

سرباز - خبرنگارها

نگاهی به شماره ۱۶۹ ماهنامه مدیریت ارتباطات



فرزاد نعمتی

خبرنگار گروه فرهنگ

شماره ۱۶۹ ماهنامه «مدیریت ارتباطات» بامدیوم مسئولی امیرعباس تقی پور منتشر شد. تقی پور در سرمقاله کوتاه اما قابل تأمل خود با اشاره به «نارضایتی شدید و ایجاد فاصله عمیق میان درصد قابل توجهی از مردم با سیاست‌های کشور» بدین نکته اشاره کرده که مردم دیگر «کلی گویی» را از کاندیداهای انتخابات نمی‌پذیرند و لازم است نامزدهای ریاست جمهوری پاسخی روشن به پرسش‌های مشخص مردم داشته باشند. از نظر او این پرسش‌ها عبارتند از: رفع فیلترینگ، نحوه مواجهه با چالش حجاب و دوقطبی ایجادشده در جامعه حول آن، لغو تحریم‌ها و روابط با جهان غرب، بازیابی امید و توقف روند مهاجرت نخبگان و جوانان. تقی پور در ادامه می‌نویسد: «اگر چه هیچ ضمانت اجرایی‌ای برای پاسخ‌های نامزدها نمی‌توان یافت، اما در اینجا نیز قول و قرار آنها مثلاً مبنی بر کناره‌گیری زود هنگام در صورت عدم تحقق خواسته‌های مردم، می‌تواند عاملی برای مشارکت بیشتر و رونق انتخابات و امید به تغییر باشد.»

پرونده اصلی این شماره «مدیریت ارتباطات» به سوگیری رسانه‌های جریان اصلی به نفع اسرائیل است. این پرونده «سرباز-خبرنگار» نام دارد و اصل سخن آن این است: «مشروعیت‌بخشیدن رسانه‌های غربی به جنایات جنگی اسرائیل در غزه و روایت یک طرفه و جانبدارانه آنها، افکار عمومی را از آگاهی نسبت به حقیقت آنچه در حال وقوع است، محروم کرده است. رسانه‌ها و روزنامه‌نگاران غربی پیش از آنکه رسالت خود را در انعکاس واقعیت و پوششی دقیق و بی طرفانه از جنگ و وقایع آن بدانند، در کمک به پیروز کردن اسرائیل و انسانیت‌زدایی از کودکان فلسطینی می‌دانند. رسانه‌ها عملاً با تحریف روایات به نفع اسرائیل و اطلاع‌رسانی نادرست، افکار عمومی را جهت‌دهی کرده و امکان ادامه کشتار فلسطینی‌ها را فراهم می‌کنند.» در همین زمینه نوشته‌ای از جرمی اسکپهیل (محمسن محمودی ترجمه کرده است. بحث نویسنده درباره «کارزار تبلیغاتی بی‌رحمانه اسرائیل برای اهریمن‌سازی از فلسطینی‌ها» است که در آن نتانیاهو از وحشت هفتم اکبر برای به راه انداختن جنگی صلیبی استفاده کرده است. باین همه از نظر او: «کارزار تبلیغاتی اسرائیل و پروپاگاندا جهانی آن فقط می‌تواند مرگ، گرسنگی اجباری، کشتار دسته‌جمعی کودکان، آپارتاید، دیوار حائل، کوچ قیامز، مهاجرت اجباری و نابودی مطلق کل جامعه فلسطین را برای مدتی طولانی پنهان کند. بی‌گمان، با گذشت زمان، پنهان کردن اقدامات اسرائیل پس از هفتم اکبر، روایت‌های دروغینی که این رژیم به کار برد و مبارزه نامیدانه نتانیاهو برای حفظ قدرت سیاسی و شخصی‌اش دشوارتر می‌شود.»

بخش مهم دیگر این شماره اما به بزرگداشت وحید عقیلی، استاد برجسته ارتباطات اختصاص دارد که در ششم خردادماه ۱۴۰۳ درگذشت. در این زمینه نازنین بقایی سراغ هادی خانیک، مجید رضائیان و محمد سلطانی فر رفته و نظر آنها را درباره «منش و دانش» وحید عقیلی پرسیده است. رضائیان و سلطانی فر در این گفت‌وگو به نقش تسلط بر زبان انگلیسی در زندگی عقیلی اشاره کرده‌اند. برای نمونه رضائیان می‌گوید: «هر زمان که مهمانی از خارج از کشور به دانشکده علوم ارتباطات و مطالعات رسانه دانشگاه آزاد واحد تهران مرکز می‌آمد، ایشان با آنکه رئیس آن دانشکده بودند، خودشان مسئولیت ترجمه هم‌زمان را بر عهده می‌گرفتند.» او شاخصه بعدی عقیلی را زاپش‌ترش تدریس دروس، صرفاً در حوزه تخصصی و مطالعاتی خودش یعنی حوزه مطالعات ارتباطی می‌داند.

«گول کلاهخود و جلیقه ناخورد» نام مصاحبه‌ای است که نازنین بقایی با آلفرد یعقوب‌زاده عکاس شهیر دارد. یعقوب‌زاده از پدري ارمی و مادری آشوری در تهران به دنیا آمده است. او اگر چه در حوزه‌های مختلف عکاسی کرده، اما شهرتش بیشتر بابت گرفتن عکس‌هایی از جنگ‌ها و درگیری‌های مختلف در سراسر جهان در چهار دهه گذشته به‌ویژه هشت سال جنگ ایران و عراق است. در این گفت‌وگو او درباره مصائب عکاسی در جنگ صحبت کرده است.



محسن عزیز؛
یک خاطره ی فراموش نشدنی منتظر توست.
با تخفیف ۱۵ درصدی برای باشگاه مشتریان
اگه مایل هستی برای اطلاعات این *سفر رویایی*
عدد ۱ رو ارسال کن

ندای لذت فقط چند قدم با تو فاصله داره
تجرباتی را که هرگز فراموش نمی‌کنی
سفرهای بی‌نهایت هیجان‌انگیز
در کنار بهترین راهنمایان
با تخفیف ویژه برای باشگاه مشتریان
تجرباتی که هرگز فراموش نمی‌کنی

دلت می‌خواهد پوست ببرد؟
میکس یا کمپوزیت کامل پوسته
با تخفیف ویژه برای باشگاه مشتریان
در روزهای ویژه
آدرس: شهرری شمسی...

امشب شام برامت چه؟!
بیتراژ سفارش بده!
سبب زینتی ویژه
تعمیر رنگانگ
حفظ تا پایان شب
بیتراژ زیبایی... ۴۲۴۲۴۲۰

هر آنچه از یک فروشنده آرازشی انتظار داری!
ارائه بهترین کیفیت
در بهترین قیمت
مشاهده محصولات در سایت
www...

کلاهبرداری از شهروندان در دسترس خواهند داشت و راحت‌تر می‌توانند اعتماد افراد را به خود جلب کنند.

▼ ای فلانی عزیز!

از سوی دیگر بسیاری از افراد با پیام‌های تبلیغاتی که به‌وفور برای آنها ارسال می‌شود، مشکل جدی دارند. در حالی برخی شرکت‌ها با نام کوچک و صمیمانه، شخص را مورد خطاب قرار می‌دهند که فرد موردنظر مطمئن است هرگز اطلاعات خود را در دسترس این شرکت نداده است. دسترسی به اطلاعات افراد در چنین شرایطی از دو طریق انجام پذیرفته است؛ یا یکی از شرکت‌هایی که این اطلاعات را داشته آن را به شرکت موردنظر فروخته یا از داده‌هایی که در اثر هک‌های گسترده احتمالاً در دارکوب در دسترس است، استفاده شده است. در هر حال نتیجه یکسان خواهد بود؛ اطلاعات فرد موردنظر بدون رضایت شخص در اختیار دیگری قرار گرفته است. اما سوءاستفاده از اطلاعات کاربران به همین جا ختم نمی‌شود. در غیاب قوانین بازدارنده، شرکت‌ها این امکان را دارند که از داده‌های کاربران خود در راستای درآمدزایی بیشتر استفاده کنند. برای مثال تصور کنید شما پلنفرم سفارش غذا هستید. تحلیل مجموعه داده‌هایی که این پلنفرم در اختیار دارد، می‌تواند نشان دهد که چه غذاهایی در چه بازه قیمتی و در چه مناطقی بیشترین فروش را دارند. حالا کافی است این شرکت اقدام به تأسیس رستوران‌هایی کند که این داده‌ها را در اختیار دارند. موفقیت تضمینی است، درحالی‌که نه رستوران‌های همکار، نه کاربران نهایی اطلاعی از این اقدام شما ندارند و نمی‌دانند از داده‌هایشان به این شکل استفاده شده است. این مدل از سوءاستفاده از اطلاعات کاربران می‌تواند در هر کسب‌وکاری بنا بر ماهیت آن اتفاق بیفتد و درآمدهای بی‌بیشتری منجر شود که از انحصار و رفتارهای ضد رقابتی نشئت می‌گیرد.

▼ قانون داریم یا نداریم؟

اتفاقاً مجموعه قوانینی در خصوص حفاظت از داده‌های کاربران در کشور وجود دارد. شورای ملی رقابت نیز قرار است با انحصار و برخورد‌های ضد رقابتی مقابله کند. اما چندین عامل سبب می‌شود بازدارندگی لازم وجود نداشته باشد. اول اینکه به‌باور کارشناسان، مجموعه قوانینی که جهت حفاظت از داده‌های کاربران وجود دارد، بیشتر واکنشی هستند. به این معنی که اتفاقی رخ داده و حالا می‌توان به‌شکلی قانونی آن را محکوم کرد. اما ناگفته پیداست که بسیاری از کاربران دانش، زمان و حوصله پیگیری‌های قضایی این چنینی را ندارند. به همین دلیل است که اتحادیه اروپا قوانین را به نحوی وضع کرده که با خاصیت پیشگیرانه نیز داشته باشند. به این معنی که با کمک کارشناسان استانداردهایی را برای فعالیت شرکت‌ها در نظر گرفته و دائماً رفتار شرکت‌ها را رصد می‌کند و بر آنها نظارت دارد تا بتواند راه سوءاستفاده را مسدود کند. در صورتی که شرکت‌ها از این استانداردها تخلف کنند، با جریمه‌های مالی بسیار سنگین مواجه خواهند شد.

در ثانی، قوانین شفاف و به‌روز نیستند و امکان تفسیرهای متعدد را فراهم می‌کنند. در صورتی که وقتی یک طرف شرکتی با امکانات حقوقی گسترده و در طرف دیگر کاربری با دانش ناکافی وجود دارد، قوانین باید تا حد امکان از شفافیت برخوردار باشند تا تضییع حقوق کاربر در صورت شکایت او، اتفاق نیفتد.

البته می‌توان این سؤال را نیز مطرح کرد که در شرایطی که سازمان‌های دولتی کوچک و بزرگ با بی‌توجهی به موارد امنیتی، اطلاعات کاربران را در معرض هک قرار می‌دهند، آیا می‌توان انتظار داشت رفتار مناسبی در مواجهه با سوءاستفاده از داده‌های کاربران و رعایت نکردن حریم خصوصی آنها صورت پذیرد؟

یک سیاست کلی هستند. خاصه در کشور ما که اگر دولت و حکومت مایل به انجام کاری نباشد، چنین عمومیت و سهولتی اساساً امکان‌پذیر نیست. پس این فروکاستگی هویت ما به‌عنوان مصرف‌کنندگانی سربراه که عمده‌ی فکرمان خوراک و پوشاک امروز و فرداست، هر چند معاییری در حقیقت زندگی اجتماعی این روزگار دارد، اما تلاشی برای تداوم و تثبیت آن نیز هست. اگر ذهن آگاه و مقاومی داشته باشیم، این اهانت مداوم، این نادیده گرفته شدن و این تقلیل معنادر به آن جانور داروینی اندک‌اندک ما را از بهبود شرایط جامعه ناامید می‌کند. یعنی درمی‌یابیم تا چه حد از جریان غالب خواسته‌های فرهنگی و اجتماعی روزگاران دور و پرتیم. چراکه عمومیت پیامک‌ها و گفت‌وگوهای حاکم بر آن‌ها شاخصی مطلوب است برای جریان غالب کردار اجتماعی مردم پیرامون ما. اگر هم ذهن آگاهی نداشته باشیم و آماده تأثیرپذیری باشیم، به سرعت تبدیل می‌شویم به همان چیزی که این محاصره تبلیغاتی در پی آن است: یک مصرف‌کننده که زندگی‌اش باید خلاصه شود در تکاپوی بی‌پایان برای ارزاق، پوشاک، بیمه و دو قران سود بیشتر از فلان حساب یا خرید و البته اگر به تثبیت نسبی اقتصادی رسید هم که باید فکر سفرهای بی‌معنا، ترمیم مو، عمل بینی، گونه و اندام و تکن‌های قاتل تفکر باشد.

حراست از داده‌های کاربران با عنوان GDPR دارد و روی نحوه جمع‌آوری و استفاده از داده‌های کاربران توسط شرکت‌ها حساس است.

شرکت اپل هم سال ۲۰۲۰ ناچار شد جریمه‌ای ۱۳ میلیارد یورویی پرداخت کند، زیرا به نقض قوانین ضد انحصارطلبی اتحادیه اروپا متهم شده بود. همچنین شرکت تیک‌تاک در سال ۲۰۱۹ به‌دلیل جمع‌آوری غیرقانونی اطلاعات کودکان زیر ۱۳ سال به پرداخت جریمه ۵/۷ میلیون دلاری به FTC محکوم شد و مضاف بر آن ۱۷۰ میلیون دلار جریمه به ایالت‌های مختلف آمریکا پرداخت کرد.

▼ اطلاعات کاربران زیر دست هکرها

با گسترش فعالیت کسب‌وکارهای فناوری‌محور و فراگیر شدن استفاده مردم از خدمات و محصولات این کسب‌وکارها، در ایران نیز شاهد موارد متعدد هک و سوءاستفاده از داده‌های کاربران هستیم. طی سال‌های اخیر موارد مختلفی در ابعاد کوچک و بزرگ روی داده، اما یکی از جنجالی‌ترین و متأخرترین آنها، هک اسنپ‌فود بود.

تا مدت‌ها توئیتر پر بود از شوخی‌هایی که مردم با سفارش نوشیدنی یکی از کاربران اسنپ‌فود می‌کردند. ولی اصل ماجرا شوخی نبود. یک گروه هکری مدعی شده بود که اطلاعات بیش از ۲۰ میلیون کاربر اسنپ‌فود را هک کرده و برای اثبات ادعای خود، تصویر از بخشی از این اطلاعات را منتشر کرده بود که به سوژه شبکه‌های مجازی تبدیل شد. در پی این اتفاق و به‌گفته خود این شرکت، اسنپ‌فود با هکرها وارد مذاکره شد و با پرداخت وجه مورد نظر آنها، از انتشار این اطلاعات جلوگیری کرد. در همان زمان بحث‌های مختلفی در خصوص ضعف قوانین در مورد حفاظت از داده‌های کاربران مطرح شد. برخی به نبود قوانین سخت و سخت در ایران در جهت حفاظت از داده‌های کاربران اشاره داشتند و معتقد بودند عدم دسترسی کاربران به حذف اطلاعات خود از پایگاه داده این شرکت، یکی از موارد نقض حریم خصوصی کاربران است و درحالی‌که بعضی از این کاربران مدت‌ها بود از خدمات این شرکت استفاده نمی‌کردند، اما به‌دلیل نگهداری داده‌هایشان در این شرکت و عدم دسترسی‌شان جهت حذف آنها، در معرض درز اطلاعات شخصی‌شان قرار گرفته بودند. برخی نیز از زاویه دیگری به این مسئله پرداخته و معتقد بودند، رقم ناچیزی که شرکت‌های بزرگ برای باگ‌بانتی (کشف و ارائه گزارش آسیب‌پذیری یا باگ از نرم‌افزار و دریافت پاداش) پرداخت می‌کنند، یکی از مهم‌ترین عواملی است که سبب‌ساز چنین اتفاقاتی می‌شود. آنها می‌گفتند این مبلغ انگیزه لازم را برای اطلاع دادن ضعف‌های امنیتی توسط برنامه‌نویسان ایجاد نمی‌کند و راه را برای سوءاستفاده هکرها باز می‌گذارد. پس از این هک، شرکت اسنپ رقم باگ‌بانتی خود را افزایش داد. اما اسنپ‌فود همان‌طور که اولین شرکتی نیست که طی سال‌های اخیر با مسئله هک مواجه شده، آخرین هم نبود و چندی بعد از این واقعه، سازمان حج و زیارت نیز هک شد.

طبیعی است که برخی شهروندان از میزان اهمیت داده‌های خود آگاهی کافی نداشته باشند. مثلاً در مورد هک اسنپ‌فود عده‌ای به شوخی می‌گفتند اینکه ما کی و کجا کباب خورده‌ایم، به کار چه کسی می‌آید و چه اهمیتی دارد؟ اما متخصصان و قانون‌گذاران می‌دانند موارد متعدد هک‌شدن شرکت‌های خصوصی و سازمان‌های دولتی کار را برای کلاهبرداران ساده‌تر از گذشته کرده و می‌تواند به افزایش موارد فیشینگ بینجامد. وقتی کلاهبرداران به اطلاعاتی جزئی مانند آدرس محل سکونت، کد ملی، شماره تلفن و... دسترسی داشته باشند، قطعاً گزینه‌های متنوع‌تری برای

دیگر شخصیت ما را نادیده می‌گیرد. دیگر نه سن و سال، نه میزان سواد و تحصیلات، نه جایگاه اجتماعی و نه احترام شهروندی و انسانی، هیچ‌یک برای ارسال‌کنندگان مهم نیست. با آن صمیمیت مسموم و ریاکارانه و آن ادبیات لمپنی، به اسم کوچک صدایمان می‌زنند و ما را ابله‌انسی از دنیا بی‌خبر تلقی می‌کنند که بدیهیات زندگی را باید تعلیم بگیریم و در اسرع وقت در رفتار و کردارمان تجدیدنظر کنیم و چنان از منظر ذهنی و شناختی عقب‌مانده و درمانده‌ایم که باید معرוב صفات پوچ و دال‌های تهی مورد استفاده آنان در باب توصیف کالاها و رویدادهای مختلف باشیم. سیاهه‌ای از این صفات‌ها را اگر پیش‌رویمان بگذاریم، متوجه این وهن عمومی خواهیم شد؛ بزرگترین، بهترین، بی‌سابقه، بی‌نظیر، خفن، مطمئن، مسئولیت‌پذیر و...

در جهان مصرف‌گرا، هیچ گریه‌ای برای رضای خدا موش نمی‌گیرد. آن‌ها در فکر منفعت خویش هستند و البته باید به‌شکلی از این منفعت برخوردار شوند که به ما نیز القا نمایند که داریم از فلان خرید یا رفتار یا سرمایه‌گذاری، سود می‌بریم و چیزی به دست می‌آوریم. اگر این پیش‌فرض را بپذیریم، متوجه خواهیم شد که از یک‌سوی این پیامک‌ها، چون مجاز هستند و در سطح گسترده به همگان می‌رسند، برخی از



▼ استفاده بدون رضایت، سوء استفاده است

این گونه نیست که شرکت‌ها این اختیار را داشته باشند تا از اطلاعاتی که کاربران به آنها ارائه می‌دهند، به هر شکلی که علاقه‌مند بودند، استفاده کنند. زمان دریافت این اطلاعات باید به‌شکل شفاف به کاربر اعلام شود که این داده‌ها در چه جاهایی قابلیت استفاده خواهند داشت. به‌علاوه بهره‌برداری از این داده‌ها در جهت ایجاد انحصار و اقدامات ضد رقابتی نیز جریمه‌های سنگینی در پی دارد. در ایالات‌متحده آمریکا و اتحادیه اروپا قوانین سخت و سختی در این خصوص وجود دارد. به‌خصوص این موضوع در اروپا با جدیت بیشتری دنبال می‌شود. کوچک یا بزرگ بودن شرکت‌ها سبب نمی‌شود تا مراجع قانونی از برخورد با آنها صرف‌نظر کنند و اتفاقاً شرکت‌های بزرگ که دسترسی به داده‌های کاربران بیشتری دارند، بیشتر هم زیر ذره‌بین قرار می‌گیرند و نهادهای نظارتی به طور مداوم فعالیت آنها و رعایت کردن استانداردها توسط این شرکت‌ها را رصد می‌کنند. شرکت فیس‌بوک که امروز آن را با نام متا می‌شناسیم، در سال ۲۰۱۹ به‌دلیل آنکه اطلاعات شخصی ۸۷ میلیون کاربر فیس‌بوک را بدون رضایت آنها جمع‌آوری کرده و در اختیار شرکت تحلیل داده کمبریج آنالیتیکس قرار داده است، پنج میلیارد دلار جریمه شد. همچنین این شرکت در سال ۲۰۲۱ نیز به‌دلیل نقض قوانین حریم خصوصی کودکان ۲۲۷ میلیون دلار جریمه پرداخت کرد.

شرکت گوگل به‌دلیل استفاده نادرست از اطلاعات شخصی کاربران جهت تبلیغات هدفمند در سال ۲۰۱۹ توسط اتحادیه اروپا ۵۰ میلیارد دلار جریمه شد. این اتحادیه دو سال پیش‌تر شرکت آمازون را نیز به‌دلیل نقض قوانین حریم خصوصی اتحادیه اروپا ۸۸۷ میلیون یورو جریمه کرده بود. اتحادیه اروپا قوانین محکمی جهت