فن‌بیز

بدون مترجم سفر کن

برای «فن‌بیز» این هفته تصمیم گرفتیم اپلیکیشن خارجی معرفی کنیم که قرار است در سفرهای خارجی همراه شما باشد. با استفاده از این اپلیکیشن می‌توانید با مردم سراسر دنیا ارتباط برقرار کنید بدون اینکه حتی زبان آنها را بلد باشید. اپلیکیشن say hi translate، محصول آمازون، یک اپلیکیشن مترجم صوتی و متنی همراه است که زبان فارسی را هم پشتیبانی می‌کند و استفاده از آن هزینه‌ای ندارد. Sayhi امکان ترجمه جملات و کلمات به بیش از صد زبان مختلف را برای کاربران فراهم کرده است.

وقتی اپلیکیشن را نصب کردید، در ابتدا باید به میکروفون اجازه دسترسی دهید. در صفحه اصلی دو میکروفون آبی و سبز می‌بینید. میکروفون آبی برای زبان مبدأ است. با انتخاب فلش زیر میکروفون، فهرست بلندبالایی را می‌بینید و از بین آنها می‌توانید زبان فارسی را برگزینید. وقتی زبان را انتخاب کنید، می‌توانید سرعت گفت‌وگو را که سریع یا کند باشد و صدای مترجم را که مرد باشد یا زن به انتخاب خود تغییر دهید. در این بخش همچنین می‌توانید انتخاب کنید آیا می‌خواهید صحبت یا تایپ کنید. پیشنهاد من این است که در محیط شلوغ، به‌جای صحبت‌کردن تایپ کنید؛ چون این اپلیکیشن حرف‌های اطراف را هم همراه با صحبت‌های شما ترجمه می‌کند و باعث سردرگمی شما می‌شود.

میکروفون سبزرنگ مخصوص کشور مقصد است. وقتی فلش زیر میکروفون را انتخاب کنید وارد فهرست زبان‌ها می‌شوید و می‌توانید هرکدام از آنها را انتخاب کنید. برای برقراری ارتباط باید میکروفون را فشار دهید و جمله خود را به فارسی بگویید. سپس اپلیکیشن جمله شما را به زبان مقصد ترجمه می‌کند. شما همچنین با انتخاب سطل آشغال می‌توانید تمام مکالمات خود را حذف کنید. این اپلیکیشن رابط کاربری بسیار ساده و دقت و سرعت بالایی در ترجمه جملات دارد.

این اپلیکیشن هم نسخه اندروید و هم نسخه iOS دارد. برای دریافت اپلیکیشن برای آیفون می‌توانید از iApps یا سایت اصلی Sayhi اقدام کنید. برای دریافت نسخه اندروید هم به کافه‌بازار، گوگل‌استور و مایکت مراجعه کنید. اپلیکیشن Sayhi در بازار نمره ۴.۵ از پنج را دریافت کرده و بیش از صد هزار بار دانلود شده است. این اپلیکیشن همچنین در گوگل‌استور نمره ۴.۶ از پنج را دارد و بیش از پنج میلیون بار دانلود شده است.

آپارات

تقابل هوش مصنوعی با خالقش

در سال ۲۰۱۴، الکس گارلند در اولین فیلم خود به نام «Ex Machina»، ربات انسان‌نمایی به نام «آوا» را خلق کرد. دو سال بعد در دنیای واقعی یک ربات انسان‌نما به نام سوفیا (Sophia) توسط هنسون روبوتیکس خلق شد؛ ربات انسان‌نمایی که حالت چهره خود را تغییر می‌دهد و از طریق هوش مصنوعی ارتباط برقرار می‌کند؛ رباتی دقیقا شبیه آوا. الکس گارلند با فیلم خود نشان داد که چند سال از زمان خود جلوتر است و امکان دارد پیش‌بینی‌های او حتی به واقعیت تبدیل شود.

Ex Machina یا فراماشین در ژانر علمی-تخیلی و تریلر روان‌شناختی محصول سال ۲۰۱۴، داستان یک برنامه‌نویس جوان به نام کیلب است که در بزرگ‌ترین شرکت اینترنتی جهان به نام بلوبوک، مشغول به فعالیت است. او پس از پیروزی در یک مسابقه اداری، به مدت یک هفته امکان حضور در اقامتگاهی را به دست می‌آورد که به مدیرعامل کمپانی بلوبوک تعلق دارد. کیلب پس از ورود به مکان مورد نظر، متوجه می‌شود که باید با اولین هوش مصنوعی جهان به نام آوا، ارتباطی مؤثر برقرار کند.

این فیلم روی روابط پیچیده بین کیلب و آوا تمرکز کرده است. می‌توان فیلم را کمی شبیه به فیلم «Her» دانست؛ با این تفاوت که در «فراماشینی» ما با یک ربات فیزیکی طرف هستیم. تمام فیلم در فضایی بسته اتفاق می‌افتد، اما این موضوع باعث نمی‌شود که حوصله مخاطب سر برود؛ چون فیلم سراسر تعلیق و هیجان است. فیلم فراماشینی به دو موضوع به‌خوبی پرداخته است و باعث شده اثر ارزشمندی شود: اول تقابل هوش مصنوعی و خالقش، موضوعی که در حال حاضر با وجود دیپ‌فیک و چت‌جی‌بی‌تی نگرانی‌هایی را برای بشر ایجاد کرده است و این سؤال ایجاد می‌شود که بشر تا چه اندازه می‌خواهد در طراحی هوش مصنوعی پیش رود و دوم روبه‌روشدن احساسات واقعی بشر با احساسات غیرواقعی هوش مصنوعی و نشان می‌دهد این تقابل چه عواقب ترسناکی خواهد داشت.

الکس گارلند پیش‌تر نویسندگی فیلم‌هایی همچون «۲۸ روز بعد» و «هرگز نگذار برم» را بر عهده داشت و با فیلم فراماشینی به عنوان نخستین بار کارگردانی را تجربه کرد و در اولین تجربه‌اش نیز این فیلم در گیشه بیش از ۳۶.۸ میلیون دلار در سراسر جهان به فروش رسید. منتقدان نیز این فیلم را به دلیل جلوه‌های بصری، فیلم‌نامه و اجرای بازیگران تحسین کردند. فراماشینی همچنین در هشتادوهشتمین دوره جوایز اسکار، برنده بهترین جلوه‌های بصری و گارلند نامزد بهترین فیلم‌نامه اصلی شد.

خبر

موبایل‌سازان چینی به اندروید پشت می‌کنند

مهر: تولیدکنندگان موبایل چینی ازجمله شیائومی، اوپو، ویوو و وان‌پلاس مشغول بررسی توسعه نسخه‌هایی از سیستم‌عامل اندروید هستند که به «سرویس‌های موبایل گوگل» (GMS) متکی نیست.

به گزارش فون‌آرنا، طبق گزارش‌هایی جدید تخمین زده می‌شود این اقدام احتمالی به دلیل تنش‌های تجاری بین چین و آمریکا و نگرانی‌ها درباره محدودیت‌های آتی، مشابه آنچه بر هوآوی تحمیل شد، انجام شود.

تحریم‌های تجاری دولت دونالد ترامپ اجازه نمی‌دهد شرکت‌های آمریکایی ازجمله گوگل نرم‌افزار و قطعات برای هوآوی تأمین کنند. همین امر سبب شد دستگاه‌های هوآوی دسترسی به گوگل‌پلی و اپلیکیشن‌های اصلی این شرکت مانند مَپس و جی‌میل را از دست بدهند و در نتیجه سهم آنها از بازار جهانی تحت تأثیر قرار گیرد. همچنین روند مذکور به توسعه پلتفرم هارمونی او اس توسط هوآوی منجر شد. طبق شایعات، برندهای ذکرشده ممکن است در این پروژه با یکدیگر همکاری کنند و احتمالا خود هوآوی نیز تا حدی در این زمینه دخیل باشد. هرچند جزئیات دقیق همکاری مشخص نیست اما سیستم‌عامل آتی شیائومی به نام HyperOS ۳ به عنوان زمینه احتمالی برای ایجاد یک سیستم مستقل از گوگل ذکر شده است. در حال حاضر مشخص نیست آیا شرکت‌ها سازگاری با اپ‌های اندروید فعلی را در برنامه خود دارند یا آنکه مانند جدیدترین سیستم عامل هوآوی (Harmony OS NEXT) پشتیبانی از اپلیکیشن‌های اندروید را به‌طور کامل حذف می‌کنند.

بررسی نقش فناوری در سیستم ارسال پیامک حجاب

چگونه ابزارهای دیجیتال در ایران به جای راحتی، محدودیت به ارمغان می‌آورند؟

سونیتا سراب‌پور

تصور کنید در حال قدم‌زدن در خیابان هستید و ناگهان پیامکی روی گوشی‌تان ظاهر می‌شود که شما را بابت نداشتن «پوشش قانونی» تهدید می‌کند. این اتفاق در روزهای اخیر برای زنان ایرانی بارها تکرار شده است. ارسال این پیامک‌ها از اصفهان شروع شد و بعد به تهران رسید و حالا هم زنان در شیراز و رشت از دریافت این پیامک‌ها خبر می‌دهند و احتمالا این چرخه به دیگر استان‌ها نیز خواهد رسید. این پیامک‌ها فقط برای زنانی که ادعا می‌شود «پوشش قانونی» ندارند، ارسال نمی‌شود و در برخی نمونه‌ها مردان یک خانواده نیز پیامک هشداری دریافت می‌کنند که «بانوان منصوب به شما بدون رعایت پوشش قانونی در سطح شهر حضور داشته‌اند». پشت پرده این پیام‌ها چیست و چگونه افراد را شناسایی و اطلاعات خصوصی آنها را در اختیار نهادهای مختلف می‌گذارد؟ برعکس برخی گزارش‌ها و خبرهایی که ادعا می‌کند حکومت در حال استفاده از فناوری‌های پیچیده و کمک‌گرفتن از دوربین‌های فوق باکیفیت و هوش مصنوعی است، کارشناسان فناوری اطلاعات و امنیت در گفت‌وگو با «فن‌زی» می‌گویند همه‌چیز آن‌طور که نشان داده می‌شود، علمی و تخیلی نیست. به گفته آنها با کمک چند ابزار ساده مانند استفاده از تصاویر دوربین‌های مداربسته، ردیابی سیگنال‌های سیم‌کارت یا شناسایی IMEI گوشی و نقض قانون مدیریت داده و اطلاعات ملی، به دیتای خصوصی کاربران دسترسی پیدا می‌کنند و پازل ارسال پیامک حجاب به زنان تکمیل می‌شود. گزارش پیش‌رو تلاش دارد با تمرکز بر جنبه‌های فناورانه، سازوکار احتمالی این نوع رصد و هشدار را بررسی کند و اینکه آیا از نظر حقوقی دسترسی به داده‌های شخصی افراد برای تذکر حجاب قانونی است؟ در این گزارش با چهار کارشناس فناوری اطلاعات و امنیت صحبت کردیم که بنا بر خواسته آنها، نام‌هایشان محفوظ مانده است.

دورزدن قانون و دولت برای دریافت اطلاعات

تجربه زنان مختلف نشان می‌دهد که پیامک‌های حجاب طی مراحل مشخص برای زنان در شهرهای مختلف ایران ارسال می‌شود. برای اخطار اول پیامک را «ستاد امر به معروف و نهی از منکر» ارسال می‌کند و در قدم بعد در صورت تکرار، اخطار دوم از سوی «معاونت اجتماعی و پیشگیری از وقوع جرم دادگستری استان» ارسال می‌شود. باز هم در صورت تکرار، «فرماندهی انتظامی استان» وارد ماجرا شده و با پیامک تندتری اعلام می‌کند: «با توجه به تذکرات قبلی درخصوص پوشش قانونی، عمل ارتکابی مصداق جریحه‌دارکردن عفت عمومی است و مستندات جرم ارتکابی به‌منظور اجرای قانون به مراجع قضائی ارسال می‌شود». با توجه به ارسال این پیامک‌ها از سمت اپراتورهای ایرانسل و همراه اول، برخی افراد در شبکه اجتماعی ایکس (توییتر سابق) این سؤال را از وزارت ارتباطات پرسیدند که آیا اپراتورها شماره افراد را در اختیار این نهادها گذاشته‌اند یا این اطلاعات از طریق سامانه فنی وزارت ارتباطات در اختیار نهادهای نظارتی قرار گرفته است؟ به دنبال تکرار این سؤال روابط‌عمومی وزارت ارتباطات در شبکه ایکس اعلام کرد که «رعایت حریم خصوصی و دفاع از حقوق شهروندی، همواره خط قرمز شخص وزیر ارتباطات و مجموعه وزارتخانه بوده، هست و خواهد بود. شما بهتر می‌دانید ارسال این دست پیامک‌ها (مثل پیامک جرایم رانندگی) متولیان خود را دارد». در همین زمینه هم سخنگوی دولت در حاشیه جلسه هیئت دولت از ارسال این پیامک‌ها اظهار بی‌اطلاعی کرد. اما آیا واقعا دولت در این چرخه نقش یا دخالتی ندارد؟ بخشی از داده‌های شخصی افراد در تمامی سامانه‌های دولتی ذخیره شده است، در این بین چطور دولت اعلام می‌کند از این اتفاق بی‌خبر است یا در آن نقشی ندارد؟

یکی از سناریوهایی که در مورد دسترسی به اطلاعات شخصی افراد از طریق نهادهایی مانند ستاد امر به معروف و نهی از منکر مطرح می‌شود، این است که این نهاد با مطرح‌کردن درخواست دسترسی به داده در کارگروه تعامل‌پذیری ذیل شورای اجرائی فناوری اطلاعات، به آنها دسترسی پیدا کرده است. در واقع نیمی از ۱۵ عضو کارگروه تعامل‌پذیری که شامل نمایندگان دولت از وزارت اطلاعات، ارتباطات، کشور و... تا نمایندگان قوه قضائیه و مجریه و سایر دستگاه‌ها ازجمله بانک مرکزی و نیروی انتظامی می‌شوند، باید به درخواست مطرح‌شده برای دسترسی به اطلاعات رأی مثبت داده باشند، در غیر این صورت دسترسی صورت نخواهد گرفت. طبق قانون هم دسترسی به داده‌های بین دستگاهی فقط باید از طریق «مرکز تبادل اطلاعات» که از زیرساخت‌های توسعه دولت الکترونیک است، اتفاق بیفتد. همچنین طبق قانون مدیریت داده و اطلاعات ملی (دوام) دسترسی به داده‌های بین دستگاهی، خارج از این مرکز غیرقانونی است.

یک کارشناس فعال در طرح توسعه دولت الکترونیک در گفت‌وگو با «فن‌زی» اعلام می‌کند که وزارت ارتباطات مسئول مرکز تبادل اطلاعات است و این مرکز طبق برنامه پنج‌ساله ششم توسعه کشور، با هدف تسهیل در تبادل و به‌اشتراک‌گذاری اطلاعات، استعلام‌ها و خدمات بین نهادها ایجاد شده است. این مرکز شامل دو بستر به نام GSB (گذرگاه خدمات دولت) و PGSB (گذرگاه خدمات عمومی دولت) است. از طریق این گذرگاه‌ها، ارتباطات میان نهادهای مختلف دولتی به منظور ارائه خدمات متنوع به شهروندان و ایجاد شفافیت در فرایندهای اداری تسهیل می‌شود. دستگاه‌های متقاضی استفاده از داده‌های این مرکز مختلف است و شامل قوه مجریه، مقننه و قضائیه می‌شود. آن‌طور که این کارشناس اعلام می‌کند، هدف از تشکیل این مرکز این بوده که داده‌ها چند جا ذخیره نشوند، یک مرکز برای نظارت روی کل داده‌ها وجود داشته باشد و در نهایت پروتکل امنیتی رعایت شود. او درباره جزئیات دسترسی به اطلاعات کاربران و ارسال پیامک حجاب می‌گوید: «برای دسترسی یک دستگاه به داده‌های خاص کاربران، باید کارگروه تعامل‌پذیری تصمیم‌گیری کند که هم نماینده دولتی در آن حضور دارد و هم غیردولتی. برای مثال اگر در کارگروه رأی به این داده شود که دوربین‌های نیروی انتظامی و شهرداری به ثبت احوال متصل شوند تا افراد مورد نظر آنها شناسایی شوند، دولت (وزارت ارتباطات) با وجود مخالفت باید این دسترسی را فراهم کند». اما این کارشناس با توجه به نحوه کار کارگروه تعامل‌پذیری تأکید می‌کند که این کارگروه تاکنون رأی به دسترسی داده کاربران خارج از قوانین و مقررات مشخص‌شده در بخش داده‌های ملی نداده است؛ چراکه اعضای آن از دولت تا غیردولتی، هیچ‌وقت نمی‌خواهند خود را در مقابل خواست مردم قرار دهند. همچنین به گفته او از طرف دیگر، تمام فعالیت‌ها و تصمیمات این کارگروه طبق قانون، در «روزنامه رسمی» منتشر می‌شود و تاکنون هیچ خبری در زمینه مجوز دسترسی به داده‌ها برای ارسال «پیامک حجاب» توسط کارگروه تعامل‌پذیری ثبت نشده است. به اعتقاد این کارشناس نهادهایی که تذکر حجاب می‌دهند با دورزدن قانون مدیریت داده، دولت، کارگروه تعامل‌پذیری و به روش سنتی این اقدام را انجام می‌دهند. او در توضیح این روش سنتی می‌گوید: «راه سنتی یعنی اینکه دستگاه‌های مربوطه بدون گرفتن مجوز برای دریافت اطلاعات از مسیر مرکز تبادل اطلاعات، به شکل مستقیم به هم متصل می‌شوند؛ یعنی ثبت احوال یک نسخه کپی از دیتای شهروندان را در اختیار دارد و اجازه اتصال دوربین‌های نیروی انتظامی و شهرداری به این داده‌ها را می‌دهد. برای پیداکردن فرد بی‌حجاب هم کافی است تصویر و داده‌ها را با یکدیگر مطابقت دهند تا فرد مورد نظر را شناسایی و برایش پیامک حجاب ارسال کنند». او تأکید می‌کند که در جریان ارسال پیامک حجاب نهادهای درگیر بدون دریافت مجوز، خلاف قانون مدیریت داده و به شکل ارتباط مستقیم با هم، داده‌های مورد نیاز خود را پیدا می‌کنند.

فناوری‌های مورد استفاده در شناسایی «زنان پیاده» چیست؟

۱- دوربین‌های پیشرفته

بازگویی شرایط و محیطی که زنان پیاده در آن پیامک حجاب دریافت کرده‌اند، برخی کارشناسان فناوری را به این ایده رسانده که ارسال پیامک به زنان در حال پیاده‌روی بدون تکیه بر فناوری‌های نظارت تصویری پیشرفته امکان‌پذیر نیست. بر پایه شواهد و اظهارات غیررسمی، به نظر می‌رسد چند فناوری کلیدی در این روند نقش دارند:

بسیاری از دوربین‌های مداربسته شهری در سال‌های اخیر به سیستم‌های تشخیص چهره (Face Recognition) مجهز شده‌اند. این فناوری با تحلیل ویژگی‌های چهره افراد از طریق الگوریتم‌های یادگیری ماشین، قادر است هویت آنها را در صورت تطابق با بانک‌های اطلاعاتی هویتی شناسایی کند. این دوربین‌ها معمولا در میادین پرتردد، ورودی متروها و مراکز خرید نصب شده‌اند.

همچنین در کنار تشخیص چهره، فناوری بینایی ماشین (Computer Vision) نیز می‌تواند نوع پوشش افراد را تحلیل کند. به گفته برخی کارشناسان، این الگوریتم‌ها توانایی شناسایی الگوهای پوشش، میزان پوشیدگی یا نحوه قرارگیری روسری را دارند. در صورت مغایرت با استانداردهای اعلام‌شده توسط نهادهای رسمی، این تخلف به‌صورت سیستمی ثبت می‌شود. اما چقدر این سناریو با شرایط حاضر و وضعیت توسعه فناوری در کشور تطابق دارد؟ یک کارشناس امنیتی در گفت‌وگو با «فن‌زی» شناسایی حجاب توسط دوربین‌هایی با فناوری پیشرفته را رد می‌کند و تأکید دارد که شناسایی از طریق این دوربین‌ها بسیار با خطا مواجه است. او در این زمینه می‌گوید: «برخی اعلام می‌کنند که تصاویر زنان با کمک دوربین‌های مشخصی شناسایی شده است. این اتفاق در صورتی باورپذیر است که در کشور یک بانک اطلاعاتی تصویری باکیفیت از افراد وجود داشته باشد. در حال حاضر تنها بانک اطلاعات تصویری کامل در کشور مربوط به تصاویر کارت ملی است که از روبه‌رو و با حجاب گرفته شده و در بیشتر مواقع این عکس شبیه به تصویر واقعی افراد نیست؛ چراکه فرد ممکن است در حالت عادی آرایش داشته باشد، عینک روی صورتش باشد، عمل زیبایی انجام داده باشد یا پوشش خاصی هم داشته باشد». او ادامه می‌دهد: «در حال حاضر خیلی از سیستم‌های تصویری حضور و غیاب در ادارات و شرکت‌ها هم با اینکه دارای داده‌ها و عکس‌های مشخص و به‌روز هستند و در یک محیط بسته اقدام به شناسایی افراد می‌کنند، به‌درستی کار نمی‌کنند و ممکن است یک فرد چندبار مقابل دوربین آن قرار بگیرد تا شناسایی شود. از طرف دیگر اگر برای ورود به گوشی از رمز شناسایی تصویر استفاده کنید، پس از بارها بازشدن رمز به واسطه تصویر شما پیام خطا می‌دهد و باید حالت صورت خود را چند بار تغییر دهید تا قفل باز شود. در این شرایط به نظر نمی‌رسد دوربین‌هایی در سطح کشور نصب شده باشد که با فناوری‌ها ویژه و هوش مصنوعی توانایی شناسایی افراد با کیفیت بالا را داشته باشد».

در حالی این کارشناس تشخیص افراد با کمک دوربین‌های نظارتی را رد می‌کند که برخی کاربران در بیان تجاربشان در این زمینه، اعلام می‌کنند که شرکت‌هایی وجود دارند که برای شناسایی افراد مشکوک یا نیروهایی که در آن شرکت کار نمی‌کنند، کدهای مشخصی در نظر گرفته‌اند و به راحتی می‌توانند افراد را شناسایی کنند. یک کارشناس امنیتی با تأیید وجود داشتن چنین سیستمی اعلام می‌کند: «داشتن دوربین با فناوری متوسط که اقدام به شناسایی افراد می‌کند، چندان عجیب و غریب نیست، اما باید به این نکته توجه کنید که شناسایی صورت با مچ یا تطبیق صورت متفاوت است. همین حالا هم سرویس گوگل‌فتوز این قابلیت را دارد که شما به او یک تصویر بدهید و مشابه آن تصویر را برایتان پیدا کند یا در گالری گوشی می‌توانید تصویر شخصی را مشخص کنید و از آن بخواهید تمام عکس‌هایی را که آن فرد که در آن وجود دارد، برایتان پیدا کند». او ادامه می‌دهد: «بنابراین کاملا طبیعی است که دوربین‌های مداربسته بانک‌ها، مترو، پاساژها و... این قابلیت اولیه را داشته باشند که شما به آن کد تصویری بدهید و آن را برای شما پیدا کند، مثلا بگویید هر تاکسی زردی که از اینجا رد شد به من نشان بده. در این روش پیداکردن تصویر، بررسی در محیط محدود یا بسته اتفاق می‌افتد و چیزی را با چیز دیگر تطبیق نمی‌دهد، صرفا حدس می‌زند که با درصد خطایی هم همراه است و در نهایت به کمک یک اپراتور انسانی نتیجه را نهایی می‌کند». او در مورد اینکه پس در این شرایط شناسایی زنان باحجاب و بدون حجاب هم در یک منطقه امکان‌پذیر است، توضیح می‌دهد: «در یک منطقه یا محیط عمومی مثل خیابان، پاساژ و مترو، هم مردان در رفت و آمد هستند و هم زنانی با حجاب مختلف حضور دارند. یک زن با چادر است، یکی دیگر با مقنعه و شال، یکی عینک زده یا ماسک به صورت دارد، در این بین افرادی هم هستند که شال روی شانه‌شان است و حتی برخی زنان حجابی دارند که نه می‌توانی بگویی بی‌حجاب هستند نه حجاب دارند. در این شرایط شناسایی یک فرد که به گفته آنها حجاب قانونی نداشته، بدون کمک نیروی انسانی سخت است». او تأکید می‌کند که ایده پردازش تصویر با کمک هوش مصنوعی و شناسایی فرد ممکن است، اما برای پیاده‌سازی آن نیاز به منابع مالی بالا و دسترسی به تکنولوژی مشخص دارد. به گفته او همچنین در کنار در اختیار داشتن فناوری، نیاز به یک دیتاسنتر با ظرفیت بالا برای ذخیره‌سازی تصاویر باکیفیت هست. آن‌طور که او توضیح می‌دهد، با توجه به نیازمندی‌های این سیستم شناسایی و وضعیت اقتصادی و سیاسی ایران، به نظر نمی‌رسد نهادهای مذکور برای شناسایی زنان از این روش استفاده کرده باشند.

۲- کمک از داده‌های تلفن همراه

کارشناسان، شناسایی افراد از طریق تصویر صرف دوربین‌های مداربسته را رد می‌کنند، اما تأکید دارند که استفاده از تصویر دوربین‌های مداربسته در کنار عوامل دیگر می‌تواند به شناسایی فرد مورد نظر بینجامد. کارشناس امنیتی دیگری در این مورد به «فن‌زی» می‌گوید: «یکی از این راه‌ها، استفاده از موقعیت سیم‌کارت فرد در شبکه است. یک مکان‌یابی در شبکه به نام مکان‌یابی مثلثی داریم که می‌تواند محدوده مکان افراد را شناسایی کند. تأکید می‌کنم که در این روش، مکان‌یابی جای دقیق فرد امکان‌پذیر نیست». او ادامه می‌دهد: «دقت مکان‌یابی مثلثی در فاصله ۱۰۰ تا ۱۵۰ متر اتفاق می‌افتد، بنابراین شناسایی یک فرد با کمک سیم‌کارت در یک محیط شلوغ به‌راحتی امکان‌پذیر نیست». او تأکید می‌کند که برای شناسایی فرد از طریق سیم‌کارت باید محدوده را کوچک و کوچک‌تر کرد تا خطا در شناسایی کاهش پیدا کند. براساس برخی گزارش‌ها، یکی دیگر از راه‌هایی که با کمک تلفن همراه منجر به شناسایی زنان در سطح شهر می‌شود، گیرنده‌های شناسه بین‌المللی مشترک تلفن‌همراه (IMSI-Catcher) است. این دستگاه‌ها با جعل هویت دکل‌های مخابراتی (BTS) کار می‌کنند و باعث می‌شوند که تلفن‌های همراه در محدوده تحت پوشش، به دلیل قدرت سیگنال بیشتر، به این دکل جعلی متصل شوند. در نهایت در لحظه اتصال، دستگاه IMSI (شناسه بین‌المللی مشترک تلفن همراه) منحصربه‌فرد سیم‌کارت را درخواست و ضبط می‌کند. همچنین گفته می‌شود برای شناسایی افراد، ممکن است گروهی با کمک دستگاهی کد IMEI (شناسه بین‌المللی تجهیزات سیار) را در یک محیط جمع‌آوری کنند. این روش از آسیب‌پذیری امنیتی در شبکه GSM سوءاستفاده می‌کند که در آن شبکه ملزم به احراز هویت خود برای تلفن همراه نیست. ادعا می‌شود دستگاه‌های پیشرفته‌تر ممکن است تلفن‌ها را مجبور به کاهش سطح شبکه از 3G، 4G و 5G به 2G کنند تا شناسایی برایشان راحت‌تر شود.

یک کارشناس امنیتی در مورد این راه‌های شناسایی به «فن‌زی» می‌گوید: «اگر شناسایی افراد از طریق IMEI گوشی اتفاق افتاده باشد به این نتیجه می‌رسیم که اطلاعات از طریق وزارت ارتباطات یا صمت در اختیار نهاد ناظر قرار گرفته است؛ چراکه دیتابیس در زمینه ریجستر گوشی تنها در اختیار این دو وزارتخانه قرار دارد. اما در اینجا باید به چند نکته توجه کرد، ازجمله اینکه سیگنال‌های دستگاه Catcher مانند شبکه موبایل به تمام جهات ارسال می‌شود و مانند یک فیلم جاسوسی یا تخیلی نیست که یک فرد را پیدا و برای شناسایی آن به طرفش سیگنال بفرستد و اطلاعاتش را به دست بیاورد». او ادعای برخی گزارش‌ها در این زمینه را که ماشینی در حال حرکت این دستگاه را روشن و باعث می‌شود شبکه از 3G، 4G و 5G به 2G تغییر کند تا کد IMEI گوشی فرد مورد نظر به دست بی‌آید را بی‌مورد می‌داند. او در ادامه اعلام می‌کند که برای صحت‌سنجی این راه‌ها، چند راهکار وجود دارد: «ابتدا باید مشخص شود که زنی که موبایل یا سیم‌کارت به نامش نبوده، مورد حجابش از طریق پیامک به صاحب گوشی و سیم‌کارت گزارش شده یا خیر؟ اگر اطلاعات برای صاحب گوشی و سیم‌کارت رفته باشد، مشخص می‌شود که اطلاعات شخصی فرد از شبکه ریجستری موبایل می‌آید، نه پردازش تصویر در بین داده‌های ثبت احوال. اگر پیامک هم برای زن ارسال شده باشد و هم پدر یا دیگر اعضای خانواده، یعنی این اطلاعات علاوه بر دیتابیس شبکه موبایل، از طریق پردازش تصویر در داده‌های تصویری افراد در سازمان ثبت احوال گرفته شده است؛ چون اطلاعات شجرنامه فقط در ثبت احوال وجود دارد».

چطور افراد چندبار شناسایی می‌شوند؟

تجارب زنان در دریافت پیامک حجاب متفاوت است. برخی در پاساژ پیامک حجاب گرفته‌اند و برای امتحان یک بار دیگر با گوشی خاموش به پاساژ بازگشته‌اند و دوباره پیامک تذکر حجاب دریافت کرده‌اند. بازگویی این تجارب پیش‌بینی برای این را که از چه فناوری برای شناسایی زنان استفاده می‌کنند، سخت می‌کند. یک کارشناس امنیتی در این زمینه به «فن‌زی» اعلام می‌کند که همه چیز در این فرایند برخلاف ظاهرش، نباید خیلی پیچیده و با کمک ابزارهای تکنولوژیکی پیشرفته و تخیلی اتفاق افتاده باشد. این کارشناس امنیتی تأکید می‌کند که با توجه به تجارب مختلف در کشور، روند شناسایی زنان در حال پیاده‌روی از تلفیق چند راه ساده اتفاق افتاده است؛ ترکیبی از نیروی انسانی و بیگ‌دیتا. او با اشاره به اینکه محتمل‌ترین سناریو در شناسایی زنان پیاده در خیابان یا پاساژ چه می‌تواند باشد، می‌گوید: «ابتدا منطقه‌ای که یک زن در آن حضور داشته را براساس عکس ثبت‌شده از طریق دوربین‌های مداربسته مشخص می‌کنند، سپس از طریق داده‌های شبکه تلفن همراه مانند ردیابی سیم‌کارت یا IMEI اطلاعات، نام و اطلاعات افرادی را که در آن منطقه بوده‌اند، فهرست می‌کنند. در نهایت یک اپراتور انسانی اطلاعات را با عکس تطابق می‌دهد و فرد مورد نظر را پیدا می‌کند و گزارش ارسال پیامک حجاب ارسال می‌شود». او در پاسخ به اینکه چگونه یک زن با گوشی روشن در یک پاساژ شناسایی می‌شود و در روز دیگر با گوشی خاموش به پاساژ می‌رود و باز شناسایی می‌شود، می‌گوید: «این اتفاق به‌سادگی رخ می‌دهد. اگر یک بار زنی در پاساژ یا محیط دیگر شناسایی و برای او پیام تذکر حجاب رفته باشد، بار دوم این فرایند به‌سادگی و سرعت بیشتری پیش می‌رود. دلیل آن هم این است که تصویر و اطلاعات از این زن و زنان دیگر در یک دیتابیس جدید جمع‌آوری می‌شود تا شناسایی در مراحل بعدی به‌راحتی اتفاق بیفتد». همچنین او تأکید می‌کند در این موارد شناسایی نباید از گزارش‌های افراد در یک خیابان یا فروشندگان پاساژ به شماره‌های نظارتی که در این زمینه در نظر گرفته شده چشم‌پوشی کرد.

حریم خصوصی، خطا و پیامدهای اجتماعی

افزایش استفاده از فناوری‌های نظارتی برای کنترل پوشش زنان، آن‌هم در فضاهای عمومی و بدون شفافیت قانونی، موجی از نگرانی‌ها را در میان شهروندان و فعالان حقوق دیجیتال به وجود آورده است. حالا در کنار چگونگی استفاده از فناوری برای شناسایی زنان در سطح شهر، سؤال‌های حقوقی هم در مورد این شیوه کنترلی مطرح است؛ ازجمله اینکه آیا ستاد امر به معروف اجازه قانونی برای دسترسی به اطلاعات شخصی افراد را دارد؟ چه کسی اجازه دسترسی نهادهایی مانند امر به معروف را برای ارسال پیام تذکر به زنان داده است؟ آیا شناسایی زنان از طریق دوربین‌های مداربسته در فضای عمومی و تطبیق آن با اطلاعات شخصی‌شان قانونی است؟ حسین تاج، وکیل دادگستری، در گفت‌وگو با «فن‌زی» با اشاره به قانون‌های کشور می‌گوید: «ابتدا در پاسخ به سؤالات شما به‌طور مشخص باید بگویم که مبنا و معیار سنجش اقدامات ستاد امر به معروف و نهی از منکر، قانون حمایت از آمران به معروف و ناهیان از منکر مصوب ۱۳۹۴/۰۱/۱۲ و دستورالعمل اجرائی آن مصوب ۱۳۹۴/۰۲/۰۹ است. براساس این قانون، هرآنچه در دایره اختیار و عمل این ستاد پیش‌بینی شده مبنای قانونی دارد و خارج از این دایره از حمایت قانون برخوردار نیست. همچنین ماده ۴ از قانون مذکور به تعریف و تبیین امر به معروف و نهی از منکر و مراتب آن پرداخته است». به گفته او براساس ماده ۴، مراتب امر به معروف و نهی از منکر، قلبی، زبانی، نوشتاری و عملی است که مراتب زبانی و نوشتاری آن وظیفه آحاد مردم و دولت است و مرتبه عملی آن در موارد و حدودی که قوانین مقرر کرده فقط وظیفه دولت است.

او با اشاره به این موارد قانونی توضیح می‌دهد: «با عنایت به صراحت قانونی، وظیفه ستاد در «مرتبه عملی»، به انعکاس گزارش به مرجع قضائی محدود است. اما در قانون و دستورالعمل مربوطه سازوکار «مرتبه عملی» مشخص نشده است. بنابراین باید با تفسیر مضیق، حقوق بنیادین شهروندان که در قانون اساسی و قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی و قانون انتشار و دسترسی آزاد به اطلاعات پیش‌بینی شده است، رعایت شود». او ادامه می‌دهد: «با رجوع به قوانین و دستورالعمل‌های مرتبط مشخص است که دسترسی مستقیم و مستقل ستاد امر به معروف و نهی از منکر به اطلاعات شخصی و هویتی افراد امری غیرقانونی است، مگر درصورت اعطای این حق از طرف مقام‌های مسئول قضائی کشور. در این فرض، اعطای چنین حقی مستلزم اطلاع‌رسانی و آگاهی عمومی است که اطلاعاتشان بین نهادهای مختلف حکومتی دست‌به‌دست می‌شود». او تأکید می‌کند بی‌تردید عدم پاسخ‌گویی و عدم شفافیت این ستاد دراین‌باره به موج بی‌اعتمادی نسبت دولت و دستگاه قضا می‌افزاید.

یکی از مدیران حقوقی سابق وزارت ارتباطات هم در گفت‌وگو با «فن‌زی» اعلام می‌کند که اقدامات ستاد امر به معروف و نهی از منکر در ارسال پیامک تذکر حجاب خلاف قانون مدیریت داده و اطلاعات ملی است. همچنین به گفته او این رویه خلاف ساختار قانونی کارگروه تعامل‌پذیری است که براساس مصوبه ۵۸ شورای عالی فضای مجازی تشکیل شده است. طبق مصوبه شورای عالی فضای مجازی، تمامی دستگاه‌ها برای تبادل اطلاعات باید از طریق مرکز ملی تبادل اطلاعات اقدام کنند و تبادل اطلاعات به شیوه سنتی و مستقیم بین دستگاه‌ها غیرقانونی است. همچنین این مصوبه مشخص کرده که دستگاه‌ها برای دریافت اطلاعات مشخص باید درخواستشان را در کارگروه تبادل‌پذیری مطرح کنند و بعد از رأی‌گیری اجازه دسترسی یا عدم دسترسی به متقاضی داده می‌شود. او تأکید می‌کند که ارسال پیامک تذکر حجاب بدون هیچ توضیح شفافی فقط به معنی دورزدن قانون و دولت است.

با گسترش ارسال پیامک‌های تذکر بدحجابی به زنان پیاده در سطح شهر، واکنش‌های گسترده‌ای در شبکه‌های اجتماعی، رسانه‌ها و حتی برخی محافل حقوقی شکل گرفته است. بسیاری از کاربران در فضای مجازی با انتشار اسکرین‌شات پیامک‌ها، به فقدان شفافیت، نبود رویه قانونی مشخص و نقض حریم خصوصی اعتراض کرده‌اند. در این بین بسیاری به فناوری هم بدبین شده‌اند. اما نکته مهم این است که فناوری در ذات خود بی‌طرف است و نحوه به‌کارگیری آن می‌تواند ابزاری برای شفافیت یا کنترل باشد. استفاده از ابزارهای هوش مصنوعی، تشخیص چهره و تحلیل تصویر برای نظارت بر پوشش زنان، آن‌هم بدون نظارت مستقل، قانون‌گذاری شفاف و امکان اعتراض رسمی، پرسش‌های بنیادینی درباره آینده حریم خصوصی در فضاهای عمومی در ایران مطرح می‌کند. آیا حرکت در شهر به معنای از دست دادن حق ناشناس‌ماندن است؟