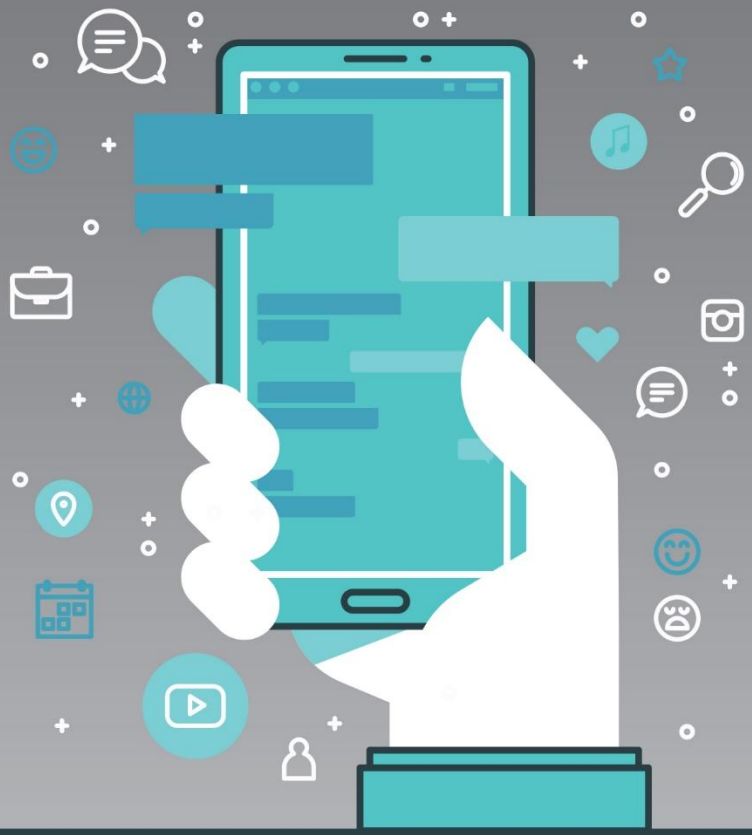
سلسله مباحث تنظیم الگوی مصرف پیام‌رسان‌های اجتماعی



۱

بررسی میزان تعهد تلگرام به حفاظت از داده‌های کاربران ایران

بسم الله الرحمن الرحيم

فهرست

حفاظت از اطلاعات کاربران در فضای مجازی ۱
قانون «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» در اتحادیه اروپا ۱
بندهای اصلی قانون صیانت از داده‌های اشخاص در اتحادیه اروپا..... ۳
حق به‌فراموشی سپرده‌شدن و حق تصحیح اطلاعات شخصی ۵
حفاظت از داده‌های کاربران فضای مجازی در ایران ۹
قانون‌گریزی تلگرام ۱۰
بی‌تعهدی تلگرام به حفاظت از داده‌های شخصی کاربران ایرانی ۱۳
جمع‌بندی..... ۱۵

حفاظت از اطلاعات کاربران در فضای مجازی

یکی از حقوق اولیه کاربران فضای مجازی، صیانت از داده‌های شخصی ایشان توسط خدمات دهندگان بسترهای ارتباطی است. مطالب اظهارشده یا پیام‌های ردوبدل شده در این بسترها جزو حریم خصوصی افراد محسوب می‌شود و ازآنجاکه می‌تواند حاوی دیدگاه‌های شخصی یا اطلاعات اقتصادی و تجاری افراد و بنگاه‌ها باشد باید مصون از دسترسی و پردازش توسط افراد و نهادهای غیرمجاز قرار گیرد.

توسعه فناوری‌های فضای مجازی موجب شده تا داده‌های بزرگ در ابعاد گسترده‌ای تولید شوند. برای حفظ اعتماد کاربران و پاسخگویی به ایشان در موارد سوءاستفاده‌های احتمالی، ضروری است سیاست‌ها، قوانین و مقرراتی بر فعالیت بسترهای ارتباطی در فضای مجازی حکم‌فرما باشد، بدون اینکه به آزادی عمل کاربران در این فضا خدشه‌ای وارد شود.

> برای حفظ اعتماد کاربران و پاسخگویی به ایشان در موارد سوءاستفاده‌های احتمالی، ضروری است قوانینی بر فعالیت بسترهای ارتباطی در فضای مجازی حکم‌فرما باشد.

یکی از بزرگ‌ترین ارائه‌دهندگان خدمات ارتباطی که در فضای مجازی کشور مورد استفاده واقع شده است پیام‌رسان تلگرام است. در این نوشتار بدین موضوع می‌پردازیم که آیا تلگرام متعهد به حقوق کاربران خود و ازجمله حفاظت از داده‌های کاربران ایرانی است یا خیر؟ جهت تمهید بحث ابتدا لازم است که شرایط مشابه در کشورهای دیگر مورد بررسی قرار گیرد.

قانون «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» در اتحادیه اروپا

برای آشنایی با نمونه مقرره گذاری در زمینه حفظ حریم خصوصی در فضای مجازی، به معرفی قانون «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» در اتحادیه اروپا می‌پردازیم. لازم به یادآوری است پیشرفته‌ترین نظام‌های حقوقی در سطح دنیا با تجربه چند صد ساله را می‌توان در کشورهای اتحادیه اروپا سراغ گرفت. قانون مذکور در مجموعه‌ای حدود صد صفحه تنظیم شده است. البته مفاد آن اختصاص به شبکه‌های پیام‌رسان نداشته و اعم از آن است.

مجموعه قوانین مرتبط با حفاظت از داده‌ها در کشورهای اروپایی (مصوب پارلمان اروپا) قِدمتی بیش از دو دهه داشته و از سال ۱۹۹۵ اجرا می‌شده است. در ژانویه سال ۲۰۱۲، کمیسیون اتحادیه اروپا طرحی را جهت اصلاحات جامع قوانین مذکور پیشنهاد کرد. این اصلاحات جامع با هدف افزایش کنترل کاربران بر داده‌های شخصی خود و کاهش هزینه‌های کسب و کار در این خصوص انجام گرفت. طبق پیش‌بینی کمیسیون، ایجاد یک قانون واحد و جامع در سطح اتحادیه اروپا در این زمینه منجر به صرفه‌جویی مالی قابل توجهی در حوزه کسب و کار خواهد شد. همچنین تقویت اعتماد مصرف‌کنندگان خدمات آنلاین و نیز رشد و توسعه اشتغال و نوآوری در اروپا را به دنبال خواهد داشت.

طرح فوق در ماه می سال ۲۰۱۶ در کمیسیون مذکور مصوب شده و متن آن در روزنامه رسمی این اتحادیه (Official Journal of the European Union) به زبان‌های مختلف منتشر گردید.[۱] اگرچه این قانون از تاریخ ۲۴ می ۲۰۱۶ در اتحادیه اروپا لازم‌الاجرا است، ولی کشورهای این اتحادیه تا تاریخ ۲۵ می ۲۰۱۸ فرصت دارند که مفاد این قانون را در قوانین ملی خود وارد نمایند.

سرفصل‌های اصلی قانون فوق عبارتند از:

- اصول پردازش داده‌های شخصی
- حقوق مالک داده (موضوع داده)
- مسئولیت کنترل‌کننده‌ها و پردازشگرها
- نحوه اعطای مجوزهای پردازش داده و شرایط بدنه اجرایی آن
- اصول و مقررات انتقال داده‌های شخصی به کشورهای دیگر و یا سازمان‌های بین‌المللی
- شرایط مقامات و مسئولین ناظر مستقل ملی و وظایف و اختیارات آن‌ها
- همکاری و توافق مسئولین ناظر کشورها با یکدیگر
- مقررات مربوط به پردازش داده‌ها در شرایط خاص

همان‌طور که از سرفصل‌های فوق نیز مشهود است، این قانون ابعاد گوناگون پردازش داده‌های شخصی افراد را در فضای مجازی در نظر گرفته است. قانون فوق به تفصیل به جزئیات تمامی حالات مرتبط پرداخته و تمهیدات متناسب از طرف اتحادیه اروپا که یکی از معتبرترین مجامع بین‌المللی است اندیشیده شده است. بدین ترتیب این قانون می‌تواند یکی از منابع مناسب برای تدوین قوانین مشابه و جامع کشور ما در این حوزه نیز باشد.

نکات کلیدی این قانون عبارتند از:

- با وجود این قانون، مجموعه‌ای واحد از قوانین حفاظت از داده در سراسر اتحادیه اروپا معتبر خواهد بود. ملزومات اداری غیرضروری، از جمله الزامات اطلاع‌رسانی برای شرکت‌ها، حذف خواهد شد و پیش‌بینی شده ۲٫۳ میلیارد یورو صرفه‌جویی سالانه برای کسب و کارها را در پی خواهد داشت.
- سازمان‌ها با یک مرجع واحد محافظت از داده ملی در کشورهای این اتحادیه سروکار دارند و مردم هم برای تأمین امنیت داده‌هایشان به یک مرجع مشخص ملی رجوع می‌کنند.
- افراد دسترسی آسان‌تری به داده‌هایشان دارند و می‌توانند داده‌های شخصی‌شان را به آسانی از یک اپراتور به اپراتور دیگر منتقل کنند (حق قابلیت انتقال داده‌ها). این امکان، رقابت بین ارائه‌کنندگان خدمات را در جلب رضایت مشتری افزایش می‌دهد.

---

[۱] متن قانون مذکور در لوح فشرده پیوست و همچنین نشانی‌های زیر (به ترتیب در قالب‌های html و pdf) قابل دسترسی است:

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- «حق به فراموشی سپرده شدن» به افراد کمک می‌کند تا بهتر بتوانند ریسک محافظت از داده‌هایشان را مدیریت کنند؛ زیرا این امکان برای افراد فراهم می‌شود تا داده‌هایی را که الزام قانونی خاصی برای نگه‌داشتن آن وجود ندارد حذف کنند.
- قوانین اتحادیه اروپا بر شرکت‌های خارجی که داده‌های شخصی را پردازش می‌کنند و در بازار اروپا فعالیت می‌نمایند و به شهروندان اروپا ارائه خدمت می‌کنند نیز اعمال می‌گردد.
- نهادهای مستقل ملی حفاظت از داده‌ها تقویت خواهد شد تا بتوانند در حوزه خود قوانین اتحادیه اروپا را به نحو بهتری به اجرا درآورند. آن‌ها این قدرت را پیدا خواهند کرد که شرکت‌های ناقض قوانین حفاظت از داده‌های اتحادیه اروپا را مجازات نمایند. میزان مجازات پیش‌بینی‌شده می‌تواند تا ۱ میلیون یورو و یا تا ۲ درصد از کل گردش مالی سالانه شرکت خاطی تعیین گردد.

میزان مجازات پیش‌بینی‌شده برای نقض قانون «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» در اتحادیه اروپا می‌تواند تا ۱ میلیون یورو و یا تا ۲ درصد از کل گردش مالی سالانه شرکت خاطی باشد.

بندهای اصلی قانون صیانت از داده‌های اشخاص در اتحادیه اروپا

قانون «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» در اتحادیه اروپا بخش‌های گوناگونی در خصوص حقوق مالکان داده و مسئولیت‌های اپراتورها دارد. در ادامه، بندهایی از این قانون و خصوصاً دو ماده آن را که تمرکز بیشتری بر حوزه محتوایی موضوع دارند – یعنی حق به فراموشی سپرده شدن و حق تصحیح اطلاعات شخصی مورد بررسی قرار می‌دهیم.

بر اساس بند ۲۴ در مقدمه این قانون،[۲] هر نهادی که به هر نحوی از داده‌های شخصی کاربران واقع در محدوده جغرافیایی اتحادیه اروپا بهره‌برداری می‌کند ملزم به تبعیت از قانون مذکور است، خواه نهاد مورد نظر در محدوده جغرافیایی اتحادیه اروپا واقع شده باشد یا خیر. ملاحظه می‌شود علی‌رغم اینکه فضای مجازی محدود به مرزهای جغرافیایی کشورها نیست اما این امر رافع مسئولیت حاکمیت کشورها جهت حفاظت از حقوق شهروندانشان در فضای مجازی نخواهد بود.

بر اساس بند ۳۹ در مقدمه این قانون،[۳] هرگونه پردازش داده‌های شخصی باید شفاف بوده و جمع‌آوری و استفاده از آن با اطلاع‌رسانی قبلی به صاحبان داده انجام پذیرد. حتی تصریح شده که این اطلاع‌رسانی باید به

---

[۲] متن این بند بدین قرار است:

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.

[۳] متن این بند بدین قرار است:

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and

زبانی ساده و قابل فهم برای صاحب داده انجام گیرد و روال‌ها و خطرات احتمالی پردازش مذکور آگاه شوند. در ذخیره‌سازی داده‌های کاربران توسط پردازشگرها نیز باید به حداقل زمان ممکن اکتفا شود.

هر نهادی که به هر نحوی از داده‌های شخصی کاربران واقع در محدوده جغرافیایی اتحادیه اروپا بهره‌برداری می‌کند ملزم به تبعیت از قانون اتحادیه اروپا است، خواه نهاد مورد نظر در محدوده جغرافیایی اتحادیه اروپا واقع شده باشد یا خیر.

بر اساس بند ۸۲ در مقدمه این قانون،[۴] چنانچه پردازشی روی اطلاعات کاربران انجام گیرد، پردازشگر موظف است سابقه آن را نزد خود نگه دارد تا در صورت لزوم و درخواست نهادهای حاکمیتی مربوطه جهت اِعمال وظایف نظارتی و رصدی خود، آن سابقه را در اختیار ایشان قرار دهد.

هرگونه پردازش داده‌ها در خصوص اَعمال مجرمانه و همچنین مسائل امنیتی کشورها می‌بایست تنها توسط نهادهای حاکمیتی مربوطه یا تحت اشراف ایشان انجام گیرد.

بر اساس بند ۱۴۸ در مقدمه این قانون،[۵] به‌عنوان ضمانت اجرای مقررات مذکور در این قانون مجازاتی از قبیل جرائم نقدی برای هرگونه نقض یا تخطی از آن در نظر گرفته خواهد شد.

ماده ۱۰ این قانون به پردازش داده‌های شخصی مربوط به اَعمال مجرمانه اختصاص دارد.[۶] بر اساس این ماده، هرگونه پردازش داده‌ها در حیطه مذکور و همچنین مسائل امنیتی کشورها می‌بایست تنها توسط نهادهای

---

transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

[۴] متن این بند بدین قرار است:

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

[۵] متن این بند بدین قرار است:

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation.

[۶] متن این ماده بدین قرار است:

Article 10 (Processing of personal data relating to criminal convictions and offences). Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member

حاکمیتی مربوطه یا تحت اشراف ایشان انجام گیرد. قید انحصاری در این ماده که بررسی امور مجرمانه و امنیتی را صرفاً در حیطه اختیارات نهادهای حاکمیتی قرار می‌دهد بسیار قابل توجه است.

حق به‌فراموشی سپرده‌شدن و حق تصحیح اطلاعات شخصی

ماده ۱۷ قانون مورد بررسی به «حق به‌فراموشی سپرده‌شدن»[۷] اختصاص دارد. مطابق بند ۱ این ماده، مالک داده (در این قانون به آن «موضوع داده» اطلاق می‌گردد) حق دارد که از اپراتور موتور جستجو (در این قانون به آن «کنترل‌کننده داده» اطلاق می‌گردد) بخواهد که داده مرتبط با وی را بدون تأخیر (یعنی بلافاصله پس از درخواست) از نتایج جستجویش حذف کند. اپراتور مربوطه نیز موظف است در صورت وجود شرایط زیر بلافاصله اقدام به حذف داده مذکور نماید:

۱- داده شخصی موردنظر پس از تاریخ درخواست، در راستای هدفی که به خاطر آن جمع‌آوری و پردازش شده است، ضروری نباشد.
۲- موضوع داده از رضایت خود برای پردازش داده‌هایش انصراف دهد و دلیل قانونی دیگری نیز برای پردازش داده‌های وی وجود نداشته باشد.
۳- چنانچه موضوع داده به پردازش داده‌هایش متعاقب بند ۱ ماده ۲۱ این قانون اعتراض داشته باشد و دلایل مشروع دیگری برای پردازش آن وجود نداشته باشد و یا اینکه موضوع داده مطابق ماده بند دوم ماده ۲۱ مخالف پردازش داده‌هایش باشد.
۴- داده‌های شخصی به‌طور غیرقانونی پردازش شوند.
۵- ضرورتی برای پاک شدن داده‌های شخصی توسط اپراتور مطابق با قانون اتحادیه اروپا و یا قوانین داخلی اعضا وجود داشته باشد.
۶- اطلاعات شخصی برای ارائه خدمات جامعه اطلاعاتی مندرج در ماده ۸ جمع‌آوری شده باشد.

مطابق بند ۲ این ماده قانونی، چنانچه اپراتور موتور جستجو (کنترل‌کننده) داده شخصی فردی را منتشر کند و مطابق بند ۱ موظف به حذف آن باشد، اپراتور با در نظر گرفتن فناوری موجود و هزینه‌های پیاده‌سازی می‌بایست گام‌های منطقی را برای اطلاع به اپراتورهایی که داده‌های شخصی را (که موضوع داده درخواست نموده) پردازش می‌کنند طی کند تا لینک‌ها، کپی‌ها و نسخه‌های تکراری آن داده شخصی را حذف نماید.

مطابق بند ۳ این ماده قانونی، بندهای ۱ و ۲ در جهت حذف داده‌های شخصی به تقاضای افراد، نباید در جایی که پردازش آن‌ها لازم است اعمال شوند. این موارد عبارتند از:

۱- چنانچه برای اعمال حق آزادی بیان و اطلاعات باشد.

State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

[۷] right to be forgotten

۲- در جایی که مطابق قانون اتحادیه اروپا یا قانون ملی کشورهای عضو، پردازش آن داده‌ها ضرورت داشته باشد.

۳- به دلیل حفظ منافع عمومی در حوزه‌هایی نظیر سلامت عمومی

۴- برای دستیابی به اهداف مرتبط با منافع عمومی، علمی، تحقیقات تاریخی، گزارش‌های آماری (مطابق بند ۱ از ماده ۸۹)

۵- برای استقرار، اعمال و یا دفاع از دعاوی حقوقی

ماده ۱۶ قانون مورد بررسی به «حق تصحیح اطلاعات شخصی»[۸] اختصاص دارد. طبق این ماده قانونی، موضوع داده حق دارد که از اپراتور موتور جستجو (کنترل‌کننده) بخواهد تا بدون تأخیر، اطلاعات شخصی اشتباه مرتبط با وی را تصحیح نماید. با در نظر گرفتن هدف پردازش، موضوع داده حق دارد که از کنترل‌کننده بخواهد تا داده‌های ناقص مرتبط با خود را با توجه به توضیحات تکمیلی ارائه شده، کامل نماید.

[۸] right to rectification

بررسی میزان تعهد تلگرام به
حفاظت از داده‌های کاربران ایران

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

Rectification and erasure

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

صفحاتی از قانون «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» در اتحادیه اروپا حاوی مواد قانونی «حق تصحیح اطلاعات شخصی» و «حق به‌فراموشی سپرده‌شدن»

با بررسی قانون «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» در اتحادیه اروپا که گزارش اجمالی آن در اینجا ارائه گردید ملاحظه می‌شود که حتی کشورهای لیبرال به وضع قوانین و مقرره‌گذاری در عرصه فضای مجازی پرداخته‌اند. لذا ادعای آزادی مطلق و رها بودن این فضا از نظارت دولت‌ها مزاحی بیش نیست. یکی از جنبه‌های مهم قوانین و مقررات مربوطه که موضوع این نوشتار است حفظ حریم خصوصی کاربران است. در ادامه با تمرکز بر این مبحث به بررسی وضعیت تلگرام در ایران از این جنبه می‌پردازیم.

> ادعای آزادی مطلق و رها بودن فضای مجازی از نظارت دولـت‌ها، حتی در کشـــورهای لیبرال نیز مزاحی بیش نیست.

حفاظت از داده‌های کاربران فضای مجازی در ایران

امروزه حفظ حریم خصوصی و صیانت از داده‌های کاربران فضای مجازی معنای بسیار گسترده‌ای یافته و یکی از ارکان توسعه این فضا است. مطابق آموزه‌های اسلامی و همچنین اصول قانون اساسی جمهوری اسلامی، حاکمیت حق دخالت در زندگی خصوصی مردم را ندارد؛ اما به همین ترتیب حاکمیت در برابر حفظ حریم خصوصی شهروندان مسئول است. هم‌اکنون شبکه‌های پیام‌رسان تهدیدی جدی برای این مهم هستند. تقریباً تمامی ایرانیانی که به گوشی هوشمند دسترسی دارند از پیام‌رسان تلگرام استفاده کنند. آیا در ایران قوانینی برای حفظ حریم خصوصی کاربران وجود دارد و آیا تلگرام متعهد به این امر است؟

نمی‌توان انکار کرد که حوزه فضای مجازی کشور ما دچار ضعف مفرط قوانین و مقررات به‌روز و کارآمد است. بنا بر اظهار دبیر شورای عالی فضای مجازی (به تاریخ ۲ اسفند ۱۳۹۶) ایران جزو کم‌قانون‌ترین کشورها در عرصه فضای مجازی است. البته در حال حاضر وزارت ارتباطات و فناوری اطلاعات در حال تهیه لایحه حمایت از حریم خصوصی کاربران است. در عین حال هم‌اکنون یک مصوبه مهم در این زمینه وجود دارد. بر اساس مصوبه شورای عالی فضای مجازی (به تاریخ ۸ خرداد ۱۳۹۵)، شرکت‌های خارجی پیام‌رسان که داخل ایران فعالیت دارند، برای ادامه فعالیت خود ملزم هستند همه اطلاعات و فعالیت‌های مرتبط با شهروندان ایرانی را به داخل منتقل کنند. بر این اساس مقرر شده بود همه شبکه‌های پیام‌رسان برخط فعال کشور ظرف یک سال آینده از این مصوبه انبارش یا ذخیره‌سازی داده‌های (دیتا) خود را در داخل کشور انجام دهند. با این وجود تلگرام تاکنون از پذیرش این مصوبه و اجرای آن استنکاف ورزیده است.

> ایران جزو کم قانون‌ترین کشورها در عرصه فضای مجازی است.

به‌علاوه، منشور حقوق شهروندی جمهوری اسلامی ایران به‌مثابه برنامه و خط‌مشی دولت برای رعایت و پیشبرد حقوق اساسی ملت ایران، در تاریخ ۲۹ آذر ۱۳۹۵ به امضای ریاست محترم جمهوری رسیده است. یکی از سرفصل‌های این منشور، «حق دسترسی به فضای مجازی» است. بر اساس ماده ۳۵ در این فصل، «حق

شهروندان است که از امنیت سایبری و فناوری‌های ارتباطی و اطلاع‌رسانی، حفاظت از داده‌های شخصی و حریم خصوصی برخوردار باشند.» یکی دیگر از سرفصل‌های منشور، «حق حریم خصوصی» است. بر اساس ماده ۳۷ در این فصل، «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 به‌موجب قانون».

ملاحظه می‌شود که بر اساس موارد فوق، حفاظت از داده‌های شخصی و پرهیز از گردآوری و پردازش اطلاعات و داده‌های شخصی شهروندان از حقوق آنان است. تلگرام تعهدی برای اجرای حقوق شهروندی کاربران ایرانی ندارد و لذا عملاً مانع قانونی برای نقض حقوق مذکور ندارد. با وجود تأکیدات الزام‌آوری که در منشور حقوق شهروندی ابراز شده، انتظار می‌رود دولت جمهوری اسلامی ایران که خود را مسئول اجرای آن منشور می‌داند تدبیرات متناسبی اتخاذ نماید.

> بر اساس منشور حقوق شهروندی جمهوری اسلامی ایران، حفاظت از داده‌های شخصی و پرهیز از گردآوری و پردازش اطلاعات و داده‌های شخصی شهروندان از حقوق آنان است.

قانون‌گریزی تلگرام

انبارش داده‌های کاربران ایرانی تلگرام در خارج از کشور صورت می‌پذیرد که برخلاف مصوبه شورای عالی فضای مجازی است. تلگرام تعهدی نیز به بندهای مرتبط از منشور حقوق شهروندی جمهوری اسلامی ایران ندارد. با این همه مشکلات حقوقی فعالیت تلگرام در ایران گسترده‌تر از این موارد است. پیام‌رسان تلگرام در ایران به ثبت رسمی نرسیده و هویت حقوقی آن مبهم است. بدین ترتیب تلگرام هیچ تعهدی به تبعیت از قوانین داخلی ایران ندارد. این امر از جنبه آسیب‌های ناشی از محتوای مجرمانه شبکه‌های اجتماعی خارجی، حفظ حریم خصوصی و اطلاعات کاربران ایرانی چالش‌برانگیز خواهد بود. تلگرام نه‌فقط از جنبه‌های متعددی تهدید امنیت ملی است، بلکه متعهد به کاربران ایرانی و صیانت از داده‌های آنان نیست. هیچ چارچوب خاصی بر فعالیت تلگرام در ایران حاکم نیست. لذا علی‌رغم آنکه تلگرام درآمد هنگفتی را از کاربران ایرانی کسب می‌کند در عین حال حاضر نیست کمترین رعایتی را در مورد قوانین و مقررات و ارزش‌های کشور ما داشته باشد.

> هیچ چارچوب خاصی بر فعالیت تلگرام در ایران حاکم نیست.

پاول دوروف، مدیر تلگرام، حتی گاه به عدم پایبندی به قوانین کشورها مباهات می‌کند. در ادامه چند نمونه را که مربوط به ایران است ملاحظه کنیم:

پاول دوروف: تلگرام وارد هیچ توافقی با هیچ دولتی در جهان نشده است. طرحی هم برای آن ندارد.

پاول دوروف: وزارت ارتباطات ایران خواسته که تلگرام ابزارهای سانسور و جاسوسی را در اختیار آن‌ها قرار دهد. ما این تقاضا را رد کردیم، آن‌ها ما را مسدود کردند.

پاول دوروف: مقامات ایرانی از ما می‌خواهند که با استفاده از تلگرام از شهروندانشان جاسوسی کنیم. ما نمی‌توانیم به آن‌ها در این زمینه کمک کنیم و در آینده نیز چنین نخواهیم کرد.

پاول دوروف: هیچ‌یک از سِروِرهای تلگرام (یا هر سِروِر دیگری که حاوی داده‌های شخصی کاربران ما باشد) به ایران منتقل نخواهد شد و در آنجا نصب نخواهد گردید.

همچنین این شرکت سابقه رد درخواست سایر دولت‌ها را نیز در کارنامه خود دارد. به عنوان نمونه در پی رد درخواست سرویس امنیتی روسیه مبنی بر در اختیار قرار دادن کلید دسترسی به پیام‌های کاربران از سوی تلگرام، دادگاهی عالی در مسکو توسعه‌دهندگان این پیام‌رسان را به میزان ۸۰۰ هزار روبل روسیه معادل ۱۴ هزار دلار جریمه کرد. سرویس امنیتی روسیه در تاریخ ۱۲ جولای ۲۰۱۷، درخواستی را برای آشکارسازی پیام‌های ردوبدل شده در تلگرام ارسال کرده بود. این درخواست می‌بایست تا تاریخ ۱۹ همان ماه عملیاتی می‌شد که از سوی مسئولین تلگرام رد شد.

ملاحظه می‌شود که مدیر تلگرام با صراحت منکر هرگونه پایبندی به الزامات دولت‌ها (ازجمله ایران) است. حتی از تقاضاهای مقامات ایرانی برای همکاری، به جاسوسی از شهروندان تعبیر کرده تا قانون‌گریزی خود را با ظاهر عامه‌پسندی جلوه دهد. آیا تلگرام به‌واقع دغدغه آن را دارد که از کاربران ایرانی حفاظت کرده و از جاسوسی از ایشان جلوگیری کند؟ استنکاف تلگرام از قرار گرفتن در چارچوب قانونی موجب شده تا عملاً بستر امنی را برای فعالیت‌های تروریستی فراهم نماید. بنا بر اعلام معاون امور فضای مجازی دادستان کل کشور (به تاریخ ۴ مرداد ۱۳۹۶)، برنامه‌ریزی و هماهنگی حملات تروریستی مسلحانه به مجلس شورای اسلامی

و حرم امام خمینی در بستر تلگرام انجام گرفته بود. فعالیت‌های تروریستی مشابهی نیز در انگلستان، فرانسه، اوکراین و ... از طریق تلگرام هماهنگ و سپس اجرا شده است که در نوشتار جداگانه‌ای مورد بررسی قرار خواهد گرفت. به خاطر داشته باشیم که چنانچه پیش از این بیان شد بر اساس مفاد قانون صیانت از داده‌های اشخاص در اتحادیه اروپا، خدمات‌دهندگان موظفند در صورت درخواست نهادهای حاکمیتی مربوطه جهت اِعمال وظایف نظارتی و رصدی خود، سابقه پردازشی اطلاعات کاربران را در اختیار قرار دهند. رویه قانون‌گریزانه‌ای که تلگرام اتخاذ کرده حتی با استانداردهای کشورهای اروپایی نیز که داعیه حقوق بشر را دارند ناهمخوان است.

به همین ترتیب تلگرام در برنامه اخیر خود اعلام کرده که می‌خواهد از عرضه رایگان خدمات و صِرف پیام‌رسانی به سمت ارائه خدمات و فعالیت‌های اقتصادی پیش برود. در عین حال برنامه تلگرام آن است که بدون اخذ هرگونه مجوزی به فعالیت‌های اقتصادی بپردازد.

در ادامه، آسیب‌های فعالیت تلگرام در خارج از چارچوب‌های قانونی کشور را از جهت مخاطراتی که برای اطلاعات و داده‌های شخصی کاربران به همراه دارد بررسی می‌کنیم.

بی‌تعهدی تلگرام به حفاظت از داده‌های شخصی کاربران ایرانی

حجم انبوهی از داده‌های کاربران ایرانی در تلگرام قرار دارد و بلکه این بستر به ثبت احوال برخط کشور و آرشیو اسناد افراد و خانواده‌ها تبدیل شده است. محبوبیت تلگرام در ایران به حدی چشمگیر است که درصد بالایی از پهنای باند اینترنت کشور در اختیار تلگرام است و این سایت در رتبه‌های اول دسترسی از طریق وب و همچنین از طریق دسترسی موبایل در ایران قرار دارد. در عین حال تلگرام هیچ‌گونه تعهدی در هیچ سطحی به کاربران خود یا مقامات مسئول در جمهوری اسلامی ایران نسپرده است. این امر فی‌نفسه مخالف رویه‌های مرسوم بین‌المللی است.

نکته حساس‌تر آن است که تلگرام از سپردن هرگونه تعهدی در خصوص حقوق کاربران ایرانی استنکاف می‌ورزد. به‌راستی داده‌های بزرگ (big data) کاربران ایرانی چگونه استفاده شده و مورد چه پردازش‌هایی قرار می‌گیرد؟ تلگرام ظاهراً به فعالیت اقتصادی نمی‌پردازد و منبع درآمدی حتی از طریق پذیرش آگهی نیز ندارد. لذا این ابهام وجود دارد که تأمین مالی تلگرام به چه نحوی انجام می‌پذیرد؟ آیا می‌توان مطمئن بود که داده‌های کاربران ایرانی در اختیار دولت‌های متخاصم بیگانه قرار نمی‌گیرد؟ توجه به این نکته لزوم حساسیت درباره شبکه پیام‌رسان تلگرام را دوچندان می‌سازد.

> تلگرام از سپردن هرگونه تعهدی در خصوص حقوق کاربران ایرانی استنکاف می‌ورزد.

مضاف بر اینکه درصد بسیار بالایی از جرائم فضای مجازی کشور در بستر تلگرام رخ می‌دهد (مطابق برخی آمارها بیش از ۸۰ درصد). ایجاد شبکه‌های عنکبوتی برای ارتکاب جرائم سازمان‌یافته (سوءاستفاده از دختران، ...) نیز یکی از عوارضی است که شبکه‌های مجازی در معرض آن هستند. با این وجود هیچ امکان پیگیری قانونی برای احقاق حق شهروندان در مورد این حجم از جرائم وجود ندارد. واضح است که جرائم سیاسی و امنیتی، بخش بسیار کوچکی از مجموعه جرائم و تخلفاتی است که در کشور رخ می‌دهد؛ اما معمولاً انعکاس رسانه‌ای این موارد بسیار بیشتر است. لذا وقتی سخن از رسیدگی به جرائم سایبری به میان می‌آید، ذهن‌ها معطوف به موارد سیاسی و امنیتی می‌شود. واقعیت ماجرا اما این نیست. در شرایط کنونی تلگرام، هزاران قاتل و تروریست و کلاهبردار و شیاد و سارق و متجاوز و کودک‌آزار و پدوفیل، آزادانه می‌توانند با استفاده از یک پیام‌رسان بیگانه به اَعمال پلید خود بپردازند و از هرگونه پیگرد قانونی در امان باشند. پذیرفتنی نیست که جان و مال و امنیت ده‌ها میلیون کاربر ایرانی که بسیاری از آن‌ها از نظر سواد رسانه در سطح پایینی هستند و در معرض انواع سوءاستفاده‌ها، این‌چنین بدون هرگونه حفاظت و ضمانتی در خطر قرار گیرد.

در شـرایط کنونی تلگرام، هزاران قاتل و تروریسـت و کلاهبردار و شـیاد و سارق و متجاوز و کودک‌آزار و پدوفیل، آزادانه می‌توانند با استفاده از یک پیام‌رسان بیگانه به اَعمال پلید خود بپردازند و از هرگونه پیگرد قانونی در امان باشند.

حق به‌فراموشی سپرده‌شدن و حق تصحیح اطلاعات شخصی نیز در تلگرام هیچ جایگاهی ندارد. پیام‌هایی که در کانال‌های تلگرامی منتشر می‌شوند، در صورت اصلاح و ویرایش و حتی در صورت حذف در دسترس باقی می‌مانند.

در چند مورد مهم رسوایی‌های بزرگی در غرب رخ داده و افکار عمومی نسبت به خطر فعالیت شبکه‌های اجتماعی بدون نظارت قانونی هوشیار شده است. آیا در ایران هم باید یک رسوایی و یا جنایت بزرگ در فضای مجازی رخ دهد تا بپذیریم که یک پیام‌رسان بیگانه با ده‌ها میلیون کاربر نمی‌تواند خارج از هرگونه نظارت قانونی در کشور عمل کند؟ حاکمیت جمهوری اسلامی ایران در چنین زمینه‌هایی که مرتبط با حفظ حقوق شهروندی است مسئول بوده و لذا کنترل وضعیت تلگرام از جهت صیانت از داده‌های کاربران ایرانی اقدام عاجلی را می‌طلبد.

جمع‌بندی

- صیانت از داده‌های شخصی یکی از حقوق اولیه کاربران فضای مجازی است
- در کشورهای پیشرفته جهت الزام بسترهای ارتباطی به حفاظت از حریم خصوصی کاربران قوانینی وضع شده است.
- اتحادیه اروپا با عنوان «صیانت از اشخاص در زمینه پردازش داده‌های شخصی» قانونی صدصفحه‌ای دارد.
- تلگرام از هرگونه همکاری و سپردن هرگونه تعهدی جهت حفاظت از اطلاعات و داده‌های کاربران ایرانی استنکاف می‌ورزد.
- اقدام عاجل در قبال بی تعهدی تلگرام به حقوق کاربران ایرانی ضروری است.