصارف روزنامه‌نگارانه، هنرمندانه، ادبی و فرهنگی نشده است. این کوتاهی جدی در قانون پیشنهادی است. نکته نگران‌کننده‌تر این‌که پردازش برای مصارف روزنامه‌نگارانه اصلا مورد توجه قرار نگرفته. لایحه، منافع مربوط به آزادی بیان را (مثلا تبادل آزاد اطلاعات توسط افراد) به رسمیت نمی‌شناسد و همچنین مصارف فوق‌الذکر هنری، ادبی و فرهنگی را.

تقریبا تمام کشورهای جهان که قوانینی در رابطه با صیانت از داده‌ها اتخاذ کرده‌اند مشخصا استثناهای روشنی برای مصارف روزنامه‌نگارانه، هنرمندانه، ادبی و سایر موارد فرهنگی قائل شده‌اند که امکان می‌دهد قوانین محدودکننده پردازش برای این مصارف لغو شوند. در ضمن باید استثناهایی لحاظ شود که ارائه عمومی اطلاعات همچون حفظ بایگانی برای مصارف تاریخی یا مصارفی در جهت منافع عمومی یا تحت قوانین دسترسی به اطلاعات مسئولیت قانونی نداشته باشد. باضافه چنین استثناها یا محدودیت‌هایی می‌بایست آنقدر وسیع تفسیر شوند که حق آزادی بیان و حق دسترسی به اطلاعات معنی داشته باشد.

این استثنا در زمینه پردازش داده‌های شخصی برای اولین بار در ماده ۹ «فرمان صیانت از داده‌های اتحادیه اروپا ۴۵/۹۵» که چارچوب حقوقی قدیمی اروپا بود مطرح شد. دیوان دادگستری اروپا در پرونده‌ای که در بالا نقل شد اعلام کرد که مواد آن فرمان فراتر از تنها رسانه‌های رسمی کاربرد دارند: «استثناها و محدودیت‌هایی که ماده ۹ فرمان مطرح کرده نه فقط در مورد فعالیت‌های رسانه‌ها که در در مورد هر فردی که مشغول امر روزنامه‌نگاری است شمول دارند.» این دادگاه اعلام کرد که استثنای روزنامه‌نگاری در صورتی کاربست دارد که «هدف، انتشار

---

https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx

اطلاعات، نظرها یا افکار نزد عموم باشد، مستقل از وسیله انتقال این اطلاعات. این محدود به فعالیت رسانه‌ها نیست و می‌تواند شامل مصارف سودآور نیز باشد.»

گستره فعالیت‌های مربوط به آزادی بیان که تحت پاسداشت هستند با اتخاذ سند «مقررات» اتحادیه اروپا گسترش یافته. در ماده ۸۰ می‌خوانیم:

پردازش داده‌های شخصی و آزادی بیان و اطلاعات

۱. قانون کشوری دولت‌های عضو بین حق صیانت از داده‌های شخصی که در این سند آمده با حق آزادی بیان و اطلاعات از جمله حق پردازش داده‌های شخصی برای مصارف روزنامه‌نگارانه و مصارف دانشگاهی، هنرمندانه و بیان ادبی ایجاد توازن می‌کند.

۲. برای پردازش داده‌های شخصی جهت مصارف روزنامه‌نگارانه یا مصارف بیان دانشگاهی، هنرمندانه و ادبی، دولت‌های عضو باید در صورتی که همگام ساختن حق پاسداشت داده‌های شخصی با حق آزادی بیان و اطلاعات نیازمند استثناها یا محدودیت‌هایی بر اصول آمده در فصل دوم (اصول)، فصل سوم (حقوق سوژه داده‌ها)، فصل چهارم (کنترل‌گر یا پردازشگر)، فصل پنجم (انتقال داده‌های شخصی به کشورهای سوم یا سازمان‌های بین‌المللی)، فصل ششم (مقامات نظارتی مستقل) یا فصل هفت (همکاری و انطباق) باشد، چنین استثناها یا محدودیت‌هایی را ارائه کنند.

کنوانسیون جدید ۱۰۸ شورای اروپا درباره پاسداشت داده‌ها هم مواد مشخصی در رابطه با آزادی بیان دارد. ماده ۱۱ (ب) اعلام می‌کند که دولت‌های عضو باید در موارد لازم برای «پاسداشت موضوع داده یا حقوق و آزادی‌های بنیادین دیگران، بخصوص آزادی بیان»[73] استثناهایی در نظر بگیرند. نظرات تفسیری که در مورد این کنوانسیون نوشته شده بیشتر توضیح می‌دهد:

«بخش ب درباره حقوق و آزادی‌های بنیادین طرفین خصوصی مثلا حقوق خود فرد موضوع داده (مثلا وقتی منافع حیاتی این فرد به علت فقدان فیزیکی او در خطرند) است یا حقوق طرفین سوم همچون آزادی بیان از جمله آزادی بیان روزنامه‌نگارانه، دانشگاهی، هنرمندانه یا ادبی و حق دریافت و ارائه اطلاعات، محرمانه بودن مراسلات و ارتباطات یا مخفی بودن داد و ستد و تجارت و سایر اسراری که تحت پاسداشت قانونی هستند. این بخصوص باید درباره پردازش داده‌های خصوصی در زمینه سمعی-بصری کاربرد داشته باشند و در بایگانی‌های خبر و کتابخانه‌های مطبوعاتی. برای در نظر گرفتن اهمیت حق آزادی بیان در تمام جوامع دموکراتیک، ضروری است که مفاهیم مربوط به آن آزادی مثل روزنامه‌نگاری وسیعا تفسیر شوند.»

در سطح داخلی، بیشتر قوانین صیانت از داده‌ها در سراسر جهان از جمله قوانین کشورهای منطقه استثنایی برای روزنامه‌نگاری قائل شده‌اند. قانون صیانت از داده‌ها در ترکیه استثناهایی در رابطه با داده‌های شخصی که درون

[73] شورای اروپا، کنوانسیون جدید برای حفاظت از افراد در رابطه با پردازش داده‌های شخصی، در تصحیح پروتکل «کنوانسیون حفاظت از افراد در رابطه با پردازش داده‌های شخصی»، ماده ۱۱، مصوب کمیته وزرا در جلسه ۱۲۸ام آن در هلسینگور در ۲۸ اردیبهشت ۱۳۹۷

https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

حیطه آزادی بیان پردازش می‌شوند قائل شده است.[74] در بحرین[75]، لبنان[76] و الجزایر[77]، قوانین صیانت از داده‌ها تاکید می‌کنند که پردازش داده‌های شخصی برای مصارف فعالیت‌های روزنامه‌نگارانه شامل این قوانین نمی‌شود.

۲. حق فراموش شدن

ماده ۹ لایحه اعلام می‌کند «درخواست انجام یا توقف پردازش داده‌های شخصی می‌تواند باهدف فراموشی مطرح شود، مشروط بر آنکه ذی‌نفع دیگری نباشد.»

به نظر می‌رسد هدف از این ماده معرفی مفهوم «حق فراموش شدن» در لایحه و در قانون ایران است. این ماده در برقراری حق تسلیم تقاضای پردازش یا توقف پردازش با «هدف فراموش شدن» شفافیت ندارد و هیچ‌گونه محدودیتی تعیین نکرده. به نظر می‌رسد به هر شخصی، مستقل از موقعیت رسمی یا عمومی او و یا مساله منفعت عموم، این حق مطلق داده می‌شود که اطلاعات مربوط به او حذف شوند.

حق فراموش شدن اولین بار در پرونده «گوگل اسپانیا» مورد بررسی دادگاه اتحادیه اروپا قرار گرفت. طبق این حق، سوژه‌های داده حق دارند از گوگل و سایر موتورهای جستجوی فعال در اتحادیه اروپا تقاضا کنند که لینک‌هایی را از نتایج جستجوی نام آن‌ها حذف کند اما به شرط لحاظ منفعت عموم.

طبق قانون بین‌المللی حق فراموش شدن حق مطلق نیست و آزادی بیان باید در نظر گرفته شود. گزارشگر ویژه سازمان ملل در موضوع آزادی نظر و بیان در گزارش سال ۲۰۱۶ خود بررسی جهانی‌ای از مسائلی که بر آزادی بیان در اینترنت تاثیر می‌گذارند انجام داد از جمله حق فراموش شدن و وظایف دولت‌ها تحت میثاق حقوق مدنی و سیاسی را یادآوری کرد:

«هرگونه خواسته، تقاضا و یا سایر اقدامات برای حذف محتوای دیجیتال یا دسترسی به اطلاعات مصرف‌کنندگان باید بر اساس قانون مصوب باشد و تحت نظارت خارجی و مستقل و یا نشان دادن شیوه ضروری و متناسب دستیابی به یکی یا چند تا از اهدافی که در ماده ۱۹(۳) میثاق بین‌المللی حقوق مدنی و سیاسی آمده. بخصوص در چارچوب تنظیم بخش خصوصی، قوانین و سیاست‌های دولتی باید به طور شفاف مورد اتخاذ و اعمال قرار بگیرند.»[78]

در قضاوت دادگاه اتحادیه اروپا که در بالا آوردیم، این محکمه به صراحت و روشنی اعلام می‌کند که حق فراموش شدن مطلق نیست و همیشه باید در توازن با سایر حقوق بنیادین همچون آزادی بیان و رسانه‌ها قرار بگیرد. این دادگاه مشخصا اعلام کرد:

«موضوع داده شاید بخواهد در پرتوی حقوق بنیادین خود تحت اصول ۷ و ۸ منشور تقاضا کند که اطلاعات مورد نظر در فهرست نتایجی که در اختیار عموم مردم قرار می‌گیرد نباشد. در این موارد... باید تاکید کرد که حق این فرد عموما فراتر از نه فقط منفعت اقتصادی عامل موتور جستجو که فراتر از منفعت عموم مردم در یافتن اطلاعات

---

[74] قانون ترکیه در موضوع صیانت از داده‌های شخصی، ماده ۲۸ (د)

[75] قانون شماره ۳۰ بحرین برای سال ۲۰۱۸ که «قانون صیانت از داده‌های شخصی» را صادر کرده است، ماده ۶

[76] قانون لبنان شماره ۸۱ در رابطه با داد و ستدهای الکترونیک و داده‌های شخصی، ماده ۱۰۵

[77] قانون الجزایر درباره پاسداشت افراد فیزیکی برای پردازش داده‌های شخصی، ۲۰ خرداد ۱۳۹۷، ماده ۲۹

[78] گزارش گزارشگر ویژه در موضوع تشویق و پاسداشت حق آزادی نظر و بیان، دیوید کی، شورای حقوق بشر، ۲۲ اردیبهشت ۱۳۹۵

ناشی از جستجوی نام او است. اما این در مورد زیر صدق نمی‌کند: اگر به دلایل مشخصی (مثلا نقشی که موضوع داده در زندگی عمومی بازی می‌کند) چنین باشد که کاستن از حقوق بنیادین او به علت منفعت قاطع عموم مردم در دسترسی به اطلاعات مورد نظر (از طریق شمول آن در فهرست نتایج) مواجه است».[79]

گروه کار اصل ۲۹ اختیارات صیانت از داده‌های اتحادیه اروپا (اکنون، «اداره صیانت از داده‌های اروپا») نیز رهنمودهایی در توضیح نیاز به رسمیت شناختن آزادی بیان هنگام کاربست این قانون منتشر کرده است:

«منفعت کاربران اینترنت در دریافت اطلاعات با استفاده از موتورهای جستجو نیز باید در نظر گرفته شود. از این لحاظ، حق بنیادین آزادی بیان که منشور حقوق بنیادین اروپا به عنوان «آزادی دریافت و انتشار اطلاعات و افکار» تعریف کرده است باید هنگام بررسی تقاضاهای افراد موضوع داده مورد نظر قرار بگیرد... موتورهای جستجو باید منفعت عموم در داشتن دسترسی به اطلاعات را در بررسی شرایط مربوط به هر تقاضا در نظر بگیرند. اگر منفعت عموم در داشتن دسترسی به این اطلاعات، قاطع است، نتایج نباید حذف شوند.[80]»

از جمله مواردی که برای بررسی تقاضاها در نظر گرفته می‌شوند:

— آیا موضوع داده نقشی در زندگی عمومی بازی می‌کند؟
— آیا موضوع داده شخصیت عمومی است؟
— آیا داده‌ها دقیق هستند؟
— آیا داده‌ها مربوط به زندگی کاری فرد می‌شوند؟
— آیا محتوای منتشرشده در چارچوب مصارف روزنامه‌نگارانه است؟

سند «مقررات» اتحادیه اروپا در دو ماده خود در بخش «حق پاک شدن» این حق را بیشتر شفاف کرده. در ماده ۱۷(۳)(الف) می‌خوانیم که حق پاک شدن در موارد مربوط به «استفاده از حق آزادی بیان و اطلاعات» پذیرفته نمی‌شود. باضافه ماده ۱۷(۳)(ج) موارد زیر را مستثنی می‌کند: «قصد بایگانی در جهت منفعت عموم یا دلایل علمی یا پژوهش تاریخی یا آماری... تا جایی که حق مورد ارجاع در بند اول احتمال دارد دستیابی به اهداف این پردازش را غیرممکن سازد یا به شدت محدود کند.» اصل تکمیلی ۶۵ بر آزادی بیان و حقوق بایگانی تاکید می‌کند:

«حفظ طولانی‌تر داده‌های شخصی باید هنگامی قانونی باشد که برای موارد زیر ضروری است: استفاده از آزادی بیان و اطلاعات، تبعیت از الزام قانونی، اجرای وظیفه‌ای در جهت منفعت عموم و یا استفاده از قدرت عمومی که به کنترل‌گر داده شده، بر مبنای منفعت عموم در زمینه بهداشت عمومی، برای مصارف بایگانی در جهت منفعت عموم، به مصارف علمی یا پژوهش تاریخی یا آماری.»

به همین سان، «گزارش توضیحی» نسخه جدید کنوانسیون ۱۰۸ اشاره می‌کند که حق پاک شدن و سایر حقوق نامحدود نیستند:

«این حقوق باید در هماهنگی با سایر حقوق و منافع مشروع در نظر گرفته شوند. این حقوق می‌توانند در انطباق با ماده ۱۱ زمانی محدود شوند که قانون مقرر کرده و این اقدامی ضروری و متناسب در جامعه‌ای دموکراتیک محسوب می‌شود.»

---

79 پرونده سی-۱۳۱۱۴، گوگل اسپانیا و گوگل علیه آ ئ پ د و ماریو کاستخا گونزالز، ۲۳ اردیبهشت ۱۳۹۳، ص ۸۱

80 گروه کاری صیانت از داده‌های ماده ۲۹، رهنمودهایی درباره اعمال حکم دیوان دادگستری اتحادیه اروپا در پرونده گوگل اسپانیا و گوگل علیه آ ئ پ د و ماریا کوستخا گونزالز، سی-۱۳۱/۱۲ مصوب ۵ آذر ۱۳۹۳ **https://www.pdpjournals.com/docs/88502.pdf**

سازمان «آرتیکل ۱۹» در یکی از اسناد سیاست‌گذاری خود در باره «حق فراموش شدن» آزمونی هفت قطعه‌ای را پیشنهاد داده است

— آیا اطلاعات مورد نظر ماهیت خصوصی دارند؛
— آیا تقاضاکننده انتظار معقولی از داشتن حریم خصوصی از جمله با در نظر گرفتن مسائلی مثل رفتار پیشین، رضایت به انتشار یا وجود قبلی اطلاعات در حوزه عمومی داشته؛
— آیا اطلاعات مورد نظر در جهت منفعت عموم هست؛
— آیا اطلاعات مورد نظر مربوط به چهره‌ای عمومی هست؛
— آیا این اطلاعات بخشی از ثبت عمومی هست؛
— آیا تقاضاکننده نشان داده که در معرض آسیب جدی قرار دارد؛
— اطلاعات مورد نظر متعلق به چند وقت پیش است و آیا همچنان از زاویه منفعت عمومی ارزش دارد.[81]

سازمان «آرتیکل ۱۹» فرای این آزمون نیز ضمانت‌های رویه‌ای زیر را در مورد اعمال این حق پیشنهاد کرده است:

— وظیفه ایجاد توازن بین منافع مربوطه مورد نظر باید بر عهده دادگاه باشد و نه موتور جستجو یا مقامات صیانت از داده‌ها.

— ارائه‌کنندگان محتوا باید بدانند که کسی تقاضای «حق فراموشی» در رابطه با محتوایشان انجام داده و بتوانند چنین تقاضاهایی را به چالش بکشند.

— ارائه‌کنندگان، مقامات دولتی و دادگاه‌های مربوطه باید موظف به انتشار گزارش‌های شفافیت‌ساز در مورد تقاضاهای «حق فراموش شدن» باشند.

۳. مقررات محلی‌سازی

لایحه در ضمن به نظر به نام صیانت از داده‌ها دسترسی ایرانیان به وب‌سایت‌ها و خدمات رایج در اینترنت را محدود می‌کند که این ناقض آزادی بیان افراد است.

فصل ۳، بخش ۵ قانون محدودیت‌های «پردازش مستقر در خارج» را تعیین می‌کند. ماده ۳۸ می‌گوید:

«ماده **38**.درخصوص پردازش داده‌های شخصی اتباع ایرانی، رعایت شرایط ذیل الزامی است:
الف:تنها در مراکز داده واقع در قلمرو حاکمیتی جمهوری اسلامی ایران یا مراکز داده خارجی مورد تایید مراجع صلاحیت‌دار ذخیره شوند.»

[81] آرتیکل ۱۹، «حق فراموش شدن»: یادآوری آزادی بیان (۲۰۱۶)، اینجا در دسترس است: https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf

این بخش از نقطه نظر آزادی بیان مشکل‌آفرین است. این قوانین «محلی‌سازی داده» در چند حیطه قضایی اعمال شده‌اند تا به بهانه محلی‌سازی دسترسی به رسانه‌های اجتماعی را محدود کنند. در روسیه از این قوانین برای محدود کردن دسترسی به توئیتر و فیس‌بوک استفاده می‌شود. باضافه، محلی‌سازی اجباری داده‌ها کار مقامات در دسترسی به ارتباطات خصوصی مخالفین و سایرین را راحت‌تر می‌سازد. این ماده در ضمن ناقض اصل عدم تبعیض است چرا که از داده‌های شخصی اتباع ایران صحبت می‌کند.[82] در ضمن معلوم نیست از چه روندی برای محلی‌سازی استفاده می‌شود چرا که بند ب از «گواهی مراجع صلاحیت‌دار ذی‌ربط» گفته بدون این‌که روشن کند صحبت از کدامست. این ماده در ادامه گفته داده‌های شخصی از طریق «شبکه‌های ارتباطی مورد اعتماد» به کشورهای خارجی منتقل خواهد شد و تعریفی ارائه نداده که معنی این در قانون چیست. گزارشگر ویژه آزادی بیان و اطلاعات سازمان دولت‌های قاره آمریکا مشکل این محلی‌سازی را اعلام کرده:

«محلی‌سازی اجباری داده‌ها می‌تواند ساز و کاری برای محدود کردن آزادی بیان به دلایل مختلف باشد. اول، محلی‌سازی اجباری واسطه‌های اینترنت باعث کاهش چشمگیر میزان عرضه خدمات و پلاتفرم‌هایی که مورد استفاده آزادانه کاربران قرار دارند می‌شود. مهم است اشاره کنیم که آزادی انتخاب دسترسی به خدمات و پلاتفرم‌ها حق کاربرانی است که از آزادی بیان خود استفاده می‌کنند و نمی‌تواند توسط دولت‌ها محدود شود مگر با نقض ماهیت ویژه اینترنت به عنوان فضایی آزاد، باز و غیرمرکزی. این فرصت انتخاب در بسیاری دولت‌ها ضروری است چرا که افراد در آن‌ها با دخالت خودسرانه دولت‌ها در حریم خصوصی‌شان مواجهند. در چنین مواردی، فرصت انتخاب یعنی فرصت استفاده بی‌مانع از آزادی بیان. به بیان دیگر، فقدان قوانین محلی مناسب یا سیاست‌های عمومی برای پاسداشت داده‌ها می‌تواند در صورتی که داده‌ها در کشور مشخصی قرار داشته باشند باعث ناامنی بیشتری در دسترسی به آن‌ها شود (نسبت به این که داده‌ها در چندین مکان مختلف باشند که باعث بهتر بودن وضعیت امنیتی می‌شود.)

... باضافه مقرر ساختن شرکت‌های ارائه دهنده اینترنت به ذخیره محلی داده می‌تواند مانعی برای ورود پلاتفرم‌ها و خدمات جدید به بازار باشد. این تاثیری منفی بر آزادی بیان کاربران می‌گذارد که شاهد کاهش دسترسی خود به منابع پژوهش، آموزش و ارتباطات خواهند بود. در واقع تبعیت از شروط محلی‌سازی داده پیچیده و پرهزینه است و به کاربران فردی یا ابتکارات جدید لطمه می‌زند چرا که می‌تواند آن‌ها را از امکان عاملیت در محیط‌های مختلف که برای ایجاد ارتباط بین‌المللی ضروری است محروم کند. آزادی بیان و دموکراسی جریان آزاد اطلاعات را شرط می‌گیرند و نیازمند پیشگیری از اقداماتی هستند که باعث ایجاد تشتت در اینترنت می‌شوند.

... از این جهت استفاده از حق آزادی بیان نیازمند شرایطی است که دسترسی کاربران به کثرت و تنوع رسانه‌ها را تشویق می‌کنند (و نه برعکس).» [83]

گزارشگر ویژه آزادی بیان و نظر در گزارش سال ۲۰۱۶ خود پیشنهاد داد که «بخصوص برای دولت‌ها حیاتی خواهد بود که از تصویب مقررات قانونی که عوامل دیجیتال را هدف می‌گیرد و آزادی بیان را محدود می‌کند خودداری کنند، از جمله (و نه فقط) موازین محلی‌سازی داده‌ها، مسئولیت‌تراشی برای اطراف میانجی و امنیت اینترنت).»[84]

در مقابل، سند «مقررات» شرطی برای ذخیره داده‌ها در کشورهای عضو اتحادیه اروپا مقرر نمی‌کند. این سند از دولت‌ها می‌خواهد مواد قانونی مربوط به صیانت از داده‌هاشان مشابه خود این سند باشد؛ داده‌های شخصی را

---

82 برای فرقی که لایحه بین شهروندان ایرانی و خارجی قائل می‌شود نگاه کنید به بخش ب ۲

83 دفتر گزارشگر ویژه آژادی بیان، کمیسیون حقوق بشر قاره آمریکا، آزادی بیان و اینترنت، ۲۰۱۳

84 دفتر گزارشگر ویژه در موضوع تشویق و پاسداشت حق آزادی نظر و بیان، آ/۷۱/۳۷۳، ۱۶ شهریور ۱۳۹۵

می‌توان به این شرط به کشور سوم منتقل کرد که سطح پاسداشت شخصیت‌های حقوقی که در این سند تضمین شده زیر سوال نرود. در دو بخش مربوط می‌خوانیم:

«ماده ۴۵: انتقال داده‌های شخصی به کشور سوم یا سازمان‌های بین‌المللی می‌تواند در شرایطی صورت بگیرد که کمیسیون تصمیم گرفته که کشور سوم، قلمرو یا یک یا چند بخش مشخص درون کشور سوم یا سازمان بین‌المللی مورد نظر سطح کافی پاسداشت را تضمین می‌کنند. چنین انتقالی نیازی به جواز مشخص نخواهد داشت.

ماده ۴۶: در فقدان تصمیم‌گیری کمیسیون در مورد دلایل کافی، کنترل‌گر یا پردازش‌گر می‌توانند داده‌های شخصی را به کشورهای سوم یا سازمان‌های بین‌المللی منتقل کنند اما فقط به این شرط‌که کنترل‌گر یا پردازش‌کننده ضمانت‌های لازم را ارائه کرده باشند و به این شرط که حقوق قابل اجرای فرد موضوع داده‌ها و جبران مافات‌های موثر حقوقی برای افراد موضوع داده در دسترس باشد.»

سایر کشورهای منطقه هم از همین رویکرد تبعیت کرده‌اند. در ترکیه، داده‌های شخصی در صورتی می‌تواند به خارج منتقل شود که ضمانت کافی در کشور خارجی که داده به آن منتقل می‌شود موجود باشد یا اداره مورد نظر چنین انتقالی را تایید کرده باشد (در صورت فقدان چنین ضمانتی.)[85] همین اصول در تونس هم برقرارند.[86]

۴. فقدان ایجاد توازن بین صیانت از داده‌ها و حق اطلاعات

حق دسترسی عمومی به اطلاعاتی که در اختیار نهادهای عمومی است از جنبه‌های بنیادین حق آزادی بیان است.[87] حق دسترسی به اطلاعات و صیانت از داده‌ها اغلب نقش مکمل دارند. تمرکز هر دوی این‌ها بر تضمین مسئولیت‌پذیری نهادهای قدرتمند نزد افراد در عصر اطلاعات است. میشل جنتوت، رئیس سابق «کمیسیون ملی فرانسه برای آزادی‌ها و اطلاعات» می‌گوید: «آزادی اطلاعات و صیانت از داده‌ها... دو شکل از ضمانت علیه دولت لویاتان هستند که هدفشان احیای توازن بین شهروند و دولت است.»

قانون بین‌المللی به روشنی مقرر داشته که حق دسترسی به اطلاعات در توازن با حق داشتن حریم خصوصی قرار بگیرد. مثل آزادی بیان، هرگونه محدودیتی را باید قانون تعیین کند و باید ضروری و متناسب باشد.[88]

شورای اروپا در قطع‌نامه‌ای در سال ۱۳۶۵ اعلام کرد که این دو حق «از یکدیگر متمایز نیستند که بخشی از سیاست کلی اطلاعات در جامعه هستند.»[89] کنوانسیون جدید ۱۰۸ شورای اروپا در بخش اضافه خود شامل ارجاع مشخص به دسترسی عمومی به اطلاعات می‌شود:

«با توجه به این‌که این کنوانسیون در اجرای قوانینی که این‌جا مطرح شده‌اند اصل دسترسی به اسناد رسمی را در نظر می‌گیرد.»

یادداشت توضیحی کنوانسیون ترمیم‌شده می‌گوید:

---

85 قانون ترکیه در زمینه صیانت از داده‌های شخصی، ماده ۹

86 قانون ارگانیک تونس ۲۰۰۴-۶۳ درباره صیانت از داده‌های شخصی، ۶ مرداد ۱۳۸۳، ماده ۵۱

87 کمیته حقوق بشر سازمان ملل، اظهار نظر عمومی شماره ۳۴

88 گزارش گزارشگر ویژه تشویق و پاسداشت حق آزادی نظر و بیان، فرانک لاروئه، A/۶۸/۳۶۲، ۱۳ شهریور ۱۳۹۲

89 پیشنهاد ۱۰۳۷ شورای اروپا در زمینه صیانت از داده‌ها و آزادی اطلاعات (۱۳۶۵)

«باضافه، کنوانسیون تاکید می‌کند که استفاده از حق صیانت بر داده‌ها، که حقی مطلق نیست، نبایست به عنوان وسیله‌ای عمومی برای جلوگیری از دسترسی عمومی به اسناد رسمی باشد.»

سند «مقررات» اتحادیه اروپا این اعلام رسمیت‌شناسی را گسترش می‌دهد. در ماده ۸۶ آن می‌خوانیم:

«داده‌های شخصی در اسناد رسمی تحت اختیار مقامات عمومی یا نهادهای عمومی یا نهادهای خصوصی مسئول اجرای وظیفه‌ای که در منفعت عموم است می‌توانند توسط آن مقام یا نهاد در تطبیق با قوانین اتحادیه اروپا یا دولت‌های عضو که مقام یا نهاد ذیل آن عمل می‌کند منتشر شوند تا بین دسترسی عمومی به اسناد رسمی با حق صیانت از داده‌های شخصی، چنان‌که در این سند آمده، هماهنگی ایجاد شود.»

بسیاری قوانین کشوری صیانت از داده‌ها در اروپا و سراسر دنیا به طور مشخص حق اطلاعات را به رسمیت می‌شناسند. در ایرلند، ماده ۴۴ قانون صیانت از داده‌های ۲۰۱۸ در اجرای سند «مقررات» می‌گوید:

«۱) برای مصارف ماده ۸۶، داده‌های شخصی که در اسناد آمده‌اند باید زمانی که تقاضای دسترسی به سندی مورد پذیرش قرار گرفته، منتشر شوند البته در تطبیق با قانون ۲۰۱۴ و در پی تقاضای آزادی اطلاعات.

۲) برای مصارف ماده ۸۶، داده‌های شخصی که درون اطلاعات زیست‌محیطی قرار دارند می‌توانند منتشر شوند به شرط این‌که انتشار این اطلاعات در انطباق با «مقررات دسترسی به اطلاعات درباره محیط زیست» باشد و در پی تقاضایی درون معنای سند «مقررات.»»

در آفریقای جنوبی، قانون «تشویق دسترسی به اطلاعات» مقرر می‌دارد که انتشار اطلاعات زمانی منع شود که «منجر به انتشار غیرمنطقی اطلاعات شخصی در مورد یکی از طرفین سوم از جمله افراد متوفی خواهد بود.» اما انتشار اطلاعات در صورت زیر ممکن است:

«اطلاعاتی که در مورد فردی است که مقام نهادی عمومی هست یا بوده و مربوط است به موقعیت یا کارکردهای فرد در مواردی مثل موارد زیر(شامل این‌ها است اما می‌تواند غیر از این هم باشد):

یک) این‌که فرد مقام نهادی دولتی هست یا بوده:
دو) عنوان، نشانی کار، شماره تلفن کار و سایر مشخصات فرد؛
سه) طبقه‌بندی، میزان دستمزد یا پاداش و مسئولیت‌های موقعیت فرد یا خدماتی که انجام داده؛ و
چهار) نام فرد در سندی که فرد در جریان اشتغال خود تهیه کرده.[90]»

باید کسب اطمینان شود که اسناد عمومی و سایر اطلاعات مربوط به عملکرد دولت و یا در جهت منفعت عموم، عمومی باقی بی‌مانند و به نام صیانت از داده‌ها با محدودیت غیرضروری مواجه نمی‌شوند. این اسناد می‌توانند در امر تضمین مسئولیت‌پذیری نقشی حیاتی بازی کنند از جمله برای تهیه اطلاعات عمومی، اسناد عمومی صاحبین شرکت‌ها، اطلاعات موجود در رابطه با جلسه مقامات شرکت با مقامات عمومی برای تاثیرگذاری بر تصمیم‌های آن‌ها، دریافت‌کننده یارانه‌ها و غیره.

90 قانون تشویق دسترسی به اطلاعات، ۳۴

بدین‌سان در ضمن ضروری است که لایحه، منفت عمومی را در مواردی که تقاضایی برای دسترسی به اسنادی که شامل اطلاعات شخصی هر نوع افراد خصوصی است مطرح می‌شود کاملا به رسمیت بشناسد.

این تقاضاها باید مورد بررسی قرار بگیرند تا معلوم شود آیا امکان جدی آسیب بلافاصله یا متعاقب مطرح هست یا نه. باید مساله را از زاویه منفعت عمومی بررسی کرد و در مورد هر تقاضا تصمیم گرفته شود که اطلاعات ارائه می‌شود یا خیر و این کار باید با در نظر گرفتن منافع مرتبط که باید مورد پاسداشت قرار بگیرند انجام شود و با بررسی هدفِ تقاضای مطرح شده.

شماری از تصمیمات در مورد چگونگی ایجاد توازن بین دو حقوق در چارچوب دسترسی به اطلاعات[91] گرفته شده‌اند. کمیسیونر اطلاعات بریتانیا اشاره کرده که:

«منفعت عمومی می‌تواند گستره وسیعی از ارزش‌ها و اصول مربوط به نفع عمومی یا آن‌چه در جهت بهترین منافع جامعه است پوشش دهد. بدین‌سان مثلا امر شفافیت و مسئولیت‌پذیری در جهت منفعت عمومی است و همچنین امر تشویق درک عمومی و امر پاسداشت روندهای دموکراتیک. از دیگر مسائلی که مربوط به منفعت عمومی می‌شوند: تصمیم‌گیری ماهرانه توسط نهادهای عمومی، دفاع از موازین راستین بودن روندها، تضمین عدالت و برخورد منصفانه با همگان، تامین بهترین استفاده از منابع عمومی و تضمین رقابت منصفانه تجاری در اقتصادهای مخلوط. این فهرست، کامل نیست؛ منفعت عموم می‌تواند اشکال مختلف بگیرد.»

اسناد تفسیری در مورد نسخه ترمیم‌شده کنوانسیون جدید ۱۰۸ شورای اروپا توضیح می‌دهد که کنوانسیون تاکید می‌کند که حق صیانت از داده‌ها که مطلق نیست بخصوص نباید به عنوان وسیله‌ای عمومی برای جلوگیری از دسترسی عموم به اسناد رسمی مورد استفاده قرار بگیرد.[92]

متاسفانه، لایحه در زمینه در نظر گرفتن و ایجاد توازن بین حق صیانت از داده‌ها و حق دسترسی به اطلاعات کوتاهی کرده است.

در ایران، حق اطلاعات توسط قانون انتشار و دسترسی آزاد به اطلاعات ممکن شده است. طبق ماده ۱۴ اطلاعات مربوط به حریم خصوصی یا داده‌های شخصی را می‌توان در صورتی که مضر به منافع فرد باشد منتشر نکرد. استثناهای وضع‌شده مطلق محسوب نمی‌شوند.[93]

هرچند باید متذکر شد که «قانون انتشار و دسترسی آزاد به اطلاعات» در ایجاد توازن میان حق داشتن حریم خصوصی و حق دسترسی به اطلاعات همانطور که بالاتر هم اشاره شد کاستی دارد. طبق ماده ۹ آیین‌نامه:

---

91 دادگاه حقوق بشر قاره آمریکا، پرونده کلاد رِیِس و سایرین علیه شیلی، حکم روز ۲۸ شهریور ۱۳۸۵.

92 گزارش توضیحی به پروتکل در ترمیم «کنوانسیون حفاظت از افراد در رابطه با پردازش خودکار داده‌های شخصی، ۱۸ مهر ۱۳۹۷، بند ۱۱

93 این تنها بدین معنی است که استثنا ها باید دارای حیطه ای محدود باشند، به روشنی و به طور مشخص تعریف شوند و آزمون اکید اضرار و منفعت عمومی در موردشان به کار رود. باید کسب اطمینان شود که اسناد ثبت شده عمومی و سایر اطلاعات مربوط به عملیات دولت یا اطلاعاتی که در جهت منفعت عموم هستند و عمومی باقی می‌مانند و به نام صیانت از داده‌ها محدودیت‌های غیرضروری برآنها اعمال نمیشود.

«مؤسسات مشمول قانون حق انتشار یا ارایه اطلاعات مربوط به حریم خصوصی و سایر موارد منع شده در قانون را ندارند، مگر در مواردی که قوانین و مقررات، انتشار یا ارائه آنها را الزامی اعلام کرده باشد.»[94]

تعریفی که در این‌جا از «اطلاعات مربوط به حریم خصوصی» ارائه شده روشن نمی‌کند که طبق بهترین تجربیات موجود و بر اساس منفعت عموم این اطلاعات شخصی نباید شامل نام مقامات یا فعالیت‌های رسمی‌شان باشد. قانون انتشار و دسترسی آزاد به اطلاعات در حال حاضر پاسداشت حریم خصوصی را شامل اطلاعاتی می‌داند که انتشارشان برای منفعت عموم ضروری است. اما مثلا در قانون حق اطلاعات یمن (۲۰۱۲) اطلاعات شخصی را زمانی می‌توان منتشر کرد که «مرتبط با وظیفه یا کارکرد مقام دولتی فرد باشد.»[95]

در مقابل، لایحه حفاظت و صیانت از داده‌های شخصی هیچ ارجاعی به «قانون انتشار و دسترسی آزاد به اطلاعات» نمی‌دهد. ماده ۱۲ این لایحه چندین شرط را فهرست می‌کند که تحت آن‌ها پردازش داده‌های شخصی درون چارچوب قوانین مربوطه بدون اجازه موضوع داده مجاز است. به طور مشخص به پرونده‌هایی اشاره می‌شود که این کار برای پاسداشت شهرت فرد، جان یا مال او و شهرت و حیات فردی دیگر یا پیشگیری از اضرار اقتصادی برای آن‌ها ضروری است. استثنایی برای تضمین حق اطلاعات و در نظر گرفتن منفعت عموم در انتشار اطلاعات وضع نشده. این ماده به نظر باعث تصادم قانون با «قانون انتشار و دسترسی آزاد به اطلاعات» می‌شود.

لایحه قانون صیانت از داده‌ها باید به عنوان یکی از اولین قدم‌ها ترمیم شود و شامل استثنای صریحی برای اطلاعات شخصی مربوط به فعالیت‌های عمومی مقامات عمومی یا سایر افرادی که تحت اختیار دولتی عمل می‌کنند یا پول دولتی خرج می‌کنند شود. چنین ترمیمی حق اطلاعات که در «قانون انتشار و دسترسی آزاد به اطلاعات» آمده منعکس می‌کند.

از این لحاظ، لایحه این خطر را دارد که قدمی رو به عقب به حساب بیاید و حقوقی را که «قانون انتشار و دسترسی به اطلاعات» داده و در قانون اساسی ضمانت شده‌اند زیر سوال ببرد.

پیشنهادها

— بخش «مقدمه» باید از نو نوشته شود تا حق آزادی بیان را که در قانون اساسی آمده نیز یادآوری کند و به منشور حقوق شهروندی اشاره کند که چارچوب ضمانت حق آزادی بیان، حق دسترسی به اطلاعات، حق داشتن حریم خصوصی و حق صیانت از داده‌های خصوصی را فراهم می‌کند. لایحه باید مسئولیت‌های ایران به عنوان دولت عضو کنوانسیون حقوق مدنی و سیاسی را در نظر بگیرد، بخصوص اصل ۱۷ (حق داشتن حریم خصوصی) و ۱۹ (حق آزادی بیان.)

— اصل ۱۲ باید مورد بازبینی قرار بگیرد تا شامل استثنای پردازشی شود که هدفش مخابره اطلاعات به عموم، افکار یا نظراتی در جهت منفعت عمومی است، از جمله برای مصارف روزنامه‌نگارانه و مصارف بیان دانشگاهی، هنرمندانه یا ادبی. ماده ۱۲ در ضمن باید از طریق شفافیت‌سازی در مورد هدف پیش‌گیری از خطرهای موجود برای نظم، امنیت یا ایمنی عمومی (یا پاسخ به آن‌ها) شامل ضمانت این شود که رویه قضایی هنگام دسترسی به داده‌های بدون رضایت دنبال می‌شود. چنین شرایطی را می‌توان در اصل ۲ تعریف کرد که «تعاریف» را آورده.

[94] آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات
[95] قانون ۱۳ سال ۲۰۱۲ درباره حق دسترسی به اطلاعات. بند ۲۵ (ب)

هدف این است که مقامات امکان نقض حقوق افراد بخصوص در تلاش برای سرکوب و تعقیب مدافعین حقوق بشر، اقلیت‌ها، روزنامه‌نگاران، وبلاگ‌نویس‌ها و فعالین را نداشته باشند.

— لایحه در ضمن باید تضمین کند که روزنامه‌نگاران و سایر کسانی که راجع به منفعت عمومی فعالیت ارتباطی می‌کنند از جمله سازمان‌های غیردولتی که اطلاعاتی در جهت منفعت عمومی منتشر می‌کنند در مقابل اجبار به انتشار منابع اطلاعات خود مورد حفاظت هستند.

— تضمین شود که تمام قوانین مربوط به حذف اطلاعات عمومی در توازن با آزادی بیان و منفعت عمومی در دسترسی به اطلاعات و بایگانی تاریخی هستند. این‌کار از طریق گنجاندن آزمون هفت بخشی سازمان «آرتیکل ۱۹» در رابطه با آن‌چه «حق فراموش شدن» نامیده می‌شود در اصل ۹ ممکن است.

— حذف این شرط که تمام داده‌های شخصی باید تحت محلی‌سازی داده‌ها قرار بگیرند. جایگزینی آن با تضمین کافی بودن پاسداشت داده‌ها در حیطه‌های قضایی خارجی.

— ترمیم اصل ۱۲ و شامل کردن استثنایی صریح برای اطلاعات شخصی مربوط به فعالیت‌های عمومی مقامات دولتی یا سایرینی که تحت اختیار عمومی عمل می‌کنند یا پول عمومی خرج می‌کنند برای انعکاس حق اطلاعات که در قانون اساسی آمده و منفعت عمومی در دستیابی به اطلاعات.

— لایحه باید به طور مشخص مواد مربوط به منفعت عمومی در «قانون انتشار و دسترسی آزاد به اطلاعات» در مورد اطلاعاتی که در اختیار نهادهای عمومی هستند در نظر بگیرد و کسب اطمینان کند که منفت عمومی در تمام تقاضاها در نظر گرفته می‌شود.

د. محدود کردن حقوق دسترسی

حق افراد برای دسترسی به اطلاعات شخصی راجع به خودشان که در اختیار طرفین سوم از جمله نهادهای عمومی و شرکت‌های خصوصی قرار دارد (که معمولا «حق دسترسی موضوع داده» یا «دسترسی فرد مورد نظر» نامیده می‌شود) از حقوق بنیادین محسوب می‌شود که تحت قانون بین‌المللی به رسمیت شناخته شده. کمیته حقوق بشر سازمان ملل در سند «اظهار نظر عمومی شماره ۱۶» به این اشاره می‌کند که این حق برای تضمین احترام به حق حریم خصوصی ضروری است:

«هر فرد برای این‌که از موثرترین پاسداشت زندگی خصوصی‌اش برخوردار باشد باید حق داشته باشد به شکلی روشن بفهمد که آیا داده‌های شخصی‌اش در پرونده‌های خودکار داده‌ها ذخیره شده‌اند و اگر آری، کدام داده‌ها و به چه دلایلی. هر فرد باید در ضمن بتواند بفهمد کدام نهادهای عمومی یا افراد و نهادهای خصوصی پرونده‌هایشان را تحت سیطره دارند یا می‌توانند داشته باشند. اگر این پرونده‌ها شامل داده‌های شخصی غیرصحیح باشد یا در روندی مغایر با قانون جمع‌آوری یا پردازش شده باشد، تمام افراد باید حق تقاضای تصحیح یا حذف آن‌ها را داشته باشند.»[96]

[96] اظهار نظر عمومی شماره ۱۶، همان‌جا در ۱۰

این حق وسیعا در قانون بین‌المللی و همچنین در توافق‌های عمده منطقه‌ای درباره صیانت از داده‌ها گنجانده شده. دادگاه حقوق بشر اروپا حق دسترسی را «از منافع حیاتی مورد پاسداشت کنوانسیون»[97] خوانده. در سند «مقررات» تمام افراد حق قوی دسترسی دارند. چنان‌که در اصول تکمیلی آمده:

«فرد موضوع داده باید حق دسترسی به داده‌های شخصی که در مورد او جمع‌آوری شده باشند داشته باشد و استفاده از این حق باید قابل دسترسی آسان و مکرر (در حد منطقی) باشد تا او بتواند از قانونی بودن کار پردازش اطلاع حاصل کند و آن‌را راستی‌آزمایی کند. این شامل حق افراد موضوع داده برای دسترسی به داده‌های موجود در سلامت‌شان هم می‌شود مثلا داده‌های موجود در اسناد پزشکی که شامل اطلاعاتی همچون تشخیص بیماری، نتایج آزمایش‌ها، بررسی توسط پزشک‌های مراقب و هرگونه درمان یا دخالت پزشکی است. تمام افراد موضوع داده باید بدین‌سان حق داشته باشند بدانند چه مراسلاتی در رابطه با پردازش داده‌های شخصی آن‌ها موجود است و به این مراسلات دسترسی داشته باشند، حتی‌الامکان برای طول دوره‌ای که این داده‌های شخصی پردازش می‌شوند. آن‌ها همچنان باید بتوانند از دریافت‌کنندگان این داده‌های شخصی، منطق هرگونه پردازش خودکار داده‌های شخصی و عواقب این پردازش (حداقل زمانی که بر اساس انتخاب نمونه‌وار انجام می‌شود) باخبر شوند. کنترل‌گر باید حتی‌الامکان بتواند دسترسی از راه دور به سامانه امنی را فراهم کند که به موضوع داده دسترسی مستقیم به داده‌هایش را می‌دهد. این حق نباید تاثیری منفی بر حقوق یا آزادی‌های دیگران از جمله رموز تجاری یا دارایی‌های فکری و بخصوص کپی‌رایت پشتیبانِ نرم‌افزارها بگذارد. اما نتیجه این ملاحظات نباید به خودداری از ارائه تمام اطلاعات به فرد موضوع داده‌ها منجر شود. در مواردی که کنترل‌گر مقادیر وسیعی از اطلاعات را در مورد فرد موضوع داده پردازش می‌کند، این کنترل‌گر باید بتواند تقاضا کند که این فرد پیش از ارائه اطلاعات مشخص کند تقاضایش مربوط به کدام اطلاعات یا فعالیت‌های پردازشی می‌شود.»[98]

منشور شهروندی[99] نیز در ماده ۳۱ خود می‌نویسد:

«حق شهروندان است که به اطلاعات شخصی خود که توسط اشخاص و مؤسسات ارائه‌دهنده خدمات عمومی جمع‌آوری و نگهداری می‌شود دسترسی داشته باشند و در صورت مشاهده اشتباه، خواستار اصلاح این اطلاعات گردند. اطلاعات خصوصی مربوط به افراد را نمی‌توان در اختیار دیگران قرار داد، مگر به‌موجب قانون یا با رضایت خود افراد.»[100]

قانون انتشار و دسترسی آزاد به اطلاعات حقوق دسترسی به اطلاعات شخصی را تجویز می‌کند. تقاضای اینگونه اطلاعات مشابه سایر انواع اطلاعات است که در این قانون آمده. اما تحت ماده ۶ قانون تنها فردی که اطلاعاتش مورد درخواست است یا نماینده حقوقی او می‌توانند چنین اطلاعات شخصی‌ای را تقاضا کنند.

---

97 گاسکین علیه بریتانیا، ۱۶ تیر ۱۳۶۸، ۴۹، سری آ شماره ۱۶۰؛ ام جی علیه بریتانیا، شماره ۳۹۳۹۳/۹۸، سه؛ گوئرا و دیگران علیه ایتالیا، ۲ مهر ۱۳۸۱؛ اودیوره علیه فرانسه، شماره ۴۲۳۲۶/۹۸، ۴۱-۴۷، دادگاه حقوق بشر اروپا، ۲۰۰۳ / ۳۰ بهمن ۱۳۷۶

98 سند «مقررات» اتحادیه اروپا،، اصل تکمیلی ۶۳

99 آقای حسن روحانی منشور حقوق شهروندی را در سال ۱۳۹۵ رو نمایی کرد. این منشور که از لحاظ حقوقی غیر الزامی محسوب میشود شامل ۱۲۰ ماده است که از تعهدات بین‌الملل موجود پیرامون حقوق مدنی، سیاسی، اجتماعی و اقتصادی از دید حق آزادی بیان، حریم خصوصی، محیط‌زیست و کار تشکیل میشود. منتقدانی همچون خانم شیرین عبادی این منشور را زاید می‌دانند، ولی همانطور که در زیر هم گفت شده در این منشور مواد جدیدی پیرامون حق دسترسی به اطلاعات وجود دارد که در قانون اساسی نیست .در سال ۱۳۹۶ دولت آقای روحانی لایحه‌هایی را به مجلس پیشنهاد داده که برخی از بخش‌های این منشور الزامی شوند.

100 متن کامل منشور : **http://citizensrights.ir/home/document/4783**

طبق ماده ۱۵ آیین‌نامه ماده ۸ قانون انتشار و دسترسی آزاد به اطلاعات، سازمان فن‌آوری اطلاعات موظف است ضرف شش ماه و در همکاری با شرکت پست سامانه‌ای اجرایی از پرونده‌های شهروندان را برای دسترسی راه‌اندازه کند. [آیین‌نامه اجرایی اصل ۸ قانون انتشار و دسترسی آزاد به اطلاعات، ۳۰ شهریور ۱۳۹۴]

در مقایسه می‌بینیم که لایحه ماده محدودی دارد که کاربست و محدودیت‌های آن عموما ناروشن هستند. ماده ۱۰ لایحه می‌گوید «در شرایط ذیل،شخص موضوع داده حق دارد به داده‌های شخصی خود به‌منظور پردازش آن‌ها دسترسی یابد:

الف)شامل اطلاعات طبقه‌بندی‌شده عمومی یا داده‌های شخصی دیگران نشود؛
ب) استنادذپذیری داده‌ها مخدوش نشود.»

این ماده تعریف نمی‌کند که «اطلاعات طبقه‌بندی‌شده عمومی» به چه معنی است.

باضافه ماده ۲۶ پردازش‌گر را موظف می‌دارد اطلاعاتی در مورد اهداف، منابع، وظایف و موارد استفاده اطلاعات ارائه نکند اما مشخصا به خود داده‌ها اشاره نمی‌کند.

نکته چشمگیر این‌جا است که لایحه حق اصلاح را صراحتا اعطا نکرده. در «اظهار نظر عمومی شماره ۱۶» می‌خوانیم که:

«اگر چنین پرونده‌هایی حاوی داده‌های شخصی نادرست باشند یا اطلاعاتی که مغایر با مواد قانونی، جمع‌آوری یا پردازش شده باشند تمام افراد حق دارند تقاضای تصحیح یا حذف این اطلاعات را کنند.»[101]

تحت سند «مقررات» اتحادیه اروپا، کنترل‌گر در ضمن باید «از تمام اقدامات منطقی برای راستی‌آزمایی هویت فرد موضوع داده که خواهان دسترسی است استفاده کند بخصوص در چارچوب خدمات اینترنتی و شناسه‌های اینترنتی. کنترل‌گر نباید داده‌های شخصی را تنها به جهت این‌که قادر به واکنش به تقاضاهای احتمالی باشد حفظ کند.»[102] این سند در ضمن «حق اصلاح» را مقرر می‌دارد و این‌گونه تعریف می‌کند: «حق این‌که کنترل‌گر بدون تاخیر دست به اصلاح داده‌های شخصی غیردقیق راجع به او بزند. با توجه به اهداف پردازش، فرد موضوع داده حق دارد خواهان تکمیل داده‌های شخصی غیرکامل شود از جمله از طریق ارائه اظهارات تکمیلی.»[103]

پیشنهادات:

— ماده ۱۰ شفاف شود تا کسب اطمینان شود که افراد دسترسی کامل و آزادانه به اطلاعات شخصی‌شان که در اختیار طرفین سوم است دارند مگر در موارد محدودی که قانون بین‌المللی مجاز ساخته که مهم‌ترینش مواردی است که در«اظهار نظر عمومی شماره ۱۶» آمده. باید تعریف شود که «اطلاعات طبقه‌بندی‌شده عمومی» که ماده ۱۰ از آن صحبت می‌کند به چه معنی است.

— به فرد موضوع داده حق اصلاح اعطا شود.

---

101 اظهار نظر عمومی شماره ۱۶، همان‌جا در ۱۰

102 سند «مقررات» اتحادیه اروپا، اصل اضافه ۶۴

103 سند «مقررات» اتحادیه اروپا، اصل اضافه ۱۶

۵. استقلال کمیسیون صیانت از داده‌های شخصی و سایر نهادهای نظارتی

سازمان «آرتیکل ۱۹» به شدت نگران استقلال نهادی است که مسئول نظارت بر کاربست لایحه است. این جنبه‌ای حیاتی از لایحه است چرا که ضمانت استقلال نهادهای کشوری ناظر بر صیانت از داده‌ها قرار است موثر بودن و قابل اتکا بودن کار نظارت بر تبعیت از مفاد قانونی مربوط به صیانت از داده‌ها را تضمین کند. در نتیجه نهادهای نظارتی هنگام عمل به وظایف‌شان باید به صورت عینی و بی‌طرف و بدون نفوذ بیرونی (از جمله نفوذ مستقیم یا غیرمستقیم دولت) عمل کنند.

۱. ساختار و اختیارات

لایحه ساختار پیچیده‌ای از نهادها را تعیین می‌کند که مسئول اعمال قوانین مربوط به صیانت از داده‌ها هستند. این پنج نهاد از این قرارند: کمیسیون صیانت از داده‌های شخصی، هیات نظارت، دبیرخانه کمیسیون، کارگروه‌های تخصصی صیانت از داده‌های شخصی و ناظر ویژه.

وظیفه کمیسیون نظارت بر این لایحه قانونی تعیین شده است. کمیسیون متشکل است از وزیر ارتباطات به عنوان رئیس آن باضافه اعضای زیر: وزیر اطلاعات، وزیر کشور، وزیر دادگستری، وزیر فرهنگ و ارشاد اسلامی، وزیر اقتصاد و امور دارایی، دبیر شورای عالی و رئیس مرکز ملی فضای مجازی، معاون پیشگیری از وقوع جرایم قوه قضائیه، رئیس کمیسیون اصل نود مجلس شورای اسلامی، دادستان کل کشور و دبیر شورای اجرایی فن‌آوری اطلاعات به عنوان دبیر کمیسیون.

اختیارات کمیسیون در مواد ۴۱ و ۴۲ تعیین شده‌اند. به کمیسیون اختیار داده شده تا ناظر بر کارگروه‌های تخصصی باشد که آن‌ها نیز مسئول نظارت بر قانون هستند و این وظیفه عمومی‌تر که نهادهای مسئول اجرا را هماهنگ کند. کارگروه‌ها در ضمن می‌بایست مسائل نظارتی را تعیین کنند.

هیات نظارت بر این نظارت می‌کند که وظایف نظارتی کارگروه‌های تخصصی چطور عملی می‌شوند و شکایت طرفین ذینفع در امر پاسداشت داده‌های شخصی را دریافت می‌کند و در موردشان پیگیری می‌کند. این به روشنی کارکردی است که باید برای خدمه کمیسیون باشد و نه نهاد نظارتی.

ناظر ویژه قرار است طبق ماده ۵۴ برای پردازش داده‌های شخصی حیاتی و حساس، پردازش کلان داده‌های شخصی، بررسی لطمات مکرر و جدی به پردازش داده‌های شخصی و سایر وظایفی که هیات نظارت تعیین می‌کند تعیین شود.

طبق لایحه کنونی، تمامی اختیارات و وظایف مربوط به اجرای قانون را کمیسیون تعیین می‌کند.

معلوم نیست چرا باید چنین ساختار پیچیده‌ای برپا شود در حالی که در سایر کشورها یک کمیسیون واحد هست که تمام فعالیت‌ها ذیل آن و توسط دبیرخانه و در بعضی موارد هیاتی نظارتی که کارش بررسی فعالیت‌های آن‌ها هست انجام می‌شود.

۲. مشکل استقلال در نهادها

در رابطه با کمیسیون، این‌طور که تعریف شده، دو مساله جای نگرانی باقی می‌گذارد. اول این‌که ترکیب آن صرفا از وزرای دولت و سایر نمایندگان نهادهای دولتی امنیتی تشکیل شده. این ترکیب به روشنی فاقد نمایندگانی است که زمینه تخصصی‌شان مربوط به حقوق بشر یا حقوق مصرف‌کنندگان می‌شود. دوم این‌که کمیسیون مستقر در وزارت ارتباطات است. این نیز جنبه دیگری از نگرانی بزرگ ما راجع به استقلال این نهاد نظارتی است.

در ضمن باید اشاره کرد که لایحه مقرر می‌دارد که هیات نظارتی و کمیسیون اعضایی مشترک مثل وزیر دادگستری داشته باشند. این جنبه تهدیدی جدی به استقلال نهادهای نظارتی است.

قانون بین‌المللی به روشنی مقرر داشته که نهاد نظارتی می‌بایست از نظر کارکردی و اجرایی مستقل از تمامی نهادهای عمومی باشد. خطوط عمومی ۱۳۶۹ برای تنظیم پرونده‌های داده‌های شخصی رایانه‌ای می‌گوید:

«قانون هر کشوری باید نهادی را تعیین کند که در انطباق با نظام قانونی داخلی آن کشور مسئول نظارت بر تبعیت از اصولی که در بالا آمده‌اند خواهد بود. این نهاد باید بی‌طرفی، استقلال نسبت به افراد یا نهادهای مسئول پردازش و برقرار ساختن داده و مهارت فنی را تضمین کند.»[104]

مورد اخیرتر قطع‌نامه مجمع عمومی درباره «حق داشتن حریم خصوصی در عصر دیجیتال» در ۲۹ آذر ۱۳۹۵ است که از دولت‌ها می‌خواهد چنین کنند

«برقراری یا حفظ ساز و کارهای مستقل، موثر، با منابع کافی و بی‌طرفِ قضایی، اداری و /یا پارلمانی برای نظارت داخلی که قادر به تضمین شفافیت در زمان مناسب و مسئولیت‌پذیری برای نظارت دولتی بر ارتباطات، ضبط آن‌ها و جمع‌آوری داده‌های شخصی باشد»[105].

سند «مقررات» اتحادیه اروپا هر دولت عضو را مقرر می‌دارد نهادهای نظارتی بر پا کند که «با استقلال کامل دست به اجرای وظایف خود می‌زند و اختیاراتش را در انطباق با این سند انجام می‌دهد.»[106] این سند در ضمن دولت‌های عضو را مقرر می‌دارد که «هر یک از اعضای نهادهای نظارتی در روندی شفاف منصوب شوند و توسط: مجلس؛ دولت‌شان؛ رئیس دولت‌شان؛ یا نهادی مستقل که مسئولیتش را از قانون دولت عضو می‌گیرد.»[107]

در یکی از پرونده‌های اخیر، دادگاه اتحادیه اروپا اشاره کرد که «مقامات نظارتی که وظیفه‌شان نظارت در قلمروی دولت‌های عضو خودشان بر کاربست مواد قانونی مورد اتخاذ دولت‌هایی است که در سند فرمان آمده‌اند می‌بایست از استقلال کامل در اجرای کارکردهایی که بهشان سپرده شده برخوردار باشند.»[108] دادگاه در ضمن گفت:

«هدف از ضمانت استقلال مقامات نظارتی کشوری تضمین موثر بودن و اتکاپذیری نظارت بر تبعیت از مفاد قانونی

---

[104] رهنمودهای نگهداری از داده‌های شخصی در کامپیوترها، قطع‌نامه مجمع عمومی سازمان ملل ۴۵/۹۵، ۲۳ آذر ۱۳۶۹ ، بند هشت

[105] حق داشتن حریم خصوصی در عصر دیجیتال، قطع‌نامه مجمع عمومی ۷۱/۱۹۹، ۲۹ آذر ۱۳۹۵

[106] سند «مقررات» اتحادیه اروپا، ماده ۵۲ (۱)

[107] سند «مقررات» اتحادیه اروپا، ماده ۵۳ (۱)

[108] پرونده سی-۱۶/۲۱۰، **Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Wirtschaftsakademie case)**، ۱۵ خرداد ۱۳۹۷، صفحه ۶۸

مربوط به پاسداشت افراد در رابطه با پردازش داده‌های شخصی است و باید در پرتوی این هدف مورد تفسیر قرار بگیرد. این ضمانت مقرر شده تا پاسداشت افراد و نهادهایی که از تصمیمات این مقامات تاثیر می‌پذیرند تقویت کند. برپایی نهادهای نظارتی مستقل در دولت‌های عضو بدین‌سان، چنان‌که در ماده تکمیلی ۶۲ در مقدمه سند فرمان ۴۶/۹۵ آمده جزئی ضروری از پاسداشت افراد در رابطه با پردازش داده‌های شخصی است.»[109]

به همین سان، کنوانسیون ۱۰۸ جدید شورای اروپا می‌گوید: «مقامات نظارتی باید در اجرای وظایف خود و استفاده از اختیارات‌شان با استقلال و بی‌طرفی کامل عمل کنند و در این راه نمی‌بایست دنبال دستورالعمل باشند و یا آن‌را بپذیرند»[110] و این‌که این نهادها «باید به تقاضاها و شکایت‌هایی بپردازند که افراد موضوع داده در رابطه با حقوق‌شان در زمینه صیانت از داده‌ها تسلیم کرده‌اند و باید به افراد موضوع داده در مورد روند پیشرفت کار توضیح دهند.» [111] اعمال موثر قوانین صیانت از داده‌ها توسط نهادهای نظارتی مستقل در طرفین قرارداد از موارد محوری اعمال عملی کنوانسیون ۱۰۸ در طی روند جدیدسازی آن است. کنوانسیون جدید از همین رو تاکید می‌کند که نهادهای نظارتی باید اختیارات و کارکردهای موثر داشته باشند و هنگام عمل به ماموریت خود از استقلال حقیقی بهره‌ور باشند.[112]

نظامی که در ایران پیشنهاد شده در ضمن استقلال کم‌تری از خیلی از همسایگان خود در منطقه دارد. مثلا «اداره صیانت از داده‌های بحرین» مقرر شده شکایت‌های فردی درباره نقض قانون صیانت از داده‌ها را دریافت کند، آن‌ها را بررسی کند و در مورد جدی بودن‌شان تصمیم بگیرد.[113] حق تقاضای تجدید نظر هم این‌گونه معرفی شده که نهادی کمیسیونی (که نامش هست «کمیته تجدیدنظر») برپا شده که به شکل کمیته‌ای قضایی است و قادر به بررسی شکایت‌های دریافتی خواهد بود.[114]
در الجزایر، «اداره صیانت از داده‌ها» از اعضایی تشکیل می‌شود که رئیس‌جمهور، قوه قضائیه، مجلس، کمیسیون ملی حقوق بشر و همچنین نمایندگان وزارتخانه‌های دفاع، امور خارجه، کشور، دادگستری، ارتباطات، بهداشت و کار انتخاب می‌کنند.[115] در تونس، «قانون ارگانیک صیانت از داده‌های شخصی» نهادی به نام «موسسه ملی صیانت از داده‌های شخصی» ایجاد کرده که نهاد قانونی خودمختاری است و بودجه مستقلی دارد که وزارت حقوق بشر برپا کرده.[116]

پیشنهادها

— ساده‌سازی ساختار نهادهای نظارتی برای کسب اطمینان از استقلال کمیسیون. این نهاد باید شکل نهاد نظارتی مستقلی را به خود بگیرد که هدفش صیانت از داده‌های شخصی است و از نظر سیاسی، اداری و مالی مستقل از هرگونه اداره دولتی است و منابع کافی برای انجام فعالیت‌هایش در اختیار دارد و اعضایش را مجلس، قوه قضائیه و دولت انتخاب می‌کنند و در ضمن شامل بعضی اعضای بخش خصوصی هم می‌شود.

---

109 پرونده سی-۱۴/۳۶۲، ماکسیمیلیان شرمز علیه کمیسیون صیانت از داده‌ها، ۱۴ مهر ۱۳۹۴، ص ۴۱

110 شورای اروپا، کنوانسیون جدید برای حفاظت از افراد در رابطه با پردازش داده‌های شخصی، در تصحیح پروتکل «کنوانسیون حفاظت از افراد در رابطه با پردازش داده‌های شخصی، ماده ۱۵ (۵)

111 ماده ۱۵ (۴)

112 دفترچه قانون صیانت از داده‌های اروپا، نسخه ۲۰۱۸

https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

113 قانون شماره ۳۰ بحرین برای سال ۲۰۱۸ که «قانون صیانت از داده‌های شخصی» را صادر کرده است، ماده ۳ ۰

114 قانون شماره ۳۰ بحرین، ماده ۳۴

115 قانون الجزایر درباره پاسداشت افراد فیزیکی برای پردازش داده‌های شخصی، ۲۰ خرداد ۱۳۹۷، ماده ۲۳

116 قانون ارگانیک تونس ۲۰۰۴-۶۳ درباره صیانت از داده‌های شخصی، ۶ مرداد ۱۳۸۳، ماده ۷۵

— تضمین شود که رئیس کمیسیون هیچ سمت دیگری ندارد، بخصوص سمت‌های سیاسی و دولتی.

و. فقدان جبران مافات مناسب

از دیگر مشکلات چشمگیر این است که قانون فاقد راه‌های قابل اعمال جبران مافات برای افرادی است که حقوق داشتن حریم خصوصی‌شان مورد تجاوز قرار گرفته.

ماده ۷۲ لایحه از هفت «ضمانت اجراهای انتظامی قابل تصویب در کمیسیون و به پیشنهاد کارگروه‌های تخصصی» صحبت میکند. از جمله: مجازات مالی، ممنوعیت از فعالیت یا خدمت در یک یا چند حرفه برای دوره‌ای مشخص، ممنوعیت از فعالیت یا خدمت در تمام یا بعضی نهادهای دولتی یا شرکت‌ها برای دوره‌ای مشخص، کاهش دوران جواز.

ماده ۵۳ که در مورد وظایف هیات نظارت است می‌گوید این نهاد کار «دریافت ... شکایات ذی‌نفعان صیانت از داده‌های شخصی» را بر عهده دارد و با تعریفی خیلی کلی می‌گوید به آن‌ها «رسیدگی» می‌کند.

لایحه هیچ راه جبران مافاتی برای افرادی که می‌خواهند علیه این‌گونه تصمیمات نزد نهادهای عالی‌تر یا قضایی شکایت کنند در نظر نگرفته.

طبق موازین بین‌المللی، اتخاذ اسناد قانونی برای تضمین پاسداشت داده‌های خصوصی کافی نیست. برای موثر ساختن قوانین مربوط به صیانت از داده‌ها، ضروری است که ساز و کارهایی برقرار شوند که به افراد امکان مقابله با نقض حقوق‌شان و دریافت غرامت بخاطر ضررهای که متحمل شده‌اند داده شود. در ضمن مهم است که نهادهای نظارتی اختیار اعمال مجازاتی را داشته باشند که موثر، پیشگیرانه و متناسب با نقض قانون مورد نظر باشد.

اهمیت داشتن راه‌های موثر جبران مافات در «اظهار نظر عمومی شماره ۱۶» اینگونه مورد تاکید قرار گرفته قرار گرفته:

«در ضمن باید مقرر شود که تمام افراد بتوانند به طور موثر از خودشان در مقابل هرگونه حمله غیرقانونی که صورت می‌گیرد دفاع کنند و راه موثری برای جبران مافات علیه کسانی که مسئول این حمله بوده‌اند داشته باشند.»[117]

در منطقه اروپا، هم قوانین شورای اروپا و هم قوانین اتحادیه اروپا به افراد حق می‌دهد در صورتی که فکر می‌کنند پردازش داده‌های شخصی‌شان مطابق با قانون پیش نمی‌رود تقاضاها و شکایت‌های خود را نزد نهاد نظارتی مربوط ارائه کنند.

کنوانسیون جدید ۱۰۸ حق افراد موضوع داده، مستقل از ملیت و محل سکونت‌شان، برای بهره‌وری از کمک نهاد نظارتی را به رسمیت می‌شناسد. تنها در موارد استثنایی می‌توان تقاضای کمک را رد کرد و افراد موضوع داده نباید

[117] اظهار نظر عمومی شماره ۱۶، همانجا در ۱۱

هزینه‌های مربوط به این کمک را پوشش دهند. کنوانسیون مشخصا در مورد افراد موضوع داده می‌گوید که آن‌ها «در مواردی که حقوق‌شان که در کنوانسیون آمده نقض شده باید راه جبران مافاتی تحت ماده ۱۲ داشته باشند»[118].

ماده ۱۲ مقرر می‌دارد که دولت‌های عضو کنوانسیون «دست به برپایی مجازات‌های مناسب قضایی و غیرقضایی و راه‌های جبران مافات برای نقض قوانین این کنوانسیون بزنند.»[119]

«گزارش توضیحی» هم بر اهمیت این‌که راه‌های جبران مافات در اختیار فرد موضوع داده قرار داده شوند تا این‌گونه اعمال موثر تضمین شود تاکید می‌کند:

«موثر بودن کاربست اقداماتی که مفاد قانونی کنوانسیون را اجرایی می‌کنند از اهمیتی حیاتی برخوردار است. نقش نهاد (یا نهادهای) نظارتی به همراه هرگونه جبران مافاتی که در اختیار افراد موضوع داده است باید در بازبینی کلی در مورد موثر بودن اعمال مفاد قانونی کنوانسیون توسط کشورهای عضو مورد نظر قرار بگیرد.»[120]

سند «مقررات» اتحادیه اروپا حاوی همین اصول هست و از نهادهای نظارتی می‌خواهد دست به اقداماتی برای تسهیل ارائه شکایات بزنند. این شکایات باید منجر به تحقیق شوند و نهاد نظارتی باید به فرد مورد نظر در مورد نتیجه بررسی به شکایتش اطلاع دهد. این سند دولت‌های عضو را مقرر می‌دارد که به فرد موضوع داده امکان شکایت قضایی علیه تصمیم‌های نهادهای کشوری را اعطا کنند. این نه فقط در مورد افراد موضوع داده که در مورد کنترل‌گرها و پردازش‌گرهایی که در رویه‌ای نزد یکی از نهادهای نظارتی حضور داشته‌اند صدق می‌کند.[121]

این حق شکایت در سطح بین‌المللی وسیعا پذیرفته و اعمال شده و سایر کشورهای منطقه به افراد موضوع داده حق داشتن جبران مافات موثر را در کنار امکان تقاضای تجدیدنظر قضایی اعطا کرده‌اند. قانون صیانت از داده‌های تونس مقرر می‌کند که نهاد صیانت از داده‌ها شکایت‌ها را دریافت کند و در مورد اقدامات لازم برای تضمین پاسداشت داده‌ها تصمیم بگیرد.[122] قانون در ضمن حق بازبینی قضایی تصمیمات نهاد نظارتی را در دادگاه تجدید نظر تونس تا یک ماه پس از صدور تصمیم ارائه می‌کند.[123] در قطر، «قانون حریم داده‌های شخصی» مقرر می‌دارد که اداره مهارت شاید تصمیمی منطقی ابلاغ کند که از کنترل‌گر یا پردازشگر می‌خواهد تخلفی که صورت گرفته و مورد شکایت در دوره‌ای مشخص که توسط خود اداره تعیین می‌شود بوده جبران کند. کنترل‌گر یا پردازشگر شصت روز وقت دارند به تصمیماتی که نزد وزیر گرفته می‌شود اعتراض کنند. وزیر به هرگونه شکایت ظرف شصت روز از تاریخ تسلیم آن رسیدگی می‌کند.[124] به همین سان در الجزایر هم «اداره صیانت از داده‌ها» شکایت‌های فردی را دریافت می‌کند و می‌تواند با دستور، هر ترمیمی که برای پاسداشت داده‌های شخصی ضروری باشد ممکن سازد از جمله فرمان به توقف پردازش و در ضمن نابودی داده‌های شخصی.

پیشنهادها

---

118 شورای اروپا، کنوانسیون جدید ۱۰۸، ماده ۹

119 شورای اروپا، کنوانسیون جدید ۱۰۸، ماده ۱۲

120 شورای اروپا، کنوانسیون جدید ۱۰۸، گزارش توضیحی، بند ۳۵

121 سند «مقررات» اتحادیه اروپا، ماده‌های ۵۷، ۷۷ و ۷۸

122 قانون ارگانیک تونس ۲۰۰۴-۶۳ درباره صیانت از داده‌های شخصی، ۶ مرداد ۱۳۸۳، ماده ۷۶

123 قانون ارگانیک تونس ۲۰۰۴-۶۳ درباره صیانت از داده‌های شخصی، ۶ مرداد ۱۳۸۳، ماده ۸۲

124 قطر، قانون حریم خصوصی داده‌های شخصی، شماره ۱۳ سال ۲۰۱۶، ماده ۲۶

— اعطای اختیارات الزام‌آور به کمیسیون برای صدور دستور توقف پردازش، اصلاحات، انتشار اطلاعات شخصی نزد فرد موضوع داده و سایر قدرت‌ها

— اعطای حق تجدید نظر به افراد تحت نهادهای قضایی در مقابل تصمیمات کمیسیون.

پنج. نتیجه‌گیری

لایحه «حفاظت و صیانت از داده‌های شخصی» به روشنی نیاز به بهبود دارد تا مطمئن شویم ایران مطابق وظایف بین‌المللی‌اش در زمینه صیانت از داده‌ها و حریم شخصی عمل می‌کند و در ضمن تضمین تبعیت آن از سند «مقررات» اتحادیه اروپا و سایر قوانینی که جریان فرامرزی اطلاعات شخصی را تسهیل می‌کند.

لایحه برای ارائه چنین حفاظت‌هایی کافی نیست و در ضمن آزادی بیان و حق دسترسی به اطلاعات که در قانون اساسی آمده‌اند زیر سوال می‌برد. این لایحه به موازین و قوانین بین‌المللی اشاره‌ای نکرده و افراد موضوع داده را در مقابل مفاد مشکل‌آفرین قانون مجازات اسلامی و قانون مجازات رایانه‌ای آسیب‌پذیر باقی گذاشته. عواقب این لایحه برای آزادی بیان بسیارند. مهمتر از همه واقعیت‌های اجرای «محلی‌سازی داده» توسط این قانون و حرکت به سوی مرکزی‌سازی اطلاعات و قرار دادنش در سیطره مقامات ایران جای نگرانی دارد. در مورد استقلال «کمیسیون صیانت از داده‌ها» و نهادهای نظارتی در کار تضمین کاربست رویه قضایی جاهای خالی و نگرانی‌های بسیاری موجود هستند. باضافه، فقدان راه‌های روشن جبران مافات برای افراد موضوع داده‌ها خلا خطرناکی است که منجر به پیشینه می‌شود و به قوه قضائیه امکان تعقیب و آزار افرادی را می‌دهد که از حق آزادی بیان خود استفاده می‌کنند. لایحه می‌بایست به کمیته‌ای که آن‌را تدوین کرده باز پس فرستاده شود و پیش از معرفی مجدد آن، جلسات مشورتی با عموم و کارشناسان برگزار شود.