

◀ آخرین یافته‌های اچ‌بی آر
درباره آینده کسب‌وکارها

Insights You Need from

**Harvard
Business
Review**

داده‌های مشتری و حریم خصوصی

انتشارات **راه‌پرداخت**

بِسْمِ اللَّهِ
الرَّحْمَنِ
الرَّحِيمِ

۱

۲

۳

۴

داده‌های مشتری و حریم خصوصی

بینش‌هایی از مجله کسب و کار هاروارد



داده‌های مشتری و حریم خصوصی: بینش‌هایی از مجله کسب و کار هاروارد لزلی کی. جان، موریس استاک، اندرو برت، دنیل دوبریگوسکی شراره شبل الحکما تهران: راه پرداخت، ۱۴۰۰. ۱۲۰ ص؛ ۴۱/۵ + ۱۲/۵ س.م. ۹۷۸-۶۲۲-۷۷۰۲-۰۵-۷ فیبا	عنوان و نام پدیدآور: نویسندگان: مترجم: مشخصات نشر: مشخصات ظاهری: شابک: وضعیت فهرست نویسی: یادداشت: عنوان اصلی:
Customer data and privacy : the insights you need from Harvard Business Review, [۲۰۲۰]. بینش‌هایی از مجله کسب و کار هاروارد. حفاظت داده‌ها Data protection حق صیانت از حریم شخصی Privacy, Right of شبل الحکما، شراره، ۱۳۷۴ -، مترجم انتشارات هاروارد بیزینس ریویو Harvard Business Review Press QAV۶/۹ ۰۰۵/۸ ۸۴۰۶۹۷۴ فیبا	عنوان دیگر: موضوع: موضوع: موضوع: موضوع: شناسه افزوده: شناسه افزوده: شناسه افزوده: رده بندی کنگره: رده بندی دیویی: شماره کتابشناسی ملی: وضعیت رکورد:

چرا از کاغذ بالکی استفاده می‌کنیم؟ ۱. کاغذ بالکی از کاغذهای تحریر سفید، سبک‌تر است ۲. در تهیه آن از مواد شیمیایی استفاده نشده و شیوه تولید آن مکانیکال است ۳. نور را منعکس نمی‌کند و مانع از خستگی چشم هنگام مطالعه می‌شود « کاغذ بالکی به دلیل موارد بالا از کاغذ تحریر سفید گران‌تر است »	 The mark of responsible forestry FSC® C009732 این کتاب با کاغذ بالکی دوستدار محیط زیست تولید شده است.
--	---

داده‌های مشتری و حریم خصوصی

بینش‌هایی از مجله کسب و کار هاروارد

نویسندگان:

لزلی کی. جان

موریس استاک

اندرو برت

دنیل دوبریگوسکی

مترجم:

شراره شبل‌الحکما



عنوان:	داده‌های مشتری و حریم خصوصی؛ بینش‌هایی از مجله کسب‌وکار هاروارد
ناشر:	راه پرداخت
نویسندگان:	لزلی کی. جان، موریس استاک، اندرو برت، دنیل دوبریگوسکی
مترجم:	شراره شبل‌الحکما
ویراستار ارشد:	مینا والی
ویراستار محتوایی:	قاسم سرافرازی
ویراستار فنی:	یلدا شایسته‌فر
بازبینی نهایی متن:	رضا قربانی
صفحه‌آرا:	بهناز سعیدی
ناظر چاپ:	قادر شهبازی
نوبت چاپ:	اول ۱۴۰۰
شمارگان:	۱۰۰۰ نسخه
شابک:	۹۷۸-۶۲۲-۷۷۰۲-۰۵-۷
تلفن:	۰۲۱-۴۴۴۳۹۶۶
دورنگار:	۸۹۷۸۴۹۰۲
ایمیل:	info@way2pay.press
وبسایت:	way2pay.shop
لیتوگرافی:	هنراشکان
چاپ و صحافی:	واژه

همه حقوق چاپ و نشر این اثر برای «انتشارات راه‌پرداخت» محفوظ است. هرگونه تکثیر، انتشار و بازنویسی این اثر یا قسمتی از آن به هر شکل و شیوه (چاپی، صوتی، ویدئویی، دیجیتال و...) بدون اجازه کتبی ناشر ممنوع است.

فهرست

- مقدمه: اعتماد؛ مزیت رقابتی جدید ۱۵
۱. رضایت کورکورانه ۲۰
۲. چرا نباید بگذاریم چند شرکت فناوری، داده‌هایمان را به انحصار خودشان درآورند؟ ۴۴
۳. حریم خصوصی و امنیت سایبری در حال تلاقی بایکدیگرند؛ چرا این موضوع برای افراد و شرکت‌ها اهمیت دارد؟ ۵۶
۴. سیاست حریم خصوصی قدرتمند می‌تواند میلیون‌ها دلار از خسارت‌های شرکت‌تان بکاهد ۶۰
۵. آیا به همان اندازه که کاربران‌تان به حریم خصوصی اهمیت می‌دهند، شما نیز به آن توجه دارید؟ ۶۹
۶. چطور قدرتی را که تقاضا نکرده بودید، به کار بگیرید ۷۵
۷. برای بازیابی اعتماد کاربران، بازیابان باید فعالیت‌های داده‌شفافی را در پیش بگیرند ۸۵
۸. بلاکچین چطور می‌تواند در ایجاد روابط بهتر مشتری به بازیابان کمک کند ۹۱
۹. خطرات حمایت‌گرایی دیجیتال ۱۰۰
۱۰. چرا شرکت‌ها ائتلاف‌های امنیت سایبری تشکیل می‌دهند؟ ۱۰۶

[یادداشت حامی]

همه مشتاق رفت و آمد با کسانی هستیم که ما را به خوبی می‌شناسند. می‌دانند چه غذاهایی، چه فیلم‌هایی، چه جاهایی و چه آهنگی‌هایی دوست داریم و حواسشان هست که در سفر و حضر، همه چیز باب میل ما پیش برود. در دنیای ماشینی امروز، حضور چنین افرادی غنیمت بزرگی است. چه چیزی لذت بخش تر از اینکه وقتی به رستوران یا هتل می‌رویم، مهمان‌دار سؤال کند همان همیشه‌گی و ما با آرامش و لبخندی بر صورت فقط سر تکان بدهیم و بدانیم تمام جزئیات مدنظر ما، از میزان ترد یا آبدار بودن غذا تا سفتی و نرمی بالش، رعایت می‌شود.

در ارتباط با برندها هم همین ماجرا برقرار است؛ ما دنبال برندهایی هستیم که خود ما برایشان مهم باشیم نه پولمان. گام نخست این مسیر، شناخت دقیق ما توسط آن‌ها و نتیجه نهایی، ارائه خدمات‌ها و محصولات سفارشی به ماست؛ درست مانند مشاوران، پزشکان یا وکلایی که به خوبی ما را می‌شناسند و بهترین‌ها را به ما پیشنهاد می‌دهند.

داستان اما زمانی دگرگون می‌شود که همین دیگران بخواهند از انبوه اطلاعاتی که به دست آورده‌اند و شناختی که باعث این همه لذت و آرامش و آسایش شده، علیه ما استفاده کنند. ماجرای اطلاعاتی که به سایت‌ها می‌دهیم نیز بر همین منوال است. تا زمانی که این داده‌ها موجب نتایج جست‌وجوی دقیق‌تر، پیشنهاد محصولات ناب‌تر (که مدت‌هاست دنبالشان می‌گردیم)، چیدمان صفحه به همان صورتی که با آن احساس راحتی می‌کنیم و

ارائه خدمات ویژه و در شأن ما باشد، همه چیز عالی است، اما کلافه و عصبانی می‌شویم وقتی دوروبرمان پر شود از تبلیغات بی‌شمار یا سوءاستفاده از اطلاعات شخصی‌مان. داده‌ها، تیغ دودم عصر جدید هستند؛ ابزارهایی که هم می‌شود دنیایی بهتر و دوست‌داشتنی‌تر برایمان بیافرینند و هم می‌توانند همه چیز را خراب کنند. فاصله میان این دو، به آمادگی و عملکرد ما بستگی دارد.

همان‌طور که این کتاب بیان می‌کند، حس بی‌اعتمادی عمومی مردم جهان نسبت به شرکت‌های فناوری، آن‌چنان زیاد شده که می‌تواند همه این سازمان‌های داده‌بنیان را در معرض خطر قرار دهد. نگرانی از آسیب به هویت دیجیتال و اطلاعات ثانویه‌ای که الگوریتم‌ها از داده‌های ما استخراج می‌کنند، به دغدغه‌ای تبدیل شده که روزبه‌روز انسان‌های بیشتری را به فکر فرو می‌برد. از سوی دیگر حملات سایبری به اتفاق پرتکرار و مرسوم این روزها تبدیل شده است. آسیبی که دود آن نه فقط در چشم سازمان قربانی که در چشم رقبای نزدیک و کل آن صنعت می‌رود و تروخشک را باهم می‌سوزاند.

افراد معمولاً به مزایا و خسارت‌های آنی بیشتر اهمیت می‌دهند تا مواردی که در آینده ممکن است برایشان اتفاق بیفتد. انداختن همه بار مراقبت و محافظت از اطلاعات بر دوش کاربران، آن‌ها را خیلی زود دچار خستگی در تصمیم‌گیری و بی‌تفاوتی می‌کند. گویی از افراد بخواهیم وقتی به رستوران می‌روند، خودشان سلامت غذا را بررسی کنند. همان‌گونه که این کار بر عهده کسب و کارها، انجمن‌های صنفی و دولت گذاشته شده و نتیجه آن مراجعه بی‌دغدغه مردم به رستوران‌هاست، در کسب و کارهای داده‌محور نیز باید چنین رویه‌ای را طی کرد. مسئولیت‌پذیر بودن و امانت‌دار اطلاعات بودن توسط پلتفرم‌ها، هم از کاربران محافظت می‌کند و هم بدون نیاز به دخالت شدید دولت، جلوی سقوط بازار را می‌گیرد. وقتی قوانین دولتی و روش‌های قابل قبولی برای استفاده از اطلاعات شخصی کاربران موجود نباشد، شرکت‌ها باید به امانت‌داران اطلاعات تبدیل شوند؛ یعنی به نفع مشتریان عمل کنند و وقتی تعارض منافع پیش می‌آید، منافع آن‌ها را به منافع خودشان ترجیح بدهند.

فناوری اطلاعات، پلتفرم‌ها و علوم داده در ایران نیز با سرعت و در حوزه‌های فراوان در حال گسترش است. با مسئولیت‌شناسی و امانت‌داری پیش‌تازان این حوزه، باید مسیری

درست را پایه‌ریزی کرد؛ مسیری که امنیت و حفظ حریم شخصی و همچنین بهره‌مندی از منافع حاصل از فناوری و هوش مصنوعی را توأمان در اختیار جامعه قرار دهد.

شرکت پردازش اطلاعات مالی پارت هشت سال پیش با مأموریت تبدیل شدن به یک دستیار هوشمند اقتصادی و با هدف آگاهی‌بخشی و توانمندسازی افراد جامعه آغاز به کار کرد؛ جامعه‌ای که بتواند با تصمیم‌ها و رفتارهای درست مالی، زندگی آرام و آسوده‌ای را برای خود رقم زند و موفقیت در سایر ابعاد زندگی را پایه‌ریزی کند. پارت خود را در دسته کسب و کارهای اجتماعی اقتصادی جانمایی کرده است؛ جایی که حل مسائل مردم و آفرینش راهکارهایی درست، توسط دانشمندان کشور، اهمیت به مراتب بیشتری از کسب درآمد دارد. انتخاب به عنوان کارآفرین برتر ملی، ارائه خدمت به حدود هشت میلیون کاربر یکتا، درخشش سامانه‌هایی چون سیگنال (پرمخاطب‌ترین اپلیکیشن مالی کشور) و مرآت (پرمخاطب‌ترین سامانه اعتبارسنجی کشور) در کنار بیش از ده سامانه دیگر، نشان از اقبال ارزشمند مردم به پارت دارد؛ جایگاهی ویژه که مسئولیت ما را مضاعف می‌کند. امیدواریم با همراهی تمام تلاشگران مجموعه پیشروی فناوری کشور، آینده‌ای درخور و سزاوار ایران پدید آوریم.

علی رسولی‌زاده/مدیرعامل پارت

[یادداشت ناشر]

بسیار خوشحالم که هشتمین جلد از مجموعه کتاب‌های آینده کسب و کارها منتشر شده و اکنون در اختیار شماست. هاروارد بیزینس ریویو نیازی به معرفی ندارد و مجموعه کتاب‌هایی که این انتشارات درباره مهم‌ترین موضوعات پیش روی کسب و کارها منتشر کرده، هم اکنون برای اهل فن شناخته شده است. این کتاب‌ها با زبانی ساده، پیچیده‌ترین موضوعات پیش روی کسب و کارها را توضیح داده‌اند و به دور از خودنمایی و پیچیده‌نمایی تلاش می‌کنند ذهن‌های جست‌وجوگر را راهنمایی کنند. قاعدتاً این کتاب‌ها را باید به عنوان شروع جست‌وجویی در نظر گرفت که بخش مهمی از آن بر دوش کسانی است که هر روز در میدان کسب و کار فعالیت می‌کنند.

خوشبختانه ادبیات کسب و کار در سال‌های گذشته رشد قابل قبولی در ایران داشته و خوشبختانه آشنایی با فناوری و نوآوری به مرحله قابل قبولی در میان مدیران رسیده است. آنچه در سال‌های گذشته اکوسیستم کسب و کارها را تغییر داده، قاعدتاً در سال‌های پیش رو تأثیرگذاری بیشتری خواهد داشت. در این مسیر و راه سخت، به قطب‌نمایی نیاز است که بدون آنها طی طریق سخت می‌شود و دشوار.

هشتمین کتاب از سری کتاب‌های اچ‌بی‌آر به موضوع کمتر پرداخته شده «داده‌های مشتری و حریم خصوصی» می‌پردازد. متأسفانه این موضوع در جهان به اندازه کافی مورد توجه قرار نگرفته و چالش‌های زیادی بر سر راه توسعه اقتصادها قرار داده است.

این کتاب سؤالات زیادی درباره موضوع مهم «اعتماد» مطرح کرده است. موضوعاتی مانند انحصار داده‌ها در دست چند شرکت بزرگ، اهمیت امنیت سایبری، سیاست حریم خصوصی، نقش بلاکچین و چند مورد دیگر از مهم‌ترین مواردی هستند که در این کتاب مورد بحث و بررسی قرار گرفته‌اند.

به مخاطب حرفه‌ای در زمینه این کتاب و البته دیگر کتاب‌های اچ‌بی‌آر نکته‌ای را باید یادآوری کنم؛ حجم کم این کتاب‌ها نباید ما را گمراه کند که این کتابی برای مطالعه سریع است یا کتابی به زبان ساده و دم‌دستی برای آشنایی با مفاهیم مهم. این کتاب را به هیچ‌وجه دست‌کم نگیرید! برای مطالعه این کتاب حتماً باید وقت بگذارید و با آرامش مقاله‌های کتاب را مطالعه کنید. باید زمان بگذارید که مفاهیم کتاب در شما رسوب کند. باید به آنچه در کتاب گفته شده و آنچه در محیط‌های واقعی کسب‌وکار خود با آن دست‌به‌گریبان هستید، به شکل تطبیقی نگاه کنید. نه این کتاب می‌خواهد راه‌حل قطعی مسائل را به شما معرفی کند و نه برای موضوعات پیچیده مربوط به آینده، چنین راه‌حلی وجود دارد. این کتابی است برای اندیشه‌ورزی در حوزه کسب‌وکار. بر خلاف عموم کتاب‌های مدیریتی که تلاش می‌کنند راه‌حل‌های صریح و قطعی ارائه دهند، این کتاب چنین چوب جادویی ندارد. بر خلاف کتاب‌های مرسوم مدیریت، این کتاب هیچ جعبه‌ابزاری به شما معرفی نمی‌کند. این کتاب خاص و مجموعه کتاب‌های اچ‌بی‌آر تلاش می‌کنند مدل‌های ذهنی را جلا دهند؛ این کتاب تلاش می‌کند مانند یک مربی خوب ما را به سوی اصل خودمان راهنمایی کند؛ کاری سخت و دشوار که برای انجام آن به همراهی صد درصدی نیاز است.

از شما دعوت می‌کنم زمان بگذارید و در میان انبوه فعالیت‌های روزمره خود هر بار صفحاتی از کتاب را بخوانید و به آنها فکر کنید. از شما دعوت می‌کنم یافته‌های خود را بنویسید و تلاش کنید این زنجیره ادامه یابد؛ شاید بتوانیم به مرور به توسعه اقتصاد ایران کمک کنیم.

{

مقدمه

}

اعتماد؛ مزیت رقابتی جدید

تیموتی موری

فرض کنید می‌خواهید دختر نوجوان‌تان را به ساحل ببرید و به او والیبال یاد دهید. قبل از آنکه از خانه بیرون بروید، شرایط آب‌وهوایی را از الکسامی پرسید و آدرس ساحل را داخل گوگل‌مپ می‌زنید تا وضعیت ترافیک مسیرتان را چک کنید. وقتی سوار خودروی تسلا مدل ۳ می‌شوید، خودرو دقیقاً می‌داند کجا می‌روید و چه کسی در حال رانندگی است. در مسیر، اسکنرهای تشخیص پلاک، مطمئن می‌شوند که عوارض راه را پرداخت کرده باشید و پیشروی شما را در مسیر کنترل می‌کنند. وقتی به مقصد می‌رسید، با استفاده از اپلیکیشن پارک‌موبایل قبض پارکینگ خود را می‌پردازید و با اپلیکیشن استارباکس برای خودتان قهوه سفارش می‌دهید. هنوز دو ساعت از شروع آخر هفته‌تان نگذشته، اما آمازون، گوگل، تسلا، دولت، ای‌تی‌اند‌تی، ارائه‌دهنده خدمات پارکینگ، استارباکس، اپل و ارائه‌دهنده خدمات پرداخت‌تان، همگی می‌دانند شما کجا هستید و چه کار می‌کنید. تازه همه اینها مربوط به قبل از زمانی است که اطلاعات شما را به دلالتان داده بفروشد.

دلالتان داده، اطلاعات شخصی شما را به شرکت‌های دیگر می‌دهند و از آن برای تجارب شخصی یا بازاریابی هدفمند استفاده می‌کنند. اما بسیاری از شما از این موضوع بی‌خبرید، نسبت به آن بی‌اعتنایید یا دیگر آن را پذیرفته‌اید. شاید فکر می‌کنید رفاهی که این پلتفرم‌ها برایتان ایجاد کرده‌اند، از زبانی که به شما می‌زنند بیشتر است و به همین خاطر به آن تن داده‌اید. این جریان باعث ایجاد «پارادوکس حریم خصوصی» شده است. در پارادوکس حریم خصوصی، افراد نسبت به شرایط‌شان نگران‌اند، اما برای بهبود آن هیچ تلاشی نمی‌کنند و تغییری در رفتارشان به وجود نمی‌آورند. با این حال، موضوع نظارت دیجیتال آن‌قدر فراگیر شده که کاربران نگران، دست به عمل زده‌اند و در حال بازخواست شرکت‌ها درباره نحوه رفتارشان با داده‌ها هستند.

دولت‌ها نیز یک قدم پیش تر رفته‌اند و در واکنش به سوءاستفاده و دسترسی غیرمجاز به داده کاربران، قوانین سخت‌گیرانه‌تری را وضع کرده‌اند. مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR) و لایحه حریم خصوصی مشتریان کالیفرنیا (CCPA) در آمریکا دو مورد از این قوانین هستند. واکنش شدید رگولاتوری تنها یکی از عواقب سوءاستفاده از داده‌های کاربران است. این موضوع حتی باعث آسیب به محبوبیت کسب‌وکارها، خسارت‌های مالی و بیکاری بسیاری از مدیران (از جمله مدیران عامل) شده است. سوءاستفاده از داده و تجاوز به آن باعث می‌شود کسب‌وکارها نتوانند کارمندان با استعدادی جذب و حفظ کنند. از همه مهم‌تر، عدم رفتار صحیح با اطلاعات مشتری باعث می‌شود کاربران تان از شما دوری کنند و اعتمادشان را نسبت به شما از دست بدهند. اگر کاربران به شما اعتماد نداشته باشند، مسلماً ارتباطشان را با شما قطع می‌کنند. اینجاست که اعتماد بیش از هر زمان دیگری اهمیت می‌یابد.

شرکت‌های قابل اعتماد می‌توانند اطلاعات بیشتری از کاربران‌شان به دست آورند و از آن اطلاعات برای بهبود خدمات‌شان استفاده کنند. این موضوع باعث می‌شود آنها نسبت به دیگران مزیت رقابتی داشته باشند. همچنین وقتی اتفاق یا خطایی از طرف این‌گونه شرکت‌ها رخ می‌دهد، افراد راحت‌تر آن را نادیده می‌گیرند و فراموش می‌کنند. بازار اسپیکرهای هوشمند را در نظر بگیرید. الکسای آمازون تقریباً ۷۰ درصد این بازار را تصاحب کرده، در حالی که اسپیکرهای پرتال فیس‌بوک، با وجود کیفیت بالا، نسبت به اسپیکرهای آمازون فروش کمتری دارند. با توجه به تعداد و وسعت تجاوز فیس‌بوک به داده‌های مشتریان، تعجبی ندارد که چرا محصولاتش این قدر کم‌طرفدار هستند. متأسفانه اعتماد با معیارهای کسب‌وکاری و شاخص‌های کلیدی عملکرد (KPI) مشخص نمی‌شود. اعتماد را باید به صورت غیرمستقیم و با توجه به میزان ریزش مشتری، سهم کیف پول مشتری، ارزش طول عمر مشتری و معیارهای نگرشی همچون شاخص خالص ترویج‌کنندگان (NPS) اندازه گرفت. اعتماد در ذهن کاربران است و به مرور زمان، بر اساس درک و تجاربی که از شما دارند، شکل می‌گیرد. به همین خاطر اعتماد موضوعی نیست که شرکت به طور کامل بر آن کنترل داشته باشد، اما می‌توانید با انجام یکسری اقدامات، احتمال مورد اعتماد واقع شدن را

افزایش دهید. فکر می کنید علاوه بر رعایت مقتضیات رگولاتوری، شرکت شما چطور می تواند اعتماد مشتریان به دست بیاورد؟

درباره نحوه استفاده از داده شفاف باشید

با جملات حقوقی ثقیل و نامفهوم عملیات مربوط به داده خود را پنهان نکنید؛ در عوض، با زبانی ساده، صادقانه و با شفافیت تمام، سیاست خود را به مشتریان توضیح دهید. مثلاً به جای آنکه تغییرات حریم شخصی برنامه را با یک پیام متنی به اطلاع کاربران برسانید و از آنها بخواهید با زدن دکمه «می پذیرم» موافقت خود را اعلام کنند، از مدیرعاملتان بخواهید برایشان یک ویدئوی کوتاه ضبط کند و موضوع را به زبان عامیانه برایشان توضیح دهد. احتمال اینکه کاربران اعلان های متنی را بخوانند بسیار کم است، ولی هیچ گاه از یک ویدئوی ساده، عبور نمی کنند. این کار نه تنها اعتماد کاربران را نسبت به شما بیشتر می کند؛ بلکه باعث می شود اگر زمانی در سیستم تان نشت داده اتفاق افتاد، کمتر شما را مجازات کنند.

به کاربران تان حق کنترل دهید

اگر به کاربران ابزاری بدهید که بتوانند نحوه تعاملات شان با شرکت شما را مدیریت کنند و همچنین صادقانه بگویند از داده های آنان چه استفاده ای می کنید، اعتمادشان نسبت به شما بیشتر می شود. این موضوع به آنها نشان می دهد که شما به خواسته هایشان احترام می گذارید و مواظب داده هایشان هستید. یک داشبورد یا پنل حریم خصوصی برای کاربران ایجاد کنید، آن را بین آنها ترویج دهید و برای آن یک لینک دانلود قرار بدهید. مطمئن شوید کار با پنل برای همه کاربران راحت است و قابلیتی را در اختیارشان قرار دهید تا بتوانند هر یک از داده هایشان را دانلود یا حذف کنند.

برای آنها مزیت دوطرفه ایجاد کنید

اخیراً، مکانیسم تبادل یک طرفه بین کاربران و ارائه دهندگان تا حدودی از بین

رفته، اما شرکت‌های معتمد باید نسبت به دیگران یک گام فراتر بروند و به ازای داده‌ای که از کاربران می‌گیرند، به آنها ارزشی معین ارائه دهند. کسب‌وکارهایی مانند اسپاتیفای و پینترست با مشاهده رفتار کاربران‌شان، پست‌های مشابهی برای آنها به نمایش می‌گذارند. در نتیجه، احتمال آنکه کاربر به آن پست اسپاتیفای گوش دهد یا محتوای پینترست را دوست داشته باشد، بیشتر می‌شود. هرچه شرکت ارزش بیشتری به کاربران خود ارائه دهد و در ارائه ارزش پیوسته‌تر عمل کند، اعتماد آنها نسبت به او بیشتر می‌شود. در حال حاضر، کاربران اعتماد را فقط بر اساس معتبر بودن یک کسب‌وکار نمی‌سنجند. درست مانند درک برند، اعتماد نیز نوعی ارزیابی احساسی است که مشتریان نسبت به شما انجام می‌دهند.

از آنچه قانون برایتان مشخص کرده، فراتر بروید

از اوایل سال ۲۰۰۰ تا اوایل ۲۰۱۰، شرکت‌های فناوری داده‌محور برای حریم خصوصی افراد هیچ قیدوبندی قائل نبودند و به همین خاطر سوءاستفاده‌های زیادی از اعتماد مشتریان می‌کردند. اما امروزه، اگر شرکتی به حریم خصوصی افراد توجه نکند، کاربران خیلی سریع آن را ترک می‌کنند و به یک پلتفرم جایگزین می‌روند. این موضوع باعث شده شرکت‌ها نسبت به سیاست‌های داده و حریم خصوصی‌شان دقیق‌تر شوند تا از دیگران عقب نمانند. همچنین سبب شده علاوه بر GDPR و CCPA قوانین دیگری هم روی کار بیاید. کسانی که قبلاً مورد سوءاستفاده شرکت‌های فناوری داده‌محور قرار گرفته‌اند، اعتمادشان را نسبت به محیط‌های این چنینی از دست داده‌اند. بنابراین، کسب‌وکارها و صنایعی که در حال دیجیتالی کردن تجربه مشتری خود هستند، سخت‌تر می‌توانند اعتماد آنها را جلب کنند. برای کسب اعتماد کاربران، باید فقط داده‌هایی را جمع‌آوری کنید که شرکت‌تان به آن نیاز دارد. همچنین درباره نحوه استفاده از داده‌ها به مشتریان‌تان اطلاع دهید و با آنان مشتری‌مدارانه رفتار کنید.

در آینده چه اتفاقی می‌افتد؟ در آینده نیز قوانین به قوت خود باقی خواهند ماند و اگر لازم باشد تغییری کنند، سخت‌گیرانه‌تر می‌شوند. در گذشته، رگولاتورها نسبت به

کسب و کارهای اینترنتی رویکردی محتاطانه داشتند و دخالتی در امور آنها نمی کردند، اما اکنون به خوبی می دانند که اطلاعات کاربران به محافظت نیاز دارد.

کسب و کارهایی که با قوانین سروکار دارند، معمولاً الزامات سختگیرترین منطقه را انتخاب کرده و طبق آن عمل می کنند؛ چون اگر بخواهند یک محصول دیجیتال جداگانه برای کالیفرنیا، یکی برای سایر نقاط آمریکا و یکی برای اتحادیه اروپا تنظیم کنند، سود چندانی نمی برند.

اشتیاق کسب و کارها نسبت به جمع آوری داده کاربران روز به روز در حال افزایش است. دسترسی به داده مزیت رقابتی کسب و کارها را افزایش می دهد؛ زیرا آنها می توانند به کمک این داده ها تجربه مشتری ارزشمندتر، متناسب تر و شخصی سازی شده ای را به کاربران شان ارائه دهند. در گذشته، تبلیغات شخصی سازی شده کار آسانی بود؛ اگرچه برای این کار از داده هایی استفاده می شد که جزء داده های حساس نبودند، اما اکنون این کار دشوارتر شده است. اپلیکیشن های پزشکی که دی ان ای و سوابق پزشکی بیمار را نگهداری می کنند، محصولات سلامت روان که از بیمار درباره سوابق بیماری های روانی اش می پرسند، یا پلتفرم های مالی که تمام تاریخچه خرید شما را ضبط می کنند، همگی به داده های بسیار حساسی دسترسی دارند؛ بنابراین کاربران به سراغ شرکت هایی می روند که قابل اعتمادتر باشند و بتوانند با خیال راحت داده هایشان را در اختیارشان بگذارند.

هنوز نمی دانیم که در آینده، نگرش افراد نسبت به حریم خصوصی داده چه تغییراتی می کند، اما برای تصمیم گیری های کسب و کاری، امن ترین راه این است که فرض کنیم تشکیک مشتریان بیشتر خواهد شد. طبق این فرضیه، شرکت ها باید به انتظارات مشتری توجه بیشتری بکنند. در فصل های مختلف این کتاب به شما یاد می دهیم چگونه به جمع آوری، نگهداری و استفاده از داده های مشتری بپردازید و در عین حال اعتماد آنها را نسبت به کسب و کارتان افزایش دهید.

۱. رضایت کورکورانه

لزلی کی. جان

وبسایت آماری یونیون یک بار مقاله‌ای با این عنوان منتشر کرد: «یک تبلیغ کفش مزاحم، خانمی را تا هشت وبسایت تعقیب کرد!» این مقاله داستانی از یک شخصیت خیالی است که هر بار آنلین می‌شود، تبلیغ یکسانی را می‌بیند. به قول خودش: «یک تبلیغ کفش مدام مرا تعقیب می‌کند و ترسناک‌ترین قسمتش این است که حتی سائیز پای مرا هم می‌داند.» هدف اصلی این مقاله این بود که به بیان طنز از ترفندهای بازاریابی زشت و رایج دنیای دیجیتال انتقاد کند. اما الان فناوری آنچنان در این مسیر پیشرفت کرده که دیگر جایی برای شوخی کردن درباره آن نمی‌ماند. قبلاً تبلیغات چنان مجازی با استفاده از کوکی‌ها و ترفند هدف‌گیری مجدد، ما را در اینترنت دنبال می‌کردند، اما اکنون دسترسی‌شان بسیار بیشتر شده است. تلفن‌های هوشمند می‌توانند حتی مکان فیزیکی ما و فاصله‌مان با افراد دیگر را هم تخمین بزنند. همان‌طور که محققان اخیراً کشف کرده‌اند، این کار حتی با خاموش کردن سیستم لوکیشن موبایل باز هم امکان‌پذیر است. حتی اگر گزینه «ردیابی» را در مرورگر وب غیر فعال کنیم، ردپای دیجیتال ما می‌تواند روی دستگاه‌های دیگر مشخص باشد و در نتیجه امکان فاش شدن هویت اصلی ما وجود دارد. دستیارهای هوشمند خانگی مانند الکسا به گفت‌وگوهای ما گوش می‌دهند و وقتی فعال می‌شوند، گفته‌های ما را ضبط می‌کنند. حتی بعضی وسایل روزمره (از عروسک‌های باربی گرفته تا دستگاه‌های پزشکی) می‌توانند به اینترنت متصل شوند و اطلاعاتی درباره حرکات، رفتار، علائق و حتی سلامت ما به دیگران بدهند. یکی از مدل‌های کسب‌وکاری فعلی در دنیای وب این است که تا جای ممکن از افراد اطلاعات جمع کنند، سپس برای متقاعد کردن، هدف قرار دادن، جریمه کردن یا تشویق افراد از آن استفاده کنند (یا آن را بفروشند). در نتیجه، اینترنت به یک اقتصاد نظارتی تبدیل شده است.

افزایش علوم داده باعث شده جمع‌آوری اطلاعات برای شرکت‌ها کارایی بیشتری داشته باشد. آنها می‌توانند با دانشی که دارند، برای هر فرد یک پروفایل داده بسازند و تمام جزئیات و اطلاعات‌شان را در آن جای دهند. فناوری یادگیری ماشین و هوش مصنوعی می‌توانند به کمک داده‌های «به‌ظاهر پراکنده» هر فرد، پیش‌بینی‌های دقیق و گهگاه ترسناکی از آنها انجام دهند. شرکت‌ها می‌توانند با کمک تجزیه و تحلیل داده، وابستگی سیاسی یا گرایش جنسی یک فرد را حدس بزنند یا حتی بفهمند که او روابط نامشروع داشته است. از وقتی فناوری‌هایی مانند «نرم‌افزار تشخیص چهره» و «آزمایش DNA در خانه» به نرم‌افزارهای موبایلی اضافه شده، تسلط کسب و کارها بر ما افزایش یافته و به‌زودی از این هم فراتر خواهد رفت، تا جایی که ناامنی در دنیای مجازی، از مشکلات امنیتی قرن بیستم (که شرکت‌ها هیچ محدودیتی برای استفاده از داده‌ها نداشتند) هم وخیم‌تر خواهد شد.

سؤال ما این است که چرا کاربران اجازه می‌دهند چنین اتفاقی بیفتد؟ من به عنوان دانشمند علوم رفتاری، پژوهشی انجام داده‌ام تا ببینم چرا افراد در فضای مجازی بر خلاف میل‌شان عمل می‌کنند. نخستین دلیل آن، دروغین بودن «رضایت‌هایی» است که شرکت‌ها از کاربران‌شان می‌گیرند. طبق قانون، شرکت‌ها برای آنکه اجازه داشته باشند در اقتصاد نظارتی فعالیت کنند، باید از کاربران «رضایت آگاهانه» بگیرند. اما بیشتر کاربران از به اشتراک گذاری داده‌های شخصی‌شان اطلاعی ندارند یا اینکه نمی‌دانند به اشتراک گذاشتن آنها به چه قیمتی برایشان تمام می‌شود (یا حتی هر دو!) درست است که مشتریان منافع هم از به اشتراک گذاری این اطلاعات می‌برند (برای مثال تبلیغات متناسب با نیازشان را دریافت می‌کنند، خدمات مشتری بهتری می‌گیرند، قیمت گذاری محصولات متناسب با شرایط آنها صورت می‌گیرد و شاید حتی بتوانند محصولات را به صورت اعتباری خریداری کنند) اما شرکت‌ها باید بین مزایای کاربران و مراقبت از حریم خصوصی‌شان تعادل ایجاد کنند. مدافعان حقوق کاربران مدام درباره فعالیت‌های تجاوزگرایانه دیجیتال هشدار می‌دهند. هر فاجعه امنیتی که به تیت‌های خبری راه پیدا می‌کند، با خشم و اعتراض شدید مردم همراه می‌شود (مانند وقتی که شرکت اعتبارسنجی آکویفاکس اطلاعات شخصی

۱۰ میلیون نفر را گم کرد، یا زمانی که هکرهای روسی، رأی مردم آمریکا را تحت تأثیر قرار دادند). متخصصان حریم خصوصی اینترنت که تا مدت‌ها مورد توجه قرار نمی‌گرفتند، اکنون در کنگره آمریکا یا کنفرانس‌های خبری شهادت می‌دهند. در اروپا نیز قانونی را برای مراقبت از حریم خصوصی کاربر وضع کرده‌اند. همچنین، حس بی‌اعتمادی عمومی نسبت به شرکت‌های فناوری آنچنان زیاد شده که می‌تواند همه شرکت‌هایی را که از داده مشتریان استفاده می‌کنند، در معرض خطر قرار دهد. بی‌جهت نبود که وقتی فیس‌بوک اعلام کرد می‌خواهد جمع‌آوری داده را کاهش دهد، حدود ۲۰ درصد از ارزش شرکتش کاسته شد.

از طرفی دیگر، اگر شرکت‌ها حریم خصوصی کاربران را ارتقا بخشند، کاربران هیچ پاداشی در ازای این کار به آنها نمی‌پردازند. فناوری‌های ارتقای حریم خصوصی چندان مورد استقبال افراد قرار نگرفته است. مردم معمولاً حاضر نیستند برای فناوری‌های مرتبط با حریم خصوصی پول بدهند و اگر هم چنین کاری کنند، فقط مبالغ متوسط را می‌پردازند. شاید فکر کنید، پس حتماً افراد اهمیتی به حریم خصوصی‌شان نمی‌دهند، اما من طور دیگری استنتاج می‌کنم؛ افراد به حریم خصوصی‌شان اهمیت می‌دهند، اما برخی عوامل باعث شده نتوانند تصمیمات عاقلانه‌ای در این باره بگیرند.

اگر هر دو طرف (چه شرکت‌ها و چه مردم) به این مسیر پرخطر ادامه بدهند، اقتصاد نظارتی ممکن است سبب شکست بازار شود. خوشبختانه قانون‌گذاران می‌توانند از این روند جلوگیری کنند. اولین قدم این است که ببینیم افراد چطور درباره اطلاعات شخصی و حریم خصوصی‌شان تصمیم می‌گیرند و چطور فریب می‌خورند و بیش از حد اطلاعات‌شان را به اشتراک می‌گذارند.

مشتریان چطور به اینجا رسیدند؟

بگذارید رک بگویم؛ افراد در تصمیمات مربوط به داده‌های محرمانه‌شان بسیار بد عمل می‌کنند. آنها مزایا و معایب تصمیمات‌شان را درک نمی‌کنند. به علاوه، سوگیری ذاتی‌شان باعث می‌شود قضاوت‌های نادرستی انجام دهند. شرکت‌های پلتفرمی و

شرکت‌هایی که به جمع‌آوری اطلاعات می‌پردازند هم محصولات و خدمات خود را طوری سازمان‌دهی می‌کنند تا به شکلی ماهرانه از این سوگیری‌ها سوءاستفاده کنند. در ادامه، عواملی را بررسی می‌کنیم که باعث تصمیم‌گیری غلط در افراد می‌شود.

بی‌طاقتی

افراد معمولاً فقط جلوی چشم‌شان را می‌بینند. یعنی، به مزایا و خسارت‌های آنی بیشتر اهمیت می‌دهند تا مواردی که ممکن است در آینده برای‌شان اتفاق بیفتد. به بیان دیگر، اگر قرار باشد امروز ۹ دلار عایدشان شود و فردا ۱۰ دلار، آنها ۹ دلار امروز را انتخاب می‌کنند. در فضای اینترنتی، این تمایل باعث می‌شود اطلاعات شخصی‌شان را به خاطر موضوعات بسیار کم‌اهمیت در اختیار وب‌سایت‌ها قرار دهند. نظر سنجی‌ها و آزمون‌های رایگان یکی از بارزترین ابزارهای جمع‌آوری اطلاعات هستند. اشخاص ثالث این آزمون را تهیه می‌کنند تا بینش‌هایی درباره شخصیت کاربر به آنها بدهند، اما در عوض، اطلاعات مهمی را از آنها دریافت می‌کنند و امنیت داده‌های آنها را به خطر می‌اندازند. برای مثال، وب‌سایت معروف real age (سن واقعی) را در نظر بگیرید. هر روزه افراد زیادی به این وب‌سایت می‌روند و مقدار زیادی از اطلاعات حساس پزشکی‌شان را وارد می‌کنند تا ببینند «سن بیولوژیک‌شان» بیشتر از سن واقعی‌شان است یا کمتر. اما نمی‌دانند که این «مزیت آنی» ممکن است در طولانی‌مدت برای‌شان «هزینه‌هایی» داشته باشد (کسی چه می‌داند، شاید شرکت‌های بیمه با استفاده از این اطلاعات افراد بیمارتر را پیدا کنند و از عمد حق بیمه ماهیانه‌شان را افزایش دهند). اما چون این خسارت‌ها مبهم و مربوط به آینده هستند، مردم توجهی به آنها نمی‌کنند و آن چند دقیقه لذتی را که با این آزمون آنلاین می‌برند، ترجیح می‌دهند.

خصلت بی‌طاقتی در انسان‌ها، حتی باعث می‌شود بی‌خیال کنترل‌های امنیتی شوند. در یک آزمایش تحقیقاتی، به افرادی که کیف پول دیجیتالی داشتند گفته شد «می‌توانید با فعال کردن قابلیت جدید در اپلیکیشن، داده‌های تراکنش و خریدتان را رمزگذاری و ایمن کنید»، اما این قابلیت خودبه‌خود فعال نمی‌شد و باید برای اضافه کردن آن

چند مرحله کار انجام می‌دادند. همین موضوع باعث شد فقط یک چهارم کاربران این خدمات را نصب و فعال کنند. سایرین حاضر نبودند حتی یک بار به خودشان زحمت بدهند و به خاطر حفاظت از داده‌هایشان در برابر سوءاستفاده‌های آتی، آن فرایند چندمرحله‌ای را انجام بدهند.

«روش‌های جمع‌آوری داده» معمولاً طوری سازمان‌دهی می‌شوند که در صورت افشای اطلاعات‌تان؛ مزایای آتی، فریبنده و قابل مشاهده‌ای عایدتان می‌شود، ولی هزینه‌های ناشی از آن معمولاً بسیار مبهم است و با تأخیر، خودشان را نشان می‌دهند. در نتیجه، بی‌طاقتی ما باعث می‌شود به سمت مزایای آتی برویم و «ارائه اطلاعات» را انتخاب کنیم. مثلاً، اگر ارائه‌دهنده کارت اعتباری آدرس ایمیل‌تان را داشته باشد، می‌تواند صورت حساب‌های مالی را برایتان ارسال کند. به این صورت، شما بدون نیاز به کاغذبازی و خیلی سریع پرداخت‌هایتان را انجام می‌دهید. این برای شما نوعی مزیت آتی است؛ اما ارائه ایمیل و اطلاعات شخصی دیگر بعداً به ضررتان تمام می‌شود. شرکت‌ها این داده‌های حساس شما را (از جمله نام، جنسیت، درآمد، موقعیت مکانی و غیره) جمع‌آوری می‌کنند، با دیگران به اشتراک می‌گذارند یا می‌فروشند. سپس می‌توانند با استفاده از آن شما را قربانی بازاریابی هدفمند قرار دهند. شاید برخی از این تبلیغات برایتان مفید باشد، ولی اکثر آنها مزاحم و آزاردهنده هستند. بعضی‌ها عقیده دارند این داده‌ها در آینده برای اهداف مؤثرتری استفاده می‌شوند. مثلاً ممکن است به کمک آنها امتیاز اعتباری شما را محاسبه کرده و آن را در تصمیم‌گیری‌های مالی‌تان اعمال کنند. این مسئله بین افراد نابرابری ایجاد می‌کند و سبب می‌شود کسانی که هم‌اکنون در محرومیت مالی هستند، همیشه در حاشیه باقی بمانند (فرضیه «محدوده قرمز دیجیتال» یا همان digital redlining).

اثر برخورداری

از لحاظ نظری، همان‌قدر که برای فروش یک کالا پول دریافت می‌کنید، باید حاضر باشید برای خرید آن هم همان‌قدر پول بپردازید. اما در حقیقت، افراد هنگام خرید کالا، ارزش کمتری برای آن قائل‌اند، تا زمانی که بخواهند آن را بفروشند. در

تصمیمات مربوط به حریم خصوصی نیز دقیقاً همین اتفاق می‌افتد. «آلیناندرو آکویتی»، «جورج لوونستین» و من در یکی از مطالعات مان دو کارت هدیه «حریم خصوصی» به مشتریان پیشنهاد دادیم؛ اولی، یک کارت ۱۰ دلاری بود که اگر آن را انتخاب می‌کردند، خریدهایشان را پیگیری نمی‌کردیم و دومی یک کارت ۱۲ دلاری بود که در ازای انتخاب آن خریدهایشان را پیگیری می‌کردیم. تعدادی از سوژه‌های تحقیق، پیش از این کارت ۱۰ دلاری داشتند و اکنون می‌توانستند با پرداخت دو دلار دیگر حریم خصوصی محافظت‌شده‌تری داشته باشند. در واقع آنها می‌توانستند فقط با پرداخت دو دلار برای خودشان حریم خصوصی «بخرند». باقی افراد، قبلاً از کارت ۱۲ دلاری استفاده می‌کردند و الان می‌توانستند با حذف آن دو دلار اضافه، حریم خصوصی‌شان را «بفروشند». در هر دو صورت، قیمت حریم خصوصی دو دلار بود. پس اینکه افراد قبلاً از چه کارتی استفاده می‌کردند، نباید در تصمیم‌گیری‌شان تأثیری می‌گذاشت، اما تحقیقات ما نشان داد ۵۰ درصد افراد حاضر بودند به خاطر دو دلار بی‌خیال حریم خصوصی‌شان شوند و فقط ۱۰ درصد افراد حاضر شدند در ازای دو دلار حریم خصوصی بخرند.

این موضوع نشان می‌دهد زمانی که می‌خواهیم حریم خصوصی دریافت کنیم، ارزش کمتری برای آن قائلیم؛ تا زمانی که می‌خواهیم حریم خصوصی مان را رها کنیم. همچنین، اینکه از ابتدا اطلاعات مان علنی بوده یا محرمانه، در تصمیم‌گیری مان تأثیر بسزایی دارد؛ وقتی اطلاعات مان به صورت پیش فرض در دسترس باشند، راحت‌تر قبول می‌کنیم آن را به اشتراک بگذاریم. اما اگر اطلاعات مان از ابتدا محرمانه باشند، سخت‌تر حاضر می‌شویم آنها را در معرض نمایش بگذاریم. به همین خاطر است که وقتی نقضی در حریم خصوصی کاربران صورت می‌گیرد، به صورت جمعی دست به اعتراض می‌زنند. اما اگر حریم خصوصی‌شان را نسبت به قبل بیشتر کنیم، به همان اندازه از ما قدردانی نمی‌کنند. این موضوع حتی می‌تواند ما را وارد نوعی چرخه معیوب، به نام «فرسایش حریم خصوصی» کند. طبق این نظریه، هرچه تجاوزهای بیشتری به حریم خصوصی افراد صورت بگیرد و اطلاعات افراد علنی‌تر شود، افراد ارزش کمتری به حریم خصوصی خود می‌دهند. این مسئله باعث می‌شود راحت‌تر با آن کنار بیایند و از

حق حریم خصوصی شان بگذرند.

به همین خاطر، شرکت‌های فناوری محور به صورت پیش فرض حریم خصوصی ضعیفی برای کاربران در نظر می‌گیرند تا افراد راحت‌تر از حق خودشان بگذرند. این مثال‌ها را در نظر بگیرید: در نوامبر ۲۰۱۶، اوبر تنظیمات پیش فرض اپلیکیشن خود را طوری تغییر داد که لازم نباشد همیشه کاربران را پیگیری کند. پس اگر کسی می‌خواست از این قابلیت استفاده کند، باید وارد تنظیمات می‌شد و این گزینه را برای خودش فعال می‌کرد. همان‌طور که حدس می‌زنید، تعداد بسیار کمی از افراد این کار را انجام دادند و چون از ابتدا چنین حقی نداشتند، برای دریافت آن تلاشی نکردند (اوبر در سال ۲۰۱۷ بعد از مواجهه با انتقادات مردم این تنظیمات را به حالت اولیه خود بازگرداند). در اپلیکیشن پرداخت و نمو نیز تراکنش‌ها به صورت پیش فرض عمومی هستند. گوگل به محض آنکه اپلیکیشن گوگل مپ را باز می‌کنید، به صورت خودکار موقعیت مکانی شما را پیدا می‌کند. بیشتر این شرکت‌ها پلتفرم‌شان را طوری ساخته‌اند که حتی اگر بخواهید این تنظیمات را لغو کنید، فرایند آن ممکن است برایتان گیج‌کننده یا گمراه‌کننده باشد. توانایی کاربران برای لغو برخی ویژگی‌های اپلیکیشن‌ها اغلب مبهم است. سناتور مارک وارنر در یکی از مقالات اخیرش می‌گوید اپلیکیشن موبایلی فیس‌بوک با استفاده از تنظیمات پیش فرض خود کاربران را فریب می‌دهد تا با رضایت خودشان شماره تلفن‌های خود را به فیس‌بوک بدهند (داده‌هایی که برای فیس‌بوک بسیار سودآور است و به آن کمک می‌کند درک بهتری از کاربر داشته باشد). زمانی که وارد اپلیکیشن فیس‌بوک می‌شوید، در اولین صفحه از شما می‌خواهد گزینه «به اشتراک گذاری دفترچه تلفن همراه» را انتخاب کنید. این موضوع باعث می‌شود فکر کنید که این تنها انتخاب شماست. در صورتی که اگر گزینه «بیشتر» را بزنید، به پایین صفحه بروید و بادقت مطالب را بخوانید، متوجه می‌شوید که می‌توانید از این مرحله صرف‌نظر کنید و اطلاعات دفترچه تلفن خود را به فیس‌بوک ندهید.

توهم کنترل

افراد به غلط فکر می‌کنند می‌توانند فرایندهای اتفاقی را کنترل کنند. به همین خاطر

است که طبق تحقیقات، ترجیح می‌دهند خودشان بلیت‌های بخت‌آزمایی را انتخاب کنند، تا اینکه به صورت تصادفی این بلیت‌ها را دریافت کنند. همچنین، آنها نشانه‌های ساختگی کنترل را با خود کنترل اشتباه می‌گیرند. «تامی کیم»، «کیت باراز» و من در مطالعاتی که پیرامون «پذیرش تبلیغات هدف‌گذاری شده» انجام دادیم، متوجه شدیم که وقتی افراد حس کنند کنترل موضوعی را در دست دارند، راحت‌تر اطلاعات‌شان را با اشخاص ثالث به اشتراک می‌گذارند، حتی اگر آنچه تحت کنترل دارند، هیچ ارتباطی با حریم خصوصی، داده‌ها، یا تبلیغاتی که می‌بینند، نداشته باشد. پلتفرم‌ها می‌توانند با ارائه حق انتخاب درباره گزینه‌های کم‌اهمیت، به کاربران این احساس را منتقل کنند که همه چیز تحت کنترل آنهاست. مثلاً با ارسال یک پیام به آنها یادآوری می‌کنند که حق دارند عکس پروفایل‌شان را خودشان انتخاب کنند. همین مسائل پیش‌پاافتاده به آنها توهم کنترل می‌دهد. تحقیقات نشان داده، افراد درباره سطح کنترل‌شان در فضای سایبری بیش از حد مطمئن هستند. در نظرسنجی اخیر شرکت «اکسپریان»، ۵۶ درصد از شرکت‌کنندگان فکر می‌کردند احتمال دزدی هویت به مرور زمان کاهش می‌یابد و ۱۰ درصد عقیده داشتند چون پول چندانی ندارند، احتمال آنکه هویت‌شان دزدیده شود، بسیار کم است.

ارائه حدی از کنترل داده به کاربران مفید است، اما در بعضی موارد، داشتن «توهم کنترل» باعث می‌شود آنها مسائل حریم خصوصی‌شان را فراموش کنند. وب‌سایت «انصراف کاربران از پروژه تبلیغات شبکه» را در نظر بگیرید. در این سایت، می‌توانید وب‌سایت‌هایی را مشاهده کنید که تبلیغات شخصی‌سازی شده برایتان می‌فرستند. سپس از بین آنها، از وب‌سایت‌هایی که دوست ندارید انصراف بدهید. وقتی من از خدمات این پلتفرم استفاده کردم، تبلیغات ۷۲ شرکت را لغو کردم و این مسئله باعث شد احساس کنترل بیشتری داشتم باشم. اما وقتی جزئیات کار را خواندم، متوجه شدم که این کار فقط باعث عدم نمایش تبلیغات در مرورگر من می‌شود و الزاماً باعث نمی‌شود آن شرکت‌ها از ردیابی فعالیت‌ها و جمع‌آوری اطلاعات من دست بردارند. این موضوع حتی ضرر بیشتری به من می‌رساند؛ زیرا از آنجایی که دیگر تبلیغی از سمت این شرکت‌ها نمی‌دیدم، ممکن بود به طور کلی فراموش کنم که آنها در حال جمع‌آوری اطلاعات من هستند.

تمایل به افشاگری

این عامل جزء سوگیری‌های انتخاب به حساب نمی‌آید. انسان‌ها به صورت ذاتی تمایل یا حتی نیاز دارند که مسائل‌شان را با دیگران به اشتراک بگذارند. هرچه نباشد، ما ذاتاً موجودات اجتماعی هستیم و با همین به اشتراک گذاشتن روابطمان را شکل می‌دهیم. در یک پژوهش، حتی کسانی که خیلی نگران حریم خصوصی‌شان بودند، به خواست خودشان اطلاعات شخصی‌شان را برای یک چت‌بات برملا کردند. وقتی رازهایتان را برای کسی برملا می‌کنید، هم از لحاظ روانی و هم از لحاظ فیزیکی احساس بهتری پیدا می‌کنید. وقتی در یک آزمون آزمایشی چند فرد غریبه را داخل یک اتاق گذاشتند و از آنها خواستند در مورد مسائل شخصی‌شان با هم صحبت کنند، سازگاری آنها با یکدیگر بیشتر شد. طبق تحقیقات، داشتن یک دفتر خاطرات روزانه که نگرانی‌هایتان را در آن یادداشت کنید، می‌تواند سلامت بدن‌تان را افزایش دهد، در حالی که نگه داشتن راز ممکن است از سلامت روانی‌تان بکاهد. تحقیقی ثابت کرد وقتی افراد اطلاعاتی را درباره خودشان افشا می‌کنند، بخش‌هایی از سامانه پاداش مغزشان فعال می‌شود. تحقیق مشابهی نشان داد بعضی از افراد ترجیح می‌دهند بین جواب‌دادن به یک سؤال شخصی و دریافت پاداش مالی، اولی را انتخاب کنند.

میل به افشاگری حتی در ابعاد دیگر روابطمان نیز به خوبی مشخص است. بیشتر ما از کسانی که پنهان‌کاری می‌کنند، خوش‌مان نمی‌آید و نسبت به آنها دیدگاه بدی داریم. تحقیقات من به همراه «کیت باراز» و «مایک نورتون» نشان می‌دهد، وقتی کسی از جواب‌دادن به سؤالات شخصی طفره می‌رود، نسبت به او بی‌اعتماد یا بی‌علاقه می‌شویم؛ آن قدر که حتی اگر اطلاعات مخربی از خودش بدهد، این قدر به او احساس بدی پیدا نمی‌کنیم. در یک تحقیق آزمایشی، شرکت‌کنندگان گفتند که اگر متقاضی کار اعتراف کند قبلاً مواد مخدر مصرف کرده، احتمال آنکه او را استخدام کنند بیشتر است تا کسی که از پاسخ‌دادن به این سؤال طفره برود.

در دنیای آنلاین، مرزهای بین تراکش‌های تجاری و اجتماعی کم‌کم از بین رفته‌اند. برای مثال، تقریباً در همه شبکه‌های اجتماعی، پیام‌های تبلیغاتی درست شبیه به پست‌های معمولی هستند. شاید هدف از این همانندسازی این بوده که

تبلیغات کمتر حالت آزاردهنده داشته باشند. اما این کار باعث شده ما همان حسی را نسبت به تبلیغات پیدا کنیم که نسبت به پست‌های معمولی داریم. در نتیجه، احتمال به‌اشتراک‌گذاری اطلاعات در ما بیشتر و نگرانی‌مان نسبت به مشکلات حریم خصوصی کمتر می‌شود. همین‌طور، رابط‌های کاربری که ظاهر خودمانی و غیرتجاری دارند، ما را بیشتر ترغیب به خودافشایی می‌کنند، حتی اگر حریم خصوصی در آنها بسیار ضعیف باشد.

در واقع، افزایش میل به افشاگری مبنای کار شبکه‌های اجتماعی است. نوشته «در ذهنت چه می‌گذرد؟» که همیشه در بالای صفحه فیس‌بوک می‌بینید، به‌خوبی نمایانگر این موضوع است. دلیل آنکه خرده‌فروشان آنلاین به فرایند فروش‌شان عناصر اجتماعی (مانند چت‌بات‌ها) اضافه می‌کنند، دقیقاً همین است. آنها می‌خواهند با مشتریان هم‌پستگی بیشتری ایجاد کرده و میل به افشای آنان را افزایش دهند. ساختار وب‌سایت و نمودار را در نظر بگیرید. در این وب‌سایت، کاربران با افزودن شماره تماس‌های خود، یک نمودار اجتماعی ایجاد می‌کنند و می‌توانند تراکنش‌هایشان را با دوستان خود در قسمت فید نرم‌افزار ببینند. این موضوع باعث می‌شود تراکنش‌های مالی شما شبیه به تعاملات اجتماعی به نظر برسند. در نتیجه، مسائلی را که به‌صورت طبیعی از افشای آن امتناع می‌کنید، خیلی راحت بر ملا خواهید کرد. شما فقط نسبت به این کار احساس بدی ندارید؛ بلکه با کمال میل آن را انجام می‌دهید. جنبه‌های اجتماعی این نرم‌افزار برای کاربران فوایدی هم دارد، اما این جنبه‌ها موجب کم‌رنگ‌تر شدن خطرات افشاسازی اطلاعات می‌شود.

برداشت غلط از مرزها

در دنیای فیزیکی، افراد به‌صورت طبیعی هنجارهای اجتماعی مربوط به روابط میان‌فردی و رازداری را درک می‌کنند و خودشان را با آنها وفق می‌دهند. مثلاً، با آنکه وسوسه می‌شویم پشت سر کسی حرف بزنیم، به‌خاطر هنجار «غیبت ممنوع» تمایل‌مان را سرکوب می‌کنیم. بیشتر ما، وقتی دیگران نزدیک‌مان باشند، رازهایمان را به یکدیگر نمی‌گوییم؛ زیرا می‌ترسیم کسی اتفاقی آن را بشنود. همچنین وقتی از

هیچ ندیده‌ای هنوز

انتشارات **راه پرداخت**

برای سفارش اینترنتی این کتاب به وبسایت انتشارات راه پرداخت مراجعه کنید

way2pay.shop

► HBR's latest thinking on
the future of business

Insights You Need from

**Harvard
Business
Review**

CUSTOMER DATA + PRIVACY



انتشارات راهپروا