FILTER WATCH

TARAAZ
TECHNOLOGY & HUMAN RIGHTS

تهیه شده
توسط
فیلتربان و
تراز

حقوق دیجیتال و مسئولیت شرکت‌های فناوری در ایران

بررسی سرویس‌های پیام‌رسان اینترنتی

سپاسنامه

این گزارش به تلاش محققان موسسه‌های فیلتربان و تراز تهیه شده است. رویا پاکزاد به همکاری ملودی کاظمی مسئولیت تحقیق و نگارش این گزارش را به‌عهده داشتند.

نویسندگان این گزارش از کاوه آذرهوش و جیمز مرچنت برای مشاوره و همکاری‌شان در تمامی مراحل تدوین این گزارش تشکر میکنند؛ همچنین سپاسگزارند از سیمین کارگر، امیر رشیدی و فرزانه بدیعی، که با وجود مشغله‌ی فراوان، با نهایت مهر، بازخوردشان از نسخه‌های اولیه‌ی این گزارش را با نویسندگان به اشتراک گذاشتند. سپاس فراوان از شکوفه دزفولی برای ترجمه‌ی روان این گزارش به زبان فارسی.

از سوراستی پوری، طراح اطلاعات موسسه‌ی اسمال‌مدیا، بینهایت قدردانیم، چرا که ارائه‌ی مفاهیم اساسی این گزارش بی مدد خلاقیت، همفکری و همکاری بی‌دریغش به سهولت میسر نمیشد.

کمال تشکر از مسئولان موسسه‌ی Ranking Digital Rights به‌خصوص از امی برولت، ناتالی مارچال و یان ریدزک برای در میان گذاشتن نظرات ریزبینانه و سازنده‌شان در طول روند تحقیق و نگارش این گزارش . در آخر، از جسیکا دیر، مدیر موسسه‌ی RDR، و ربکا مک‌کینن، مدیر-موسس RDR برای حمایت‌های بی‌دریغشان از این پروژه سپاسگزاریم؛ امیدمان این است که گزارش پیش رو انگیزه‌ای باشد برای سایر محققان حوزه حقوق دیجیتال و گروه‌های مدنی تا از شاخص رتبه‌بندی RDR برای پاسخگو نگه‌داشتن شرکت‌های فناوری و هدایتشان به رعایت حقوق کاربران استفاده کنند.

این گزارش با همکاری موسسه‌های زیر تهیه شده است:

FILTER WATCH

TARAAZ
TECHNOLOGY & HUMAN RIGHTS

RANKING DIGITAL RIGHTS
METHODOLOGY ADAPTATION

فهرست مطالب

چکیده اجرایی

گزارش

«حقوق دیجیتال و مسئولیت شرکت‌های فناوری در ایران»، به تاثیر عملکرد شرکت‌های فناوری بر حقوق کاربران ایرانی می‌پردازد و مسئولیت این شرکت‌ها را در قبال حقوق کاربران خود مورد بررسی قرار میدهد. ما از ژانویه تا سپتامبر سال ۲۰۲۰، تعهدات حقوق بشری چند شرکت فناوری در ایران را مورد بررسی قرار دادیم. روش پژوهش این گزارش بر اساس نسخه‌ی برگرفته شده از «شاخص رتبه‌بندی مسئولیت شرکت‌ها در قبال حقوق دیجیتال (RDR)» تهیه شده است. از سال ۲۰۱۵ شاخص RDR به ارزیابی شیوه‌ها و سیاست‌گذاری‌های علنی قدرتمندترین شرکت‌های اینترنتی، تلفنی و مخابراتی دنیا و تاثیر آنها بر حق آزادی بیان و حریم خصوصی کاربران، پرداخته است. پژوهشگران حوزه حقوق دیجیتال در سراسر جهان، از جمله روسیه، کنیا، سنگال، کشورهای عربی، هند و پاکستان نیز این روش را برای ارزیابی شرکت‌ها در کشورهای خود به کار گرفته‌اند و برای هدایت شرکت‌ها به سمت شفافیت بیشتر از آن استفاده می‌کنند.[1] حالا این اولین بار است که روش پژوهش شاخص RDR برای بررسی سیاست‌گذاری‌های شرکت‌های فناوری در ایران، به کار گرفته می‌شود.

اولین قدم برای اینکه شرکت‌ها تعهدات خود را نسبت به حقوق بنیادین کاربران نشان دهند، این است که سیاست‌گذاری‌ها و روش‌های کاری خود را که بر این حقوق تاثیر می‌گذارند، به صورت علنی اعلام کنند. شفافیت، تقاضا برای مسئولیت‌پذیری را میسر می‌سازد؛ وقتی که سیاست‌گذاری‌ها و شیوه‌های کار به صورت علنی در دسترس باشند، روزنامه‌نگاران می‌توانند از آنها در گزارش‌های تحقیقاتی خود استفاده کنند؛ ناظران فناوری می‌توانند تطابق ادعا و عمل را در محصولات به بوته آزمایش بگذارند؛ و گروه‌های جامعه مدنی و متخصصان حوزه قضایی می‌توانند نقاط قوت و ضعف سیاست‌های سازمانی را ارزیابی کنند. ما امیدواریم که با انتشار این گزارش، اهمیت وجود شفافیت و پایبندی به حقوق بشر را - آنچنان که در«اصول راهنمای تجارت و حقوق بشر سازمان ملل» آمده است - در ارتباط با شرکت‌های فناوری ایرانی، در مرکز توجه قرار دهیم.[2]

ما در این نسخه از گزارش، روش‌های کاری و سیاست‌گذاری‌های علنی سرویس‌های پیام‌رسانی که روزانه از طرف کاربران ایرانی مورد استفاده قرار می‌گیرند را بررسی کردیم. این شرکت‌ها شامل چهارسرویس پیام‌رسان داخلی: «سروش»، «گپ»، «بله» و «بیسفون» و همچنین دو همتای غیر ایرانی آن‌ها یعنی «واتس‌اپ» و «تلگرام» هستند. هر چند تصمیم گرفتیم که اپلیکیشن‌های پیام‌رسان را ارزیابی کنیم، خوانندگان این گزارش باید بدانند که تقریباً تمام مولفه‌های مورد استفاده برای سنجش اپلیکیشن‌های پیام‌رسان، می‌توانند در مورد دیگر خدمات تلفن همراه و شرکت‌های اینترنتی نیز به کار گرفته شوند.

یافته‌ها و مشاهدات کلیدی

- تقریباً تمام شرکت‌های مورد بررسی، اطلاعاتی را درباره سیاست‌گذاری‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات، به صورت علنی ارائه می‌دهند. در چندین مورد، هم در بین اپلیکیشن‌های داخلی و هم خارجی، چنین اطلاعاتی به جای اینکه در بخشی مخصوص این قوانین قرار بگیرند، در بخش «سوالات متداول» یا در بین مطالب عمومی دیگری روی وبسایت این شرکت‌ها تعبیه شده بودند. بسیار مهم است که اینگونه اطلاعات پیش از ثبت‌نام و ایجاد حساب کاربری به راحتی در دسترس کاربران باشند.

- شرکت‌ها پایین‌ترین امتیاز را در بخش شفاف‌سازی درباره درخواست‌های نهادهای دولتی و قضایی و

1 RDR Adaptations, Ranking Digital Rights, https://bit.ly/2H4OQcT
2 The UN Guiding Principles on Business and Human Rights, HR/PUB/11/04, United Nations, 2011, https://bit.ly/2IyyOZ7

طرفین ثالث برای دسترسی به اطلاعات کاربران، سانسور کردن محتوا و محدود کردن صفحات کاربری، دریافت کردند. هیچ‌کدام از شرکت‌های ایرانی اظهار نکرده‌اند که شرایط و ضوابط استفاده از خدمات و حریم خصوصی خود را تا چه حد و به چه شکل اعمال می‌کنند. علاوه بر این، هیچ‌کدام از این شرکت‌های داخلی درباره برنامه‌های آموزشی برای کارکنان خود در زمینه حقوق دیجیتال، اجرای سنجش اثرات حقوق بشر و همکاری با گروه‌های جامعه مدنی و دیگر ذینفعان، اطلاعات شفافی ارائه نکرده‌اند.

- سرویس‌های پیام‌رسان‌های خارجی نیز از دریافت امتیاز کامل فاصله بسیار دارند. با در نظر گرفتن تعداد بالای کاربر ایرانی و فارسی‌زبانِ این شرکت‌ها، عدم وجود نسخه‌های فارسی از سیاست‌های حریم خصوصی و قوانین و ضوابط استفاده از خدمات، مطالب آموزشی درباره حفظ امنیت، روند درخواست‌های تجدیدنظر، و همینطور فقدان شفافیت در مورد رویه‌های اعمال شرایط و ضوابط استفاده از خدمات در بستر ایران و زبان فارسی، همه و همه می‌تواند اثرات تبعیض‌آمیزی بر کاربران ایرانی داشته باشد، مخصوصاً برای افرادی که از سواد دیجیتالی پایین‌تری برخوردارند. علاوه بر این، عرضه‌ی API های شرکت‌ها، به‌خصوص در مورد تلگرام، موجب به‌وجود آمدن روش‌هایی جدیدی برای سواستفاده و نقض حریم خصوصی افراد شده است. این موضوع نشانگر اهمیت نقش شرکت‌ها در جلوگیری از چنین سواستفاده‌هایی از طریق انجام سنجش‌های حقوق بشری، بررسی امنیت توسعه‌ی APIها و اعمال ضوابط استفاده از خدمات مابین شرکت‌ها و توسعه‌دهندگان میباشد.

- در مورد یکی از شرکت‌های پیام‌رسان ایرانی، ما متوجه ناهمخوانی بین اظهارات در نسخه انگلیسی در مقابل نسخه‌های فارسی و عربی بر روی وبسایت آن پیام‌رسان شدیم. این شرکت همچنین یک محصول را تحت نام تجاری دیگری برای کاربران بین‌المللی خود معرفی کرده است. در این مورد، توجیه این بوده که از تحریم‌های فناوری علیه شرکت‌های ایرانی اجتناب کرده و راه خود را برای ورود به بازارهای بین‌المللی هموار کند. با این حال، این روش‌ها موجب ایجاد ابهاماتی درباره سازوکارهای مسئولیت‌پذیری و پاسخگویی شرکت‌ها در حیطه اختیارات و نظارت بر حفاظت از داده، می‌شود. ما همچنین متوجه شدیم که با وجود ادعاهای برخی شرکت‌های ایرانی در مورد اعمال الگوهای برتر مانند رمزنگاری سرتاسری، هیچگونه مدرک علنی درباره جزئیات فنی این ادعاها وجود ندارد.

- برنامه‌های بومی‌سازی اینترنت در ایران — که با همکاری، کنترل و سرمایه‌گذاری‌های دولت ایران برای رشد بخش فناوری داخلی نیز همراه می‌باشد — ابهاماتی را درباره مسئولیت‌پذیری و روش‌های سیاست‌گذاری شرکت‌ها به وجود آورده است. اضافه کردن خدمات دولت دیجیتال به اپلیکیشن‌های پیام‌رسان، نگرانی‌های تازه‌ای درباره‌ی جمع‌آوری اطلاعات کاربران و به اشتراک‌گذاری آن میان شرکت‌های خصوصی و نهادهای دولتی مثل بانک مرکزی ایران، وزارت آموزش و پرورش و سازمان صدا و سیمای جمهوری اسلامی ایران، ایجاد کرده است. این‌ها نمونه‌هایی هستند که نشان می‌دهند چطور امکان تعدی به حق حریم خصوصی و آزادی بیان میتواند از دایره این حقوق فراتر رفته و سایر حقوق اجتماعی-اقتصادی، فرهنگی، مدنی و سیاسی افراد را نیز تهدید کند. انتظار می‌رود که در سال‌های آینده نه تنها در ایران، بلکه در کشورهای دیگری که برنامه‌های بومی‌سازی اینترنت از سوی رهبرانشان در حال پیاده‌سازی است، چنین روابط نگران کننده و مبهمی بین بخش خصوصی و نهادهای دولتی بیش از پیش گسترش پیدا کنند.

روی هم رفته، ارزیابی ما نشان می‌دهد که با وجود تلاش‌های اندک شرکت‌ها برای اعلان سیاست‌هایشان در زمینه‌ی حقوق دیجیتال، هنوز راه درازی برای دریافت امتیاز کامل و کسب اعتماد کاربران ایرانی باقیست. امید ما بر این است که شرکت‌ها از این گزارش به عنوان راهنما استفاده کرده، کمبودهای شناسایی شده را برطرف کنند و کاربران خود را از آسیب‌های فعلی و احتمالی به حقوق انسانی‌اشان در امان نگه دارند.

توصیه‌هایی برای شرکت‌ها

- شرکت‌ها می‌بایست سیاست‌های خود را در قبال برخورد با درخواست‌های نهادهای دولتی و قضایی برای دسترسی به اطلاعات کاربران، سانسور کردن محتوا و محدود کردن حساب‌های کاربری به طور شفاف و مکتوب اعلام کنند. علاوه بر این، می‌بایست درباره چگونگی اعمال شرایط و ضوابط استفاده از خدمات، مهار نشت اطلاعات کاربران وحفره‌های امنیتی، اطلاعاتی را به شکل جامع و سازمان‌یافته بر روی وبسایت خود منتشر کرده و این اطلاعات را مرتبا به‌روزرسانی نمایند.

- سرویس‌های پیام‌رسان داخلی باید در مورد همکاری‌های خود با نهادهای دولتی یا وابسته به حکومت شفاف باشند و به طور مکتوب اعلام کنند که مشارکت و سرمایه‌گذاری نهادهای حکومتی هرگز موجب امتیاز ویژه یا دسترسی این نهادها به اطلاعات کاربران نخواهد شد. علاوه بر این، این شرکت‌ها می‌بایست درباره ساختار حاکمیت و مالکیت خود شفاف باشند. این شفاف‌سازی می‌تواند از طریق اضافه کردن صفحاتی مثل «درباره ما» و «ارتباط با ما» بر روی وبسایت رسمی شرکت و تولید حساب‌های رسانه‌های اجتماعی، صورت بگیرد. علاوه بر این، اقدامات رسمی‌تری مثل انتشار اطلاعات درباره میزان و نوع همکاری با دیگر نهادهای خصوصی و دولتی، گزارش‌های مالی، اطلاعاتی درباره هیئت مدیره، و گزارش جلسات سازمانی سالانه، می‌تواند برای ایجاد شفافیت صورت بگیرد.

- شرکت‌ها می‌بایست الگوهای برتر طراحی و توسعه خدمات دیجیتال مانند طراحی بر مبنای حفظ حریم خصوصی (privacy by design) را به کار گیرند. آنها همچنین باید درباره اقدامات انجام‌شده برای بررسی امنیت سایبری محصولات خود شفاف باشند و جزئیات فنی این اقدامات را منتشر کنند؛ می‌بایست برنامه‌های باگ باونتی ارائه دهند تا پژوهشگران حوزه امنیت سایبری بتوانند خدمات آنها را بررسی کرده و نقاط ضعفشان را در زمینه امنیت و حریم خصوصی بیابند.

- شرکت‌ها می‌بایست از «اصول راهنمای تجارت و حقوق بشر سازمان ملل» پیروی کنند. آنها باید تعهدات سازمانی مربوط به حقوق بشر را تهیه و منتشر کرده و به طور منظم به سنجش اثر فعالیت‌ها و محصولات خود بر حقوق کاربران، به خصوص حقوق گروه‌های آسیب‌پذیرتر جامعه مانند کودکان، اقلیت‌های دینی، جنسی و جنسیتی، قومی و پناهندگان، بپردازند؛ شرکت‌ها باید به طرح‌های چند ذینفعی بپیوندند و با گروه‌های جامعه مدنی گفتگو کنند. شرکت‌ها همچنین می‌بایست دسترسی کارکنان خود را به داده‌های کاربران محدود کنند و به کارکنان خود درباره حقوق دیجیتال آموزش دهند.

توصیه‌هایی برای نهادهای مسئول در ایران

- نهادهای مسئول در ایران می‌بایست برنامه‌های بومی‌سازی اجباری و بررسی‌نشده‌ی اینترنت که اصول بی‌طرفی شبکه را نقض می‌کنند، متوقف کنند. این برنامه‌ها که عموماً با قطع دسترسی به سرویس‌های بین‌المللی از طریق فیلترینگ یا تخصیص تعرفه‌هایی با امتیازات خاص به خدمات داخلی، همراه است، آزادی انتخاب و حق دسترسی به اطلاعات آزاد را از کاربران ایرانی سلب می‌کند و به صورت ناعادلانه‌ای بر آزادی انتخاب و حقوق دیجیتال گروه‌های آسیب‌پذیرتر جامعه، که در موقعیت اقتصادی-اجتماعی پایین‌تری قرار دارند، تاثیرات نامطلوبی می‌گذارد. اپلیکیشن‌های بخش خصوصی که در ابتدا اعلام شده بود هدف اصلی طراحی‌شان تولید «پیام‌رسان» است، تبدیل به پلتفرم‌هایی شده‌اند که یک روز میزبان خدمات دیجیتال یک نهاد دولتی هستند و روز دیگر محل ارائه‌ی خدمات مالی دیگر نهاد مسئول. اضافه کردن امکان خدمات دولتی به اپلیکیشن‌های پیام‌رسان داخلی، تشویق‌های مالی کوته‌نظرانه برای استفاده از شبکه ملی اطلاعات به جای اینترنت بین‌المللی، یا حمایت‌های دولتی از شرکت‌های نوپا از طریق فراهم آوردن خدمات

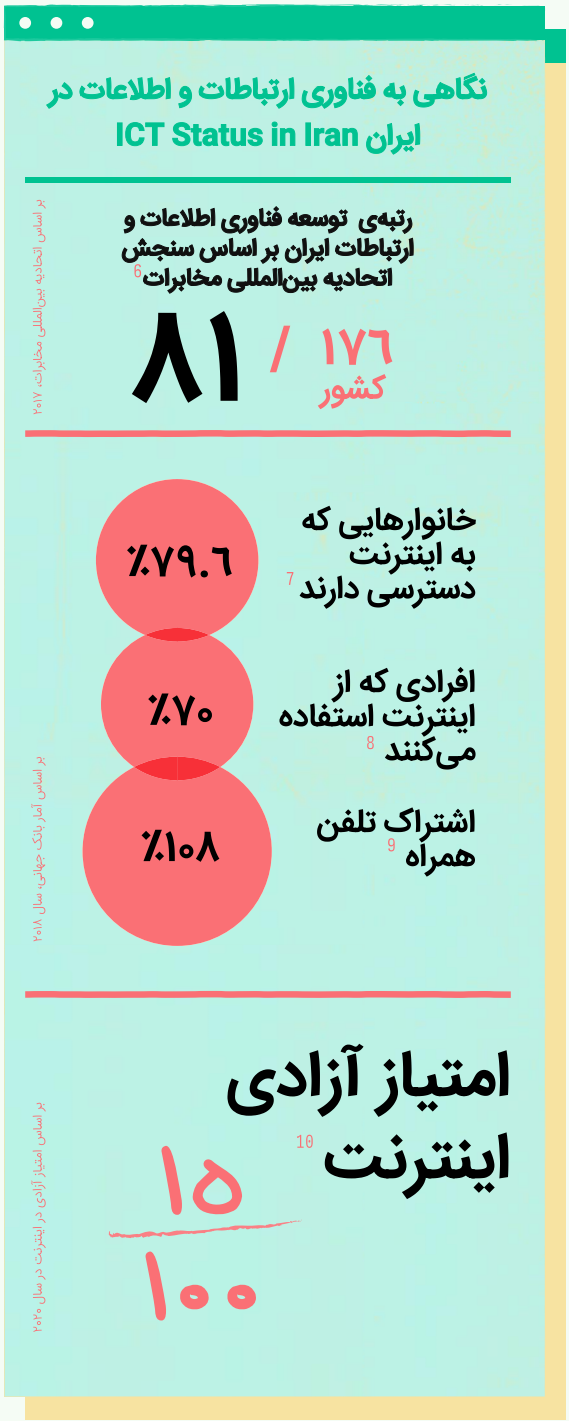
دولتی، مانند دسترسی رایگان به مراکز داده، نباید به سادگی به عنوان برنامه‌های مرسوم دولت برای حمایت از خدمات داخلی تلقی و تبلیغ شوند. در نبود سازوکارهای نظارتی شفاف و عمومی، این گونه همکاری‌های عجولانه و مبهمی، موجب از بین رفتن اطمینان کاربران به این شرکت‌ها می‌شود. همچنین، چنین سیاست‌هایی باعث کنترل و نظارت بیش از حد نهادهای دولتی بر کار این شرکت‌ها، ترویج فرهنگ تبعیض بین دولت و بخش خصوصی و تشویق‌کننده‌ی رقابت ناعادلانه بین شرکت‌های فناوری خصوصی شده است که امکان ورود و رشد در بازارهای بین‌المللی را برای شرکت‌های فناوری ایرانی محدود می‌کند.

نهادهای سیاست‌گذار در ایران می‌بایست چارچوب قانونی قوی و مبسوطی برای محافظت از داده اعمال کند که با استانداردهای بین‌المللی حقوق بشر مطابقت داشته باشد. دولت باید برای شرکت‌ها، ضوابط کارشناسانه‌ای مربوط به امنیت و حریم خصوصی تنظیم کند. تا زمانی که یک چارچوب قانونی، جامع و مبتنی بر اصول حقوق بشری وجود نداشته باشد، مسئولین باید پیشبرد طرح ساماندهی پیام‌رسان‌های اجتماعی را متوقف کند، چرا که این طرح، آزادی‌های اینترنتی مردم ایران را محدود کرده و کنترل درگاه‌های اینترنتی را تحت نظارت نیروهای مسلح قرار می‌دهد.

۱

مروری بر حقوق دیجیتال در ایران

[Fig 1]



در سال ۲۰۱۶ شورای حقوق بشر سازمان ملل متحد، قطعنامه‌ای منتشر کرد مبنی بر اینکه «همان حقوقی که افراد در فضای حقیقی از آن برخوردارند، در فضای مجازی نیز می‌بایست رعایت شود»[۳]. دسترسی به اینترنت نقش اساسی در برخورداری از حقوق انسانی ما در عصر دیجیتال به عهده دارد، و در حالی که مرز میان دنیای حقیقی و مجازی روز به روز کمرنگ‌تر می‌شود، خطر نقض این حقوق انسانی نیز تبدیل به واقعیتی در زندگی در عصر اینترنت شده است. ایران، به عنوان تصویب کننده‌ی «میثاق بین‌المللی حقوق مدنی و سیاسی» و «میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی»، وظیفه دارد تا مطابق با موازین سازمان ملل، به حقوق شهروندان خود احترام گذاشته، از آنها محافظت کرده و آنها را برآورده سازد.[۴] برای به‌دست آوردن درک درستی از سابقه ایران در در قبال تعهدات خود به حقوق شهروندان در عصر دیجیتال، باید کمی به عقب برگردیم و نگاهی بیندازیم به فناوری‌های دیجیتال در ایران از منظر فنی و سیاست‌گذاری‌ها.

در طول دهه‌ی گذشته، فناوری اطلاعات و ارتباطات در ایران، رشد قابل ملاحظه‌ای داشته است. در سال ۲۰۰۶، دولت ایران برنامه‌ی خود را جهت ایجاد «شبکه ملی اطلاعات» معرفی کرد، یکی از اهداف عنوان شده در این برنامه ایجاد زیرساخت‌های لازم برای بهبود سرعت و دسترسی به اینترنت بوده است. از دیگر اهداف اصلی این برنامه می‌توان به این موارد اشاره کرد: تقویت تاب‌آوری با در نظر گرفتن امکان وقوع تحریم‌های مالی و فناوری؛ فراهم کردن اقدامات امنیتی لازم در مقابل حملات سایبری؛ کمک مالی و تشویق شرکت‌های نوپای داخلی، مشاغل اینترنتی و طرح‌های کارآفرینانه.[۵]

3 “The promotion, protection and enjoyment of human rights on the Internet,” A/HRC/32/L.20, UN Human Rights Council, June 27, 2016, https://bit.ly/3oKIDUH

4 Both UN conventions were ratified by Iran in 1976. You can find the information on Status of Ratification: Interactive Dashboard, https://indicators.ohchr.org/

حال، واضح است که قصد دیگر دولت ایران برای راه‌اندازی شبکه ملی اطلاعات، این است که از این شبکه به عنوان ابزاری برای کنترل فضای مجازی و اجرای سیاست‌های مضر بومی‌سازی اینترنت استفاده کند. چنین استراتژی‌های بومی‌سازی‌ای که به دور از بررسی‌های کارشناسانه و شفافی صورت میگیرند، اصل بی‌طرفی شبکه (net neutrality) را زیر پا گذاشته است و شرکت‌های ارائه‌دهنده خدمات اینترنتی را تحت فشار قرار داده تا جلوی دسترسی به سرویس‌ها و محتوای آنلاین را بگیرند.[11] رهبران ایران به جای اینکه بخواهند اینترنت در ایران بخشی از اینترنت جهانی باقی بماند، بیش از پیش به دنبال ایجاد وابستگی کاربران ایرانی به شبکه ملی اطلاعات و فناوری‌های دیجیتال بومی هستند که معمولا به صورت مستقیم یا غیرمستقیم تحت نظارت و کنترل حکومت هستند. بسیاری از سازمان‌های حقوق بشری هشدار داده‌اند که این روند به احتمال زیاد به جداسازی و انزوای بیشتر کاربران ایرانی در آینده ختم خواهد شد.[12]

در این رابطه، همچنین باید به تلاش‌های آمریکا برای منزوی کردن و تحریم ایران نیز توجه داشت؛ تلاش‌هایی که در واقع به دولت ایران کمک کرده است تا برنامه‌های بومی‌سازی اینترنت خود را پیش ببرد.[13] از این گذشته، مشکل اصلی همیشه خود تحریم‌های آمریکا نیست، بلکه ابهامات ناشی از آن است. در سال ۲۰۱۴ دولت ایالات متحده، پروانه عمومی D-۱ را صادر کرد که به شرکت‌های فناوری آمریکایی اجازه می‌دهد تا با هدف تقویت آزادی اینترنتی در ایران، برخی فناوری‌های «ارتباطات شخصی» را برای ایرانیان فراهم کنند. تا به امروز، پروانه عمومی D-۱ دست نخورده باقی مانده است.[13] با این حال، به نظر می‌رسد بسیاری از شرکت‌های فناوری آمریکایی، برای پرهیز از هرگونه خسارت اقتصادی، اعتباری و قانونی، سعی می‌کنند تا از دردسرهای تجارت با ایران و ایرانیان، حتی اگر قانونی هم باشد، اجتناب کنند.[15] نتیجه‌اش به وجود آمدن دشواری‌های فراوان برای کاربران و کارآفرینان فناوری در ایران است، که به اهداف دولت ایران کمک می‌کند تا بومی‌سازی اینترنت را پیش برده و به توسعه‌دهندگان فناوری‌های داخلی تحمیل کند که تنها راه پیش رو برای آنها این است که به روش حکومت عمل کنند.

با این حال، هدف از این گزارش، نه ارائه تحلیل کاملی از نقشی است که رهبران ایران در محدود کردن حقوق دیجیتال مردم ایران بازی می‌کنند، و نه بررسی تاثیر کشورها یا شرکت‌های غیرایرانی. در عوض، **این گزارش به نقشی که شرکت‌های فناوری ایرانی به حیث احترام به حقوق دیجیتال کاربرانشان برعهده دارند می‌پردازد. هدف این تحقیق این است که نشان دهیم عملکرد شرکت‌های فناوری ایرانی چطور می‌تواند روی حقوق دیجیتال تاثیر بگذارد و مسئولیت این شرکت‌ها در قبال احترام به این حقوق چیست.**

5 Supreme Council for Cyberspace Resolution,“Explanatory Document on the Requirements of the National Information Network,” Islamic Parliament Research Center of The Islamic Republic of Iran, September 18, 2017, https://bit.ly/3jExXD8

6 “Measuring the Information Society Report 2017”, International Telecommunication Union, https://bit.ly/3khbMDW

7 “UPR Session 34, Iran Freedom of Expression andInternet Freedom”, UPROAR, https://bit.ly/2HfId76

8 “Individuals Using the Internet”, World Bank, 2018, https://bit.ly/3464BZY

9 “Mobile Cellular Subscriptions (per 100 people) - Islamic Republic of Iran”, World Bank, 2018 https://bit.ly/3j4MqIf

10 “Freedom on the Net Report 2020 - Iran”, Freedom House, 2020, https://bit.ly/2TztVkN

11 “Tightening the Net: Internet Security and Censorship in Iran - Part 1: The National Internet Project”, Article 19, 2016, https://bit.ly/3k4gKnL

12 “Joint submission to the Universal Periodic Review of the Islamic Republic of Iran by Article 19 and Access Now”, Access Now, April 4 2019, https://bit.ly/3m5CKzh Fa version: https://bit.ly/2H88DIv

13 Azin Mohajerin, “To Help the Iranian People, Reverse Tech Sanctions Asap”, Atlantic Council, January 17, 2020, https://bit.ly/3o09lIf

14 Mahsa Alimardani and Roya Pakzad, “Silicon Valley preaches diversity and inclusion while excluding Iranians”, Atlantic Council, April 8, 2019, https://bit.ly/3dug3BC

15 برای مثال می‌توان به تصمیم گوگل برای بستن App Engine و Google Cloud Platform ، یا تصمیم آمازون برای بستن AWS بر روی ایرانیان داخل کشور اشاره کرد. برای دیدن سرویس‌هایی که در ایران بسته هستند به این لینک مراجعه کنید: https://bit.ly/31eB0eL

شرکت‌های فناوری و حقوق بشر

بررسی سرویس‌های پیام رسان اینترنتی

در سال‌های اخیر، روزی نگذشته که خبری جدید درباره‌ی رابطه‌ی درهم‌تنیده‌ی حقوق بشر و فناوری نشنیده باشیم. این خط سیر زمانی، بعضی از این اتفاقات بسیار مهم در سطح جهانی را به نمایش می‌گذارد؛ اتفاقاتی که در پانزده سال گذشته شرکت‌های فناوری را در مرکز مسائل مربوط به حقوق بشر قرار داده‌اند.

[Fig 2]

16 Rebecca MacKinnon, “Consent of the Networked: The Worldwide Struggle For Internet Freedom,” (Basic Books, 2013), 133

17 The Global Network Initiative, 2008, https://bit.ly/37ck4JD

18 Google Transparency Report, https://bit.ly/37eFvKm

19 Glenn Greenwald, “NSA Prism Program Taps into User Data of Apple, Google and Others”, Guardian, June 7, 2013, https://bit.ly/3khddlO

20 Samuel Gibbs, “Ebay Urges Users to Reset Passwords After Cyberattack”, Guardian, May 21, 2014, https://bit.ly/342gShJ

21 Lotus Ruan, Jeffrey Knockel, Jason Q. Ng, and Masashi Crete-Nishihata, “One App, Two Systems How WeChat uses one censorship policy in China and another internationally,” November 2016, https://bit.ly/2SXyZPN

22 Hillary Leung, “Airbnb Faces Renewed Criticism Over Listing Occupied West Bank”, Time, May 15, 2019, https://bit.ly/2T6FkrX

23 Angwin et al., “Machine Bias”, ProPublica, May 23, 2016, https://bit.ly/2T1QsGA

24 Microsoft Security Response Center, “Customer Guidance for WannaCrypt Attacks” Microsoft, May 12, 2017, https://bit.ly/31bHFX8

25 “NSO Group/ Q Cyber Technologies: Over One Hundred New Abuse Cases”, CitizenLab, October 29, 2019, https://bit.ly/3j5YU2m

حقوق بشر و شرکت‌های فناوری در ایران

وقتی صحبت بر سر رابطه‌ی درهم تنیده‌ی میان شرکت‌های فناوری و حقوق بشر باشد، نمی‌توان شرکت‌های فناوری در ایران را از این موضوع مستثنی دانست. در اینجا فهرستی از چند رویداد در ایران ارائه می‌کنیم تا نگرانی‌های نوظهور در مورد شرکت‌های فناوری و حقوق بشر را با دقت بیشتری بررسی کنیم، به‌خصوص نگرانی‌هایی در زمینه حفاظت از اطلاعات کاربران، حذف محتوا، درخواست‌های دولت، ابهام در مورد اعمال دستورالعمل برای کاربران، میزان شفافیت شرکت و غیره.

مثال ۱
نسخه‌های غیررسمی تلگرام و نشت اطلاعات کاربران

در فروردین ۱۳۹۹، خبر نشت اطلاعات ۴۲ میلیون کاربر از نسخه‌های غیررسمی تلگرام، از جمله هات‌گرام و طلاگرام، اعلام شد. این اطلاعات شامل نام‌های کاربری، شناسه‌ها، شماره تلفن‌ها و موقعیت آخرین اتصال کاربران به این اپلیکیشن‌ها بود.[۲۶] بعد از چند روز وبسایتی که این اطلاعات را میزبانی می‌کرد، امکان دسترسی به داده‌ها را قطع کرد، با این حال، واضح است که این مسئله باعث به خطر افتادن حریم شخصی کاربران شد. این اولین باری نبود که حامیان حقوق دیجیتال درباره نسخه‌های غیررسمی تلگرام، اظهار نگرانی کرده بودند. در طول انتخابات مجلس در سال ۱۳۹۸، تعداد زیادی از کاربران ناخواسته به گروه‌های تلگرامی این نسخه‌های غیررسمی اضافه شده بودند.[۲۷] این‌طور تصور می‌شود که با دادن قول مقداری پول، این گروه‌های تلگرامی از کاربران می‌خواستند تا جای ممکن کاربران بیشتری به گروه دعوت کنند. هر چقدر تعداد کاربرانی که به اجبار وارد این گروه‌ها می‌شدند بیشتر بود، فرد دعوت‌کننده پول بیشتری دریافت می‌کرد!

مثال‌های بالا نشان می‌دهد که وقتی خدمات دیجیتالی در هنگام جمع‌آوری و ذخیره اطلاعات، از ضمانت‌های لازم جهت حفاظت از داده‌ها برخوردار نیستند، حریم خصوصی ما بسیار آسیب‌پذیر خواهد بود. بدون وجود شفافیت درباره نحوه‌ی جمع‌آوری اطلاعات کاربران، نحوه‌ی ذخیره‌ی این اطلاعات و اینکه چه کسانی به این اطلاعات دسترسی خواهند داشت، تقریباً غیرممکن است که در زمان وقوع چنین خساراتی بتوان کسی را پاسخگو نگه داشت. مثال فوق این واقعیت را نشان می‌دهد که هر اپلیکیشن پیام‌رسانی می‌بایست اصول «طراحی بر مبنای حریم خصوصی» یا "privacy by design" را بکار گرفته و امکان کنترل وضعیت حریم خصوصی را برای کاربران ایجاد کند تا از چنین مواردی جلوگیری شود.[۲۸]

موضوع دیگر این است که هات‌گرام و تلگرام طلایی هر دو نسخه‌های غیررسمی تلگرام هستند و قابل دانلود ازفروشگاه‌های ارائه‌کننده اپلیکیشن‌ها. جدا از سازنده‌ی این اپلیکیشن‌ها، این مسئله نشان می‌دهد که فروشگاه‌های ارائه‌کننده اپلیکیشن‌ها (مثل کافه بازار، مایکت یا سیب‌اپ) هم به دلیل میزبانی این اپلیکیشن‌ها مسئولیتی بر عهده دارند. هر چند که نباید تمام مسئولیت را بر دوش فروشگاه‌های ارائه‌کننده اپلیکیشن‌ها بگذاریم، بلکه می‌بایست شرایط و مقررات سرویس‌دهی API (رابط برنامه‌نویسی کاربردی) تلگرام را نیز زیر سوال ببریم. تلگرام تا چه حد می‌توانسته روی روش‌هایی که توسعه‌دهندگان از API تلگرام برای ساخت بات‌ها و نسخه‌های تقلبی استفاده می‌کنند، نظارت و بررسی داشته باشد؟

مثال ۲
تاکسی ماکسیم و درخواست شهرداری تهران

در فروردین ۱۳۹۸، شهرداری تهران از اپلیکیشن تاکسی ماکسیم خواست تا به «اطلاعات خام و پردازش شده» کاربرانش دسترسی پیدا کند. حمید برزگر، مدیر عامل این شرکت، این درخواست را رد کرد. او اشاره کرد که اطلاعات

26 Melody Kazemi, "Data Insecurity On Iran's Localised Internet," Filterwatch, Jun 19, 2020, https://bit.ly/2H80a7J
27 "Add Your Friends, Make Money!," ISNA, February 15, 2020, https://bit.ly/31cSxEk
28 "A Guide to Privacy by Design," October 2019, https://bit.ly/3nVlkXJ

کاربران آن‌ها، خط قرمز این شرکت است و آنها از این خط قرمز نمی‌گذرند. برزگر اضافه کرد که نمی‌خواهد اعتمادی که شرکتش بین کاربران خود به‌دست آورده را با قبول این درخواست، به خطر بیندازد و در ادامه گفت که اطلاعات کاربران نباید به اشتراک گذاشته شود، مگر تحت شرایطی خاص که حکم دادگاه از مقامی رسمی در قوه قضاییه جهت این درخواست وجود داشته باشد.[۲۹]

این مورد نشان می‌دهد که در نبود روند شفاف قانونی، هر شخص و نهاد غیرقضایی می‌تواند به راحتی برای دسترسی پیدا کردن به داده‌های خصوصی درخواست ارائه دهد. همچنین نشان می‌دهد که شرکت‌ها موظفند در برابر درخواست‌هایی که از مجاری رسمی و قانونی عبور نکرده‌اند مقاومت کنند.

مثال ۳
دیجی‌کالا و شناسایی هویت

یک کاربر ایرانی روی توییتر در مورد ایمیلی که از دیجی‌کالا — یک استارتاپ فروش دیجیتالی کالا در ایران— دریافت کرد ابراز نگرانی کرد. این شرکت از فرد مورد نظر درخواست کرده بود نسخه‌های اسکن شده از کارت ملی و کارت‌های بانکی خود را در اختیار شرکت قرار دهد. طبق رشته توییت این کاربر، دیجی‌کالا از وی خواسته بود که کپی کارت‌های او را دریافت کند تا هویتش را تایید و هزینه کالای پس‌داده شده را به او پرداخت کنند.[۳۰] اما درخواست دسترسی به اطلاعات حساس کاربران از طریق ایمیل نقض حریم خصوصی محسوب می‌شود و امنیت کاربران را به خطر می اندازد. همچنین مشخص نیست که کدام یک از کارمندان و چه تعدادی از آنها در دیجی‌کالا می‌توانند به این کپی کارت ملی دسترسی داشته باشند، یا اینکه دیجی‌کالا برای چه مدتی این اطلاعات را نگهداری می‌کند. این نمونه، این نگرانی را ایجاد می‌کند که چه شرکت‌های دیگری ممکن است بدون در نظر گرفتن پروتکل‌های امنیت سایبری چنین درخواست‌های نابجایی را برای دسترسی به اطلاعات حساس افراد داشته باشند، بدون اینکه این کارشان با مانعی روبه‌رو شود و چه تعداد از شرکت‌ها به خاطر چنین اعمالی از کاربران خود عذرخواهی کرده و سعی می‌کنند تا به شکل مناسبی این آسیب را جبران کنند؟

مثال ۴
سرویس‌های وبلاگ فارسی و حذف محتوا

در سال ۱۳۸۹، مدیران سه سرویس وبلاگ فارسی، بلاگفا، میهن بلاگ و بلاگ اسکای نامه‌ای سرگشاده منتشر کردند تا ناخشنودی خود را از فیلترینگ دولتی روی وب‌سایت‌های خود اعلام کنند.[۳۱] آنها در این نامه، به این موضوع اشاره کردند که گاهی اوقات بر اساس تصمیم «کارگروه تعیین مصادیق محتوای مجرمانه» که مسئول جلوگیری از انتشار محتوای «غیراخلاقی» است، وبلاگی تنها به خاطر پستی که سال‌ها پیش نوشته شده است، می‌بایست به کل مسدود می‌شد. این مدیران اشاره کردند که به منظور درخواست تجدیدنظر، صاحبان این وبلاگ‌ها مجبور هستند تا به صورت حضوری به دفتر این نهاد مراجعه کنند و برای رفع مسدودیت وبلاگ‌های خود اجازه بگیرند. این نوع برخوردها، نه تنها موجب نقض حق آزادی بیان در فضای آنلاین می‌شود، بلکه به گفته مدیران این وبلاگ‌ها، تاثیر مخربی داشته و کاربران ایرانی را به انتخاب سرویس‌های وبلاگی غیرایرانی به جای سرویس‌های داخلی سوق می‌دهد. نویسندگان این نامه از این نهاد خواستند تا به آنها اجازه دهد تا به جای اینکه بدون هیچ اطلاع قبلی وبلاگ این افراد را مسدود کنند، حداقل ابتدا هشداری به وبلاگ‌نویس‌ها بدهند.

29 Arash Karimbeigi, “Maxim Taxi: The Municipality wants our Customer Data,” ICTAna, April 14, 2019, https://bit.ly/2HbyPkW

30 Twitter thread from an Iranian user, Twitter, April 18, 2020, https://bit.ly/3j1dmbL

31 “Performance of the Filtering Organisation and the Weakening Position of Farsi Weblog Services,” BlogFa, December 4, 2010, https://bit.ly/3443sBT

شفافیت و مسئولیت‌پذیری در شرکت‌های فناوری

در بخش قبل درباره‌ی اینکه چطور روش کار شرکت‌های فناوری می‌تواند به نقض حقوق دیجیتال ختم شود، صحبت کردیم. اما نمونه‌هایی را نیز مشاهده کردیم که سیاست برخی از این شرکت‌ها نقش مثبتی در حفاظت از شهروندان ایرانی در مقابل درخواست‌های نابجای نهادهای حکومتی بازی کرده است، درخواست‌هایی که ناقض احترام به حقوق دیجیتال کاربرانند.

با وجود اینکه سیاست‌های شرکت‌های فناوری در هر کشوری وابسته به نظام سیاسی، ساختار اقتصادی و چارچوب‌های قانونی آن کشور است، اما همچنان شباهت‌های فراوانی میان رویکرد شرکت‌ها به مسائل مربوط به حقوق دیجیتال وجود دارد. در اینجا نگاهی می‌اندازیم به برخی منابع که بر اساس اصول پذیرفته شده‌ی بین‌المللی مطرح شده‌اند. این منابع به حامیان حقوق بشر کمک می‌کند تا سیاست‌های شرکت‌های فناوری را ارزیابی کنند و آن‌ها را در جهت روش‌های همسو با حقوق بشر، هدایت کنند.

اصول راهنمای تجارت و حقوق بشر سازمان ملل

یکی از چارچوب‌های پذیرفته شده بین‌المللی برای توضیح وظایف حقوق بشری شرکت‌ها، «اصول راهنمای تجارت و حقوق بشر سازمان ملل» است.[۳۲] در سال ۲۰۱۱ شورای حقوق بشر سازمان ملل متحد به اتفاق آرا این دستورالعمل را به عنوان چارچوب رسمی برای تجارت و حقوق بشر، قابل اجرا در هر کشور و شرکت تجاری در دنیا، تایید کرد. این راهنما از ۳۱ اصل تشکیل شده که به سه محور اصلی تقسیم شده‌اند: وظیفه حکومت در حفظ حقوق بشر، وظیفه شرکت‌ها در احترام به حقوق بشر، و وظیفه حکومت‌ها و شرکت‌ها در جبران خسارات.

همچنین حائز اهمیت است که با احترام به حقوق بشر و پیروی از چارچوب‌های بین‌المللی، شرکت‌ها با ریسک‌ها کمتری در زمینه‌های مالی، اعتباری و قانونی مواجه خواهند بود، چرا که از این طریق اعتماد کاربران خود را کسب می‌کنند، از تحریم و بایکوت علیه خودشان جلوگیری می‌کنند، از شرکت‌های رقیب پیشی می‌گیرند و مشارکت‌های بین‌المللی و سرمایه‌گذاری‌های فراملی بیشتری را به خود جذب می‌کنند. این موضوع به‌خصوص برای شرکت‌های نوپایی که می‌خواهند بازار خود را فرای مرزهای ایران گسترش دهند، بسیار اهمیت دارد. بر اساس سنجش آماری نصر (سازمان نظام صنفی رایانه‌ای کشور) از ۳۴۷ شرکت نوپا یا استارتاپ ایرانی، ۱۱.۸٪ از گفته‌اند که در بازارهای بین‌المللی فعالیت می‌کنند و امیدوارند تا حضور بین‌المللی خود را در آینده نزدیک پررنگ‌تر کنند.[۳۳] این شرکت‌ها باید بدانند که برای ورود و فعالیت دربازارهای بین‌المللی، موظفند طبق استانداردهای بین‌المللی هم عمل کنند.

ارزیابی تعهدات شرکت‌های فناوری به اصول حقوق بشر

اصول راهنمای تجارت و حقوق بشر سازمان ملل برای تمام صنایع از جمله بخش فناوری اطلاعات و ارتباطات، قابل اجرا است. برای اینکه این دستورالعمل برای شرکت‌های فناوری و اطلاعات، کاربردی‌تر باشد، محققان فناوری و حقوق بشر منابعی را فراهم کرده‌اند تا شرکت‌ها را ارزیابی کنند و آن‌ها را به سمت روش‌های منطبق با حقوق بشر هدایت کنند. یکی از این منابع، «شاخص رتبه‌بندی مسئولیت شرکت‌ها

32 The UN guiding Principles on Business and Human Rights, HR/PUB/11/04, United Nations, 2011, https://bit.ly/2IyyOZ7

33 “An Analysis of of the Startup Space in Iran”, Computer Guild Organisation of Iran, November/December 2019, https://bit.ly/3j0MkS1

چارچوب سه رکنی در اصول راهنمای تجارت و حقوق بشر سازمان ملل

رکن اول وظیفه حکومت در حفاظت از حقوق بشر

دولت‌ها می‌بایست از طریق ایجاد قوانین، نظارت و سیاست‌گذاری‌ها به حفاظت از حقوق بشر پرداخته و اطمینان حاصل کنند که عملکرد شرکت های تجاری، موجب تعدی به حقوق بشر نمی‌شود.

رکن دوم وظیفه شرکت‌ها در احترام به حقوق بشر

شرکت‌های تجاری، فارغ از اینکه چه ابعادی دارند، مربوط به چه بخشی هستند و از چه مدل مالکیتی پیروی می‌کنند، می‌بایست در تمام بخش‌های کاری خود به حقوق بشر احترام بگذارند.

برای پایبندی به وظایف خود، می‌بایست به سنجش صلاحیت‌های حقوق بشری خود بپردازند. این سنجش شامل مراحل زیر است:

- داشتن سیاست‌گذاری حقوق بشری که به شکل همگانی در دسترس عموم باشد؛
- اجرای سنجش‌های اثرات حقوق بشر به این منظور که بفهمند چگونه خدمات، فعالیت‌ها و روابط تجاری‌شان می‌تواند تاثیرات منفی بر حقوق بشر داشته باشد؛
- اعمال یافته‌های سنجش‌ها در عملکرد شرکت و سیاست‌گذاری‌های خود؛
- پیگیری عکس‌العمل‌ها در مورد تاثیرات منفی شناسایی شده و اطلاع‌رسانی در مورد اقدامات لازم برای رفع آن‌ها.

رکن سوم وظیفه حکومت‌ها و شرکت‌ها در جبران خسارات

زمانی که حقوق بشر به دلیل خدمات و فعالیت‌های تجاری نقض می گردد، هم دولت و هم شرکت‌ها مسئولیت دارند از دسترسی قربانیان به راه حل موثر برای جبران خسارات اطمینان حاصل کنند.

[Fig 3]

در قبال حقوق دیجیتال» یا شاخص RDR است، که در سراسر جهان، قدرتمندترین شرکت‌های اینترنتی، خدمات تلفن همراه و مخابراتی را، براساس سیاست‌های علنی آنها در زمینه آزادی بیان و حریم خصوصی کاربران ارزیابی می‌کند.[۳۴]

34 “2019 Ranking Digital Rights Corporate Accountability Index”, Ranking Digital Rights, https://bit.ly/2SZb42l

رتبه‌بندی براساس حقوق دیجیتال: مسئولیت و شفافیت در شرکت‌های فناوری ایرانی

در این پروژه، از روش پژوهش مطرح شده در شاخص RDR سال ۲۰۱۹، برای ارزیابی تعهدات شرکت‌های فناوری در ایران به حقوق دیجیتال استفاده کردیم. در حالی که این شاخص بر حق برخورداری از حریم شخصی و حق آزادی بیان تمرکز دارد، مخاطب این نوشته باید این مطلب را درنظر بگیرد که تمامی حقوق بشر، مرتبط، وابسته به یکدیگر و تفکیک‌ناپذیر، هستند. نقض هرحق می‌تواند موجب پایمالی حق دیگر شود، و حفظ یکی از این حقوق می‌تواند ضامن برآورده کردن حق دیگری باشد. پیامدهای نقض حریم خصوصی در فضای آنلاین و آزادی بیان، به‌خصوص در مورد گروه‌های آسیب‌پذیرتر جامعه، از محدوده این حقوق فراتر می‌رود و روی سایر حقوق مدنی، سیاسی، فرهنگی، اجتماعی و اقتصادی افراد تاثیر منفی می‌گذارد. برای مثال، این یک حقیقت است که دولت ایران با نپذیرفتن بهاییان به دانشگاه‌های کشور، حق آنها را برای دسترسی به تحصیلات عالی محدود می‌کند. در نتیجه ممکن است این گروه اقلیت مذهبی برای برآوردن حق طبیعی خود، یعنی آموزش عالی، به فضاهای آنلاین اتکا کنند.[۳۵] حال تصور کنید که به دلیل عدم رعایت امنیت سایبری از طرف یک سرویس یا اپلیکیشن اینترنتی و یا به دلیل همدستی شرکت فراهم‌کننده‌ی این سرویس با نهادهای حکومتی ایران، نشت یا واگذاری داده‌ای اتفاق بیفتد. در این صورت، می‌بینیم که این فقط حق کاربران به حریم خصوصی نیست که زیر پا گذاشته می‌شود، بلکه ممکن است حق تحصیل، آزادی عقیدتی و مذهبی، و حتی حق زندگی، آزادی و امنیت نیز به خطر بیافتد.

ما به دلایل ذیل تصمیم گرفتیم تا از روش پژوهش شاخص RDR استفاده کنیم:

1. روش پژوهش شاخص RDR بر اساس چارچوب‌های حقوق بشر که به صورت بین‌المللی پذیرفته شده‌اند، تهیه شده است و با اصول راهنمای تجارت و حقوق بشر سازمان ملل مطابقت دارد. این روش مختص به ناحیه یا کشور خاصی نیست، بلکه شیوه‌ای جهانی است.

2. این روش با فراهم آوردن ۳۵ مولفه مرتبط با حریم خصوصی، آزادی بیان و سیاست‌گذاری شرکت — و ارائه چندین زیرمولفه برای هر یک از این مولفه‌ها — نه تنها برای ارزیابی و رتبه‌بندی شرکت‌ها استفاده می‌شود، بلکه می‌تواند ابزاری کاربردی باشد تا شرکت‌ها نقاط ضعف و قوت خود را بررسی کنند. این روش همچنین به محققان حوزه‌ی حقوق دیجیتال کمک می‌کند تا بر اساس بررسی دقیق هر کدام از مولفه‌ها، پیشنهادهای کاربردی‌تری به شرکت‌ها ارائه دهند.

3. محققان حوزه حقوق دیجیتال در کشورهای مختلف (از جمله روسیه، کنیا، سنگال، کشورهای عربی، هند، پاکستان) نیز این روش را برای ارزیابی شرکت‌ها در کشورهای خود به کار گرفته‌اند و برای هدایت شرکت‌ها به سمت شیوه‌های مطابق با حقوق بشر از آن استفاده می‌کنند[۳۶]. ما امیدواریم با اضافه کردن تحقیقی در زمینه‌ی شرکت‌های فناوری ایرانی به فهرست در حال افزایش پروژه‌هایی RDR تصویر واضح‌تری از وضعیت حقوق دیجیتال و بخش خصوصی، بالاخص در کشورهایی با نظام سیاسی بسته و نیمه‌بسته در گفتمان جهانی ارائه کنیم.

در این گزارش، ما روش پژوهش RDR را روی شرکت‌های سازنده اپلیکیشن‌های پیام‌رسان اعمال کردیم. با وجود

35 Tara Sepehri Far, “Glimmer of Hope in Iran for Long-Persecuted Baha’is?,” Human Rights Watch, Jan. 29, 2019, https://www.hrw.org/news/2019/01/29/glimmer-hope-iran-long-persecuted-bahais, https://www.hrw.org/news/2019/01/29/glimmer-hope-iran-long-persecuted-bahais and “Iran: Allow Baha’i Students Access to Higher Education,” Human Rights Watch, Sep. 19, 2007, https://www.hrw.org/news/2007/09/19/iran-allow-bahai-students-access-higher-education

36 “What are Human Rights,” The Office of the High Commissioner for Human Rights (UN Human Rights), https://bit.ly/2TwHFwG

37 Mark Zuckerberg, “A Privacy-Focused Vision for Social Networking,” Facebook, March 6, 2019, https://bit.ly/3k82UAO

تصمیم ما برای بررسی اپلیکیشن‌های پیام‌رسان، خواننده این گزارش باید بداند که تقریبا تمام مولفه‌های استفاده شده در این تحقیق، روی دیگر خدمات و شرکت‌های اینترنتی نیز قابل اجرا هستند. دلایل ما برای انتخاب اپلیکیشن‌های پیام‌رسان این است که:

1. در تمام دنیا، محبوبیت و کاربرد اپلیکیشن‌های پیام‌رسان در زندگی مردم بیش از پیش در حال افزایش است. در ماه مارس سال ۲۰۱۹، مارک زاکربرگ، مدیرعامل فیسبوک، در این رابطه گفت که «اهمیت پلتفرم‌های ارتباطی که بر حریم خصوصی متمرکز هستند، در آینده حتی از پلتفرم‌های عمومی کنونی نیز بیشتر خواهد شد». و اینکه «آینده ارتباطات هر چه بیشتر به سمت خدماتی پیش خواهد رفت که خصوصی هستند و قابلیت رمزگذاری شدن دارند.»[۳۷] علاوه بر این، طبق طبقه‌بندی We Are Social، سرویس‌های پیام‌رسان، بعد از فیس‌بوک و یوتیوب، از جمله پراستفاده‌ترین خدمات در تمام دنیا هستند.[۳۸] ایران نیز از این روند جهانی مستثنی نیست. در ایران، با در نظر گرفتن این موضوع که رسانه‌ها یا در انحصار حکومت هستند و یا آزادی‌شان بسیار محدود است، سرویس‌های پیام‌رسان نقش بسیار مهمی برای برآورده کردن حق دسترسی به اطلاعات و آزادی بیان بازی می‌کنند. قبل از اینکه تلگرام فیلتر شود، این اپلیکیشن ۴۰ میلیون کاربر در ایران داشت[۳۹] و پیام‌رسان واتس‌اپ، ۳۳ میلیون بار از کافه بازار دانلود شده بود.[۴۰] حتی سرویس‌های پیام‌رسان داخلی بر روی کافه بازار جزو اپلیکیشن‌هایی هستند که تعداد دانلود قابل توجهی دارند.

2. دولت با حمایت‌های مالی و حقوقی خود، اپلیکیشن‌های پیام‌رسان را در مرکز برنامه‌ی بومی‌سازی اینترنت ایران قرار داده است. محمد جواد آذری جهرمی، وزیر کنونی ارتباطات و فناوری اطلاعات، در موقعیت‌های متعددی، حمایت خود را از اپلیکیشن‌های پیام‌رسان داخلی ابراز کرده است.[۴۱] در صورت تصویب پیش‌نویس کنونی «طرح ساماندهی پیام‌رسان‌های اجتماعی»، و با در نظر گرفتن فقدان قوانین سفت و سخت برای حفاظت از اطلاعات کاربران در ایران، این طرح موجب ایجاد تغییرات زیادی در اپلیکیشن‌های پیام‌رسان خواهد شد و بیش از امروز راه را برای کنترل و نظارت حکومتی روی این اپلیکیشن‌ها هموار خواهد کرد.[۴۲] علاوه بر این، دولت برای پیشبرد مقاصد حکومتی بومی‌سازی اینترنت، تصمیم گرفت تا تعرفه‌های اینترنت (دیتا) برای اپلیکیشن‌های پیام‌رسان داخلی را کاهش دهد.[۴۳] همچنین برای تشویق بیشتر کاربران به استفاده از این سرویس‌ها، نهادهای متعدد دولتی و بانک مرکزی ایران با پیام‌رسان‌های داخلی، همکاری کرده تا ویژگی‌های بانکداری الکترونیک و خدمات دولت الکترونیک به این اپلیکیشن‌ها اضافه گردد. برای مثال در فروردین ۱۳۹۹، در واکنش به همه‌گیری کووید-۱۹ و بسته شدن مدارس، وزارت آموزش و پرورش، اپلیکیشنی را به نام «شاد» به عنوان اپلیکیشن رسمی آموزش الکترونیکی برای استفاده دانش‌آموزان و معلمان ارائه داد که در اصل روی زیرساخت یک پیام‌رسان بومی پیاده شده است.[۴۴]

دو دلیل فوق نشانگر اهمیت نقشی است که اپلیکیشن‌های پیام‌رسان در زندگی شخصی و حرفه‌ای

38 Claire Wardle, “Monitoring and Reporting Inside Closed Groups and Messaging Apps,” Verification Handbook 3, https://bit.ly/3lSGO5M
39 “How Many Iranian Telegram and Domestic Messaging App Users are There,” IRNA , May 22, 2019, https://bit.ly/2T2jRk9
40 WhatsApp Download Page, Cafe Bazaar, https://bit.ly/31cTUmm
41 “Jahromi: We are Obligated to Support Domestic Messaging Apps”, IRINN, May 23, 2018, https://bit.ly/37fd6DY
42 Melody Kazemi, “Policy Monitor - July 2020,” Filterwatch, Aug. 14, 2020, https://bit.ly/3gxr2Kv
43 “Use Domestic Messaging Apps with 1/3 [Data] Traffic”, Pars Online, https://bit.ly/37aTnVI
44 “Student Social Network (SHAD) is Ready for Operation,” Iran’s Ministry of Education, April 9, 2020, https://bit.ly/3k76KKh
45 Abeba Birhane, “The Algorithmic Colonization of Africa,” July 18, 2019, Real Life, https://bit.ly/342wmSR

مردم ایران، و در رابطه با حقوق مدنی، سیاسی، اقتصادی، اجتماعی و فرهنگی آن‌ها، بازی می‌کند. به طور خلاصه می‌توان گفت، **ارزیابی اپلیکیشن‌های پیام‌رسان، می‌تواند نقطه شروع و آزمونی باشد برای شناسایی نقاط قوت و ضعف شرکت‌های نوپای فناوری در ایران.**

این گزارش برای چه کسانی تهیه شده است؟

این گزارش — و راهنمای ضمیمه شده به آن— برای این گروه‌ها طراحی شده است:

- **شرکت‌های فناوری در ایران** که می‌بایست احترام به حقوق بشر را جز تعهدات خود بدانند و از کاربران خود محافظت کنند. بخش رتبه‌بندی به شرکت‌ها کمک می‌کند تا نقاط قوت و ضعف خود را یافته، و خود را با رقبایشان مقایسه کنند.

راهنمای ضمیمه شده به شرکت‌ها این امکان را می‌دهد تا بحث درباره‌ی حقوق دیجیتال را از درون شرکت آغاز کنند. این راهنما به شرکت‌ها کمک می‌کند تا با آگاهی، مسائل مربوط به حقوق دیجیتال را درلایه‌های مختلف یک شرکت، از جایگاه مدیران ارشد، اعضای هیئت مدیره، طراحان و متخصصان فناوری، مدیریت منابع انسانی و همین‌طور گروه‌های حقوقی و روابط عمومی خود، بررسی کنند و راه درست محافظت از حقوق کاربرانشان را بیابند.

علاوه بر این، این گزارش به سرمایه‌گذاران ایرانی و خارجی این امکان را می‌دهد تا عملکرد شرکت‌ها را بر مبنای میزان احترام‌شان به استانداردهای بین‌المللی بررسی کنند. سرمایه‌گذاران می‌توانند از مولفه‌های حریم خصوصی، آزادی بیان و سیاست‌گذاری شرکت استفاده کرده و پیشینه شرکت‌ها را در رابطه با حقوق دیجیتال ارزیابی، و با آگاهی کامل برای سرمایه‌گذاری تصمیم بگیرند.

فعالان جامعه مدنی، روزنامه‌نگاران و پژوهشگرانی که در داخل و خارج از ایران به ارزیابی خدمات اینترنتی می‌پردازند و به کاربران کمک می‌کنند تا در انتخاب این خدمات تصمیم‌های بهتری بگیرند. با اینکه ما فقط چند اپلیکیشن پیام‌رسان را در این تحقیق بررسی کردیم، این گزارش و راهنمای ضمیمه آن به حامیان حقوق دیجیتال در داخل ایران کمک می‌کند تا اپلیکیشن‌های تلفن همراه و اینترنتی دیگر را نیزمورد ارزیابی قرار دهند و آن‌ها را بر اساس مولفه‌های حقوق دیجیتال با هم مقایسه کنند. این موضوع نه تنها کمک می‌کند تا این روزنامه‌نگاران و پژوهشگران بتوانند خواستار شفافیت بیشتر و استانداردهای بالاتری از شرکت‌ها باشند، بلکه این امکان را فراهم می‌کند تا سیاست‌های دولت را در رابطه با حقوق دیجیتال و شرکت‌های فناوری موشکافی کنند. ما هم‌چنین از پژوهشگران امنیت سایبری می‌خواهیم تا از این گزارش برای آزمودن محصولات شرکت‌ها استفاده کرده و از این موضوع اطمینان حاصل کنند که آنچه این شرکت‌ها درباره استانداردهای فنی خود اظهار می‌کنند، با عمل مطابقت داشته باشد.

- **کاربرانی** که می‌خواهند از خود در مقابل آسیب‌های اینترنتی محافظت کنند و در هنگام انتخاب خدمات اینترنتی، حقوق دیجیتال را در مرکز تصمیم‌گیری خود قرار دهند.

- **پژوهشگران حوزه حقوق دیجیتال و دست‌اندرکاران حوزه‌ی تجارت و حقوق بشر** که قصد دارند از روش پژوهش RDR برای بررسی شرکت‌های فناوری در نظام‌های بسته و نیمه‌بسته‌ی سیاسی استفاده کنند. این گزارش می‌تواند به حامیان حقوق دیجیتال در سطح جهانی کمک کند تا ریزه‌کاری‌های استراتژی بومی‌سازی اینترنت را بهتر درک کنند. فعالیت ما به پژوهشگران حقوق دیجیتال کمک می‌کند تا بتوانند بین موضوع بومی‌سازی اینترنت — که به خاطر سیاست‌های تحمیلی دولت‌ها به صورت مخربی اتفاق می‌افتد—، از یک سو، و روش‌های بی‌قاعده و استثمارگرایانه شرکت‌های بزرگ چند ملیتی در قبال کشورهای در حال توسعه —روندی که معمولاً به

عنوان «استعمار دیجیتالی» از آن یاد می‌شود— از سوی دیگر، راه متعادلی بیابند[۳۵].

جمع آوری داده و تجزیه و تحلیل

بخش تحقیق این گزارش از ژانویه تا سپتامبر ۲۰۲۰ صورت گرفته است.

مرحله ۱

از ژانویه تا ماه مه ۲۰۲۰، اولین محقق سیاست‌گذاری‌های مربوط به حریم خصوصی، شرایط و ضوابط استفاده از خدمات، سوالات متداول، پست‌های وبلاگی و دیگر مدارک (یا محتوای چندرسانه‌ای) را جمع‌آوری و بررسی کرد. لازم به ذکر است که ما فقط منابعی را که از سوی آن شرکت به صورت رسمی منتشر شده‌اند، در دسترس عموم هستند و برای دسترسی به آنها نیازی به ساختن حساب کاربری و ثبت‌نام در وبسایت نبوده است، جمع‌آوری کرده‌ایم. بر اساس این مدارک، شرکت پیام‌رسان مورد نظر در مجموع بر اساس ۳۳ مولفه‌ی RDR (مشتمل بر مجموعا ۱۵۸ زیرمولفه) ارزیابی شد. این مولفه‌ها به سه گروه «حریم خصوصی»، «آزادی بیان» و «سیاست‌گذاری شرکت» تقسیم شده‌اند. لازم به ذکر است که شاخص RDR، شرکت‌ها را بر اساس شیوه‌ها و سیاست‌گذاری‌های علنی آنها که بر موضوعات حریم خصوصی و آزادی بیان تاثیر می‌گذارند، رتبه‌بندی می‌کند. این روش نه محصولات شرکت‌ها را از نظر فنی تست می‌کند و نه سیاست‌گذاری‌های غیرعلنی آنها را ارزیابی می‌کند.[۳۶]

۱۵۸ زیرمولفه‌ی «حریم خصوصی»، «آزادی بیان» و «سیاست‌گذاری شرکت» به این شکل امتیازگذاری شدند:

برای هر زیرمولفه، ۳ نوع امتیاز در نظر گرفته شد:

- اگر شرکت شفافیت کاملی در مورد سیاست‌های خود در قبال آن زیرمولفه ارائه داد، امتیاز ۱۰۰ به آن زیرمولفه تعلق گرفت. شفاف‌سازی کامل به این معنی است که اظهارات یک شرکت، اینطور نشان می‌دهد که شروط لازم برای موضوع خاص مطرح‌شده در یک زیرمولفه را داراست.

- اگر شرکت شفافیتی در مورد سیاست‌های خود در قبال زیرمولفه‌ای ارائه داد ولی میزان شفافیت کافی نبود، امتیاز ۵۰ به آن زیرمولفه تعلق گرفت. شفاف‌سازی ناکافی به این معناست که ما توانستیم اطلاعاتی درباره وجود سیاست‌های لازم در آن زیرمولفه پیدا کنیم اما اظهارات آن شرکت به اندازه کافی شفاف و کامل نبوده است.

- اگر شرکت هیچ شفافیتی در مورد سیاست‌های خود در قبال زیرمولفه‌ای ارائه نداد و یا سیاست‌هایی در خلاف آن زیرمولفه ارائه داد امتیاز صفر به آن زیرمولفه تعلق گرفت.

برای اطلاعات بیشتر درباره هر کدام از مولفه‌ها و زیرمولفه‌های مربوط به هر شرکت پیام‌رسان به **این لینک** مراجعه کنید.

امتیاز نهایی برای هر مولفه را با جمع امتیازات هر یک از زیرمولفه‌ها، تقسیم بر تعداد زیرمولفه، محاسبه کردیم.

مرحله ۲

دومین محقق امتیاز داده شده از سوی محقق اول به هر یک از زیرمولفه‌ها را صحت‌سنجی کرد.

مرحله ۳

اولین محقق، نتایج را با هم مقایسه کردند تا از تطابق این ارزیابی اطمینان حاصل پیدا کنند.

46 این موضوع از این لحاظ حائز اهمیت است که گاهی اوقات شرکتی در عمل دارای شروط لازم برای آزادی بیان و یا حفظ امنیت است (مثلا سیاست‌های لازم برای مقابله با درخواست‌های دولت برای دسترسی به داده را دارد یا از پژوهشگران امنیت سایبری می‌خواهد تا سرویس آنها را مورد بررسی قرار دهند)، اما این موضوع را به صورت علنی اظهار نمی‌کند. برعکس این حالت هم ممکن است پیش بیاید، اینکه شرکتی اظهار کند که سیاست‌های لازم را به کار می‌گیرد ولی در واقع این سیاست‌ها را اعمال نمی‌کند.

مرحله ۴

محقق سوم نحوه‌ی امتیازگذاری هر کدام از زیرمولفه‌ها را بین تمامی شرکت‌ها مقایسه کرد تا از تطابق این ارزیابی برای همه‌ی شرکت‌ها اطمینان حاصل کند.

مرحله ۵

تیم محققان امتیازات نهایی را حساب کرده و پیش‌نویس گزارش را تهیه کردند.

مرحله ۶

گزارش به دست پژوهشگران در RDR و همینطور سه پژوهشگر دیگر متخصص در حوزه‌ی حقوق دیجیتال (یک حقوقدان، یک متخصص اداره امور شبکه‌های اجتماعی و یک متخصص امنیت سایبری) که هر سه فارسی زبان بوده‌اند بازبینی شد.

مرحله ۷

راهنمای ضمیمه برای کمک بیشتر به شرکت‌ها تهیه شد تا بتوانند وظایف خود را در رابطه با حقوق دیجیتال مورد توجه قرار دهند. راهنمای ضمیمه را از **اینجا** دانلود کنید.

نتایج تحقیق

ما شفاف‌سازی تمام شرکت‌ها را بر اساس مولفه‌های آزادی بیان و حریم خصوصی ارزیابی کردیم. شما می‌توانید فهرست کامل مولفه‌ها و زیر-مولفه‌ها را در پیوست این گزارش و همینطور در **این صفحه** ببینید. برای خلاصه‌سازی و مصور کردن نتایج، مولفه‌های حریم خصوصی و آزادی بیان را به شش دسته‌ی اصلی تقسیم کردیم:

- هر شش شرکت مورد بررسی، در زمینه شفاف‌سازی از نقطه مطلوب فاصله‌ی زیادی دارند. واتس‌اپ با امتیاز ۴۸.۱۹ از ۱۰۰ رتبه اول و «گپ»با امتیاز ۱۲.۶۳ از ۱۰۰ پایین‌ترین رتبه را به خود اختصاص داده‌اند.

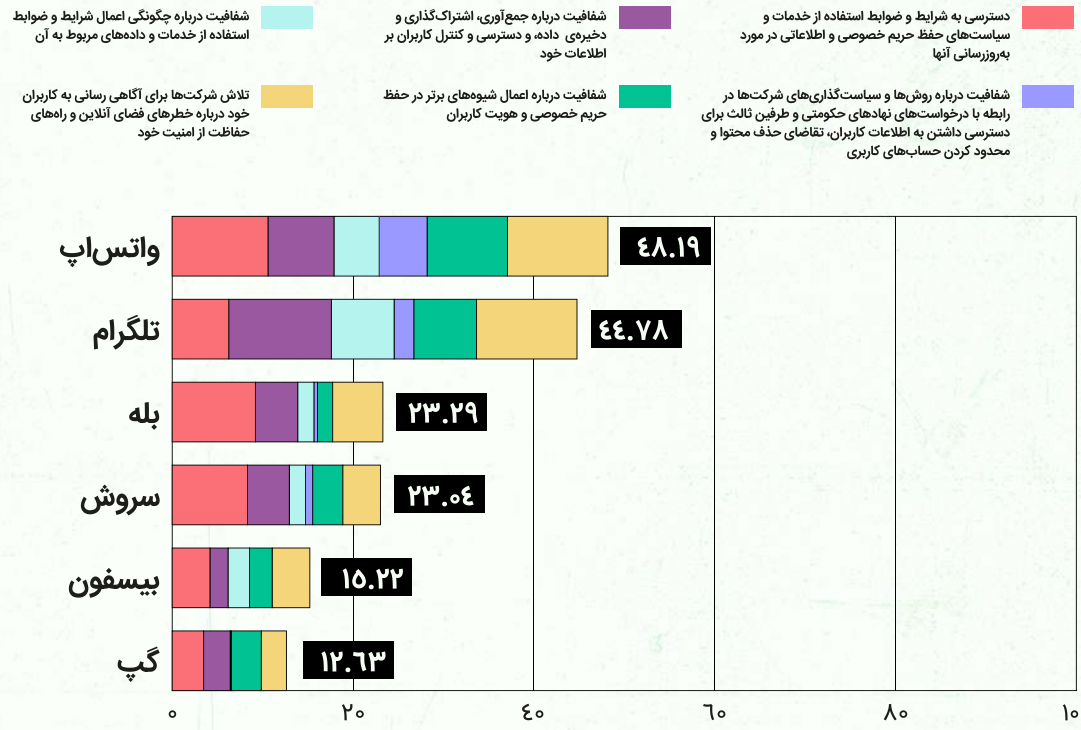
- در بین شرکت‌های ایرانی، «بله» بالاترین امتیاز را در شفاف‌سازی در زمینه‌ی آزادی بیان و احترام به حریم خصوصی کاربران، دریافت می‌کند. بعد از آن، به ترتیب «سروش»، «بیسفون» و «گپ» قرار دارند. با این حال تمام شرکت‌های ایرانی در این شاخص با بیشتر از ۲۰ امتیاز اختلاف، پایین‌تر از دو پیام‌رسان خارجی، یعنی واتس‌اپ و تلگرام قرار می‌گیرند.

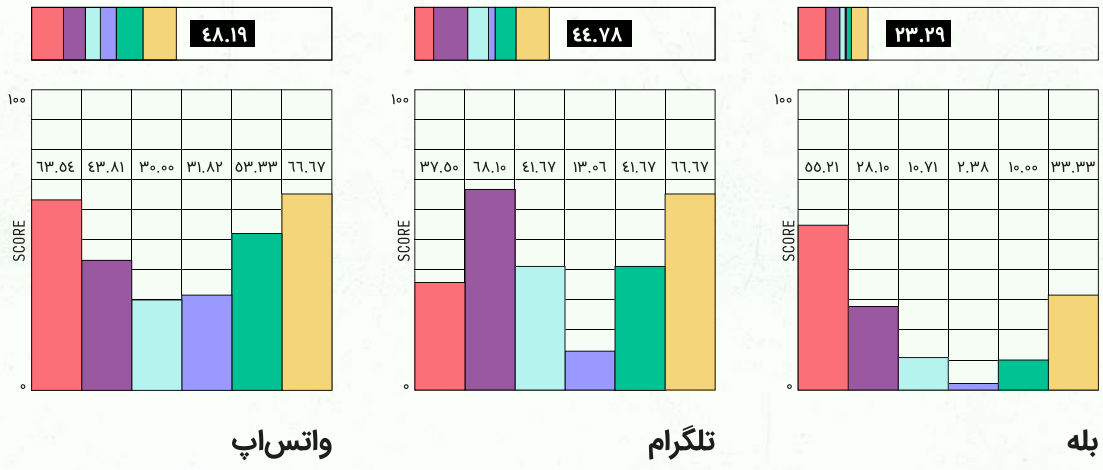
[Fig 4]

دسترسی به شرایط و ضوابط استفاده از خدمات و سیاست‌های حفظ حریم خصوصی و اطلاعاتی در مورد به‌روزرسانی آنها	F1,F2, P1,P2
شفافیت درباره جمع‌آوری، اشتراک‌گذاری و دخیره‌ی داده، و دسترسی و کنترل کاربران بر اطلاعات خود	P3, P9, P4, P5, P6, P7, P8
شفافیت درباره چگونگی اعمال شرایط و ضوابط استفاده از خدمات و داده‌های مربوط به آن	F3, F4
شفافیت درباره روش‌ها و سیاست‌گذاری‌های شرکت‌ها در رابطه با درخواست‌های نهادهای حکومتی و طرفین ثالث برای دسترسی داشتن به اطلاعات کاربران، تقاضای حذف محتوا و محدود کردن حساب‌های کاربری	P10, P11, P12, F5, F6, F7, F8
شفافیت درباره اعمال شیوه‌های برتر در حفظ حریم خصوصی و هویت کاربران	P13, P14, P15, P16, F11
تلاش شرکت‌ها برای آگاهی رسانی به کاربران خود درباره خطرهای فضای آنلاین و راه‌های حفاظت از امنیت خود	P17, P18

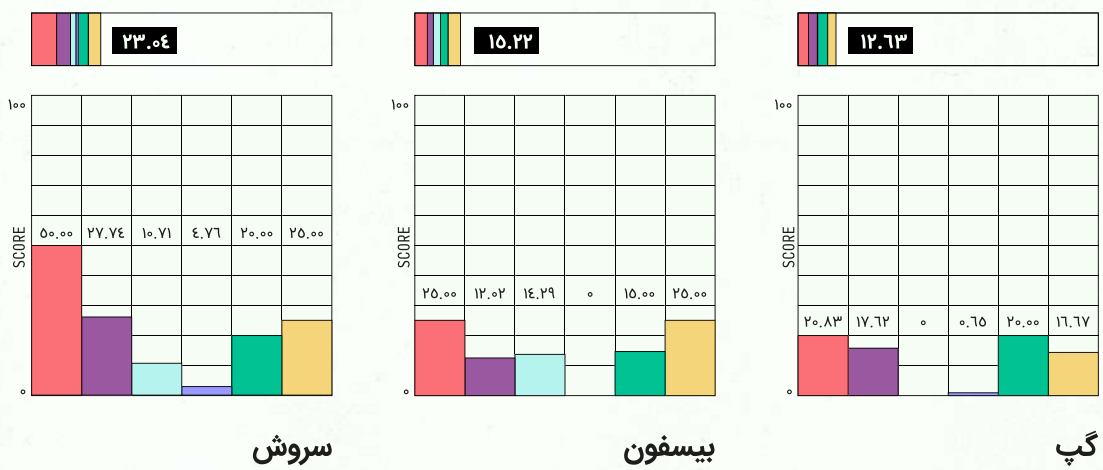
[Fig 5]

نگاهی بر نتایج تحقیق





واتس‌اپ تلگرام بله



سروش بیسفون گپ

- تمام شرکت‌های ایرانی برای انتشار اطلاعاتی در زمینه حریم خصوصی و شرایط و ضوابط استفاده از خدمات، امتیاز دریافت می‌کنند. با این حال در چندین مورد، هم در اپلیکیشن‌های خارجی و هم ایرانی، به جای اینکه هر کدام از این اطلاعات جداگانه در صفحه مربوط به خود قرار بگیرد، این اطلاعات در صفحات سوالات متداول تعبیه شده بود. تلگرام و واتس‌اپ هر دو برای فراهم نکردن کامل سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات به زبان فارسی، امتیاز ناقص دریافت می‌کنند.

- هیچ‌کدام از شرکت‌های ایرانی، گزارش‌های شفافیت خود را در رابطه با جزئیات چگونگی اعمال شرایط و ضوابط استفاده از خدمات، (مانند تعداد حساب‌های کاربری بسته شده، تعداد و نوع محتوای سانسور و حذف شده، یا درخواست‌های دولت و طرفین ثالث برای دسترسی به اطلاعات کاربران)، منتشر نمی‌کنند. شرکت مادر واتس‌اپ، یعنی فیسبوک، گزارش‌های شفافیت منتشر می‌کند. با این حال سامانه‌ی شفافیت فیسبوک، داده‌ها را بر اساس نوع خدمات تفکیک نمی‌کند. تلگرام دارای یک کانال شفافیت است، ولی این کانال تا به حال اطلاعاتی منتشر نکرده است؛ البته لازم به ذکر است که این شرکت در کانال ISIS-Watch خود، داده‌هایی درباره مسدود کردن صفحات کاربری تروریستی منتشر می‌کند[۴۷].

- در بین شرکت‌های ایرانی، تمام شرکت‌ها به استثنای «گپ»، فهرستی دارند تا به کاربر آگاهی دهند که بر اساس شرایط و ضوابط استفاده از آن پیام‌رسان چه نوع محتوا و فعالیتی غیر مجاز محسوب میشود. البته برخی از تعاریف موجود در این فهرست مبهم بوده و هر کسی می‌تواند تفسیر متفاوتی از آنها داشته باشد، از جمله عباراتی همچون «غیراخلاقی» یا «اقدام علیه امنیت ملی». «بله» اذعان می‌کند که این شرکت تابع قوانین جمهوری اسلامی ایران است و تمام قوانین کنونی کشور در فضای مجازی باید رعایت شود. این اپلیکیشن حتی اضافه می‌کند که کاربران می‌توانند موارد غیر قانونی را مستقیماً به مقامات قضایی اطلاع دهند[۴۸].

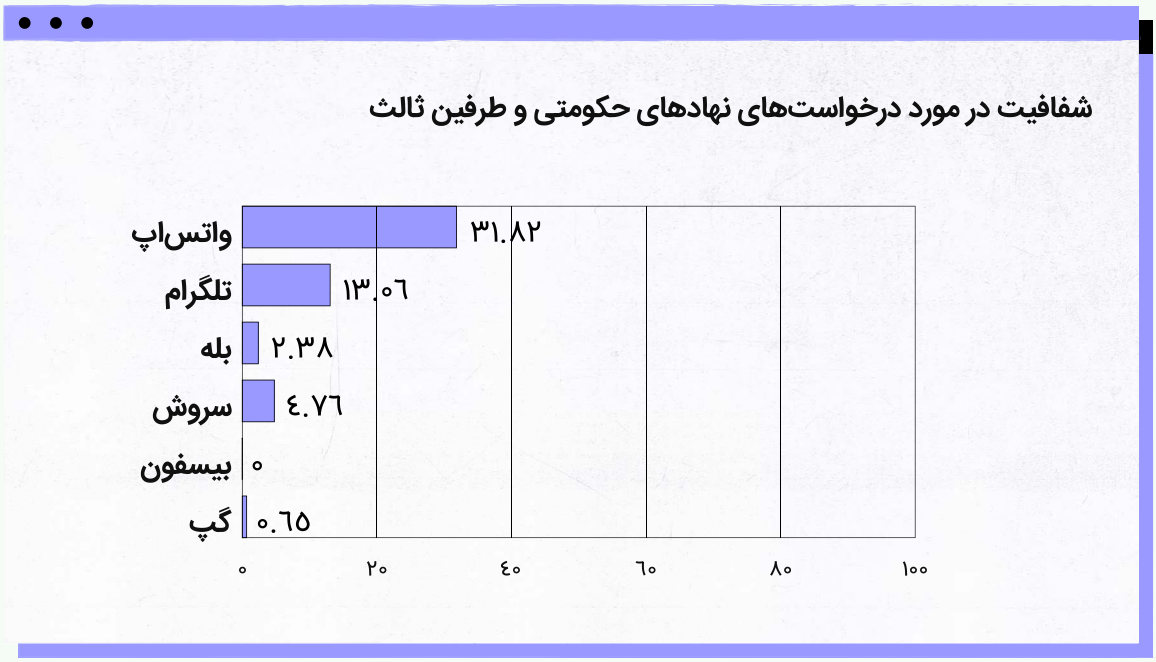
- «گپ» هیچ امتیازی برای شفافیت در زمینه چگونگی اعمال شرایط و ضوابط استفاده از خدمات دریافت نمی‌کند. همچنین «بیسفون» امتیازی برای شفافیت درباره درخواست‌های دولت و طرفین ثالث برای دسترسی به اطلاعات کاربران و یا حذف و محدودیت محتوا و صفحات کاربری، دریافت نمی‌کند.

در نمودارهای پیش رو جزئیات بیشتری از امتیاز شرکت‌ها ارائه میدهیم:

47 Telegram's ISIS Watch channel, https://t.me/isiswatch, Only a preview version of the channel exists for people who don't have a Telegram account. RDR assesses companies based on their public disclosure, without having to log-in or create an account. This affected our accoring about Telegram's transparency in publishing ToS enforcement data.

48 "[...] فضای اپلیکیشنهای رسمی بخشی از قلمرو حاکمیت قوانین جمهوری اسلامی ایران است و کلیه قوانین رایج کشور در محیط مجازی نیز لازم الاتباع است و مسئولیت حقوقی یا کیفری ناشی از نقض این قوانین با کاربر متخلف است. اعمال تروریستی، اقدامات علیه امنیتی ملی، اقدامات علیه تمامیت ارضی و استقلال کشور و نیز جاسوسی و سایر موارد که مطابق با مقررات موضوعه داخلی یا بین المللی جرم تلقی شده است و مسئولیت سوء استفاده از این اپلیکیشن در ارتباط با امور مجرمانه به هر شکل با کاربر است. کاربران محترم در خصوص این موارد باید نهایت دقت و جدیت را داشته باشند و البته می‌توانند هر یک از موارد نقض را به مقامات صالح یا ضابطین قضایی اطلاع رسانی نمایند."
Bale, Terms of Use, https://bale.ai/terms/, Accessed in April 2020

شفافیت در مورد درخواست‌های نهادهای حکومتی و طرفین ثالث [Fig 6]



[Fig 7]

این امتیاز میانگین مولفه‌های ذیل میباشد

P۱۰. روند واکنش به درخواست‌های طرفین ثالث برای دسترسی به اطلاعات کاربران
شرکت‌ها می‌بایست به صورت علنی روند پاسخگویی به درخواست‌های نهادهای حکومتی و طرفین ثالث برای دسترسی به اطلاعات کاربران را اعلام کنند.

P۱۱. داده‌های مربوط به درخواست‌های طرفین ثالث برای دسترسی به اطلاعات کاربران
شرکت‌ها باید به طور مداوم داده‌های خود را در ارتباط با درخواست‌های نهادهای حکومتی و طرفین ثالث برای دسترسی به اطلاعات کاربران منتشر کنند.

P۱۲. اطلاع رسانی به کاربران در مورد درخواست‌های طرفین ثالث برای دسترسی به اطلاعات
شرکت‌ها باید کاربران خود را تا جایی که در محدوده قانون می‌گنجد از اینکه اطلاعاتشان مورد درخواست نهادهای حکومتی و طرفین ثالث قرار گرفته، مطلع کنند.

F۵. روند واکنش به درخواست‌های طرفین ثالث برای توقیف صفحات کاربری و حذف محتوا
شرکت‌ها باید به صورت شفاف شیوه‌ی خود را در واکنش به درخواست‌های نهادهای حکومتی (که شامل دستورات قضایی نیز می‌شود) و درخواست‌های خصوصی برای حذف، فیلتر و توقیف محتوا و صفحات کاربری، اعلام کنند.

F۶. داده‌های مربوط به درخواست‌های دولت برای توقیف محتوا و صفحات کاربری
شرکت‌ها می‌بایست مرتبا داده‌های مربوط به درخواست‌های نهادهای حکومتی را (که شامل دستورات قضایی نیز می‌شود) برای حذف، فیلتر کردن و توقیف محتوا و صفحات کاربری، منتشر کنند.

F۷. داده‌های مربوط به درخواست‌های نهادهای خصوصی برای توقیف محتوا و صفحات کاربری شرکت‌ها می‌بایست مرتبا داده‌های مربوط به درخواست‌های خصوصی برای حذف، فیلتر کردن و توقیف محتوا و صفحات کاربری را منتشر کنند.

F۸. اطلاع رسانی به کاربران درباره توقیف حساب کاربری و محتوای صفحاتشان شرکت‌ها باید اعلام کنند که آیا کاربران خود را از بسته شدن حساب کاربری و حذف محتوای صفحه‌شان مطلع می سازند یا نه.

- **شرکت‌های ایرانی و خارجی همگی، کمترین امتیاز را در بخش درخواست‌های نهادهای حکومتی و طرفین ثالث دریافت کردند.** شرکت‌های ایرانی وضعیت بسیار بدتری نسبت به همتایان خارجی خود در این بخش دارند.

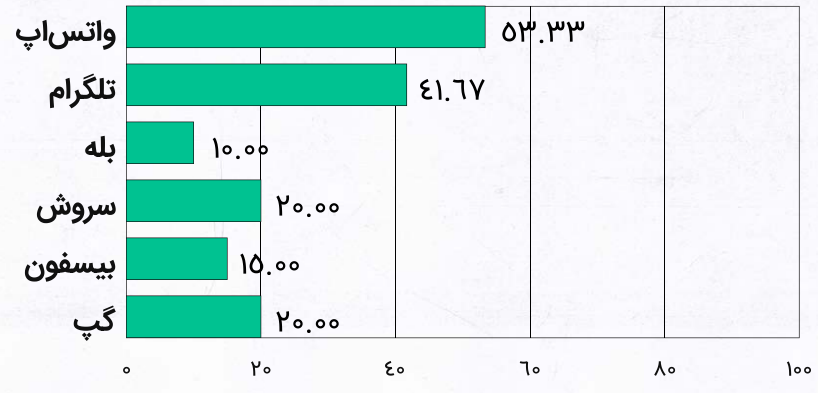
- در بین شرکت‌های ایرانی، «سروش» بخشی از مولفه‌ی P۱۲ را با اعلام این موضوع که «تحت هیچ شرایطی اطلاعات کاربران خود را بدون اجازه آنها در دسترس هیچ نهاد/شخص/سازمانی قرار نمی‌دهد»، تامین کرده و به همین دلیل بیشترین امتیاز را دریافت کرده است. «بله» نیز بخشی از امتیاز زیر-مولفه‌ی F۵/۵ را در رابطه با شرایط قانونی که ممکن است این شرکت تحت آن با درخواست‌های دولتی موافقت کند، دریافت می‌کند.

- نکته‌ی قابل ذکر در مورد شرکت‌های غیر ایرانی این است که هرچند واتس‌اپ در مقایسه با تلگرام امتیاز بیشتری برای انتشار گزارش شفافیت دریافت میکند، اما این امتیاز در حقیقت بر اساس بررسی گزارش شفافیت شرکت مادر واتس‌اپ، یعنی فیسبوک، محاسبه شده است. از این رو این نکته حائز اهمیت است که سامانه شفافیت فیسبوک داده‌ها را بر اساس نوع سرویس‌های ارائه شده (مثلاً «واتس‌اپ»، مسنجر و غیره) تفکیک نمی‌کند.

شفافیت درباره شیوه‌های برتر در خصوص حفظ حریم خصوصی، امنیت و محافظت از هویت کاربران

[Fig 8]

شفافیت درباره شیوه‌های برتر در خصوص حفظ حریم خصوصی، امنیت و محافظت از هویت کاربران



[Fig 9]

این امتیاز میانگین مولفه‌های ذیل میباشد:

P۱۳. نظارت بر امنیت شرکت‌ها می‌بایست به صورت علنی اعلام کنند که به چه روش‌هایی ، امنیت محصول و خدمات خود را حفظ می‌کنند.

P۱٤. برطرف کردن «ضعف‌های امنیتی» در صورت پیدا شدن «ضعف‌های امنیتی»، شرکت‌ها می بایست این ضعف‌ها را برطرف کنند.

P۱۵. نشت‌های اطلاعاتی شرکت‌ها می‌بایست رویه‌ی خود را در واکنش به نشت‌های اطلاعاتی به صورت علنی اعلام کنند.

P۱٦. رمزنگاری محتوای خصوصی و ارتباطات کاربران شرکت‌ها می‌بایست محتوای خصوصی و ارتباطات کاربران را رمزنگاری کنند تا افراد بتوانند در مورد اینکه چه کسی به این اطلاعات دسترسی داشته باشد، کنترل داشته باشند. باشند.

F۱۱. سیاست‌های مربوط به هویت افراد شرکت‌ها نباید از کاربران بخواهند که هویت خود را از طریق کارت‌های شناسایی دولتی تایید کنند. همچنین روش‌های دیگر احراز هویت کاربری نباید به‌گونه ای باشد که باعث برملا شدن هویت واقعی کاربران شود.

- هیچ یک از شش شرکت بررسی‌شده، درباره راه‌های برخورد خود با نشت داده‌ای، به صورت علنی اطلاعاتی را منتشر نمی‌کنند، و معلوم نیست که آیا کاربران و مسئولان مربوطه را از چنین اتفاقاتی مطلع می‌سازند یا خیر. علاوه بر این، هیچ‌کدام از این شرکت‌ها اعلام نمی‌کنند که آیا برای محدود کردن دسترسی کارکنان خود به اطلاعات کاربران، سیستم خاصی تعبیه کرده‌اند یا نه. پیش از این چندین نمونه از سرک کشیدن‌های کارکنان در اطلاعات کاربران و از آن بدتر، جاسوسی برای دولت‌ها اتفاق افتاده است که توجه به این موضوع را حساس‌تر نیز می‌کند.[۴۹]

- **واتس‌اپ و تلگرام، هر چند هر دو از دریافت امتیازات کامل در این بخش بسیار فاصله دارند، اما درباره استانداردهای رمزنگاری سرتاسری خود، اطلاعاتی را به صورت علنی اعلام می‌کنند:**[۵۰] تلگرام از رمزنگاری سرتاسری MTProto's[۵۱] ۲٫۰، که فقط برای گپ محرمانه (Secret Chat) پیاده شده است، استفاده میکند و واتس‌اپ استاندارد رمزنگاری Signal Protocol را به صورت پیش‌فرض برای تمامی تماس‌ها و پیام‌های دو-نفره و گروهی تعبیه کرده است. توجه داشته باشید که کد تلگرام هنوز به طور کامل متن-باز(open source) نیست.

- **شرکت‌های ایرانی در رتبه‌بندی بخش الگوهای برتر طراحی و توسعه خدمات دیجیتال، پایین‌تر از همتایان خارجی خود قرار می‌گیرند.** با این وجود در بین این شرکت‌ها، «بیسفون» تنها شرکتی است که بخشی از امتیاز مولفه‌ی P۱۶ را که مربوط به رمزنگاری محتوای خصوصی و ارتباطات کاربران است، دریافت می‌کند. دلیل دریافت این امتیاز از سوی «بیسفون» این است که این شرکت ادعا می‌کند قابلیت رمزنگاری سرتاسری

49 Greg Bensinger Ellen Nakashima, “Former Twitter Employees Charged with Spying for Saudi Arabia by Digging into the Accounts of Kingdom Critics,” The Washington Post, November 12, 2019, https://wapo.st/2T28OY2 and “Facebook Has Fired Multiple Employees for Snooping on Users,” Sources: Facebook Has Fired Multiple Employees for Snooping on Users, accessed September 18, 2020, https://bit.ly/3j24cvx

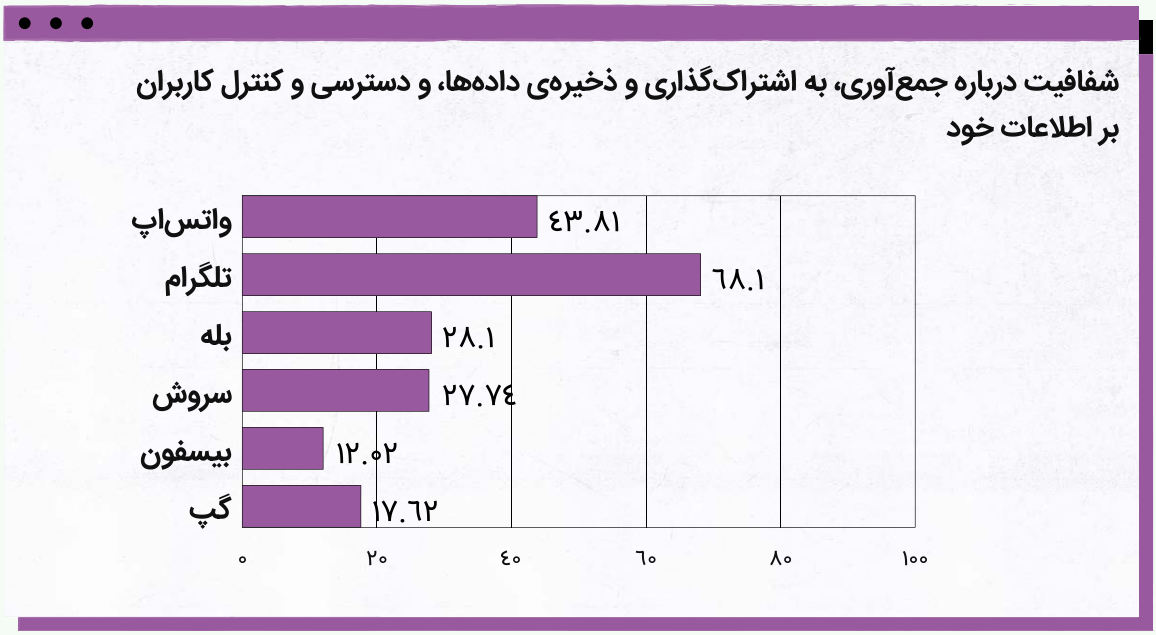
را، هر چند به صورت غیر پیش‌فرض، فراهم می‌کند. ما نتوانستیم هیچگونه اطلاعاتی درباره جزییات فنی رمزنگاری این شرکت بر روی صفحه گیت‌هاب آنها پیدا کنیم.[۵۲]

- **«بله» در این بخش در پایین‌ترین رتبه در میان همتایان ایرانی خود قرار گرفت.** با توجه به همکاری این شرکت با بانک مرکزی ایران (نهادی متعلق به حکومت) برای ارائه خدمات بانک دیجیتال و سروکار داشتن با اطلاعات حساس مالی کاربران، امتیاز پایین «بله» در این بخش موضوعی بسیار نگران‌کننده است.

شفافیت درباره جمع‌آوری، به اشتراک‌گذاری و ذخیره‌ی داده‌ها، و دسترسی و کنترل کاربران بر اطلاعات خود

- **در این بخش، تلگرام بیشترین امتیاز را دریافت کرده است.** در میان تمام شرکت‌های مورد بررسی، تلگرام بیشترین شفافیت را درباره روش‌های جمع‌آوری داده خود داشته و تاکید می‌کند که جمع‌آوری داده‌های کاربران را تا جایی که فقط برای کارکرد خدمات ارائه شده ضروری باشد، جمع‌آوری و نگه‌داری میکند. یک دلیل این موضوع می‌تواند این باشد که مدل کسب و کار تلگرام، در مقایسه با شرکت مادر واتس‌اپ، یعنی فیسبوک، متکی بر تبلیغات هدفمند (targeted advertising) نیست و این شرکت به شکلی شفاف این موضوع را اعلام می‌کند. پژوهشگران RDR در گزارشی با عنوان «موضوع اصلی مدل کسب و کار است: چطور سود-محوری شرکت‌های بزرگ فناوری باعث اغتشاش حوزه عمومی شده است و دموکراسی را تهدید می‌کند» نشان داده‌اند که اتکا به تبلیغات هدفمند، موجب می‌شود که شرکت‌ها شیوه‌هایی به کار گیرند که ناقض حریم خصوصی هستند تا بتوانند اطلاعات هر چه بیشتری درباره کاربران جمع‌آوری

[Fig 10]



50 Telegram's FAQ, https://bit.ly/3dvk4Wx
51 End-to-End Encryption, Telegram, https://bit.ly/3dvk4Wx and WhatsApp Encryption Overview, WhatsApp, December 19, 2017, https://bit.ly/2GVPfhV
52 BisPhone, https://bit.ly/31clEaN date accessed: June 5, 2020

[Fig 11]

این امتیاز میانگین مولفه‌های ذیل میباشد:

P۳.جمع‌آوری اطلاعات کاربران شرکت‌ها می‌بایست به شکلی شفاف اعلام کنند که چه اطلاعاتی را و به چه شیوه‌ای جمع‌آوری می‌کنند.

P٤. به اشتراک‌گذاری اطلاعات کاربران شرکت‌ها می‌بایست به شکلی شفاف اعلام کنند که چه اطلاعاتی از کاربران با چه کسانی به اشتراک گذاشته می‌شود.

P٥. هدف از جمع‌آوری و به اشتراک‌گذاری اطلاعات کاربران شرکت‌ها می‌بایست به شکلی شفاف اعلام کنند که به چه دلیل اطلاعات کاربران را جمع‌آوری کرده و به اشتراک می‌گذارند.

P٦.نگه‌داری اطلاعات کاربران شرکت‌ها می‌بایست به شکلی شفاف اعلام کنند که برای چه مدت اطلاعات کاربران را ذخیره می‌کنند.

P٧. کنترل کاربران بر اطلاعات خود شرکت‌ها می‌بایست به شکلی شفاف به کاربران اعلام کنند که چه گزینه‌هایی برای جمع‌آوری، نگه‌داری و استفاده از اطلاعات کاربران وجود دارد.

P٨. دسترسی کاربران به اطلاعات خود شرکت‌ها می‌بایست به کاربران خود اجازه دهند که تمامی اطلاعات کاربری خود را که در اختیار شرکت است، اخذ نمایند.

P٩. جمع‌آوری اطلاعات کاربران از طرفین ثالث شرکت‌ها می‌بایست به شکلی شفاف روش‌های خود را در ارتباط با جمع‌آوری داده‌های کاربران از اپلیکیشن‌ها یا وب‌سایت‌های طرفین ثالث به واسطه روش‌های فنی، اعلام کنند.

کنند.[۵۳] دلیل دیگر می‌تواند این باشد که فیسبوک به عنوان شرکت مادر، خدمات مختلفی (اینستاگرام، واتس‌اپ، فیس‌بوک مسنجر و غیره) ارائه می‌دهد و شفافیت لازم درباره روش‌های به اشتراک‌گذاری داده، در بین سرویس‌های خود فیسبوک نیز وجود ندارد.

- **ما نتوانستیم هیچ اطلاعاتی درباره روش‌های تبلیغات هدفمند در شرکت‌های ایرانی پیدا کنیم،**[۵۴] همینطور هیچگونه اظهارات علنی درباره شیوه‌های به اشتراک‌گذاری داده در بین اپلیکیشن‌های پیام‌رسان، شرکت‌های مادر و یا بین سرویس‌های مختلفی که از سوی یک شرکت مادر ارائه می‌شوند، پیدا نکردیم.

- **نکته‌ی مثبت در این بخش این است که سرویس‌های پیام‌رسان ایرانی درباره اختیار کاربران برای حذف داده‌های خود، نسبتاً شفاف عمل کرده‌اند؛** هر چهار شرکت اظهار کردند که اطلاعات کاربران را پس از اینکه کاربران، حساب خود را می‌بندند، پاک می‌کنند، و به همین خاطر امتیازاتی در این بخش دریافت کرده‌اند. **با این حال هیچکدام از این شرکت‌ها به صورت علنی اعلام نمی‌کنند که آیا اطلاعات کاربری را «هویت-روبی» (de-identify) می‌کنند یا خیر.** از این گذشته،

53 "It's the Business Model: How Big Tech's Profit Machine Is Distorting the Public Sphere and Threatening Democracy," Ranking Digital Rights, August 24, 2020, https://bit.ly/3jFrg3u

54 Note that Soroush hinted at using cookies to gain information about the patterns of using Soroush in order to provide relevant support/services. It's not clear what those services are and if they are related to targeted advertising: https://hi.sapp.ir/privacy

«بله» تنها شرکتی است که اظهار می‌کند ممکن است اطلاعات کاربران را با دولت یا مقامات قضایی به اشتراک بگذارد؛ بقیه شرکت‌ها چیزی در این‌باره نگفته‌اند.

شفاف‌سازی و سیاست‌گذاری شرکت

شاخص‌های RDR شامل شش مولفه برای ارزیابی سیاست‌گذاری شرکت‌ها و سازوکارهای نظارت در ارتباط با حفظ حریم خصوصی و آزادی بیان، است. این بخش به ارزیابی تعهد شرکت‌ها به اصول راهنمای تجارت و حقوق بشر سازمان ملل می‌پردازد؛ و اینکه شرکت‌ها چطور این تعهدات را در تمام قسمت‌های کار خود، به کار می‌گیرند: آیا صلاحیت خود را مطابق با حقوق بشر ارزیابی می‌کنند؟ آیا با گروه‌های جامعه مدنی و دیگر ذینفعان همکاری می‌کنند؟ آیا به بررسی شکایات مربوط به نقض حقوق بشر می‌پردازند؟ این مولفه‌ها به شرح ذیل هستند:

تمام شرکت‌های ایرانی در بخش سیاست‌گذاری شرکت، امتیاز صفر دریافت کرده‌اند. این موضوع تا حدی به این دلیل است که هیچکدام از شرکت‌های مورد بررسی، در طرح‌های چند ذینفعی که موجب همکاری و حاکمیت جمعی میان شرکت‌ها، سازمان‌های جامعه مدنی، موسسات دانشگاهی، سرمایه‌گذاران، دولت‌ها و دیگر گروه‌های ذینفع می‌شود، مشارکت نداشته‌اند. در میان شرکت‌های مورد بررسی، شرکت مادر واتس‌اپ، یعنی فیسبوک، تنها شرکتی است که در طرح چند-ذینفعی (Global Network Initiative)، عضویت دارد. (GNI یک طرح چند-ذینفعی است که به منظور کمک به شرکت‌ها برای احترام به آزادی بیان و حریم خصوصی - بالاخص وقتی دولت‌ها، شرکت‌ها را تحت فشار قرار می‌دهند تا داده‌های کاربران خود را در اختیارشان قرار دهند، یا محتوایی را حذف کنند- بنیان گذاشته شده است.[۵۵] ما سعی کردیم نمونه‌های ایرانی و منطقه‌ای مشابه چنین طرح‌های چند ذینفعی را شناسایی کنیم، اما موفق نشدیم.

[Fig 12]

G۱.تعهد به قوانین شرکت‌ها می‌بایست به حقوق کاربران خود در رابطه با آزادی بیان و حریم خصوصی احترام گذشته و به صورت علنی این تعهد را اظهار کنند.

G۲. سیاست‌گذاری شرکت و سازوکارهای نظارت مدیران ارشد شرکت‌ها می‌بایست بر تاثیرات شیوه‌ها و سیاست‌گذاری‌های شرکت خود بر آزادی بیان و حریم خصوصی، نظارت داشته باشند.

G۳. اجرای درون سازمانی شرکت‌ها می‌بایست سازوکارهایی داشته باشند تا تعهدات خود به آزادی بیان و حریم خصوصی را، به شکل درون سازمانی به اجرا بگذارند.

G٤. سنجش اثرات شرکت‌ها می‌بایست عملکرد خود را به صورت مرتب، جامع و معتبر ارزیابی کنند، برای مثال می‌بایست تاثیرات حقوق بشری خود را ارزیابی کرده تا بدانند چطور تمام بخش‌های کاری آنها بر آزادی بیان و حریم خصوصی تاثیر می‌گذارد، و در صورت وجود مواردی که این حقوق را نقض می کنند، بتوانند به کاهش و رفع این مشکلات بپردازند.

G۵. همکاری با نهادهای ذینفع شرکت‌ها می‌بایست با نهادهای مختلفی در زمینه آزادی بیان و حریم خصوصی همکاری کنند.

G٦. جبران خسارات شرکت‌ها می‌بایست دارای سازوکارهایی برای ارائه جبران خسارات و بررسی شکایات در زمینه معضلات مربوط به حریم خصوصی و آزادی بیان باشند.

55 Global Network Initiative, https://globalnetworkinitiative.org/

- در مورد مولفه G۴ (سنجش اثرات)، اینکه تمام شرکت‌های ایرانی امتیاز صفر دریافت کرده‌اند، نگران‌کننده است. به دلیل ماهیت ناپایدار سرویس‌های پیام‌رسان از نظر مجموعه‌ی خدمات و ویژگی‌های آنها و همکاری‌های متغیر و گاهی بی‌ثبات با دولت، این موضوع بسیار حیاتی است که پیش از اضافه کردن خدمات جدید و یا شروع یک همکاری تازه، اثرات حقوق بشری چنین اقداماتی سنجیده شود. برای مثال، می‌توان به نمونه اخیر اپلیکیشن «شاد» و قوانین ثبت‌نام در آن اشاره کرد. شاد یک سرویس آموزش دیجیتال است که مطابق با زیرساخت‌های اپلیکیشن‌های پیام‌رسان داخلی ساخته شده است. در اردیبهشت ۱۳۹۹، انجمن حمایت از پناهندگان «حامی»، درباره دسترسی کودکان پناهنده افغان به این اپلیکیشن اظهار نگرانی کرد، چرا که این اپلیکیشن برای ثبت‌نام نیازمند شماره کارت ملی افراد است، چیزی که بیشتر کودکان پناهنده در اختیار ندارند.[۵۶] سازندگان این اپلیکیشن و وزارت آموزش و پرورش این مشکل را رفع کردند، اما با این حال، چنین اشتباهاتی نشان‌دهنده‌ی فقدان آگاهی درباره اهمیت اجرای سنجش‌های اثرات حقوق بشر و دیگر مولفه‌های سیاست‌گذاری شرکت مانند همکاری فعال با سازمان‌های جامعه مدنی و داشتن راهکارهایی برای جبران خسارات است.

ما امیدواریم که شرکت‌های مورد بررسی، از این گزارش و راهنمای ضمیمه استفاده کنند تا اصول راهنمای تجارت و حقوق بشر سازمان ملل را وارد گفتمان درون سازمانی خود کرده و در گزارش‌های آینده، امتیاز مولفه‌های سیاست‌گذاری شرکت را به‌دست آورند. شرکت‌ها همچنین می‌توانند از ابزارهای دیگری مانند «سنجش مبنای حقوق بشر برای شرکت‌های فناوری کوچک و متوسط» استفاده کرده تا مسئولیت‌های خود را در زمینه مولفه‌های سیاست‌گذاری شرکت به درستی انجام دهند.[۵۷]

56 Melody Kazemi, “Policy Monitor – April 2020,” Filterwatch, May 14 2020, https://bit.ly/3dzeQZW
57 “Human Rights Baseline Assessment for Small and Medium Sized Technology Companies”, Global Partners Digital and Open Technology Institute, January 2020, https://bit.ly/2H84vb2

کارت عملکرد شرکت‌ها

در این بخش می‌توانید کارت عملکرد مربوط به هر شرکت را مطالعه کنید. ما این شرکت‌ها را بر اساس معیارهای مختلفی از جمله تعداد دانلود، میزان پوشش رسانه‌ای دریافت شده، و حمایت نهادهای دولتی از آنها، انتخاب کرده‌ایم. هر کارت عملکرد شامل جزئیاتی درباره معیار انتخاب، امتیازات آن شرکت و پیشنهادهایی برای بهبود عملکرد است.

سروش/سروش پلاس

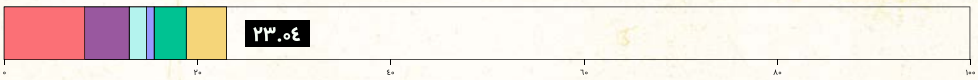
با سه میلیون دانلود از کافه بازار، این اپلیکیشن یکی از پراستفاده‌ترین پلتفرم‌های پیام‌رسان داخلی در ایران است.

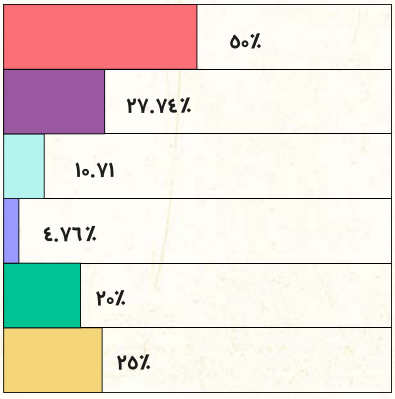
در اردیبهشت سال ۱۳۹۸، شورای عالی فضای مجازی، سروش را به عنوان یکی از اپلیکیشن‌های پیام‌رسان مورد تایید خود معرفی کرد.

مالکیت این اپلیکیشن در دست صدا و سیمای جمهوری اسلامی (نهاد رسانه‌ای حکومت) بود. در اوایل سال ۱۳۹۹، صدا و سیما تصمیم به فروش این شرکت گرفت.

صفحه‌ی سیاست‌های حفظ حریم خصوصی	✓
صفحه‌ی شرایط و ضوابط استفاده از خدمات	✓
الگوهای برتر طراحی و توسعه خدمات دیجیتال	
رمزنگاری	ما هیچ اطلاعات یا گزارش فنی‌ای درباره نحوه‌ی رمزنگاری داده‌ها پیدا نکردیم. سروش پیام‌ها را به صورت سرتاسری (End to End Encryption) رمزنگاری نمی‌کند.
امنیت سایبری	ما هیچ اطلاعاتی در مورد اقدامات شرکت برای بررسی امنیت سایبری و فراهم کردن برنامه‌های باگ باونتی (bug bounty) پیدا نکردیم.
آیا این شرکت گزارش شفافیت (Transparency Report) منتشر می‌کند؟	خیر

امتیازات:





دسترسی به سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات، و به‌روزرسانی این سیاست‌ها:

شفافیت در مورد جمع‌آوری داده، به اشتراک‌گذاری و نگهداری داده و کنترل کاربران بر داده‌های خود:

شفافیت در مورد چگونگی اعمال سیاست‌های مربوط به شرایط و ضوابط استفاده از خدمات:

شفافیت در مورد درخواست‌های نهادهای حکومتی و طرفین ثالث:

شفافیت در مورد به کارگیری الگوهای برتر طراحی و توسعه خدمات دیجیتال:

تلاش‌های شرکت در آگاهی رسانی به کاربران درباره خطرهای آنلاین و چگونگی حفاظت از خود:

توصیه‌های فوری:

- اینکه سروش به کاربران خود می‌گوید که بر اساس ضوابط پیام‌رسان چه عملی مجاز یا غیرمجاز است، نکته ی مثبتی است. با این حال، ساز و کار بررسی و اِعمال این ضوابط استفاده از خدمات به صورت شفاف بیان نشده است. سروش می‌بایست روش‌هایی (خودکار یا غیرخودکار) که برای اِعمال این ضوابط مورد استفاده قرار می‌دهد را به صورت علنی اعلام کند.
- سروش هیچگونه اطلاعاتی درباره پروتکل‌های رمزنگاری مورد استفاده خود اعلام نکرده است. این شرکت می‌بایست فوراً گزارش فنی خود را منتشر کرده و اعلام کند که آیا داده‌های کاربران خود را در حین انتقال و در زمان ذخیره‌سازی، رمزنگاری می‌کند یا خیر؛ اگر پاسخ مثبت است بر اساس چه استانداردهای رمزنگاری این کار را انجام می‌دهد.
- این شرکت می‌بایست گزارش شفافیت منتشر کند. در این گزارش‌ها، سروش باید مشخص کند چه تعداد محتوا و حساب‌های کاربری به درخواست نهادهای غیردولتی، دولتی و قضایی ،به تفکیک نوع نهادها، حذف شده‌اند.
- سروش باید در مورد مشارکت‌های خود با نهادهای دولتی یا وابسته به حکومت شفاف باشد و به طور مکتوب اعلام کند که مشارکت و سرمایه‌گذاری نهادهای حکومتی و یا دریافت وام از این نهادها هرگز موجب امتیاز ویژه یا دسترسی این نهادها به اطلاعات کاربران نخواهد شد.

گپ

گپ جزو اپلیکیشن‌های پیام‌رسانی است که از سوی شورای عالی فضای مجازی تایید شده است.

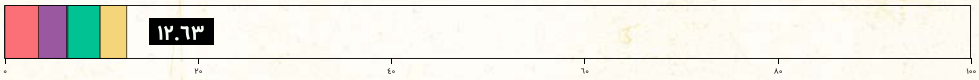
گپ متعلق به شرکت TS Information Technology Ltd (TSIT) است.

براساس مطلبی از وبلاگ این شرکت، گپ در بازار بین‌المللی نیز حضور و دفتری در بریتانیا دارد. این اپلیکیشن با نام «ویدا» برای کاربران غیرایرانی، و با نام «گپ» برای کاربران داخل ایران در دسترس است. در همین وبلاگ به امکان همکاری آن با شرکت مخابراتی MTN در آفریقای جنوبی، نیز اشاره شده است.[58]

در دی ماه سال ۱۳۹۷، گپ، همکاری تجاری خود را با شرکت مخابرات ایران به منظور تسهیل پرداخت قبوض به صورت آنلاین، اعلام کرد.[59]

صفحه‌ی سیاست‌های حفظ حریم خصوصی انگلیسی | فارسی | عربی	✓
صفحه‌ی شرایط و ضوابط استفاده از خدمات	✗
الگوهای برتر طراحی و توسعه خدمات دیجیتال	
رمزنگاری	بر اساس اظهارات منتشر شده از طرف گپ روی اپ استور ایرانی کافه بازار، این اپلیکیشن، رمزنگاری سرتاسری (End to End Encryption) ارائه می‌کند ولی ما اطلاعاتی درباره جزئیات الگوریتم‌های رمزنگاری مورد استفاده و یا گزارش فنی‌ای در این باره پیدا نکردیم.[60]
امنیت سایبری	ما هیچ اطلاعاتی در مورد اقدامات شرکت برای بررسی امنیت سایبری و فراهم کردن برنامه‌های باگ باونتی (bug bounty) پیدا نکردیم.
آیا این شرکت گزارش شفافیت (Transparency Report) منتشر می‌کند؟	خیر

امتیازات:



دسترسی به سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات، و به‌روزرسانی این سیاست‌ها:

شفافیت در مورد جمع‌آوری داده، به اشتراک‌گذاری و نگهداری داده و کنترل کاربران بر داده‌های خود:

شفافیت در مورد چگونگی اعمال سیاست‌های مربوط به شرایط و ضوابط استفاده از خدمات:

شفافیت در مورد درخواست‌های نهادهای حکومتی و طرفین ثالث:

شفافیت در مورد به کارگیری الگوهای برتر طراحی و توسعه خدمات دیجیتال:

تلاش‌های شرکت در آگاهی رسانی به کاربران درباره خطرهای آنلاین و چگونگی حفاظت از خود:

توصیه‌های فوری:

- گپ می‌بایست صفحه‌ی «شرایط و ضوابط استفاده از خدمات» بر روی وبسایت خود اضافه کند.
- گپ می‌بایست نسخه‌ای فارسی برای صفحه‌ی «سوالات متداول» خود ارائه دهد. در حال حاضر این صفحه فقط به انگلیسی موجود است.
- این شرکت باید در رابطه با دامنه‌ی رسمی‌ای که در آن فعالیت دارد و به نظام حقوقی آن متعهد است، شفاف باشد. در حال حاضر مشخص نیست که این شرکت به قوانین رسمی ایران پایبند است یا انگلستان و یا هیچکدام. این موضوع شامل شفافیت در مورد به اشتراک گذاشتن داده‌های کاربران با سرویس‌های دیگر شرکت TSIT و فراشرکتی از جمله ویدا و رینگ، و همینطور در مورد شیوه‌های ذخیره داده‌ها در خارج و داخل مرزهای ایران است.
- سیاست‌های حفظ حریم خصوصی این اپلیکیشن در زبان انگلیسی متفاوت با زبان فارسی و عربی آن است. این شرکت باید فوراً این ناهماهنگی را رفع کند، چرا که این مورد می‌تواند نشاندهنده‌ی دوگانگی اعمال سیاست‌های حریم خصوصی و آزادی بیان برای کاربران ایرانی و غیرایرانی باشد.
- گپ می‌بایست شرایط و ضوابط استفاده از API خود را در پورتال توسعه‌دهندگان خود قرار دهد.
- گپ باید در مورد مشارکت‌های خود با نهادهای دولتی یا وابسته به حکومت شفاف باشد و به طور مکتوب اعلام کند که مشارکت و سرمایه‌گذاری نهادهای حکومتی و یا دریافت وام از این نهادها هرگز موجب امتیاز ویژه یا دسترسی این نهادها به اطلاعات کاربران نخواهد شد.

بله

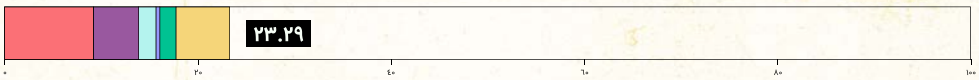
این اپلیکیشن، ترکیبی است از یک پیام‌رسان و یک اپلیکیشن پرداخت الکترونیک که خدمات پیام‌رسانی اجتماعی، بانکداری الکترونیک و دولت الکترونیک ارائه می‌دهد.

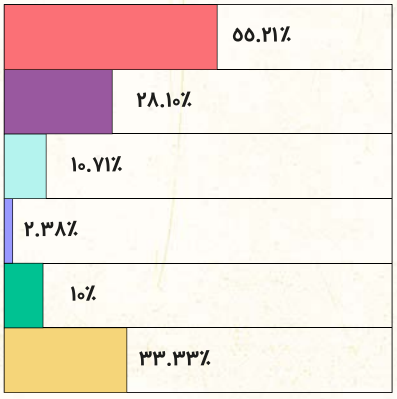
«بله» از سوی بانک مرکزی ایران نظارت می شود.[61]

شورای عالی فضای مجازی «بله» را به عنوان یکی از اپلیکیشن‌های مورد تایید خود معرفی کرده است.

صفحه‌ی سیاست‌های حفظ حریم خصوصی	✓
صفحه‌ی شرایط و ضوابط استفاده از خدمات	✓
الگوهای برتر طراحی و توسعه خدمات دیجیتال	
رمزنگاری	ما هیچ اطلاعات یا گزارش فنی درباره نحوه‌ی رمزنگاری داده‌ها پیدا نکردیم. بله پیام‌ها را به صورت سرتاسری (End to End Encryption) رمزنگاری نمی‌کند.
امنیت سایبری	ا هیچ اطلاعاتی در مورد اقدامات شرکت برای بررسی امنیت سایبری و فراهم کردن برنامه‌های باگ باونتی (bug bounty) پیدا نکردیم.
آیا این شرکت گزارش شفافیت (Transparency Report) منتشر می‌کند؟	خیر

امتیازات:





دسترسی به سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات، و به‌روزرسانی این سیاست‌ها:

شفافیت در مورد جمع‌آوری داده، به اشتراک‌گذاری و نگهداری داده و کنترل کاربران بر داده‌های خود:

شفافیت در مورد چگونگی اعمال سیاست‌های مربوط به شرایط و ضوابط استفاده از خدمات:

شفافیت در مورد درخواست‌های نهادهای حکومتی و طرفین ثالث:

شفافیت در مورد به کارگیری الگوهای برتر طراحی و توسعه خدمات دیجیتال:

تلاش‌های شرکت در آگاهی رسانی به کاربران درباره خطرهای آنلاین و چگونگی حفاظت از خود:

توصیه‌های فوری:

- این شرکت می‌بایست بخش «سیاست‌های حفظ حریم خصوصی» را از بخش «شرایط و ضوابط استفاده از خدمات» جدا کرده و هر دو را روی صفحه اول وبسایت خود ارائه دهد.
- این شرکت باید به صورت منظم، حداقل یک بار در سال، گزارش شفافیت منتشر کند. در مقایسه با اپلیکیشن‌های پیام‌رسان ایرانی دیگری که ما بررسی کردیم، «بله» شفافیت بیشتری درباره‌ی جزئیات ضوابط استفاده از خدمات و حفظ حریم خصوصی نشان داده است، با این حال، گزارشی مبنی بر شفافیت در روش های خود منتشر نمی‌کند. بنابراین انتشار گزارش شفافیت بر روی وبسایت، می‌بایست قدم بعدی باشد.
- اپلیکیشن «بله» می‌بایست درباره ساختار سیاست‌گذاری شرکت خود به‌خصوص در رابطه با همکاری با بانک مرکزی ایران و روش‌های اشتراک‌گذاری و جمع‌آوری اطلاعات با این نهاد شفافیت داشته باشد. همچنین باید به روشنی اعلام کند که مشارکت و سرمایه‌گذاری نهادهای دولتی یا وابسته به حکومت و یا دریافت وام از این نهادها هرگز موجب امتیاز ویژه یا دسترسی این نهادها به اطلاعات کاربران نخواهد شد.
- به دلیل داشتن امکان پرداخت الکترونیک و دسترسی به داده‌های بسیار حساس مالی، «بله» می‌بایست اعلام کند که الگوهای برتر طراحی و توسعه خدمات دیجیتال را سرلوحه‌ی کار خود قرار می‌دهد. این الگوها شامل پیاده‌سازی برترین استانداردهای رمزنگاری، بررسی‌های منظم امنیت سایبری، جلوگیری از نشت اطلاعات، و اطلاع رسانی به کاربران در صورت نشت اطلاعات است.

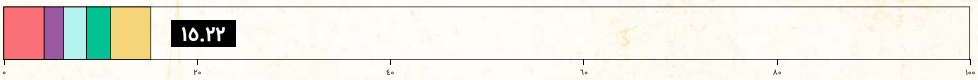
بیسفون

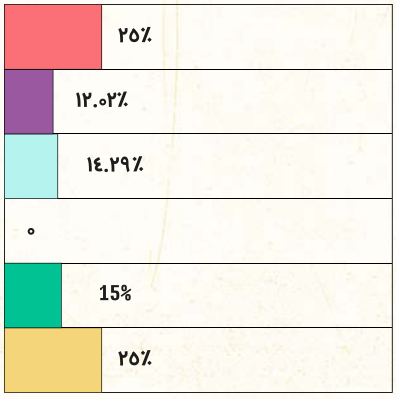
«بیسفون» یکی دیگر از پیام‌رسان‌های داخلی است که با فراهم کردن رمزنگاری سرتاسری (End to End Encryption)، خود را از همتایانش متمایز می‌سازد. البته رمزنگاری سرتاسری این اپلیکیشن به صورت پیش‌فرض (by default) پیاده‌سازی نشده و ما هیچ اطلاعاتی درباره جزئیات فنی پروتکل‌های رمزنگاری این شرکت پیدا نکردیم.

بیسفون متعلق به شرکت تراشه سبز تهران (TSTonline) است.

صفحه‌ی سیاست‌های حفظ حریم خصوصی	✗
صفحه‌ی شرایط و ضوابط استفاده از خدمات	✓
الگوهای برتر طراحی و توسعه خدمات دیجیتال	
رمزنگاری	گزینه رمزنگاری سرتاسری به صورت انتخابی ارائه شده است. هیچ گزارش فنی درباره جزئیات الگوریتم های رمزنگاری یافت نشد.
امنیت سایبری	ما هیچ اطلاعاتی در مورد اقدامات شرکت برای بررسی امنیت سایبری و فراهم کردن برنامه‌های باگ باونتی (bug bounty) پیدا نکردیم.
آیا این شرکت گزارش شفافیت (Transparency Report) منتشر می‌کند؟	خیر

امتیازات:





دسترسی به سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات، و به‌روزرسانی این سیاست‌ها:

شفافیت در مورد جمع‌آوری داده، به اشتراک‌گذاری و نگهداری داده و کنترل کاربران بر داده‌های خود:

شفافیت در مورد چگونگی اعمال سیاست‌های مربوط به شرایط و ضوابط استفاده از خدمات:

شفافیت در مورد درخواست‌های نهادهای حکومتی و طرفین ثالث:

شفافیت در مورد به کارگیری الگوهای برتر طراحی و توسعه خدمات دیجیتال:

تلاش‌های شرکت در آگاهی رسانی به کاربران درباره خطرهای آنلاین و چگونگی حفاظت از خود:

توصیه‌های فوری:

- این شرکت می‌بایست «سیاست‌های حفظ حریم خصوصی» را به طور شفاف بیان کرده و لینک آن را روی صفحه اول وبسایت خود قرار دهد.
- به عنوان اولین اپلیکیشنی که وعده‌ی رمزنگاری سرتاسری به کاربران داده است، «بیسفون» می‌بایست گزارش فنی خود را با ذکر جزییات فنی الگوریتم‌های رمزنگاری پیاده‌سازی شده منتشر کند.
- رمزنگاری سرتاسری باید به صورت پیش‌فرض تعبیه شود و نه گزینه‌ای انتخابی.
- «بیسفون» باید به روشنی اعلام کند که همکاری با نهادهای دولتی یا وابسته به حکومت و دریافت حمایت های مالی به صورت مستقیم و غیرمستقیم (مانند دسترسی رایگان به مرکز داده مادر شبکه ملی)، موجب نخواهد شد که دسترسی به اطلاعات کاربران به شکل ویژه‌ای برای این نهادها فراهم شود. 62

دیگر اپلیکیشن‌های پیام‌رسان

با وجود تلاش‌های حقوقی و مالی دولتی برای حمایت از سرویس‌های پیام‌رسان داخلی، این اپلیکیشن‌ها هنوز هم به اندازه همتایان غیرایرانی خود، مورد استفاده قرار نمی‌گیرند. تلگرام، با حدود ۴۰ میلیون کاربر، و واتس‌اپ، با حدود ۳۳ میلیون کاربر، از جمله پرطرفدارترین اپلیکیشن‌ها در بین مردم ایران هستند.[۶۳] علاوه بر این، اپلیکیشن‌های داخلی معمولاً خود را از لحاظ طراحی، قابلیت اطمینان و امنیت، با همتایان غیرایرانی خود مقایسه می‌کنند.
ما به همین دلیل تصمیم گرفتیم تا واتس‌اپ و تلگرام را نیز در این ارزیابی به شمار بیاوریم. هر چند باید توجه داشت که به دلایل مختلفی همچون دایره‌ی حقوقی‌ای که این شرکت‌ها تحت آن به فعالیت می‌پردازند و همینطور موضوع زبان، مقایسه‌ی کامل این اپلیکیشن‌ها با اپلیکیشن‌های ایرانی امکان‌پذیر نیست. با این حال به دلیل اینکه میلیون‌ها ایرانی از آنها استفاده می‌کنند، این شرکت‌ها نیز تعهدات و وظایفی در قبال حقوق دیجیتال کاربران ایرانی خود دارند.

58 “Gap Messaging App Agrees to Expand International Services to Countries in the Region,” Gap Blog, July 20,2019, https://bit.ly/319JdB3, it is important to note that in August 2020, MTN South Africa decided to divest and leave Iran’s market partly due to the sanctions.
59 “Agreement Between Gap Messaging App and Telecommunication Company of Iran,” Gap Blog, January 15, 2019, https://bit.ly/2H8xbRn
60 Cafe Bazaar, https://bit.ly/31dyq97, date accessed: Jun. 5, 2020
61 Sina Zakery, “Analysis of Bale Messaging App; Banking Replacement for Telegram,” ITResan, April 16, 2018, https://bit.ly/344jo7b
62 Massoumeh Bakhshipour, “Free Services for Domestic Messaging Apps from National Information Network’s Primary Data Centre,” August 29, 2020, Mehr News, https://bit.ly/3duHdZ8
63 “How Many Iranian Telegram and Domestic Messaging App Users are There,” IRNA , May 22, 2019, https://bit.ly/2T2jRk9 and WhatsApp Search on Cafe Bazaar, Cafe Bazaar, accessed Jul. 5, 2020 https://bit.ly/35Mfpfc

واتس‌اپ

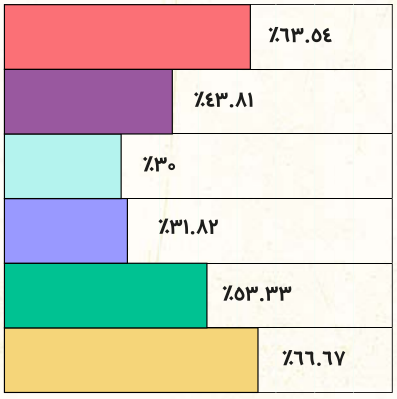
واتس‌اپ، یک سرویس پیام‌رسان و VoIP است که روی کافه بازار(فروشگاه اپلیکیشن های اندروید در ایران) دارای ۳۳ میلیون دانلود است.

واتس‌اپ یک شرکت خصوصی آمریکایی و متعلق به فیسبوک است.

صفحه‌ی سیاست‌های حفظ حریم خصوصی	✓
صفحه‌ی شرایط و ضوابط استفاده از خدمات	✓
الگوهای برتر طراحی و توسعه خدمات دیجیتال	
رمزنگاری	رمزنگاری سرتاسری در واتس‌اپ به صورت پیش‌فرض تعبیه شده است.
امنیت سایبری	واتس‌اپ دارای برنامه‌های باگ باونتی (bug bounty) است، اما واتس‌اپ یک اپلیکیشن متن-باز (open source) نیست.
آیا این شرکت گزارش شفافیت (Transparency Report) منتشر می‌کند؟ فیسبوک به عنوان شرکت مادر واتس‌اپ، گزارش شفافیت منتشر می‌کند اما این گزارش‌ها بر اساس نوع سرویس‌ها (از جمله واتس‌اپ، اینستاگرام، فیسبوک مسنجر و سایر سرویس‌های فیسبوک) تفکیک نمی‌شوند.	

این شرکت دارای صفحه‌ی اطلاعات حقوقی به زبان فارسی است، اما تمام مطالب درباره سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات به زبان فارسی ترجمه نشده است.

امتیازات:



دسترسی به سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات، و به‌روزرسانی این سیاست‌ها:

شفافیت در مورد جمع‌آوری داده، به اشتراک‌گذاری و نگهداری داده و کنترل کاربران بر داده‌های خود:

شفافیت در مورد چگونگی اعمال سیاست‌های مربوط به شرایط و ضوابط استفاده از خدمات:

شفافیت در مورد درخواست‌های نهادهای حکومتی و طرفین ثالث:

شفافیت در مورد به کارگیری الگوهای برتر طراحی و توسعه خدمات دیجیتال:

تلاش‌های شرکت در آگاهی رسانی به کاربران درباره خطرهای آنلاین و چگونگی حفاظت از خود:

توصیه‌های فوری:

- واتس‌اپ می‌بایست نسخه‌های کامل و قابل فهمی از صفحات «سیاست‌های حفظ حریم خصوصی» و «شرایط و ضوابط استفاده از خدمات» به زبان فارسی منتشر کند. این موضوع که زبان فارسی یکی از زبان‌های مورد تایید این اپلیکیشن است، نکته مثبتی است. با این حال، در حال حاضر اطلاعات فارسی روی وبسایت این اپلیکیشن، محدود به اطلاعاتی ابتدایی درباره حفظ حریم خصوصی، قابلیت‌های اپلیکیشن و سوالات متداول است.
- واتس‌اپ باید بداند که خصوصیت رمزگذاری سرتاسر (E۲EE) هرچند که بسیار مفید و لازم است، اما این سرویس را به طور ۱۰۰٪ در مقابل خطراتی مانند فیشینگ‌های هدف‌دار (spear phishing)، که برای جاسوسی در کار کنشگران حقوق بشر و روزنامه‌نگاران به کار می‌رود، مصون نگه نمی‌دارد. واتس‌اپ می‌بایست برای جلوگیری از چنین خطراتی که کاربران ایرانی را مورد هدف قرار می‌دهند، اقدام کند. علاوه بر این، می‌بایست مطالب آموزشی و کاربردی بیشتری به زبان فارسی، برای آگاهی رسانی در مورد این خطرات، به کاربران خود که سطح سواد دیجیتالی مختلفی دارند، ارائه کند.
- واتس‌اپ می‌بایست درباره مشارکت خود در طرح‌های چند-ذینفعی (multi-stakeholders initiative) اطلاعات بیشتری را به صورت علنی اعلام کند. این نوع رایزنی‌ها نباید به گروه‌های ساکن در آمریکای شمالی و اروپا خلاصه شود. بلکه واتس‌اپ باید ثابت کند که این نوع مشارکت‌ها برای گروه‌های مختلف مدنی ساکن در کشورهای در حال توسعه نیز امکانپذیر است و نظرات و مشکلات این گروه‌ها به دقت و جدیت بررسی می‌شوند.
- فیسبوک (شرکت مادر واتس‌اپ) می‌بایست اعلام کند که با درخواست‌های دولت ایران و طرفین ثالث که می‌خواهند به اطلاعات کاربران ایرانی دسترسی داشته باشند، به چه صورت برخورد می‌کند. بر اساس آنچه در گزارش شفافیت این شرکت نوشته شده است، در مواردی دولت ایران درخواست اضطراری دریافت اطلاعات کرده است، که البته این درخواست‌ها از طرف فیسبوک بی‌پاسخ هم نمانده‌اند. اما درباره‌ی ماهیت و نوع این درخواست‌ها هیچگونه شفافیتی وجود ندارد.

تلگرام

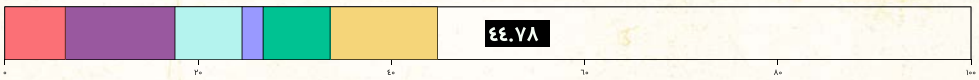
تلگرام با وجود اینکه از سال ۲۰۱۸ فیلتر شده است، با حدود ۴۰ میلیون کاربر همچنان یکی از پرطرفدارترین اپلیکیشن‌های پیام‌رسان در ایران است. این شرکت با فراهم آوردن APIهای متعددی مانند bot APIs، TDLib، و Telegram API، به توسعه‌دهندگان ایرانی این امکان را داده است تا بتوانند بات‌های اینترنتی متعدد و حتی نسخه‌های غیررسمی تلگرام، مانند تلگرام طلایی، طلاگرام و هات‌گرام، بسازند.[67]

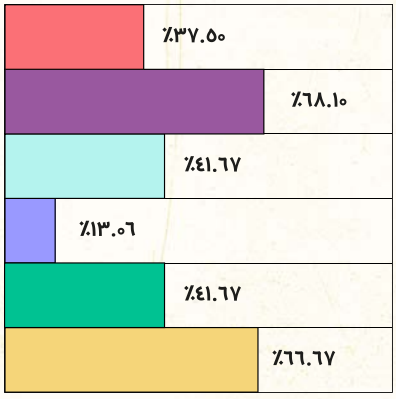
این شرکت تحت نام Telegram FZ LLC در انگلستان ثبت شده و تیم آنها در حال حاضر در شهر دبی امارات مستقر هستند.[68]

صفحه‌ی سیاست‌های حفظ حریم خصوصی	✓
صفحه‌ی شرایط و ضوابط استفاده از خدمات	✓
الگوهای برتر طراحی و توسعه خدمات دیجیتال	
رمزنگاری	گروه‌ها و کانال‌های تلگرام به صورت سرتاسری رمزگذاری نشده‌اند. با این حال، کاربران اگر می خواهند ارتباط رمزگذاری شده‌ای داشته باشند می‌توانند گزینه‌ی گپ محرمانه "Secret Chats" را انتخاب کنند.
امنیت سایبری	تلگرام دارای برنامه‌های باگ بانونتی نیست، اما این اپلیکیشن نه به طور کامل ولی تا حدودی متن-باز است. گزارش‌های فنی این اپلیکیشن در دسترس هستند. این شرکت همچنین برای محققانی که بتوانند ضعف‌های امنیتی تلگرام را بیابند، جایزه در نظر می‌گیرد.[69]
آیا این شرکت گزارش شفافیت (Transparency Report) منتشر می‌کند؟	تلگرام، یک کانال شفافیت دارد اما هیچ اطلاعاتی داخل این کانال موجود نیست.

بخش سوالات متداول تلگرام، که اطلاعات زیادی درباره حریم خصوصی و شرایط و ضوابط استفاده از خدمات دارد، به زبان فارسی موجود است.

امتیازات:





دسترسی به سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات، و به‌روزرسانی این سیاست‌ها:

شفافیت در مورد جمع‌آوری داده، به اشتراک‌گذاری و نگهداری داده و کنترل کاربران بر داده‌های خود:

شفافیت در مورد چگونگی اعمال سیاست‌های مربوط به شرایط و ضوابط استفاده از خدمات:

شفافیت در مورد درخواست‌های نهادهای حکومتی و طرفین ثالث:

شفافیت در مورد به کارگیری الگوهای برتر طراحی و توسعه خدمات دیجیتال:

تلاش‌های شرکت در آگاهی رسانی به کاربران درباره خطرهای آنلاین و چگونگی حفاظت از خود:

توصیه‌های فوری:

- سیاست‌های حفظ حریم خصوصی و صفحه‌ی شرایط و ضوابط استفاده از خدمات باید روی صفحه اول وبسایت تلگرام در دسترس باشند.
- در زمان نوشتن این گزارش، واسط کاربری (UI) تلگرام فارسی به صورت بتا وجود داشت. به جز صفحه سوالات متداول ابتدایی، مطالب دیگر مانند سوالات متداول تخصصی، سیاست‌های حفظ حریم خصوصی و صفحه‌ی شرایط و ضوابط استفاده از خدمات به زبان فارسی در دسترس نیستند. این شرکت می‌بایست نسخه‌های فارسی این مطالب را فراهم کند.
- تلگرام باید اطلاعاتی درباره‌ی حذف محتوا، حذف صفحات کاربری، درخواست‌های طرفین ثالث و درخواست تجدید نظر، در گزارش شفافیت و روی وبسایت خود منتشر کند تا همه بتوانند بدون نیاز به ساخت یک حساب کاربری به این اطلاعات دسترسی داشته باشند.[70] تلگرام، یک کانال شفافیت دارد اما هیچ اطلاعاتی داخل این کانال منتشر نمی‌شود. همچنین کانال دیگری به نام ISIS-Watch وجود دارد که تعداد حساب‌های کاربری تروریستی توقیف شده روی آن گزارش داده می‌شود، اما درباره صفحات کاربری دیگر و محتواهایی که محدود یا توقیف می‌شوند، اطلاعاتی وجود ندارد.
- تلگرام می‌بایست روی صفحه‌ی API خود، جزییات و ضوابط مربوط به استفاده‌ی نابجا از API و همینطور سیاست‌های جلوگیری و برخورد با استفاده نادرست از بات‌های اینترنتی را اضافه کند. (مطالعه راهنمای سال ۲۰۲۰ RDR درباره سیاست‌های استفاده از بات‌های اینترنتی را در این **لینک** بخوانید.)

توصیه‌های کلی

ما توصیه‌های خود را به دو بخش توصیه‌هایی برای شرکت‌های فناوری ایرانی و توصیه‌هایی برای نهادهای مسئول در ایران تقسیم کردیم.

توصیه‌هایی برای شرکت‌های فناوری در ایران

با وجود اینکه ما تنها تعداد معدودی از اپلیکیشن‌های پیام‌رسان را در این تحقیق بررسی کرده‌ایم، اما این توصیه‌ها به اکثر شرکت‌هایی که فعالیت اصلی‌اشان تولید اپلیکیشن و خدمات اینترنتی و موبایلی است، تعمیم داده می‌شود:

شفافیت در سیاست‌های حفظ حریم خصوصی

- سیاست‌های حفظ حریم خصوصی باید به زبانی ساده و غیرتخصصی نوشته شود. این مطالب باید روی وب‌سایت شرکت‌ها و فروشگاه‌های اپلیکیشن در دسترس باشند.
- هر موقع شرکت‌ها سیاست‌های حفظ حریم خصوصی خود را به‌روزرسانی می‌کنند، می‌بایست با فرستادن پیام، ایمیل یا notification کاربران را از این تغییرات مطلع ساخته و آرشیو تغییرات را روی وبسایت خود نگه دارند.
- شرکت‌ها باید به صورت علنی اعلام کنند که چه نوع داده‌هایی جمع‌آوری می‌شود، به چه دلیل جمع‌آوری می‌شوند، به چه صورت ذخیره می‌شوند، و برای چه مدتی نگه داشته می‌شوند.
- شرکت‌ها باید در بخش سیاست‌های حفظ حریم خصوصی و داده‌ها، درباره روش‌های به اشتراک‌گذاری داده با شرکت‌های تبلیغاتی و کارگزاران داده، چگونگی استفاده از کوکی‌ها و همینطور سیاست‌های عرضه‌ی APIهای خود، شفافیت داشته باشند.

شفافیت در شرایط و ضوابط استفاده از خدمات و چگونگی اعمال این ضوابط

- با ایجاد ضوابطی شفاف، شرکت‌ها باید نوع محتوا و فعالیت‌های مجاز و غیرمجاز بر روی سرویس خود را اعلام کنند.
- شرکت‌ها باید به صورت شفاف اعلام کنند که چطور شروط لازم برای کاربری و ضوابط استفاده از خدمات را اعمال می‌کنند. باید اعلام کنند که از چه شیوه‌های خودکار یا غیرخودکاری برای نظارت و کنترل فعالیت‌ها و محتوای منتشر شده استفاده می‌کنند، و اگر این ضوابط زیر پا گذاشته شوند، با آن کاربر یا محتوای منتشر شده چه برخوردی می‌کنند. در مورد

64 WhatsApp scores are from RDR's 2019 assessment. We used the assessment to ensure our scoring is consistent with the RDR's internal scoring system. You can find it on https://bit.ly/3j62Kby
65 Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab Research Report No. 113, University of Toronto, Sep. 2018, https://bit.ly/34Af3Jk
66 Facebook Transparency page for Iran, accessed on Jul. 5, 2020, https://transparency.facebook.com/government-data-requests/country/IR
67 See the search for Telegram on Cafe Bazaar, accessed July 5, 2020, https://bit.ly/37ctuVF and Telegram APIs, Telegram, accessed Jul. 5, 2020, https://core.telegram.org/
68 Telegram FAQ, Telegram, accessed on Jul. 8, 2020, https://bit.ly/3nWof29
69 "$300,000 for Cracking Telegram Encryption," Telegram, Nov. 4, 2014, https://bit.ly/31aU8KU
70 Pavel Durov, "Telegram and the Freedom of Speech," October 29, 2017, https://bit.ly/2IyUpAF

اپلیکیشن‌های پیام‌رسان، بسته به نوع عملکرد هر سرویس، آن شرکت باید به صورت علنی اعلام کند که چه تفاوت‌هایی میان ضوابط استفاده از سرویس‌های خصوصی و عمومی، مانند چت‌های دو نفره، گروهی، و کانال‌های خصوصی و عمومی وجود دارد و از چه روش‌هایی برای اعمال این قوانین در هر بخش استفاده می‌شود.

- در صورت زیر پا گذاشتن ضوابط، اگر شرکتی بخواهد محتوای منتشر شده را حذف کند یا دسترسی آن کاربر را به خدمات شرکت محدود کند، باید پیش از این اقدام کاربر را مطلع سازد و به صورت شفاف دلیل این کار را توضیح دهند.

- شرکت‌ها می‌بایست ضوابط استفاده از API و بات‌های اینترنتی خود را به صورت شفاف برای توسعه‌دهندگان و برنامه‌نویسان مشخص کنند. همچنین باید اطلاعاتی درباره روش‌های مبتنی بر اصول امنیت سایبری خود برای جلوگیری از سوء استفاده از APIها، در نظر بگیرند.

گزارش شفافیت

- شرکت‌ها می‌بایست بر روی وبسایت خود سامانه شفافیت داشته باشند. شرکت‌ها باید دست کم، قواعد «سانتا کلارا درباره شفافیت و پاسخگویی» را رعایت کنند.

- در سامانه شفافیت، آنها می‌بایست گزارش‌های خود را به صورت متناوب (هر شش ماه یا هر یک سال یک‌بار) منتشر کرده و با اعلام علنی موارد زیر، درباره عملکرد خود شفاف‌سازی کنند:

  - تعداد پست‌ها و صفحات کاربری که حذف شده‌اند، چه به صورت خودکار و چه به صورت غیرخودکار.

  - تعداد درخواست‌های دریافت شده از نهادهای دولتی و مقامات قضایی برای حذف محتوا و صفحات کاربری افزون بر اینکه چه تعداد از این درخواست‌ها پذیرفته شده و چه تعداد رد شده است.

  - تعداد درخواست‌های دریافت شده از نهادهای غیردولتی (طرفین ثالث، شرکت‌های دیگر، کاربران و غیره) برای حذف محتوای سایر کاربران و درخواست دسترسی به اطلاعات آنها، افزون بر اینکه چه تعداد از این درخواست‌ها پذیرفته و چه تعداد رد شده است.

  - طبقه‌بندی محتوا، صفحات و حساب‌های کاربری، و بات‌های حذف شده بر اساس نوع تخطی در ضوابط استفاده از خدمات (برای مثال: مطالب مربوط به سوءاستفاده و آسیب جنسی به کودکان، زیر پا گذاشتن قانون کپی‌رایت، پورنوگرافی، اقدام تروریستی، وغیره)

- شرکت‌ها باید سامانه‌ی مخصوصی برای درخواست‌های نهادهای دولتی، مقامات قضایی و انتظامی برای دسترسی به اطلاعات کاربران و یا حذف محتوا، داشته باشند. شرکت‌ها در این سامانه، می‌بایست خط قرمزهای خود و روند رسمی مرحله به مرحله‌ی خود را برای دریافت چنین درخواست‌هایی از مقامات و چگونگی بررسی آنها ارائه دهند. همچنین باید نمونه‌های فرضی از درخواست موجه و غیرموجه را نیز در این سامانه اضافه کنند.

طراحی بر مبنای حفظ حریم خصوصی و امنیت سایبری

- شرکت‌ها می‌بایست برای رمزنگاری داده‌ها از الگوریتم‌های قوی و مورد تایید پژوهشگران حریم خصوصی استفاده کنند تا اطلاعات کاربران را در زمان انتقال و همینطور تا زمانی که این داده‌ها ذخیره می‌شوند، حفاظت کنند. رمزنگاری قوی باید به صورت پیش‌فرض (by default) تعبیه شود. در جایی که این امکان وجود داشته باشد، از جمله اپلیکیشن‌های پیام‌رسان و سرویس‌های VoIP، باید رمزگذاری سرتاسری (End to End Encryption) پیاده‌سازی شود. گزارش‌های فنی که شامل توضیحات درباره الگوریتم‌های رمزنگاری هستند، باید به صورت علنی روی صفحات آنلاین رسمی هر شرکت، در دسترس عموم و بالاخص پژوهشگران حریم خصوصی و امنیت سایبری قرار بگیرند.

- شرکت‌ها برای سرویس‌هایی که نیازمند ساخت حساب کاربری هستند، می‌بایست از کاربران بخواهند تا رمز عبور قوی و مطمئن انتخاب کنند. اگر شرکتی به اطلاعات حساس افراد مانند نام، شماره تلفن، نشانی و غیره دسترسی دارد، باید حتماً گزینه‌ی تصدیق حساب چند مرحله‌ای (Multi-factor Authentication) را برای کاربران خود فراهم کند.

- شرکت‌ها می‌بایست جمع‌آوری اطلاعات کاربران خود را به میزانی که فقط برای ارائه‌ی صحیح سرویس ضروری است محدود کنند. بسته به نوع سرویس، جمع‌آوری، پردازش، و ذخیره‌ی اطلاعات حساس کاربران باید از روش‌های مخفی نگه داشتن هویت، مانند مستعارسازی (pseudonymization)، ناشناس سازی (anonymization) و غیره استفاده شود.

- طراحان UX/UI، هنگام طراحی یک اپلیکیشن باید دسترسی به تنظیمات مربوط به حریم خصوصی و امنیت را تا حدی ساده طراحی کنند که افراد با سطوح مختلف سواد دیجیتالی و همینطور افراد با توانایی‌های متفاوت جسمانی و بینایی نیز بتوانند این تنظیمات را متوجه شده و از آنها استفاده کنند.

- شرکت‌ها می‌بایست یک تیم داخلی مخصوص امنیت سایبری داشته باشند - که بتوانند شیوه‌های مرسوم امنیت سایبری مانند تشکیل تیم قرمز و آبی (red and blue teaming) یا مدل‌سازی تهدیدهای سایبری (threat modeling) را برای سرویس‌های شرکت پیاده‌سازی کنند - این تیم‌ها باید پیش از عرضه یک محصول، تست‌های مختلف امنیت سایبری را روی آن محصول اجرا کنند. علاوه بر این، شرکت‌ها باید پذیرای دریافت گزارش بررسی از محققان امنیت و حریم خصوصی نیز باشند؛ این محققان نقاط ضعف و باگ‌های امنیتی را در یک نرم‌افزار پیدا می‌کنند، روشی متداول که باگ باونتی (bug bounty) نامیده می‌شود. علاوه بر این، هنگام طراحی و کدنویسی یک نرم افزار، شرکت‌ها باید بهترین روش‌های امنیتی را، از جمله پرهیز استفاده از کتابخانه‌های ناامن، بکار گیرند. برای دریافت اطلاعات بیشتر در زمینه روش‌های حفظ امنیت و حریم خصوصی در طراحی و کدنویسی برای خدمات خود به منابعی چون the Digital Standards و **OWASP Security Testing Guide** رجوع کنید. (بخش پیوست دیده شود)

- روش‌های طراحی به کار گرفته شده به منظور حفظ حریم خصوصی و امنیت، مانند گزارش‌ها و جزییات فنی، کدهای متن-باز و غیره باید روی وبسایت (وبلاگ رسمی، شبکه‌های چندرسانه‌ای و پلتفرم‌های میزبانی نرم‌افزار مانند GitHub و صفحات کدنویسان و سوالات متداول)، برای عموم در دسترس باشد.

روند دریافت و بررسی درخواست‌های تجدیدنظر و کانال‌های دریافت نظر و پیشنهاد

- شرکت‌ها می‌بایست روندی ساده و قابل فهم برای درخواست‌های تجدیدنظر فراهم کنند. کاربری که محتوا یا صفحه او محدود یا مسدود شده است، باید به راهی دسترسی داشته باشد که بتواند درخواست تجدیدنظر کند و یا توضیحات واضح شرکت در مورد این تصمیم را جویا شود.

- شرکت‌ها می‌بایست آدرس ایمیل، شماره تلفن برای خدمات مشترکین، شبکه‌های رسانه اجتماعی، فرم‌های آنلاین و پرسشنامه داشته باشند تا بین خود، کاربران و هر گروه دیگری که در عملکرد این شرکت سهیم است، امکان ارتباط و دریافت نظرها و پیشنهادها را فراهم کنند.

شفافیت در ساختار سیاست‌گذاری شرکت

- شرکت‌ها می‌بایست روی وبسایت خود، بخش «درباره ما» داشته باشند. در این صفحه باید با شفافیت درباره اینکه این شرکت متعلق به چه سازمان یا شخصی است و اینکه آیا از سوی یک شرکت مادر اداره می‌شود توضیح دهند. همچنین اعلام کنند که اسم شرکت مادر چیست، آیا وابسته به نهادی دولتی یا حکومتی است یا خیر.

- در صورت وقوع هرگونه نشت اطلاعاتی، شرکت‌ها موظف هستند تا عموم را از طریق نشر اطلاعیه‌ی عمومی و فرستادن ایمیل به کاربران، از ابعاد و نحوه‌ی ایجاد این نشت مطلع سازند. علاوه بر این، تمام این اطلاعات را باید در گزارش شفافیت خود که به صورت متناوب منتشر می‌شود، درج کنند.

- شرکت‌ها می‌بایست از «اصول راهنمای تجارت و حقوق بشر سازمان ملل» جهت ارزیابی اثرات حقوق بشری — که به سبب ارائه خدمات و فعالیت‌های شرکت در آن دخیلند— استفاده کنند. آنها باید به صورت علنی اعلام کنند که به حقوق بشر احترام می‌گذارند و از طریق عضویت در طرح‌های چند-ذینفعی با جامعه مدنی — بالاخص با نهادهایی که با گروه‌های آسیب‌پذیر جامعه مانند کودکان، اقلیت‌های قومی، جنسی و جنسیتی، مذهبی و پناهجویان کار می‌کنند— مشاوره کنند. شما می‌توانید از راهنمای ضمیمه شده به این گزارش استفاده کنید تا گفت‌وگو در این زمینه را در شرکت خود آغاز کنید. برای دانلود راهنما به این **لینک** مراجعه کنید.

- برای حصول اطمینان از این موضوع که کارکنان یک شرکت با مسائل مربوط به حقوق دیجیتال آشنایی دارند، آن شرکت می‌بایست برای کارکنان خود (از مدیران عالی‌رتبه گرفته تا کارشناسان فنی، و گروه‌های حقوقی، فروش، منابع انسانی) مطالب و ورکشاپ‌های آموزشی فراهم کند تا کارکنان بدانند چطور باید از آسیب‌های احتمالی به حقوق کاربران در فعالیت‌های مرتبط با حرفه‌ی خود جلوگیری کرده یا آن‌ها را محدود کنند.

- شرکت‌ها باید در روند قانونگذاری کشور، در جایی که مرتبط با حوزه‌ی تکنولوژی است، با کمیسیون‌های مجلس و نهادهای دولتی گفتگو داشته باشند، نگرانی‌های خود را اعلام کنند و از حقوق دیجیتال کاربران خود پشتیبانی کنند. اتحادهای میان-شرکتی، نوشتن نامه‌های سرگشاده به مسئولان، گفتگو با رسانه‌ها و مطبوعات از جمله راهکارهایی است که به تحقق این امر کمک می‌کند.

توصیه‌هایی برای نهادهای مسئول در ایران

- نهادهای مسئول در ایران می‌بایست برنامه‌های بومی‌سازی اجباری و بررسی‌نشده‌ی اینترنت که اصول بی‌طرفی شبکه را نقض می‌کنند، متوقف کنند. این برنامه‌ها که عموماً با قطع دسترسی به سرویس‌های بین‌المللی از طریق فیلترینگ یا تخصیص تعرفه‌هایی با امتیازات خاص به خدمات داخلی، همراه است، آزادی انتخاب و حق دسترسی به اطلاعات آزاد را از کاربران ایرانی سلب می‌کند و به صورت ناعادلانه‌ای بر آزادی انتخاب و حقوق دیجیتال گروه‌های آسیب‌پذیرتر جامعه، که در موقعیت اقتصادی-اجتماعی پایین‌تری قرار دارند، تاثیرات نامطلوبی می‌گذارد. اپلیکیشن‌های بخش خصوصی که در ابتدا اعلام شده بود هدف اصلی طراحی‌شان تولید «پیام‌رسان» است، تبدیل به پلتفرم‌هایی شده‌اند که یک روز میزبان خدمات دیجیتال یک نهاد دولتی هستند و روز دیگر محل ارائه‌ی خدمات مالی دیگر نهاد مسئول. اضافه کردن امکان خدمات دولتی به اپلیکیشن‌های پیام‌رسان داخلی، تشویق‌های مالی کوته‌نظرانه برای استفاده از شبکه ملی ارتباطات به جای اینترنت بین‌المللی، و یا حمایت‌های دولتی از شرکت‌های نوپا از طریق فراهم آوردن خدمات دولتی، مانند دسترسی رایگان به مراکز داده، نباید به سادگی به عنوان برنامه‌های مرسوم دولت برای حمایت از خدمات داخلی تلقی و تبلیغ شوند. در نبود سازوکارهای نظارتی شفاف و عمومی، این گونه همکاری‌های عجولانه و مبهم، موجب از بین رفتن اطمینان کاربران به این شرکت‌ها می‌شوند. به علاوه، چنین سیاست‌هایی باعث کنترل و نظارت بیش از حد نهادهای دولتی بر کار این شرکت‌ها، ترویج فرهنگ تبعیض بین دولت و بخش خصوصی و تشویق‌کننده‌ی رقابت ناعادلانه بین شرکت‌های فناوری خصوصی شده است که امکان ورود و رشد در بازارهای بین‌المللی را برای شرکت‌های فناوری ایرانی محدود می‌کند.
نهادهای سیاست‌گذار در ایران می‌بایست چارچوب

قانونی قوی و مبسوطی برای محافظت از داده اعمال کند که با استانداردهای بین‌المللی حقوق بشر مطابقت داشته باشد. دولت باید برای شرکت‌ها، ضوابط کارشناسانه‌ای مربوط به امنیت و حریم خصوصی تنظیم کند. تا زمانی که یک چارچوب قانونی، جامع و مبتنی بر اصول حقوق بشری وجود نداشته باشد، مسئولین باید پیشبرد طرح ساماندهی پیام‌رسان‌های اجتماعی را متوقف کند، چرا که این طرح، آزادی‌های اینترنتی مردم ایران را محدود کرده و کنترل درگاه‌های اینترنتی را تحت نظارت نیروهای مسلح قرار می‌دهد.

سخنی کوتاه با فعالان جامعه مدنی و محققان فناوری

- باید این موضوع را دوباره تاکید کنیم که این گزارش، تاثیرات منفی وارد شده به حقوق دیجیتال کاربران ایرانی اینترنت را که ممکن است به دلیل عدم شفافیت در سیاست‌های شرکت‌های فناوری اتفاق بیفتد، بررسی می‌کند.

هدف این گزارش، ارزیابی صداقت و صحت ادعاهای هیچ‌کدام از این شرکت‌ها و یا اعمال موازین حقوق بشر در فعالیت‌های دیگری، مثل زیرساخت‌های فنی، تاثیرگذاری آنها در شکل‌گیری سیاست‌های دیجیتال در ایران و یا مسائل خارج از حوزه فعالیت این گزارش، نیست. بنابراین، بررسی وجوه دیگر فعالیت این شرکت‌ها، نیازمند این است که جامعه مدنی تحلیل گسترده‌تری از این موارد ارائه داده و شرکت‌ها را در صورت نقض حقوق بنیادین کاربران پاسخگو نگاه دارد.

پیوست‌های روش تحقیق

چالش‌ها و آموخته‌ها

- روش تحقیق شاخص RDR برای بررسی شرکت‌های خدمات اینترنتی، مخابراتی و تلفن همراه به کار می‌رود. ما پژوهش خود را با شرکت‌های مخابراتی ایرانی آغاز کردیم. ولی از اوایل کار متوجه شدیم که وبسایت بیشتر این شرکت‌ها حتی قوانین ابتدایی استفاده از خدمات و سیاست‌های حفظ حریم خصوصی را ندارد. علاوه بر این، بیشتر شرکت‌های مخابراتی به صورت مستقیم یا غیرمستقیم متعلق به نهادهای وابسته به حکومت هستند و به همین دلیل، تحت تعریف استاندارد از «بخش خصوصی» قرار نمی‌گیرند.

- براساس روش تحقیق شاخص RDR، قبل از انتشار نتیجه نهایی، این امکان به شرکت‌ها داده میشود تا بازخورد خود را از نتایج اولیه ارزیابی شرکتشان با نویسندگان تحقیق در میان بگذارند.[VI] البته همه شرکت‌ها بازخورد خود را اعلام نمی‌کنند و RDR صرف نظر از اینکه شرکتی نظرات خود را راجع به نتایج اولیه تحقیق بیان کند یا نه، آن شرکت را مورد ارزیابی نهایی قرار میدهد. به دلایل متعددی ما نتوانستیم در این فرآیند دریافت بازخورد با شرکت‌های فناوری ایرانی ارتباطی برقرار کنیم. دلیل اصلی این موضوع حفظ امنیت گردآورندگان این پژوهش و همینطور مسئولین شرکت‌ها بود. امیدواریم که در پژوهش‌های بعدی بتوانیم برای شرکت‌ها پرسشنامه‌ای فراهم کنیم تا بتوانند نظرات خود را به صورت ناشناس با ما به اشتراک بگذارند. همچنین امیدواریم که با پژوهشگران RDR همکاری کرده تا راه‌های جایگزین ارتباط با شرکت‌ها را در آینده بررسی کنیم.

- عملکرد هیچ‌کدام از شرکت‌های مورد بررسی در این گزارش، در هیچ یک از مولفه‌های «سیاست‌گذاری شرکت» رضایت‌بخش نیست. این موضوع در تصمیم ما مبنی بر اینکه امتیازات قیاسی بین شرکت‌ها را چطور به تصویر بکشیم، تاثیرگذار بوده است. ما تصمیم گرفتیم که به هر شرکت، جمع امتیازات (امتیاز حریم خصوصی + امتیاز آزادی بیان + امتیاز سیاست‌گذاری) تعلق نگیرد، و به جای آن، امتیازات را از طریق شش گروه مولفه‌های ارزیابی شده در گزارش به نمایش گذاشتیم.

- معمولا درنظام‌های بسته یا نیمه‌بسته سیاسی، شفافیت لازم و یا حد و مرز مشخصی برای مداخله نهادهای حکومتی در تصمیمات اقتصادی و مدیریتی شرکت‌های فناوری بخش خصوصی وجود ندارد. این عدم شفافیت — به‌خصوص در شیوه‌های اشتراک‌گذاری داده — تاثیر بسیار شدیدی بر حقوق انسانی کاربران دارد. بنابراین اضافه کردن مولفه‌هایی ساده مربوط به مالکیت شرکت‌ها، مانند وجود صفحه «درباره ما»، جلسه‌های سالانه، گزارش‌های مالی، نقش اعضای هیئت مدیره، داشتن آدرس ایمیل و شبکه‌های اجتماعی، می‌تواند در بالا بردن شفافیت و پاسخگویی موثر واقع شود. علاوه بر این، هدف ما این است که در گزارش‌های بعدی، گزینه‌های موجود را برای شرکت‌های ایرانی ارزیابی و معرفی کنیم، تا اگر به دلایل مختلف سیاسی و اقتصادی این شرکت‌ها قادر نیستند به طرح‌های چند ذینفعی MSI بین‌المللی بپیوندند، بتوانند با نهادهای جامعه مدنی به صورت امن و موثری ارتباط برقرار کنند.

- باید اذعان داشت که حکومت‌های مستبد، قدرت بی‌حد و حصری برای کنترل، نظارت بیش از حد و

71 “2019 Research Process”, Ranking Digital Rights, 2019, https://bit.ly/3nQUBeK

جریمه و مجازات شرکت‌های خصوصی دارند. اگر به شکل واقع‌بینانه به موضوع نگاه کنیم، به نظر آرمان‌گرایانه می‌رسد که انتظار داشته باشیم شرکت‌ها در برابر درخواست‌های بی‌مرز و غیرمجاز دولت‌ها، که حقوق دیجیتال افراد را به خطر می‌اندازند، به تمام و کمال مقاومت کنند. بنابراین، در چنین کشورهایی، اقدامات پیش‌گیرانه همچون طراحی سرویس بر مبنای حفظ حریم خصوصی ، پیاده‌سازی امنیت به صورت پیش‌فرض، طراحی UX/UI با محوریت حقوق بشر، و سواد دیجیتالی، نقش بسیار مهمی در محافظت از کاربران ایفا می‌کند. به همین دلیل ما بخشی را تحت عنوان «طراحی بر مبنای حفظ حریم خصوصی و امنیت سایبری » به توصیه‌های خود اضافه کردیم.

- در زمان انجام این پژوهش، متوجه شدیم که ضوابط کدنویسی و شرایط و ضوابط استفاده از خدمات API شرکت‌ها (مانند استفاده از APIها که ساخت بات‌ها را ممکن می‌سازد، سرویس‌های دیجیتالی را تعامل‌پذیر می‌کند و تولید نسخه‌های غیررسمی از یک سرویس را ممکن می‌سازد) راه‌های جدیدی را برای سواستفاده باز کرده‌اند. باید توجه داشت که مطالعه راهنمای RDR برای سال ۲۰۲۰، مولفه‌های مربوط به سیاست‌های بات‌رانی را نیز شامل می‌شود که تا حدی نگرانی‌های ما درباره بکارگیری APIها را پوشش می‌دهد.

- روش‌های جمع‌آوری و به اشتراک‌گذاری داده از طریق APIها بین توسعه‌دهندگان ثالث و شرکت‌ها، باعث شده که ارزیابی ما با چالش روبه‌رو شود. اطلاعات درباره شرایط و ضوابط استفاده از خدمات برای توسعه‌دهندگان را می‌توان با اضافه کردن راهنمای تحقیق "research guidance" به مولفه‌های جمع‌آوری داده و اشتراک‌گذاری داده شخص ثالث مانند P۳, P۴, P۹ به تفصیل بررسی کرد.

- همچنین، لازم است که شرکت‌ها درباره چگونگی اجرای شرایط و ضوابط استفاده از خدمات برای توسعه‌دهندگان، شفافیت بیشتری داشته باشند، به‌خصوص در مورد سوءاستفاده از کدهای مبدأ و ساخت نسخه‌های غیررسمی از یک سرویس، که می‌تواند حریم خصوصی افراد را به خطر اندازد. تقاضا برای تعامل‌پذیرتر شدن (interoperability) خدمات دیجیتالی احتمالا موجب خواهد شد که در آینده، درباره روابط توسعه‌دهندگان ثالث و شرکت‌ها در خصوص حقوق دیجیتال بیشتر بشنویم.

- نگرانی‌های حقوق بشری ویژه‌ای درباره اپلیکیشن‌های پیام‌رسان وجود دارد. برخی از این نگرانی‌ها شامل این موارد است: آزار و اذیت در فضای آنلاین، دست به دست شدن (وایرال شدن) محتوای گمراه‌کننده و نادرست، داکسینگ (نشر عمومی اطلاعات شخصی) و بسیاری موارد دیگر. برای بررسی چگونگی برخورد شرکت‌ها با چنین معضلاتی، نیاز به مولفه‌های ویژه‌ای وجود دارد. با این حال، ما تصمیم گرفتیم که چنین مولفه‌های خاصی را به این پژوهش اضافه نکنیم، چرا که یکی از هدف‌های اصلی این گزارش این است که برای شرکت‌های فناوری دیگر (که خدمات گسترده دیگری همچون پلتفرم‌های نشر آنلاین، موتورهای جستجو، خدمات ایمیلی، تجارت الکترونیک، شبکه‌های اجتماعی و غیره را ارائه می‌دهند)، نیز قابل استفاده باشد. علاوه بر این، با وجود اینکه نگرانی‌های فراوانی درباره راهکارهای الگوریتم‌های یادگیری ماشین جهت تعدیل محتوا به صورت خودکار و اصلاح و ایجاد تغییر وجود دارد، ما تصمیم گرفتیم که در این پژوهش روی چنین مسائلی تمرکز نداشته باشیم. شاید در گزارش‌های آینده این مسائل را لحاظ کنیم. برای کسب اطلاعات بیشتر درباره مولفه‌های مربوط به تبلیغات هدفمند و سیستم‌های الگوریتمی، به مطالعه راهنمای RDR سال ۲۰۲۰ مراجعه کنید و مولفه‌های جدیدی را که مبنای شاخص RDR برای ارزیابی مسئولیت پذیری سازمانی در سال ۲۰۲۱ خواهند بود، ببینید.[۷۲]

72 "RDR pilot study underscores the need for rights-based standards in targeted advertising and algorithmic systems," Ranking Digital Rights, March 16, 2020, https://bit.ly/34671aZ

مولفه‌ها

ما در این پژوهش، از شاخص RDR سال ۲۰۱۹ استفاده کردیم. برخی از مولفه‌ها قابل اجرا بر روی سرویس‌های پیام‌رسان نبودند (F۹, F۱۰). زیرمولفه‌های F۶٫۳, F۷٫۳, F۳٫۴ و F۳٫۵ قابل اجرا بر روی واتس‌اپ نیستند، چرا که به دلیل رمزگذاری سرتاسری، این شرکت به محتوای پیام‌ها دسترسی ندارد. زیرمولفه‌ی P۷٫۳ قابل اجرا بر روی تلگرام نیست چرا که تلگرام از تبلیغات هدفمند (targeted advertising) استفاده نمی‌کند. برای زیرمولفه‌های P۱٫۲ و F۱٫۲ تمام شرکت‌ها را بر اساس در دسترس بودن سیاست‌های حفظ حریم خصوصی و شرایط و ضوابط استفاده از خدمات به زبان فارسی، امتیازبندی کردیم.

دسترسی به شرایط و ضوابط استفاده از خدمات

شرکت‌ها باید سیاست‌های شرایط و ضوابط استفاده از خدمات خود را به زبانی قابل فهم نوشته و در دسترس عمومی قرار دهند.

F1.1 آیا شرایط و ضوابط استفاده از خدمات به راحتی قابل دسترس است؟

F1.2 آیا شرایط و ضوابط استفاده از خدمات به زبانی که اکثریت کاربران به آن زبان صحبت میکنند نوشته شده است؟

F1.3 آیا شرایط و ضوابط استفاده از خدمات به زبان ساده وقابل‌فهمی نوشته شده است؟

F2. تغییرات در شرایط و ضوابط استفاده از خدمات

F2.1 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران خود را از هرگونه تغییر در شرایط و ضوابط استفاده از خدمات خود مطلع می‌سازد؟

F2.2 آیا این شرکت به صورت علنی اعلام می‌کند که چگونه کاربران را مستقیما از هرگونه تغییری مطلع خواهد ساخت؟

F2.3 آیا این شرکت مدت زمان لازم برای اطلاع رسانی پیش از اعمال تغییرات را به صورت علنی اعلام می‌کند؟

F2.4 آیا این شرکت دارای یک بایگانی عمومی یا سیاهه تغییرات می‌باشد؟

F3. فرآیند مربوط به اجرای شرایط و ضوابط استفاده از خدمات

F3.1 آیا این شرکت به صورت علنی اعلام می‌کند که چه نوع محتواها یا فعالیت‌هایی را جایز نمی‌شمرد؟

F3.2 آیا این شرکت به صورت علنی اعلام می‌کند که به چه دلیل ممکن است حساب کاربری فردی را ببندد؟

F3.3 آیا این شرکت روند شناسایی محتوا و یا حساب‌های کاربری که قوانین شرکت را زیر پا گذاشته‌اند را به صورت علنی اعلام می‌کند؟

F3.4 آیا این شرکت به صورت علنی اعلام می‌کند که آیا مقام‌های دولتی امتیاز ویژه‌ای برای گزارش درخواست حذف یا محدود کردن محتوا (زمانی که تصور می شود آن محتوا قوانین شرکت را زیر پا گذاشته) دریافت می‌کنند؟

F3.5 آیا این شرکت به صورت علنی اعلام می‌کند که آیا برخی نهادهای خصوصی امتیاز ویژه‌ای برای گزارش درخواست حذف یا محدود کردن محتوا (زمانی که تصور می شود آن محتوا قوانین شرکت را زیر پا گذاشته) دریافت می‌کنند؟

F3.6 آیا این شرکت روند به اجرا گذاشتن قوانین خود را به صورت علنی اعلام می‌کند؟

F3.7 آیا این شرکت مثال‌های روشنی برای کاربران خود فراهم می‌کند تا کاربران بهتر متوجه قوانین و چگونگی اعمال آنها باشند؟

F4. داده‌های مربوط به اجرای شرایط و ضوابط استفاده از خدمات

F4.1 آیا این شرکت داده‌هایی را که نشان می‌دهند که چه مقدار از محتواها و حساب‌های کاربری با چه ماهیت‌هایی، به خاطر زیر پا گذاشتن قوانین بسته شده‌اند، به صورت علنی اعلام می‌کند؟

F4.2 آیا این شرکت این نوع داده‌ها را دست کم یک بار در سال منتشر می‌سازد؟

F4.3 آیا داده‌های منتشر شده توسط این شرکت قابلیت ذخیره شدن در قالب یک فایل داده‌ای ساختاری [مثل اکسل یا جیسون] را دارند؟

F5. روند واکنش به درخواست‌های طرفین ثالث برای توقیف صفحات کاربری و حذف محتوا
شرکت‌ها باید به صورت علنی شیوه‌ی خود را در واکنش به درخواست‌های نهادهای حکومتی (که شامل دستورات قضایی نیز می‌شود) و درخواست‌های خصوصی برای حذف، فیلتر و توقیف محتوا و صفحات کاربری، اعلام کنند.

F5.1 آیا این شرکت روند خود را برای واکنش به درخواست‌های غیر قضایی به صورت علنی اعلام می‌کند؟

F5.2 آیا این شرکت روند خود را برای واکنش به دستورات قضایی به صورت علنی اعلام می‌کند؟

F5.3 آیا این شرکت روند خود را برای واکنش به درخواست‌های دولت‌های خارجی به صورت علنی اعلام می‌کند؟

F5.4 آیا این شرکت روند خود را برای واکنش به درخواست‌های نهادهای خصوصی به صورت علنی اعلام می‌کند؟

F5.5 آیا در توضیحات این شرکت، زیرساخت قانونی‌ای که ممکن است تحت آن با درخواست های نهادهای حکومتی موافقت شود، به صورت علنی ذکر شده است؟

F5.6 آیا در توضیحات این شرکت، زیرساختی که ممکن است تحت آن با درخواست های نهادهای خصوصی موافقت شود، به صورت علنی ذکر شده است؟

F5.7 آیا این شرکت به صورت علنی اعلام می‌کند که پیش از اینکه تصمیم بگیرد چطور به درخواست‌های نهادهای حکومتی واکنش نشان دهد، بررسی‌های لازم را انجام می‌دهد یا نه؟

F5.8 آیا این شرکت به صورت علنی اعلام می‌کند که پیش از اینکه تصمیم بگیرد چطور به درخواست‌های نهادهای خصوصی واکنش نشان دهد، بررسی‌های لازم را انجام می‌دهد یا نه؟

F5.9 آیا این شرکت متعهد می‌شود که در مقابل درخواست‌های بی‌مورد و مبهم نهادهای حکومتی مقاومت کند؟

F5.10 آیا این شرکت متعهد می‌شود که در مقابل درخواست‌های بی‌مورد و مبهم نهادهای خصوصی مقاومت کند؟

F5.11 آیا این شرکت مثال‌های روشنی از چگونگی روند واکنش به درخواست‌های دولتی فراهم می‌کند؟

F5.12 آیا این شرکت مثال‌های روشنی از چگونگی روند واکنش به درخواست‌های نهادهای خصوصی فراهم می‌کند؟

F6. داده‌های مربوط به درخواست‌های نهادهای حکومتی برای توقیف محتوا و صفحات کاربری
شرکت‌ها می‌بایست مرتبا داده‌های مربوط به درخواست‌های نهادهای حکومتی را (که شامل دستورات قضایی نیز می‌شود) برای حذف، فیلتر کردن و توقیف محتوا و صفحات کاربری، منتشر کنند.

F6.1 آیا این شرکت تعداد درخواست‌های دریافتی را بر اساس کشور، مجزا و دسته‌بندی می‌کند؟
F6.2 آیا این شرکت تعداد حساب‌های کاربری‌ای که تحت تاثیر قرار گرفته‌اند را فهرست می‌کند؟
F6.3 آیا این شرکت تعداد محتواها و صفحه‌های وب های تحت تاثیر قرار گرفته را فهرست می‌کند؟
F6.4 آیا این شرکت نوع موضوعات مرتبط با درخواست‌های دریافتی را فهرست می‌کند؟
F6.5 آیا این شرکت تعداد درخواست‌هایی که از طرف مقامات مختلف قضایی دریافت می‌کند را فهرست می‌کند؟
F6.6 آیا این شرکت تعداد درخواست‌هایی که از طرف مقامات دولتی برای بستن حساب‌های کاربری یا حذف محتوا، به صورت‌های غیر رسمی دریافت می‌شود را فهرست می‌کند؟
F6.7 آیا این شرکت تعداد درخواست‌هایی را که با آنها موافقت کرده است، فهرست می‌کند؟
F6.8 آیا این شرکت نسخه اصلی درخواست‌ها را منتشر می‌سازد و یا کپی آنها را در اختیار یک بایگانی عمومی طرف ثالث قرار می‌دهد؟
F6.9 آیا این شرکت گزارش این داده‌ها را دست کم یک بار در سال منتشر می‌سازد؟
F6.10 آیا این داده‌ها قابلیت ذخیره شدن در قالب یک فایل داده‌ای ساختاری را دارند؟

F7. داده‌های مربوط به درخواست‌های نهادهای خصوصی برای توقیف محتوا و صفحات کاربری
شرکت‌ها می‌بایست مرتبا داده‌های مربوط به درخواست‌های خصوصی برای حذف، فیلتر کردن و توقیف محتوا و صفحات کاربری را منتشر کنند.

F7.1 آیا این شرکت تعداد درخواست‌های دریافتی را بر اساس کشور، مجزا و دسته‌بندی می‌کند؟
F7.2 آیا این شرکت تعداد حساب‌های کاربری‌ای که تحت تاثیر قرار گرفته‌اند را فهرست می‌کند؟
F7.3 آیا این شرکت تعداد محتواها و یا یوآرال های تحت تاثیر قرار گرفته را فهرست می‌کند؟
F7.4 آیا این شرکت دلایل حذف محتوا یا حساب‌های کاربری مربوط به درخواست‌های دریافتی را فهرست می‌کند؟
F7.5 آیا این شرکت توضیح می‌دهد که درخواست‌های دریافتی از طرف چه نوع نهادهایی می‌باشند؟
F7.6 آیا این شرکت تعداد درخواست‌هایی را که با آنها موافقت کرده است، فهرست می‌کند؟
F7.7 آیا این شرکت نسخه اصلی درخواست‌ها را منتشر می‌سازد و یا کپی آنها را در اختیار یک بایگانی عمومی طرف ثالث قرار می‌دهد؟
F7.8 آیا این شرکت گزارش این داده‌ها را دست کم یک بار در سال منتشر می‌سازد؟
F7.9 آیا این داده‌ها قابلیت ذخیره شدن در قالب یک فایل داده‌ای ساختاری را دارند؟
F7.10 آیا این شرکت به صورت علنی اعلام می‌کند که گزارشات منتشر شده، تمام انواع درخواست‌های نهادهای خصوصی را شامل میشود یا نه؟

F8. اطلاع رسانی به کاربران درباره توقیف حساب کاربری و محتوای صفحاتشان
شرکت‌ها باید اعلام کنند که آیا کاربران خود را از بسته شدن حساب کاربری و حذف محتوای صفحه‌شان مطلع می‌سازند یا نه.

F8.1 اگر یک شرکت محتوای تولید شده توسط کاربران را میزبانی می‌کند، آیا به صورت علنی اعلام می‌کند که کاربران خود را از منع محتوایشان مطلع می‌سازد یا خیر؟
F8.2 آیا این شرکت به صورت علنی اعلام می‌کند که اگر کاربری تلاش می‌کند تا به محتوای ممنوع شده‌ای دسترسی پیدا کند، او را از این موضوع مطلع می‌سازد یا نه؟
F8.3 آیا این شرکت در اطلاعیه خود، علت ممنوع شدن محتوا را (چه قانونی باشد چه نباشد) به صورت علنی ذکر می‌کند؟
F8.4 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران را از ممنوع شدن حسابشان مطلع می‌سازد یا نه؟

F11 سیاست‌های شناسایی هویت
شرکت‌ها نباید از کاربران بخواهد هویت خود را با شناسنامه صادر شده توسط دولت یا سایر اشکال شناسایی که می تواند به هویت آفلاین آنها متصل شود ، تأیید کنند.

F11.1 آیا این شرکت از کاربران می خواهد هویت خود را با شناسنامه صادر شده توسط دولت یا سایر اشکال شناسایی که می تواند به هویت آفلاین آنها متصل شود ، تأیید کنند؟

مولفه‌های مربوط به حریم خصوصی

P1. دسترسی به خط مشی‌های مربوط به حریم خصوصی: شرکتها می‌بایست خط مشی مربوط به حریم خصوصی خود را به شکلی ارائه کنند که به راحتی قابل پیدا کردن و به سادگی قابل فهم باشند.

P1.1 آیا خط مشی‌های مربوط به حریم خصوصی این شرکت به راحتی قابل پیدا کردن هستند؟

P1.2 آیا خط مشی‌های مربوط به حریم خصوصی به زبان‌هایی که کاربران این شرکت معمولا به آن سخن می‌گویند، در دسترس هستند؟

P1.3 آیا خط مشی‌ها به شیوه‌ای قابل فهم ارائه شده‌اند؟

P2. تغییرات در خط مشی‌های مربوط به حریم خصوصی: شرکت‌ها می‌بایست به صورت علنی اعلام کنند که در صورت ایجاد تغییر در خط مشی‌های مربوط به حریم خصوصی، کاربران را مطلع ساخته و مستندات را ارائه می‌کنند.

P2.1 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران خود را از هرگونه تغییری در خط مشی‌های مربوط به حریم خصوصی خود مطلع می‌سازد یا نه؟

P2.2 آیا این شرکت به صورت علنی اعلام می‌کند که چگونه کاربران خود را مستقیما از هرگونه تغییری مطلع می‌سازد؟

P2.3 آیا این شرکت به صورت علنی اعلام می‌کند که چه مدت قبل از اعمال تغییرات، اطلاع‌رسانی می‌کند؟

P2.4 آیا این شرکت دارای یک بایگانی عمومی یا سیاهه تغییرات می‌باشد؟

P3. جمع‌آوری اطلاعات کاربران

شرکت‌ها می‌بایست به شکلی علنی اعلام کنند که چه اطلاعاتی را و به چه شیوه‌ای جمع‌آوری می‌کنند.

P3.1 آیا این شرکت به صورت علنی اعلام می‌کند که چه نوع اطلاعاتی را از کاربران جمع‌آوری می‌کند؟

P3.2 آیا برای هر کدام از انواع اطلاعاتی که این شرکت از کاربران جمع‌آوری می‌کند، به صورت علنی اعلام می‌کند که چگونه این جمع‌آوری را انجام می‌دهد؟

P3.3 آیا این شرکت به صورت علنی اعلام می‌کند که جمع‌آوری اطلاعات کاربران را تنها محدود به مسائلی می‌کند که ضروری بوده و مستقیما به ارائه خدمات خود مربوط باشد؟

P4. به اشتراک‌گذاری اطلاعات کاربران

شرکت‌ها می‌بایست به شکلی علنی اعلام کنند که چه اطلاعاتی از کاربران با چه کسانی به اشتراک گذاشته می‌شود.

P4.1 آیا این شرکت به صورت علنی اعلام می‌کند که هر یک از انواع اطلاعات جمع‌آوری شده از کاربران را به اشتراک می‌گذارد یا نه؟

P4.2 آیا این شرکت به صورت علنی اعلام می‌کند که هر یک از انواع اطلاعات جمع‌آوری شده از کاربران را با چه کسانی (چه طرفین ثالثی) به اشتراک می‌گذارد؟

P4.3 آیا این شرکت به صورت علنی اعلام می‌کند که ممکن است اطلاعات کاربران را با مقامات دولتی یا قضایی به اشتراک بگذارد؟

P4.4 آیا این شرکت اسامی تمام نهادها یا طرفین ثالثی که هر یک از انواع اطلاعات جمع‌آوری شده از کاربران را با آنها به اشتراک می‌گذارد، به صورت علنی اعلام می‌کند؟

P5. هدف از جمع‌آوری و به اشتراک‌گذاری اطلاعات کاربران

شرکت‌ها می‌بایست به شکلی علنی اعلام کنند که به چه دلیل اطلاعات کاربران را جمع‌آوری کرده و به اشتراک می‌گذارند.

P5.1 آیا این شرکت به صورت علنی اعلام می‌کند که هر یک از انواع اطلاعات جمع‌آوری شده از کاربران به چه هدفی جمع‌آوری شده است؟

P5.2 آیا این شرکت به صورت علنی اعلام می‌کند که اطلاعات کاربران از سرویس‌های ارائه شده مختلف را، با هم تلفیق می‌کند یا نه، و در صورتی که این کار را انجام می‌دهد، آیا دلیل خود را اعلام می‌کند؟

P5.3 آیا این شرکت به صورت علنی اعلام می‌کند که هر یک از انواع اطلاعات به اشتراک گذاشته شده کاربران، با چه هدفی اشتراک‌گذاری شده‌اند؟

P5.4 آیا این شرکت به صورت علنی اعلام می‌کند که اطلاعات کاربران را فقط برای هدف اصلی‌ای که به آن دلیل آنها را جمع‌آوری کرده است، به کار میگیرد؟

P6. نگه‌داری اطلاعات کاربران

شرکت‌ها می‌بایست به شکلی علنی اعلام کنند که برای چه مدت اطلاعات کاربران را ذخیره می‌کنند.

P6.1 آیا این شرکت به صورت علنی اعلام می‌کند که برای چه مدتی هر یک از انواع اطلاعات جمع‌آوری شده کاربران را، نگه می‌دارد؟

P6.2 آیا این شرکت به صورت علنی اعلام می‌کند که چه اطلاعات هویت-روبی شده‌ای (de-identified) را از کاربران نگه می‌دارد؟

P6.3 آیا این شرکت روند هویت روبی کردن (de-identifying) اطلاعات کاربران خود را به صورت علنی اعلام میکند؟

P6.4 آیا این شرکت به صورت علنی اعلام می‌کند که بعد از اینکه کاربران حساب خود را می‌بندند، تمام اطلاعاتشان را پاک می‌کند یا نه؟

P6.5 آیا این شرکت به صورت علنی اعلام می‌کند که چه مدت بعد از اینکه کاربران حساب خود را می‌بندند، اطلاعاتشان را پاک می‌کند؟

P7. کنترل کاربران بر اطلاعات خود

شرکت‌ها می‌بایست به شکلی علنی به کاربران اعلام کنند که چه گزینه‌هایی برای جمع‌آوری، نگه‌داری و استفاده از اطلاعات کاربران وجود دارد.

P7.1 آیا این شرکت در مورد هر یک از انواع اطلاعاتی که از کاربران جمع‌آوری می‌کند، اعلام می‌کند که آیا کاربران می‌توانند بر اطلاعات جمع‌آوری شده از خودشان کنترلی داشته باشند؟
P7.2 آیا این شرکت در مورد هر یک از انواع اطلاعاتی که از کاربران جمع‌آوری می‌کند، اعلام می‌کند که آیا کاربران می‌توانند این اطلاعات را پاک کنند؟
P7.3 آیا این شرکت به صورت علنی اعلام می‌کند که برای کاربران خود شرایطی فراهم کرده است که این کاربران درباره بکار گرفته شدن اطلاعاتشان در تبلیغات هدفمند (targeted advertising) انتخاب داشته باشند؟
P7.4 آیا این شرکت به صورت علنی اعلام می‌کند که گزینه تبلیغات هدفمند (targeted advertising) به صورت پیش‌فرض خاموش می‌باشد؟

P8. دسترسی کاربران به اطلاعات خود
شرکت‌ها می‌بایست به کاربران خود اجازه دهند که تمامی اطلاعات کاربری خود را که در اختیار شرکت است، اخذ نمایند.
P8.1 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران می‌توانند نسخه‌ای از اطلاعات کاربری خود اخذ نمایند؟
P8.2 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران چه نوع اطلاعات کاربری را می‌توانند اخذ نمایند؟
P8.3 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران می‌توانند اطلاعات کاربری خود را تحت فرمت ساخت‌یافته‌ای structured data اخذ نمایند؟
P8.4 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران می‌توانند تمام اطلاعات کاربری خصوصی و عمومی خود را که یک شرکت از آنها نگه می‌دارد، اخذ کنند؟

P9. جمع‌آوری اطلاعات کاربران از طرفین ثالث
شرکت‌ها می‌بایست به شکلی علنی روش‌های خود را در ارتباط با جمع‌آوری داده‌های کاربران از اپلیکیشن‌ها یا وب‌سایت‌های طرفین ثالث به واسطه روش‌های فنی، اعلام کنند.
P9.1 آیا این شرکت به صورت علنی اعلام می‌کند که چه اطلاعاتی را از وب‌سایت‌های طرفین ثالث به واسطه روش‌های فنی، درباره کاربران خود جمع‌آوری می‌کند؟
P9.2 آیا این شرکت به صورت علنی توضیح می‌دهد که چطور اطلاعات کاربران را از وب‌سایت‌های طرفین ثالث به واسطه روش‌های فنی، جمع‌آوری می‌کند؟
P9.3 آیا این شرکت هدف خود را از جمع‌آوری داده‌های کاربران از وب‌سایت‌های طرفین ثالث به واسطه روش‌های فنی، به صورت علنی اعلام می‌کند؟
P9.4 آیا این شرکت به صورت علنی اعلام می‌کند که برای چه مدتی اطلاعات کاربران را که از وب‌سایت‌های طرفین ثالث به واسطه روش‌های فنی جمع‌آوری کرده است، نگه می‌دارد؟
P9.5 آیا این شرکت به صورت علنی اعلام می‌کند که به انتخاب کاربران برای انصراف از جمع‌آوری داده، احترام می‌گذارد یا نه؟

P10. روند واکنش به درخواست‌های طرفین ثالث برای دسترسی به اطلاعات کاربران
شرکت‌ها می‌بایست به صورت علنی روند پاسخگویی به درخواست‌های نهادهای حکومتی و طرفین ثالث برای دسترسی به اطلاعات کاربران را اعلام کنند.
P10.1 آیا این شرکت روند واکنش به درخواست‌های غیر قضایی را به صورت علنی اعلام می‌کند؟
P10.2 آیا این شرکت روند واکنش به دستورات دادگاهی را به صورت علنی اعلام می‌کند؟
P10.3 آیا این شرکت روند واکنش به درخواست‌های دولتهای خارجی را به صورت علنی اعلام می‌کند؟
P10.4 آیا این شرکت روند واکنش به درخواست‌هایی که از طرف نهادهای خصوصی دریافت می‌شود را به صورت علنی اعلام می‌کند؟
P10.5 آیا در توضیحات این شرکت، زیرساخت قانونی‌ای که ممکن است تحت آن با درخواست های دولتی موافقت شود، به صورت علنی ذکر شده است؟
P10.6 آیا در توضیحات این شرکت، زیرساخت قانونی‌ای که ممکن است تحت آن با درخواست های نهادهای خصوصی موافقت شود، به صورت علنی ذکر شده است؟
P10.7 آیا این شرکت به صورت علنی اعلام می‌کند که پیش از اینکه تصمیم بگیرد چطور به درخواست‌های نهادهای حکومتی واکنش نشان دهد، بررسی‌های لازم را انجام می‌دهد یا نه؟
P10.8 آیا این شرکت به صورت علنی اعلام می‌کند که پیش از اینکه تصمیم بگیرد چطور به درخواست‌های نهادهای خصوصی واکنش نشان دهد، بررسی‌های لازم را انجام می‌دهد یا نه؟
P10.9 آیا این شرکت متعهد می‌شود که در مقابل درخواست‌های بی‌مورد و مبهم نهادهای حکومتی مقاومت کند؟
P10.10 آیا این شرکت متعهد می‌شود که در مقابل درخواست‌های بی‌مورد و مبهم نهادهای خصوصی مقاومت کند؟
P10.11 آیا این شرکت مثال‌های روشنی از چگونگی روند واکنش به درخواست‌های نهادهای حکومتی فراهم می‌کند؟
P10.12 آیا این شرکت مثال‌های روشنی از چگونگی روند واکنش به درخواست‌های نهادهای خصوصی فراهم می‌کند؟

P11. داده‌های مربوط به درخواست‌های طرفین ثالث برای دسترسی به اطلاعات کاربران
شرکت‌ها باید به طور منظم داده‌های خود را در ارتباط با درخواست‌های نهادهای حکومتی و طرفین ثالث برای دسترسی به اطلاعات کاربران منتشر کنند.

P11.1 آیا این شرکت تعداد درخواست‌های دریافتی را بر اساس کشور، فهرست می‌کند؟
P11.2 آیا این شرکت تعداد درخواست‌های دریافتی برای اطلاعات کاربری ذخیره شده و همینطور برای دسترسی همزمان به ارتباطات را فهرست می‌کند؟
P11.3 آیا این شرکت تعداد حساب‌های کاربری‌ای که تحت تاثیر قرار گرفته‌اند را فهرست می‌کند؟
P11.4 آیا این شرکت در فهرست خود اعلام می‌کند که تقاضاهای دریافتی به دنبال محتوای ارتباطات هستند یا به دنبال داده‌های غیرمحتوایی و یا هردو؟
P11.5 آیا این شرکت، مقامات قضایی یا نوع روند قانونی‌ای را که درخواست‌های مربوط به امنیت ملی و نیروی انتظامی از طریق آنها انجام می‌شوند را تعیین می‌کند؟
P11.6 آیا این شرکت درخواست‌هایی که از طرف دادگاه دریافت می‌کند را (در فهرست خود) درج می‌کند؟
P11.7 آیا این شرکت تعداد درخواست‌های دریافتی از نهادهای خصوصی را فهرست می‌کند؟
P11.8 آیا این شرکت تعداد درخواست‌های پذیرفته شده را براساس نوع تقاضا دسته‌بندی می‌کند؟
P11.9 آیا این شرکت نوع درخواست‌های نهادهای حکومتی را که قانوناً مجاز نیست علنی کند، فهرست می‌کند؟
P11.10 آیا داده‌های گزارش شده توسط این شرکت قابلیت ذخیره شدن(اکسپورت) در قالب یک فایل داده‌ای ساختاری را دارند؟

P12. اطلاع رسانی به کاربران در مورد درخواست‌های طرفین ثالث برای دسترسی به اطلاعات
شرکت‌ها باید کاربران خود را تا جایی که در محدوده قانون می‌گنجد از اینکه اطلاعاتشان مورد درخواست نهادهای حکومتی و طرفین ثالث قرار گرفته، مطلع کنند.
P12.1 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران خود را از اینکه اطلاعاتشان مورد درخواست نهادهای حکومتی (از جمله دادگاه و دیگر ارگان‌های قضایی) قرار گرفته، مطلع می‌کند؟
P12.2 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران خود را از اینکه اطلاعاتشان مورد درخواست نهادهای خصوصی قرار گرفته، مطلع می‌کند؟
P12.3 اگر تحت شرایطی این شرکت کاربران خود را مطلع نسازد، آیا این شرکت این شرایط را به صورت علنی اعلام میکند و همینطور نوع درخواست‌های دولتی‌ای را که قانوناً مجاز نیست علنی کند، توضیح می‌دهد؟

P13. نظارت بر امنیت
شرکت‌ها می‌بایست به صورت علنی اعلام کنند که به چه روش‌هایی ، امنیت محصول و خدمات خود را حفظ می‌کنند.
P13.1 آیا این شرکت به صورت علنی اعلام می‌کند که برای محدود کردن و نظارت بر دسترسی کارکنان به اطلاعات کاربران، قواعدی را در نظر گرفته است؟
P13.2 آیا این شرکت به صورت علنی اعلام می‌کند که از یک تیم حفاظتی برای نظارت بر امنیت محصولات و خدمات خود برخوردار است؟
P13.3 آیا این شرکت به صورت علنی اعلام می‌کند که گروه‌های شخص ثالثی را برای نظارت بر امنیت محصولات و خدمات خود به کار می‌گیرد؟

P14. برطرف کردن «ضعف‌های امنیتی»
در صورت پیدا شدن «ضعف‌های امنیتی»، شرکت‌ها می‌بایست این ضعف‌ها را برطرف کنند.
P14.1 آیا این شرکت به صورت علنی اعلام می‌کند که از سازوکارهایی برخوردار است که محققان امنیتی از طریق آن بتوانند نقاط ضعفی را که پیدا می‌کنند، گزارش دهند؟
P14.2 آیا این شرکت بازه زمانی‌ای را که در آن به بررسی گزارشات درباره نقاط ضعف می‌پردازد، به صورت علنی اعلام می‌کند؟
P14.3 آیا این شرکت متعهد می‌شود که اقدامات حقوقی علیه محققانی که نقاط ضعف و کاستی‌های این شرکت را در چارچوب سازوکارهای این شرکت گزارش می‌دهند، اتخاذ نکند؟

P15. نشت‌های اطلاعاتی
شرکت‌ها می‌بایست رویه‌ی خود را در واکنش به نشت‌های اطلاعاتی به صورت علنی اعلام کنند.
P15.1 آیا این شرکت به صورت علنی اعلام می‌کند که در صورت پیش آمدن یک نشت داده‌ای، مقامات مربوطه را بدون فوت وقت مطلع می‌سازد؟
P15.2 آیا این شرکت روند خود را برای اطلاع‌رسانی به افرادی که ممکن است تحت تاثیر یک نشت داده‌ای قرار گرفته باشند، به صورت علنی اعلام می‌کند؟
P15.3 آیا این شرکت به صورت علنی اعلام می‌کند که برای رسیدگی به تاثیراتی که یک نشت داده‌ای بر کاربرانش خواهد داشت، چه نوع اقداماتی را به کار می‌گیرد؟

P16. رمزنگاری محتوای خصوصی و ارتباطات کاربران
شرکت‌ها می‌بایست محتوای خصوصی و ارتباطات کاربران را رمزنگاری کنند تا افراد بتوانند در مورد اینکه چه کسی به این اطلاعات دسترسی داشته باشد، کنترل داشته باشند.
P16.1 آیا این شرکت به صورت علنی اعلام می‌کند که انتقال ارتباطات (داده‌های) کاربران به صورت پیش‌فرض رمزنگاری شده است؟

P16.2 آیا این شرکت به صورت علنی اعلام می‌کند که انتقال ارتباطات (داده‌های) کاربران با استفاده از کلیدهای منحصر به فرد، رمزنگاری شده است؟

P16.3 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران می‌توانند محتواهای خصوصی خود را با استفاده از رمزنگاری سرتاسری و یا روش full-disk encryption (در صورت امکان) محفوظ بدارند؟

P16.4 آیا این شرکت به صورت علنی اعلام می‌کند که رمزنگاری سرتاسری و یا full-disk encryption به صورت پیش‌فرض تعبیه شده‌اند؟

P17. امنیت حساب کاربری

(شرکت‌های اینترنتی، تولیدکننده نرم‌افزار و دستگاه‌های کامپیوتری) شرکت‌ها می‌بایست به کاربران خود در ایمن نگه داشتن حساب‌های کاربریشان کمک کنند.

P17.1 آیا این شرکت به صورت علنی اعلام می‌کند که برای جلوگیری از دسترسی متقلبانه، روش‌های پیشرفته برای تصدیق حساب کاربری را بکار می‌گیرد؟

P17.2 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران می‌توانند فعالیت‌های اخیر حساب کاربری خود را مشاهده کنند؟

P17.3 آیا این شرکت به صورت علنی اعلام می‌کند که کاربران را درباره فعالیت‌های غیرمعمول و احتمال دسترسی بدون اجازه به حساب‌های کاربریشان، مطلع می‌سازد؟

P18. آگاهی‌رسانی و آموزش به کاربران درباره احتمال ریسک‌های موجود: شرکت‌های می‌بایست اطلاعاتی را منتشر کنند که به کاربران کمک می‌کند تا در برابر خطرات سایبری از خود محافظت کنند.

P18.1 آیا این شرکت مطالبی کاربردی در ارتباط با محصول یا خدمات خود برای آموزش به کاربران منتشر می‌کند تا افراد بدانند که چطور در برابر خطرات سایبری از خود محافظت کنند؟

مولفه‌های مربوط به سیاست‌گذاری شرکت

G1. تعهد به قوانین

شرکت‌ها می‌بایست به حقوق کاربران خود در رابطه با آزادی بیان و حریم خصوصی احترام گذشته و به صورت علنی این تعهد را اظهار کنند.

G1.1 آیا این شرکت به شکلی صریح و با بیانی شفاف در سیاست‌گذاری‌های خود، به حقوق بشر از جمله حق آزادی بیان و حق حریم خصوصی، متعهد می‌شود؟

G2. سیاست‌گذاری شرکت و سازوکارهای نظارت

مدیران ارشد شرکت‌ها می‌بایست بر تاثیرات شیوه‌ها و سیاست‌گذاری‌های شرکت خود بر آزادی بیان و حریم خصوصی، نظارت داشته باشند.

G2.1 آیا این شرکت به صورت علنی این مسئله را اعلام می‌کند که هیئت مدیره به صورت رسمی بر اینکه فعالیت‌های این شرکت چه تاثیری بر آزادی بیان و حریم خصوصی دارد، نظارت می‌کند؟

G2.2 آیا این شرکت به صورت علنی این مسئله را اعلام می‌کند که یک گروه، برنامه، مامور و یا هیئت در سطح اجرایی، بر اینکه فعالیت‌های این شرکت چه تاثیری بر آزادی بیان و حریم خصوصی دارد، نظارت دارند؟

G2.3 آیا این شرکت به صورت علنی این مسئله را اعلام می‌کند که یک گروه، برنامه، مامور و یا هیئت در سطح مدیریتی، بر اینکه فعالیت‌های این شرکت چه تاثیری بر آزادی بیان و حریم خصوصی دارد، نظارت دارند؟

G3. اجرای درون سازمانی

شرکت‌ها می‌بایست سازوکارهایی داشته باشند تا تعهدات خود به آزادی بیان و حریم خصوصی را، به شکل درون سازمانی به اجرا بگذارند.

G3.1 آیا این شرکت به صورت علنی اعلام می‌کند که برای کارکنان خود دوره‌های آموزشی درباره مسائل مربوط به آزادی بیان و حریم خصوصی فراهم می‌کند؟

G3.2 آیا این شرکت به صورت علنی اعلام می‌کند که سازوکاری برای افشاگری ایجاد کرده تا کارکنان از طریق آن بتوانند نگرانی‌های موجود در ارتباط با نوع برخورد شرکت با حق آزادی بیان و حریم خصوصی کاربرانش را گزارش دهند؟

G4. سنجش اثرات

شرکت‌ها می‌بایست عملکرد خود را به صورت مرتب، جامع و معتبر ارزیابی کنند، برای مثال می‌بایست تاثیرات حقوق بشری خود را ارزیابی کرده تا بدانند چطور تمام بخش‌های کاری آنها بر آزادی بیان و حریم خصوصی تاثیر می‌گذارد، و در صورت وجود مواردی که این حقوق را نقض می‌کنند، بتوانند به کاهش و رفع این مشکلات بپردازند.

G4.1 آیا این شرکت به عنوان بخشی از روند تصمیم‌گیری‌های خود این موضوع را درنظر می‌گیرد که قوانینی که در حوزه اختیاراتش هستند، چگونه بر آزادی بیان و حریم خصوصی تاثیر می‌گذارند؟

G4.2 آیا این شرکت مرتباً ریسک‌های موجود در رابطه با آزادی بیان و حریم خصوصی را در محصولات و خدمات خود می‌سنجد؟

G4.3 آیا این شرکت ریسک‌های مرتبط با آزادی بیان و حریم خصوصی موجود در یک فعالیت جدید از جمله عرضه و یا خرید محصولات، خدمات و شرکت‌های جدید یا ورود به بازارهای جدید را، می‌سنجد؟

G4.4 آیا این شرکت ریسک‌های مرتبط با آزادی بیان و حریم خصوصی موجود در روندها و سازوکارهای بکار گرفته در اعمال شرایط و ضوابط استفاده از خدمات را، می‌سنجد؟

G4.5 آیا این شرکت ریسک‌های مرتبط با آزادی بیان و حریم خصوصی را که ممکن است در سیستم‌های تصمیم گیری خودکار از جمله الگوریتم‌ها و یا هوش مصنوعی وجود داشته باشند، می‌سنجد؟

G4.6 آیا این شرکت ریسک‌های مرتبط با آزادی بیان و حریم خصوصی را که ممکن است در شیوه‌ها و سیاست‌گذاری‌های مربوط به تبلیغات هدفمند (targeted advertising) وجود داشته باشند، می‌سنجد؟

G4.7 آیا این شرکت هر زمانی که در برآوردهای احتمال خطر، متوجه نکات نگران‌کننده‌ای شود، ارزیابی‌های مضاعفی را بکار می‌بندد؟

G4.8 آیا مدیران اجرایی ارشد و یا اعضای هیئت مدیره این شرکت، نتایج ارزیابی‌ها را بررسی کرده و اقدامات لازم را در تصمیم‌گیری‌های خود به کار می‌بندند؟

G4.9 آیا این شرکت مرتباً عملکرد خود را ارزیابی می‌کند؟

G4.10 آیا صحت ارزیابی‌های این شرکت از عملکردش، توسط شخص (یا گروه) ثالثی بیرون از شرکت، تضمین می‌گردد؟

G4.11 آیا این شخص ثالث که صحت ارزیابی‌ها را تضمین می‌کند، خود توسط یک سازمان معتبر با استانداردهای حقوق بشری قابل اطمینان، اعتباربخشی شده است؟

G5. همکاری با نهادهای ذینفع

شرکت‌ها می‌بایست با نهادهای مختلفی در زمینه آزادی بیان و حریم خصوصی همکاری کنند.

G5.1 آیا این شرکت در یک طرح چند-ذینفعی که متعهد به تقویت آزادی بیان و حریم خصوصی بر اساس اصول بین‌المللی حقوق بشر باشد، مشارکت می‌کند؟

G5.2 اگر این شرکت در یک طرح چند-ذینفعی مشارکت نمی‌کند، آیا عضو سازمانی می‌باشد که با ذینفعان غیر دولتی و غیرصنعتی به طور منظم و اصولی درباره آزادی بیان و حریم خصوصی تعامل داشته باشد؟

G5.3 اگر این شرکت عضو یکی از این سازمان‌ها نمی‌باشد، آیا راه‌اندازی یا شرکت در جلسات با نمایندگان، حامیان و یا خود افراد ذینفعی که حق آزادی بیان و حریم خصوصی‌اشان به صورت مستقیم متاثر از فعالیت‌های تجاری این شرکت است، را به صورت علنی اعلام می‌کند؟

G6. جبران خسارات

شرکت‌ها می‌بایست دارای سازوکارهایی برای ارائه جبران خسارات و بررسی شکایات در زمینه معضلات مربوط به حریم خصوصی و آزادی بیان باشند.

G6.1 آیا این شرکت به صورت علنی اعلام می‌کند که سازوکاری برای شکایات ایجاد کرده تا کاربران در صورتی که احساس کنند که حق آزادی بیان و حریم خصوصیشان توسط فعالیت‌ها و سیاست‌گذاری‌های این شرکت به صورت منفی تحت تاثیر قرار گرفته است، از طریق آن بتوانند شکایات خود را گزارش کنند؟

G6.2 آیا این شرکت رویه خود را برای رسیدگی به شکایات مرتبط با حریم خصوصی و آزادی بیان و جبران نارضایتی‌ها، به صورت علنی اعلام می‌کند؟

G6.3 آیا این شرکت زمان مورد نیاز برای رسیدگی به شکایات و جبران نارضایتی‌ها را به صورت علنی اعلام می‌کند؟

G6.4 آیا این شرکت تعداد شکایات دریافتی مرتبط با حریم خصوصی و آزادی بیان را به صورت علنی اعلام می‌کند؟

آیا این شرکت به صورت علنی شواهدی مبنی بر جبران کردن نارضایتی‌های مرتبط با حریم خصوصی و آزادی بیان، ارائه می‌کند؟

تطابق حرف با عمل

شاخص RDR، شرکت‌ها را بر اساس شیوه‌ها و سیاست‌گذاری‌های علنی آنها که بر موضوعات حریم خصوصی و آزادی بیان تاثیر می‌گذارند، رتبه‌بندی می‌کند. بنابراین، ما در این گزارش محصولات را از نظر فنی تست نکردیم. در نتیجه نمی‌دانیم آنچه شرکت‌ها در سیاست‌های علنی خود می‌گویند، تا چه میزان با عملکرد فنی محصولاتشان مطابقت دارد. برای تست

محصولات می‌توانید از منابع زیر استفاده کنید:

- راهنمای The Open Web Application Security Project یا OWASP، روشی برای مهندسی معکوس اپلیکیشن‌های موبایل و تست آنها بر مبنای استانداردهای حریم خصوصی و امنیت:

- راهنمای OWASP، روشی برای تست قدرت رمزنگاری:
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption

- «استاندارد دیجیتال»، راهنمایی برای پیاده‌سازی استانداردهای حریم خصوصی و امنیت سایبری، کاری از گروه‌های The Cyber Independent Testing Lab. و Ranking Digital Rights و Consumer Reports
https://www.thedigitalstandard.org/the-standard

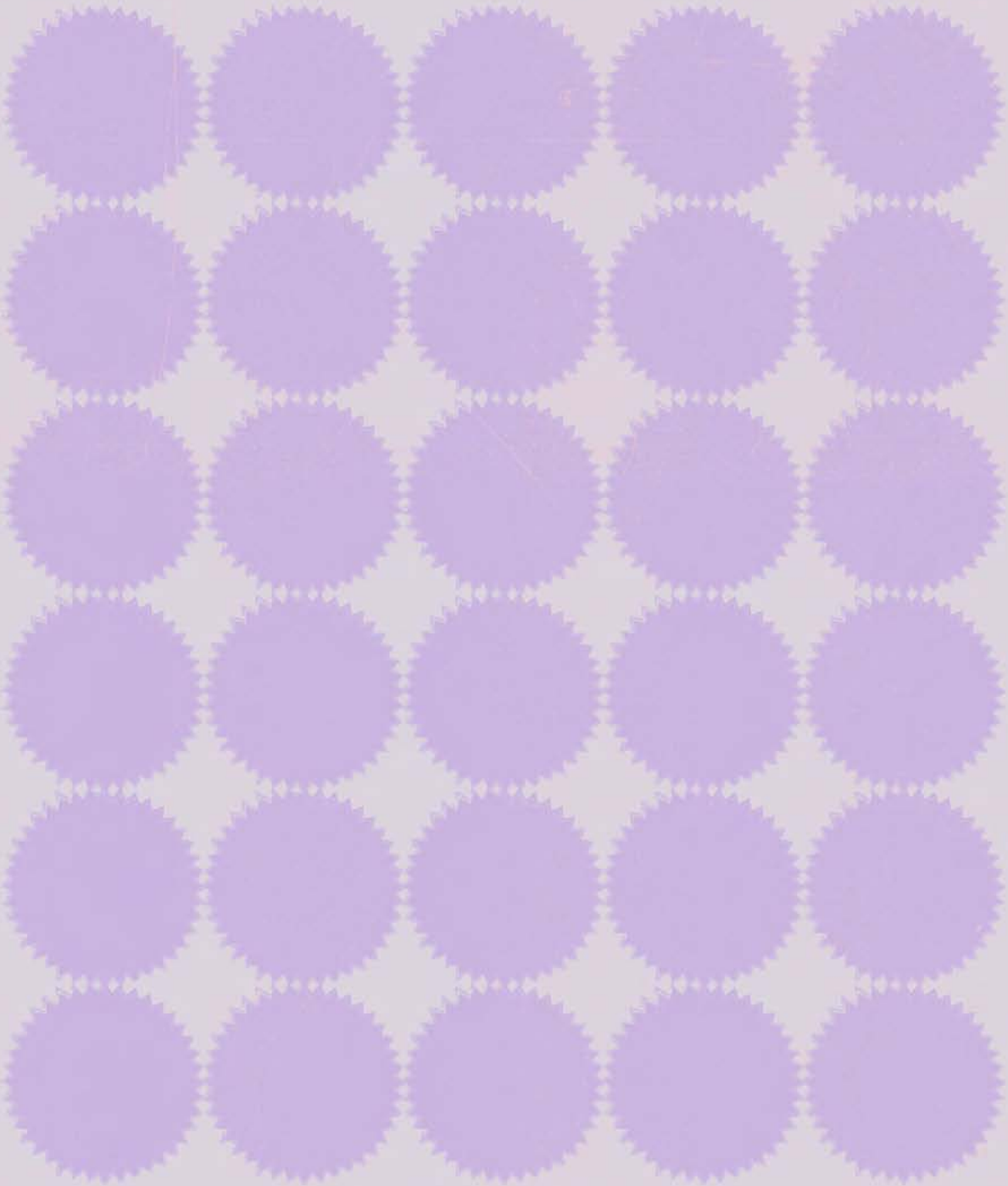
- The Mozilla Observatory، ابزاری برای تست امنیت وبسایت‌ها:
https://observatory.mozilla.org/

- چک‌لیستی برای امنیت دیجیتال و حفاظت از حریم خصوصی در طراحی UI/UX :
https://static1.squarespace.com/static/5e28cfb6752be803fc51f907/t/5eaa5b9f4f2f3e5a01d381ba/1588222879354/Secure+UX+Checklist.pdf

دفترچه‌ی راهنمای رعایت حقوق دیجیتال کاربران

(تهیه شده برای شرکت‌های فناوری نوپا)

طراحی شده توسط فیلتربان و تراز



دفترچه‌ی راهنمای رعایت حقوق دیجیتال کاربران

(تهیه شده برای شرکت‌های فناوری نوپا)

راهنمایی برای اعمال شاخص رتبه‌بندی Ranking Digital Rights برای هدایت شرکت‌های فناوری ایرانی به سمت شفافیت بیشتر و به‌کارگیری شیوه‌های بهتر برای احترام به حقوق دیجیتال کاربران

این دفترچه راهنما برای چه کسانی تهیه شده است؟

این دفترچه راهنما به این منظور طراحی شده تا به شرکت‌ها در روند خودآزمایی آنها کمک کند. مخاطب این دفترچه به ویژه شرکت‌های فناوری نوپا در ایران می‌باشد که می‌خواهند ارزش‌های حقوق دیجیتال را از همان قدم‌های اول در تمامی فعالیت‌های مربوط به طراحی و توسعه‌ی محصولشان اجرا کنند.

چطور می‌توانید از این دفترچه‌ی راهنما استفاده کنید؟

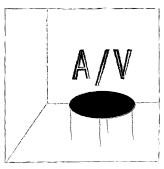
ما پیشنهاد می‌کنیم که ورکشاپ‌های یک روزه یا دو روزه‌ای ترتیب دهید تا زیرمولفه‌های مختلف این دفترچه راهنما را با دقت مرور کنید.

مقدمات ورکشاپ

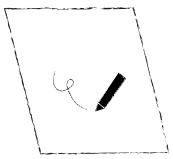
یکی از اعضای تیم مدیریتی/اجرایی باید برای ترتیب دادن یک ورکشاپ پیش‌قدم شود. این شخص، پیش از هر چیز، باید این گزارش و دیگر منابع از جمله اصول راهنمای تجارت و حقوق بشر سازمان ملل را مطالعه کند، سپس این منابع را بین اعضای تیم پخش کند. فرد متصدی باید اعضای بخش‌هایی که در زیر فهرست شده‌اند را برای شرکت در این ورکشاپ دعوت کند:

- **عضو(های) بخش مدیریتی و اجرایی**
- **عضو(های) بخش مهندسی و تکنولوژی**
  (مانند برنامه‌نویسان، مدیران سیستم، و از این دست)
- **عضو(های) بخش طراحی و پژوهش UX/UI**
- **عضو(های) بخش حقوقی و سیاست‌گذاری**
- **عضو(های) بخش روابط عمومی و ارتباطات**

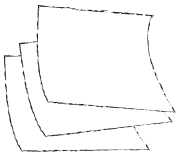
وسایل مورد نیاز:



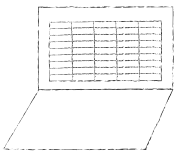
- **یک اتاق کنفرانس مجهز به سیستم صوتی-تصویری**



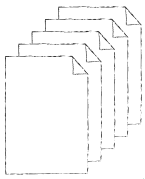
- **وایت‌بورد**



- **کاغذ یادداشت**



- **یک لپتاپ برای کار کردن بر روی دفترچه راهنما**
  (از اینجا دانلود کنید)



- **نسخه‌های فتوکپی از شرایط و ضوابط استفاده از خدمات و سیاست‌های حریم خصوصی شرکتتان (در صورت موجود)**

فعالیت‌های ورکشاپ

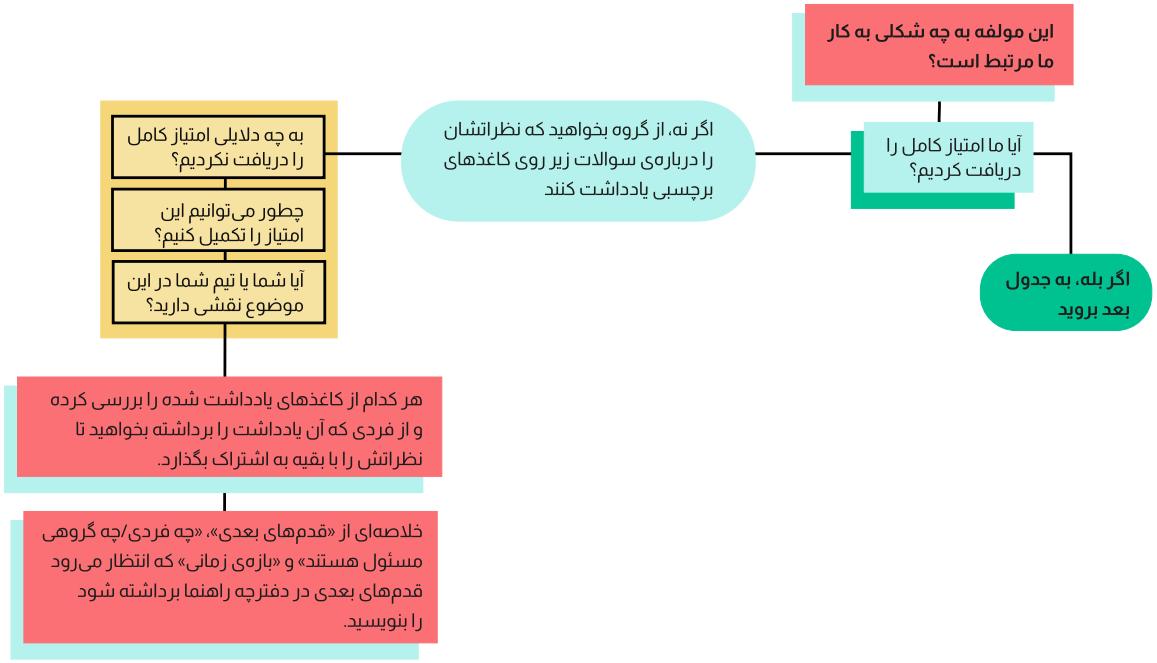
فرد متصدی، ورکشاپ را با ارائه یک پرزنتیشن کوتاه درباره اصول راهنمای تجارت و حقوق بشر سازمان ملل و شاخص رتبه‌بندی مسئولیت شرکت‌ها در قبال حقوق دیجیتال (RDR) آغاز خواهد کرد. پس از آن به اهداف و دلایل برگزاری ورکشاپ می‌پردازد. شخص برگزار کننده همچنین می‌بایست فعالیت‌های ورکشاپ را توضیح داده و یک نفر را برای یادداشت‌برداری و یک داوطلب را برای جمع‌آوری یادداشت‌ها و کمک در بهتر برگزار شدن گفتگو، برگزینند.

جدول‌های مولفه‌ها

به دفترچه راهنمای اکسل مراجعه کنید و فایل‌های اکسل حریم خصوصی، آزادی بیان و سیست‌گذاری‌های شرکت را دانلود کنید.

گفتگوی گروهی

فرد برگزارکننده، هر یک از مولفه‌ها (در دفترچه راهنما) را می‌خواند و گروه، گفتگو را با پاسخ دادن به این سوالات آغاز می‌کند:



واژه‌نامه اصطلاحات

حقوق دیجیتال
حقوق بشر در عصر دیجیتال، اشاره دارد به بهره‌مندی از حقوق بنیادین بشر، از جمله حقوقی که در اعلامیه جهانی حقوق بشر به رسمیت شناخته می‌شوند، و تعمیم دادن آنها به فناوری‌های دیجیتال و اینترنت.

ICCPR
میثاق بین‌المللی حقوق مدنی و سیاسی

ICESCR
میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی

حق حریم خصوصی
ماده ۱۲ اعلامیه جهانی حقوق بشر حق حریم خصوصی را اینطور تشریح می‌کند: «هیچ احدی نمی‌بایست در قلمرو خصوصی، خانواده، محل زندگی یا مکاتبات شخصی، تحت مداخله [و مزاحمت] خودسرانه قرار گیرد. به همین سیاق شرافت و آبروی هیچ‌کس نباید مورد تعرض قرار گیرد. هر کسی سزاوار و محق به حفاظت قضایی و قانونی در برابر چنین مداخلات و تهاجماتی است.»

حق آزادی عقیده و بیان
ماده ۱۹ اعلامیه جهانی حقوق بشر حق آزادی عقیده و بیان را اینطور تشریح می‌کند: «هر انسانی محق به آزادی عقیده و بیان است؛ و این حق شامل آزادی داشتن باور و عقیده‌ای بدون [نگرانی] از مداخله [و مزاحمت]، و حق جستجو، دریافت و انتشار اطلاعات و افکار از طریق هر رسانه‌ای بدون ملاحظات مرزی است.»

RDR
رتبه‌بندی حقوق دیجیتال

UN
سازمان ملل متحد

UNGP
اصول راهنمای تجارت و حقوق بشر سازمان ملل

UDHR
اعلامیه جهانی حقوق بشر

ICT
فناوری اطلاعات و ارتباطات

Bug Bounty
باگ باونتی- برنامه‌ای که معمولاً از سوی وب‌سایت‌ها و برنامه‌نویسان تهیه می‌شود و افراد در ازای پیدا کردن و گزارش باگ‌های نرم‌افزارها، پاداش دریافت می‌کنند.

Encryption
رمزگذاری- هر روندی که در رمزنویسی استفاده می‌شود تا یک نوشته‌ی ساده را به نوشته‌ی رمزی تبدیل کند، به گونه‌ای که تنها افراد مجاز قادر به خواندن آن باشند.

End-to-End Encryption (E2EE)
رمزگذاری سرتاسر- یک سیستم برقراری ارتباط که در آن فرستنده اولیه یک پیام را به یک پیام رمزی تبدیل کرده و این نوشته‌ی رمزی تنها به دست گیرنده‌ی نهایی قابل رمزگشایی است.

API
رابط برنامه‌نویسی کاربردی

Bot
بات- یک نرم‌افزار کاربردی است که وظایف خودکاری را از طریق اینترنت انجام می‌دهد.

2FA
احراز هویت دو عاملی

IRIB
سازمان صدا و سیمای جمهوری اسلامی ایران

CDICC
کارگروه تعیین مصادیق محتوای مجرمانه

MSI یا Multi-Stakeholder Initiatives

طرح‌های چندذینفعی- همکاری‌های داوطلبانه بین شرکت‌ها، سازمان‌های جامعه مدنی، موسسات دانشگاهی، سرمایه‌گذاران، دولت‌ها و دیگر ذینفعان برای ایجاد یک Global Network Initiative. حاکمیت دسته جمعی نمونه از این طرح‌ها است.

نکات مربوط به ترجمه‌ی متن فارسی

کلمه‌ی government در **متن انگلیسی این گزارش** به معنای نهادهای مسئول یک کشور در امور قانونگذاری، سیاست‌گذاری، کنترل، اجرا و اعمال قوانین و سیاست‌های آن کشور به کار برده شده است. در ترجمه‌ی فارسی، بسته به فحوای متن، این کلمه به عباراتی نظیر نهادهای مسئول، سیاست‌گذاران، مسئولین، نهادهای دولتی، دولت و نهادهای حکومتی ترجمه شده است.

Government

noun.

I. The governing body of a nation, state, or community.

1.1 The system by which a nation, state, or community is governed.

1.2 The action or manner of controlling or regulating a nation, organization, or people.

1.3 The group of people in office at a particular time; administration.

(from Oxford English dictionary)

در ترجمه‌ی فارسی، به صلاحدید محققان گزارش، برای توضیح روان‌تر و دقیق‌تر متن، عباراتی اضافه شده است که در متن انگلیسی موجود نیست؛ هر چند که مفهوم و پیام جملات در هر دو زبان یکسان است.

حقوق دیجیتال و مسئولیت شرکت‌های فناوری در ایران

بررسی سرویس‌های پیام‌رسان اینترنتی

TARAAZ

TECHNOLOGY & HUMAN RIGHTS