

SOSIALISASI KEAMANAN DATA PRIBADI: PONDASI DASAR PENGUNAAN KECERDASAN BUATAN (AI) YANG AMAN DI RUMAH GEMILANG INDONESIA

Dede Handayani^{1*}, Ahmad Nursodiq², Oke Hariansyah³, Daniel Siteja⁴

¹⁻⁴ Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang

*E-mail: dosen02411@unpam.ac.id

ABSTRAK

Kegiatan Pengabdian kepada Masyarakat (PkM) ini bertujuan untuk meningkatkan pemahaman dan keterampilan siswa-siswi dalam menjaga keamanan data pribadi di era digital, khususnya dalam penggunaan teknologi kecerdasan buatan (Artificial Intelligence/AI). Kegiatan dilaksanakan di Diklat Rumah Gemilang Indonesia Kota Depok dengan metode edukatif, interaktif, dan aplikatif yang meliputi ceramah, diskusi, studi kasus, serta simulasi praktik. Permasalahan utama yang dihadapi peserta adalah rendahnya literasi keamanan data, kurangnya pemahaman terhadap risiko penggunaan AI, serta kebiasaan berbagi data pribadi secara tidak bijak. Oleh karena itu, kegiatan ini difokuskan pada peningkatan kesadaran akan pentingnya privasi digital dan penggunaan teknologi secara aman dan bertanggung jawab. Hasil kegiatan menunjukkan adanya peningkatan pemahaman peserta yang signifikan, yang dibuktikan melalui perbandingan hasil pre-test dan post-test. Rata-rata persentase pemahaman peserta meningkat dari 30,13% sebelum kegiatan menjadi 84,62% setelah kegiatan. Selain itu, peserta juga mampu mengenali berbagai ancaman digital seperti phishing, pencurian identitas, dan kebocoran data, serta memiliki keterampilan dasar dalam melindungi data pribadi. Dengan demikian, kegiatan sosialisasi ini dinilai efektif dalam meningkatkan literasi digital, khususnya dalam aspek keamanan data pribadi. Diharapkan kegiatan ini dapat mendukung kesiapan peserta dalam menghadapi dunia kerja berbasis teknologi serta mendorong penggunaan AI yang aman, etis, dan bertanggung jawab.

Kata Kunci : keamanan data pribadi, kecerdasan buatan, literasi digital, privasi digital, pengabdian kepada masyarakat

ABSTRACT

This Community Service Program (PkM) aims to improve students' understanding and skills in protecting personal data security in the digital era, particularly in the use of Artificial Intelligence (AI) technology. The activity was conducted at the Rumah Gemilang Indonesia Training Center in Depok City using educational, interactive, and applicative methods, including lectures, discussions, case studies, and practical simulations. The main problems identified among participants were low data security literacy, limited awareness of risks in using AI, and the tendency to share personal data unwisely. Therefore, this program focused on increasing awareness of digital privacy and promoting safe and responsible use of technology. The results showed a significant improvement in participants' understanding, as evidenced by the comparison of pre-test and post-test results. The average level of understanding increased from 30.13% before the activity to 84.62% after the activity. In addition, participants were able to identify various digital threats such as phishing, identity theft, and data breaches, and gained basic skills in protecting personal data. In conclusion, this socialization activity proved to be effective in improving digital literacy, particularly in personal data security. It is expected that this program will support participants' readiness to face technology-based work environments and encourage the safe, ethical, and responsible use of AI.

Keywords : personal data security, artificial intelligence, digital literacy, digital privacy, community service

PENDAHULUAN

Akselerasi teknologi informasi di era kecerdasan buatan (Artificial Intelligence/AI) telah membawa perubahan signifikan dalam lanskap pendidikan dan pelatihan vokasi. Integrasi AI mampu mengoptimalkan proses belajar, personalisasi materi, serta meningkatkan efisiensi penyelesaian tugas secara adaptif (Hadnagy, 2018). Generasi muda masa kini yang tergolong sebagai digital natives sangat aktif memanfaatkan gawai dan berbagai platform digital untuk menunjang aktivitas belajar maupun interaksi sosial sehari-hari. Namun demikian, pesatnya adopsi teknologi ini memunculkan isu kritis terkait perlindungan privasi dan keamanan data pribadi. Sistem kecerdasan buatan bekerja dengan memproses, menganalisis, dan menyimpan kumpulan data dalam skala masif (Zuboff, 2019). Ketika interaksi tersebut tidak diimbangi dengan pemahaman keamanan informasi yang memadai, keterbukaan akses digital justru membuka celah kerentanan baru terhadap kejahatan siber, seperti kebocoran data (data breach), manipulasi audio-visual berbasis AI (deepfake), pencurian identitas, hingga penipuan rekayasa sosial (phishing) (Smith et al., 2017). Isu kerentanan keamanan siber tersebut teridentifikasi secara nyata di Diklat Rumah Gemilang Indonesia (RGI), Sawangan, Kota Depok (Prensky, 2010). Sebagai lembaga pelatihan kerja yang mempersiapkan generasi muda usia produktif memasuki dunia industri, RGI membekali para siswa dengan keterampilan berbasis komputer dan teknologi informasi. Berdasarkan analisis situasi awal yang dilakukan tim pengabdian bersama mitra, ditemukan beberapa permasalahan mendasar yang perlu segera diselesaikan (Floridi et al., 2018):

1. Rendahnya Literasi Keamanan Data: Sebagian besar siswa belum memahami bahwa instruksi atau perintah (prompt) yang dimasukkan ke platform AI kerap melibatkan pemrosesan data sensitif yang berpotensi terekam di peladen pihak ketiga (Luckin et al., 2016).
2. Kebiasaan Berbagi Data Berlebihan (Over-sharing): Peserta cenderung membagikan data identitas pribadi maupun berkas internal secara bebas tanpa mempertimbangkan risiko eksploitasi data digital.
3. Keterbatasan Keterampilan Teknis Proteksi: Peserta belum mengimplementasikan proteksi akun berlapis, seperti penggunaan kata sandi yang kuat dan aktivasi autentikasi dua faktor (Two-Factor Authentication/2FA).
4. Belum Adanya Edukasi Terstruktur: Kurikulum pelatihan kejuruan yang ada belum secara spesifik memuat modul keamanan digital dan etika pemanfaatan AI yang aman untuk lingkungan kerja.

Guna mengatasi rangkaian permasalahan tersebut, tim Pengabdian kepada Masyarakat (PkM) dari Program Studi Teknik Informatika Universitas Pamulang menyelenggarakan kegiatan bertajuk "Sosialisasi Keamanan Data Pribadi: Pondasi Dasar Penggunaan Kecerdasan Buatan (AI) yang Aman di Rumah Gemilang Indonesia". Solusi yang ditawarkan dirancang secara sistematis melalui metode ceramah edukatif, studi kasus riil penyalahgunaan data siber, serta simulasi praktik langsung mengenai pengaturan privasi akun, sanitasi data pada prompt AI, dan pengamanan kredensial digital.

METODE

Rencana pelaksanaan untuk mencapai tujuan kegiatan secara efektif, metode pelaksanaan sosialisasi dirancang dengan menggabungkan pendekatan edukatif, interaktif, dan praktis (Whitman & Mattord, 2019). Metode kegiatan yang digunakan adalah sebagai berikut:

1. Metode Ceramah (Penyampaian Materi)

Pemateri memaparkan konsep dasar keamanan informasi secara sistematis dan terstruktur dengan bantuan media presentasi (slide/proyektor) (Russell & Norvig, 2021). Materi yang disampaikan meliputi:

- a. Konsep dasar keamanan data pribadi dan privasi digital.
- b. Pengenalan teknologi Kecerdasan Buatan (Artificial Intelligence/AI).
- c. Risiko dan ancaman penggunaan AI terhadap kerahasiaan data.
- d. Cara dan etika menggunakan teknologi digital/AI secara aman dan bertanggung jawab.

2. Metode Diskusi Interaktif dan Tanya Jawab

Sesi dua arah antara narasumber dan peserta yang bertujuan untuk (Westin, 2015):

- a. Menggali pengalaman peserta dalam berinteraksi dengan platform digital dan AI (Stallings, 2018).
- b. Mengidentifikasi kendala atau potensi bahaya digital yang pernah dihadapi siswa. Memberikan ruang bagi peserta untuk menanyakan hal-hal yang belum dipahami seputar perlindungan identitas digital.

3. Metode Studi Kasus

Peserta diberikan contoh kasus nyata terkait kejahatan dan insiden siber untuk dianalisis bersama, seperti (Kaspersky, 2020):

- a. Rekayasa sosial (phishing) dan penipuan daring (online scam).
- b. Kasus kebocoran data (data breach).
- c. Ancaman manipulasi berbasis AI seperti deepfake dan pencurian identitas.

Peserta diajak mencari solusi dan langkah pencegahan yang tepat dari kasus-kasus tersebut (OECD, 2019).

4. Metode Simulasi / Praktik Langsung

Peserta tidak hanya menerima teori, tetapi langsung mempraktikkannya pada perangkat/gawai masing-masing, meliputi (World Economic Forum, 2020):

- a. Praktik membuat kata sandi (password) yang kuat dan aman.
- b. Pengaturan privasi dan keamanan akun media sosial.
- c. Aktivasi autentikasi dua faktor (Two-Factor Authentication / 2FA).
- d. Simulasi penggunaan aplikasi AI generatif tanpa membagikan data sensitif (sanitasi prompt).
- e. Mengenali ciri-ciri platform atau aplikasi AI yang aman.

5. Metode Evaluasi

Metode untuk mengukur efektivitas dan keberhasilan kegiatan sosialisasi melalui (Solove, 2021):

- a. Pre-Test: Diberikan sebelum penyampaian materi untuk mengukur

pemahaman awal peserta.

- b. Post-Test: Diberikan setelah pelatihan dan praktik selesai menggunakan 6 indikator soal yang sama untuk mengukur peningkatan pemahaman.
- c. Observasi Langsung: Pengamatan tim pelaksana terhadap keaktifan, antusiasme, dan kemampuan peserta selama praktik.
- d. Umpan Balik (Feedback): Kuesioner tanggapan peserta terhadap pelaksanaan kegiatan (Nissenbaum, 2019).

HASIL DAN PEMBAHASAN

Dalam kegiatan Pengabdian kepada Masyarakat ini kami mendapatkan hasil positif dengan melihat pemahaman siswa-siswi yang di buktikan dengan poin dari hasil dari survey yang kami lakukan (pre-Test dan Post-Test). Berikut beberapa pertanyaan dalam survey yang kami sebarakan pada peserta sebanyak 26 (dua puluh enam) peserta yang hadir sebagai berikut:

1. Apa yang dimaksud dengan "Digital Twin" atau aset digital kita?
2. Apa yang dimaksud dengan ancaman "Deepfake" yang menggunakan teknologi AI?
3. Semakin banyak data yang kita berikan kepada sistem AI, maka..
4. Mengapa kita harus melakukan verifikasi hasil (cross-check) terhadap informasi yang diberikan oleh AI?
5. Apa yang TIDAK BOLEH dimasukkan saat memberikan perintah (prompt) ke aplikasi AI?
6. Apa kegunaan utama dari mengaktifkan Two-Factor Authentication (2FA) pada akun digital kita?

Dari pertanyaan-pertanyaan tersebut kami sudah menyertakan pilihan-pilihan jawaban untuk menggambarkan sejauh apa pemahaman peserta terhadap Keamanan Data Pribadi: Pondasi Dasar Penggunaan Kecerdasan Buatan (AI). Dari hasil survey yang dilakukan maka hasil antara sebelum pelaksanaan dan sesudah pelaksanaan didapat hasil sebagai berikut.

Pertanyaan ke-1

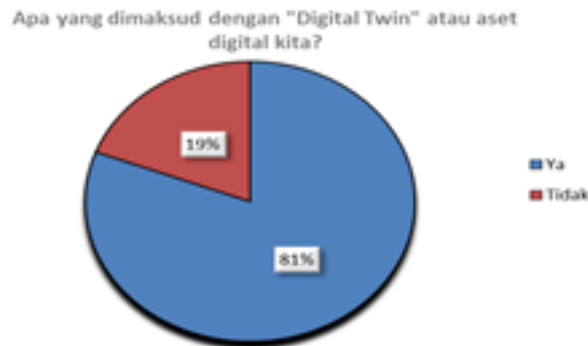
Sebelum Penyampaian Materi



Hasil Pre-Test Peserta PkM Pertanyaan 1

Dari pertanyaan yang diberikan sebelum penyampaian materi (Pre-test), hasil yang di dapatkan dari 26 peserta mayoritas belum mengetahui **Apa yang dimaksud dengan "Digital Twin" atau aset digital kita?** dengan presentase 38% menjawab “Ya” dan 62% menjawab “Tidak”.

Sesudah Penyampaian Materi



Hasil Post-Test Peserta PkM Pertanyaan 1

Dari pertanyaan yang diberikan setelah penyampaian materi (Post-test), kita bisa lihat ada peningkatan secara signifikan dimana persentase yang mengetahui **Apa yang dimaksud dengan "Digital Twin" atau aset digital kita?** adalah meningkat menjadi 81% menjawab “Ya”, dan 19% menjawab “Tidak”.

Pertanyaan ke- 2

Sebelum Penyampaian Materi

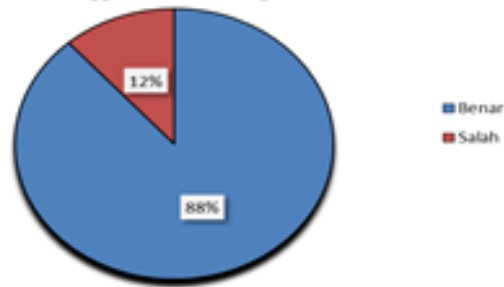


Hasil Pre-Test Peserta PkM Pertanyaan 2

Dari pertanyaan yang diberikan sebelum penyampaian materi (Pre-test), hasil yang di dapatkan dari 26 peserta mayoritas tidak mengetahui **Apa yang dimaksud dengan ancaman "Deepfake" yang menggunakan teknologi AI?** itu dengan presentase 23% menjawab “Benar” dan 77% menjawab “Salah”.

Sesudah Penyampaian Materi

Apa yang dimaksud dengan ancaman "Deepfake" yang menggunakan teknologi AI?

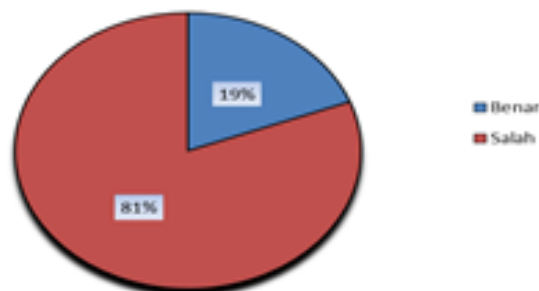


Hasil Post-Test Peserta PkM Pertanyaan 2

Dari pertanyaan yang diberikan setelah penyampaian materi (Post-test), kita bisa lihat ada peningkatan secara signifikan dimana persentase yang mengetahui **Apa yang dimaksud dengan ancaman "Deepfake" yang menggunakan teknologi AI?** itu meningkat menjadi 88% menjawab "Benar", dan 12% menjawab "Salah".

Pertanyaan ke- 3 Sebelum Penyampaian Materi

Semakin banyak data yang kita berikan kepada sistem AI, maka...

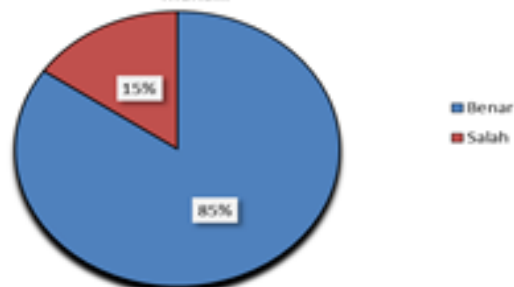


Hasil Pre-Test Peserta PkM Pertanyaan 3

Dari pertanyaan yang diberikan sebelum penyampaian materi (Pre-test), hasil yang di dapatkan dari 26 peserta sebagian belum mengetahui **Semakin banyak data yang kita berikan kepada sistem AI, maka...** dengan presentase 19% menjawab "Benar" dan 81% menjawab "Salah".

Sesudah Penyampaian Materi

Semakin banyak data yang kita berikan kepada sistem AI, maka...



Hasil Post-Test Peserta PkM Pertanyaan 3

Dari pertanyaan yang diberikan setelah penyampaian materi (Post-test), kita bisa lihat ada peningkatan secara signifikan dimana persentase yang mengetahui **Semakin banyak data yang kita berikan kepada sistem AI, maka...** meningkat menjadi 85% menjawab “Benar”, dan 15% menjawab “Salah”.

Pertanyaan ke- 4 Sebelum Penyampaian Materi



Hasil Pre-Test Peserta PkM Pertanyaan 4

Dari pertanyaan yang diberikan sebelum penyampaian materi (Pre-test), hasil yang di dapatkan dari 26 peserta sebagian belum mengetahui **Mengapa kita harus melakukan verifikasi hasil (cross-check) terhadap informasi yang diberikan oleh AI?** dengan presentase 35% menjawab “Benar” dan 65% menjawab “Salah”.

Sesudah Penyampaian Materi



Hasil Post-Test Peserta PkM Pertanyaan 4

Dari pertanyaan yang diberikan setelah penyampaian materi (Post-test), kita bisa lihat ada peningkatan secara signifikan dimana persentase yang mengetahui **Mengapa kita harus melakukan verifikasi hasil (cross-check) terhadap informasi yang diberikan oleh AI?** meningkat menjadi 88% menjawab “Benar”, dan 12% menjawab “Salah”.

Pertanyaan ke- 5 Sebelum Penyampaian Materi



Hasil Pre-Test Peserta PkM Pertanyaan 5

Dari pertanyaan yang diberikan sebelum penyampaian materi (Pre-test), hasil yang di dapatkan dari 26 peserta sebagian belum mengetahui **Apa yang TIDAK BOLEH dimasukkan saat memberikan perintah (prompt) ke aplikasi AI?** dengan presentase 38% menjawab “Benar” dan 62% menjawab “Salah”.

Sesudah Penyampaian Materi



Hasil Post-Test Peserta PkM Pertanyaan 5

Dari pertanyaan yang diberikan setelah penyampaian materi (Post-test), kita bisa lihat ada peningkatan secara signifikan dimana persentase yang mengetahui **Apa yang TIDAK BOLEH dimasukkan saat memberikan perintah (prompt) ke aplikasi AI?** meningkat menjadi 81% menjawab “Benar”, dan 19% menjawab “Salah”.

Pertanyaan ke- 6

Sebelum Penyampaian Materi



Hasil Pre-Test Peserta PkM Pertanyaan 6

Dari pertanyaan yang diberikan sebelum penyampaian materi (Pre-test), hasil yang di dapatkan dari 26 peserta sebagian belum mengetahui **Apa kegunaan utama dari mengaktifkan Two-Factor Authentication (2FA) pada akun digital kita?** dengan presentase 27% menjawab “Benar” dan 73% menjawab “Salah”.

Sesudah Penyampaian Materi



Hasil Post-Test Peserta PkM Pertanyaan 6

Dari pertanyaan yang diberikan setelah penyampaian materi (Post-test), kita bisa lihat ada peningkatan secara signifikan dimana persentase yang mengetahui **Apa kegunaan utama dari mengaktifkan Two-Factor Authentication (2FA) pada akun digital kita?** meningkat menjadi 85% menjawab “Benar”, dan 15% menjawab “Salah”.

Dari hasil diatas menunjukkan bahwa dengan pelaksanaan PkM ini Siswa-siswi Diklat Rumah Gemilang Indonesia Kota Depok masih banyak yang belum mengetahui Keamanan Data Pribadi: Pondasi Dasar Penggunaan Kecerdasan Buatan (AI) sebelum diadakannya pelaksanaan PkM ini, namun setelah kegiatan PkM ini dilaksanakan Siswa-siswi Diklat Rumah Gemilang Indonesia Kota Depok kini memiliki peningkatan dari sisi keilmuan dan wawasan di bidang teknologi tentunya untuk dapat mempercepat Transformasi Digital di dunia Pendidikan. Hal ini dibuktikan dengan hasil survey yang kita lakukan sebelum pelaksanaan (pre-test) sosialisasi pemahaman siswa-siswi yang diikuti sebanyak 26 peserta, namun setelah diadakannya pelatihan peserta mengisi kembali soal post-test yang diikuti sebanyak 26 peserta dimana hasil survey dengan mengajukan beberapa pertanyaan dengan rata-rata peningkatan nilai yang dihasilkan untuk ketepatan jawaban adalah sebagai berikut:

Hasil Post test & Pre test

Jenis Pertanyaan	Persentase jawaban benar sebelum sosialisasi	Persentase jawaban benar sesudah sosialisasi
Pertanyaan 1	38%	81%
Pertanyaan 2	23%	88%
Pertanyaan 3	19%	85%
Pertanyaan 4	35%	88%

Pertanyaan 5	38%	81%
Pertanyaan 6	27%	85%
Rata-Rata Persentase	30.13%	84.62%

Tentunya dengan pembekalan keilmuan dan wawasan ini, diharapkan lulusan Siswa-siswi Diklat Rumah Gemilang Indonesia Kota Depok dapat lebih siap menempuh pendidikan untuk mendukung kemajuan pendidikan dalam bidang Teknologi Informasi

KESIMPULAN

Berdasarkan hasil pelaksanaan kegiatan Pengabdian kepada Masyarakat (PkM) yang telah dilakukan di Diklat Rumah Gemilang Indonesia Kota Depok dengan tema “Sosialisasi Keamanan Data Pribadi: Pondasi Dasar Penggunaan Kecerdasan Buatan (AI) yang Aman”, dapat disimpulkan bahwa:

1. Kegiatan sosialisasi dan pelatihan ini berjalan dengan baik dan mendapatkan respon yang positif dari peserta. Hal ini terlihat dari antusiasme peserta selama mengikuti kegiatan, baik dalam sesi penyampaian materi, diskusi, maupun praktik.
2. Terjadi peningkatan pemahaman peserta yang signifikan terkait keamanan data pribadi dan penggunaan AI secara aman. Hal ini dibuktikan dengan hasil pre-test dan post-test yang menunjukkan peningkatan rata-rata dari 30,13% menjadi 84,62%.
3. Peserta mulai memahami berbagai risiko dalam penggunaan teknologi digital dan AI, seperti kebocoran data, phishing, pencurian identitas, serta pentingnya menjaga privasi digital.
4. Peserta juga memperoleh keterampilan dasar dalam menjaga keamanan data pribadi, seperti membuat password yang kuat, mengaktifkan Two-Factor Authentication (2FA), serta lebih bijak dalam membagikan informasi di platform digital.
5. Kegiatan ini berkontribusi dalam meningkatkan literasi digital peserta, khususnya dalam aspek keamanan data, sehingga dapat mendukung kesiapan mereka dalam menghadapi dunia kerja berbasis teknologi.

DAFTAR PUSTAKA

(Model Sitasi APA)

- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., & Vayena, E. (2018). {AI4People}---{A}n ethical framework for a good {AI} society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707.
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Wiley.
- Kaspersky. (2020). *Cybersecurity Report*.
- Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). *Intelligence Unleashed: An Argument for {AI} in Education*. Pearson.

- Nissenbaum, H. (2019). *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2nd ed.). Stanford University Press.
- OECD. (2019). *{OECD} Digital Economy Outlook 2019*. OECD Publishing.
- Prensky, M. (2010). *Teaching Digital Natives: Partnering for Real Learning*. Corwin Press.
- Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
- Smith, A., Jones, M., & Anderson, K. (2017). Identity theft and fraud in the digital age. *Journal of Cybersecurity*, 5(2), 45–60.
- Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.
- Stallings, W. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson.
- Westin, A. F. (2015). *Privacy and Freedom*. IG Publishing.
- Whitman, M. E., & Mattord, H. J. (2019). *Principles of Information Security* (6th ed.). Cengage Learning.
- World Economic Forum. (2020). *The Future of Jobs Report 2020*.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.