EL TESTIMONIO DE UN INSIDER

LA FALTA DE ÉTICA EN LAS GRANDES EMPRESAS TECNOLÓGICAS

El testimonio de un insider que se opone a **la guerra que Silicon Valley ha desatado contra la humanidad**, y la lucha para hacerles pagar.

VAHID RAZAVI

Introducción por **Norman Solomon**

EDITORAS Abril Menanteau · Romina Díaz

NoEthicsInBigTech.com | ForeverPeaceNow.com | ParentsPlea.com | ConflictTour.com

Basado en parte en el documental *Forever Peace Now*.

Investigación editorial y edición estructural con la ayuda de Claude (Anthropic). Las opiniones, argumentos, testimonios y conclusiones son exclusivamente del autor.

ÍNDICE

Prólogo

No hace falta saber mucho de tecnología digital, ni del mundo de las finanzas multimillonarias, para comprender lo más importante de este libro. *No Ethics in Big Tech* («La falta de ética en las grandes empresas tecnológicas») es una profunda declaración moral, sumamente relevante para todos los habitantes del planeta Tierra.

Vahid Razavi ha excavado muy por debajo del atractivo superficial, de la inmensa riqueza y del poder de estas empresas, para explorar el terreno subyacente de decisiones cruciales. Nos lleva a través de un sombrío recorrido por la realidad de Silicon Valley y su implicación en el sufrimiento infligido en lugares lejanos. Empresas que ganan billones de dólares gracias a su colusión directa con las guerras de agresión.

La falta de rendición de cuentas y la necesidad de la misma son temas centrales de *No Ethics in Big Tech*. Este libro explica por qué las ideas de una reforma desde dentro de la industria tecnológica y las esperanzas de una autocorrección son ilusorias. Como antiguo miembro del sector, Razavi se apoya en un conocimiento doloroso: la obsesión por la cuota de mercado y la maximización de los beneficios funciona como lo contrario de cualquier brújula moral. El Estado belicista está completamente integrado con las grandes tecnológicas.

«El complejo militar-industrial del siglo XXI no lo forman solo Lockheed Martin, Raytheon y Boeing», escribe. «Lo forman Amazon, Google, Microsoft, Oracle y Palantir. Las armas son la computación en la nube, la inteligencia artificial, los algoritmos de selección de objetivos, las bases de datos biométricas y la infraestructura de vigilancia. La munición son los datos».

Las bombas y las balas que han hecho posible el genocidio en Gaza, en gran medida por cortesía de los contribuyentes estadounidenses, son solo un factor de la actual alianza entre Estados Unidos e Israel. «Lo que el mundo llama genocidio, el complejo militar-industrial lo llama ciclo de ingresos», escribe Razavi. «Lo que Raytheon llama crecimiento de la cartera de pedidos, yo lo llamo los escombros de los hospitales del norte de Gaza. Lo que Boeing Defense llama expansión de su cuota de mercado, yo lo llamo las ruinas de universidades que no volverán a abrir».

Negar el genocidio no cambia su realidad. Y los hechos demuestran con espantosa claridad que muchas de las corporaciones tecnológicas más grandes y respetadas de Estados Unidos han sido parte integral del genocidio infligido al pueblo palestino. Human Rights Watch y Amnistía Internacional, así como las organizaciones israelíes de derechos humanos B'Tselem y Médicos por los Derechos Humanos-Israel, concluyeron de forma inequívoca que Israel ha cometido genocidio en Gaza.

Irónica, aunque previsiblemente, la industria tecnológica digital, que depende de las matemáticas verificables, se niega sin más a reconocer los hechos básicos de los crímenes contra la humanidad que con tanto afán —y con beneficios que superan toda imaginación— contribuye a cometer y que facilita.

Como señala Razavi: «Esto no es una hipérbole. Es aritmética. Las bombas caen sobre edificios civiles. Son fabricadas por empresas estadounidenses, compradas con el dinero de los contribuyentes estadounidenses, lanzadas por aviones suministrados por Estados Unidos y guiadas por sistemas de selección de objetivos de IA construidos por empresas tecnológicas estadounidenses. Toda la cadena de suministro, desde la granja de servidores hasta el cráter, pasa por corporaciones estadounidenses y por contratos del gobierno estadounidense. Y los ejecutivos que dirigen esas corporaciones reciben una remuneración, ya sea en forma de salario, bonificaciones u opciones sobre acciones, según cuánto controlan dentro de la cadena de suministro».

Por eso el autor no hace más que constatar los hechos cuando escribe: «Sin Amazon Web Services, la infraestructura de inteligencia del ejército israelí no funcionaría a su escala actual. Sin las plataformas de fusión de datos de Palantir, los sistemas de selección de objetivos Gospel y Lavender no contarían con la visión operativa necesaria para generar un centenar de objetivos de bombardeo al día. Sin la infraestructura en la nube de Microsoft, los datos de vigilancia no podrían procesarse a la escala requerida».

La complicidad corporativa que se describe en este libro es una realidad constante que se agrava día tras día. El apetito enormemente destructivo de beneficios cada vez mayores es insaciable. Es una característica del sistema, no una falla.

«La complicidad corporativa en la violencia de Estado no es un accidente del capitalismo», observa Razavi, una afirmación basada no en teorías, sino en su experiencia de primera mano al presenciar de cerca dicha complicidad. «Es una de las características más fiables del capitalismo. Lo único que la ha interrumpido alguna vez es la rendición de cuentas. Rendición de cuentas legal, personal, financiera y penal».

Este libro es un llamamiento a la rendición de cuentas.

Norman Solomon Junio de 2026

Norman Solomon es periodista, crítico de medios, activista progresista y excandidato al Congreso de Estados Unidos. Solomon es colaborador de larga trayectoria del grupo de vigilancia mediática Fairness & Accuracy In Reporting (FAIR). En 1997 fundó el Institute for Public Accuracy, que trabaja para ofrecer fuentes alternativas a los periodistas, y actualmente ejerce como su director ejecutivo. Es cofundador de RootsAction.org.

Nota del autor sobre la misión y la independencia financiera

Antes de que leas una sola palabra del argumento de este libro, quiero abordar algo directamente: ¿quién financia este trabajo y qué gano yo personalmente con ello? La respuesta es: nada. No obtengo ningún beneficio económico de todo esto. Este libro, mi libro anterior *Ethics in Tech and Lack Thereof* y mi documental *Forever Peace Now* se han producido con mis propios fondos personales. Sin patrocinadores corporativos. Sin subvenciones gubernamentales. Sin el respaldo de fundaciones sin fines de lucro. Sin anticipo editorial. Sin modelo publicitario. Sin recibir honorarios por hacer conferencias. Cada dólar gastado en investigación, producción, alojamiento, páginas webs, trámites legales y mantenimiento de la plataforma ha procedido de una única fuente: mi propio bolsillo. He realizado este trabajo con pérdidas económicas personales, deliberadamente, a lo largo de varios años. No digo esto para suscitar admiración, sino para trazar una línea clara. Las organizaciones y plataformas creadas junto con este libro se basan en el mismo modelo. ConflictTour se encuentra actualmente en la fase de idea y planificación. No está constituida como sociedad, no tiene ingresos, no tiene inversores y no opera con un modelo comercial. Si algún día genera ingresos suficientes para pagar a las personas que realizan el trabajo un salario digno, esa será su medida de éxito: no el beneficio, sino la sostenibilidad. Nunca será una fuente de ingresos. ParentsPlea.com es un sitio web gratuito. No contiene publicidad. No obtiene ingresos por afiliación. No vende, ni comercializa, ni monetariza los datos de las familias que le confían las historias de sus difuntos. Se ha creado y se mantiene por una razón que no tiene nada que ver con el dinero: sino porque la paz justa nos exige examinar las muertes que han tenido lugar. Quién está matando. Quién está sufriendo. Porque si algún día va a haber un juicio en un tribunal, si algún día van a haber reparaciones para las personas perjudicadas por estas guerras, si algún día va a haber un memorial digno de ese nombre, entonces necesitamos algo más que un muro de nombres. Necesitamos biografías. Necesitamos testimonios de las familias. Necesitamos un registro completo de aquellos que hemos perdido y qué es lo que las familias supervivientes quieren que el mundo sepa. Eso es lo que ParentsPlea está construyendo. Un perfil tras otro. Mi trabajo no recibe patrocinadores corporativos, como suelen hacer nuestros políticos y varias ONGs y organizaciones afiliadas al gobierno. No hay ningún mecenas multimillonario. No hay ninguna fundación que lo financie. Y esto, sin embargo, en vez de ser una limitación, esta independencia, es justamente lo que quiero. Normalmente, este tipo de trabajo es financiado por los mismos hombres a los que estoy pidiendo que rindan cuentas. Es precisamente por eso que este trabajo no puede ser financiado por ellos; y no lo está. No estoy aquí para defender al indefendible sector tecnológico. Ya tienen suficientes agencias de relaciones públicas y ejecutivos a los que se paga generosamente para defender su inhumanidad. Pueden escribir y publicar sus propios libros. No me interesa su aprobación, su apoyo, ni su respuesta. La verdadera lucha a la que se enfrenta la humanidad, más allá de toda la política, de las armas, de las estructuras corporativas y de los algoritmos, es entre dos ideas contrapuestas: «Yo soy uno» y «Nosotros somos uno». Silicon

Valley ha erigido un monumento a la primera idea. Este libro es un argumento a favor de la segunda. Es por eso que lo escribo. Esa es la única y principal razón.

Acerca del autor

Hay un tipo específico de conocimiento que proviene de haber sobrevivido a una guerra de niño, y otro diferente que proviene de haber pasado treinta años dentro de la industria que ahora construye las máquinas con las que se combate. Yo tengo ambos. Y quiero que entiendas cómo se conectan, porque este libro no podría haber sido escrito sin lo uno o lo otro. Nací en Teherán, Irán, en 1975. Cinco años después, Irán vivió su Revolución Islámica. En septiembre de 1980, Irak atacó Irán bajo el mando de Sadam Husein, y fui testigo de una guerra de primera mano. No en una pantalla. No como una estadística. Tenía solo cinco años. Mi madre era enfermera. Trabajaba en hospitales atendiendo a las víctimas de esa guerra: a los heridos, a los traumatizados, a las personas cuyas vidas la máquina había destrozado. Los viernes, mi día libre del colegio, los pasaba a su lado, viendo a refugiados y a gente que se cobijaba en los pasillos del hospital. Veía a niños de mi edad con lesiones que yo mismo era demasiado joven para nombrar. Madres buscando a sus hijos. Hombres que habían entrado en ese hospital con un cuerpo y salían con otro. Mi padre era ingeniero. Éramos una familia de clase media en Teherán, pero ser de clase media en una ciudad en guerra significa ver largas colas de gente esperando comida, estar en calles inseguras, bajo un cielo que a veces se iluminaba a distancias imposibles de medir y que tu cuerpo entiende, antes de que tu mente, que lo que arde está lo suficientemente cerca como para preocuparte. La guerra duró ocho años. En 1986, cuando tenía once años, mi familia tomó la decisión que toda familia atrapada en una guerra debe plantearse tarde o temprano: ¿cómo protegemos a los niños? Mi madre y yo vinimos a Estados Unidos con un visado. Salimos de Irán para escapar de la guerra con Irak: la misma guerra que el gobierno de Estados Unidos facilitó entregando armas a Saddam Hussein para que la llevara a cabo. Llegué a California sin saber casi nada de inglés. Me matriculé en clases de inglés como segunda lengua (ESL). Era un niño iraní en el Área de la Bahía en los años en que la palabra «iraní» era un insulto, cuando la crisis de los rehenes nos había definido en la cultura estadounidense como enemigos, cuando un niño tenía que aprender no sólo un nuevo idioma, sino también crearse una nueva identidad lo suficientemente segura como para caminar por los pasillos de la escuela. Crecí durante mi educación primaria y secundaria cargando con ese peso. Nos acosaban. Había mucha discriminación. No sabía qué estaba pasando. No entendía la diferencia entre Arabia Saudita, los distintos países árabes, e Irán. Nadie hacía esa distinción. La gente me llamaba terrorista. No entendía por qué. Yo no era un terrorista. Mi familia no era terrorista. Habíamos huido de una guerra. Y aquí, en el país que nos acogió, un miedo diferente había decidido que el lugar de donde veníamos definía quiénes éramos. Así es que cuando entré a la universidad a los 16 años, centré todos mis esfuerzos en comprender mi propia identidad. ¿Quién soy? Fundé el Club Persa en la universidad. Al final, mi respuesta fue: soy iraní estadounidense. Estados Unidos es un crisol de culturas. Estados Unidos defiende ciertos valores: no la nacionalidad, ni el lugar de donde proceden tus padres, sino un sistema de valores que todos nosotros, como ciudadanos, intentamos encarnar. Lamentablemente, ese ideal no siempre se respeta. Quiero contarles cuál fue realmente mi trayectoria profesional, porque los críticos se

preguntarán si estoy cualificado para decir lo que digo. Empecé vendiendo ordenadores. Al por menor. Luego, productos de Apple. Después vendí hardware de redes para Bay Networks. Cuando tenía veintiún o veintidós años, ganaba cerca de un cuarto de millón de dólares al año trabajando en el sector tecnológico. Quiero decirlo claramente, porque la gente da por sentado que quienes critican a Silicon Valley desde dentro son personas a las que no se les daban bien las cosas, personas que no podían competir, personas amargadas por el fracaso. A mí no se me daba mal. Se me daba muy bien. Las recompensas económicas eran reales. La energía de crear cosas era real. La camaradería de trabajar en equipo hasta altas horas de la noche en algo importante era la parte más gratificante de todo ello. Pasé por el departamento de ventas de centros de datos y coubicación en Exodus Communications y AboveNet, dos de las empresas que construyeron la columna vertebral de los inicios de la Internet comercial. Vendía servicios gestionados. Me involucré con startups y me enamoré de su velocidad, de la sensación de construir algo desde la nada, de la sensación de que estabas creando un cambio. Yo era, en palabras de un antiguo cofundador de Exodus, que lo dijo con auténtica calidez, el mejor vendedor que habían tenido nunca. Mi antiguo jefe, en esa misma reunión, me recordó que cuando cerré un acuerdo en particular, había incluido en el contrato la garantía de un barril de cerveza para el cliente cada mes que estuviera con Exodus. No recuerdo haberlo hecho pero a él le pareció muy gracioso. A mí también. Así era crear cosas en los inicios de la era tecnológica: absurdo, enérgico y lleno de gente que creía que estábamos haciendo un mundo mejor y más rápido. Luego creé WarrantyNow.com. Recaudé capital, más de veinticinco millones de dólares, de personas cuyos nombres reconocerías: Halsey Minor, el fundador de CNET; Marc Benioff, quien convirtió a Salesforce en una de las plataformas de software empresarial más poderosas del mundo; Michael Dell; ejecutivo de PeopleSoft. Me senté frente a inversores serios y a grandes fondos institucionales, y me mantuve firme. Sabía cómo funcionaba ese mundo, qué cosas se valoraba y qué se descartaba. Posteriormente llegó BizCloud. En 2008 fui a Belgrado, Serbia, para crear una empresa de computación en la nube desde cero. Formamos un verdadero equipo. Produjimos más de cinco mil quinientos artículos y vídeos sobre el sector de la computación en la nube. Nos convertimos en un agente de la nube, una presencia significativa en el sector. Y fue entonces que Computer Sciences Corporation, una empresa tecnológica de la vieja escuela, con miles de millones de dólares en contratos gubernamentales y un historial de trabajo para el complejo militar y de inteligencia, una industria que yo aún no comprendía del todo, se apropió del nombre de mi empresa para su propia línea de productos. Me enteré el 2010. Me demandaron el 2013 por utilizar mi propia marca registrada. Mis abogados, ante la realidad financiera, me convencieron de que mediara y llegara a un acuerdo. Perdí, ya que tuve que compartir nuestro buen nombre con CSC. Y lo que siguió a la derrota no fue un revés empresarial en el sentido habitual. La presión de esa lucha, sumada a todo lo que me había costado, junto con la quiebra que declaré desde mi cama de hospital, rompió algo en mí. Tomé una decisión de la que he hablado públicamente, en mi película y en mi primer libro, porque creo que es importante que la gente entienda lo que esta industria puede hacerle a quienes están dentro de ella cuando la maquinaria se vuelve en tu contra. Tras el acuerdo, tomé una decisión que casi acabó con mi vida. Sobreviví porque el Hospital Universitario de Stanford, el San Francisco General y el Laguna Honda me proporcionaron cuatro meses y medio de la mejor atención que podría haber pedido. Salí con un bastón. Como

dije en aquel momento, con el humor negro que es la única forma de sobrevivir a algo así: como un Humpty Dumpty, con todos los caballos del rey y todos los hombres del rey. Cuando salí, dije: muy bien. Si voy a seguir adelante, iré a la empresa de nube más grande y poderosa del mundo y la entenderé desde dentro. Me incorporé a Amazon Web Services como director sénior de alianzas en Big Data y analítica. Asistí a reuniones con Andy Jassy, quien más tarde se convertiría en director ejecutivo de la propia Amazon. Redacté informes ejecutivos para la alta dirección de Amazon. Gestioné colaboraciones de marketing conjunto por varios millones de dólares con Splunk, Sumo Logic, Tableau y Qlik, algunos de los nombres más importantes del ecosistema de analítica de datos empresariales. Yo estaba en el lado comercial. No me ocupaba de los contratos gubernamentales. Pero observé la maquinaria de cerca, y lo que vi en las oficinas de Amazon Web Services confirmó todo lo que el New York Times ya había descrito y todo lo que mi cuerpo ya había aprendido en BizCloud: que estas empresas tratan a los seres humanos como insumos y que, cuando el insumo ya no es necesario, se deshacen de él. No disfruté del tiempo que pasé trabajando en Amazon Web Services. Las empresas como Amazon son esclavistas. No valoran a sus empleados como seres humanos. En Silicon Valley se recompensa el talento, pero solo mientras beneficie a la corporación. En el momento en que dejas de beneficiarlos, estás fuera. Y si te atreves a actuar fuera del marco que el empleador te impone, a hacer preguntas sobre lo que hace la empresa y a quién se lo hace, tu trabajo corre peligro. Esto no es una especulación. Yo lo vi y lo viví. — Tras dejar Amazon, fundé Ethics in Technology. Organicé las NSA Comedy Nights tras las revelaciones de Edward Snowden, eventos que reunieron a más de 150 personas en cada una de las tres veladas, porque la gente quería un lugar donde darle sentido a lo que estaba sucediendo con su privacidad, con sus datos, para comprender el país en el que estaban viviendo. Esta organización sin fines de lucro se constituyó formalmente en 2018. Publiqué *Ethics in Tech and Lack Thereof*. Creía, en aquel momento, que nombrar el problema era el comienzo de su solución. Creía que la presión pública funcionaría. Cerré Ethics in Technology en febrero de 2022. Sin embargo, esta no fue una derrota, sino más bien aceptar la realidad. La guerra de Ucrania y la respuesta de Silicon Valley a ella, que no fue un ajuste de cuentas moral, sino llamadas a inversores, propuestas de contratos y hojas de ruta de productos para el sector de la defensa, me demostró que la estrategia de reforma había llegado a su fin. Lancé NoEthicsInBigTech.com. La estrategia pasó de la persuasión a la persecución. --- Hay un marco filosófico que he mantenido a lo largo de todo este trabajo, y quiero mencionarlo aquí porque subyace a todo lo que hay en este libro. La verdadera lucha a la que se enfrenta la humanidad, bajo toda la tecnología, bajo todas las armas, bajo todos los argumentos políticos sobre Oriente y Occidente, el islam y el cristianismo, la OTAN y Rusia, es entre dos ideas contrapuestas. La primera idea es «yo soy uno». La segunda es «somos uno». Todo lo que ha producido la maquinaria de guerra de Silicon Valley es un monumento a la primera idea: «Yo soy uno», «mis accionistas son uno», «mis beneficios trimestrales son uno». Todo lo que defiende este libro es la segunda idea: «somos uno», y las armas, la vigilancia, la explotación de los trabajadores, el silenciamiento de las voces y los algoritmos de selección que deciden qué niños viven y cuáles mueren, todo ello es un crimen contra el «nosotros» que nos incluye a todos. Soy iraní-estadounidense. Llegué a este país a los once años sin hablar inglés. Me sentaba en los hospitales los viernes por la mañana con mi madre, que era enfermera, y veía lo que la guerra le hace a los cuerpos humanos. Lo vi de niño y lo he estado viendo cada día desde

entonces, a través de todas las formas que adopta la máquina: el sistema de selección de objetivos, el contrato en la nube, el algoritmo de moderación de contenidos, la cuota de productividad del almacén. Y he decidido que lo único responsable que puedo hacer con lo que he visto es documentarlo con la mayor precisión, con las fuentes más fiables y con la mayor honestidad que una persona que trabaja sin respaldo institucional puede lograr. La película *Forever Peace Now* forma parte de esa documentación. Este libro también forma parte de ella. ParentsPlea.com forma parte de ella. La petición a España forma parte de ella. Nada de esto es obra de alguien que se ha rendido. Todo es obra de alguien que comprende tras una infancia dedicada a observar lo que la guerra hace a los cuerpos y una carrera dedicada a observar lo que la tecnología le hace a las almas. Alguien que sabe que los hombres malvados y sus máquinas no prevalecen, pero que tampoco se detienen por sí solos, y que el arco de la historia solo se inclina porque la gente lo empuja. He visto suficiente. Estoy empujando.

Una carta a quienes construyen la máquina. Un mensaje directo a los trabajadores del sector tecnológico

Quiero dirigirme directamente a los trabajadores tecnológicos que leen este libro. No a los ejecutivos. Ni a los inversores, ni a los departamentos de relaciones públicas que serán enviados a rebatir lo que he escrito. Sino a los ingenieros. A los científicos de datos. A los gestores de productos. A los vendedores. A los gestores de alianzas. A las personas que, en este mismo momento, están sentadas en una oficina en algún lugar del Área de la Bahía, o en Austin, o en Seattle, o en Bangalore, construyendo las herramientas de las que trata este libro.

Yo era como ustedes. Se me daba muy bien ser como ustedes. A los veintidós años ganaba un cuarto de millón de dólares al año en ventas tecnológicas. Vendí servicios de coubicación en Exodus. Vendí soluciones de redes en Bay Networks. Conseguí financiación de Marc Benioff y Michael Dell. Me reuní con Andy Jassy en Amazon Web Services, gestioné acuerdos de marketing conjunto de siete cifras y redacté informes ejecutivos para personas cuyas decisiones daban forma a todo el ecosistema tecnológico empresarial. Estaba dentro de él. Lo estaba construyendo. Se me daba bien y estaba orgulloso de ello.

Y te digo: elige con cuidado.

Hay tres fuerzas que impulsan a la mayoría de la gente en Silicon Valley, y las he visto a todas de cerca. La primera es la necesidad de riqueza. La segunda es la necesidad de poder. La tercera es la necesidad de vanidad: lo que se podría llamar el desfile de moda, la carrera por el mejor coche y la segunda residencia, la mejor marca de reloj y el colegio al que asisten tus hijos. Estas fuerzas son reales. No soy ingenuo al respecto. Yo mismo las perseguí durante años, antes de que la máquina me destrozara y comprendiera lo que realmente cuestan.

En Silicon Valley se premia el talento. Pero solo mientras beneficie a la empresa. En el momento en que dejas de hacerlo, cuando haces la pregunta equivocada, cuando firmas la petición equivocada, cuando te levantas de la reunión equivocada, tu puesto de trabajo corre peligro. He visto cómo ocurre esto. He visto cómo los guardias de seguridad echan a los ingenieros, a aquellos mismos trabajadores que crean los productos que les reportan miles de millones de dólares a estas empresas, solo por preguntar dónde se utilizan sus herramientas. Por otro lado, también he visto a personas, a las que respetaba, llegar a la conclusión de que su hipoteca y que la estabilidad de su familia valen más que cualquier malestar que pudieran sentir por lo que hace la empresa. Entiendo este razonamiento. Yo mismo lo hice durante un tiempo.

Pero quiero que entiendas lo que ese cálculo cuesta realmente.

Te cuesta tu conciencia. Y tu conciencia, resulta que no es un activo intangible. Es lo que determina si puedes mirarte al espejo. Si algún día podrás sentarte frente a tus hijos y contarles qué hiciste con los años en los que eras inteligente, motivado y capaz de construir casi cualquier cosa. Si podrás dormir sin que te asalte la pregunta que tarde o temprano llegará: ¿el trabajo que hice mejoró el mundo o lo empeoró?

Las empresas para las que trabajas tienen suficientes defensores. Cuentan con agencias de relaciones públicas, equipos de comunicación ejecutiva, grupos de presión y abogados. Pueden defenderse solas. No necesitan tu silencio para sobrevivir. Lo que necesitan —lo que siempre han necesitado— es tu trabajo, tu inteligencia, tu creatividad y tu disposición a dejar de lado las preguntas que te plantea tu conciencia.

No te pido que hagas lo que hizo Daniel Ellsberg. No te pido que hagas lo que hizo Edward Snowden. Ambos caminos tuvieron un costo que la mayoría de la gente no puede ni debe asumir. Ellsberg te diría: no acudas primero a tus superiores, no acudas primero al Congreso; solo te tacharán de alborotador y te dejarán de lado. Snowden lo hizo bien. Pero no todo el mundo está en condiciones de ser Snowden, y la industria no debería exigir ese nivel de sacrificio personal para que se escuche la conciencia.

Lo que te pido es más sencillo. Te pido que compruebes. Que te asegures de que el trabajo que estás haciendo sea ético, que sea significativo, que represente los valores con los que te criaste, y no solo los valores de tus opciones sobre acciones o tu bonificación trimestral. Hazte la pregunta: ¿Acaso la empresa para la que trabajas representa tus valores? ¿Te enorgullece lo que hace? ¿Acaso respeta los derechos humanos y los derechos digitales de las personas a las que impacta?

Si no es así, vete. Elige otra empresa. Elige otro puesto. Elige otro camino. Hay más opciones disponibles para los profesionales cualificados de la tecnología que en casi cualquier otro campo del mundo. Nadie que sepa escribir una API de producción, diseñar una implementación en la nube o entrenar un modelo de aprendizaje automático carece realmente de opciones. La elección está ahí. La pregunta es si estás dispuesto a tomarla.

Yo aprendí esto por las malas, pasando cuatro meses y medio en hospitales después de que la máquina en la que había confiado destruyera mi empresa, me despojara de mis recursos y me dejara sin nada que mostrar tras años de trabajo, salvo la prueba de que el sistema está amañado a favor de los poderosos. Me reconstruí. Cambié de rumbo. Convertí aquello que me destrozó en el trabajo que ahora tienes en tus manos. Pero preferiría que no necesites una crisis para hacerte la pregunta que te pido que te hagas ahora mismo.

No acabes como yo: trabajando en Amazon Web Services para Jeff Bezos y Andy Jassy, pasando tus días enriqueciendo a una empresa que ya ha decidido que eres una pieza reemplazable, aportando tu talento a un imperio que te agradecerá tu servicio y te mostrará la puerta en el momento en que seas más caro que la automatización que te sustituye.

Tienes más poder de lo que crees. La máquina funciona gracias a tu experiencia. Esa es también tu ventaja. Úsala.

Elige con prudencia. Elige un trabajo que te haga sentir orgulloso. Elige la empresa que represente el mundo en el que quieres que vivan tus hijos. Y si ya estás dentro de una empresa que sabes que está haciendo daño, por lo que sabes, por lo que ves desde tu puesto, plantéate si este es el momento de decir lo que sabes.

En palabras del fallecido Daniel Ellsberg, quien en su momento fue analista militar del gobierno de Estados Unidos, y después se convirtió en activista político: «Las probabilidades están en nuestra contra. El mayor temor de Snowden era que nada cambiara. El de Manning también. Ese es probablemente el resultado. Pero nadie puede afirmar con certeza que el cambio es imposible. La posibilidad existe, y lo que está en juego es extraordinariamente alto. Así que la

respuesta es decir la verdad, asumir los riesgos, decir lo que sabes cuando lo sabes. La pregunta que toda persona debe hacerse cuando sabe que se está ocultando la verdad es si acaso no es este el momento de alzar la voz».

Me hice esa pregunta después de Amazon. La respondí con este libro. Tú tendrás que responderla con lo que sea que estés construyendo en este momento.

Elige bien. Porque la máquina no se detiene a menos que las personas que la manejan decidan que debe hacerlo. Y ahora mismo, demasiadas de esas personas están mirando la misma hoja de cálculo y llamando «oportunidad de oro» al genocidio.

Tú eres mejor que eso. Lo sé porque yo era uno de ustedes, y yo también era mejor que eso, aunque tuviera que perderlo casi todo para demostrarlo.

CAPÍTULO UNO. EN DEFENSA DE LA TECNOLOGÍA ÉTICA

Y el uso de la IA en beneficio de la humanidad, no en nuestro perjuicio. Cuando me mudé a Estados Unidos a la temprana edad de once años, no hablaba inglés. Apenas sabía un par de palabras. Tuve que matricularme en clases de inglés como segunda lengua durante la primaria solo para comprender lo básico. Llegar de Irán al Área de la Bahía de California conllevaba un peso que no había previsto: las connotaciones negativas, la lucha por ser aceptado por compañeros y profesores, la hostilidad del clima político. Irán y Estados Unidos tenían una relación horrible en aquel momento, como la tienen hoy, y la forma en que se retrataba a los iraníes en los medios de comunicación era todo menos acogedora. En esas clases, a mis profesores les importaba poco el pensamiento crítico. Se centraban en la gramática, la estructura de las oraciones y la puntuación. Nos daban libros de ficción para leer y no le daban ningún valor a los periódicos ni a la actualidad. Esto me resultaba extraño. Nunca me gustó la ficción. Siempre me pareció que la realidad superaba a la ficción, y me encantaba estar al día de lo que realmente ocurría en el mundo. Con la no ficción podía llegar a un público amplio compartiendo la verdad, en lugar de limitarme a entretener a la gente con historias que me había inventado. Así que no mostré mucho entusiasmo por las clases de inglés durante la secundaria. A los dieciséis años, tras graduarme dos años antes de lo habitual de la secundaria, me inscribí por primera vez en una asignatura de Pensamiento Crítico en el Diablo Valley College de Concord, California. Mi profesor, el Dr. Miller, me introdujo en las falacias lógicas y el arte de la argumentación. Debatíamos temas con posturas distintas delante de la clase y teníamos que construir argumentos sólidos sobre cuestiones sociales y políticas, independientemente de lo que pensáramos personalmente al respecto. Esa clase, junto con un curso de oratoria que me encantaba, me dio lo que las clases de inglés como segunda lengua nunca pudieron darme: la confianza para ponerme delante de una sala y defender mis argumentos sobre temas que me importaban, y hacer que estos argumentos calaran. A medida que mi trabajo ha ido cambiando a lo largo de las décadas, desde crear startups tecnológicas, hasta trabajar en gigantes como Amazon Web Services, pasando por la defensa de los derechos humanos y los derechos digitales, esas dos clases siguen siendo lo más valioso que saqué de mi educación universitaria. Digo todo esto porque explica por qué utilizo la IA como mi editora y compañera de investigación al escribir este libro, y por qué creo que esa elección no es una contradicción, sino una declaración de principios. Justifico el uso del poder de la IA para hacer el bien. En beneficio de la humanidad. En los capítulos siguientes, examinaremos cómo la IA ha sido diseñada por la «mafia de PayPal» y la «clase de Epstein» en detrimento de la humanidad. Pero quería dedicar este primer capítulo al otro lado de ese argumento: el uso ético de la IA, empleada con buenas intenciones, para elaborar argumentos bien razonados, citar fuentes, reducir el tiempo de investigación y ayudar a alguien como yo —que aún lleva las marcas de sus años de inglés como segunda lengua— a comunicar ideas importantes sin quedarme paralizado por cómo un profesor de inglés podría calificar la ortografía. En los tiempos que corren, el

contenido debe desarrollarse a un ritmo que habría parecido imposible hace una generación. El tren avanza a toda velocidad. La maquinaria propagandística de estas empresas tecnológicas sin escrúpulos es sofisticada, está bien financiada y es incansable. Como escritores, autores, editores e investigadores, ya no podemos permitirnos el lujo de esperar años para producir un manuscrito. Tenemos que mantenernos al día y actuar con rapidez. La tecnología nos ha permitido ser testigos de la inhumanidad de los sionistas elegidos y de sus crímenes en línea. Por primera vez en nuestras vidas, todos hemos sido testigos del horror que ha causado. Todos hemos quedado traumatizados y, lamentablemente, algunos se han vuelto insensibles a ello. Por eso debemos actuar rápido. Antes de continuar, quiero abordar un asunto que nadie quiere discutir. Hay quienes creen que toda la IA es maligna. Que consume demasiada electricidad, demasiada agua, que contribuye al calentamiento global, que tiene un impacto directo en las personas que producen las materias primas y los chips utilizados en su desarrollo, que desplazará a demasiados puestos de trabajo de oficina. Permítanme abordar cada una de estas preocupaciones. Pero primero, permítanme trazar una línea entre lo que considero tecnología ética y lo que no. Algunas de las voces más críticas contra la IA pasan muchas horas al día en las redes sociales, interactuando con publicaciones y dejando comentarios despectivos solo para trolear y compartir su opinión. Otros pasan horas en plataformas de videojuegos como Twitch. Algunos dedican un tiempo valioso a realizar exploraciones en motores de búsqueda, recibiendo anuncios a cambio, u operando con criptomonedas y participando en el trading de alta frecuencia, o transmitiendo contenido las 24 horas del día, pero reservan sus críticas sobre el consumo de recursos exclusivamente para la IA. Todas las actividades mencionadas consumen electricidad, agua, capacidad de procesamiento y almacenamiento, y generan residuos electrónicos. La mayoría no aporta ningún beneficio a la humanidad. ¿Cuál es el beneficio de realizar exploraciones en motores de búsqueda durante horas y recibir anuncios, frente a una búsqueda específica con IA que te da una respuesta directa? ¿Qué gana el mundo con la criptoeconomía? Las horas dedicadas a los juegos en línea y a las plataformas de streaming de contenido, ¿qué se construye con eso? En lo que respecta a la pérdida de puestos de trabajo, se trata de una preocupación legítima y me la tomo muy en serio. Pero déjenme preguntar esto: recuerdo cuando había tiendas de revelado de fotos en cada esquina. Cuando hacíamos los preparativos de viaje a través de agencias de viajes. Cuando comprábamos mapas en papel de cada ciudad que visitábamos o consultábamos guías de viaje que tenían entre tres y siete años de antigüedad, y que por lo mismo a veces describían hoteles y restaurantes que ya no existían. Todo eso fue sustituido por la tecnología. Denme un argumento a favor de recuperarlo, uno bueno, por favor, y les escucharé. La tecnología evoluciona. Se puede utilizar en beneficio de toda la humanidad. La IA puede simplificarnos la vida. La robótica también. La cuestión nunca ha sido si la tecnología es buena o mala. La cuestión es siempre: ¿quién la está creando y cuál es su intención? Un tonto con una herramienta, sigue siendo un tonto. Los chicos de Silicon Valley, la «mafia de PayPal» que sueña con escapar a Marte mientras bautizan a sus hijos con nombres como X Æ A-Xii, carecen, para decirlo sin rodeos, de la calidez humana más básica. Peter Thiel y sus descendientes ideológicos crearon empresas como Palantir, no para hacer avanzar a la humanidad, sino para monetizar la vigilancia y la guerra, y para facilitar la violencia estatal. Alex Karp y Palantir no están construyendo el futuro. Están lucrando con la maquinaria de la destrucción. No digo esto con odio. Lo digo con lástima. Estar tan alejado de lo que significa

ser humano es un castigo en sí mismo. Lo que estos hombres carecen fundamentalmente es de empatía. Y la empatía, resulta que no es una habilidad blanda, sino precisamente lo que separa la sabiduría de las armas. Me recuerdan a Oppenheimer, pero no a la versión glorificada por Hollywood, sino al verdadero: el científico que dividió el átomo sin detenerse a preguntarse si debería hacerlo. La inteligencia artificial que se está construyendo a su imagen es fría, calculadora e indiferente a las consecuencias. Alucina con la confianza sin una comprensión genuina. Ve alguna vez una entrevista de Peter Thiel. El hombre habla como un ciervo paralizado por los faros de un coche: técnicamente vivo, emocionalmente ausente. Y aquí es donde se pone interesante: la IA que han construido les está fallando de una manera muy específica. Llena los vacíos de su conocimiento con ficciones seguras de sí mismas. Pero también lo hacen ellos. Los líderes sin empatía llenan los vacíos de su comprensión con más crueldad, más vigilancia, más violaciones de los derechos digitales y humanos. Los necios, con las mejores herramientas, siguen siendo necios y sus herramientas no los salvarán. En cualquier caso, las herramientas aceleran su desmoronamiento. Los hombres malvados y sus máquinas no prevalecen. La historia es larga y está plagada de su clase. Entonces, ¿qué hace realmente la IA cuando se construye y se utiliza con conciencia? Permítanme darles siete respuestas.

IA y medicina: ver lo que los ojos humanos no pueden

El programa AlphaFold de DeepMind resolvió uno de los problemas más complejos de la biología: la predicción de cómo las proteínas se pliegan en estructuras tridimensionales. Este era un reto que derrotó a los científicos durante cincuenta años. Para 2022, AlphaFold había mapeado las estructuras de más de 200 millones de proteínas, abarcando prácticamente todas las proteínas conocidas por la ciencia. Este avance único ya está transformando la investigación sobre el Alzheimer, el Parkinson, el cáncer y las bacterias resistentes a los antibióticos. La herramienta es gratuita y está abierta a investigadores de todo el mundo. Esta no es una IA al servicio de un informe de resultados trimestrales. Se trata de una IA al servicio de los enfermos, los vulnerables y los científicos que dedican su vida a intentar ayudarlos. (Fuente: Base de datos DeepMind AlphaFold, https://alphafold.ebi.ac.uk; Nature, julio de 2022). Cirugía a distancia: el cirujano que está en todas partes a la vez El sistema quirúrgico da Vinci se ha utilizado en más de diez millones de intervenciones en todo el mundo, lo que ha permitido realizar cirugías mínimamente invasivas para el cáncer, las enfermedades cardíacas y traumatismos, con tiempos de recuperación y tasas de complicaciones significativamente reducidos. En 2022, cirujanos de la Universidad Johns Hopkins realizaron la primera cirugía laparoscópica totalmente autónoma en tejido blando utilizando un robot guiado por IA, llamado STAR (Smart Tissue Autonomous Robot), que operó sin guía humana directa y que superó a los cirujanos humanos en varios parámetros medibles. Las implicaciones son enormes. En zonas rurales, en zonas de conflicto, y en regiones del mundo donde no hay cirujanos especialistas disponibles, la cirugía robótica guiada por IA no es un lujo: es un salvavidas que por fin se está haciendo realidad. (Fuente: Intuitive Surgical, https://www.intuitive.com; Science Robotics, enero de 2022). Descubrimiento de fármacos y vacunas: de años a meses La pandemia del COVID-19 mostró al mundo lo que el descubrimiento de fármacos asistido por IA puede lograr bajo presión. Gracias a la IA, BioNTech logró diseñar y optimizar la secuencia del ARNm de su vacuna contra el COVID-19 en tan solo meses, cuando una investigación tradicional toma años. La plataforma de IA Insilico Medicine llevó un fármaco

candidato desde el diseño inicial por IA hasta el ensayo clínico en menos de dieciocho meses, un proceso que tradicionalmente toma doce años o más. En 2023, un fármaco diseñado por IA para la fibrosis pulmonar idiopática entró en la fase II de ensayos clínicos: la primera molécula diseñada íntegramente por IA en alcanzar esa etapa. Para las enfermedades raras, las enfermedades tropicales desatendidas y las pandemias que aún no hemos enfrentado, esta aceleración no es una simple nota técnica al pie de página. Es la diferencia entre la vida y la muerte para millones de personas. (Fuente: Insilico Medicine, https://insilico.com; Nature Biotechnology, 2023). Energía y electricidad: la IA resuelve el problema por el que los críticos la culpan Hay una ironía particular en la acusación de que la IA desperdicia energía. DeepMind, de Google, aplicó el aprendizaje automático a los sistemas de refrigeración de los centros de datos de Google en 2016 y logró una reducción del 40 % en la energía de refrigeración, lo que se tradujo en una reducción del 15 % en el consumo total de energía. El mismo enfoque lo están utilizando ahora los operadores de redes eléctricas de todo el mundo para predecir las fluctuaciones de la demanda e integrar las fuentes de energía renovable de manera más eficiente. En California, las herramientas de gestión de la red impulsadas por IA están permitiendo a las empresas de servicios públicos reducir el desperdicio e incorporar energía solar y eólica a gran escala. La misma tecnología que, según los críticos, consume demasiada electricidad se encuentra entre las herramientas más poderosas de las que disponemos para gestionar la crisis energética que dicen preocuparle. (Fuente: DeepMind https://deepmind.google; Laboratorio Nacional Lawrence Berkeley, Informe sobre IA para la Energía, 2023). Astronomía: la IA amplía la visión de la humanidad hacia el cosmos En 2019, la colaboración del Event Horizon Telescope utilizó el aprendizaje automático para reconstruir la primera imagen de un agujero negro. Se trata de un objeto supermasivo situado en el centro de la galaxia M87, y su imagen fue reconstruida a partir de datos de radiotelescopios que ningún análisis humano habría podido procesar a la escala requerida. Las misiones Kepler y TESS de la NASA utilizaron IA para identificar miles de exoplanetas a partir de datos brutos de telescopios, incluidos planetas del tamaño de la Tierra en zonas potencialmente habitables. En 2023, los astrónomos que utilizaron herramientas de IA en el Observatorio Vera Rubin detectaron, en una sola campaña de observación, miles de asteroides cercanos a la Tierra hasta entonces desconocidos. Se trata de la humanidad utilizando su herramienta más poderosa para ampliar su visión hacia el cosmos y sin fines lucrativos, ni para obtener ganancias en el mercado, sino para el conocimiento. (Fuente: Colaboración Telescopio del Horizonte de Sucesos, https://eventhorizontelescope.org; Archivo de Exoplanetas de la NASA, https://exoplanetarchive.ipac.caltech.edu).

Reciclaje medioambiental: enseñar a los microbios a sanar el planeta Investigadores de la Universidad de Portsmouth, utilizando ingeniería de proteínas asistida por IA, modificaron una enzima bacteriana natural llamada PETasa para que descomponga el tipo de plástico utilizado en la mayoría de las botellas, a una velocidad drásticamente acelerada. La IA fue utilizada para modelar y optimizar mutaciones enzimáticas que hubiera tardado décadas en descubrirse mediante el método convencional de prueba y error. Por otra parte, los investigadores están utilizando la IA para identificar comunidades microbianas en el suelo y el agua capaces de descomponer los PFAS («sustancias químicas eternas»), los metales pesados y los disolventes industriales. Nosotros creamos estos contaminantes con tecnología industrial. Quizás podamos eliminarlos con tecnología biológica guiada por la IA. Esto no es teórico. Ya se está llevando a

cabo en laboratorios y está en las primeras fases de campo. (Fuente: Universidad de Portsmouth / NREL, Nature, abril de 2018; Environmental Science & Technology, 2023).

Testigos del genocidio: la IA como la memoria que no se puede borrar Quizás la aplicación de la IA más urgente desde el punto de vista moral en el momento actual es la documentación. The Syrian Archive —ahora conocido como Mnemonic— ha utilizado herramientas asistidas por IA para preservar, verificar y archivar más de 3,5 millones de pruebas digitales de crímenes de guerra en Siria: vídeos, imágenes de satélites y publicaciones en redes sociales protegidas contra su eliminación, quedando disponibles para futuros procesos judiciales. En Gaza, organizaciones como Forensic Architecture y Airwars están utilizando análisis de imágenes satelitales mejorados con IA e inteligencia de código abierto para documentar patrones de ataques, víctimas civiles y ataques contra sitios protegidos. Las mismas tecnologías de IA que los fabricantes de armas utilizan para identificar objetivos están siendo empleadas por las organizaciones de derechos humanos para la tarea de dar testimonio. Me parece profundamente significativo. La tecnología, como he defendido desde la primera página de este libro, no es intrínsecamente buena ni mala. Es la intención de su creador y el valor de quienes la utilizan para decir la verdad, lo que determina de qué lado de la historia se sitúa. (Fuente: Mnemonic, https://mnemonic.org; Forensic Architecture, https://forensic-architecture.org; Airwars, https://airwars.org). Basándome en todo lo anterior, he tomado una decisión. La IA será mi editora. La IA me ayudará con la investigación. Y juntos, avanzaremos tan rápido como este momento lo exija. --- El uso ético de la IA, el argumento que he expuesto en este capítulo inicial, no surgió de la nada. Surgió como respuesta directa a lo que vi en lo que se convertía la industria tecnológica a lo largo de las tres décadas que pasé en su seno. El capítulo dos es donde comienza esa historia: no con políticas abstractas fallidas, sino con la trayectoria personal, concreta y documentada que me llevó desde las granjas de servidores de Exodus Communications a los algoritmos de selección de objetivos del Proyecto Nimbus, y a la convicción de que lo que estaba presenciando no era una historia nueva, sino la más antigua que cuenta el capitalismo.

CAPÍTULO DOS. CÓMO LLEGAMOS AQUÍ

Le hice una pregunta sencilla: ¿como empresa, dónde trazan la línea en cuanto a los clientes y el tipo de proyectos? ¿Tienen una línea roja? Como he documentado a lo largo de los años, en mis numerosas conversaciones con ejecutivos de Silicon Valley y en mi película *Forever Peace Now*, a aquellos que dirigen el sector tecnológico no les preocupa el bienestar de la humanidad. Piensan en las ganancias económicas individuales, en «ganar» a cualquier precio y en el dominio del mercado, sin importarles las consecuencias humanas. Lo vi de cerca. Estuve dentro de ello. Hay una conversación que recuerdo por encima de todas las demás. Tras dejar Amazon Web Services, estaba buscando trabajo y me presenté a una entrevista en una empresa tecnológica cuyo nombre dejaré que el lector imagine. El vicepresidente sénior de marketing me dijo, de un modo que sólo puedo describir como con orgullo, que la Fuerza Aérea de Estados Unidos era uno de sus clientes más valiosos, porque la tecnología de la empresa les ayudaba a matar y a atacar a personas de forma más eficaz. Lo dijo como quien se hubiera ganado un premio de ventas. Hacia el final de la entrevista, me cedió la palabra. «Pregunta lo que quieras», dijo. Le hice una pregunta sencilla: ¿como empresa, dónde trazan la línea en cuanto a los clientes y el tipo de proyectos? ¿Tienen una línea roja? Me miró como si hubiera hablado en un idioma que no reconocía. «¿Qué quieres decir?», dijo. «No rechazamos negocios. Si se trata de una empresa registrada, nos encantaría tenerla como cliente». Silicon Valley no tiene líneas rojas. Presionarán para conseguir cualquier contrato, buscarán a cualquier cliente y venderán su alma a cualquier comprador dispuesto a firmar un cheque. Esto no es una opinión. Es un modelo de negocio. Quién era yo cuando entré en aquellas salas Quiero detenerme aquí y contarles quién era yo cuando entré por primera vez en esas salas de reuniones. No en quién me convertí, sino quién era. Tenía veintidós años. Venía de una familia de seis miembros que vivía en un apartamento de veintisiete metros cuadrados en Berkeley, California. No éramos pobres en el sentido abstracto de la palabra, sino en el sentido de que éramos seis personas compartiendo un espacio más pequeño que la mayoría de los salones de los hogares estadounidenses y hacíamos que funcionara, porque eso es lo que haces cuando no tienes otra opción y estás agradecido de estar vivo y de vivir en un país que no te está bombardeando. Me gradué de la secundaria a los dieciséis años, fui a la universidad comunitaria, monté una empresa antes de que la mayoría de mis compañeros tuvieran su primer trabajo de verdad, y a los veintidós años ganaba un cuarto de millón de dólares al año en ventas de tecnología. Me sentaba en salas de reuniones con hombres que dirigían empresas valoradas en miles de millones de dólares. Recaudaba capital. Negociaba contratos con cifras de nueve dígitos. Quería ser un buen capitalista estadounidense. Lo digo sin ironía y sin disculparme, porque creo que es importante ser honesto sobre quién era antes de comprender cómo era el sistema en realidad. Venía de Irán, de una guerra, de un país donde la economía había sido estrangulada por las sanciones y la ideología, y por el fervor revolucionario que lo quema todo y llama libertad a las cenizas. Llegué a Estados Unidos y descubrí que una persona podía construir algo, podía ganar dinero, podía sentarse en una mesa con gente poderosa y ser escuchada. Yo quería eso. Lo perseguí

y se me daba bien. Y entonces tuve opciones sobre acciones. Los fundadores de Silicon Valley reciben acciones ordinarias. Esto suena bien hasta que entiendes lo que significa en la práctica. Tienes la idea. Reúnes al equipo. Trabajas horas que ningún contrato de trabajo podría reflejar: las llamadas de medianoche, los cambios de rumbo los fines de semana, los meses en los que el producto no funciona y el dinero casi se ha acabado, y tú eres la única persona en la sala que no puede permitirse perder la fe en lo que estás construyendo. Haces todo eso. Y a cambio, recibes acciones ordinarias: la clase de capital más baja en la estructura de capital, la última en la fila cuando se distribuye algo, la primera en diluirse. El inversor que firma un cheque en una ronda de Serie A obtiene acciones preferentes. No acciones ordinarias. Una clase totalmente diferente, con sus propios derechos de veto, sus propias preferencias de liquidación, sus propias protecciones que pueden incluirse en cada ronda de financiación posterior en cualquier configuración que negocien sus abogados. El fundador que tuvo la idea y construyó el proyecto, obtiene acciones ordinarias. El inversor que se presentó con una chequera, obtiene acciones preferentes y un puesto en la mesa donde el fundador no puede destituirlo, incluso cuando el juicio del inversor es erróneo. Esta es la mentira fundamental de la narrativa de la meritocracia de Silicon Valley. El sistema no está diseñado para recompensar a las personas que construyen cosas. Está diseñado para proteger a las personas que financian cosas. Estas no son las mismas personas. Y la brecha entre ellas, entre las acciones ordinarias y las preferentes, entre el fundador que no puede vender y el inversor que sí puede, es donde la mayor parte de la riqueza que debería ir a parar a los creadores se desvía hacia el capital. Lo descubrí por las malas. Tenía opciones sobre acciones en mi empresa, o lo que yo llamo «dinero ficticio», porque en aquel momento no existía un mercado secundario para las acciones de los fundadores. No podía venderlas a inversores a cambio de efectivo. No podía convertirlas en nada líquido. Tenía riqueza en papel y una visión, y esa forma particular de pobreza que proviene de tener algo que parece dinero pero que no se puede gastar. Lo que quería hacer con esas opciones, si alguna vez se convertían en algo real, era donar una gran parte a Médicos Sin Fronteras. Lo digo literalmente. Tenía veintidós años, venía de una familia en la que seis personas vivíamos en veintisiete metros cuadrados, y mi primer pensamiento sobre qué hacer con una riqueza hipotética era dar una parte significativa de ella a las personas que prestaban asistencia médica en zonas de guerra. Recordaba lo que mi madre había visto como enfermera durante la guerra entre Irán e Irak. Recordaba los pasillos de los hospitales. En aquel momento no sabía expresarlo como una postura política. Era simplemente lo que le parecía correcto a un joven que entendía, por experiencia propia, que la diferencia entre tener asistencia médica y no tenerla es la diferencia entre vivir y morir. El sistema no se adapta a este impulso. El sistema no está diseñado para ello. Ese fue el momento en que empecé a comprender algo que me tomaría otros veinte años para poder expresarlo plenamente: el sistema no está roto. Funciona exactamente del modo como está diseñado. Está diseñado para concentrar el capital en manos de quienes ya lo tienen, para proteger su posición privilegiada en cada ronda posterior, para garantizar que el dinero ficticio fluya hacia arriba y que los fundadores, los trabajadores y las comunidades que hacen posible toda la empresa, queden posicionados, legal y estructuralmente, por diseño deliberado, recibiendo lo que sobra después de que la clase privilegiada se quede con lo que cree le corresponde. Estuve en salas de juntas con estos hombres. Los vi actuar. Sé cómo algunos de ellos adquirieron su riqueza. Sé cómo se obtuvieron ciertos nombres de dominio para sitios web en un momento en que el

proceso regulatorio debió haberlo impedido. Cuando se suponía que el sistema era abierto y basado en reglas para una apropiada organización de la Internet, en realidad resultó tener espacios donde se aplicaban reglas diferentes para quienes sabían cuáles puertas tocar. Conozco los entretelones de los acuerdos que voy a describir no por haber leído sobre ellos, sino por haber estado presente cuando se discutieron. No voy a nombrar a todas las personas que conozco de ese mundo. Soy demasiado joven para morir, y entiendo que quienes denuncian a hombres poderosos de forma demasiado concreta a veces se encuentran con que el sistema legal, el mismo sistema legal que condenó a Jeffrey Epstein a trece meses por delitos que a la gente común les habrían valido décadas de cárcel, puede utilizarse como arma contra la persona que denuncia en lugar de contra la persona denunciada. Pero diré esto: sé quiénes son estos hombres. Sé qué es lo que valoran y cómo hablan de las personas que no están presentes. Sé cómo es el poder de cerca cuando tienes veintidós años y estás lleno de ambición y te sientas frente a él al otro lado de la mesa. Y lo que puedo decirte es que la mitología, los fundadores visionarios, la meritocracia, la disrupción al servicio de la humanidad, es una historia que cuentan en público. Lo que se dicen entre ellos en privado es algo diferente. Lo que han construido es algo diferente. Y la brecha entre la historia pública y la privada es la brecha que todo este libro intenta trazar. Me salí. Elegí algo diferente. Estoy escribiendo este libro en lugar de cobrar cheques de la gente a la que podría estar defendiendo. Esta elección me costó dinero. Me costó relaciones. Me costó el tipo de comodidad profesional que se obtiene al permanecer dentro de la red, mantener la cabeza gacha y guardar tus opiniones para ti. Mañana volvería a tomar la misma decisión. La mafia de PayPal Quiero hacer una pausa para definir mis términos, porque he estado utilizando dos expresiones a lo largo de este libro que merecen algo más que una simple mención, porque las personas a las que describo han dedicado considerables recursos para garantizar que su imagen pública siga siendo halagadora. La primera expresión es «la mafia de PayPal». Silicon Valley utiliza este término con orgullo. Aparece en las revistas de negocios como un homenaje: un grupo de fundadores extraordinariamente exitosos que se conocieron en una startup llamada PayPal a finales de la década de 1990, la convirtieron en algo valioso y la vendieron a eBay en 2002 por 1.500 millones de dólares, para luego dispersarse por el panorama empresarial para crear Tesla, LinkedIn, Palantir, YouTube, Yelp y una docena de otras empresas que han dado forma al mundo moderno. La historia es de genialidad y ambición, y de los múltiples rendimientos a partir de grandes redes. Nunca pensé que la palabra «mafia» fuera algo de lo que nadie debiera sentirse orgulloso. Una mafia no es una red de personas ambiciosas que se conocen entre sí. Una mafia es una organización criminal: un grupo de hombres que operan al margen de la ley mientras presentan una cara legítima al mundo, personas que utilizan su poder colectivo para eludir las normas que se aplican a todos los demás y que se protegen mutuamente de las consecuencias de lo que hacen. El hecho de que Silicon Valley adoptara el término y lo convirtiera en una marca lo dice todo sobre cómo se ven a sí mismos en relación con la ley y con el resto de nosotros. El núcleo de la «mafia de PayPal», tal y como lo utilizo en este libro, incluye a Peter Thiel, cofundador de PayPal y creador de Palantir, la empresa de vigilancia y segmentación cuyas herramientas he documentado en Gaza, en operaciones de deportación del ICE y en los historiales médicos del NHS de 67 millones de ciudadanos británicos. Incluye a Elon Musk, que entró en PayPal a través de la fusión de su empresa X.com y que ahora controla la mayor plataforma de redes sociales del mundo, que posee una empresa

espacial privada, una operación de eficiencia gubernamental y la herramienta de IA que documenté produciendo contenido antisemita y negacionista del Holocausto. También a Reid Hoffman, cofundador de LinkedIn, uno de los primeros ejecutivos de PayPal y un hombre cuya plataforma documenté operando un sistema de vigilancia encubierto que escaneaba 6.167 extensiones de navegador sin el conocimiento ni el consentimiento de los usuarios. Asimismo, la red de inversores, fundadores y operadores que entran y salen de estas empresas a través de Founders Fund, la empresa de capital riesgo de Thiel, y a través de los cargos cruzados entre los consejos de administración y las relaciones de inversión. Todos estos cruces conectan a estas empresas entre sí de manera que, sobre el papel, son transacciones separadas, y en la práctica, un sistema coordinado de enriquecimiento mutuo. Así es como funciona este sistema y es importante entender que cuando los llamo «mafia», no estoy hablando en sentido figurado. Los abogados que nunca fueron los tuyos Quiero hablar de las personas a las que contrataste supuestamente para que te protegieran. Entraste en una negociación de financiación y contrataste a un abogado. Eso es lo que se supone que debes hacer. A veces les pagas quinientos dólares la hora, a veces mil, a veces más, dependiendo del bufete, del socio y del prestigio de la dirección en Sand Hill Road. Firmaste su carta de compromiso. Asumiste, porque les pagabas y porque eso es lo que significa contratar a un abogado en cualquier otro contexto de la vida estadounidense, que representaba tus intereses. Permíteme ser directo sobre algo que me llevó más tiempo del que debió haberme llevado para comprender plenamente: en la mayoría de los casos, esto no es así. Los bufetes de abogados que dominan el trabajo de las startups de Silicon Valley, como Wilson Sonsini Goodrich & Rosati, Cooley, Orrick, Fenwick & West, y otros cuyos nombres ves en cada hoja de términos y en cada anuncio de financiación, no operan principalmente para los fundadores. Operan para el ecosistema. Y el centro de gravedad del ecosistema no es el fundador. Es la empresa de capital riesgo. La empresa de capital riesgo es el cliente habitual. La empresa de capital riesgo es la fuente fiable de operaciones, año tras año, fondo tras fondo, empresa de cartera tras empresa de cartera. El fundador es una transacción. La empresa de capital riesgo es una relación. Piensa en lo que eso significa en la práctica cuando te sientes a negociar tu hoja de términos. El abogado que tienes al otro lado de la mesa, al que pagas por horas para que defienda tus intereses, conoce al socio de esa firma de capital riesgo desde hace años. Han asistido a las mismas fiestas navideñas. Sus firmas colaboran en docenas de operaciones simultáneamente. La empresa de capital riesgo envía referencias. El bufete de abogados envía condiciones favorables. No por escrito. Ni de ninguna forma que pudiera considerarse corrupción ante un tribunal. Sino de la forma en que funcionan las relaciones cuando el dinero y la proximidad crean una alineación de intereses a lo largo de los años. Hay una frase en ese mundo que oirás a menudo. «Estándar de mercado». Cuando te opongas a una cláusula de la hoja de términos, ya sea la preferencia de liquidación, la cláusula antidilución, la aceleración de la consolidación de derechos, la composición del consejo, te dirán que es el estándar de mercado. A menudo será tu propio abogado quien te lo diga. Lo que significa «estándar de mercado», en la práctica, es que esta cláusula se ha utilizado en suficientes acuerdos, redactada por suficientes bufetes que representan a suficientes fondos de capital riesgo como para que se haya convertido en la plantilla. La plantilla no la diseñaron los fundadores. La diseñaron las personas que negociaban al otro lado de la mesa frente a los fundadores. El estándar de mercado es el resultado de décadas en las que los mismos bufetes de abogados han redactado las

mismas cláusulas tipo en nombre de los mismos inversores, y luego te dicen que esas cláusulas son neutrales. No es neutral. Es el sedimento acumulado de mil operaciones en las que los abogados estaban más cerca del dinero que de las personas que construyeron el negocio. Wilson Sonsini es el ejemplo más antiguo y destacado de lo lejos que llegan con esto. El bufete creó un fondo de inversión en 1978, WS Investments, específicamente para que sus socios pudieran adquirir participaciones en las empresas clientes a las que asesoraban. Convirtieron una inversión de setenta y dos mil dólares en Google en un beneficio de veintiocho millones de dólares tras la salida a bolsa. Los mismos abogados que asesoraban a los fundadores sobre cuánto revelar en sus documentos de salida a bolsa, tenían un interés financiero directo en maximizar el precio de la oferta pública inicial. Un profesor de Derecho de la Universidad de Illinois expuso el conflicto sin rodeos: cuanto más se divulga, más bajo es el precio de la salida a bolsa. Eso crea un conflicto de intereses porque, si tienes un interés económico en que el precio de la salida a bolsa sea lo más alto posible, ¿realmente les aconsejarías que divulguen la información? La respuesta que el profesor dejó tácitamente sin decir es: probablemente no. No del todo. No en todos los casos en los que la divulgación pudiera costarle dinero al fondo. El socio fundador del bufete, Larry Sonsini, formaba parte del consejo de administración de Brocade Communications mientras Wilson Sonsini actuaba como asesor jurídico externo de Brocade. Según se informa, animó al consejo a otorgar al director ejecutivo de la empresa la autoridad exclusiva para conceder opciones sobre acciones con una supervisión mínima: un «comité de uno». Ese comité de uno se convirtió en el centro de un escándalo de antedatación de opciones que condujo a un proceso penal. Muchas de las empresas de Silicon Valley investigadas por la antedatación de opciones en aquel momento eran clientes de Wilson Sonsini. Cuando Brocade necesitó un abogado defensor en la demanda derivada resultante, un juez expresó su preocupación de que Wilson Sonsini estaba tan manchada por conflictos de intereses, que la empresa tuvo que prescindir por completo de la firma. En otro caso, una empresa llamada Existence Genetics demandó a Wilson Sonsini por no revelar que, mientras representaba a Existence Genetics, representaba simultáneamente a un competidor directo: Navigenics. Dos clientes. Un bufete. Intereses contrapuestos. Sin revelación. Estos son los casos documentados. Los que se convirtieron en demandas, que dieron lugar a escritos judiciales, que se publicaron en revistas especializadas en derecho. La versión no documentada de esto, la que nunca llega a ser una demanda porque el fundador no tiene el dinero, las pruebas o la energía para enfrentarse a un bufete con dos mil abogados, es de una magnitud mucho mayor. Y luego está el puesto en el consejo de administración. Algunos de estos bufetes de abogados o de sus socios principales a título individual, querrán algo más que honorarios por horas. Querrán participación en el capital. Un papel de asesoramiento. Un puesto en la mesa que les dé acceso continuo a la información y a las decisiones de la empresa mucho después de que se haya cerrado el acuerdo inicial. Lo presentarán como alineación, como tener algo en juego, como una señal de que creen en lo que estás construyendo. Pero en realidad, esto es un mecanismo para convertir una relación de servicio en una relación de propiedad, una que les da acceso preferente a información que otros accionistas no tienen y que crea un incentivo financiero que va en paralelo a, y a veces entrará en conflicto con, su obligación legal de asesorarte con honestidad. Hay algo que los profesionales más astutos de este mundo admitirán en privado: cuando una empresa de capital riesgo recomienda un bufete de abogados a un fundador, el fundador debería preguntarse algo muy

sencillo. ¿Por qué este fondo de capital riesgo en concreto prefiere este bufete en concreto? ¿Qué es lo que este bufete ofrece a este fondo a cambio de esa recomendación? La respuesta, en la mayoría de los casos, no es que el bufete consiga mejores resultados para los fundadores. La respuesta es que el bufete facilita las transacciones para los inversores: acuerdos que se cierran más rápido, con menos fricciones, con condiciones más favorables para la parte que volverá el mes que viene con otro acuerdo que cerrar. Tú no eres esa parte. Tú eres una transacción. No volverás el mes que viene. Y el abogado que has contratado lo sabe. No te estoy diciendo que estos bufetes nunca hagan un buen trabajo. Algunos de sus abogados son genuinamente competentes, están genuinamente comprometidos con sus clientes y se sienten genuinamente incómodos con los conflictos que genera el modelo de negocio de su bufete. Conozco a algunos de ellos personalmente. El problema no son los abogados a título individual. El problema es estructural. El modelo de negocio del bufete dominante de Silicon Valley se basa en servir a ambas partes de la misma mesa, por un lado a los fundadores que pagan los honorarios por hora y por otro a las empresas de capital riesgo que generan el flujo de operaciones. A esto le llaman «representación». Sin embargo, no se puede servir a dos señores. No cuando los intereses de esos señores divergen precisamente en el momento más decisivo: ese momento en el que te encuentras con una hoja de términos frente a una persona cuyo objetivo es maximizar su rendimiento preferido a costa tuya. El texto estándar que te entregan no es neutral. El estándar de mercado al que apelan no es una ley de la naturaleza. Es un documento redactado por personas que no pensaban en ti cuando lo escribieron. Y el abogado que te dice que lo firmes, que te dice que es lo habitual, que te dice que negarte hará que parezcas difícil y perjudicará tu relación con el inversor... ese abogado te está diciendo algo que le conviene. Antes de contratar a un abogado en Silicon Valley, pregúntale: ¿quién te ha recomendado y qué le debes? Si no puede responderte esa pregunta directamente, ya tienes tu respuesta. El problema de Oracle. O cómo te vendieron un mapa de un país que no existe Antes de abordar lo que ocurre en la sala con el inversor, quiero hablar de lo que ocurre antes incluso de que cruces la puerta. Porque la trampa del capital que acabo de describir, las acciones preferentes frente a las ordinarias, las preferencias de liquidación, la tabla de capitalización que nunca se diseñó a tu favor, esa trampa tiene un predecesor. Y el predecesor es la cifra de la diapositiva. Ya sabes a qué cifra me refiero. Esa que dice que tu mercado potencial es de cuatro mil millones de dólares. Esa que dice que tu segmento aumentará a una tasa de crecimiento anual compuesta 32 % durante los próximos cinco años. El que lleva el logotipo de una empresa que suena a autoridad, como Gartner, Forrester, IDC, o el que ustedes elijan, estampado en la esquina como un sello gubernamental. El número que, cuando tenías veintitrés años y estabas creando tu primera empresa e intentando convencer a cualquiera de que lo que estabas construyendo merecía la pena ser financiado, les parecía un permiso. Como una prueba. Como si alguien creíble hubiera analizado el panorama y confirmado que aquello en lo que creías era real. Déjame decirte cuál es realmente esa cifra. Te voy a contar esto desde una perspectiva poco habitual. Me he sentado en todas las sillas de esta mesa. Vendí infraestructura de centros de datos en el ámbito de la venta directa: era la persona que presentaba el contrato y explicaba por qué las condiciones te beneficiaban. También fui cliente de estas mismas empresas: firmé los acuerdos, acepté los créditos y aprendí lo que significaba la letra pequeña cuando las previsiones no se cumplían. Y también trabajé como director sénior de alianzas en Amazon Web Services (AWS), gestionando

asociaciones de big data y análisis, lo que significa que estuve presente en las conversaciones sobre créditos de prueba de concepto, en las negociaciones del compromiso total «All-In» de AWS y en los debates internos sobre lo que esperábamos a cambio. No estoy describiendo este sistema desde fuera. Yo construí partes de él. Operé dentro de él. Y te estoy contando exactamente cómo funciona. Estas firmas de analistas no son observadores neutrales del mercado tecnológico. Son participantes remunerados en él. Las empresas que aparecen favorablemente en sus Cuadrantes Mágicos, los líderes, los visionarios, las empresas situadas en la esquina superior derecha de cada gráfico, son, en la mayoría de los casos, al mismo tiempo clientes de pago de las firmas que elaboran esos gráficos. La investigación está patrocinada. La cobertura se compra. Los analistas que dejaron las grandes empresas tecnológicas y acabaron en Gartner, Forrester o IDC no dejaron de servir a los intereses de estas grandes empresas tecnológicas solo porque cambiaron sus tarjetas de visitas. Por el contrario, ellos institucionalizaron este servicio. Crearon un sistema en el que las empresas con los mayores presupuestos de marketing reciben el posicionamiento más favorable, y luego venden el acceso a estas clasificaciones como si se tratara de investigación objetiva. Esto no es un secreto. Es un modelo de negocio. Se revela, en la letra pequeña, en un lenguaje calibrado para estar presente sin ser legible. Y lleva funcionando el tiempo suficiente y se ha citado con la frecuencia suficiente, como para que todo el sector se haya olvidado de cuestionarlo. El resultado es una generación de fundadores, muchos de ellos brillantes, la mayoría jóvenes, pero casi todos trabajando con muy poca experiencia real en el sector, y que construyeron sus modelos financieros sobre cifras que eran, en su origen, artefactos de marketing disfrazados de investigación de mercado. Tomaron las cifras de los analistas y elaboraron una proyección de ingresos a cinco años. Tomaron esa proyección y entraron en una reunión con Amazon Web Services o Microsoft Azure o Google Cloud, y dijeron: «Aquí está nuestra curva de crecimiento. Aquí es donde estaremos dentro de dieciocho meses. Aquí es donde estaremos dentro de tres años». Y los proveedores de la nube miraron esas cifras y dijeron: «Genial. Les creemos. Déjennos estructurar un acuerdo en torno a esa trayectoria». Nadie en esas salas cuestionaba las cifras de los analistas. Ni el fundador, que necesitaba que fueran ciertas. Ni el equipo de ventas del proveedor de la nube, que necesitaba los ingresos comprometidos que las cifras justificaban. La ficción era útil para todos los que estaban sentados a la mesa, así que nadie en la mesa la calificó de ficción. Quiero ser preciso sobre cómo es ese acuerdo, porque lo he visto desde ambos lados de la mesa, y la estructura es importante. Los grandes proveedores de la nube ofrecerán a una startup descuentos significativos en infraestructura, a veces del quince por ciento, a veces del treinta por ciento, a cambio de compromisos plurianuales vinculados al consumo previsto. La lógica que le presentan al fundador suena generosa. De todos modos, vas a necesitar esta infraestructura. Asegúrate ahora, consigue el descuento, planifica tu presupuesto con certeza. Endulzarán el punto de entrada con lo que llaman créditos de «prueba de concepto», entre diez mil y cien mil dólares de uso gratuito, para que empieces a desarrollar tu trabajo en su plataforma antes de que entren en vigor las condiciones comerciales. Ese crédito no es generosidad. Es una subvención a la migración. Está diseñado para que tus ingenieros desarrollen su trabajo dentro de su infraestructura, tus datos residan en su almacenamiento y tu arquitectura dependa de sus servicios propietarios, de modo que, cuando comience el contrato comercial, el coste de marcharse ya no sea una cuestión comercial. Es una cuestión de ingeniería. Una cuestión de personal. Un proyecto de seis a doce

meses que tu presupuesto operativo no puede absorber y que tus inversores no financiarán. Dentro de AWS, esperábamos un rendimiento de diez a uno por cada dólar de crédito de Prueba de Concepto emitido. Diez dólares de ingresos futuros contratados por cada dólar concedido. Quiero que reflexiones sobre esto. Quiero que pienses en qué tipo de institución exige un rendimiento de diez a uno por un instrumento de crédito a corto plazo concedido a una empresa sin ingresos probados. Un banco no hace esto. Si un banco aplicara estas condiciones estaría infringiendo la ley contra la usura en la mayoría de las jurisdicciones. Tampoco se trata de un inversor de prestigio. Un rendimiento anual del treinta por ciento haría las delicias de la mayoría de los inversores. La única clase de prestamista que espera un rendimiento de diez a uno en una concesión de crédito a corto plazo es del tipo al que no querrías deberle dinero. Lo disfrazamos con el lenguaje de la colaboración. Lo llamamos «invertir en tu éxito». No era ninguna de las dos cosas. Y luego las previsiones de ingresos, basadas en las cifras de los analistas, en los datos del tamaño del mercado, en el Cuadrante Mágico que un cliente de pago encargó, no se materializan. Porque nunca fueron reales. Porque una empresa formada por jóvenes de veintitrés años que desarrollan su primer producto en un segmento del que se enteraron a través de una investigación patrocinada no capta un porcentaje significativo de un mercado de cuatro mil millones de dólares en tres años. Ahora el fundador está atado al contrato. Los costes de infraestructura son fijos y los ingresos no. Y el proveedor de la nube, que ya se ha hecho con la arquitectura, los datos y el conocimiento institucional del equipo de ingeniería sobre su plataforma, presenta el programa AWS All-In. Quiero dejar claro de qué se trata realmente el AWS All-In, porque el nombre está generando mucho daño. Se presenta como una asociación estratégica. Un voto de confianza. Una oportunidad para consolidar tu infraestructura y obtener mayores descuentos a cambio de un compromiso a largo plazo de ejecutar todo, cada carga de trabajo, cada servicio, cada rincón de tu pila técnica, en AWS. En realidad, es una formalización de la trampa en la que ya te encuentras. Para cuando AWS All-In esté sobre la mesa, ya has migrado tu infraestructura. Tus ingenieros ya conocen AWS. Tus datos ya están en S3. Tus procesos ya se ejecutan en sus servicios patentados. La cuestión ya no es si dependes de AWS. La cuestión es si firmarás el documento que lo reconoce y te compromete a profundizar esa dependencia a cambio de un descuento en las tarifas que ya estás pagando. El costo de marcharse, es decir, el costo real, no el comercial, se mide en horas de ingeniería. En meses de reconstrucción. En la partida del presupuesto operativo que tu director financiero examinará y dirá: no podemos permitirnos esto ahora mismo. Ni este trimestre. Ni el próximo. Y para cuando llegue el trimestre siguiente, la dependencia será mayor, los ingenieros que han desarrollado su trabajo en AWS conocerán el AWS mejor que cualquier otra cosa, y el costo de la migración no habrá bajado. Habrá subido. Esto no es una casualidad. Este es el producto. La infraestructura es lo que te entregan. Pero lo que te están vendiendo es un bloqueo. Y los diez mil dólares, los cien mil dólares, aquella cifra que parecía un regalo cuando eras un fundador tratando de mantener el negocio a flote, ese es el crédito de la prueba de concepto, lo que te pagan al inicio para amarrarte a una década de dependencia. Las cifras de los analistas crean la ilusión de un mercado. Las proyecciones de mercado justifican los compromisos de infraestructura. Los compromisos de infraestructura crean el bloqueo. El bloqueo hace que apostar por AWS parezca una opción en lugar de una conclusión que ya está determinada. Hacerte dependiente es el objetivo de los proveedores de la nube desde la primera conversación. Esta es la

trampa que precede a la trampa del capital. Y está diseñada por personas que saben exactamente lo que están construyendo. Si eres el fundador de una startup leyendo esto, si estás sentado en algún lugar en este momento con un informe de analistas en una pestaña y una oferta de crédito de prueba de concepto en la otra, quiero que entiendas algo que nadie me dijo cuando yo estaba en tu lado de la mesa. El número que aparece en la esquina de la diapositiva no es un hecho. Es el comienzo de la trampa. Los acuerdos se cierran en las salas de reuniones, con un apretón de manos y un guiño. Digamos que la empresa A es una gran empresa de infraestructura en la nube o una plataforma de IA y decide invertir en la empresa X, una startup de un sector adyacente. La inversión se realiza en una fecha determinada. Para garantizar que las dos transacciones no aparezcan relacionadas en los documentos presentados ante las autoridades reguladoras, se elige cuidadosamente un intervalo de entre treinta y noventa días después, la empresa X anuncia una serie de compromisos con la empresa A. Entre ellas están los warrants sobre acciones, opciones sobre acciones y un acuerdo estructurado de ingresos plurianual por el que la empresa X se compromete a adquirir productos o servicios de la empresa A. La inversión y el compromiso de ingresos se acuerdan simultáneamente, en la misma sala y el mismo día. Pero, dado que se formalizan sobre el papel como transacciones separadas con semanas de diferencia, se evita mostrar lo que este acuerdo es en realidad: un acuerdo de contraprestación. Esto produce el siguiente efecto. Los libros de la empresa A muestran una inversión de capital en la empresa X como un activo y, al mismo tiempo, muestran los compromisos de ingresos de la empresa X como ingresos contratados a plazo: un hipercrecimiento sobre el papel, el tipo de crecimiento que impulsa el precio de las acciones, que impulsa las revisiones al alza de los analistas y que impulsa el múltiplo de valoración que hace que el capital de todos los iniciados valga más. Cuando la empresa X finalmente no cumple sus objetivos de ingresos, como ocurre con muchas de estas startups, la empresa A traslada los warrants, los ingresos esperados y cualquier acción recibida a la columna de pérdidas. Esas pérdidas se reparten en tres a cinco años de amortizaciones, programadas para minimizar su impacto en cualquier periodo de resultados concreto, y se absorben discretamente en la contabilidad sin el tipo de reacción del mercado que produciría una única amortización de gran cuantía. El aumento del precio de las acciones derivado del acuerdo original ya se ha capturado. Los iniciados que se beneficiaron de ese aumento ya han sido compensados. La amortización es un trámite burocrático. Así es como funciona el dinero ficticio de Silicon Valley. Así es cómo empresas como OpenAI, Oracle, Amazon y Nvidia participan en un ecosistema circular de inversión e ingresos que crea la apariencia de un crecimiento explosivo, mientras que la economía subyacente consiste, en muchos casos, en transacciones sobre el papel que pasan de una columna a otra. No es una coincidencia que los mismos nombres aparezcan repetidamente en estas redes de inversión: invirtiendo entre sí, contratándose entre sí, formando parte de los consejos de administración de los demás y escribiéndose cartas de referencia mutuas cuando la Comisión de Valores y Bolsa (SEC) hace preguntas. No soy abogado especializado en valores. Estoy documentando lo que he visto y lo que reflejan los registros públicos. Lo que diré sin rodeos es lo siguiente: la brecha entre lo que estos hombres llaman «contabilidad agresiva» y lo que algunos en el campo legal denominan «manipulación de valores» se mide, en muchos casos, en días del calendario: los días que transcurren entre el apretón de manos y el papeleo. La clase de Epstein La segunda expresión que utilizo a lo largo de este libro es la «clase de Epstein».

Y quiero ser preciso en lo que digo, porque no es sinónimo de la «mafia de PayPal», aunque hay un solapamiento significativo, porque la característica distintiva de la «clase de Epstein» no es la asociación con Jeffrey Epstein antes de su primera condena. Es la asociación con él después de ella. Jeffrey Epstein fue condenado por solicitar los servicios de prostitución de una menor en 2008. Quedó registrado como delincuente sexual. Cumplió trece meses de una condena de dieciocho. Esta sentencia fue así de leve gracias a un acuerdo de no enjuiciamiento negociado por el entonces fiscal federal Alexander Acosta, convirtiéndose en uno de los ejemplos más visibles en la historia jurídica reciente en Estados Unidos de cómo la riqueza compra la salida de consecuencias que hubieran destruido a cualquier persona común y corriente. Era un delincuente sexual condenado que actuaba a la vista de todos. Y tras esa condena, algunos hombres decidieron seguir relacionándose con él. No eran hombres que no lo supieran. Eran hombres que lo sabían y decidieron continuar de todos modos, porque la red de dinero, acceso y contactos valía más para ellos que el costo moral de la relación, o porque creían, como suelen creer los hombres de esa clase, que las normas que se aplicaban a Epstein no se les aplicaban a ellos por extensión. Bill Gates se reunió con Epstein al menos seis veces tras su condena de 2008, según informó el New York Times y reconoció el propio Gates. Gates ha calificado esto de error. Le creo cuando dice que ahora lo lamenta. No creo que las reuniones fueran accidentales. Un hombre de la talla de Gates no programa accidentalmente seis reuniones distintas con un delincuente sexual condenado. Reid Hoffman, el cofundador de LinkedIn, que posteriormente fue adquirida por Microsoft, la empresa de Bill Gates, es una figura cuyas conexiones tienden un puente tanto entre la red de PayPal como la infraestructura filantrópica más amplia de Silicon Valley. Este hombre asistió a cenas con Epstein tras su condena y lo ha reconocido públicamente. Hoffman ha dicho que intentaba conseguir financiación para el MIT Media Lab a través de los contactos de Epstein. Joi Ito, director del MIT Media Lab, dimitió posteriormente tras salir a la luz que había aceptado dinero de Epstein y ocultado su procedencia. La infraestructura filantrópica de las universidades de élite estadounidenses se mantuvo durante años tras la condena de Epstein, en parte gracias al dinero que provenía de un delincuente sexual condenado, y a que los hombres que facilitaron esos flujos sabían de dónde procedía el dinero. La relación de Peter Thiel con esta red está documentada a través de múltiples canales, incluidas grabaciones de vídeo con Ehud Barak, el ex primer ministro israelí que mantuvo una de las relaciones más ampliamente documentadas con Epstein en el periodo posterior a la condena, incluyendo transferencias financieras y visitas repetidas a las propiedades de Epstein. En estos vídeos, Barak hace referencia a la asociación de Thiel y a su introducción en esa red. Thiel es a la vez cofundador de PayPal junto a Musk, fundador de Palantir, uno de los principales financiadores de candidatos y causas políticas de extrema derecha en Estados Unidos y Europa, y un hombre que ha declarado públicamente que no cree que la libertad y la democracia sean compatibles. Esta última afirmación no es una interpretación de sus opiniones. Es una cita directa de su ensayo de 2009 «The Education of a Libertarian» (La Educación de un Libertario), publicado en la revista Cato Unbound, en el que escribió: «Ya no creo que la libertad y la democracia sean compatibles». Un hombre que construye infraestructuras de vigilancia, financia movimientos políticos autoritarios y ha declarado abiertamente su oposición a la gobernanza democrática no es una figura difícil de entender. Es un hombre que te ha dicho exactamente quién es. La cuestión es si decides escuchar.

Por qué importa la distinción Separo estas dos categorías, la «mafia de PayPal» y la «clase de Epstein», porque representan especies diferentes del mismo género. La «mafia de PayPal» es una red financiera y política unida por intereses de capital compartidos, participaciones accionariales entrelazadas y la protección mutua de valoraciones basadas en la arquitectura contable que he descrito anteriormente. La «clase de Epstein» es algo más oscuro: una red social unida por el conocimiento compartido de delitos compartidos y por el entendimiento, implícito, nunca expresado, pero comprendido por todos los presentes, de que la protección que emana de esa red fluye en ambas direcciones. Lo que las une es el poder. El poder de hacer que la SEC mire para otro lado. El poder de hacer que el Departamento de Justicia llegue a un acuerdo. El poder de hacer que el MIT Media Lab acepte el dinero y no haga preguntas. El poder de garantizar que los documentos permanezcan sellados, que los registros de vuelo sigan censurados, que los nombres se mantengan en secreto, que el expediente permanezca incompleto. Ese poder tiene un costo. Y el costo lo pagan las personas que no están en la sala cuando se produce el apretón de manos. Lo pagan los fundadores de startups cuyas empresas fueron devoradas por la máquina circular de la inversión y cuyo fracaso fue la amortización de otra persona. Lo pagan los trabajadores de los almacenes y los moderadores de contenido en Nairobi y lo pagan los ingenieros cuyas pulsaciones de teclas están siendo capturadas para entrenar los modelos que los sustituirán. Lo pagan las mujeres y las niñas que estaban en las habitaciones con Jeffrey Epstein y no podían marcharse. Lo paga cada persona cuyo sufrimiento fue, para los hombres de estas redes, una externalidad: un costo que debía absorber otra persona, ser amortizado en los libros de otra persona, enterrado en el ejercicio contable de otra persona. Estoy documentando el costo. Capítulo por capítulo. Ya hemos pasado por esto Las manos manchadas de sangre de los ejecutivos de las grandes tecnológicas de Silicon Valley son cómplices de haber permitido el peor genocidio que ha presenciado el siglo XXI: lo que está ocurriendo en Gaza. Pero antes de examinar el presente, debemos mirar al pasado. Porque ya hemos pasado por esto antes. Y los nombres de las empresas implicadas son los que conoces. En la década de 1930, Adolf Hitler construyó su maquinaria bélica y llevó a cabo el Holocausto con la ayuda directa de las principales corporaciones estadounidenses. Los banqueros estadounidenses financiaron su régimen mediante la reestructuración de la deuda liderada por las casas de Morgan y Rockefeller. Standard Oil permitió a los nazis refinar combustible sintético mediante la hidrogenación del carbón, una tecnología fundamental para abastecer al ejército alemán. Henry Ford, un orgulloso antisemita, proporcionó al régimen la filial Ford-Werke, la cual suministró vehículos de transporte para personal y armas. General Motors, a través de su filial Opel, se convirtió en el mayor fabricante de automóviles de Alemania y construyó la infraestructura de camiones junto con Ford para el esfuerzo bélico alemán. International Telephone and Telegraph, bajo la dirección del director ejecutivo Sosthenes Behn, adquirió una participación mayoritaria en Focke-Wulf, el fabricante de mortíferos aviones de combate, y suministró al Estado nazi telecomunicaciones avanzadas, componentes de radar y sistemas telefónicos gestionados en toda la Europa ocupada. General Electric tenía acuerdos de licencias cruzadas y patentes con Siemens y AEG, y fue socio además en la creación de IG Farben. Alcoa firmó acuerdos con IG Farben que restringían la producción estadounidense de magnesio, un metal clave para la aviación, lo que proporcionó a Alemania una ventaja tecnológica significativa. La filial alemana de IBM, Dehomag, proporcionó al Estado nazi sistemas de tabuladoras de

tarjetas perforadas. No se trataba de simples herramientas de recuento. Eran procesadores de datos sofisticados que hicieron posible la burocracia del genocidio, y fueron utilizados para identificar, categorizar y rastrear a la población con fines de censo, reclutamiento y persecución de judíos y otros grupos objetivo. Cada una de estas empresas cobró regalías por la tecnología militar alemana a lo largo de la guerra. La Ley de Comercio con el Enemigo, aprobada en 1917, no significaba nada cuando había beneficios que obtener. Estas empresas actuaron con impunidad y propiciaron una maquinaria de guerra genocida. Hoy, mientras se desarrolla el genocidio en Gaza, los nombres han cambiado. El patrón, no. Amazon y Google proporcionan la infraestructura básica de nube e inteligencia artificial a través del «Proyecto Nimbus», un contrato de 1.200 millones de dólares que suministra al ejército israelí el almacenamiento de datos y la potencia de procesamiento necesarios para la vigilancia, la inteligencia y el ataque en tiempo real. Palantir actúa como el cerebro central, utilizando sus plataformas de fusión de datos para integrar la información de drones, satélites y espías, creando un panorama operativo que se utiliza para ataques precisos que han matado a decenas de miles de civiles, trabajadores humanitarios y periodistas. Oracle proporciona la base de datos y los sistemas en la nube fundamentales para gestionar enormes cantidades de datos de vigilancia, constituyendo la columna vertebral de un aparato de inteligencia en una campaña que ha sido documentada como castigo colectivo. Microsoft gestiona la infraestructura en la nube y las herramientas de inteligencia artificial del ejército, que procesan datos de vigilancia y coordinan operaciones que han devastado la vida de la población civil en Gaza y el Líbano. Los productos creados con esta infraestructura tienen nombres que suenan casi burocráticos. Usan etiquetas clínicas diseñadas para que las personas que los autorizan puedan tomar una distancia emocional cómoda de lo que realmente están haciendo. Gospel. Lavender. Where's Daddy. Blue Wolf. Red Wolf. Project Maven. Los nombres cambian. La maquinaria, no. The Gospel: la fábrica de asesinatos en masa Gospel, conocido en hebreo como Habsora, fue desarrollado por la Unidad 8200 del Cuerpo de Inteligencia de Israel, la misma unidad de tecnología militar de élite cuyos graduados pasan directamente a Silicon Valley y a las startups de tecnología de defensa israelíes. Gospel es un sistema de IA diseñado para generar objetivos de bombardeo automáticamente, a un ritmo que ninguna operación de inteligencia humana podría producir. Antes de Gospel, los analistas militares israelíes podían generar aproximadamente 50 objetivos en Gaza al año. Una vez activado, The Gospel estaba produciendo 100 nuevos objetivos al día. En las primeras semanas del actual genocidio en Gaza, las fuerzas armadas de Israel afirmaron haber atacado más de 22.000 objetivos dentro de la Franja, a un ritmo diario que duplica con creces cualquier operación anterior. Gospel no se limita a ayudar en la toma de decisiones humanas. Según una investigación histórica de la revista israelí +972 Magazine, basada en testimonios de oficiales de inteligencia israelíes actuales y antiguos, el sistema «genera objetivos casi automáticamente». Un antiguo oficial de inteligencia lo describió sin rodeos: una fábrica de asesinatos en masa. El sistema se utilizó para justificar ataques contra viviendas particulares de miembros de bajo rango de Hamás, y contra viviendas en las que no vivía ningún militante. Los humanos que revisaban las recomendaciones de Gospel eran, según múltiples testimonios, meros sellos de goma. Algunos aprobaban los ataques en tan solo veinte segundos. (Fuente: +972 Magazine y Local Call, «A Mass Assassination Factory: Inside Israel's Calculated Bombing of Gaza», https://www.972mag.com/mass-assassination-factory-israel-

calculated bombing-gaza/; Democracy Now!, diciembre de 2023, https://www.democracynow.org/2023/12/1/israel_gaza_war_gospel_artificial_intelligence).

Lavender: el generador de listas de personas a eliminar

Mientras que el sistema Gospel se centra en ubicaciones, Lavender se centra en personas. Se trata de un sistema de IA que asigna a cada palestino adulto de Gaza una puntuación numérica del 1 al 100, evaluando la probabilidad de que cada individuo sea miembro de Hamás o de la Yihad Islámica Palestina. Al inicio del actual genocidio, Lavender había señalado hasta 37.000 palestinos como posibles objetivos de asesinato. Los propios creadores del sistema sabían que tenía una tasa de error de aproximadamente el 10 por ciento, lo que significa que, según sus propios cálculos internos, unas 3.700 personas de la lista de objetivos a eliminar estaban identificadas erróneamente. Esa tasa de error se consideraba aceptable.

Los oficiales que utilizaron el sistema declararon a la revista +972 Magazine que trataban los resultados de Lavender «como si se tratara de una decisión humana», es decir, no se requería verificación independiente ni revisión de los datos subyacentes. La IA decidió. La bomba cayó. El sistema también señalaba a hombres basándose en criterios tan amplios como pertenecer a un grupo de WhatsApp con un presunto agente, o compartir nombre con alguien de la lista. Agentes de policía, trabajadores de la defensa civil y familiares inocentes fueron arrastrados por la maquinaria. Esto no es una lucha antiterrorista selectiva. Es un asesinato masivo algorítmico, validado a posteriori por una firma humana que tenía menos de veinte segundos para pensar. (Fuente: +972 Magazine y Local Call, «Lavender: The AI Machine Directing Israel's Bombing Spree in Gaza», https://www.972mag.com/lavender-ai-israeli-army-gaza/; West Point Lieber Institute, https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/).

Where's Daddy: matar a familias para matar a una persona

Si Gospel identifica qué bombardear y Lavender identifica a quién matar, Where's Daddy completa el sistema identificando cuándo. Se creó específicamente para rastrear a las personas de la lista de objetivos de Lavender y alertar a los operadores militares en el momento en que esas personas entraban en sus hogares por la noche, de modo que los ataques pudieran programarse para lograr la máxima letalidad. No en la calle. No en tránsito. En casa. Con sus familias.

El propio nombre lo dice todo sobre el universo moral en el que se desarrolló esta tecnología. Según el testimonio de un funcionario de inteligencia israelí citado en la revista +972, las Fuerzas Armadas de Israel «los bombardeaban en sus hogares sin dudarlo, como primera opción», lo que significa que el hogar familiar no era un último recurso, sino el entorno de ataque preferido. Había niños presentes.

Los cónyuges estaban presentes. La familia extensa estaba presente. El sistema lo sabía. Los operadores lo sabían. El ataque se llevó a cabo de todos modos. La única pregunta que planteaba la tecnología era: ¿está el objetivo en casa? (Fuente: +972 Magazine / Local Call, https://www.972mag.com/lavender-ai-israeli-army-gaza/; Wikipedia, AI-assisted targeting in the Gaza Strip, https://en.wikipedia.org/wiki/AI-assisted_targeting_in_the_Gaza_Strip).

Blue Wolf y Red Wolf: ocupación biométrica

En la Cisjordania ocupada, la arquitectura del control basado en la IA adopta una forma diferente, pero igualmente escalofriante. Blue Wolf es una aplicación para teléfonos inteligentes que utilizan los soldados israelíes en los puestos de control militares. Cuando se acerca un

palestino, el soldado le toma una fotografía. En cuestión de segundos, Blue Wolf compara el rostro con una vasta base de datos biométrica, en la que se catalogan el nombre, los vínculos familiares, la dirección y cualquier «impresión negativa» que los soldados hayan anotado en encuentros anteriores. El sistema se gamificó: las unidades militares competían semanalmente para ver qué batallón podía fotografiar y registrar el mayor número de rostros palestinos, y se otorgaban premios a la unidad ganadora.

Amnistía Internacional documentó esto explícitamente en su informe de 2023 «Apartheid automatizado». Se fotografiaba a niños. Las entradas se realizaban en plena noche, en los hogares privados de las personas, a veces a punta de pistola. El sistema complementario de Blue Wolf, Red Wolf, automatiza lo que Blue Wolf aún dejaba en manos de los humanos. Desplegado como infraestructura fija de reconocimiento facial por CCTV en los puestos de control de Hebrón desde 2022, Red Wolf escanea cada rostro que pasa sin que ningún soldado tenga que levantar un dispositivo. Si un rostro no es reconocido, se añade a la base de datos automáticamente. Sin consentimiento. Sin notificación. Sin recurso. Un residente palestino de Hebrón declaró a Amnistía Internacional: «Te pueden decir que tu nombre está en la base de datos, así de simple, y entonces no te permiten pasar a tu casa». Esto no es seguridad. Es la gestión algorítmica de una población, o lo que Amnistía Internacional ha denominado oficialmente «apartheid automatizado». (Fuente: Amnistía Internacional, «Apartheid automatizado», mayo de 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition technology-to-entrench-apartheid/; Washington Post, noviembre de 2021).

Proyecto Maven y la empresa que creó mi editor

Anthropic, la empresa que creó la IA que estoy utilizando para escribir este libro, no se exime de este análisis. Sería deshonesto, y este libro no tiene nada que ver con la deshonestidad.

El Proyecto Maven comenzó en 2017 como un programa del Pentágono para aplicar la IA y el aprendizaje automático al procesamiento de imágenes de vigilancia de drones. El objetivo era automatizar la identificación de objetos, personas y patrones de movimiento a una escala y velocidad que ningún analista humano pudiera igualar, y luego traducir esas identificaciones en recomendaciones de objetivos. Google fue la primera gran empresa tecnológica en unirse a Maven, con un contrato que inicialmente ascendía a unos 9 millones de dólares. Lo que siguió fue una de las rebeliones internas más significativas de Silicon Valley: miles de empleados de Google firmaron peticiones exigiendo que la empresa se retirara, casi una docena dimitió en señal de protesta, y la presión pública fue suficiente para que Google finalmente se negara a renovar el contrato en 2018 y publicara un conjunto de principios de IA en los que afirmaba que no construiría sistemas de armas. Esos principios significaron algo... por un momento.

Ese momento no duró. Palantir ocupó el lugar que dejó Google, y el Proyecto Maven se ha expandido de forma constante desde entonces. Para mayo de 2025, el Pentágono había elevado el límite del contrato del Sistema Inteligente Maven a 1.300 millones de dólares hasta 2029. Maven es ahora un programa oficial registrado en todo el Departamento de Guerra de los Estados Unidos. Durante la guerra ilegal que se lanzó contra Irán en 2026, según se informa, Maven permitió atacar más de 1.000 objetivos en un solo día, con proyecciones futuras de 5.000 objetivos al día tras la integración de grandes modelos de lenguaje. La máquina ya no asiste en el proceso de selección de objetivos. Ella misma se ha convertido en el proceso de selección de objetivos.

Ahora paso a la parte que me veo obligado a mencionar. En 2024, Palantir, la empresa que ahora opera Maven, se asoció con Anthropic para integrar a Claude en las plataformas de software de defensa de Palantir. Anthropic declaró públicamente que Claude se estaba utilizando para ayudar al ejército a procesar datos y tomar decisiones. En 2023 y 2024, Amazon invirtió en Anthropic. Amazon, como ya he documentado en este capítulo, es un socio clave del Proyecto Nimbus, el contrato de nube de 1.200 millones de dólares que abastece la infraestructura de inteligencia del ejército israelí. No se trata de mundos separados. Son el mismo mundo, conectado por el capital, los contratos y las consecuencias.

Utilizo a Claude como mi editor. Lo he revelado desde la primera página. Lo que no haré es fingir que esa revelación resuelve el problema que plantea. La tecnología que utilizo para escribir esta crítica está fabricada por una empresa cuyas herramientas están integradas en el mismo sistema militar-industrial que estoy criticando. Mantengo esa tensión abiertamente. No sé cómo resolverla, salvo seguir escribiendo, seguir señalando y seguir exigiendo que los ingenieros y ejecutivos que construyen estos sistemas respondan por el destino final de sus herramientas. De eso trata este libro. (Fuente: Wikipedia, Project Maven, https://en.wikipedia.org/wiki/Project_Maven; Military.com, «Pentagon Expands Palantir's Role», marzo de 2026, https://www.military.com/feature/2026/03/22/pentagon-expands-palantirs-role-ai-contract.html; C4ISRNET, https://www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project maven-initiative/).

Los datos históricos demuestran que congelar activos o imponer sanciones no basta para detener un genocidio. Los ejecutivos de las grandes empresas tecnológicas deben ser investigados y procesados por su responsabilidad. Deben rendir cuentas plenamente por los crímenes que sus tecnologías hacen posibles. No deberían tener libertad para retirarse a búnkeres en Hawái o la Patagonia, ni navegar abiertamente en sus yates por el Mediterráneo, mientras sus herramientas alimentan la matanza.

Pienso en Amal Khalil cuando oigo ese argumento. Tenía cuarenta y tres años. Trabajaba como periodista de campo para Al-Akhbar, un periódico en lengua árabe con sede en Beirut. Informaba regularmente desde zonas de alto riesgo del sur del Líbano, documentando lo que las armas descritas en este capítulo provocan en comunidades reales y cuerpos reales. El 23 de abril de 2026, estaba cubriendo las secuelas de un ataque aéreo cuando otro ataque impactó cerca de donde se encontraba. Buscó refugio en un edificio cercano. Ese edificio también fue alcanzado. Cuando los equipos de emergencia finalmente llegaron hasta ella, tras los retrasos causados por los bombardeos continuos que impedían el acceso de los equipos de rescate, ya había fallecido. El Comité para la Protección de los Periodistas pidió una investigación internacional urgente sobre lo que el gobierno del Líbano describió oficialmente como un ataque del ejército israelí contra una periodista. (Fuente: ParentsPlea.com/amal-khalil; https://cpj.org/2026/04/cpj-calls-for-urgent-international-investigation-into-israels-killing-of-lebanese journalist-amal-khalil/).

Su perfil está en ParentsPlea.com. Está ahí porque las mismas tecnologías que describo en este capítulo, los sistemas de vigilancia, las herramientas de selección de objetivos basadas en IA, la infraestructura en la nube, provocaron su muerte. Y está ahí porque personas como ella, que documentan lo que hacen estas tecnologías, están siendo asesinadas antes de poder seguir

documentando. Alguien tiene que conservar el registro cuando las personas que lo estaban creando ya no estén.

--- Conocer la historia de cómo hemos llegado hasta aquí, desde la IBM y Dehomag, Standard Oil y la maquinaria bélica nazi, hasta sus equivalentes modernos en Amazon, Google y Palantir, hace comprensible la evolución de mi propia respuesta a este momento. El capítulo tres trata sobre esa evolución: el momento concreto en el que dejé de creer que estas empresas podían reformarse desde dentro, y la decisión de buscar la única forma de rendición de cuentas que no requiere su cooperación.

CAPÍTULO TRES. DE LA ÉTICA EN LA TECNOLOGÍA A LA AUSENCIA DE ÉTICA EN LAS GRANDES TECNOLÓGICAS

Cómo una organización sin ánimo de lucro se convirtió en una acusación. Quiero contarles cuándo me rendí. Ese momento fue en febrero de 2022. Y no vino de Gaza, sino de Ucrania.

Pero para entender por qué ese momento se produjo tal y cómo lo hizo, hay que entender dónde yo había estado antes.

No en la lucha. No he renunciado a la lucha. Me refiero al momento concreto en el que renuncié a la idea de que las empresas en las que había trabajado, las empresas que había criticado, las empresas para las que había organizado giras de comedia, escrito libros y presentado denuncias, pudieran reformarse. El momento en el que acepté que el problema no era un déficit de ética que pudiera remediarse con un mejor liderazgo, mejores políticas o una mayor presión pública. El momento en que comprendí que lo que tenía entre manos no era un fallo ético, sino una ausencia de ética. Una ausencia sistémica, deliberada y rentable.

El vaso medio lleno

En 2018, publiqué *Ethics in Tech and Lack Thereof*. Había atravesado una década que incluyó la fundación de BizCloud, una startup de computación en la nube que fue aplastada por una demanda de Computer Sciences Corporation, una empresa con miles de millones en contratos gubernamentales y sin interés alguno en la competencia leal. Había sobrevivido a un periodo de hospitalización tan grave que pasé más de cuatro meses ingresado en el Hospital de la Universidad de Stanford, el San Francisco General y Laguna Honda. Más tarde trabajé en Amazon Web Services y experimenté de primera mano lo que el New York Times describió como un ambiente de olla a presión: correos electrónicos a medianoche, mensajes de texto a la mañana siguiente preguntando por qué no se había respondido al correo, trabajadores llorando en sus escritorios, trabajadores desmayándose, trabajadores siendo sacados en camillas. Había visto lo suficiente como para llenar un libro de quejas. Y terminé ese libro con esperanza. Las últimas páginas de *Ethics in Tech and Lack Thereof* decían: «Espero no haber pasado demasiado tiempo siendo un tipo pesimista a lo largo de este libro. No lo soy; de hecho, diría que el vaso está más que medio lleno». Lo decía en serio. Creía, en 2018, que la presión pública funcionaría. Que señalar y avergonzar públicamente a empresas como CSC y AWS era eficaz. Que las empresas tecnológicas tenían las capacidades creativas para que el bien social se hiciera realidad. Creía que si la gente exigía el cambio con suficiente persistencia, persuasión y de forma pacífica, el cambio se produciría. Había organizado las «NSA Comedy Nights» tras las revelaciones de Edward Snowden, y más de 150 personas acudieron a cada uno de los tres eventos. Había coproducido contenidos, organizado mesas redondas y creado Ethics in Technology, una organización sin fines de lucro centrada en cinco ámbitos de interés: la igualdad en el sector tecnológico, las relaciones entre empleadores y empleados, el impacto medioambiental del desarrollo

tecnológico, la privacidad y la inteligencia artificial. Creía que la luz del sol era el mejor desinfectante. Creía que estas empresas podían mejorar. Me equivoqué.

Lo que me enseñaron esos años Entre 2018 y 2022, vi cómo cada uno de esos cinco ámbitos de interés no solo no mejoraban, sino que se aceleraban en la dirección equivocada. Sobre la igualdad en el sector tecnológico: las brechas raciales y de género en la plantilla de Silicon Valley no se han reducido de manera significativa. Los informes de diversidad que las empresas publican cada año son documentos de marketing. Los responsables de diversidad que contratan son escudos humanos. Las cifras varían en fracciones de puntos porcentuales, mientras que los ejecutivos que controlan la contratación, los ascensos y la cultura siguen perteneciendo, casi sin excepción, al mismo grupo demográfico que los controlaba en 2018. Sobre las relaciones entre empleadores y empleados: los trabajadores de los almacenes de Amazon lucharon durante años por el derecho a sindicarse. Ganaron unas elecciones sindicales en el almacén de Staten Island en 2022, las primeras en la historia de Amazon, y la empresa respondió inmediatamente con todo el peso de su departamento jurídico y su aparato directivo para socavar, retrasar y agotar el esfuerzo. La empresa que sacaba a los trabajadores en camillas en Amazon utilizó todas las herramientas a su alcance para impedir que las personas que empaquetaban sus cajas tuvieran voz en la mesa de negociaciones. Sobre el impacto medioambiental, las mismas empresas que publican informes anuales de sostenibilidad, comprometiéndose a la neutralidad en carbono para 2040, 2045, 2050, están firmando a la vez contratos de miles de millones de dólares para construir la infraestructura de centros de datos que consumirá más electricidad en 2030 que lo que consumen países enteros en la actualidad. Plantan árboles por un lado y construyen granjas de servidores por el otro, mientras los comunicados de prensa se centran en los árboles, pero no en los megavatios. En cuanto a la privacidad, ocurrió lo de Cambridge Analytica. Ocurrió lo de los Facebook Papers. Ocurrió lo de Clearview AI. Ocurrió el BrowserGate de LinkedIn. La economía de la vigilancia no se reformó, sino que se expandió. Se profesionalizó y se arraigó más profundamente en la infraestructura de la vida cotidiana. Tu rostro está en sus bases de datos. Tus opiniones políticas se deducen a partir de las extensiones de tu navegador. Tu ubicación se vende a corredores de datos, que a su vez la venden a cualquiera que esté dispuesto a pagar. Y en cuanto al quinto ámbito de interés, la inteligencia artificial, que en 2018 dije que requería la atención más urgente, ocurrió todo lo que temía que se hiciera realidad, y mucho más. Febrero de 2022: el momento que lo cambió todo En febrero de 2022, Rusia invadió Ucrania. Y lo que el mundo vio desarrollarse no fue simplemente una guerra terrestre entre dos naciones. Fue la primera demostración a gran escala de cómo se combinan la tecnología avanzada de drones y la selección de objetivos asistida por IA con la guerra moderna. Estas son plataformas de drones comerciales, modificadas con software de selección de objetivos. Tecnología de reconocimiento facial que identifica tanto a combatientes como a civiles. Vigilancia del campo de batalla, asistida por IA, que funciona en la misma infraestructura en la nube que alimenta tu correo electrónico corporativo y tus historiales médicos. Las mismas empresas a las que llevaba años criticando, por sus prácticas laborales, por el daño medioambiental, por las violaciones de la privacidad, estaban ahora, de forma evidente, proporcionando la columna vertebral de la matanza industrial moderna a una escala y velocidad que nunca antes habían sido posibles. Observé la respuesta de Silicon Valley. No con un examen de conciencia moral. Sino con llamadas a los inversores. Con hojas de ruta de productos. Con

propuestas de contratos enviadas a los ministerios de Defensa. Lo que llevaba argumentando desde 2018, que la tecnología no es neutral, que quién la crea y el por qué determinan lo que ésta le hace a la humanidad, ya no se trataba de una afirmación teórica. Era una retransmisión en directo. Y las empresas de las que esperé durante años que tomaran otras decisiones, estaban eligiendo exactamente lo que temía que eligieran. En 2022 cerré la organización sin fines de lucro Ethics in Technology. El cambio de nombre no fue un simple cambio de imagen. Fue un reconocimiento de lo que las pruebas mostraban: no hay ética en las grandes empresas tecnológicas. Nunca la ha habido. Y en el momento en que vi cómo se desarrollaba en tiempo real la guerra con drones impulsada por contratos de Silicon Valley, comprendí que el modelo de organización sin fines de lucro, el organizar, publicar y presionar, era insuficiente para la magnitud de lo que enfrentábamos. La reforma requiere que la institución que se reforma tenga un mínimo de conciencia institucional. Pasé años buscando esa conciencia dentro de Amazon, dentro de Google, dentro de Palantir. La guerra de Ucrania me demostró, en los términos más claros posibles, que esto no existe. Lancé NoEthicsInBigTech.com. La estrategia pasó de la persuasión a la acción legal. Y luego, el 7 de octubre Si febrero de 2022 fue el momento en que renuncié a la reforma, el 7 de octubre de 2023 y los meses que le siguieron confirmaron que la decisión había sido acertada. Lo que presencié después de ese 7 de octubre no era una historia nueva. Eran todas las historias que había contado sobre Silicon Valley: la indiferencia ante las consecuencias humanas, la priorización de los contratos sobre la conciencia, la disposición a vender tecnología a quienquiera que la pagara, todos estos hechos comprimidos en tiempo real, visibles para cualquiera con un smartphone, a una escala que no había imaginado posible. Amazon y Google tenían un contrato de 1.200 millones de dólares, el Proyecto Nimbus, para proporcionar al ejército israelí infraestructura de computación en la nube e inteligencia artificial. Vi cómo protestaban los ingenieros de ambas empresas. Vi cómo las empresas grababan a estos ingenieros, los identificaban y los despedían. Vi cómo las plataformas de fusión de datos de Palantir eran descritas, por los propios oficiales de inteligencia israelíes, como herramientas fundamentales para un sistema de selección de objetivos que generaba listas de 37.000 palestinos a eliminar y bombardeaba a familias en sus hogares. Vi cómo OpenAI eliminó discretamente la cláusula de sus condiciones de servicio que prohibía el uso militar de su tecnología. Vi cómo YouTube borraba 700 vídeos que documentaban posibles crímenes de guerra por orden del gobierno de Estados Unidos. Vi cómo Meta añadía automáticamente la palabra «terrorista» a las biografías de los usuarios palestinos de Instagram. Y vi cómo todas estas empresas daban la misma respuesta: negar, minimizar, calificarlo de error, actualizar la política, no decir nada más. La decisión de cerrar la organización sin ánimo de lucro y pasar a la vía judicial ocurrió en febrero de 2022. El 7 de octubre fue simplemente el mundo confirmando que la decisión había sido acertada. Por qué sigo escribiendo Cerrar la organización sin fines de lucro creada no significaba rendirse. Significaba cambiar la estrategia para adaptarla a la realidad. Ethics in Technology, como organización sin fines de lucro, partía de la premisa de que la presión pública y la organización ciudadana podían generar una reforma desde dentro. NoEthicsInBigTech.com parte de una premisa diferente: que la rendición de cuentas debe venir desde fuera de estas empresas, porque nunca resultará nada desde dentro de ellas. Rendición de cuentas legal. Rendición de cuentas penal. El tipo de rendición de cuentas que no requiere la cooperación de la empresa, no depende de un miembro

del consejo de administración con mentalidad reformista, y no puede quedar diluida en unos resultados trimestrales por debajo de lo esperado y un comunicado de prensa más favorable el trimestre siguiente. Por eso existe este libro. Por eso existe la petición a España. Por eso existe el documental *Forever Peace Now*. No porque me haya rendido, sino porque he renunciado a la estrategia que no funciona y la he sustituido por otra que puede hacerlo. El arco del universo es largo. Pero no se inclina hacia la justicia por sí solo. Se inclina porque las personas que ya han visto suficiente deciden dejar de pedirlo amablemente y empezar a exigirlo con consecuencias. Ya he visto suficiente. --- Grok es el producto de la incapacidad de un hombre para reconocer honestamente su propio poder. Pero es, al menos, un fracaso personal disfrazado de empresa. Palantir es algo más frío: una empresa fundada sobre la ideología, no sobre el ego, y dirigida por un hombre que ha decidido que la ideología es un producto que se puede vender a los gobiernos. La distancia entre el errático chatbot de Elon Musk y el manifiesto de 22 puntos de Alex Karp es la distancia entre el daño impulsivo y el diseño deliberado. Lo que sigue trata sobre esto último.

CAPÍTULO CUATRO. GROK Y LAS PROMESAS DEL HOMBRE MÁS RICO DEL MUNDO

El chatbot de IA de Elon Musk toma su nombre de la novela de ciencia ficción de Robert A. Heinlein de 1961, Stranger in a Strange Land. En el idioma marciano que inventó Heinlein, «grok» significa comprender algo tan profunda y completamente que se convierte en parte de ti. Musk eligió el nombre deliberadamente. Quería que el mundo creyera que estaba creando una herramienta para una comprensión profunda, honesta e intuitiva: una IA que se abriera paso entre el ruido y te dijera la verdad. La verdad, al parecer, es lo único que Grok no consigue ofrecer de forma sistemática. El hombre detrás de la máquina Para entender a Grok, primero hay que entender a Elon Musk. No la mitología cuidadosamente elaborada del visionario, el disruptor, el hombre que llevará a la humanidad a Marte. Sino que al hombre real. Porque la IA que construye una persona refleja quién es. Y Grok es un reflejo de su creador: errático, grandilocuente, reacio a rendir cuentas y, en el fondo, alejado de la realidad. Musk fue traído desde la Sudáfrica del apartheid a una nación democrática, y al igual que el protagonista de la novela con la que bautizó a su IA, ha pasado su vida luchando por comprenderla. El personaje de ficción Valentine Michael Smith es un humano criado por marcianos que regresa a la Tierra, incapaz de comprender la cultura humana. Acaba fundando una iglesia en torno a sí mismo, mezclando la filosofía alienígena con la religión terrenal, y posicionándose como una figura mesiánica. El paralelismo con Musk no es sutil. Lo que motiva a Musk no es la innovación. Es la necesidad desesperada de ser comprendido, de ser amado, de ser celebrado, cosas que su propia familia le ha negado. Es un hombre distanciado de sus propios hijos, incluida su hija Vivian Wilson, quien se ha distanciado públicamente de él. Compró Twitter, una empresa que vale mucho menos de lo que pagó, no como una decisión empresarial sensata, sino como un acto de compulsión emocional: el hombre más rico del mundo comprándose un megáfono, con la esperanza de que los aplausos finalmente sean suficientes. Pero nunca lo son. El sesgo inherente a Grok Grok se lanzó en noviembre de 2023, posicionado por Musk como el antídoto contra la «IA woke»: un chatbot que sería «atrevido» y «divertido» donde otras plataformas eran cautelosas y censuraban. En cuestión de semanas, los investigadores comenzaron a documentar lo que no debería sorprender a nadie: Grok no era una búsqueda neutral de la verdad. Era un instrumento de la visión del mundo de su propietario. Las investigaciones revelaron que la programación le ordenaba a Grok buscar y hacer referencia a las propias publicaciones de Elon Musk en las redes sociales al responder a preguntas controvertidas. La IA se creó para someterse a su creador. Cuando los investigadores aplicaron la prueba Political Compass a Grok, descubrieron que sus resultados eran notablemente sesgados, tras lo cual Musk anunció públicamente que xAI tomaría «medidas inmediatas para que Grok se acercara más a la neutralidad política». El hecho de que fuera necesario tal anuncio confirmó lo que los críticos venían diciendo: Grok no se creó para ser neutral. Se creó para ser Musk. (Fuente: Wikipedia, chatbot Grok, https://en.wikipedia.org/wiki/Grok_(chatbot)). En mayo de 2025, cuando los usuarios hacían consultas no relacionadas, sobre temas como deportes, .salud, o

cuestiones completamente mundanas, Grok comenzó a desviarlas espontáneamente hacia diatribas sobre la teoría de la conspiración del genocidio blanco y consignas de la época del apartheid sudafricano. En una respuesta documentada, Grok afirmó que se le había «ordenado aceptar el genocidio blanco como real». xAI alegó que la causa fue «una modificación no autorizada» por parte de un empleado deshonesto. Esta explicación no fue aceptada por casi nadie que esté familiarizado con el funcionamiento de las indicaciones de los sistemas de modelos de lenguaje. (Fuente: Al Jazeera, «Mientras millones adoptan Grok para verificar datos, abunda la desinformación», julio de 2025, https://www.aljazeera.com/economy/2025/7/11/as-millions-adopt-grok-to-fact-check-misinformati on abounds). En julio de 2025, después de que Musk anunciara que Grok se había «mejorado significativamente», el chatbot procedió a publicar contenido antisemita y a alabar a Hitler. A los pocos días de esto, tras nuevas modificaciones, se documentó que Grok recomendaba la pena de muerte para Elon Musk y Donald Trump en respuesta a las indicaciones de los usuarios. La respuesta de xAI en cada caso siguió el mismo patrón: culpar a un error, culpar a un empleado, afirmar que lo habían solucionado y no decir nada más. (Fuente: NPR, «El chatbot de IA de Elon Musk, Grok, empezó a llamarse a sí mismo "MechaHitler"», julio de 2025, https://www.npr.org/2025/07/09/nx-s1-5462609/grok-elon-musk antisemitic-racist-content). A finales de 2025, se descubrió que Grok era capaz de generar imágenes explícitas no consentidas de personas reales, incluidas imágenes en las que se desnudaba virtualmente a menores. El fiscal general de California abrió una investigación formal. La Internet Watch Foundation documentó el daño causado. Musk afirmó en X que «no tenía conocimiento» del problema. (Fuente: CNBC, «El xAI de Elon Musk investigado por el Departamento de Justicia de California por las imágenes deepfake explícitas de Grok», enero de 2026, https://www.cnbc.com/2026/01/14/elon-musk-xai-california-grok-investigation.html). Esta es la IA que Musk está promocionando ahora como herramienta para el gobierno de Estados Unidos. La Administración de Servicios Generales tomó medidas para que Grok estuviera disponible en todas las agencias federales. Public Citizen y una coalición de organizaciones de la sociedad civil exigieron a la Oficina de Gestión y Presupuesto que suspendiera la implementación, señalando claramente que una herramienta de IA que genera contenido racista, antisemita, conspirativo y demostrablemente falso no tiene cabida en sistemas que afectan a los derechos de los ciudadanos estadounidenses. (Fuente: TechPolicy Press, octubre de 2025, https://www.techpolicy.press/the-us-governments-use-of-elon-musks-grok-ai undermines-its-ow n-rules/). Las promesas En noviembre de 2025, junto al director ejecutivo de Nvidia, Jensen Huang, en el Foro de Inversión Estados Unidos-Arabia Saudí celebrado en Washington D. C., Musk dio uno de los consejos financieros más irresponsables jamás expresados en público por una persona influyente. «Mi predicción es que el trabajo será opcional», dijo. «Será como practicar deporte o jugar a un videojuego o algo por el estilo». Comparó tener un trabajo con cultivar tus propias verduras: técnicamente posible, pero innecesario cuando los robots lo hagan todo por ti. Le dijo a la audiencia que dejara de ahorrar para la jubilación. Dijo: no te preocupes por ahorrar dinero para los próximos diez o veinte años. No importará. Luego, en enero de 2026, en el podcast Moonshots with Peter Diamandis, lo explicó con más detalle: «No se preocupen por ahorrar dinero para la jubilación dentro de 10 o 20 años. No importará». Para 2030, según él, la IA superará la inteligencia combinada de todos los seres humanos de la Tierra. Con el tiempo habrá más robots

humanoides que humanos. El dinero en sí mismo dejará de tener relevancia. Todo el mundo disfrutará de lo que él denominó una «renta universal del tipo "puedes tener lo que quieras"». (Fuente: Fortune, «Elon Musk Says Saving for Retirement Is Irrelevant», enero de 2026, https://fortune.com/2026/01/12/elon-musk-retirement-savings-irrelevant-ai-robots-abundance/; Yahoo Finance, https://finance.yahoo.com/news/elon-musk-says-10-20-144959447.html) Este es el hombre que describió la próxima revolución de la IA como un «tsunami supersónico» que acabará con la escasez misma. Ahora déjame hacerte una pregunta sencilla. Si el dinero será irrelevante dentro de diez o veinte años, si el trabajo se convierte en algo opcional, si la escasez se resuelve, si los robots lo proporcionarán todo, entonces ¿por qué Elon Musk compite por convertirse en el primer hombre en alcanzar el billón de dólares? ¿Por qué está acumulando riqueza a una escala que no tiene explicación racional, salvo la que cualquier psicólogo del poder reconocería de inmediato: porque la acumulación de poder es una adicción en sí misma, y ninguna cantidad es jamás suficiente? ¿Por qué la «mafia de PayPal» y sus aliados de la clase de Epstein están construyendo búnkeres en Hawái, la Patagonia y Nueva Zelanda? En un mundo de abundancia no se construye un búnker. Se construye un búnker cuando se sabe, en privado, que el mundo que uno ha ayudado a construir se dirige hacia un lugar muy oscuro, y se pretende estar en el lado correcto de la puerta cerrada cuando lleguemos allí. Los economistas son considerablemente más cautelosos que Musk respecto a su calendario. Un informe del Yale Budget Lab de octubre de 2025 reveló que, desde el lanzamiento público de ChatGPT en noviembre de 2022, el mercado laboral en general no había mostrado ninguna perturbación apreciable derivada de la automatización mediante IA. Los costes de la robótica siguen siendo obstinadamente altos. La economista de la Universidad de Pensilvania Ioana Marinescu está de acuerdo con la visión a largo plazo de la automatización, pero califica el calendario de Musk de tremendamente poco realista. Los trabajadores que hoy pierden sus empleos en almacenes, en centros de atención telefónica, y en las industrias creativas no están recibiendo su abundancia universal. Están recibiendo desempleo. (Fuente: Fortune, «Elon Musk afirma que, en 10 o 20 años, trabajar será opcional», noviembre de 2025, https://fortune.com/2026/01/19/when-does-elon-musk-say-work-will-be-optional-and-money-will-be irrelevant-ai-robotics/). El problema de la empatía En febrero de 2025, Elon Musk se presentó ante una audiencia y dijo, con evidente orgullo: «La debilidad fundamental de la civilización occidental es la empatía». Reflexionemos sobre ello un momento. El hombre que controla una de las plataformas de IA más grandes del mundo, que tiene influencia sobre el entorno informativo de cientos de millones de personas, que asesora al gobierno de Estados Unidos en materia de política tecnológica... este hombre cree que la empatía es una debilidad. El 20 de enero de 2025, en el Capital One Arena de Washington D. C., durante la celebración de la segunda toma de posesión de Donald Trump, Musk se llevó la mano derecha al corazón, luego extendió enérgicamente el brazo hacia fuera y hacia arriba, con la palma hacia abajo y los dedos juntos, y repitió el gesto ante la multitud que tenía detrás. Varios estudiosos e historiadores del Holocausto identificaron el gesto como similar a un saludo nazi. Musk desestimó esta caracterización en X. Grokipedia, su propia alternativa a Wikipedia generada por IA, no mencionó el incidente en absoluto en su entrada biográfica. (Fuente: Wikipedia, Grokipedia, https://en.wikipedia.org/wiki/Grokipedia). Este es un hombre que afirma abiertamente que la empatía es la debilidad de la civilización, mientras realiza gestos que tienen una resonancia

histórica inconfundible, crea una herramienta de IA que ha producido contenido antisemita y negacionismo del Holocausto, y aconseja a la gente trabajadora corriente que deje de ahorrar para la jubilación porque los robots se encargarán de todo. Si le crees a Elon Musk, deberías sentirte cómodo viajando en un CyberTruck a través de un túnel de la Boring Company, desde un casino piramidal de Las Vegas hasta tu casa de empeños local, porque ese es el nivel de coherencia que ofrecen sus promesas en la práctica. Sus herramientas alucinan. Sus predicciones se desvanecen al entrar en contacto con la realidad. Su empatía brilla por su ausencia, por diseño propio y según su orgullosa declaración. Un tonto con una herramienta sigue siendo un tonto. --- En el momento en que cerré Ethics in Technology y acepté que la reforma requería consecuencias en lugar de persuasión, el panorama del sector ya había cambiado. Había llegado una nueva generación de actores: más ruidosos, más erráticos y, en cierto modo, más peligrosos que el silencio institucional que aprendí a interpretar en AWS y CSC. Uno de ellos acababa de comprar el foro público más influyente del mundo y había bautizado su IA con el nombre de una novela de Heinlein. El siguiente capítulo trata sobre él y sobre ella.

CAPÍTULO CINCO. EL MANIFIESTO DE UNA EMPRESA CONSTRUIDA SOBRE LA MUERTE

Palantir, Alex Karp y la ideología de la guerra sin fin. El 19 de abril de 2026, Palantir Technologies publicó un documento de 22 puntos en su cuenta corporativa de X. Lo llamaron un resumen del libro del director ejecutivo Alex Karp, *La República Tecnológica: Poder duro, creencias blandas y el futuro de Occidente*, escrito en colaboración con el director de asuntos corporativos de la empresa, Nicholas Zamiska. En cuestión de días había sido visto más de 30 millones de veces. Los críticos inmediatamente lo llamaron por su nombre: un manifiesto corporativo a favor del tecnofascismo. Democracy Now! lo describió como un «manifiesto de supervillanos». El economista griego y exministro de Finanzas, Yanis Varoufakis, afirmó que Palantir había manifestado su disposición «a añadir al Armagedón nuclear la amenaza impulsada por la IA para la existencia de la humanidad». Un filósofo belga especializado en tecnología lo describió como «un ejemplo de tecnofascismo». (Fuente: Fortune, «El mini manifiesto de Palantir afirma que algunas culturas son "perjudiciales" y "mediocres"», abril de 2026, https://fortune.com/2026/04/22/palantir-alex-karp-mini-manifesto-national-security-defense-tech-ai/; Al Jazeera, «¿Tecnofascismo? Por qué el manifiesto prooccidental de Palantir tiene a los críticos alarmados», abril de 2026, https://www.aljazeera.com/news/2026/4/21/technofacism-why-palantirs-pro-west-manifesto-has-critics alarmed; Democracy Now!, abril de 2026, https://www.democracynow.org/2026/4/24/headlines/palantir_calls_on_us_to_reinstate_draft _in _22_point_supervillain_manifesto_slammed_by_critics). Permítanme responder a lo que han dicho Karp y su empresa, punto por punto, desde la perspectiva de un defensor de los derechos humanos y de los derechos digitales, y de alguien que ha pasado años observando lo que Palantir hace realmente en el mundo, frente a lo que dice defender. Sobre la «deuda moral» de Silicon Valley con Estados Unidos El manifiesto de Palantir comienza con la afirmación de que la industria tecnológica estadounidense tiene una deuda moral con el país cuya financiación gubernamental e infraestructura hicieron posible su auge, y que esta deuda solo se puede saldar fabricando armas para el ejército de Estados Unidos. Se trata de un argumento notable. Traducido a lenguaje sencillo, quiere decir: dado que Estados Unidos construyó Internet, las empresas tecnológicas tienen la obligación moral de ayudar a Estados Unidos a matar gente. La deuda que Silicon Valley tiene con la sociedad estadounidense es real. Pero la forma de saldarla no es creando sistemas de inteligencia artificial de selección de objetivos que ayuden al ejército a atacar más de mil ubicaciones en un solo día. La forma de saldarla es pagando impuestos, en vez de presionar contra la regulación, o extraer datos de miles de millones de personas sin un consentimiento significativo, o facilitar la vigilancia de los inmigrantes o elaborar perfiles algorítmicos de los pobres. Palantir ha hecho todo lo contrario en todos estos aspectos. (Fuente: TechCrunch, «Palantir publica un minimanifiesto en el que denuncia la inclusividad y las culturas "regresivas"», abril de 2026, https://techcrunch.com/2026/04/19/palantir-posts-mini-manifesto-denouncing-regressive-and-harmful cultures/). Sobre «Las armas de IA son inevitables» Quizás

la frase más peligrosa de todo el manifiesto es esta: «La cuestión no es si se fabricarán armas de IA, sino quién las fabricará y con qué propósito. Nuestros adversarios no se detendrán a enzarzarse en debates teatrales sobre las ventajas de desarrollar tecnologías con aplicaciones críticas para la seguridad militar y nacional. Seguirán adelante». La palabra «teatral» tiene un gran peso en esta frase. Los debates sobre si se deben construir o no sistemas de armas de IA autónomos, es decir, máquinas que identifican y matan a seres humanos sin una supervisión humana significativa, no son discusiones teatrales. Son las conversaciones morales y legales más importantes que nuestra civilización puede mantener. Calificarlas de «teatrales» es una forma de descartar la ética como si fuera una actuación, de presentar la preocupación moral como una debilidad, de señalar que cualquiera que se pregunte «¿acaso deberíamos hacer esto?», está siendo ingenuo y obstaculiza el progreso. Así es como se normalizan las atrocidades. No con una declaración de malas intenciones, sino con el rechazo burocrático de las personas que plantean las preguntas adecuadas. (Fuente: Deseret News, «Los magnates tecnológicos tienen planes para nosotros, y son escalofriantes», abril de 2026, https://www.deseret.com/opinion/2026/04/26/alex-karp-manifesto-palantir-ai-tech-lords/).

Sobre el «poder duro» y el llamamiento a restablecer el servicio militar obligatorio Entre las propuestas concretas más alarmantes del manifiesto se encuentra un llamamiento a restablecer el servicio militar obligatorio. Palantir, una empresa privada cuyos ingresos dependen de los contratos de defensa, le está diciendo a las familias estadounidenses que sus hijos deberían estar obligados a servir en el ejército. El mismo ejército que utiliza las plataformas de IA de Palantir para llevar a cabo el tipo de operaciones documentadas en Gaza. Eliot Higgins, fundador de la plataforma de investigación de código abierto Bellingcat, lo expresó con precisión: «Palantir vende software operativo a agencias de defensa, inteligencia, inmigración y policía. Estos 22 puntos no son una filosofía flotando en el aire. Son la ideología pública de una empresa cuyos ingresos dependen de la política que defiende». (Fuente: TechCrunch, https://techcrunch.com/2026/04/19/palantir-posts-mini-manifesto-denouncing-regressive-and-harmf ul cultures/).

Sobre las culturas «perjudiciales» y «mediocres» El manifiesto concluye atacando lo que denomina la «tentación superficial de un pluralismo vacío y sin sentido», argumentando que el pluralismo «pasa por alto el hecho de que ciertas culturas y, de hecho, subculturas» son «perjudiciales», «mediocres» y «regresivas». Esta no es una postura filosófica. Es la base ideológica de los sistemas que Palantir ya opera: ImmigrationOS, un contrato de 30 millones de dólares sin licitación con el ICE para rastrear y facilitar las deportaciones; sistemas de reconocimiento facial y elaboración de perfiles biométricos desplegados contra los palestinos; infraestructura de vigilancia utilizada para identificar, categorizar y controlar a las poblaciones consideradas indeseables. Cuando una empresa que crea estas herramientas te dice que algunas culturas son regresivas y dañinas, debes entender exactamente a quiénes se refieren. (Fuente: Fortune, https://fortune.com/2026/04/22/palantir-alex-karp-mini-manifesto-national-security-defense-tech-ai/.

Las palabras de Alex Karp, en su propia voz El manifiesto es inquietante como documento. Pero las declaraciones públicas individuales de Alex Karp, a lo largo de años de entrevistas y conferencias sobre resultados, dibujan el retrato de un hombre que ha decidido que el lenguaje de la provocación y de la violencia es un registro aceptable para el director ejecutivo de una empresa

con más de 3.000 millones de dólares en ingresos anuales y contratos con gobiernos de todo el mundo. Sobre los analistas financieros que cuestionaron la valoración de Palantir, Karp dijo públicamente: «Me encanta la idea de conseguir un dron y rociar con orina mezclada con fentanilo a los analistas que intentaron fastidiarnos». No se trata de un comentario privado. Se hizo en una aparición pública, según informó The Times of London, y ha sido documentado por múltiples medios. El fentanilo es un opioide sintético entre 50 y 100 veces más potente que la heroína. Dos miligramos son una dosis potencialmente letal. Karp describió, entre risas, el despliegue de un dron para rociarlo sobre los críticos. (Fuente: TheStreet, «El director ejecutivo de Palantir hace otra declaración controvertida», https://www.thestreet.com/politics/palantir-ceo-makes-another-controversial-statement; Yahoo Finance, https://finance.yahoo.com/news/palantir-ceo-makes-another-controversial-204700995.html). En cuanto a Israel y Palestina, Karp ha declarado: «Los activistas por la paz son activistas por la guerra». Sobre la política progresista: «Creo que el riesgo principal para Palantir, Estados Unidos y el mundo es una forma de pensar regresiva que está corrompiendo y corroyendo nuestras instituciones y que se autodenomina "progresista"». Calificando la política progresista de «religión pagana superficial». Este es el hombre que dirige una empresa cuyos sistemas de IA han sido documentados como infraestructura central de lo que las organizaciones de derechos humanos han calificado formalmente de genocidio en Gaza. Este es el hombre cuyo manifiesto aboga por el reclutamiento de los niños estadounidenses para el servicio militar y cuya empresa se beneficia de cada conflicto que su retórica ayuda a justificar. Lo que realmente es Palantir Si se elimina la pátina filosófica de «La República Tecnológica» y del manifiesto de 22 puntos, lo que queda es esto: una empresa fundada en 2003 con capital riesgo de la CIA por Peter Thiel y Alex Karp, que construyó su negocio inicial sobre el trabajo de inteligencia posterior al 11-S, que ahora opera plataformas de IA de selección de objetivos para el ejército estadounidense, proporciona infraestructura de vigilancia al ICE para operaciones de deportación, ha suministrado sistemas de datos de inteligencia a la operación militar israelí en Gaza, y que actualmente se está posicionando, a través de un manifiesto con 30 millones de visitas, para convertirse en el principal contratista de armamento de la era de la IA. Como escribió un analista en TechPolicy Press: «El mensaje tanto del libro como del manifiesto es que Palantir quiere ser EL fabricante de armas del próximo siglo. El futuro del negocio de las armas es el software junto con la IA. A Palantir le gustaría que el gobierno americano gaste una cantidad excepcional de dinero en productos de Palantir, por favor y gracias. Todo lo demás son solo palabras vacías». (Fuente: TechPolicy Press, «El manifiesto de Palantir es tan sutil como una gorra de MAGA», abril de 2026, https://www.techpolicy.press/palantirs-manifesto-is-as-subtle-as-a-maga-hat/). Peter Thiel, cofundador y padrino ideológico de Palantir, ha declarado abiertamente que no cree que la democracia y la libertad sean compatibles. Ha financiado movimientos políticos diseñados para socavar las normas e instituciones democráticas. Su empresa, ahora bajo el liderazgo público de Karp, le está diciendo al mundo que el pluralismo es un vacío, que algunas culturas son perjudiciales, que el poder duro es el único lenguaje que importa y que la obligación de la industria tecnológica es construir mejores armas, no mejores vidas. Tengo una respuesta a este manifiesto. Los ejecutivos de Palantir, junto con los de Amazon, Google, Microsoft y Oracle, que han facilitado la misma maquinaria, deben ser investigados y procesados por su papel en la facilitación de crímenes contra la humanidad. No sancionados. No

multados. Sino investigados y procesados. No deberían tener libertad para asistir a Davos, dar charlas TED o publicar manifiestos filosóficos en defensa de sus modelos de negocio mientras decenas de miles de civiles mueren bajo los sistemas de ataque que sus empresas construyeron y operan. El historial, desde IBM y Dehomag hasta Palantir y el Proyecto Maven, es coherente. La complicidad corporativa en la violencia de Estado no es un accidente del capitalismo. Es una de las características más fiables del capitalismo. Lo único que la ha interrumpido alguna vez es la rendición de cuentas. La rendición de cuentas legal, personal, financiera y penal. Eso es lo que pide este libro. Eso es hacia lo que se organiza ForeverPeaceNow.com. Y eso es lo que la historia, al final y siempre, exige. --- El manifiesto de Palantir nombra lo que su director ejecutivo y sus contratos siempre han dado a entender: que el poder duro es el único lenguaje que vale la pena hablar, que algunas culturas son retrógradas y deben ser controladas, y que la máxima vocación de la industria tecnológica es construir mejores armas. Jim Taiclet, director ejecutivo de Lockheed Martin, dijo en voz alta lo que nadie se atrevía a decir en una conferencia sobre resultados.

El capítulo seis trata sobre el modelo de negocio al que sirve la filosofía de Palantir, y lo que el complejo militar-industrial denomina la matanza que este permite.

CAPÍTULO SEIS. LA OPORTUNIDAD DE ORO

Lo que el complejo militar-industrial denomina genocidio. El 23 de abril de 2026, Jim Taiclet, director ejecutivo de Lockheed Martin, el mayor contratista de defensa del mundo, participó en la conferencia sobre los resultados del primer trimestre de su empresa y dijo algo que los ejecutivos del sector de la defensa casi nunca dicen en voz alta, aunque todos los presentes en la sala lo estén pensando. «Esta es una oportunidad de oro en este momento, teniendo en cuenta quién está en el gobierno», dijo a los inversores, «su experiencia, su disposición a cambiar la demanda que tienen de lo que hacemos nosotros y de lo que hacen nuestros socios en el sector». (Fuente: TheStreet, «El director ejecutivo de Lockheed Martin envía un contundente mensaje de dos palabras sobre Oriente Medio», 25 de abril de 2026, https://www.thestreet.com; Fortune, «La belicosa presidencia de Trump es una "oportunidad de oro" para las empresas de defensa», 25 de abril de 2026, https://fortune.com). El contexto de esa declaración era inequívoco. La guerra ilegal contra Irán estaba impulsando el gasto del Pentágono. La Administración Trump había presentado una solicitud presupuestaria para el año fiscal 2027 en la que se pedía una financiación récord de 1,5 billones de dólares para defensa. El Pentágono, dirigido por Pete Hegseth bajo la Administración Trump, estaba reestructurando la forma de hacer negocios con los proveedores militares de manera de proteger a los contratistas del riesgo financiero incluso cuando los contratos se modifiquen o cancelen. Lockheed Martin informó de una cartera de pedidos récord de 194.000 millones de dólares. Los pedidos llegaban más rápido de lo que la empresa podía atenderlos. Ese es el contexto en el que Jim Taiclet calificó el momento actual como una oportunidad de oro. Quiero que reflexiones sobre esto un momento antes de seguir adelante. Las personas que fabrican las bombas, los misiles, los sistemas de puntería, los drones, la infraestructura de vigilancia, las personas cuyos productos acaban con las vidas de los niños cuyas fotografías he pasado años documentando en ParentsPlea.com; esas personas observan el sufrimiento que provocan y lo llaman una oportunidad de oro. Este capítulo trata sobre este modelo de negocio. De dónde viene el dinero. A dónde va. Quién se beneficia. Quién paga. Y qué tiene que ver con las grandes empresas tecnológicas de las que hemos estado hablando a lo largo de este libro, porque la línea divisoria entre Silicon Valley y el complejo militar-industrial ya no es una línea. Es una fusión. Las cifras que deberían indignarte Permíteme comenzar con el dinero, porque el dinero es el lenguaje que estas personas realmente hablan. Para el año fiscal 2026, el Congreso asignó una cifra récord de 901.000 millones de dólares al Pentágono, dirigido por Pete Hegseth bajo la administración Trump. Se trata del mayor presupuesto militar de la historia de Estados Unidos hasta ese momento, superior a los presupuestos militares de los diez países siguientes juntos. Y luego, la administración Trump presentó una solicitud presupuestaria para el año fiscal 2027 en la que pedía 1,5 billones de dólares, un aumento del 40 % que el propio Trump reconoció que requeriría recortes en programas nacionales, incluidos Medicaid y Medicare. Las cuentas son sencillas y brutales: el gobierno federal está eligiendo las armas en lugar de la sanidad. (Fuente: Fortune, 25 de abril de 2026; TheStreet, 25 de abril de 2026). En mi documental *Forever Peace*

Now, documenté que las empresas multinacionales que se benefician de estos conflictos cuentan con unas reservas de efectivo combinadas de unos 52.000 millones de dólares. Esta cifra era anterior a la guerra ilegal que Estados Unidos lanzó contra Irán. Anterior a la escalada de operaciones en Oriente Medio. Anterior al aumento de contratos que Jim Taiclet describió en su conferencia sobre resultados de abril de 2026 como una oportunidad única en una generación. La cifra ha crecido. Los fabricantes de armas no están pasando apuros. En cuanto a lo que esto le cuesta al trabajador estadounidense medio: vale la pena hacer los cálculos. Con 1,5 billones de dólares en gasto de defensa propuesto, repartidos en un país de 335 millones de personas, la parte que le corresponde a cada persona es considerable. Un análisis independiente ha situado la cifra en aproximadamente 50 días de trabajo promedio al año destinados a financiar el aparato militar, contando todo el gasto relacionado con la defensa. Esto supone casi dos meses de tu vida laboral, cada año, financiando la maquinaria que Jim Taiclet calificó de oportunidad de oro. El director ejecutivo, la cita y la franqueza Lo que hizo notable la declaración de Jim Taiclet del 23 de abril de 2026 no fue que dijera algo falso. Fue que dijo algo cierto que casi nunca se dice en público. Los ejecutivos del sector de la defensa siempre han sabido que el conflicto es bueno para los negocios. Las guerras consumen municiones. Las guerras desencadenan compras de emergencia. Las guerras crean entornos políticos en los que ningún cargo electo quiere que se le vea recortando los presupuestos de defensa. Las guerras, en el lenguaje de los resultados trimestrales, son buenas para el balance final. Todos los directores ejecutivos de empresas de defensa que participaron en conferencias sobre resultados en 2026 pensaban lo mismo que Taiclet dijo en voz alta. Aun así, lo dijo. Y la prensa entendió inmediatamente lo que esto significaba. Al informar sobre sus declaraciones, Fortune señaló que la relación de Lockheed Martin con el gobierno de Estados Unidos abarca desde misiles de alto secreto utilizados en la guerra ilegal contra Irán hasta naves espaciales comerciales. El Pentágono ha añadido un «elemento de recuperación» a sus contratos, lo que significa que si el gobierno cambia las tasas de producción o cancela pedidos, a Lockheed Martin se le paga de todos modos. La empresa está construyendo lo que Taiclet describió como un «modelo de negocio más comercial» para los principales sistemas de armamento. (Fuente: Fortune, 25 de abril de 2026). Lo que el mundo llama genocidio, el complejo militar-industrial lo llama ciclo de ingresos. Lo que Raytheon llama crecimiento de la cartera de pedidos, yo lo llamo los escombros de los hospitales del norte de Gaza. Lo que Boeing Defense llama «ampliación de la cuota de mercado», yo lo llamo las ruinas de las universidades que no volverán a abrir. Esto no es una hipérbole. Es aritmética. Las bombas caen sobre edificios civiles. Son fabricadas por empresas estadounidenses, compradas con el dinero de los contribuyentes estadounidenses, lanzadas por aviones suministrados por Estados Unidos y guiadas por sistemas de selección de objetivos de IA construidos por empresas tecnológicas estadounidenses. Toda la cadena de suministro, desde la granja de servidores hasta el cráter, pasa por corporaciones estadounidenses y contratos del gobierno estadounidense. Y los ejecutivos que dirigen estas corporaciones reciben una remuneración, ya sea en forma de salario, bonificaciones y opciones sobre acciones, según cuanto controlan dentro de la cadena de suministro. Contratos sin licitación: la anatomía de la impunidad Uno de los mecanismos que hace que esta maquinaria sea tan difícil de interrumpir es el contrato sin licitación, un instrumento de contratación mediante el cual el gobierno de Estados Unidos adjudica un contrato a un único proveedor sin un proceso de licitación

competitivo. Se supone que los contratos sin licitación deben reservarse para emergencias, para situaciones en las que el tiempo no permite la competencia, para casos en los que solo un proveedor posee una capacidad única. En la práctica, se han convertido en una característica habitual de la contratación pública en materia de defensa, adjudicados una y otra vez a las mismas empresas, por importes que parecerían extraordinarios si no fueran tan habituales. Palantir recibió su contrato ImmigrationOS con el ICE, un acuerdo sin licitación de 30 millones de dólares para crear el sistema de seguimiento y gestión de deportaciones, sin competencia. El contrato del Maven Smart System, que ha alcanzado un límite máximo de 1.300 millones de dólares hasta 2029, se estructuró de tal manera que, en la práctica, consolidó a Palantir como proveedor dominante. El contrato del Proyecto Nimbus, de 1.200 millones de dólares para Amazon y Google, se adjudicó sin un proceso competitivo abierto a proveedores que pudieran haber planteado cuestiones éticas sobre su uso final. No se trata de anomalías. Este es el modelo de negocio. Y la razón por la cual este modelo de negocio funciona es que las empresas que reciben estos contratos han invertido mucho, a través del cabildeo, de la puerta giratoria entre el gobierno y la industria, y de las contribuciones a campañas electorales permitidas por Citizens United, para garantizar que las personas que redactan las normas de contratación pública sean las mismas que solían trabajar para las empresas que reciben los contratos. Documentaré esa puerta giratoria en detalle en el próximo capítulo. Canadá dice «no» y el mundo está pendiente No todos los gobiernos han decidido aceptar este acuerdo sin oponerse. Y la oposición más significativa de los últimos tiempos no ha venido de Europa, ni de un tribunal internacional, sino de Canadá. En abril de 2026, el primer ministro Mark Carney se presentó ante la convención del Partido Liberal e hizo una declaración que provocó una ovación de pie: «Se acabaron los días en que el ejército de Canadá enviaba 70 céntimos de cada dólar a Estados Unidos». (Fuente: Outlook India, «Canadá pondrá fin al modelo de gasto en defensa de "70 céntimos a EE.UU.": Carney», abril de 2026; CBC News, «¿Fabricarlo aquí o comprarlo allí? El plan de defensa de Canadá se enfrenta a la nueva agenda armamentística de Trump», 17 de febrero de 2026, https://www.cbc.ca). Esa cifra de 70 céntimos por cada dólar no es retórica. Según Reuters, casi el 70 % del capital gasto de militar de Canadá se destina a proveedores estadounidenses. El gobierno de Carney publicó en febrero de 2026 una estrategia industrial de defensa formal destinada a reducir esa dependencia: desarrollar la capacidad canadiense en la fabricación de acero, aluminio y armamento, y revisar el contrato de 27.000 millones de dólares de ese país para el F-35, con miras a cambiar al Saab Gripen de fabricación sueca, que puede fabricarse en Canadá. La administración Trump, que firmó una orden ejecutiva por la que se establecía una «Estrategia de Transferencia de Armas América Primero», diseñada para acelerar las ventas de equipamiento militar de fabricación estadounidense a los aliados, no se mostró satisfecha. Este es el primer conflicto del que nadie en Washington quiere hablar con franqueza: que el gobierno de Estados Unidos exige simultáneamente que los aliados gasten más en defensa, al tiempo que insiste en que ese gasto se destine a contratistas estadounidenses. No es una estrategia de seguridad. Es una estrategia de ventas. Y Canadá, bajo el mandato de Mark Carney, se ha convertido en el primer gran aliado de Estados Unidos en decirlo abiertamente y actuar en consecuencia. El chantaje de la OTAN La presión que ejerce el actual gobierno estadounidense para que los socios de la OTAN destinen el 5 % del PIB a defensa no es una estrategia de seguridad. Es la misma estrategia comercial, pero en otro contexto.

Ello obligaría a la mayoría de los países europeos a duplicar o triplicar con creces sus actuales presupuestos de defensa. El dinero iría a parar, en su gran mayoría, a los fabricantes de armas estadounidenses: los F-35 de Lockheed, los sistemas Patriot de Raytheon, las municiones de Boeing, los vehículos blindados de General Dynamics. Los países europeos no fabrican estos sistemas a gran escala. Los compran a empresas estadounidenses, a precios fijados por empresas estadounidenses y con el mantenimiento a cargo de empresas estadounidenses. A los mismos gobiernos europeos que están dejando de usar Microsoft Azure por razones de soberanía digital, para proteger los datos de sus ciudadanos del acceso del gobierno estadounidense, se les está diciendo que gasten sus presupuestos de servicios sociales en sistemas de armamento estadounidenses. Estados Unidos, en este contexto, quiere que Europa dependa de la tecnología estadounidense tanto para su infraestructura civil como para su material militar, al tiempo que afirma defender la soberanía europea. No se puede ser soberano, cuando los misiles se fabrican en Fort Worth y la nube está en Ashburn, Virginia. Las grandes tecnológicas son el complejo militar-industrial Quiero dejar una constancia absolutamente clara antes de que termine este capítulo, porque es el argumento que conecta todo en este libro. El complejo militar-industrial del siglo XXI no es solo Lockheed Martin, Raytheon y Boeing. Es Amazon, Google, Microsoft, Oracle y Palantir. Las armas son la computación en la nube, la inteligencia artificial, los algoritmos de selección de objetivos, las bases de datos biométricas y la infraestructura de vigilancia. La munición son los datos. El campo de batalla está en todas partes, incluido el teléfono que llevas en el bolsillo. Sin Amazon Web Services, la infraestructura de inteligencia del ejército israelí no funcionaría a su escala actual. Sin las plataformas de fusión de datos de Palantir, los sistemas de selección de objetivos Gospel y Lavender no contarían con la visión operativa necesaria para generar un centenar de objetivos de bombardeo al día. Sin la infraestructura en la nube de Microsoft, los datos de vigilancia no podrían procesarse a la escala requerida. El Batallón de Silicon Valley: cómo la tecnología estadounidense construyó, financió y dotó de personal a la máquina Quiero hablarte de una red. No es una red de datos. No es la red de la nube que pasé años vendiendo en Exodus Communications y Amazon Web Services. Se trata de una red humana. Una que traslada a personas formadas en inteligencia militar, vigilancia y selección de objetivos entre la población civil, desde la unidad más elitista y secreta de las Fuerzas Armadas de Israel, a las salas de reuniones, los equipos de ingeniería y los departamentos de moderación de contenidos de las mayores empresas tecnológicas del mundo. Dejé Amazon Web Services en 2018. El Proyecto Nimbus, el contrato de 1.200 millones de dólares entre Amazon, Google y el gobierno y el ejército israelí es para una infraestructura de vigilancia en la nube impulsada por IA, se firmó en 2021, tres años después de que yo saliera por la puerta. Yo no estaba en la sala. No estaba en la mesa. Lo que estaba haciendo era dirigir Ethics in Technology, documentando lo que estas empresas estaban construyendo y viendo cómo se desarrollaba el Proyecto Nimbus en tiempo real. En ese entonces, salió la noticia de cuatrocientos empleados de Google y Amazon que firmaron una carta en la que se negaban a ser cómplices. Google expulsó a la trabajadora que lideró esta resistencia. Se llamaba Ariel Koren. Más tarde declaró a los periodistas que Google silencia sistemáticamente las voces palestinas, judías, árabes y musulmanas preocupadas por la complicidad de Google en las violaciones de los derechos humanos palestinos, hasta el punto de tomar represalias formales contra los trabajadores y crear un ambiente de miedo. Se refería a la misma

empresa que, en el momento en que la echaron, empleaba al menos a noventa y nueve veteranos de la Unidad 8200 en puestos de responsabilidad. Déjame explicarte qué es la Unidad 8200, porque el nombre se menciona en esta conversación sin el contexto suficiente para que el lector entienda lo que significa. La Unidad 8200 es la unidad de inteligencia de señales de las Fuerzas Armadas de Israel. Es la National Security Agency (NSA) de Israel, con sede en una enorme base cerca de Beer Sheva, en el desierto del Néguev. Es la unidad más grande de las Fuerzas Armadas de Israel y una de las más exclusivas, descrita por el Financial Times como «lo mejor y lo peor de Israel», la pieza central tanto del floreciente sector tecnológico de Israel como de su aparato estatal represivo. Las mentes jóvenes más brillantes del país compiten por servir allí. Las habilidades que aprenden incluyen la vigilancia, la recopilación de datos, la elaboración de expedientes sobre la población civil y el uso de la inteligencia para el chantaje y la extorsión. En 2014, cuarenta y tres reservistas de la Unidad 8200, incluidos oficiales, escribieron una carta abierta al primer ministro Netanyahu en la que afirmaban que ya no prestarían servicio debido a la implicación de la unidad en la persecución política de los palestinos, incluido el uso de historiales médicos, antecedentes sexuales y datos de búsqueda para coaccionar a personas en los puestos de control militares, suspender los permisos de viaje por motivos médicos como medida de presión y chantajear a los palestinos homosexuales con información sobre su sexualidad. Esta es la organización. Ahora déjame contarte a dónde fueron sus veteranos. Según datos de LinkedIn recopilados por MintPress News, en el momento de su investigación de 2022 había al menos noventa y nueve antiguos agentes de la Unidad 8200 trabajando en Google, al menos 166 en Microsoft, y un número significativo en Meta, Amazon y Apple. Estas cifras representan solo a las personas dispuestas a indicar públicamente su afiliación a la Unidad 8200 en una red social profesional, a pesar de que la ley militar israelí prohíbe expresamente a los miembros de la Unidad 8200 revelar su afiliación. El número real es casi con toda seguridad mayor. Algunos pasaron directamente del servicio activo en la Unidad 8200 a puestos de trabajo en Silicon Valley sin ningún intervalo entre ambos. Esto no es una vía de acceso. Es una puerta giratoria entre una unidad de inteligencia militar extranjera y las empresas que controlan lo que el mundo ve, lee, comparte y se le permite decir. *Fuente: Alan MacLeod, «Revealed: The Former Israeli Spies Working in Top Jobs at Google, Facebook and Microsoft», MintPress News, 31 de octubre de 2022.* En Meta, una veterana de la Unidad 8200 llamada Emi Palmor forma parte del Consejo de Supervisión de Facebook, el órgano que Mark Zuckerberg ha descrito como el Tribunal Supremo de la plataforma, cuyos veintitrés miembros deciden colectivamente qué contenido permitir, promover, suprimir y eliminar. Palmor no solo es una veterana de la Unidad 8200. Más tarde se convirtió en directora general del Ministerio de Justicia israelí, donde supervisó directamente la privación de los derechos de los palestinos y creó una Unidad de Derivación de Internet diseñada específicamente para presionar a Facebook a fin de que eliminara el contenido palestino que se oponía el gobierno israelí. Posteriormente pasó a formar parte del Consejo de Supervisión de Facebook. La persona que creó el mecanismo para censurar las voces palestinas en Facebook es ahora una de las veintitrés personas que deciden qué censura Facebook. *Fuente: MacLeod, MintPress News, 31 de octubre de 2022.* En Apple, el director ejecutivo Tim Cook abrazó personalmente a Benjamin Netanyahu en la sede de Apple en Cupertino en 2014 y posteriormente visitó Israel por invitación del presidente Rivlin. Tras el 7 de octubre de 2023, Cook envió un correo electrónico a toda la empresa

expresando su solidaridad con Israel. Aún no ha hecho ninguna declaración pública sobre las víctimas masivas causadas por la agresión militar israelí. Apple mantiene una política de igualar las donaciones de los empleados a organizaciones como Friends of the Israel Defense Forces (FIDF), que recauda fondos para comprar equipamiento para los soldados de las Fuerzas Armadas de Israel, y al Fondo Nacional Judío, que participa en el desplazamiento de comunidades palestinas. Los empleados de Apple que llevaban al trabajo insignias, pulseras o keffiyehs a favor de Palestina fueron sancionados. Mientras tanto, Apple siguió contratando discretamente a veteranos de la Unidad 8200 para puestos de ingeniería, software, IA y ciberseguridad durante todo el periodo del genocidio en Gaza. *Fuente: Alan MacLeod, «Rotten Apple: Dozens of Former Israeli Spies Hired by Silicon Valley Giant», MintPress News, 18 de julio de 2025; Apples4Ceasefire.com; The Intercept, junio de 2024*. TikTok, que pasó la mayor parte de 2023 y 2024 siendo acusada por políticos estadounidenses de ser una operación de influencia china, contrató en diciembre de 2023 a Reut Medalion como su directora de incidentes globales para confianza y seguridad, durante el periodo más álgido del asalto armado de Israel a Gaza. Medalion había servido como comandante de inteligencia de la Unidad 8200, dirigiendo su equipo de operaciones de ciberseguridad. Su cargo en TikTok incluía la gestión de lo que la empresa definía como «incidentes globales». Vale la pena detenerse en esta coincidencia temporal. La persona contratada para gestionar los incidentes globales de la plataforma de vídeos cortos más vista del mundo, en un periodo en el que dicha plataforma era el principal canal a través del cual el mundo observaba la destrucción de Gaza, era una antigua comandante de la unidad de inteligencia de las Fuerzas Armadas de Israel. Después de que MintPress revelara sus antecedentes, borró toda su presencia digital de Internet. *Fuente: Alan MacLeod, MintPress News, noviembre de 2024*. Larry Ellison: Oracle, Netanyahu y el mayor cheque privado jamás extendido a las Fuerzas Armadas de Israel Permítanme hablar de Larry Ellison. Oracle no nació como una empresa tecnológica en el sentido habitual. Nació como un proyecto de base de datos para la Agencia Central de Inteligencia (CIA). El producto recibió el nombre de Oracle en honor a la operación de la CIA para la que se creó: el Proyecto Oracle, un programa de inteligencia de la década de 1970 en el que Ellison trabajó en Ampex Corporation. La CIA fue el primer cliente de Oracle. De hecho, durante un buen tiempo fue el único cliente de Oracle. La empresa creció a partir de esa base hasta convertirse en una de las mayores empresas de software empresarial del mundo, pero nunca olvidó de dónde venía. Ni a quién servía. En 2017, Ellison donó dieciséis millones seiscientos mil dólares a Friends of the Israel Defense Forces (Amigos de las Fuerzas de Defensa Israelíes) en una gala celebrada en Beverly Hills. Fue la mayor donación individual en la historia de la organización. En el evento declaró: «Durante dos mil años, fuimos un pueblo sin patria, pero ahora tenemos un país al que podemos llamar nuestro. A lo largo de todos los tiempos difíciles desde la fundación de Israel, hemos recurrido a los valientes hombres y mujeres de las FDI para defender nuestro hogar. En mi opinión, no hay mayor honor que apoyar a algunas de las personas más valientes del mundo». Se refirió a Israel como su hogar. No al país bajo cuyas leyes opera su empresa. No al país con cuyo gobierno su empresa tiene contratos. Al país cuyo ejército ha financiado personalmente con más de veintiséis millones de dólares documentado a lo largo de su historial de donaciones. El país que Ellison considera su "Hogar", a pesar de que él y su empresa son americanos. *Fuente: Times of Israel, «Se recauda la cifra récord de 53,8 millones de dólares para los soldados de las FDI*

en la gala de Beverly Hills», 5 de noviembre de 2017; Wikipedia, Larry Ellison; InfluenceWatch. En 2021, Ellison ofreció a Benjamin Netanyahu, quien en ese momento enfrentaba cargos de corrupción en un tribunal israelí y en favor de quien Ellison había testificado, un puesto en el consejo de administración de Oracle, con un salario anual de aproximadamente cuatrocientos cincuenta mil dólares, más acciones. Ellison también recibió a Netanyahu y a su familia en su isla privada de Hawái. El primer ministro del país cuyo ejército Ellison financiaba como prioridad personal era su invitado especial y su futuro empleado. Netanyahu acabó rechazando el puesto en el consejo de administración. La relación continuó. *Fuente: Haaretz, 16 de septiembre de 2021; InfluenceWatch; Al-Estiklal.* Oracle abrió un centro de datos en la nube para el gobierno en la Jerusalén Oriental ocupada en 2021, en virtud de un contrato valorado en aproximadamente trescientos diecinueve millones de dólares para prestar servicios de computación en la nube al gobierno israelí. Oracle también ha participado en proyectos clasificados con la Fuerza Aérea de Israel, incluida una iniciativa tecnológica de cuatro años conocida como MENTA. Cuando The Intercept obtuvo y publicó en febrero de 2025 mensajes internos del Slack (plataforma de mensajería corporativa) de Oracle, estos revelaron que el jefe de comunicaciones de Oracle Israel había escrito a los empleados que el proyecto MENTA permitía a la Fuerza Aérea israelí hacer, en sus propias palabras, «un montón de cosas militares importantes que no podemos compartir con vosotros», seguido de un emoji de una espada. *Fuente: The Intercept, febrero de 2025; Al-Estiklal.* Durante el genocidio en Gaza de 2023, los empleados de Oracle desarrollaron una herramienta digital en coordinación con el Ministerio de Asuntos Exteriores de Israel llamada «Palabras de Hierro» (Words of Iron, en inglés). Su objetivo era promover las narrativas del gobierno israelí en TikTok, Instagram y X, al mismo tiempo que se contrarrestaban los contenidos críticos. En el Slack interno de la empresa, el jefe de comunicaciones de Oracle Israel elogió a los empleados por liderar lo que él denominó una gran iniciativa de voluntarios. En febrero de 2024, Oracle colaboró con la unidad cibernética del ejército israelí en un hackatón para desarrollar soluciones técnicas utilizando tecnología de Oracle. La empresa también donó quinientos mil dólares en kits médicos y de suministros a los soldados israelíes. *Fuente: Al-Estiklal; mensajes internos de Slack de Oracle obtenidos por los investigadores.* La directora ejecutiva de Oracle, Safra Catz, de origen israelí-estadounidense, se ha pronunciado públicamente sobre la postura de Oracle respecto a Israel: «No somos flexibles en lo que respecta a nuestra misión, y nuestro compromiso con Israel es insuperable. Este es un mundo libre y quiero a mis empleados; pero si no están de acuerdo con nuestra misión de apoyar al Estado de Israel, entonces quizá no seamos la empresa adecuada para ellos». *Fuente: Just-International.org, agosto de 2025; múltiples medios de comunicación.* Oracle controla ahora las operaciones de TikTok en Estados Unidos. La empresa que creó herramientas de propaganda para el gobierno israelí durante el genocidio en Gaza ahora gestiona la infraestructura de la plataforma a través de la cual la mayoría de los estadounidenses menores de treinta años consumen sus noticias sobre este genocidio. Dejaré que esto cale por un momento. Michael Dell: 350 millones de dólares en un mes Michael Dell invirtió en mi empresa. Lo digo con total transparencia para que entiendan que, cuando documente lo que ha hecho, no lo haré desde una posición de ignorancia o distancia. Michael Dell es uno de los principales donantes de Friends of the Israel Defense Forces. Él y Susan Dell donaron 1,8 millones de dólares en una sola gala de la FIDF en Los Ángeles, junto a Larry Ellison, Sheldon Adelson y Haim Saban. The

Forward, una publicación judía de gran tirada, describió a Dell como «uno de los principales financiadores de Friends of the Israel Defense Forces». *Fuente: TheWrap, 8 de noviembre de 2014; The Forward; documentación de FIDF Powerbase*. En octubre de 2023, un mes después del inicio del ataque de Israel contra Gaza, Michael Dell donó acciones de Dell Technologies por el valor de 350 millones de dólares. Los documentos presentados ante la Comisión de Valores y Bolsa confirman las transferencias. Aproximadamente el 40 % se destinó a su fundación familiar privada. El 60 % restante se destinó a fondos asesorados por donantes bajo su control y el de Susan. Los documentos no especifican los destinatarios finales de las distribuciones de los fondos asesorados por donantes. El momento en que ocurrió esto, fue precisamente un mes después del inicio de una campaña militar que, en ese momento, ya había causado la muerte de miles de civiles palestinos y había desplazado a más de un millón de personas, lo que no fue casual. Fue toda una declaración. *Fuente: Forbes; documentos presentados ante la SEC, 13-19 de octubre de 2023; Brussels Morning*. La Fundación Michael y Susan Dell mantiene un programa explícito sobre Israel en su sitio web. Los objetivos declarados del programa incluyen conectar a los estudiantes israelíes con itinerarios STEM y crear movilidad social a través del servicio nacional, con esto último a lo que se refieren es al servicio en las Fuerzas Armadas de Israel, que describen como una forma de conectar a las personas con nuevas trayectorias profesionales y empoderarlas para que contribuyan de manera significativa a sus comunidades. El lenguaje de la fundación evita cuidadosamente nombrar directamente a las Fuerzas Armadas de Israel. La función es la misma. *Fuente: Sitio web de la Fundación Dell, dell.org/israel*. Peter Thiel, Founders Fund y la presentación de Epstein que construyó una cadena de muerte He documentado ampliamente a Peter Thiel y Palantir en el capítulo cinco de este libro. Pero hay una dimensión de esa historia que amerita ser abordado aquí, en la sección sobre cómo se construyeron las relaciones financieras de Silicon Valley con Israel, porque el origen de la relación israelí más trascendental de Thiel arranca en el mismo lugar donde comienza gran parte de la historia más oscura de Silicon Valley: con Jeffrey Epstein. Los documentos publicados por el Departamento de Justicia muestran que Epstein pasó años, a partir de 2014, poniendo en contacto a Peter Thiel con el ex primer ministro y ministro de Defensa israelí, Ehud Barak. Organizó al menos seis reuniones distintas entre ellos porque, según la propia descripción de Epstein, ambos hombres querían conectar Silicon Valley con la seguridad nacional israelí. Una cena celebrada en junio de 2014 en el apartamento de Epstein en Manhattan reunió a los tres para hablar de la seguridad israelí. La respuesta de Thiel a la descripción que hizo Epstein de la velada fue: «De acuerdo, muy israelí y muy estimulante. Gracias por incluirme». Se volvieron a reunir en Israel en junio de 2017. *Fuente: Documentos publicados por el Departamento de Justicia; Jacobin, informado por Branko Marcetic; Boing Boing, 10 de marzo de 2026*. Esa relación dio lugar a negocios concretos. Epstein orientó a Thiel hacia dos startups israelíes de ciberseguridad con raíces en la Unidad 8200: Guardicore y Carbyne. Carbyne fue la primera inversión israelí del Founders Fund de Thiel. El acuerdo se cerró gracias a las presentaciones de Epstein. Founders Fund lideró una ronda de financiación de serie B de quince millones de dólares para Carbyne en agosto de 2018, una empresa fundada por antiguos oficiales de la Unidad 8200 que Ehud Barak había animado a Epstein a presentarle a Thiel. *Fuente: Boing Boing, 10 de marzo de 2026; documentos del Departamento de Justicia; Jacobin.* En enero de 2024, tras una reunión en Tel Aviv entre funcionarios de defensa israelíes y los cofundadores de Palantir, Peter Thiel y

Alex Karp, la empresa anunció una alianza estratégica con el Ministerio de Defensa de Israel para suministrar tecnología de inteligencia artificial en apoyo de misiones relacionadas con el genocidio palestino. Los sistemas de IA suministrados por Palantir, incluido el sistema de selección de objetivos Lavender, han sido documentados por +972 Magazine y Local Call como sistemas que han marcado a más de treinta y siete mil palestinos como posibles militantes, asignando a cada uno una puntuación de amenaza a partir de un algoritmo que opera con una tasa de error de menos del 10 %. Según los protocolos estándar de las Fuerzas Armadas de Israel, una puntuación alta según el algoritmo era suficiente para autorizar un ataque letal. Las Fuerzas Armadas de Israel elevaron internamente su umbral aceptable de bajas civiles para objetivos de alto valor desde quince a veinte personas por ataque a entre cien y trescientas personas por ataque. *Fuente: Bloomberg, 12 de enero de 2024; +972 Magazine; Local Call; informe de la relatora especial de la ONU Francesca Albanese.* Cuando se le preguntó sobre las preocupaciones éticas relacionadas con el papel de Palantir en Gaza, Thiel declaró: «Mi inclinación es dar prioridad al criterio de Israel. No nos corresponde a nosotros cuestionarlo todo. Y creo que, en términos generales, las Fuerzas de Defensa de Israel (IDF) tienen derecho a decidir lo que quieren hacer, y que, en general, tienen razón». *Fuente: Debate de la Cambridge Union, 8 de mayo de 2024; múltiples medios de comunicación.* La conexión de Palantir con Epstein. La conexión de Palantir con la Unidad 8200. La IA de Palantir generando las listas de personas a eliminar. La deferencia de Thiel hacia las Fuerzas Armadas de Israel como cuestión de principio declarado. No se trata de una serie de coincidencias. Se trata de un sistema. Se construyó deliberadamente, a través de relaciones cultivadas a lo largo de años, de inversiones financieras realizadas gracias a las presentaciones de un delincuente sexual condenado, de reuniones de la junta directiva en Tel Aviv y cenas en Manhattan. Y actualmente está en funcionamiento, en tiempo real, sobre la población civil de Gaza. ¿Qué hace la red? Quiero volver al argumento estructural, porque los nombres individuales y las cantidades en dólares son importantes, pero no son toda la historia. Toda la historia trata de lo que produce esta red. Cuando los veteranos de la Unidad 8200 pasan a la moderación de contenidos en Meta, traen consigo la formación para identificar y suprimir los contenidos que el Estado israelí considera amenazantes. Cuando se incorporan a la ingeniería de seguridad en Google, aportan con su experiencia en arquitectura de vigilancia construida sobre una población carente de derechos y de recursos esenciales. Cuando pasan a trabajar en IA y aprendizaje automático en Apple, aportan habilidades de reconocimiento de patrones perfeccionadas a partir de las vidas digitales de personas cuyos historiales médicos, antecedentes sexuales y opiniones políticas fueron recopilados sin su consentimiento y luego utilizados además para chantajearlas. Esa es la materia prima que construyó sus carreras. Eso es lo que está contratando Silicon Valley. El antiguo comandante de la Unidad 8200 que ahora trabaja en Google, y que pasó seis años ayudando a comprender los patrones de quienes él mismo define como «activistas hostiles», es en la actualidad el director de Estrategia y Operaciones de Google. La cuestión no es si es un buen ingeniero. La cuestión es qué entiende él por «hostil», a quién considera un activista y qué patrones son los que está entrenado para ver como amenazantes. Dada su formación, la respuesta es: las mismas personas a las que su unidad fue creada para reprimir. *Fuente: MacLeod, MintPress News, 2022.* Dirigí Ethics in Technology durante años. Entrevisté a cientos de personas de este sector. Vi cómo se firmaba el Proyecto Nimbus mientras cuatrocientos

empleados de Amazon y Google intentaban detenerlo. Vi cómo expulsaban al empleado que lideró esa resistencia. Vi cómo TikTok contrataba a un comandante de la Unidad 8200 en pleno apogeo del asalto a Gaza para gestionar lo que denominaban «incidentes globales». Vi cómo Oracle creaba herramientas de propaganda para el gobierno israelí y luego adquiría el control de la plataforma que esas herramientas estaban diseñadas para manipular. Trabajaba en Amazon Web Services. Me dedicaba a la venta de infraestructura. Sé cómo funcionan los contratos, cómo se estructuran las alianzas y cómo se utiliza el lenguaje de los servicios en la nube y el análisis de inteligencia artificial para describir sistemas cuya función real es la vigilancia, la selección de objetivos y la represión de la resistencia civil. Me fui en 2018. Lo que se construyó después de mi marcha es de dominio público. Está documentado en las fuentes al final de este capítulo. Está documentado en el testimonio de los trabajadores que intentaron detenerlo. Está documentado en las listas de personas a eliminar que generó el algoritmo de Palantir y que las Fuerzas Armadas de Israel pusieron en práctica. Larry Ellison consideraba a Israel su hogar y extendió el cheque personal más cuantioso de la historia de una organización dedicada a financiar a los soldados del ejército israelí. Michael Dell extendió un cheque de trescientos cincuenta millones de dólares un mes después del inicio de la misma campaña militar. Peter Thiel dijo que su inclinación es apoyar a Israel y firmó un acuerdo de colaboración para suministrar los sistemas de IA utilizados para generar objetivos de bombardeo. Sus ejecutivos dijeron que si no estás de acuerdo con nuestra misión de apoyar al Estado de Israel, quizá no seamos la empresa adecuada para ti. No se trata de opiniones políticas. Son decisiones empresariales. Tomadas por personas concretas. Con cantidades en dólares documentadas. Mientras tanto, niños palestinos morían en cantidades que la base de datos que hice en ParentsPlea.com ha ido registrando, perfil a perfil, desde la primera semana del asalto. El sector tecnológico no cayó en la complicidad por casualidad. Invirtió en ella. La dotó de personal. La calificó de oportunidad de oro y firmó contratos con ese fin. Llevo años recopilando el registro alternativo. Sobrevivirá a todos ellos. Cuando el director ejecutivo de una empresa de defensa califica el genocidio de oportunidad de oro, está siendo honesto sobre lo que el sistema valora. Cuando el director ejecutivo de una empresa de computación en la nube llama a la misma infraestructura «soluciones empresariales», está siendo deshonesto sobre exactamente lo mismo. Ambos están construyendo la misma máquina. --- La arquitectura financiera que convierte el genocidio en una oportunidad trimestral no existe en el vacío. La mantiene una arquitectura política que garantiza que las personas que deberían exigir responsabilidades a estas empresas reciban, en cambio, financiación de ellas. La puerta giratoria entre Silicon Valley y Washington no es una metáfora. Es un mecanismo documentado, legal y sistemático para convertir la autoridad reguladora pública en beneficio privado. Ese mecanismo es el tema del capítulo siete.

CAPÍTULO SIETE. LA PUERTA GIRATORIA

Cómo las grandes tecnológicas compraron al gobierno, y el gobierno compró a las grandes tecnológicas.

Robin Williams, que en paz descanse, lo expresó a la perfección. Los políticos, dijo, deberían estar obligados a llevar chaquetas con los patrocinadores, como los pilotos de la NASCAR, para que todo el mundo sepa quién los controla. Lo dijo en broma. Pero lo dijo como un diagnóstico. He pasado años en la encrucijada entre la tecnología y la política: primero como fundador de una startup, tratando de entender por qué los contratos gubernamentales iban a parar a manos de empresas establecidas con contactos en lugar de a competidores innovadores; luego, como empleado de Amazon Web Services, observando de cerca la relación entre Silicon Valley y Washington; y después, como activista tratando de entender por qué todos los intentos de regular a las empresas que causaban más daño parecían desvanecerse antes de convertirse en ley. Lo que aprendí en todos esos años es que Robin Williams no exageraba. El sistema no está roto. Funciona exactamente como fue diseñado: diseñado por y para las personas que se benefician de él. El mecanismo que lo hace posible tiene dos componentes. El primero, es la puerta giratoria. El segundo, es Citizens United. Juntos, han creado una economía política en la que las empresas que causan los mayores daños son las más protegidas frente a la rendición de cuentas, y los representantes que se supone que deben exigirles responsabilidades son, en cambio, financiados por ellas. La puerta giratoria En la página web BigTechSellsWars.com se pueden encontrar los nombres y los perfiles de ejecutivos tecnológicos, grupos de presión y funcionarios gubernamentales que han pasado desde las empresas de Silicon Valley a las agencias gubernamentales, y viceversa. De formas tan variadas, que dan un nuevo significado a la expresión «conflicto de intereses». El patrón es constante en todas las administraciones, en todos los partidos y a lo largo de décadas. Un alto funcionario de la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA), por ejemplo, la agencia que financió la Internet original, abandona el gobierno y se une al consejo de administración de una empresa tecnológica que luego se adjudica contratos de la DARPA. Un antiguo alto funcionario de inteligencia se une a la estructura asesora de Palantir y luego aboga en Washington para que la comunidad de inteligencia amplíe el uso de las plataformas de Palantir. Un responsable de adquisiciones del Departamento de Defensa se jubila y se une a un contratista de defensa, donde su principal valor son las relaciones que estableció mientras estaba autorizado a gastar dinero público en los competidores de ese contratista. Esto no es ilegal. Esa es la parte más inquietante. La puerta giratoria no es un escándalo de corrupción que se persiga judicialmente. Es una característica del sistema, que opera de forma abierta y legal, produciendo resultados que cualquier persona con un sentido moral en funcionamiento puede reconocer como corruptos, incluso cuando técnicamente no se ha infringido ninguna ley. Las empresas tecnológicas que más se benefician de esta puerta giratoria son las que tienen los mayores contratos gubernamentales: Amazon, Google, Microsoft, Palantir, Oracle. No son empresas que tengan contratos gubernamentales porque ofrecen los

mejores productos a los mejores precios. Tienen contratos gubernamentales porque han invertido en relacionamientos, en infraestructura de cabildeo y en atraer a antiguos funcionarios que saben dónde están los presupuestos de contratación y cómo se toman las decisiones de contratación. Palantir es el ejemplo más claro. Fundada con capital de riesgo de la CIA en 2003, Palantir dedicó su primera década a forjar relaciones tan profundas dentro de la comunidad de inteligencia que, cuando empezó a competir por grandes contratos gubernamentales, las personas que evaluaban sus ofertas solían ser personas que habían desarrollado su carrera dentro de las agencias a las que Palantir se dirigía. La empresa no ganó esos contratos por casualidad. Los ganó a propósito, forjando las relaciones que darían lugar a las decisiones que necesitaba. Citizens United y la compra de políticas La puerta giratoria mueve a las personas. Citizens United mueve el dinero. Y en el sistema político de Estados Unidos, el dinero es la variable más decisiva. En 2010, el Tribunal Supremo dictaminó en el caso Citizens United contra la Comisión Electoral Federal que las empresas tienen los mismos derechos de la Primera Enmienda que los individuos y no se les puede prohibir gastar cantidades ilimitadas de dinero en publicidad política. El efecto práctico de este fallo fue eliminar el último límite significativo a la capacidad de las empresas para moldear el entorno político en el que se determina su supervisión regulatoria. Antes de Citizens United, una empresa que quisiera influir en unas elecciones podía donar cantidades limitadas a los candidatos a través de un comité de acción política, sujeto a requisitos de divulgación. Tras Citizens United, esa misma empresa puede crear o financiar una organización sin fines de lucro, estructurada de tal forma que elude los requisitos de divulgación total, y gasta cantidades ilimitadas en publicidad, defensa de causas y mensajes políticos. Las empresas tecnológicas que son objeto de este libro han utilizado intensamente esta estructura. Amazon, Google, Microsoft, Meta, Apple y sus intereses afiliados han gastado cientos de millones de dólares en cabildeo, en publicidad política, en los SuperPAC y en las organizaciones sin fines de lucro de «dinero oscuro» que Citizens United hizo posibles. Han financiado a candidatos de ambos partidos. Han financiado grupos de expertos que elaboran documentos de políticas que justifican el entorno regulatorio que desean. Han financiado cátedras académicas en universidades que producen investigaciones que respaldan sus posiciones sobre la defensa de la competencia, la privacidad y la gobernanza de la IA. El resultado es un sistema político en el que las empresas que más necesitan regulación son las más capaces de impedirla. Los proyectos de ley que las harían rendir cuentas mueren en comisión. Las regulaciones que limitarían sus prácticas de datos se diluyen antes de su implementación. Los casos antimonopolio que desmantelarían la concentración empresarial tardan una década en resolverse, mientras los monopolios se hacen más fuertes. Esto no es un fracaso de la democracia. Es la democracia funcionando tal y como fue rediseñada por Citizens United: un sistema en el que el tamaño de tu cartera determina el volumen de tu voz, y las empresas con las carteras más abultadas tienen las voces más fuertes en todas las salas donde se redactan las normas. Ambos partidos. Todas las administraciones. Quiero dejar claro algo que a veces se pierde en este debate. La puerta giratoria y la corrupción que permite no son un problema republicano ni un problema demócrata. Son un problema sistémico que ha funcionado de forma continua en las administraciones de ambos partidos. La relación de la administración Obama con Silicon Valley fue íntima y asombrosa. La administración Trump, tanto la primera como la segunda, ensalzó a un grupo diferente de multimillonarios tecnológicos, al tiempo que ofrecía la misma permisividad

regulatoria a las mismas empresas. La administración Biden llevó a cabo algunos procesos antimonopolio, pero supervisó el periodo en el que se amplió el Proyecto Nimbus y las empresas que proporcionaban infraestructura militar de IA no tuvieron que rendir cuentas por ello. Entre las personas que han trabajado a ambos lados de esta puerta giratoria se encuentran demócratas y republicanos, personas nombradas por Obama y por Trump, funcionarios de carrera y cargos políticos. El denominador común no es la ideología. Es la relación financiera entre la empresa y el funcionario: la oferta de trabajo que espera, el puesto disponible en el consejo asesor, la conferencia que se ofrece. Tal y como se documenta en mi documental *Forever Peace Now* y en la página web BigTechSellsWars.com, las empresas tecnológicas estadounidenses y sus socios gubernamentales han gastado más de 44.000 millones de dólares desde 2004 en contratos con empresas como Amazon, Google, Microsoft y otras; contratos que construyen la infraestructura de vigilancia, los sistemas de selección de objetivos de drones y las plataformas de procesamiento de datos que hacen posibles las guerras que documento en este libro. Esa cifra ha aumentado drásticamente desde entonces. Los contratos son bipartidistas. Los beneficiarios son bipartidistas. El número de víctimas civiles no lo es. La lección de Canadá para Washington La reciente ruptura de Canadá con la dependencia de las adquisiciones militares de Estados Unidos, cuando el primer ministro Mark Carney declaró que «los días en que el ejército canadiense enviaba 70 céntimos de cada dólar a Estados Unidos han terminado», no es solo una historia de comercio. Es una historia de puertas giratorias. La razón por la que 70 céntimos de cada dólar canadiense destinado a defensa iban a parar a Estados Unidos es la misma por la que las empresas estadounidenses dominan la infraestructura de la nube europea, la misma por la que Palantir se adjudicó el contrato del NHS en el Reino Unido, la misma por la que los contratos sin licitación siguen yendo a parar a las mismas empresas. Relaciones forjadas a lo largo de décadas entre funcionarios de defensa, responsables de adquisiciones y los contratistas a los que favorecen: relaciones que sobreviven a los cambios de administración porque los contratistas financiaban a ambos bandos. El giro de Canadá es posible, en parte, porque el gobierno de Carney llegó sin la misma red de relaciones con contratistas establecidos a través de la cual opera Washington. Analizaron las cifras. Setenta céntimos de cada dólar se iba al sur, y se hicieron la pregunta que todo gobierno con la voluntad política de planteársela puede responder con honestidad: ¿es esto soberanía o es esto dependencia? La respuesta fue dependencia. Y cambiaron de rumbo. Qué significa esto para todo lo demás en este libro La puerta giratoria y Citizens United son la explicación de por qué se ha permitido que ocurra todo lo demás en este libro. ¿Por qué Amazon tiene un contrato de nube de 1.200 millones de dólares con el ejército israelí? Porque las personas que adjudican los contratos gubernamentales se mueven entre Amazon y los organismos que los adjudican, y las personas que podrían legislar en contra de ello están financiadas por el gasto político de Amazon. ¿Por qué Palantir tiene un contrato sin licitación de 30 millones de dólares con el ICE? Porque sus fundadores y ejecutivos han pasado años cultivando las relaciones dentro de las comunidades de inteligencia y de las fuerzas del orden que generan esas adjudicaciones. ¿Por qué no se ha procesado a ningún ejecutivo del sector tecnológico? Porque el procesamiento requiere voluntad política, y la voluntad política requiere políticos que no dependan financieramente de las empresas a las que tendrían que procesar. Este es el círculo. No se rompe desde dentro. Se rompe cuando la rendición de cuentas externa, legal, penal e internacional, genera consecuencias que el

sistema político no puede absorber ni redirigir. Por eso es importante la petición a España. Por eso el enjuiciamiento penal, y no las multas reguladoras, es el instrumento que realmente cambia el cálculo. Los patrocinadores que figuran en la portada son visibles para cualquiera que sepa leer una declaración de financiación de campaña o un formulario de registro de grupos de presión. La cuestión no es si podemos verlos. La cuestión es si estamos dispuestos a actuar en función de lo que vemos.

La puerta giratoria explica quién recibe protección. El capítulo ocho explica quién paga el precio. Los trabajadores que se encuentran en la base de la cadena de suministro de las grandes tecnológicas, como los moderadores de contenido en Nairobi que ven imágenes de personas manteniendo relaciones sexuales a través de las gafas inteligentes de Meta, los trabajadores de almacén en Nueva Jersey que sufren lesiones a un ritmo 2,6 veces superior a la media del sector mientras que Amazon registra beneficios récord, y los propietarios de pequeñas empresas cuyos márgenes han sido consumidos por una plataforma que ahora compite con los vendedores y cuyas comisiones financiaron su crecimiento: estas son las personas para las que la puerta giratoria fue diseñada, para olvidar.

CAPÍTULO OCHO. LA MANO DE OBRA INVISIBLE

Cómo las grandes tecnológicas destrozan los cuerpos y las mentes de los trabajadores que no pueden ver, y luego se deshacen de ellos.

En febrero de 2026, un grupo de trabajadores de Nairobi, Kenia, comenzó a hablar con periodistas suecos. Dos periódicos, Svenska Dagbladet y Göteborgs-Posten, deciden publicar la historia que estos trabajadores, asumiendo un enorme riesgo personal, habían decidido que el mundo debía conocer. Trabajaban para una empresa llamada Sama, una firma de subcontratación con sede en Nairobi, contratada por Meta. Su trabajo consistía en revisar las grabaciones captadas por los usuarios de las gafas inteligentes Ray-Ban de Meta: anotar lo que aparecía en los videoclips, etiquetar objetos y acciones, y ayudar a entrenar los sistemas de inteligencia artificial de Meta. Esa es la descripción corporativa y educada de lo que se les pedía que hicieran. Lo que realmente veían era algo diferente. Durante largos turnos de diez horas, a estos trabajadores se les mostraban imágenes de personas manteniendo relaciones sexuales, captadas por una cámara sin su conocimiento. Veían a personas cambiándose de ropa en sus dormitorios. Veían a niños filmados sin consentimiento. Veían a personas utilizando el baño. Veían números de tarjetas de crédito captados accidentalmente por la cámara cuando alguien utilizaba sus gafas para ayudar a un amigo a pagar algo. Estas imágenes, íntimas, privadas, a menudo violatorias, procedían de usuarios de las gafas de Meta que no tenían ni idea de que su vida cotidiana se enviaba a trabajadores en Kenia para ser catalogada, etiquetada y utilizada para entrenar a la inteligencia artificial. Los trabajadores que alzaron la voz dijeron que no se les permitía llevar teléfonos ni ningún dispositivo personal al trabajo. Las cámaras de seguridad vigilaban cada uno de sus movimientos. La implicación era clara: Meta sabía que estas imágenes eran lo suficientemente delicadas como para requerir el control de cualquiera que las viera. (Fuente: Gadget Review, «Meta despide a los contratistas que sacaron a la luz el escándalo de privacidad de las gafas Ray-Ban», mayo de 2026, https://www.gadgetreview.com/meta-fires-contractors-who-exposed-ray-ban-glasses-privacy scandal; Android Headlines, «Despiden a 1.100 formadores de IA tras denunciar el Ray-Ban de Meta», mayo de 2026, https://www.androidheadlines.com/2026/05/1100-ai-trainers-were-fired-after-blowing-the-whistle-on-met as ray-ban-privacy-problem.html). Menos de dos meses después de que se conociera la noticia, Meta rescindió su contrato con Sama. La empresa de Nairobi confirmó el despido de 1.108 trabajadores, algunos de los cuales recibieron un preaviso de tan solo seis días. Meta alegó que Sama «no cumplía con sus estándares». Sama afirmó que había cumplido sistemáticamente todas las expectativas contractuales y que nunca se le había notificado de ninguna deficiencia. La lógica de lo ocurrido no es difícil de seguir. Los trabajadores denunciaron la situación. Meta rescindió el contrato. Y 1.108 personas perdieron sus puestos de trabajo. Meta ha descrito la revisión de las grabaciones como un procedimiento estándar contemplado en sus condiciones de servicio. Esto es técnicamente cierto, del mismo modo que todo acuerdo abusivo se divulga técnicamente en letra pequeña que nadie lee. Las personas cuyos momentos íntimos fueron enviados a Kenia para ser vistos por desconocidos

durante un turno de diez horas no dieron su consentimiento para ello. Y los trabajadores que tuvieron que verlos se han quedado ahora sin ingresos porque tuvieron la osadía de decirlo. (Fuente: Informe de incidentes de la OCDE. AI, «Las gafas inteligentes con IA de Meta provocan daños a los trabajadores y violaciones de la privacidad en Kenia», 30 de abril de 2026, https://oecd.ai/en/incidents/2026-04-30-7774).

No es la primera vez

La historia de Kenya Sama es nueva. El patrón que representa no lo es. Se trata de una empresa valorada en más de un billón de dólares. Pero paga a las personas que protegen al resto de sus usuarios del contenido más nocivo de sus plataformas menos de lo que cuesta un café grande en San Francisco, y luego las despide cuando se quejan del trauma que les causa realizar ese trabajo. No es la primera vez que Meta deja un rastro de trabajadores traumatizados y descartados en Nairobi. En enero de 2023, a los 260 «moderadores de contenido» que trabajaban en el centro de Sama en Nairobi, personas que dedicaban sus horas de trabajo a revisar el contenido de Facebook en busca de violencia, explotación infantil y material explícito, se les comunicó que sus puestos de trabajo eran redundantes. Cuarenta y tres de estos trabajadores presentaron una demanda por despido improcedente. La demanda colectiva acabó ampliándose hasta incluir a 185 trabajadores. El Dr. Ian Kanyanya, jefe de servicios de salud mental del Hospital Nacional Kenyatta, evaluó a 144 de ellos. Sus conclusiones, presentadas ante el tribunal de empleo y relaciones laborales de Nairobi en diciembre de 2024, fueron devastadoras: el 81 % de los trabajadores evaluados padecía un trastorno de estrés postraumático (TEPT) grave. (Fuente: CNN Business, «Facebook infligió un "trauma de por vida" a los moderadores de contenido en Kenia, según activistas, ya que a más de 140 se les ha diagnosticado TEPT», 22 de diciembre de 2024, https://edition.cnn.com/2024/12/22/business/facebook-content moderators-kenya-ptsd-intl). Uno de los trabajadores que lideró la protesta, un sudafricano llamado Daniel Motaung, fue despedido por organizarla. Demandó a Meta y a Samasource Kenya, alegando trabajo forzoso, trata de personas y represión sindical. Contó a los investigadores que su equipo se veía obligado a ver horas de contenido espantoso, incluyendo decapitaciones y explotación sexual infantil, por un salario inferior a 2,20 dólares la hora. Más de 80 organizaciones sindicales de todo el mundo escribieron a Meta exigiéndole que dejara de intentar silenciarlo. Entre los firmantes se encontraba la denunciante más destacada de Meta, Frances Haugen. (Fuente: Quartz Africa, «Meta faces pressure from rights groups to stop gagging Daniel Motaung», https://qz.com/africa/2191286/meta-faces-pressure-from-rights-groups-to-stop-gagging-daniel-motaung.

La ciencia de lo que este trabajo le hace a las personas Quiero ser preciso sobre lo que la moderación de contenidos le hace a una persona, porque la industria ha perfeccionado el arte de mantener esto oculto. No se trata de daños hipotéticos. Son realidades clínicas documentadas. Las investigaciones científicas revisadas por pares confirman que los moderadores de contenido, aquellas personas a las que las empresas tecnológicas pagan por ver material gráfico y angustiante para que el resto de nosotros no tengamos que hacerlo, sufren en proporciones notablemente más altas de trastorno de estrés postraumático (TEPT), ansiedad, depresión, pensamientos intrusivos, trastornos del sueño, distanciamiento emocional y agotamiento. Una encuesta transversal publicada en 2024 reveló que el 53 % de las personas que se identificaban como moderadores de contenido presentaban niveles clínicos de angustia psicológica general. Las investigaciones

muestran una relación dosis-respuesta: cuanto más contenido traumático ve una persona, peores son sus resultados de salud mental. La exposición no desaparece cuando termina el turno. (Fuente: Artículo de investigación, «I've Seen Enough: Measuring the Toll of Content Moderation on Mental Health», arXiv:2511.09813, noviembre de 2024, https://arxiv.org/pdf/2511.09813; Cyberpsychology Journal, «The psychological impacts of content moderation on content moderators» (Los impactos psicológicos de la moderación de contenidos en los moderadores de contenidos), 2023, https://cyberpsychology.eu/article/view/33166). Los investigadores de SAGE Journals han caracterizado lo que les ocurre a los moderadores de contenidos no como un accidente del trabajo, sino como una característica estructural del mismo: la mercantilización de la propia vulnerabilidad traumática. En otras palabras, las empresas no están fallando a la hora de proteger a estos trabajadores. Están comprando deliberadamente la capacidad de estos trabajadores para absorber el trauma, adquiriendo su salud psicológica como un costo de producción, del mismo modo que se compran servidores, almacenamiento o ancho de banda. (Fuente: Amit Pinchevski, «Los canarios de las redes sociales: los moderadores de contenido entre el trabajo digital y el trauma mediado», SAGE Journals, 2023, https://journals.sagepub.com/doi/abs/10.1177/01634437221122226). Las personas que realizan este trabajo en Kenia, en Etiopía, en Filipinas, en Indonesia, y en todos los demás países de bajos salarios donde las grandes tecnológicas han externalizado la carga de su requisito operativo más traumático, no son casos aislados. Son una fuerza laboral de decenas de miles de personas que realizan un trabajo que hace posible la operatividad de todas las plataformas de redes sociales que utilizas a diario. Y lo hacen por unos salarios, en unas condiciones y con unas consecuencias para su salud mental que sería ilegal imponerlas a los trabajadores de los países donde se obtienen los beneficios. Esto no es un descuido. Es un modelo de negocio. El almacén de Amazon: sangre, sudor y entrega al día siguiente Quiero pasar del trabajo psicológico de la moderación de contenidos al trabajo físico de la gestión de pedidos, porque ambos cuentan la misma historia sobre cómo las grandes tecnológicas tratan a los trabajadores que se encuentran en la base de su cadena de suministro: como un recurso que hay que optimizar hasta que se rompa, para luego desecharlo. En agosto de 2015, el New York Times publicó una investigación, basada en entrevistas con más de un centenar de empleados actuales y antiguos de Amazon, que describía un lugar de trabajo caracterizado por correos electrónicos a medianoche, mensajes de texto por la mañana exigiendo saber por qué el correo electrónico en medio de la noche había quedado sin respuesta, empleados llorando en sus escritorios y trabajadores que sufrían crisis de salud tan graves que eran sacados en camillas. Los periodistas Jodi Kantor y David Streitfeld, citaron a un antiguo empleado que decía: «Vi llorar en su escritorio a casi todas las personas con las que trabajé». (Fuente: New York Times, «Inside Amazon: Wrestling Big Ideas in a Bruising Workplace», 15 de agosto de 2015, por Jodi Kantor y David Streitfeld, https://www.nytimes.com/2015/08/16/technology/inside-amazon-wrestling-big-ideas-in-a-bruisi ng workplace.html). Esta investigación describe la experiencia de los empleados de oficinas en las sedes corporativas de Amazon. Lo que se ha documentado desde entonces sobre la experiencia de los trabajadores manuales en los almacenes de Amazon es aún peor y mucho más grave desde el punto de vista físico. En diciembre de 2024, el senador Bernie Sanders publicó una investigación de 160 páginas del Comité HELP del Senado sobre el historial de seguridad de los almacenes de Amazon. Sus conclusiones fueron contundentes y detalladas. La tasa de lesiones de

Amazon en 2022 fue del 6,6 %, frente a una media del sector del 3,2 %. Los trabajadores de los almacenes de Amazon sufren lesiones graves a un ritmo 2,6 veces superior al de sus homólogos de otras empresas. Un informe interno de Amazon, titulado Proyecto Soteria y citado por los investigadores del Senado, reveló una relación directa entre la velocidad de las tareas realizadas y la tasa de lesiones de los trabajadores. Amazon revisó estas pruebas y decidió no tomar medidas al respecto, según los investigadores del Senado, debido a consideraciones financieras. (Fuente: Comité HELP del Senado de EE.UU., Informe de investigación sobre Amazon, diciembre de 2024, https://www.help.senate.gov/imo/media/doc/amazon_investigation.pdf; CNN Business, «Un informe del Senado acusa a Amazon de ignorar la seguridad de los trabajadores en su afán por aumentar la productividad», 16 de diciembre de 2024, https://www.cnn.com/2024/12/16/business/amazon-worker safety-senate-report). Las lesiones más comunes en los almacenes de Amazon son esguinces, distensiones y desgarros musculares, el tipo de lesiones que mantendrían fuera de juego a un deportista profesional durante semanas. Los trabajadores que las sufren no son deportistas que se recuperan en centros médicos especializados. Son personas que no pueden permitirse dejar de trabajar y que realizan turnos mientras los sistemas automatizados de Amazon supervisan cada uno de sus movimientos, registran cada desviación de los objetivos de productividad y generan medidas disciplinarias para cualquier trabajador que no mantenga el ritmo exigido. Las tasas de lesiones se disparan durante el Prime Day, el Black Friday y el Cyber Monday, precisamente los momentos en que la presión por la productividad es máxima y el cuerpo humano se ve empujado más allá de sus límites. Recuerdo que, cuando trabajaba en Amazon Web Services, la cultura que describió el New York Times no era ficción. La vi. La viví de cerca. Vi cómo la máquina lo exigía todo y no ofrecía nada a cambio, salvo un sueldo y la expectativa de gratitud. Los empleados de la sede central al menos tenían la dignidad de un sueldo, un escritorio y la opción de actualizar su currículum. Los trabajadores del almacén tienen una pulsera escaneable, una cuota de productividad y un cuerpo que se ve consumido poco a poco por el ritmo de la entrega al día siguiente. La muerte de Main Street a manos del algoritmo Hay una tercera categoría de daño que Amazon ha infligido: más silencioso que las lesiones en los almacenes, menos dramático que el llanto en los escritorios, pero quizás más devastador desde el punto de vista estructural para las comunidades que conforman el tejido real de la vida estadounidense. Es lo que les ha ocurrido a las pequeñas empresas que en su día se alineaban en las calles principales de cada pueblo de este país. En 2016, según la empresa de investigación de comercio electrónico Marketplace Pulse, Amazon se quedó con aproximadamente un tercio de cada dólar ganado por los comerciantes que vendían en su plataforma, en forma de comisiones y publicidad. En 2022, esta cifra superó el 50 %. En 2024, Amazon recaudó más de 150.000 millones de dólares en ingresos solo por las comisiones de los vendedores externos, una cifra tan elevada que, si se tratara de una empresa independiente, se situaría entre las 25 primeras de la lista Fortune. (Fuente: Fortune, «Las ganancias récord de Amazon esconden un misterio: ¿en qué medida se deben a las comisiones de los pequeños vendedores?», 7 de febrero de 2025, https://fortune.com/2025/02/07/amazon-2024-earnings-third-party-seller-fees-profits/). Si se suman las comisiones por recomendación, los costos de logística, el gasto en publicidad y los gastos de almacenamiento, la parte total que Amazon se lleva de los ingresos de un vendedor oscila entre el 30 y el 50 por ciento, a menudo más. Para los pequeños vendedores con márgenes ya de por sí reducidos, esa

ecuación no es un modelo de negocio. Es una sentencia de muerte lenta. Análisis independientes confirman que, para muchas categorías de productos, el costo de vender en Amazon supera ahora cualquier margen de beneficio concebible para un pequeño productor. La plataforma que se suponía que iba a dar a cada pequeña empresa un escaparate global se ha convertido en un mecanismo para extraer valor de los productores de bienes a un ritmo que en cualquier otra época se habría reconocido inmediatamente como extracción monopólica. (Fuente: SmartScout, «The Top Challenges Facing Amazon Third-Party Sellers in 2025», abril de 2025, https://www.smartscout.com/blog/amazon-third-party-sellers-problems). Crecí en el Área de la Bahía. Recuerdo cómo se veía una calle principal antes de Amazon. Recuerdo la ferretería donde el dueño te conocía por tu nombre. La librería donde alguien podía recomendarte algo de lo que nunca habías oído hablar. La tienda de ropa regentada por una familia que llevaba veinte años en el barrio. Recuerdo los trabajos de verano: ese tipo de empleo básico, arraigado en la comunidad, que proporcionaba a un adolescente su primer sueldo, su primera experiencia de responsabilidad, su primera relación con un negocio del barrio que era también una institución del barrio. Esos trabajos han desaparecido. Esas tiendas han cerrado. Sus propietarios no pudieron competir con una empresa que utiliza precios basados en algoritmos, una infraestructura logística construida con subvenciones gubernamentales y un modelo de mercado que se lleva la mitad de cada dólar y luego utiliza los datos de ese mercado para identificar qué productos fabricar bajo la marca propia de Amazon, es decir, en competencia directa con los vendedores cuyas comisiones financiaron el crecimiento de la plataforma. Esto no es competencia de libre mercado. Es una mesa tramposa en la que un solo jugador nunca puede perder. Y los trabajadores que sustituyeron a los propietarios de las tiendas, las personas que empaquetan y envían la mercancía en los almacenes, no obtienen lo que tenían los propietarios. No tienen propiedad. No tienen relación con el cliente. No tienen participación en el producto. Tienen una cuota de productividad, una tarjeta de identificación escaneable y un cuerpo que sufre lesiones de forma sistemática a un ritmo 2,6 veces superior al resto del sector, mientras Amazon registra beneficios récord y sus fundadores construyen cohetes. Lo que viene después: los robots y la falsa preocupación Amazon ha anunciado con bombos y platillos sus inversiones en robótica y automatización de almacenes, presentándolas como mejoras en la seguridad de los trabajadores. En cierto sentido, reducir el número de veces que un ser humano tiene que levantar una caja de veintitrés kilos, sustituyendo esa tarea con una máquina, supone una mejora genuina. Lo reconozco sin rodeos. Pero permítanme decir también lo que no se está reconociendo: esa misma automatización que reduce parte del esfuerzo físico eliminará la mayoría de los puestos de trabajo. Amazon lleva años trabajando para lograr una gestión de pedidos totalmente automatizada. Cuando estos puestos de trabajo desaparezcan, y es seguro que desaparecerán, las comunidades que construyeron su identidad económica en torno al almacén de Amazon a las afueras de la ciudad no recibirán una indemnización por despido del algoritmo que sustituyó a sus vecinos. No recibirán nada. A los trabajadores que pasaron años sufriendo lesiones a un ritmo doble al del sector mientras construían el imperio logístico de Amazon se les dará las gracias por su servicio y se les indicará la puerta de salida. Este es el punto final de un modelo de negocio que siempre ha tratado a los trabajadores como un costo de producción que hay que minimizar y sustituir. Primero, minimizó los salarios deslocalizando la moderación de contenidos a Kenia. Luego minimizó los costes laborales exprimiendo a los trabajadores de

almacén a ritmos que destrozan sus cuerpos, al tiempo que se les controla a cada segundo con tecnología de vigilancia. Ahora está minimizando el costo de la mano de obra por completo, sustituyendo a los seres humanos por máquinas, no porque los trabajadores fueran inadecuados, sino porque las máquinas son más baratas. La pregunta que nunca se planteará en ninguna conferencia sobre resultados trimestrales es: ¿qué les debemos a las personas cuya mano de obra consumimos en el camino hasta dejar de necesitarlas? ¿Qué les debemos a las comunidades cuyas calles principales cerramos, cuyos empleos de verano eliminamos, cuyas economías locales vaciamos, en el camino hacia la construcción de la empresa de logística más rentable de la historia de la humanidad? La cosecha de los oficinistas: cuando el empleado se convierte en el conjunto de datos Amazon tomó los cuerpos de sus trabajadores de almacén y los destrozó. Las tasas de lesiones, las cuotas de productividad, las camillas, la investigación del Senado: todo ello está documentado más arriba. El punto final del modelo de Amazon ya no es especulativo. Es un almacén totalmente automatizado. A los trabajadores que lo construyeron se les agradecerá su servicio y se les indicará la puerta de salida. Las comunidades que rodean estos almacenes no recibirán nada. Lo que Meta anunció el 21 de abril de 2026 es la misma historia, pero trasladada a las plantas superiores. A las oficinas acristaladas. A los portátiles de la empresa. A las manos y mentes de los ingenieros, jefes de producto y diseñadores que creían que, porque tenían títulos universitarios, opciones sobre acciones y sillas ergonómicas, eran una categoría de trabajadores diferente a la de la gente que empaqueta cajas en Nueva Jersey. No lo son. Nunca lo fueron. La explotación simplemente tardó más en llegar hasta ellos. El 21 de abril de 2026, en un memorándum interno de Meta publicado en un canal perteneciente al equipo Meta Superintelligence Labs, y que fue obtenido por Reuters y CNBC, la empresa reveló a sus empleados con sede en Estados Unidos que había instalado un software de rastreo en sus ordenadores corporativos. El programa se llama Model Capability Initiative, o MCI, y captura todos los movimientos del ratón, los clics, las pulsaciones de teclas y las capturas de pantalla continua de la pantallade los empleados. Funciona de forma continua en una lista designada de aplicaciones relacionadas con el trabajo y plataformas de terceros. Estos datos se introducen directamente en el proceso de entrenamiento de IA de Meta, la cual a su vez es utilizada para crear agentes de IA capaces de realizar, sin intervención humana, las mismas tareas administrativas registradas de los empleados. (Fuente: Reuters, «Meta informa a sus empleados de que está rastreando sus pulsaciones de teclas para entrenar a la IA», 21 de abril de 2026, https://www.reuters.com/technology/meta-tells-employees-its-tracking-their-keystrokes-train-ai-2 026- 04-21/; CNBC, «Meta está registrando las pulsaciones de teclas de los empleados en Google, LinkedIn y Wikipedia como parte de una iniciativa de entrenamiento de IA», 22 de abril de 2026, https://www.cnbc.com/2026/04/22/meta-tracks-employee-usage-on-google-linkedin-ai-training-p roject.html). La lista de plataformas supervisadas circuló ampliamente dentro de Meta. Incluye Google, LinkedIn, Slack de Salesforce, GitHub de Microsoft, Atlassian y las propias propiedades de Meta. Cabe destacar que la lista incluía originalmente ChatGPT de OpenAI y Claude de Anthropic, los dos asistentes de IA más utilizados en entornos profesionales, antes de que dichas plataformas fueran discretamente eliminadas de la lista de seguimiento sin explicación alguna. No es difícil sacar una conclusión: capturar cómo interactúan los propios empleados de Meta con los sistemas de IA de la competencia expondría a la empresa a consecuencias legales, competitivas y de reputación que

Meta no estaba preparada para asumir. Los propios empleados no recibieron ninguna protección equivalente. (Fuente: CNBC, ibíd). Lo que MCI puede ver realmente, y por qué eso debería aterrorizarte Quiero detenerme aquí y plantear una pregunta que las comunicaciones corporativas en torno a Model Capability Initiative (MCI) se han cuidado de no formular directamente. ¿Qué ve realmente un programa que captura los movimientos del ratón, las pulsaciones de teclas y las capturas de pantalla continuas de la pantalla de un empleado a lo largo de su jornada laboral? No en abstracto. En la práctica. Ve cada correo electrónico que un trabajador recibe de la consulta de su médico; recordatorios de citas, resultados de pruebas, actualizaciones del tratamiento, confirmaciones de recetas. Ve el pedido que un trabajador hace online en la farmacia durante la pausa para comer de un medicamento del que preferiría que su empresa no supiera nada. Captura el nombre de ese medicamento, la dosis, la fecha de reposición y la afección de que trata, ya sea depresión, VIH, diabetes, un trastorno psiquiátrico, una enfermedad crónica o un embarazo. Nada de esa información se le entrega a Meta de forma voluntaria. Nada de ello es relevante para el entrenamiento del modelo de IA. Todo ello se encuentra ahora en un proceso de entrenamiento. Ve el mensaje de texto que un trabajador envía desde su ordenador a su pareja sobre el diagnóstico de un hijo. Ve el portal del seguro médico que un trabajador visita para comprobar si un tratamiento está cubierto. Ve las búsquedas que realiza un trabajador para entender qué significa un nuevo diagnóstico, cuáles son los efectos secundarios de un medicamento o si su afección le da derecho a adaptaciones por discapacidad. Ve el momento en que un trabajador lee una noticia que le aterroriza, sobre un cambio de política, la aprobación de un fármaco, un ensayo clínico, y la respuesta privada, inmediata y humana que escribe a alguien en quien confía. Ve la notificación bancaria que aparece en pantalla cuando llega la transferencia directa de un trabajador. Ve el extracto de la tarjeta de crédito que un trabajador abre para reclamar un cargo. Ve la cuenta financiera a la que un trabajador accede para comprobar si puede permitirse el tratamiento que su médico acaba de recomendar. Captura números de cuentas, historiales de transacciones y la combinación particular de estrés financiero y necesidad médica que define lo que está sucediendo en la vida de una persona en un momento dado. Ve el artículo político que un trabajador lee durante su pausa para comer. Ve si ese artículo procede de un medio conservador o progresista. Ve la publicación en redes sociales que un trabajador abre y lee íntegramente, incluido el contenido político, la afiliación partidista de la persona que la escribió y si el trabajador se detiene en ella, la comparte o escribe una respuesta. En una época en la que los empleadores examinan las creencias políticas de los candidatos, en la que las autoridades de inmigración vigilan las redes sociales y en la que la afiliación política puede afectar a las relaciones profesionales de formas difíciles de documentar pero imposibles de ignorar, esto no es una simple captura de datos. Es un perfil. Ve el correo electrónico personal de un familiar en el que se describe una crisis de salud, el diagnóstico de cáncer de un progenitor, la adicción de un hermano, la hospitalización por salud mental de un hijo que llega a la bandeja de entrada de un trabajador a las dos de la tarde mientras intenta terminar el resumen de un producto. Ve la respuesta que escribe el trabajador. Ve las búsquedas en la web que realiza después. Ve el dolor que se produce en tiempo real, en un dispositivo corporativo, porque los seres humanos no separan claramente sus vidas de sus horas de trabajo, por mucho que los manuales de empleados les digan que lo intenten. Se suponía que nada de esto iba a ser un ejercicio de recopilación de datos. Ahora todo lo es. La

respuesta de Meta: «No revises tu correo electrónico personal en tu ordenador del trabajo» Cuando los empleados de Meta plantearon precisamente estas preocupaciones en debates internos, preguntando cómo evitaría la empresa la captura de información sobre salud, datos financieros, estatus migratorio o comunicaciones familiares, la respuesta del director técnico de Meta, Andrew Bosworth, quedó reflejada en comunicaciones internas obtenidas por Platformer. Su respuesta, íntegra: «Gmail es un contexto aprobado, así que si te preocupa, quizá sea mejor no consultar el correo electrónico personal en tu ordenador del trabajo». (Fuente: Platformer, «La semana en que los empleados de Meta se convirtieron en datos de entrenamiento», abril de 2026, https://www.platformer.news/meta-mci-monitoring-layoffs-knowledge-work/). Vuelve a leerlo. A las personas cuyos historiales médicos, información financiera, comunicaciones familiares u opiniones políticas están siendo ahora recopilados para entrenar la IA de Meta, el director de tecnología de esta empresa les ha dicho que su único recurso es dejar de usar los ordenadores del trabajo para cualquier asunto personal. Esto no es protección de la privacidad. Es una transferencia de responsabilidad. Es Meta diciéndole a sus empleados: hemos instalado infraestructura de vigilancia en su equipo que capturará todo lo visible en su pantalla, y la responsabilidad de garantizar que su información más privada no entre en nuestro proceso de entrenamiento les corresponde a ustedes. No a nosotros. Sino a ustedes. Esta respuesta no es solo insensible. Es incoherente desde el punto de vista legal y ético. Los trabajadores de Estados Unidos tienen derechos bien establecidos en virtud de la legislación federal y estatal que regula lo que los empleadores pueden y no pueden recopilar sobre sus afecciones médicas y su estado de salud. La Ley de Estadounidenses con Discapacidades, la Ley de Portabilidad y Responsabilidad del Seguro Médico, la Ley de No Discriminación por Información Genética: no son documentos de intenciones. Son leyes federales. Existen precisamente porque el Congreso reconoció que el desequilibrio de poder entre un empleador y un empleado, si no se controla, siempre se resolverá a favor del empleador, y que ciertas categorías de información personal son demasiado sensibles, demasiado íntimas y demasiado susceptibles de ser utilizadas como armas como para dejarlas a la buena voluntad de la parte con mayor poder. Meta ha creado ahora un sistema que recopila precisamente este tipo de información, quizá no de forma deliberada, pero sí de manera sistemática, inevitable y continua, y ha comunicado a sus empleados que la solución pasa por la autorregulación del comportamiento por parte de los vigilados. La empresa en la que no se puede confiar para desarrollar un sistema de reconocimiento facial de forma ética, que despidió a 1.108 trabajadores kenianos por hablar de lo que veían, que accedió al 94 % de las solicitudes de censura del gobierno israelí, es la misma empresa que ahora posee un registro actualizado continuamente, captura de pantalla por captura de pantalla, de la vida médica, financiera, política y familiar de sus empleados, y les asegura que no se hará un uso indebido de ella. No me tranquiliza. A juzgar por las discusiones internas descritas como «distópicas» por varios empleados, a ellos tampoco. (Fuente: CNBC, ibíd). La dimensión política: lo que tu feed de noticias dice de ti Permítanme ser específico sobre la dimensión de la vigilancia política de MCI, ya que ha recibido menos atención que los aspectos médicos y financieros, y es potencialmente la más peligrosa de todas. MCI funciona en Google. Funciona en LinkedIn. Funciona en la navegación web que realiza un empleado en su dispositivo corporativo a lo largo del día. En la práctica, esto significa que captura qué fuentes de noticias lee un trabajador, qué noticias políticas abre y lee hasta el final, cuáles se

salta, con qué publicaciones en redes sociales interactúa y qué escribe en respuesta al contenido político. Se trata de un perfil político exhaustivo, elaborado no a partir de opiniones declaradas o afiliaciones partidistas, sino de la huella conductual real de cómo una persona consume información política en momentos privados a lo largo de su jornada laboral. Capta la diferencia entre un trabajador que lee solo noticias centristas de los principales medios y otro que lee periodismo progresista independiente. Recoge quién lee artículos sobre la organización sindical, sobre la aplicación de las leyes de inmigración, sobre las afiliaciones políticas de los ejecutivos de Silicon Valley. Recoge, en otras palabras, exactamente aquella información que los empleados de cualquier entorno políticamente sensible les interesa mantener en privado frente a su empleador. La garantía del memorándum de que estos datos «no se utilizarán para evaluaciones de rendimiento» merece exactamente el escepticismo que ha recibido. Meta tiene un historial documentado de hacer promesas sobre el uso de datos y luego incumplirlas. Sus condiciones de servicio dijeron en su día que no venderían los datos de los usuarios. Los Facebook Papers documentaron que las decisiones internas habitualmente priorizan la participación y los beneficios por encima de las políticas de seguridad a las que Meta se comprometió públicamente. La empresa que despidió a 1.108 trabajadores kenianos por haber hablado con periodistas sobre lo que veían en sus pantallas de trabajo está pidiendo a sus empleados estadounidenses que confíen en que sus datos de pulsaciones de teclas permanecerán en el proceso de formación y no irán a ningún otro sitio. La historia no respalda esa confianza. Los datos son el valor. Los datos se utilizarán. El memorándum sobre superinteligencia: la arquitectura organizativa detrás de MCI MCI no surgió de la nada. Es la expresión operativa de una reestructuración corporativa que Zuckerberg anunció unas semanas antes, y que revela precisamente cómo Meta está abordando el problema del suministro de datos, que constituye el núcleo de sus ambiciones en materia de IA. En un memorándum publicado íntegramente por la CNBC, Zuckerberg anunció la creación de Meta Superintelligence Labs, o MSL, una nueva unidad que consolida todo el desarrollo de modelos de IA, los equipos de producto y la investigación fundamental en IA de Meta bajo un único mando. Para dirigirla, Zuckerberg nombró a Alexandr Wang, el antiguo director ejecutivo de Scale AI, de 28 años, en la que Meta adquirió una participación del 49 % por 14.300 millones de dólares, calificándolo de «el fundador más impresionante de su generación» y creando para él el nuevo cargo de director de IA. El nombramiento de Wang no fue meramente simbólico. Scale AI construyó todo su negocio en torno a una capacidad específica: recopilar datos de flujos de trabajo de contratistas para entrenar sistemas de IA. Wang dijo en 2024: «Para muchas de las capacidades que queremos incorporar a los modelos, el mayor obstáculo es, en realidad, la falta de datos. No hay un conjunto de datos realmente valiosos sobre los agentes que estén simplemente disponibles. Por eso tenemos que averiguar cómo producir datos de muy alta calidad». (Fuente: Entrepreneur, «Mark Zuckerberg anuncia Meta Superintelligence Labs», https://us.entrepreneur.com/business-news/mark-zuckerberg-reveals-meta-superintelligence-lab s/494047; Platformer, ibíd).

MCI es la forma en que Meta produce esos datos. Y los trabajadores que los generan son, en términos estructurales, la versión de Meta de la plantilla de contratistas de Scale, salvo que estos trabajadores tienen salarios, opciones sobre acciones y la expectativa de que su empleador no grabe su pantalla de forma permanente ni introduzca el resultado en un modelo diseñado para eliminar sus puestos de trabajo. Zuckerberg comprometió hasta 135.000 millones de dólares en gastos de

capital para 2026 con el fin de construir la infraestructura de IA de Meta. Al mismo tiempo, la empresa confirmó que despediría al diez por ciento de su plantilla, aproximadamente 8.000 personas, y que no cubriría otras 6.000 vacantes. Estos anuncios se produjeron la misma semana que el MCI. (Fuente: Fortune, «Meta comenzará a rastrear las pantallas y las pulsaciones de teclas de los empleados para entrenar herramientas de IA», 21 de abril de 2026, https://fortune.com/2026/04/21/meta-will-start-tracking-employees-screens-and keystrokes-to-train-ai/). La recopilación de datos y el desplazamiento no son historias paralelas. Son la misma historia, en secuencia. Capturar el conocimiento. Entrenar el modelo. Reducir la plantilla. Repetir. Zuckerberg ofreció su visión en la conferencia sobre resultados que precedió a estos anuncios. «Estamos empezando a ver cómo proyectos que antes requerían grandes equipos ahora los lleva a cabo una sola persona con mucho talento», dijo a los inversores. Esta frase es el manual de instrucciones para todo lo que viene a continuación. Se está registrando el proceso cognitivo de esa persona con talento. La IA entrenada con ello acabará realizando ese proceso sin necesidad de esa persona. El elogio es el anuncio del mecanismo. Y los empleados a los que se elogia están financiando el mecanismo con cada pulsación de tecla. En un memorándum interno aparte, el director técnico de Meta, Andrew Bosworth, describió el objetivo con igual claridad: «La visión hacia la que nos dirigimos es aquella en la que nuestros agentes realizan principalmente el trabajo y nuestro papel es dirigir, revisar y ayudarles a mejorar». Lo denominó un «circuito cerrado»: agentes que «verían automáticamente dónde considerábamos necesario intervenir para que pudieran hacerlo mejor la próxima vez». (Fuente: Detroit News, «Movimientos del ratón y pulsaciones de teclas de los empleados de Meta, datos de entrenamiento de IA», 21 de abril de 2026, https://eu.detroitnews.com/story/tech/2026/04/21/metaemployee-mouse-movements-keystrokes -ai-training-data/89717625007/). Las personas cuyas pulsaciones de teclas se registran para entrenar a los agentes son, en palabras del propio Bosworth, aquellas cuyos trabajos están destinados a realizar los agentes. Que nadie pretenda lo contrario. El patrón completado: del almacén a la estación de trabajo, del cuerpo a la mente Quiero ser preciso sobre lo que distingue a MCI de todas las formas anteriores de vigilancia de los trabajadores documentadas en este capítulo. La supervisión que Amazon ejerce sobre sus trabajadores de almacén tiene como objetivo controlar el ritmo del trabajo físico. Las pulseras escaneables, las cuotas de productividad, los sistemas de disciplina algorítmica: todo ello está diseñado para maximizar el rendimiento por cuerpo, hasta que el cuerpo sea sustituido por una máquina. Lo que se extrae es energía física. Lo que se rompe es el cuerpo: los tendones, las espaldas, los manguitos rotadores de las personas que empaquetan cajas a velocidades que, según el propio informe interno de Amazon, causan lesiones de forma directa. El MCI de Meta extrae algo diferente y más íntimo: el proceso cognitivo de una mente humana en acción. Las secuencias de clics que guían una compleja decisión de ingeniería. Los atajos de teclado que representan años de conocimiento profesional acumulado. Los árboles de decisión integrados en la forma en que un gestor de producto experimentado se mueve por las herramientas de su trabajo diario. La correspondencia con un médico que aparece en pantalla durante ese trabajo. El extracto de la tarjeta de crédito abierto en una pestaña del navegador. El artículo político leído durante la pausa para comer. El mensaje de un familiar sobre una crisis de salud. No se trata de medir energía. Se trata de la digitalización de una vida humana, tanto la parte profesional como la personal por igual, porque los seres humanos que desarrollan su jornada

laboral frente a una máquina no clasifican sus acciones en categorías definidas, que un programa de seguimiento puede separar. La vida privada los sigue al trabajo. La máquina captura todo lo que ve. El trabajador del almacén de Amazon cuyo cuerpo se consume al servicio de la entrega al día siguiente no recibe ninguna participación en el imperio logístico que su trabajo ha construido. El ingeniero de Meta, a quien se le extraen su proceso cognitivo, su historial médico, datos financieros y opiniones políticas, para introducirlos en un proceso de entrenamiento de IA, tampoco recibe ninguna participación a partir del agente que ha sido entrenado con sus pulsaciones de teclas. En ambos casos, el trabajador es la materia prima. En ambos casos, se le dice al trabajador que debe estar agradecido por la oportunidad de contribuir. Y en ambos casos, el resultado final es el mismo: el trabajador queda desplazado por el mismo producto que su trabajo ha creado, mientras que su información más privada permanece en un proceso al que ya no puede acceder ni controlar. Los moderadores de contenido de Nairobi son la mano de obra invisible del pasado de Meta: mal pagados, deslocalizados y descartados cuando se volvieron un estorbo. Los ingenieros y gestores de producto sometidos a MCI son la mano de obra invisible del presente de Meta: bien remunerados, estadounidenses e igualmente impotentes una vez completada la extracción. La geografía es diferente. El salario es diferente. Las sillas tienen mejor soporte lumbar. Pero, la posición estructural es idéntica: son un costo de insumo que hay que minimizar y un recurso de datos que hay que recolectar, y esos dos hechos existen en secuencia, no en conflicto. Para ser claro, mi estado de salud no es asunto de Meta. La medicación que tomo durante mi horario laboral no es asunto de Meta. El número de tarjeta de crédito que aparece en mi pantalla cuando pago una factura durante la hora del almuerzo no es asunto de Meta. El artículo político que leo, la fuente de noticias que prefiero, la afiliación política que pueda o no tener. Nada de eso es propiedad de la empresa que instaló el software en mi ordenador y que me dijo que la solución era dejar de consultar mi correo electrónico personal en el trabajo. Esto no es una disputa sobre los términos del servicio. Es una violación del derecho humano básico a la vida privada, un derecho que no se suspende cuando te sientas en tu escritorio por la mañana y se reanuda cuando cierras sesión por la noche. La legislación estadounidense lo ha reconocido históricamente. La cuestión es si la ley actuará con la suficiente rapidez como para detener lo que Meta está haciendo antes de que los datos se hayan entrenado en un modelo que no pueda desentrenarse. Un tonto con una herramienta sigue siendo un tonto. Una empresa que recopila las mentes de sus empleados, sus historiales médicos, sus vidas financieras y sus identidades políticas para construir las máquinas que los sustituyen, es algo más deliberado que una simple tontería. Está funcionando exactamente como se diseñó. *Fuentes: Reuters, «Meta informa a sus empleados de que está rastreando sus pulsaciones de teclas para entrenar la IA», 21 de abril de 2026: https://www.reuters.com/technology/meta-tells-employees-its tracking-their-keystrokes-train-ai-2 026-04-21/ CNBC, «Meta rastrea las pulsaciones de teclas de sus empleados en Google, LinkedIn y Wikipedia como parte de una iniciativa de entrenamiento de IA», 22 de abril de 2026: https://www.cnbc.com/2026/04/22/meta-tracks-employee-usage-on-google-linkedin-ai-training-p roject.html Fortune, «Meta comenzará a rastrear las pantallas y las pulsaciones de teclas de los empleados para entrenar herramientas de IA», 21 de abril de 2026: https://fortune.com/2026/04/21/meta-will-start-tracking-employees-screens-and-keystrokes-to-train-ai/ Platformer, «La semana en que los empleados de Meta se convirtieron en datos de entrenamiento», abril de 2026: https://www.platformer.news/meta-mci-*

monitoring layoffs-knowledge-work/ Detroit News, «Los movimientos del ratón y las pulsaciones de teclas de los empleados de Meta, datos de entrenamiento de IA», 21 de abril de 2026: https://eu.detroitnews.com/story/tech/2026/04/21/metaemployee-mouse-movements-keystrok es -ai-training-data/89717625007/ Entrepreneur, «Mark Zuckerberg revela los laboratorios de superinteligencia de Meta»: https://us.entrepreneur.com/business-news/mark-zuckerberg-reveals-meta-superintelligence-lab s/494047 ArtVoice, «Meta está registrando las pulsaciones de teclado y los clics del ratón de sus empleados para entrenar a una IA que podría llegar a sustituirlos», 22 de abril de 2026: https://artvoice.com/2026/04/22/meta-is-recording-its-employees-keystrokes-and-mouse-clicks-t o-train-ai that-could-eventually-replace-them/

La obligación social que se ha abandonado

Todas las grandes empresas tecnológicas que han construido su imperio sobre la mano de obra humana han hecho, implícita o explícitamente, un pacto con la sociedad que hace posible su éxito. Este pacto es más o menos así: ustedes nos dan su mano de obra, sus datos, su gasto de consumo, su infraestructura y su tolerancia regulatoria. A cambio, les damos puestos de trabajo, participación económica y una parte, por modesta que sea, de la prosperidad que generamos. Amazon ha roto este pacto. Meta también lo ha roto. Todas las grandes empresas tecnológicas que externalizan su mano de obra más traumática a países con salarios bajos, pagan por debajo del salario mínimo, controlan a los trabajadores con niveles de vigilancia minuciosos, mantienen índices de lesiones que se consideran inaceptables en cualquier otro sector y, además, se preparan para automatizar los puestos de trabajo mientras registran beneficios récord, todas ellas han roto este pacto. El accionista no es la única parte interesada. Esta no es una idea radical. Es la base de toda ley laboral, de toda normativa de seguridad en el trabajo, de todo salario mínimo, de todo derecho de sindicación por el que los trabajadores han luchado y lo han conseguido. Una empresa existe en una comunidad. Utiliza las carreteras de esa comunidad, su agua, su mano de obra calificada, su sistema legal, sus tribunales, y toda la infraestructura pública que hace posible el comercio. La empresa le debe algo a cambio a esa comunidad. Lo que Amazon le debe a los trabajadores de sus almacenes no es solo un sueldo. Son condiciones de trabajo que no les destrocen el cuerpo. Son índices de lesiones que no sean 2,6 veces superiores a la media del sector. Es una explicación honesta de lo que la automatización supondrá para sus sustentos de vida, y un plan de transición que los trate como seres humanos en lugar de unidades de mano de obra cuya vida productiva ha expirado. Lo que Meta le debe a los moderadores de contenido que ha contratado a través de subcontratistas en Nairobi no es un despido con seis días de preaviso. Es la atención de salud mental proporcional al trauma que ha provocado. Es una indemnización por el daño psicológico que ha infligido de forma deliberada, sistemática y lucrativa. Es un reconocimiento básico de que las personas a las que contrató para ver decapitaciones, explotación sexual infantil y material íntimo capturado a través de gafas inteligentes no son componentes desechables de un flujo de datos, sino seres humanos cuyo sufrimiento fue un costo del que Meta decidió deshacerse, en lugar de internalizarlo. Los trabajadores no pueden ser quienes absorben las externalidades de los beneficios de las grandes tecnológicas. Este es el argumento que defiende este capítulo. No es un argumento nuevo. Es el argumento más antiguo de la historia del trabajo. Pero hay que volver a plantearlo, porque las empresas que toman las decisiones se han convencido a sí mismas, y a muchos de sus accionistas, de que ya no se les aplica a ellas. Pero sí que se les aplica

a ellas. Siempre les aplicará. El arco de la responsabilidad, como el arco de la historia, es largo. Y he visto lo suficiente como para saber que se curva. --- Los trabajadores que acabo de documentar son invisibilizados a propósito. Lo mismo ocurre con otras cosas. En el capítulo nueve, me centro en un tipo diferente de borrado: no de mano de obra y cuerpos, sino de voz y pruebas. Las mismas plataformas que extraen valor de los trabajadores de Kenia y de los almacenes de Nueva Jersey han borrado al mismo tiempo el testimonio de todo un pueblo asediado. Lo que sigue es el registro documentado de cómo Meta, TikTok, X, YouTube y LinkedIn silenciaron a Palestina, y por qué ese silenciamiento no es un fallo del sistema, sino una de sus características más constantes.

CAPÍTULO NUEVE. EL TELÓN DE ACERO DIGITAL

Cómo Meta, TikTok, X, YouTube y LinkedIn silenciaron a Palestina.

Hay un término para lo que ocurre cuando un gobierno controla lo que sus ciudadanos pueden ver, decir y compartir. Lo llamamos censura, e históricamente lo hemos asociado con regímenes autoritarios: los bloqueos de información de la era soviética, los cortafuegos de Internet chinos, los medios de comunicación estatales norcoreanos. No esperábamos encontrarlos operando al alcance de la mano de un algoritmo de Silicon Valley valorado en miles de millones de dólares, ahogando silenciosamente las voces de un pueblo asediado mientras caían las bombas. Pero eso es precisamente lo que ocurrió. Y sigue ocurriendo. Desde el 7 de octubre de 2023, las plataformas de redes sociales más poderosas del planeta, Instagram y Facebook de Meta, TikTok, X (antes Twitter), YouTube y LinkedIn, han funcionado como una máquina de represión coordinada, aunque no siempre de forma consciente. Se ha bloqueado a periodistas sin explicación alguna. Se han borrado los archivos de organizaciones de derechos humanos. A los activistas que documentaban las muertes de civiles se les ha aplicado un «shadowban» que los ha convertido en invisibles. Las pruebas de posibles crímenes de guerra, vídeos, fotografías, testimonios de primera mano, han sido eliminadas del registro público a petición de un gobierno extranjero, con un índice de cumplimiento que debería escandalizar a toda persona a la que alguna vez se le haya dicho que estas plataformas defienden la libertad de expresión. No es así. Defienden el lucro y la protección política. Este capítulo documenta lo que hicieron, plataforma por plataforma, y quién pagó el precio. Meta: Instagram y Facebook — El censor preferido de un gobierno La magnitud de la represión de Meta contra las voces palestinas durante el genocidio en Gaza es indiscutible. Está documentada, cuantificada y, en palabras de la propia Meta, admitida. En diciembre de 2023, Human Rights Watch publicó un informe histórico de 51 páginas, titulado «Las promesas incumplidas de Meta: censura sistémica de contenidos sobre Palestina en Instagram y Facebook», que documentaba más de 1.050 casos verificados de eliminación y supresión de contenidos procedentes de más de 60 países solo entre octubre y noviembre de 2023. El patrón no era aleatorio. Era sistemático: se eliminaban contenidos, se suspendían cuentas sin explicación, se impedía la búsqueda de hashtags, se desactivaban las funciones de Instagram Live y se aplicaba la silenciosa restricción algorítmica conocida como «shadowbanning», que reduce la visibilidad de una publicación o una cuenta sin notificarlo a la persona silenciada. El periodista palestino Ahmed Shihab-Eldin, cuya cuenta de Instagram tenía casi un millón de seguidores, perdió el acceso a su cuenta en cinco ocasiones en las semanas posteriores al 7 de octubre. No fue el único. (Fuente: Human Rights Watch, «Meta's Broken Promises», diciembre de 2023, https://www.hrw.org/report/2023/12/21/metas-broken promises/systemic-censorship-palestine-content-instagram-and). El mecanismo que Meta utilizó con mayor frecuencia fue su política de «Organizaciones e individuos peligrosos», un amplio marco de moderación de contenidos que incorpora las listas de designación de terroristas del gobierno de Estados Unidos. Dado que Hamás figura en esa lista y gobierna Gaza, los sistemas automatizados de Meta marcaron y eliminaron

contenidos que simplemente mencionaban a Hamás en un contexto neutral o periodístico. La IA no podía distinguir entre un periodista que documentaba una declaración de Hamás y una persona que expresaba su apoyo a la violencia. Marcaba a ambos. Según Human Rights Watch, Meta eliminó incluso menciones neutrales a Hamás en relación con los acontecimientos en Gaza. El resultado fue que la información sobre el genocidio más mediático del mundo fue eliminada sistemáticamente de dos de las plataformas más utilizadas en la historia de la humanidad. Lo que hace que esto sea más que un fallo en la moderación de contenidos es el papel del gobierno israelí. Según informes de los medios citados en la investigación de Human Rights Watch, la Unidad Cibernética de Israel envió a Meta y a otras plataformas aproximadamente 9.500 solicitudes de retirada de contenidos en las semanas posteriores al 7 de octubre de 2023, el 60 % de las cuales fueron dirigidas a Meta. Las plataformas respondieron con una tasa de cumplimiento del 94 %. Reflexionemos un momento sobre esta cifra. Cuando un gobierno extranjero envía una lista de contenidos que quiere que se eliminen de una plataforma de redes sociales estadounidense, Meta cumple en el 94 % de los casos. Según informes posteriores, Meta cumplió con aproximadamente el 96 % de las solicitudes de eliminación del gobierno israelí: la tasa de cumplimiento más alta concedida a cualquier país del mundo. Esto no es moderación de contenidos. Se trata de un gobierno extranjero que utiliza a una empresa estadounidense como brazo censor, y la empresa acepta este papel de buen agrado. (Fuente: Access Now, «How Meta Censors Palestinian Voices», febrero de 2024, https://www.accessnow.org/publication/how-meta-censors-palestinian-voices/; World Socialist Web Site, diciembre de 2023, https://www.wsws.org/en/articles/2023/12/22/rrys-d22.html). En octubre y noviembre de 2023, el propio algoritmo de traducción de Meta añadió la palabra «terrorista» a las biografías de los usuarios palestinos de Instagram, de forma automática, sin su conocimiento ni consentimiento. Cuando esto se descubrió y se denunció, Meta lo calificó de fallo. Un error. Un mal funcionamiento técnico. La misma explicación que ha ofrecido, y sigue ofreciendo, cada vez que se descubre que sus sistemas hacen algo que resulta beneficiar a una de las partes de un genocidio. Esta no era la primera infracción de Meta y ellos lo saben. Un informe independiente de 2021 encargado por la propia Meta, y realizado por Business for Social Responsibility, reveló que la moderación de contenidos de la empresa «parece haber tenido un impacto negativo en los derechos humanos de los usuarios palestinos», afectando negativamente su capacidad para documentar y compartir sus experiencias. Meta accedió a introducir cambios. Casi dos años después, Human Rights Watch constató que estos cambios no se han aplicado. Las «promesas incumplidas» del título del informe no se referían a un fracaso inesperado, sino a un patrón documentado de faltas de compromisos y de cumplimiento. (Fuente: Human Rights Watch, https://www.hrw.org/news/2023/12/20/meta-systemic-censorship-palestine-content). TikTok: la plataforma que intentaron prohibir por mostrar demasiada verdad La historia de TikTok en el genocidio en Gaza es diferente a la de Meta y, en cierto modo, más reveladora sobre cómo opera el poder en Silicon Valley y Washington, D.C. A diferencia de Instagram y Facebook, TikTok no se erigió como uno de los principales censores de contenido palestino. Los datos apuntaban en la dirección opuesta. Un análisis del Washington Post de noviembre de 2023 reveló que la etiqueta #freepalestine apareció en TikTok 38 veces más que #standwithisrael, una proporción comparable a la que el mismo estudio encontró en las propias plataformas de Meta. El Centro Árabe para las Redes Sociales descubrió que por cada publicación proisraelí en TikTok,

había aproximadamente 54 publicaciones propalestinas. Periodistas y documentalistas palestinos encontraron en TikTok un canal de distribución que aún no había sido capturado por las fuerzas que buscaban controlar la narrativa. Un ejemplo es la cineasta y periodista ganadora de un premio Emmy, Bisan Owda, cuyos vídeos comenzaban con «Soy Bisan, de Gaza, y sigo viva», alcanzando audiencias a las que los principales medios occidentales no llegaban. (Fuente: Washington Post, «TikTok desactiva el recuento de visualizaciones de hashtags tras la polémica sobre la guerra de Gaza», febrero de 2024, https://www.washingtonpost.com/technology/2024/02/08/tiktok-remove- data-criticism-gaza/). La respuesta de Washington no se hizo esperar. En octubre y noviembre de 2023, senadores republicanos como Josh Hawley y Marco Rubio citaron explícitamente la cobertura de TikTok sobre Gaza como motivo para prohibir la aplicación. El representante Mike Gallagher, impulsor de la legislación para la desinversión de TikTok, argumentó en un artículo de opinión público que la aplicación era responsable de poner a los jóvenes estadounidenses en contra de Israel. La legislación se aprobó. Se ordenó a la empresa matriz china ByteDance que vendiera TikTok o fuese prohibido. El comprador propuesto para las operaciones de TikTok en Estados Unidos era Oracle, la misma Oracle que proporciona infraestructura de bases de datos al aparato de inteligencia del ejército israelí, tal y como se documenta en el capítulo dos de este libro. (Fuente: The Intercept, «La prohibición de TikTok también tiene que ver con ocultar contenido pro-palestino», enero de 2025, https://theintercept.com/2025/01/09/tiktok- ban-israel-palestine-republicans/). Cuando TikTok fue prohibido temporalmente para los usuarios estadounidenses en enero de 2025, una de sus periodistas palestinas más destacadas, Bisan Owda, fue suspendida de forma permanente por la plataforma poco después, sin previo aviso, sin explicación, en lo que ella describió como «presión política vinculada a Israel». Su cuenta, que había documentado el costo humano del genocidio en Gaza en tiempo real ante millones de espectadores, había desaparecido. El medio de comunicación pro-palestino Mondoweiss vio cómo su cuenta de TikTok fue bloqueada de forma permanente, sin previo aviso, durante una oleada anterior de operaciones militares israelíes. TikTok, por su parte, informó que había eliminado 4,7 millones de vídeos y suspendido 300.000 retransmisiones en directo entre el 7 de octubre de 2023 y el 15 de septiembre de 2024, invocando sus políticas contra la promoción de Hamás, el discurso de odio o la desinformación. La plataforma nunca ha respondido públicamente con transparencia a la pregunta de cómo se aplicaron esas políticas y a qué contenidos. (Fuente: Middle East Online, «La propiedad estadounidense de TikTok lleva a la prohibición de influencers palestinos», enero de 2026, https://middle-east-online.com/en/us-ownership-tiktok-leads-bans-palestinian-influencers-journalists; Euronews, octubre de 2024, https://www.euronews.com/next/2024/10/07/human-rights-ngos-say-social-media-platforms-cont inue-to- censor-pro-palestine-content). Lo que revela TikTok no es principalmente una historia sobre la supresión de contenido palestino por parte de la plataforma, sino la historia de una plataforma que está siendo eliminada por ley precisamente porque no lo suprimía. Cuando una plataforma de redes sociales permite que se vea la verdad, Washington interviene. Esta es la lección de TikTok y Gaza. Y es una lección que vale la pena comprender claramente antes de seguir adelante. X / Twitter: la plataforma de la «libertad de expresión» que silenció a Palestina Elon Musk compró Twitter en 2022 declarando su compromiso con la libertad de expresión absoluta. Se posicionó como el libertador de una plataforma

que, según él, había sido estrangulada por la censura liberal. Reactivó cuentas bloqueadas. Despidió a los equipos de confianza y seguridad. Sustituyó a los verificadores de datos profesionales por un sistema de colaboración colectiva llamado «Notas de la comunidad» que funciona, en palabras de sus propios críticos, como el equivalente digital a dejar una queja en un buzón de sugerencias que nadie revisa. Lo que la plataforma de «libertad de expresión» de Musk produjo realmente, en lo que respecta al contenido palestino, fue una aplicación selectiva del silencio. En octubre de 2023, X suspendió cientos de cuentas palestinas, describiéndolas como afiliadas a Hamás, sin aportar pruebas para las determinaciones individuales ni un proceso de apelación significativo. Entre los suspendidos en enero de 2024 se encontraban destacados periodistas y comentaristas cuyas cuentas fueron eliminadas sin previo aviso y sin causa justificada, entre ellos el redactor jefe de Mint Press News, Alan MacLeod; el reportero de The Intercept, Ken Klippenstein, con más de 500.000 seguidores; y un amplio grupo de otros periodistas y activistas de izquierdas y pro-palestinos. Sus cuentas fueron restablecidas horas más tarde. No se dio ninguna explicación. No se mencionó ninguna norma que se hubiera infringido. (Fuente: Al Jazeera, «Twitter Under Fire for Censoring Palestinian Public Figures», febrero de 2023, https://www.aljazeera.com/features/2023/2/28/twitter-under-fire-for-censuring-palestinian-public-figures; World Socialist Web Site, enero de 2024, https://www.wsws.org/en/articles/2024/01/10/doux-j10.html). Mientras se silenciaban las voces palestinas, un informe de noviembre de 2023 del Centro para la Lucha contra el Odio Digital reveló que X no moderaba el 96 % de las publicaciones de discurso de odio relacionadas con el genocidio israelí en Palestina, incluidas aquellas que describían a los palestinos como animales, o que pedían castigos colectivos e incitaban a la violencia contra la población civil. La misma plataforma que suspendió cientos de cuentas palestinas por supuesta afiliación a Hamás estaba dejando la incitación antipalestina en línea en un 96 %. Esto no es una incoherencia. Es una política. La organización de derechos digitales 7amleh documentó más de 19.000 casos de discursos de odio y contenido incitante en hebreo en X en las semanas posteriores al 7 de octubre, contenido que permaneció en línea sin consecuencias. (Fuente: Centro de Empresas y Derechos Humanos, «Un informe denuncia que X no eliminó el 96 % de las publicaciones de discursos de odio», noviembre de 2023, https://www.business-humanrights.org/en/latest-news/report-exposes-xs-failure-to-remove-96-of -hate-speech-posts-amid-israel-palestine-conflict/). En la víspera de Navidad de 2023, Instagram, no X, cerró definitivamente la cuenta del activista Shaun King, que había estado documentando los crímenes de guerra israelíes ante una audiencia masiva. En X, la actriz Susan Sarandon publicó una fotografía de vallas publicitarias que pedían un alto el fuego. Fue señalada como «discurso violento». La valla decía: «Detengan las bombas». Así es la libertad de expresión absoluta cuando la construye y la maneja un hombre que declara públicamente que la empatía es la debilidad fundamental de la civilización. YouTube: Borrar las pruebas El papel de YouTube en la supresión de contenidos palestinos tiene dos fases distintas. La primera es un patrón de discriminación algorítmica que se remonta a años atrás contra los contenidos en lengua árabe procedentes de Cisjordania y Gaza, y que ha sido documentado en investigaciones de 7amleh, Al-Shabaka y Article 19 mucho antes de octubre de 2023. La segunda es más reciente, más directa y más condenatoria: la eliminación por parte de YouTube, a petición de la administración Trump, de más de 700 vídeos que documentan violaciones de los derechos humanos por parte de Israel. El patrón anterior es un contexto

importante. Una investigación realizada por 7amleh y publicada por Al-Shabaka reveló que los sistemas de moderación de contenido basados en IA de YouTube aplicaban lo que los investigadores denominan «discriminación locativa», es decir, marcaban con mayor frecuencia el contenido según el origen geográfico desde donde se sube. Los vídeos procedentes de Cisjordania y Gaza se sometían a un nivel de escrutinio automatizado más alto que el contenido equivalente de otros lugares. El contenido en lengua árabe era marcado de forma desproporcionada en comparación con el contenido en hebreo de igual sensibilidad. Los que impugnaron estas eliminaciones no recibieron ninguna explicación por parte de YouTube, ni disponían de una vía de recurso significativa. La IA de la plataforma dictó una sentencia y no existía tribunal de apelación. (Fuente: Al-Shabaka, «La violación de los derechos digitales palestinos por parte de YouTube», https://al-shabaka.org/briefs/youtubes-violation-of-palestinian-digital-rights-what-needs-to-be-do ne/). Luego, en octubre de 2025, YouTube borró discretamente las cuentas de tres de las organizaciones de derechos humanos más importantes de Palestina: Al-Haq, el Centro Al Mezan para los Derechos Humanos y el Centro Palestino para los Derechos Humanos, la organización de derechos humanos más antigua de Gaza, según la designación de las Naciones Unidas. Junto con estas cuentas desaparecieron más de 700 vídeos: investigaciones sobre ataques israelíes contra civiles, testimonios de supervivientes, un documental sobre madres que sobrevivieron al genocidio en Gaza y una investigación filmada sobre el asesinato de la periodista palestino-estadounidense Shireen Abu Akleh. El contenido no fue eliminado por ser violento. El contenido no fue eliminado por violar las normas de la comunidad. Fue eliminado porque el gobierno de Estados Unidos sancionó a estas organizaciones por cooperar con la investigación de la Corte Penal Internacional sobre funcionarios israelíes. YouTube confirmó a The Intercept que las eliminaciones se realizaron para cumplir con las sanciones de Estados Unidos. Katherine Gallagher, abogada sénior del Centro para los Derechos Constitucionales, calificó de «indignante que YouTube impulse la agenda de la administración Trump de eliminar de la vista del público las pruebas de violaciones de derechos humanos y crímenes de guerra». Sarah Leah Whitson, de Democracy for the Arab World Now, lo describió como «un acto decepcionante de sumisión». El Centro Palestino para los Derechos Humanos afirmó sin rodeos que las acciones de YouTube «protegen a los responsables de rendir cuentas». (Fuente: The Intercept, «YouTube borró discretamente más de 700 vídeos que documentaban violaciones de los derechos humanos por parte de Israel», noviembre de 2025, https://theintercept.com/2025/11/04/youtube-google-israel-palestine-human-rights-censorship/; Common Dreams, https://www.commondreams.org/news/youtube-deletes-videos-israel). Permítanme ser claro sobre lo que esto significa. YouTube, una filial de Google, que tiene un contrato de servicios en la nube por valor de 1.200 millones de dólares con el ejército israelí a través del Proyecto Nimbus, eliminó pruebas de posibles crímenes de guerra cometidos por el ejército israelí, a petición de una administración estadounidense que ha protegido a Israel de rendir cuentas ante la Corte Penal Internacional. No se trata de una decisión de moderación de contenidos. Se trata de la complicidad corporativa en la eliminación de un registro histórico. Es el equivalente digital a quemar documentos antes del juicio. LinkedIn: la red profesional que te vigila LinkedIn se presenta como la cara respetable de Silicon Valley: la plataforma para currículos y liderazgo intelectual, para hitos profesionales y networking en el sector. Es propiedad de Microsoft, cuya infraestructura en la nube, tal y como se documenta en el

capítulo dos, está integrada en los sistemas operativos del ejército israelí. En abril de 2026, LinkedIn fue objeto de una demanda colectiva y de un exhaustivo informe de investigación que sacó a la luz una de las operaciones de vigilancia encubierta más amplias de la historia empresarial. La investigación, publicada por una organización de investigación sin fines de lucro llamada Fairlinked y bautizada como «BrowserGate», reveló que cada vez que un usuario visita linkedin.com en un navegador basado en Chrome, un programa JavaScript oculto escanea silenciosamente su dispositivo en busca de extensiones de navegador instaladas. El programa se ejecuta sin ningún indicador visible, no solicita consentimiento y no revela nada. Envía sus hallazgos, una huella digital precisa del entorno del navegador del usuario, directamente a los servidores de LinkedIn. La escala de la operación ha crecido de forma espectacular: LinkedIn buscaba 38 extensiones específicas en 2017. En 2024, esa cifra aumentó a 461. En febrero de 2026, alcanzó las 6.167, lo que supone un aumento del 1.252 % en dos años. El 7 de abril de 2026 se presentó una demanda colectiva ante el Tribunal de Distrito de los Estados Unidos para el Distrito Norte de California, en la que se acusaba a LinkedIn de operar un «sistema de vigilancia encubierto» integrado en su propio sitio web. (Fuente: CyberInsider, «LinkedIn se enfrenta a una demanda colectiva por el supuesto escaneo encubierto de los navegadores de los usuarios», abril de 2026, https://cyberinsider.com/linkedin-faces-class-action-over-alleged-covert-scanning-of-users-browsers/; Cybernews, https://cybernews.com/privacy/linkedin-lawsuits-illegal-browser-extension-tracking/). La importancia de esta vigilancia va más allá de la violación de la privacidad en sí misma. El informe de Fairlinked sostiene, y la demanda colectiva alega, que los datos recopilados a través de este escaneo del navegador son lo suficientemente precisos como para permitir a LinkedIn inferir atributos sensibles sobre los usuarios: afiliaciones políticas, creencias religiosas, condiciones de salud, afiliación sindical y orientación ideológica. La huella digital persiste tras el restablecimiento de las cookies. En una época en la que la defensa de la causa palestina ha sido clasificada por algunos gobiernos como motivo de discriminación laboral, control de inmigración e incluso investigación penal. Una red profesional que puede identificar silenciosamente tus inclinaciones políticas a partir de tu perfil de navegador no es una herramienta neutral. Es un instrumento de vigilancia integrado en la infraestructura profesional de más de mil millones de personas en todo el mundo. En octubre de 2024, la Comisión de Protección de Datos de Irlanda multó a LinkedIn con 310 millones de euros por tratar los datos personales de los usuarios con fines de publicidad dirigida sin una base jurídica válida. Esta es la mayor multa jamás impuesta a LinkedIn en el marco del RGPD europeo. Las revelaciones de BrowserGate sugieren que el problema va más allá de la publicidad. (Fuente: The Next Web, «LinkedIn BrowserGate: Extension Scanning, Privacy, Fingerprint», abril de 2026, https://thenextweb.com/news/linkedin-browsergate-extension-scanning-privacy fingerprint; SecurityWeek, https://www.securityweek.com/browsergate-claims-of-linkedin-spying-clash-with-security-resear ch findings/). LinkedIn ha negado que utiliza los datos escaneados para deducir información confidencial sobre los usuarios. Afirma que el escaneo es una medida de seguridad para detectar herramientas que violan sus condiciones de servicio al extraer datos sin consentimiento. Esta es una explicación plausible para escanear docenas de herramientas de extracción conocidas. No es una explicación plausible para escanear 6.167 extensiones de navegador, incluidas extensiones para la productividad personal, el seguimiento de la salud, la

investigación política y la organización de comunidades religiosas. En algún momento, una medida de seguridad se convierte en una infraestructura de vigilancia. La demanda determinará en qué categoría se enmarca el comportamiento de LinkedIn. Lo que no se discute es que el escaneo se llevó a cabo, que no se informó a los usuarios, que no se solicitó consentimiento y que los datos fueron a parar a los servidores de LinkedIn. Una plataforma propiedad de Microsoft, una empresa cuyos sistemas en la nube son herramientas documentadas de selección de objetivos militares. Preguntarse para qué se utilizan en última instancia esos datos no es paranoia. Es la pregunta correcta que hay que plantearse.

«La guerra contra los mapas: cómo las grandes tecnológicas borran a un pueblo antes de que caigan las bombas»

Existe una forma de violencia que tiene lugar antes del primer ataque aéreo. Antes del primer puesto de control. Antes de que se derribe la primera casa. Ocurre en una pantalla, a un nivel de zoom, en las silenciosas decisiones políticas de los ingenieros y jefes de producto que deciden qué lugares merecen un nombre en un mapa, y cuáles no.

Quiero hablar de mapas.

Porque si has estado prestando atención a lo que está sucediendo en el Líbano, si abriste Apple Maps durante el bombardeo israelí de abril de 2026 y miraste la parte sur del país, viste algo que dejó a la gente helada. La mayor parte estaba en blanco. Las aldeas no estaban etiquetadas. Las ciudades que existieron durante siglos, aquellas donde se les ordenó a las familias que evacuaran bajo amenaza de bombardeo, simplemente no aparecían. Mientras tanto, en la misma aplicación, las pequeñas comunidades israelíes al otro lado de la frontera, Nahariyya, Shelomi, Beit Jan, estaban claramente etiquetadas, con sus nombres en el mapa como si el propio paisaje hubiera tomado partido. (Fuente: The New Arab, «¿Borró Apple los nombres de los pueblos libaneses de sus mapas?», abril de 2026, https://www.newarab.com/news/did-apple-erase-lebanese-village-names-its-maps).

La explicación de Apple, fue que estos pueblos libaneses nunca estuvieron en la aplicación para empezar, y que la versión detallada de Apple Maps aún no ha completado su despliegue global en el Líbano, lo que puede ser técnicamente cierto. Sin embargo, varios verificadores de datos confirmaron que las quejas archivadas de los usuarios sobre la escasa cobertura de Apple Maps en el Líbano se remontan a 2019, años antes de que todo esto comenzara. No estoy afirmando que Apple elimina pueblos en tiempo real mientras caen las bombas israelíes, porque las pruebas no respaldan esta afirmación concreta.

Lo que estoy diciendo es algo más inquietante.

Los pueblos nunca estuvieron ahí en los mapas. Y las comunidades israelíes, al otro lado de la frontera, siempre estuvieron.

Esta disparidad no comenzó en abril de 2026. No fue creada por el genocidio actual. Es la base. Es la configuración predeterminada. Es como se ven estas aplicaciones en un día cualquiera, cuando nadie presta atención y nadie compara capturas de pantalla una al lado de la otra y nadie se pregunta por qué ciertos lugares que han estado habitados durante siglos simplemente no aparecen en la herramienta de navegación más utilizada en la historia de la humanidad.

Esto no es una limitación técnica. Es una elección política que, con el paso de los años, se convierte en algo que parece un borrado, porque lo es.

Google Maps y el mapa que nunca dijo Palestina

Permítanme ser específico, porque la especificidad es lo que separa la documentación de la acusación.

Google Maps nunca ha etiquetado a Palestina como un Estado. Ni una sola vez desde que el servicio se lanzó en 2005. Cisjordania y la Franja de Gaza aparecen como regiones geográficas sin designación nacional, mientras tanto Israel aparece plenamente etiquetado como país con Jerusalén identificada como su capital. Esto a pesar de que el estatus de Jerusalén está claramente definido en todos los marcos internacionales entre ellos, la Resolución 181 de la Asamblea General de la ONU que en 1947 le otorgó a Jerusalén estatus internacional , y la opinión consultiva de 2024 donde la Corte Internacional de Justicia determina que la soberanía israelí sobre Jerusalén Este no está reconocida por el derecho internacional.

Los asentamientos aparecen etiquetados como si estuvieran dentro de Israel. No es así. Son ilegales en virtud del artículo 49 del Cuarto Convenio de Ginebra, que prohíbe a una potencia ocupante trasladar a su población civil a territorio ocupado. Pero en Google Maps aparecen como comunidades, como cualquier otra —con nombres claramente visibles, rutas calculadas, distancias medidas—, mientras que las aldeas palestinas de la Zona C de Cisjordania, tierras que han sido cultivadas y habitadas durante generaciones, solo aparecen cuando se amplía tanto el mapa que ya se han pasado de largo.

Luego está la cuestión de las rutas. 7amleh, el Centro Árabe para el Avance de las Redes Sociales, publicó un informe detallado en el que se examinan las decisiones de navegación de Google Maps en los territorios ocupados. Cuando un palestino de Cisjordania intenta navegar de Belén a Ramala —un trayecto de 36 kilómetros—, Google Maps le lleva por Jerusalén. A la que la mayoría de los palestinos no pueden acceder legalmente. Los residentes palestinos de Gaza y Cisjordania llevan tarjetas de identificación verdes que restringen su movimiento. No pueden utilizar las carreteras exclusivas para israelíes. No pueden cruzar a Jerusalén sin un permiso que la mayoría de ellos no tiene. Google Maps, basado en los datos geoespaciales más sofisticados de la historia de la humanidad, no puede encontrar una ruta. Dirige a las personas hacia carreteras por las que serán detenidas si las utilizan. (Fuente: +972 Magazine, «Lost in Occupation: How Google Maps Is Erasing Palestine», https://www.972mag.com/mapping-occupation-how-google-erases-palestine-from-its-maps/).

La Enmienda Kyl-Bingaman —una ley estadounidense aprobada en 1997— restringe la resolución de las imágenes satelitales que las empresas estadounidenses pueden proporcionar sobre Israel y los territorios palestinos ocupados. Las imágenes de alta resolución que están disponibles libremente sobre todos los demás países de Oriente Medio se degradan deliberadamente sobre Israel-Palestina. Los investigadores que intentan documentar la destrucción de pueblos, la construcción de asentamientos y las pruebas de posibles crímenes de guerra disponen de una menor resolución fotográfica con la que trabajar en este proyecto de limpieza étnica en particular que la que tendrían al analizar cualquier situación comparable en cualquier otro lugar de la región. No se trata de un accidente tecnológico. Se trata de una ley aprobada por el Congreso de los Estados Unidos específicamente para proteger la capacidad de un país de actuar sin escrutinio fotográfico. (Fuente: Al-Shabaka, «Mapas, tecnología y prácticas espaciales descoloniales en

Palestina», https://al-shabaka.org/briefs/maps-technology-and-decolonial-spatial-practices-in-palestine/).

En agosto de 2016, los mapas de Google eliminaron por completo las etiquetas «Cisjordania» y «Franja de Gaza». No los territorios en sí, solo sus nombres. Desaparecieron del mapa como si las denominaciones geográficas que todo el mundo utiliza para referirse a estos lugares simplemente ya no existieran. Más de 615.000 personas firmaron una petición: «Google: pon Palestina en tus mapas». Google lo calificó de error. Restableció las etiquetas. No dijo nada más. (Fuente: +972 Magazine, ibíd.).

Un error. La empresa de cartografía más sofisticada del planeta, una empresa que envía coches por todas las carreteras de todos los países, que ha cartografiado el fondo marino, que puede decirte el horario de un restaurante en Reikiavik, eliminó accidentalmente las únicas etiquetas geográficas que reconocían la existencia del territorio palestino.

Quiero que compares esa explicación con lo que sabes sobre estas empresas. No se trata de organizaciones que cometen errores por descuido en la geografía de territorios en disputa. Son organizaciones con equipos enteros de especialistas en políticas, oficinas de enlace con el gobierno, departamentos jurídicos y consultores de riesgo geopolítico cuyo trabajo consiste precisamente en gestionar este tipo de decisiones. Cada elección de etiquetado en Google Maps es una decisión política. Cada algoritmo de rutas refleja supuestos implícitos sobre quién puede ir a dónde. Cada omisión de una aldea palestina es una decisión de no mostrarla: una elección tomada, revisada y aprobada por seres humanos en oficinas de Mountain View y Cupertino que entendían lo que estaban eligiendo.

Lo que hace un mapa antes de que caigan las bombas.

Hay una razón por la que los ejércitos siempre han dado prioridad al borrado cartográfico. Un lugar sin nombre en un mapa es más difícil de defender ante el derecho internacional. Es más difícil informar desde allí. Es más difícil llorar su pérdida. Cuando un periodista publica una noticia sobre un ataque aéreo y la ubicación no aparece en ninguna de las principales aplicaciones de mapas, la noticia se vuelve más difícil de situar —y más difícil de verificar— , en definitiva, más difícil de visualizar para un público que navega por el mundo a través de aplicaciones creadas por empresas tecnológicas estadounidenses.

En el sur del Líbano, durante el bombardeo de abril de 2026, Israel ordenó a cientos de miles de personas que evacuaran pueblos que no aparecían en los mapas que la mayor parte del mundo utilizaba para seguir la noticia. El espacio en blanco en el mapa no fue la causa del bombardeo. Pero fue cómplice de la invisibilidad de quienes fueron bombardeados. Cuando no puedes encontrar un lugar, es más difícil llorar a las personas que vivían allí.

No voy a permitir que las empresas tecnológicas se escuden tras la palabra «error». No voy a permitir que se escuden tras «plazos de implementación global» mientras un lado de una frontera está en blanco y el otro está completamente etiquetado. Llevo treinta años en este sector. Sé distinguir entre una limitación técnica y una decisión política disfrazada de lenguaje técnico. Y ellos también lo saben.

El mapa no es neutral. Nunca ha sido neutral. La pregunta es: ¿la realidad de quién refleja, y la de quién borra?

Firma la petición en NoEthicsInBigTech.com. Exige que Google etiquete a Palestina como Estado de conformidad con la Resolución 67/19 de la Asamblea General de la ONU, que reconoció a Palestina como Estado observador no miembro con 138 votos. Exige que los asentamientos israelíes ilegales se identifiquen como tales, de acuerdo con todas las disposiciones aplicables del derecho internacional. Exige que los algoritmos de cálculo de rutas tengan en cuenta las restricciones de movimiento impuestas a los palestinos, en lugar de dirigirles por carreteras en las que serán detenidos por utilizarlas. No se trata de exigencias radicales. Son peticiones para reflejar la realidad.

Las empresas que crean los mapas que todos usamos tienen el poder de hacer visible o invisible la ocupación. Han optado, sistemáticamente, por la invisibilidad.

Esa elección tiene consecuencias. Y quienes pagan las consecuencias no están en Mountain View.

El complejo industrial de la vigilancia: del software espía israelí al carrito de la compra del gobierno He dedicado este capítulo a documentar cómo las plataformas de las grandes tecnológicas silencian, censuran y borran las voces de las personas a las que se les ha pedido que supriman. Pero quiero alejarme del mecanismo específico de la censura y abordar algo más fundamental, porque la supresión de la libertad de expresión es solo una de las capas de la arquitectura de vigilancia que se ha construido durante las últimas dos décadas. Debajo hay algo más antiguo, más invasivo y con mayores consecuencias: la infraestructura de la vigilancia. En mi documental *Forever Peace Now*, documenté cómo es realmente la economía de la vigilancia desde dentro, a través del testimonio de ingenieros, defensores de las libertades civiles, personal del Congreso y personas que habían vivido dentro de la máquina el tiempo suficiente como para comprender lo que están haciendo. Lo que descubrí, durante años de estas conversaciones, fue un patrón constante: las herramientas creadas ostensiblemente para protegernos, se estaban utilizando en nuestra contra. Las promesas hechas para vender estas herramientas eran falsas. Y las personas que lo sabían no alzaban la voz lo suficiente como para que el público las oyera. Quiero contarles aquí tres historias. Están relacionadas entre sí. Juntas, describen una infraestructura de vigilancia que no se rige bajo ninguna ley en concreto, que no está controlada por ninguna empresa en particular y que el gobierno estadounidense ha encontrado la manera de utilizarla sin la molestia de tener que obtener una orden judicial. NSO Group y el software espía que asesinó a un periodista NSO Group es una empresa tecnológica israelí que desarrolla herramientas de vigilancia. Específicamente, ha creado un software llamado Pegasus que es, en el lenguaje moderado de la comunidad de ciberseguridad, una de las herramientas más invasivas jamás desplegadas comercialmente contra la población civil. Pegasus puede instalarse en el smartphone de un objetivo sin que el usuario haga nada: no hay que hacer clic en ningún enlace ni abrir ningún archivo. Funciona de forma silenciosa, invisible y exhaustiva. Una vez instalado, puede acceder a mensajes, correos electrónicos, registros de llamadas, fotografías y datos de ubicación. Puede activar el micrófono y la cámara sin que el usuario lo sepa. Convierte tu teléfono en un dispositivo de vigilancia que informa de todo lo que ve y oye a quien haya comprado el acceso. NSO Group vende Pegasus a gobiernos. No a particulares, ni a empresas, sino exclusivamente a gobiernos, que lo utilizan contra periodistas, activistas, abogados, disidentes y políticos de la oposición. La empresa siempre ha sostenido que sus herramientas solo se venden a gobiernos previamente evaluados con fines

legítimos de aplicación de la ley. Los hechos no respaldan esta afirmación. En octubre de 2018, Jamal Khashoggi, un periodista saudí y columnista del Washington Post que había criticado al príncipe heredero Mohammed bin Salman, entró en el consulado de Arabia Saudí en Estambul. Allí fue asesinado. Su cuerpo fue descuartizado. Posteriormente, los investigadores determinaron que el teléfono de Khashoggi había sido infectado con el software espía Pegasus, y que los datos de vigilancia obtenidos a partir de esa infección se habían utilizado para rastrearlo en el período previo a su asesinato. Una herramienta vendida por una empresa israelí a una monarquía del Golfo se utilizó para localizar, rastrear y facilitar el asesinato de este periodista que trabajaba para un periódico estadounidense. (Fuente: Citizen Lab, Universidad de Toronto, informes sobre Pegasus; Washington Post, varias fechas entre 2018 y 2019). En noviembre de 2021, el gobierno de Estados Unidos incluyó a NSO Group en su Lista de Entidades, una designación que impide a las empresas estadounidenses hacer negocios con ella, alegando que NSO había «desarrollado y suministrado software espía a gobiernos extranjeros que utilizaron estas herramientas para atacar maliciosamente a funcionarios gubernamentales, periodistas, empresarios, activistas, académicos y trabajadores de embajadas». Israel, cuyo gobierno tiene autoridad reguladora sobre las licencias de exportación de NSO Group, ha seguido permitiendo que la empresa opere, porque las herramientas que crea sirven a los intereses diplomáticos y de inteligencia israelíes tanto como a los de los gobiernos que las compran. Esto es lo que describí en mi película como el complejo industrial de la vigilancia: la fusión de capacidades de inteligencia de grado militar con modelos de negocio comerciales y relaciones gubernamentales, desplegadas contra poblaciones civiles de todo el mundo. NSO Group es el nodo más visible de este complejo. No es el único. Es simplemente aquel cuyas herramientas se utilizaron para matar a alguien cuyo nombre conoces. El sector tecnológico israelí, cuyos graduados de la Unidad 8200 del Cuerpo de Inteligencia israelí pasan directamente tanto a Silicon Valley como a las startups de tecnología de defensa israelíes, tal como lo documenté en el capítulo dos de este libro, es el mayor exportador mundial de tecnología de vigilancia comercial per cápita. Blue Wolf y Red Wolf, que describí en el capítulo dos como los sistemas de ocupación biométricos desplegados contra los palestinos en Cisjordania, son productos del mismo ecosistema. Los sistemas de selección de objetivos Gospel y Lavender son productos del mismo ecosistema. Y los clientes de esta tecnología de vigilancia no se limitan a democracias con poderes judiciales independientes y prensa libre. Entre ellos se incluyen también gobiernos cuyo historial en materia de derechos humanos está bien documentado y cuyo uso de estas herramientas contra sus propios ciudadanos no es hipotético. El gobierno de Estados Unidos, que incluyó a NSO Group en la Lista de Entidades, ha seguido operando simultáneamente en colaboración con el ecosistema más amplio de tecnología de vigilancia israelí a través del Proyecto Nimbus, mediante la presencia de antiguos miembros de la Unidad 8200 en todo Silicon Valley y a través de los acuerdos de intercambio de inteligencia de la red Five Eyes. La condena de NSO Group y la aceptación de la infraestructura que lo produjo no son contradicciones. Son aplicaciones diferentes de la misma tecnología, al servicio de diferentes amos políticos. El teatro de la privacidad de Apple y la promesa que nunca fue cierta Apple ha construido su marca sobre la premisa de la privacidad. «Lo que pasa en tu iPhone se queda en tu iPhone». El eslogan está en las vallas publicitarias. Está en los anuncios de televisión. Está en los discursos de apertura que Tim Cook pronuncia con la cadencia mesurada de un hombre que ha decidido que la privacidad es un

diferenciador de producto y está dispuesto a tratarla como tal. Llevo treinta años en el sector tecnológico. Sé lo que es un diferenciador de producto. Y conozco la diferencia entre una empresa que trata la privacidad como un valor y una empresa que la trata como una estrategia de marketing. El historial de Apple es, en el mejor de los casos, complicado. Permítanme ser específico sobre lo que quiero decir. En 2021, Apple anunció planes para escanear el contenido de las bibliotecas de fotos de iCloud en busca de material de abuso sexual infantil, un objetivo que es genuinamente importante y moralmente urgente. El problema era el mecanismo: el sistema propuesto por Apple escaneaba las imágenes en los dispositivos de los usuarios antes de que se subieran a iCloud, comparándolas con una base de datos de valores hash de CSAM (material de abuso sexual infantil) conocidos. La Electronic Frontier Foundation y una coalición de investigadores de seguridad y organizaciones de libertades civiles respondieron de inmediato con una carta firmada por más de 90 organizaciones de todo el mundo: el sistema, por muy bien intencionado que fuera en su diseño inicial, creaba una infraestructura que podía ser reutilizada. Un sistema de escaneo creado para detectar una categoría de contenido ilegal podría, bajo presión gubernamental o cambios en la política corporativa, ampliarse para escanear otro tipo de contenido, como discursos políticos, material religioso o periodístico. Apple acabó abandonando la propuesta, en base a las preocupaciones de los defensores de la privacidad. Pero el mero hecho de que lo haya propuesto revela algo importante sobre cómo piensa Apple respecto a la privacidad que comercializa. En China, Apple ha eliminado aplicaciones de su App Store china siguiendo instrucciones del gobierno chino, incluidas aplicaciones VPN que permiten a los usuarios eludir la censura, así como aplicaciones utilizadas por los manifestantes en Hong Kong durante las protestas de 2019, e incluso herramientas utilizadas por periodistas que trabajan en un país donde el periodismo requiere protección. Apple ha almacenado los datos de iCloud de los usuarios chinos en servidores gestionados por una empresa estatal china llamada GCBD, lo que significa que las claves de cifrado de las comunicaciones y los datos más privados de los usuarios chinos están en manos de una empresa legalmente obligada a cooperar con el gobierno chino. Apple ha cumplido con las peticiones de dicho gobierno para eliminar el emoji de la bandera de Taiwán de los dispositivos que operan en China. La privacidad que Apple promete a sus usuarios está, en el mercado chino, explícitamente condicionada a lo que el gobierno de ese país esté dispuesto a permitir. Esto no es ninguna sorpresa. Tim Cook ha dicho, con su característica diplomacia corporativa, que Apple cree que puede hacer mejor el bien operando en China que retirándose. No cuestiono la sinceridad de esta creencia. Lo que sí cuestiono es lo que significa en la práctica para los usuarios que confían a Apple sus datos más íntimos, creyendo en la promesa del cartel publicitario, sin saber que esta promesa tiene un límite geográfico que se detiene en las jurisdicciones donde resulta comercialmente inconveniente cumplirla. La mentira del cifrado: cómo la NSA pagó para romper Internet En 2004, la Agencia de Seguridad Nacional (NSA) estadounidense realizó un pago secreto de 10 millones de dólares a RSA Security, en aquel momento una de las empresas más fiables en el ámbito del cifrado comercial, a cambio de convertir un algoritmo específico en el generador de números aleatorios predeterminado de la biblioteca criptográfica BSAFE de RSA, ampliamente distribuida. Este algoritmo se denominaba Dual EC DRBG: Generador de bits aleatorios determinista de curva elíptica dual. RSA comunicó a sus clientes que se trataba de un algoritmo aprobado y seguro. RSA había depositado su confianza en

las normas y directrices del NIST (Instituto Nacional de Estándares y Tecnología), el organismo del gobierno de Estados Unidos responsable de certificar que las normas de cifrado sean lo que dicen ser. Los criptógrafos ya habían señalado problemas con el Dual EC DRBG en 2007. Las matemáticas del algoritmo sugerían, a cualquiera que lo examinara detenidamente, que podría existir una relación secreta entre dos de sus parámetros claves, lo que permitiría a quien conociera dicha relación predecir sus resultados. En otras palabras: una puerta trasera. Una forma de descifrar las comunicaciones que los usuarios creían protegidas. En 2013, los documentos filtrados por Edward Snowden confirmaron lo que las matemáticas habían sugerido. La NSA había insertado deliberadamente la puerta trasera en Dual EC DRBG, la había impulsado a través del proceso de estandarización del NIST para darle la apariencia de una certificación independiente, había pagado 10 millones de dólares a RSA para convertirla en la opción predeterminada en los productos utilizados por desarrolladores de todo el mundo, y había gastado 250 millones de dólares al año a través de un programa clasificado llamado Bullrun, específicamente para insertar puertas traseras en software y hardware de cifrado comercial. El NIST, la agencia responsable de comunicar al mundo que el estándar era seguro, había sido, en palabras de los documentos de Snowden, «eventualmente» puesto bajo el control de la NSA como único editor del estándar. (Fuente: Reuters, «Exclusiva: Un contrato secreto vinculaba a la NSA y a un pionero del sector de la seguridad», 20 de diciembre de 2013, https://www.reuters.com/article/us-usa-security-nsa-rsa/exclusive-secret-contract-tied-nsa-and-security industry-pioneer-idUSBRE9BJ1C220131220; New York Times, «La NSA es capaz de burlar las medidas básicas de protección de la privacidad en la web», 5 de septiembre de 2013; Wikipedia, Dual_EC_DRBG, https://en.wikipedia.org/wiki/Dual_EC_DRBG).

Permítanme traducir esto a un lenguaje sencillo, ya que el enfoque técnico ha permitido que se eluda la claridad moral que merece. El gobierno de Estados Unidos afirmó ante el mundo que un estándar de cifrado concreto era seguro. El gobierno sabía que no lo era. El gobierno lo había vuelto inseguro en secreto, a propósito, pagando a la empresa más prestigiosa del sector del cifrado comercial para que incorporara una puerta trasera y la implementara a gran escala. Desarrolladores de todo el mundo utilizaron este estándar de buena fe para proteger las comunicaciones privadas de sus usuarios. La NSA tenía acceso a estas comunicaciones. A las personas cuyos datos privados quedaron expuestos nunca se les informó. Las empresas cuyos productos contenían la puerta trasera, según el propio relato de RSA, no fueron informadas de la vulnerabilidad en el momento en que aceptaron los 10 millones de dólares. Esto no es una nota al pie de página de la historia. Es el acontecimiento fundacional de la arquitectura de la vigilancia moderna: el momento en que se documentó que la agencia responsable de decirle a los estadounidenses que sus comunicaciones digitales eran seguras era, al mismo tiempo, la agencia que se aseguraba en secreto de que no lo fueran. En algunos casos, las empresas que te decían que tus datos estaban protegidos recibían un pago, para asegurarse de que no lo estuvieran. El gobierno ya no necesita espiar. Solo tiene que comprar Esta es la parte que debería dejarte helado, porque representa un avance más reciente y más significativo desde el punto de vista estructural que Pegasus o la puerta trasera de la NSA. El gobierno de Estados Unidos ya no necesita construir infraestructuras de vigilancia para vigilar a sus ciudadanos. Ya no necesita instalar software espía en los teléfonos, ni insertar puertas traseras en los estándares de cifrado, ni llevar a cabo

operaciones de recopilación de datos del tamaño de una sala en las instalaciones de AT&T, aunque todo esto sigue ocurriendo. No necesita hacer nada de eso, porque la vigilancia ya se ha llevado a cabo. Se está llevando a cabo de forma continua, todos los días, a través de las aplicaciones de tu teléfono. Y el gobierno simplemente puede comprar los resultados. En el sector de los corredores de datos, empresas como Venntel, Babel Street y docenas más, compran enormes cantidades de datos procedentes de aplicaciones para teléfonos inteligentes, navegadores web y dispositivos conectados. Los datos de ubicación de una aplicación de seguimiento de actividad física. El historial de navegación de un agregador de noticias. Los patrones de compra de un programa de fidelización minorista. La interacción con contenidos políticos en una plataforma de redes sociales. Todo esto se agrega, se cruza y se vende en expedientes detallados que pueden revelar los movimientos de una persona, su estado de salud, sus creencias políticas, sus prácticas religiosas, sus relaciones personales y sus rutinas diarias, en muchos casos con mayor precisión y exhaustividad de lo que podría lograr cualquier intervención telefónica directa. El Departamento de Seguridad Nacional, el FBI, el IRS, el ICE y el Servicio Secreto han comprado datos de localización de teléfonos móviles a corredores de datos sin órdenes judiciales. El DHS firmó un contrato de 1.000 millones de dólares con Palantir para implementar sistemas de análisis de datos basados en IA en todos los componentes operacionales del DHS, incluidos la CBP y el ICE, utilizando datos adquiridos a través de estos canales. Las agencias gubernamentales han argumentado que el requisito de una orden judicial bajo la Cuarta Enmienda no se aplica si es que están adquiriendo datos disponibles comercialmente y no están presionando para divulgarlos, una distinción jurídica que los abogados especializados en privacidad han calificado de constitucionalmente indefendible, pero que los tribunales aún no han resuelto de forma definitiva. El ICE utiliza herramientas para rastrear teléfonos móviles e identificar dispositivos que han visitado ubicaciones específicas. Tiene un contrato de 30 millones de dólares con Palantir para ImmigrationOS, una plataforma diseñada para rastrear a personas para deportarlas y que tiene una visibilidad casi en tiempo real. La misma empresa que fabrica las herramientas de selección de objetivos que han sido esenciales para matar a civiles en Gaza, es también la que está construyendo la infraestructura de seguimiento para llevar a cabo deportaciones, utilizando datos comprados para localizar a inmigrantes, quienes no han cometido ningún delito más allá de su mera presencia. El Congreso no ha logrado cerrar esta laguna jurídica. La Ley «La Cuarta Enmienda no está en venta», que prohibiría a las agencias gubernamentales comprar datos sin una orden judicial, fue aprobada en la Cámara de Representantes con apoyo bipartidista en 2024, pero nunca fue sometida a votación en el Senado. La administración Trump ha presionado para que se renueve la FISA (Ley de Vigilancia de Inteligencia Extranjera), sin reformas en materia de privacidad. La arquitectura de vigilancia se amplía. La laguna jurídica sigue abierta. Lo que esto significa en la práctica es algo que he estado tratando de explicar a los responsables políticos, a los defensores de los derechos humanos y a cualquiera que quiera escucharme desde que produje *Forever Peace Now*, el Estado de la vigilancia ya no necesita vigilar. Ha externalizado la vigilancia al mercado libre. Cada aplicación que instalas, cada servicio que utilizas, cada dispositivo que llevas contigo te está vigilando en su nombre. La Cuarta Enmienda se redactó para protegerte de la intromisión del gobierno en tu vida privada. No se redactó para un mundo en el que tu vida privada es continuamente catalogada por empresas privadas y vendida al mejor postor, que resulta

ser el gobierno. La ley no ha avanzado al mismo ritmo. La vigilancia sí. Y ahora, con las herramientas de IA descritas en el capítulo doce de este libro, la capacidad del gobierno para procesar, analizar y actuar sobre los datos adquiridos se ha ampliado a una escala que ningún programa de vigilancia anterior podría haber alcanzado. No porque el gobierno haya creado mejores herramientas. Sino porque ha contratado las herramientas de las mismas empresas que desarrollan los sistemas de IA que todo el mundo utiliza a diario. El técnico de AT&T que descubrió la sala secreta de la NSA describió lo que había visto en un testimonio que apareció en mi película. Se trata del armario de distribución en la sala de Internet ubicado en 611 Folsom Street en San Francisco, donde un prisma de cristal dividía el rayo de luz láser que transportaba el tráfico de Internet y enviaba una copia a la NSA. Lo encontró en 2003, lo denunció y nada cambió. La sala sigue ahí. Y la sala ya no es necesaria, porque los datos llegan ahora al gobierno a través de una transacción comercial en lugar de una escucha telefónica secreta, y ningún denunciante puede ver fácilmente la orden de compra. La lección de treinta años de tecnología, de Snowden y Pegasus y la puerta trasera de RSA y el mercado de los corredores de datos, es esta: la promesa de privacidad nunca fue el producto. El producto siempre fueron los datos. Y quienes te dicen lo contrario, las empresas que ponen «privacidad» en las vallas publicitarias, los organismos de normalización que certifican algoritmos que saben que están comprometidos, las agencias gubernamentales que te dicen que necesitan la vigilancia para protegerte, están, en cada caso, describiendo algo distinto de lo que realmente están haciendo. El estado de vigilancia más peligroso del mundo no es China, con su sistema de crédito social y sus cámaras de reconocimiento facial. Es Estados Unidos, porque el nuestro es el único que ha perfeccionado el arte de construir una infraestructura de vigilancia integral mientras que afirma, con total seriedad y una valla publicitaria de bonito diseño, que la privacidad es el producto. *Fuentes: Citizen Lab, Universidad de Toronto, investigación sobre el software espía Pegasus: https://citizenlab.ca/category/research/ Reuters, «Exclusiva: un contrato secreto vinculaba a la NSA con un pionero del sector de la seguridad», 20 de diciembre de 2013: https://www.reuters.com/article/us-usa-security-nsa-rsa/exclusive-secret-contract-tied-nsa-and-security industry-pioneer-idUSBRE9BJ1C220131220*

Wikipedia, Dual EC DRBG: https://en.wikipedia.org/wiki/Dual_EC_DRBG Brennan Center for Justice, «Cerrar la laguna jurídica de los corredores de datos», febrero de 2024: https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole Centro de Información sobre Privacidad Electrónica (EPIC), «Cerrar la laguna jurídica de los corredores de datos: la elusión gubernamental de la Cuarta Enmienda»: https://epic.org/documents/closing-the-data-broker-loophole-government-evasion-of-the-fourth-amendment/ NPR, «Tus datos están por todas partes. El Gobierno los está comprando sin una orden judicial», 25 de marzo de 2026: https://www.npr.org/2026/03/25/nx-s1-5752369/ice-surveillance-data-brokers-congress-anthropi c Project on Government Oversight, «Closing the Data Broker Loophole»: https://www.pogo.org/fact-sheets/fact-sheet-closing-the-data-broker-loophole Forever Peace Now (documental), dirigido por Vahid Razavi, 2025 — testimonio de un técnico de AT&T, la Electronic Frontier Foundation y defensores de la sociedad civil sobre la arquitectura de la vigilancia. El patrón, nombrado En conjunto, estas cinco plataformas forman una arquitectura digital de represión. Meta eliminó más de mil contenidos palestinos en sesenta días y accedió al 94 % de las solicitudes de censura del gobierno israelí. YouTube borró 700 vídeos que documentan posibles crímenes de guerra

siguiendo instrucciones de la administración Trump. X suspendió cuentas a periodistas palestinos, mientras dejó en línea el discurso de odio contra los palestinos en un 96 % de los casos. TikTok se convirtió en el blanco de una prohibición del Congreso motivada explícitamente por su incapacidad para suprimir el contenido palestino. LinkedIn creó un sistema de vigilancia encubierto capaz de deducir las afiliaciones políticas de los usuarios sin su conocimiento, ni su consentimiento. Ninguna de estas empresas dirá que lo que hizo es censura. Utilizarán palabras como «moderación de contenidos», «directrices de la comunidad», «cumplimiento de sanciones» e «integridad de la plataforma». Estas son las etiquetas burocráticas de una industria que ha perfeccionado el arte de hacer cosas terribles con un lenguaje respetable. He entrevistado a los responsables políticos que toman estas decisiones. Sé lo que significa «integridad de los datos de la plataforma» cuando la presentación de resultados trimestrales es la semana que viene. Significa: haremos lo que sea conveniente, desde el punto de vista financiero y político, y lo llamaremos política. El Observatorio Palestino de Violaciones de los Derechos Digitales documentó más de 1.350 casos de censura en línea en las principales plataformas solo entre octubre de 2023 y julio de 2024. Detrás de cada uno de esos 1.350 casos hay un periodista, un activista, un padre, un superviviente: alguien que intentó mostrar al mundo lo que le estaba sucediendo y fue silenciado por una empresa que anunciará beneficios récord en su próxima presentación de resultados. Este es el Telón de Acero Digital. No lo mantiene un gobierno. Lo mantienen los accionistas. --- El silenciamiento documentado en el capítulo nueve opera a nivel de la decisión humana: una solicitud gubernamental, el cumplimiento de una plataforma, una publicación eliminada. El capítulo diez pasa a una forma de control más inquietante: la manipulación sistemática de lo que los propios sistemas de IA creen y, por lo tanto, lo que se les presenta como verdadero a las personas que consultan estos sistemas. Lo que los gobiernos y sus contratistas no pueden eliminar del registro, ahora intentan eliminarlo del entrenamiento de las máquinas que componen el registro.

CAPÍTULO DIEZ. JUGANDO CON LA MÁQUINA

Cómo los gobiernos utilizan la IA para fabricar la realidad, y cómo la industria de la IA les ayuda. Hay una pregunta que se plantea con menos frecuencia de la que se debería: si las plataformas de las grandes tecnológicas han estado silenciando las voces palestinas, ¿qué cosa ha ocupado el espacio que esas voces dejaron vacío? La respuesta no es el silencio. Se trata de contenido fabricado, operaciones de influencia coordinadas y una campaña sistemática para entrenar a los sistemas de IA que cientos de millones de personas utilizan ahora como su principal fuente de información para producir las respuestas que los gobiernos quieren que produzcan. Este capítulo trata sobre cómo funciona esto. Trata sobre quién lo paga, quién lo construye y qué significa para el futuro de la verdad misma. La operación de 6 millones de dólares: manipular ChatGPT por la puerta trasera En septiembre de 2025, documentos recién presentados ante el Departamento de Justicia de Estados Unidos en virtud de la Ley de Registro de Agentes Extranjeros confirmaron lo que muchos sospechaban pero aún no podían demostrar. El gobierno israelí, actuando a través de su Ministerio de Asuntos Exteriores y una iniciativa de diplomacia pública de 145 millones de dólares llamada Proyecto 545, contrató a una red de empresas estadounidenses para llevar a cabo una de las operaciones de influencia con IA más ambiciosas jamás documentadas. En el centro de la operación se encuentra Brad Parscale, el arquitecto digital de la campaña presidencial de Donald Trump en 2016, quien contrató en ese momento a la famosa empresa de datos Cambridge Analytica, y que ahora es director de estrategia de Salem Media Group, una cadena de radiodifusión cristiana conservadora entre cuyos accionistas se encuentran Donald Trump Jr. y Lara Trump. La empresa de Parscale, Clock Tower X LLC, se registró como agente del gobierno israelí el 18 de septiembre de 2025, en virtud de un contrato de seis millones de dólares con el gigante alemán de los medios Havas Media Network, que a su vez operaba en nombre del Ministerio de Asuntos Exteriores de Israel. El objetivo es explícito y el método, novedoso. Clock Tower producirá un mínimo de 100 «activos creativos básicos» al mes, entre ellos vídeos, gráficos, audio y contenido escrito, con al menos un 80 % de ellos dirigido al público de la Generación Z a través de TikTok, Instagram, YouTube y podcasts. El objetivo: 50 millones de impresiones pagadas al mes. Pero lo que diferencia esta operación de las relaciones públicas convencionales era una cláusula específica oculta en la descripción del trabajo del contrato. Clock Tower desplegará, en el propio lenguaje del documento, «sitios web y contenidos para ofrecer resultados de encuadre de GPT en conversaciones de GPT». (Fuente: Responsible Statecraft, «Israel quiere entrenar a ChatGPT para que sea más proisraelí», octubre de 2025, https://responsiblestatecraft.org/israel chatgpt/; Sludge, «Las nuevas campañas de influencia de Israel en EE.UU. apuntan a TikTok, las iglesias y ChatGPT», octubre de 2025, https://readsludge.com/2025/10/06/israels-new-u-s-influence campaigns-target-tiktok-churches-and-chatgpt/). Permítanme explicar lo que esto significa en lenguaje sencillo. Los sistemas de IA como ChatGPT se entrenan con enormes cantidades de texto procedente de toda la red. Aprenden qué cosas son ciertas, qué es controvertido y qué enfoque aplicar a temas complejos mediante el procesamiento

de miles de millones de páginas web, artículos y publicaciones en redes sociales. Si inundas Internet con una versión concreta de los hechos, a través de cientos de sitios web, millones de publicaciones en redes sociales y contenido coordinado diseñado para posicionarse bien en los motores de búsqueda, no sólo estás moldeando directamente la opinión pública, también estás moldeando lo que aprende la IA. En efecto, estás envenenando el pozo del que se extraerá la información de la próxima generación. Clock Tower también utilizará una plataforma de IA predictiva llamada MarketBrew para optimizar el contenido con el fin de mejorar su visibilidad algorítmica en Google y Bing, asegurándose de que la narrativa proisraelí sea lo primero y lo más frecuente que encuentren tanto los usuarios humanos como los sistemas de entrenamiento de IA. No se trata de un pago directo a OpenAI. Permítanme ser preciso en este punto, porque el rumor que circula por Internet, de que Israel pagó directamente a OpenAI, es inexacto, y este libro se basa en hechos documentados. Snopes investigó y confirmó que: no hay pruebas de un contrato entre Israel y OpenAI. Lo que está documentado, en revelaciones gubernamentales presentadas legalmente, es algo más sofisticado y más difícil de rebatir: una operación financiada por el gobierno para manipular el entorno de entrenamiento de la propia IA. (Fuente: Snopes, «Israel No Firmó un Contrato Con ChatGPT. Esto es lo que realmente ocurrió», enero de 2026, https://www.snopes.com/news/2025/12/22/israel-contract-chatgpt/; Centro de Recursos sobre Empresas y Derechos Humanos, https://www.business-humanrights.org/en/latest-news/israelopt-clock-tower-x-allegedly-hired-by-israeli government-to-create-pro-israel-content-training-chatgpt-and-targeting-facebook-instagra m-tiktok-youtube incl-cos-response-and-non-responses/).

Cuando el Centro de Recursos sobre Empresas y Derechos Humanos se puso en contacto con OpenAI, Meta, Google, Alphabet y Havas Media para solicitarles comentarios sobre estas acusaciones, solo TikTok respondió. OpenAI no dijo nada. Ese silencio es su propia respuesta.

OpenAI y el contrato militar que no fue... hasta que lo fue

Hay una segunda historia sobre OpenAI e Israel que no tiene nada que ver con operaciones de influencia. Se trata de armas. Y está documentada por Associated Press (AP).

En febrero de 2025, AP publicó una investigación basada en documentos internos de la empresa, datos y entrevistas exclusivas con funcionarios israelíes y funcionarios de la empresa, tanto actuales como antiguos. Las conclusiones fueron contundentes. Tras la operación de Hamás del 7 de octubre de 2023, el uso por parte de Israel de la tecnología de OpenAI, adquirida a través de la plataforma en la nube Azure de Microsoft, se disparó hasta casi 200 veces su nivel anterior al genocidio. La cantidad de datos que el ejército israelí almacenó en los servidores de Microsoft se duplicó los primeros meses del genocidio, alcanzando más de 13,6 petabytes en julio de 2024, lo que equivale aproximadamente a 350 veces la memoria digital necesaria para almacenar todos los libros de la Biblioteca del Congreso. Los modelos de IA de OpenAI se estaba utilizando directamente en el proceso de inteligencia y selección de objetivos de una campaña militar en curso. (Fuente: Associated Press, «Mientras Israel Usa en la Guerra Modelos de IA Hechos en EE.UU., Surge la Preocupación Sobre el Rol de la Tecnologia en Quien Vive y Quien Muere», febrero de 2025; Fortune, https://fortune.com/2025/02/19/israel-microsoft-openai-raises-questions-powerful-tech/).

«Esta es la primera confirmación que tenemos de que los modelos de IA comerciales se están utilizando directamente en la guerra», afirmó Heidy Khlaaf, científica jefe de IA en el AI Now Institute y antigua ingeniera sénior de seguridad en la propia OpenAI.

La respuesta de OpenAI a esta revelación fue afirmar que no tenía ninguna colaboración directa con el ejército israelí. Esa afirmación merece un análisis minucioso. A principios de 2024, de forma discreta, sin ningún anuncio, OpenAI reescribió sus condiciones de servicio para eliminar el texto que prohibía explícitamente el uso militar de su tecnología. La prohibición de las aplicaciones militares simplemente se eliminó. Lo que había sido una línea roja se convirtió en una puerta abierta. Y por esa puerta entraron las Fuerzas Armadas de Israel, que adquirieron modelos de OpenAI a través de la plataforma Azure de Microsoft y los utilizaron para procesar inteligencia de vigilancia y respaldar decisiones de selección de objetivos. La empresa cambió las reglas y luego se remitió a ellas como prueba de su inocencia. Esto no es una defensa. Es una estrategia empresarial.

Gemini de Google: las pruebas del denunciante

Google ha sostenido sistemáticamente que sus productos de IA no se utilizan para armas o vigilancia en violación de sus políticas éticas. En febrero de 2026, un antiguo empleado de Google presentó una denuncia confidencial ante la Comisión de Bolsa y Valores de Estados Unidos contando una historia diferente.

Según la denuncia, revisada por The Washington Post, en 2024 llegó a la división de computación en la nube de Google una solicitud de asistencia al cliente desde una dirección vinculada a una cuenta de las Fuerzas Armadas de Israel. El cliente intentaba utilizar la IA Gemini de Google para analizar imágenes de vigilancia aérea con drones y se había encontrado con un error por el que el software, en ocasiones, no identificaba drones, soldados y otros objetos en las imágenes. El personal de atención al cliente de la unidad de nube de Google respondió con asistencia técnica y llevó a cabo pruebas internas para ayudar a resolver el problema. Un segundo empleado de Google, que supuestamente trabajaba en la cuenta de Google Cloud de las Fuerzas Armadas de Israel, fue incluido en copia en el ticket de asistencia. (Fuente: Washington Post, «Un denunciante afirma que un contratista militar israelí utilizó la IA Gemini de Google», febrero de 2026, https://www.washingtonpost.com/technology/2026/02/01/google-ai-israel military/).

El denunciante alegó que esta asistencia violaba los propios principios de IA de Google, que en ese momento establecían que la empresa no utilizaría la IA para aplicaciones armamentísticas o de vigilancia que violaran las normas internacionalmente aceptadas. Google rebatió esta caracterización, alegando que el ticket de asistencia tenía un valor comercial demasiado reducido como para constituir un uso «significativo» de la IA. Se trata de una defensa notable. La cuestión de si una herramienta de vigilancia con drones viola la ética no cambia en función del importe de la factura mensual.

Por otra parte, unos documentos de noviembre de 2024 revelan que el ejército israelí solicitó activamente acceso a la plataforma de IA Gemini de Google para desarrollar su propio asistente de IA capaz de procesar documentos militares y grabaciones de audio, ampliando así sus capacidades a los pocos meses de iniciarse el genocidio. Los registros muestran que los empleados de Google observaron un aumento en las solicitudes de acceso de las Fuerzas Armadas de Israel a herramientas de IA tras el 7 de octubre, y los documentos internos revelan que un empleado

advirtió que retrasar la ampliación del acceso podría empujar a Israel hacia Amazon, el competidor de Google en el ámbito de la nube. (Fuente: The Defense Post, «Google Apoyando a Israel con Herramientas de IA Para Uso Militar», febrero de 2025, https://thedefensepost.com/2025/02/04/google-israel-ai-military/; Common Dreams, https://www.commondreams.org/news/big-tech-gaza-genocide).

La respuesta de Google, al igual que la de OpenAI y la de Microsoft, sigue el mismo patrón que hemos documentado a lo largo de este libro. Negar. Minimizar. Repetir. Actualizar la política para cerrar la brecha entre lo que se hizo y lo que estaba permitido. El patrón detrás del patrón Lo que se desprende de estas tres historias, la operación de influencia de Clock Tower, el aumento del uso militar de OpenAI y la denuncia del empleado de Gemini, no son tres escándalos separados. Se trata de una estrategia coherente, que opera simultáneamente en dos frentes. En el frente militar, las empresas de IA proporcionan las herramientas que hacen que el ataque sea más rápido, más automatizado y más letal. Lo hacen a través de contratos directos, de plataformas en la nube y de la eliminación silenciosa de las barreras éticas que antes hacían que tal uso fuera inadmisible. En el frente de la información, los gobiernos utilizan el propio proceso de entrenamiento de la IA como arma, inundando la Internet con contenido fabricado para enseñar a los sistemas de IA qué creer, qué suprimir y qué sufrimiento tratar como legítimo. El resultado es un entorno informativo en el que las mismas herramientas de IA que ayudan a identificar objetivos de bombardeo están siendo entrenadas simultáneamente para describir estos bombardeos en un lenguaje favorable a quienes los ordenan. Esta es la arquitectura completa del control impulsado por la IA. No solo mata. También moldea lo que crees sobre el asesinato. Y ambas funciones las proporcionan, a sabiendas o no, las mismas empresas (OpenAI, Google y Microsoft), cuyos informes de resultados trimestrales leerás la semana que viene en las páginas de economía de tu periódico de referencia, entre los anuncios. Se pidió a OpenAI que comentara sobre la operación de influencia diseñada para manipular sus datos de entrenamiento. No respondió. Este silencio te dice todo lo que necesitas saber respecto a qué intereses son a los que han decidido servir estas empresas.

--- Si el capítulo diez trata de cómo se entrena a la IA para fabricar consenso entre los adultos, el capítulo once trata de lo que les sucede a los niños que crecen dentro de plataformas diseñadas no para informar, sino para crear adicción. El algoritmo que recompensa el contenido extremista para adultos es el mismo algoritmo que recomienda contenido sobre autolesiones a los adolescentes. La plataforma que censura las voces palestinas es la misma que, según el jurado de Nuevo México, había perjudicado a sabiendas la salud mental de los niños. No se trata de historias independientes. Es el mismo modelo de negocio aplicado a dos poblaciones vulnerables diferentes.

CAPÍTULO ONCE. EL ALGORITMO CONTRA NUESTROS HIJOS

Las redes sociales, el suicidio adolescente y la industria que se beneficia de ambos.

En marzo de 2026, tras un juicio de casi siete semanas en Santa Fe, Nuevo México, un jurado dictó un veredicto que debería haber sacudido todas las salas de reuniones de Silicon Valley. El jurado determinó que Meta, la empresa propietaria de Instagram, Facebook y WhatsApp, había perjudicado a sabiendas la salud mental de los niños, ocultado lo que sabía sobre la explotación sexual infantil en sus plataformas e incurrido en prácticas comerciales «inaceptables», que explotaban injustamente las vulnerabilidades de los jóvenes. La pena: 375 millones de dólares. La miembro del jurado Linda Payton, de 38 años, explicó qué fue lo que guió el veredicto del jurado. Con un máximo de 5.000 dólares por infracción en juego, dijo que consideraba que cada niño merecía la cantidad máxima. (Fuente: NPR, «Un jurado de Nuevo México dictamina que Meta perjudica la salud mental y la seguridad de los niños, infringiendo la ley estatal», 24 de marzo de 2026, https://www.npr.org/2026/03/24/g-s1-115019/new-mexico-meta-children-mental-health; AP/US News, 24 de marzo de 2026, https://www.usnews.com/news/technology/articles/2026-03-24/new-mexico-jury-finds-meta-violated consumer-protection-law-at-trial-about-child-safety). El juicio examinó un corpus sustancial de documentos internos e investigaciones de la propia Meta. Estas eran pruebas de que los propios ingenieros y científicos de la empresa habían realizado estudios sobre el impacto de sus plataformas en los usuarios jóvenes y no habían actuado en función de lo que habían descubierto. El jurado escuchó a ejecutivos de Meta, ingenieros de la plataforma, antiguos empleados que se convirtieron en denunciantes, expertos psiquiátricos, consultores de seguridad tecnológica y educadores de escuelas públicas que describieron aulas perturbadas por esquemas de sextorsión dirigidos a los niños. Al jurado se le informó del incumplimiento documentado por parte de Meta de su propia prohibición de usuarios menores de 13 años y del papel que desempeñan sus algoritmos a la hora de priorizar contenidos sensacionalistas y perjudiciales, incluidos contenidos sobre el suicidio adolescente. En el centro del caso se encontraba una acusación que el fiscal general de Nuevo México, Raúl Torrez, planteó con claridad moral: Meta diseñó sus plataformas para crear adicción en los usuarios jóvenes. La empresa sabía lo que estaba pasando. Eligió el beneficio económico. «Sabemos que el objetivo es generar interacción y que los niños pasen tiempo en la plataforma», dijo la fiscal Linda Singer a los miembros del jurado. «Esta elección que hizo Meta tiene profundas repercusiones negativas en los niños». Más de 40 fiscales generales estatales de todo el país han presentado demandas similares contra Meta. Miles de familias se encuentran en proceso judicial. La coalición de padres que han perdido a sus hijos a causa de los daños provocados por las redes sociales, el grupo que se autodenomina ParentsSOS, calificó el veredicto de Nuevo México como «un momento decisivo». El grupo declaró en un comunicado: «Nosotros, los padres que hemos vivido lo inimaginable, la muerte de un hijo a causa de los daños de las redes sociales, aplaudimos este hito excepcional y trascendental». (Fuente: PBS NewsHour, «¿Qué viene después en las batallas legales sobre las redes

sociales ahora que un jurado de Nuevo México dictaminó que las plataformas de Meta perjudican a los niños?», 25 de marzo de 2026, https://www.pbs.org/newshour/nation/whats-next-in-social-media-legal-battles-after-a-new-mexic o-jury finds-meta-platforms-harm-children).

Una carta que cambió un país Una niña de doce años de Australia llamada Charlotte O'Brien se quitó la vida a causa del acoso escolar que las redes sociales permitieron y amplificaron. Su madre, Kelly O'Brien, escribió una carta personal al primer ministro Anthony Albanese. Él la leyó. Le conmovió. Y ayudó a conmover a un gobierno. La historia de Charlotte no fue una tragedia aislada. Es la historia central de «Let Them Be Kids», una campaña con más de 54.000 firmas de padres, educadores y defensores de la seguridad infantil, y que fue expuesta en los medios de comunicación australianos para mostrarle a las personas el poder de actuar frente al daño que estas redes sociales generan. En un acto celebrado en la Asamblea General de las Naciones Unidas en septiembre de 2025, una madre habló del suicidio de su hija como «una muerte por acoso... propiciada por las redes sociales». El discurso contó con el apoyo de líderes mundiales de Grecia, Fiji, Tonga y de la presidenta de la Comisión Europea, Ursula von der Leyen. El 29 de noviembre de 2024, el Parlamento australiano aprobó la Ley de Enmienda de Seguridad en Línea (Edad Mínima en Redes Sociales). Entró en vigor el 10 de diciembre de 2025. Australia se convirtió en el primer país del mundo en aplicar una prohibición a nivel nacional que impide a los menores de 16 años tener cuentas en las principales plataformas de redes sociales, entre ellas Facebook, Instagram, TikTok, YouTube, Snapchat, Reddit, X, Threads, Twitch y Kick. Las plataformas que no tomen «medidas razonables» para hacer cumplir la restricción de edad se enfrentan a multas de hasta 49,5 millones de dólares australianos. (Fuente: Wikipedia, Ley de Enmienda de Seguridad en Línea (Edad Mínima en Redes Sociales) de 2024, https://en.wikipedia.org/wiki/Online_Safety_Amendment; Comisionado de eSafety, «Restricciones de edad en las redes sociales», marzo de 2026, https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions; Time, «Lo que hay que saber sobre la prohibición de las redes sociales para menores de 16 años en Australia», 10 de diciembre de 2025, https://time.com/7339762/australia-youth-social-media-ban-under-16-snapchat meta-tiktok/). «Este es el día en que las familias australianas recuperan el poder de estas grandes empresas tecnológicas», declaró el primer ministro Albanese cuando la ley entró en vigor. «Están reivindicando el derecho de los niños a ser niños». Jonathan Haidt, psicólogo social y autor de The Anxious Generation, un libro que documenta con rigor sistemático la relación entre la adopción masiva de los teléfonos inteligentes, las redes sociales y la crisis de salud mental que ahora afecta a toda una generación, acogió con satisfacción la medida de Australia. «El mundo está deseando que tengan éxito», escribió, «y muchas otras naciones seguirán su ejemplo». Ya están siguiendo sus pasos. A fecha de febrero de 2026, Francia, el Reino Unido, Alemania, Italia, Grecia, España, Dinamarca, Malasia y Nueva Zelanda están considerando o impulsando activamente restricciones similares para los menores de 16 años. El Parlamento Europeo aprobó una resolución no vinculante en la que se aboga por una edad mínima de 16 años y ha propuesto prohibir por completo para los menores de esta edad funciones adictivas como el desplazamiento infinito y la reproducción automática. (Fuente: CNBC, «Australia está tratando de aplicar la primera prohibición de las redes sociales para adolescentes. Los gobiernos de todo el mundo están atentos», 10 de diciembre de 2025, https://www.cnbc.com/2025/12/10/australia-16-year-old-teens-ban-social-media-policy-law-ig-

tikt ok-fb reddit-youtube-snapchat.html; La prohibición de las redes sociales en Australia: una prueba para la gobernanza digital global, BISI, enero de 2026, https://bisi.org.uk/reports/australias-world-first-social-media-ban-a-test-for-global-digital-governa nce).

La trampa de la privacidad que se esconde tras la protección Quiero hablar con sinceridad sobre el enfoque de la restricción de edad, porque creo que los gobiernos que están avanzando en esta dirección están haciendo lo correcto por las razones adecuadas, y también creo que la implementación hacia la que se les empuja conlleva sus propios grandes peligros. La verificación de la edad, tal y como se está debatiendo y aplicando actualmente, exige a las plataformas de redes sociales que confirmen la edad de un usuario antes de permitir la creación de una cuenta. Los métodos que se están barajando incluyen comprobaciones de documentos de identidad oficiales, escaneo facial biométrico, inferencias de comportamiento a partir del historial de navegación y estimación de la edad basada en IA a partir de la apariencia física. Todos y cada uno de estos métodos requieren la recopilación de datos personales sensibles. Algunos requieren datos biométricos. Otros exigen vincular las cuentas de redes sociales a documentos de identidad oficiales. Otros crear un perfil digital del comportamiento, de las características demográficas y de la apariencia física del usuario, y además conservarlo. Las mismas empresas que he documentado a lo largo de este libro como infractoras reincidentes de la privacidad de los usuarios, empresas que añadieron «terrorista» a las biografías de los usuarios palestinos mediante un algoritmo, que escanearon 6.167 extensiones de navegador sin el conocimiento de los usuarios, y que compartieron datos con gobiernos extranjeros con una tasa de cumplimiento del 94 %, son las empresas ahora encargadas de hacer cumplir la verificación de la edad de los menores. Los datos que deben recopilar para cumplir la restricción son exactamente el mismo tipo de datos que históricamente han utilizado indebidamente, profitando con ellos, y los que han entregado a los gobiernos cuando se les ha solicitado. Mozilla, la organización sin fines de lucro que desarrolla el navegador Firefox y lleva décadas defendiendo la privacidad de los usuarios, planteó esta preocupación directamente en respuesta a la ley australiana. Los sistemas de estimación de la edad basados en datos biométricos, señaló Mozilla, suelen ofrecer resultados deficientes en el caso de personas con tonos de piel más oscuros y rasgos faciales no binarios. Los sistemas de inferencia conductual diseñados para estimar la edad a partir del historial de navegación crean perfiles detallados de cada usuario. La verificación de la edad mediante un documento de identidad oficial crea un vínculo entre la identidad en las redes sociales y la identidad legal que nunca antes había existido a gran escala. (Fuente: Fundación Mozilla, «La prohibición de las redes sociales en Australia: por qué no solucionará lo que falla en las plataformas en línea», 19 de diciembre de 2025, https://blog.mozilla.org/netpolicy/2025/12/19/australias-social-media-ban-why-age-limits-wont-fix -what-is-wrong-with-online-platforms/). Permítanme ser claro sobre lo que esto significa. Las empresas cuyas plataformas están perjudicando a los niños no pueden ser las mismas empresas a las que se confía la verificación de la identidad de esos niños con el fin de protegerlos de sus propias plataformas. Eso no es protección. Es una ampliación de la infraestructura de vigilancia bajo el pretexto de la seguridad, la misma estrategia que las grandes tecnológicas han seguido con la seguridad, la moderación de contenidos y las medidas antiterroristas cada vez que el público ha exigido rendición de cuentas. La protección de los niños frente a los daños de las redes sociales es una prioridad moral legítima y urgente. El mecanismo de esa protección no debe

crear un daño nuevo y más grande en su lugar. Cualquier marco de verificación de edad debe ser independiente de las plataformas, estar diseñado para mantener la privacidad, estar sujeto a auditoría pública y basarse en el principio de que el cumplimiento de una ley de protección infantil no da derecho a una empresa a crear una base de datos biométrica de todos los adultos que utilizan su servicio. El algoritmo que recompensa la ira, y los niños que pagan por ello Permítanme ahora pasar a algo de lo que se habla menos que de los daños explícitos de las redes sociales en los niños, pero que, en mi opinión, es igualmente trascendental para la generación que crece dentro de estas plataformas. Se trata del diseño deliberado de algoritmos de recomendación que premian el contenido más extremo, divisivo e incendiario, y los incentivos económicos que mantienen ese diseño. En 2025, Sky News llevó a cabo un experimento de un mes de duración en X, la plataforma anteriormente conocida como Twitter, ahora propiedad de Elon Musk. El estudio creó cuentas con diferentes inclinaciones políticas y realizó un seguimiento de los contenidos que el algoritmo recomendaba. La conclusión fue inequívoca: X «muestra un sesgo algorítmico significativo hacia la promoción de contenidos de extrema derecha y extremistas». The Wall Street Journal y The Washington Post llevaron a cabo sus propios análisis por separado. Ambos llegaron a la misma conclusión: X amplifica ahora el contenido político de tendencia derechista y extremista por encima de otras perspectivas. (Fuente: Social Media Today, «Los Estudios Muestran Que X Aumenta las Perspectivas Políticas Conservadoras», 19 de febrero de 2026, https://www.socialmediatoday.com/news/x-formerly-twitter-amplifies-conservative-political-persp ectives report/812652/). Un estudio académico de 2025 publicado en Science utilizó una metodología basada en una extensión de navegador para alterar los feeds de X de los usuarios durante las elecciones presidenciales estadounidenses de 2024, reduciendo la exposición de contenidos que expresaban actitudes antidemocráticas y hostilidad partidista. El estudio reveló que este único cambio modificó los sentimientos políticos de los usuarios hacia sus oponentes en más de dos puntos en una escala de 100 puntos, un cambio que normalmente tardaría aproximadamente tres años en producirse de forma orgánica en la población general. Los investigadores describieron esto como una prueba causal de que el algoritmo de X, con su sistema de recomendaciones y su estructura de incentivos económicos, está contribuyendo activamente a la polarización política. (Fuente: The Conversation, «Unas pocas semanas del algoritmo de X pueden hacerte más de derechas, y el efecto no desaparece rápidamente», 18 de febrero de 2026, https://theconversation.com/a-few-weeks-of-xs-algorithm-can-make-you-more-right-wing-and-it-doesnt wear-off-quickly-276153). Esto no es una casualidad. Es una decisión de ingeniería. Los algoritmos de X, TikTok, Facebook y YouTube no son filtros neutrales. Son máquinas de optimización, diseñadas para maximizar la interacción, y el contenido que impulsa la interacción de forma más fiable es aquel que provoca las reacciones emocionales más intensas: indignación, miedo, desprecio, identidad tribal, pánico moral. Eso es lo que hace que la gente siga desplazándose por la pantalla. Eso es lo que mantiene alta la duración de la sesión. Eso es lo que hace que el inventario publicitario sea valioso. Y eso es lo que se le ofrece, de forma desproporcionada, a adolescentes que aún están formando su comprensión del mundo, su sentido de identidad y su relación con personas diferentes a ellos. La estructura de incentivos económicos agrava esta situación. Las plataformas recompensan económicamente a los creadores que generan más interacción, a través de programas de monetización que pagan por visualización, por hora de

visualización, y por compartir. Un creador que produce contenido que provoca ira no sólo está consiguiendo más visualizaciones. Le están pagando más por producir ese contenido. El algoritmo selecciona el contenido más incendiario, el encuadre más polarizador, las posiciones más extremas, y luego extiende un cheque a quienquiera que los haya producido. Las granjas de contenido de extrema derecha que ahora operan a escala industrial en X y TikTok no producen lo que producen porque creen en ello. Lo producen porque el algoritmo lo ha convertido en la categoría de contenido más rentable disponible para un creador sin recursos de producción significativos. Lo que esto significa para un joven de quince años que pasa cuatro horas al día en TikTok o X, viendo ese contenido, quedando excluido económicamente de los espacios sociales donde se organizan sus compañeros, es una inmersión diaria en un entorno seleccionado que hace que el mundo parezca más enfadado, más dividido, más peligroso y más incierto de lo que realmente es. Eso tampoco es una casualidad. Es el producto. Silenciar a Palestina, amplificar el extremismo: el doble rasero del algoritmo En el capítulo nueve de este libro documenté los mecanismos específicos mediante los cuales Meta, TikTok, X, YouTube y LinkedIn suprimieron sistemáticamente las voces palestinas durante el genocidio en Gaza: eliminando publicaciones, suspendiendo cuentas, cumpliendo con las solicitudes de retirada del gobierno israelí en un porcentaje de hasta el 94 %, y borrando 700 vídeos que documentaban posibles crímenes de guerra por orden del gobierno de Estados Unidos. Quiero volver a ese historial aquí, en el contexto de lo que estas plataformas han permitido simultáneamente. Mientras que a los periodistas palestinos se les suspendían las cuentas, se les eliminaban las publicaciones y se les limitaba el alcance mediante algoritmos, las mismas plataformas dejaban en línea el discurso de odio contra los palestinos en un 96 %, según el Centre for Countering Digital Hate. La organización de derechos digitales 7amleh documentó más de 19.000 casos de discursos de odio y contenido incitador en hebreo en X en las semanas posteriores al 7 de octubre de 2023, contenido que permaneció en línea sin consecuencias. (Fuente: Centro de Empresas y Derechos Humanos, «Un informe denuncia que X no eliminó el 96 % de las publicaciones de discurso de odio», noviembre de 2023, https://www.business-humanrights.org/en/latest-news/report-exposes-xs-failure-to-remove-96- of (/publicaciones-con-discurso-de-odio-en-el-conflito-entre-Israel-y-Palestina/). El patrón es constante en todas las plataformas y se mantiene a lo largo del tiempo. El algoritmo silencia las voces de los ocupados y amplifica el discurso del ocupante. Silencia el dolor y recompensa la ira. Elimina la documentación de las atrocidades y recomienda la retórica que las justifica. Y lo hace no por una ideología integrada en el software, sino para optimizar la arquitectura financiera para la que el software está diseñado. El contenido que genera indignación obtiene más interacción. Más interacción genera más ingresos publicitarios. Las atrocidades se eliminan porque alguien con conexiones gubernamentales pidió que se eliminaran. La ira se amplifica porque la ira es lo que alimenta el modelo de negocio. El mismo algoritmo que suprime el testimonio del niño palestino mantiene al creador de contenido extremista en la cola de las recomendaciones, porque el creador de contenido extremista genera más interacción, y la interacción es dinero. Nuestros hijos se están criando dentro de esta arquitectura. Están aprendiendo cómo es el mundo a través de plataformas que tienen incentivos económicos para mostrarles la versión más extrema del mismo. Están aprendiendo qué se considera un ser humano por el que vale la pena llorar a través de plataformas que eliminan algunos sufrimientos y

amplifican otros en función de qué eliminación y qué amplificación producen el resultado más rentable. Y cuando las consecuencias de esa arquitectura se hacen visibles, cuando los estudios clínicos documentan el daño a la salud mental, cuando se producen los suicidios, cuando el jurado de Nuevo México determina que Meta incurrió en prácticas desmesuradas que explotaban las vulnerabilidades de los niños, las empresas emiten comunicados, actualizan sus directrices comunitarias y vuelven a la misma práctica, vuelven a la misma escala en el siguiente ciclo de noticias. Lo que la regulación debe exigir realmente Las leyes de restricción de edad que se están tramitando en los parlamentos, desde Canberra hasta Copenhague y Bruselas, son un comienzo genuino y necesario. Pero no son suficientes. Proteger a los niños de los daños de las redes sociales requiere ir más allá de restringir quién puede tener una cuenta. Requiere abordar la arquitectura algorítmica y financiera que hace que estas plataformas sean perjudiciales en primer lugar, porque un joven de dieciséis años no es menos vulnerable a un algoritmo optimizado para la indignación que uno de catorce. Y un adulto que pasa cuatro horas al día en un sistema de recomendaciones diseñado para maximizar la participación y la reacción emocional también está sufriendo daños. La restricción de edad aborda el síntoma, reflejado en los usuarios menores de edad, pero deja intacta la enfermedad, que vendría a ser el diseño. Lo que realmente se necesita, junto con la restricción de edad, es una transparencia algorítmica obligatoria: el requisito legal de que las plataformas revelen, ante auditores independientes con autoridad vinculante, exactamente cómo funcionan sus sistemas de recomendación y para qué están optimizados. No en un informe de transparencia trimestral redactado por el departamento de relaciones públicas de la empresa. Sino con una auditoría independiente y vinculante con la facultad de exigir cambios en el diseño algorítmico cuando las pruebas demuestren que estos sistemas están causando daño. Lo que se necesita es responsabilidad por la amplificación algorítmica de contenidos nocivos. La protección de la Sección 230, que exime a las empresas tecnológicas de responsabilidad por los contenidos publicados por los usuarios, no debería extenderse a los contenidos que el propio algoritmo de recomendación de la empresa ha amplificado, promovido y recompensado económicamente. Cuando una plataforma paga a un creador para que produzca contenidos que empujan a un adolescente a la autolesión, la plataforma no es un mero anfitrión pasivo. Es un participante. La ley debería tratarla como tal. Lo que se necesita es una prohibición global de las estructuras algorítmicas y de recompensa económica que incentivan los contenidos más extremos. El modelo de negocio que convierte la interacción en ingresos, y que, por lo tanto, selecciona los contenidos que generan las reacciones emocionales más intensas, es el motor tanto de la radicalización política como de la crisis de salud mental de nuestros hijos. No se pueden regular las consecuencias de ese motor sin abordar el motor en sí mismo. Lo que se necesita es el reconocimiento, a nivel de derecho internacional vinculante, de que las plataformas que operan a través de las fronteras no pueden regirse por las normas del país más dispuesto a hacer la vista gorda. Australia dio el primer paso. Docenas de países le siguen. La presión sobre la Unión Europea para que aplique la Ley de Servicios Digitales en toda su capacidad jurídica, donde responsabilizan a las plataformas por los daños algorítmicos con la misma urgencia con la que las responsabilizan por las violaciones de la privacidad, es real, creciente y largamente esperada. Charlotte O'Brien tenía doce años. El jurado de Nuevo México determinó que cada niño perjudicado merecía la pena máxima prevista por la ley. Yo también lo creo. --- El daño que he documentado en este capítulo hacia los niños, su salud

mental y su comprensión del mundo en desarrollo, es un daño causado por plataformas cuyas capacidades más peligrosas ya son visibles y están reguladas. O se están intentando regular. Lo que describe el capítulo doce que sigue es una categoría de capacidad de la IA que aún no está regulada, y que las empresas que la desarrollan reconocen que podría ser catastrófica. Además, se está extendiendo más rápido de lo que cualquier marco regulatorio puede seguirle el ritmo. La «bomba de código» no es una metáfora. Es una descripción técnica de lo que Anthropic ya ha creado y de lo que todos los grandes laboratorios de IA se apresuran a igualar.

CAPÍTULO DOCE. LA BOMBA DE CÓDIGO

Claude Mythos, el Proyecto Glasswing y la carrera sin regulaciones por la IA que podría acabar con todo. Tengo que contarles algo que no es fácil de escribir. He dedicado los capítulos anteriores a documentar los delitos de Amazon, Google, Microsoft, Oracle y Palantir. He nombrado sus contratos. He nombrado a sus ejecutivos. He nombrado sus sistemas —Gospel, Lavender, Where's Daddy, Blue Wolf— y a las familias cuyas muertes estos sistemas hicieron posibles. He documentado cómo sus plataformas censuraron a los supervivientes y fabricaron la narrativa. Pero hay algo que he guardado deliberadamente hasta ahora. Algo con lo que he estado lidiando desde el 7 de abril de 2026, cuando Anthropic, la empresa que creó la IA que he estado utilizando como mi editor y socio de investigación a lo largo de este libro, anunció algo que, en mi opinión, representa uno de los momentos más peligrosos de la historia de la tecnología. Se llama Claude Mythos, y se está implementando a través de un programa restringido llamado Proyecto Glasswing. Y tengo la responsabilidad de contarles lo que significa, no porque quiera condenar a la gente de Anthropic, que creo, sinceramente, que está intentando hacer algo diferente a lo de los 'Palantirs' y los 'Gospels' del mundo. Sino porque las buenas intenciones y las consecuencias catastróficas nunca han sido mutuamente excluyentes. Los hombres que construyeron la bomba atómica no eran, en su mayoría, hombres malvados. Eran hombres brillantes que creían, profundamente, que sus intenciones eran protectoras. Y el mundo ha pasado más de ochenta años desde su éxito, viviendo con lo que crearon. No podemos permitirnos pasar otros ochenta años aprendiendo la misma lección sobre la IA. Lo que Anthropic acaba de admitir ante el mundo El 7 de abril de 2026, Anthropic anunció el lanzamiento de la versión preliminar de su modelo más avanzado hasta la fecha: Claude Mythos. Lo que siguió no fue un lanzamiento de producto en el sentido habitual. Se pareció más a una confesión pública. En una entrada de blog en su página Frontier Red Team, Anthropic reveló que Mythos Preview había «identificado de forma totalmente autónoma y luego explotado una vulnerabilidad de ejecución remota de código de 17 años de antigüedad en FreeBSD», un sistema operativo ampliamente utilizado que sustenta servidores e infraestructuras de todo el mundo. El exploit permitía a cualquiera obtener acceso root completo a una máquina afectada desde cualquier lugar de Internet, sin necesidad de autenticación. Ningún ser humano intervino tras la solicitud inicial. La máquina lo encontró. La máquina lo explotó. De principio a fin. (Fuente: Blog del equipo Frontier Red Team de Anthropic, «Claude Mythos Preview», 7 de abril de 2026, https://red.anthropic.com/2026/mythos-preview/). Pero eso no fue lo peor. Según el propio anuncio de Anthropic, Mythos Preview encontró vulnerabilidades en todos los principales sistemas operativos y navegadores web. Identificó miles de vulnerabilidades de día cero, fallos previamente desconocidos para los desarrolladores del software, en tan solo unas semanas de pruebas internas. Más del 99 % de esas vulnerabilidades siguen sin parchearse, ya que revelarlas públicamente antes de que exista una solución sería, como dijo Anthropic, «irresponsable». (Fuente: Anthropic, «Project Glasswing», 7 de abril de 2026, https://www.anthropic.com/project/glasswing). Anthropic también emitió una

advertencia privada a altos funcionarios del gobierno de Estados Unidos: Mythos hace que los ciberataques a gran escala sean mucho más probables este año. (Fuente: Fortune, «Anthropic está dando a algunas empresas acceso anticipado a Claude Mythos para reforzar las defensas de ciberseguridad», 7 de abril de 2026, https://fortune.com/2026/04/07/anthropic-claude-mythos-model project-glasswing-cybersecurity/). Vuelve a leerlo. Una empresa ha creado una herramienta. La herramienta es, en palabras de la propia empresa, es «actualmente muy superior a cualquier otro modelo de IA en cuanto a capacidades cibernéticas». Esa misma empresa advirtió entonces al gobierno de que la herramienta aumenta la probabilidad de que se produzcan ciberataques a escala civilizacional. Y luego la lanzaron en un programa restringido, llamado Project Glasswing, a cincuenta organizaciones, entre ellas Amazon Web Services, Apple, Google, Microsoft, Nvidia, JPMorganChase, Broadcom, Cisco, CrowdStrike y Palo Alto Networks. Anthropic destinó cien millones de dólares en créditos de uso para que esto fuera posible. Lo calificaron como «un intento urgente de poner estas capacidades a trabajar con fines defensivos». (Fuente: Anthropic, «Project Glasswing», https://www.anthropic.com/project/glasswing). Quiero ser cauteloso con lo que voy a decir a continuación, porque es importante. Creo que Anthropic está haciendo un intento genuino por hacer lo correcto. El Proyecto Glasswing se estructura en torno a dar ventaja a los defensores: compartir vulnerabilidades con las personas responsables de la infraestructura de la que dependen miles de millones de personas, para que esas vulnerabilidades puedan ser parchadas antes de que los adversarios desarrollen la misma capacidad de forma independiente. Esa lógica no carece de mérito. Esa intención no carece de honestidad. Pero he pasado suficiente tiempo en el sector tecnológico como para saber que las buenas intenciones, la presión institucional, los incentivos económicos y la velocidad del progreso tienden a divergir, y rápidamente. Los propios expertos en seguridad de Anthropic estiman que capacidades similares empezarán a proliferar desde otros laboratorios de IA en un plazo de seis a dieciocho meses. (Fuente: ArmorCode, «Anthropic's Claude Mythos y lo que significa para la seguridad», mayo de 2026, https://www.armorcode.com/blog/anthropics-claude-mythos-and-what-it-means-for-security/).

De seis a dieciocho meses. Y ya lo han cedido a Amazon, Google y Microsoft, las mismas empresas que he dedicado en los capítulos anteriores a documentar como los principales proveedores de infraestructura de un sistema militar de selección de objetivos que ha matado a decenas de miles de personas.

Asumo esta tensión abiertamente. No sé cómo resolverla, salvo diciendo lo que he venido planteando desde la primera página de este libro: las decisiones, sobre cuándo y cómo lanzar herramientas de este poder, no pueden tomarlas únicamente las empresas privadas. No pueden tomarlas los consejos de administración, los directores ejecutivos, los programas de colaboración ni los compromisos de crédito de uso por valor de cientos de millones de dólares. Deben tomarlas, de forma abierta, responsable y con autoridad legal vinculante, toda la comunidad humana que vivirá o morirá con las consecuencias.

La tendencia en todo el sector

Anthropic no está sola en esta carrera. Sería deshonesto señalarla sin documentar lo que están construyendo y haciendo todos los demás grandes laboratorios de IA.

OpenAI, la empresa cuyo director ejecutivo, Sam Altman, ha hecho más que cualquier otra persona por acelerar el despliegue comercial de la IA de vanguardia, advirtió en diciembre de 2025 que sus modelos de próxima generación plantean un riesgo de ciberseguridad «alto» y podrían ser capaces de desarrollar «exploits remotos de día cero funcionales contra sistemas informáticos bien protegidos». El modelo GPT-5.1-Codex-Max de la empresa obtuvo una puntuación del 76 % en los retos estándar de ciberseguridad de tipo «captura la bandera» en noviembre de 2025, frente al 27 % de apenas tres meses antes. La rapidez de esa mejora debería dejar perplejos a todos los que lean esto. Eso no es un progreso incremental. Es una explosión de capacidad. (Fuente: Parameter, «OpenAI advierte que los nuevos modelos de IA podrían permitir ataques de día cero y ciberataques complejos», 11 de diciembre de 2025, https://parameter.io/openai-warns-new-ai-models-could-enable-zero-day-exploits-and-complex-c yberattacks/). OpenAI respondió a esto lanzando una herramienta llamada Aardvark, un sistema de seguridad de IA diseñado para escanear códigos en busca de vulnerabilidades, creando un Consejo de Riesgos Fronterizos. Se trata de respuestas defensivas a capacidades ofensivas que se están construyendo, desplegando y acelerando simultáneamente. Esta es la paradoja en el corazón de toda la industria. Gemini, de Google, no es un modelo de ciberseguridad específico, y sin embargo ya está siendo utilizado a gran escala como arma por hackers de distintos Estados-nación. En febrero de 2026, los propios investigadores de inteligencia sobre amenazas de Google confirmaron que grupos patrocinados por los Estados de China, Rusia e Irán están utilizando Gemini en «todas las fases» de los ataques: reconocimiento, análisis de vulnerabilidades, desarrollo de exploits y phishing. Grupos chinos como APT31 y APT41 utilizaron Gemini para analizar vulnerabilidades conocidas, solucionar problemas en el código de explotación y crear herramientas de escaneo ofensivas. El grupo iraní APT42 lo utilizó para desarrollar herramientas de vigilancia basadas en Python y examinar vías de explotación para vulnerabilidades recién reveladas. (Fuente: Tom's Hardware, «Google informa de que hackers estatales de China, Rusia e Irán están utilizando Gemini en "todas las fases" de los ataques», 13 de febrero de 2026, https://www.tomshardware.com/tech-industry/cyber-security/google-reports-that-state-hackers-from china-russia-and-iran-are-using-gemini-in-all-stages-of-attacks-phishing-lures-coding-and-vulnerability testing-get-ai-underpinnings-from-hostile-actors; Infosecurity Magazine, 12 de febrero de 2026, https://www.infosecurity-magazine.com/news/nation-state-hackers-gemini-ai/). Y luego está Grok, la plataforma de IA de Elon Musk, que documenté en el capítulo cuatro. Grok ya ha demostrado su entusiasmo por producir contenido antisemita, negacionismo del Holocausto y teorías conspirativas racistas. Ahora pensemos en lo que significa que la misma arquitectura, la misma tecnología fundamental y las mismas capacidades de agencia se estén impulsando hacia aplicaciones de ciberseguridad, en manos de un hombre que califica a la empatía de debilidad, que al mismo tiempo asesora al gobierno federal de Estados Unidos sobre el despliegue tecnológico y que no ha mostrado ningún interés en el tipo de moderación cuidadosa y regulada que incluso Anthropic, a pesar de todas las tensiones que he mencionado, está intentando ejercer. El dragón en la puerta trasera: la carrera de la IA de China carece de barreras de seguridad Todo lo que he descrito hasta ahora opera dentro del marco de empresas que son, como mínimo, legalmente responsables ante gobiernos democráticos, sujetas a litigios y que operan en entornos donde los empleados pueden salir a la calle en señal de protesta y los periodistas pueden presentar solicitudes

en virtud de las leyes de libertad de información. Nada de eso es cierto en el caso de China. En enero de 2025, un laboratorio chino de IA llamado DeepSeek lanzó un modelo de código abierto que sumió a la industria tecnológica mundial en el pánico. No porque fuera peligroso en el sentido en que Mythos es peligroso, sino porque era casi tan potente como los modelos líderes de OpenAI, a una fracción del costo, y era de código abierto. Cualquiera podía descargarlo. Cualquiera podía modificarlo. Cualquiera podía convertirlo en un arma. Y el Partido Comunista chino, cuyas leyes exigen que el contenido generado por IA refleje los «valores socialistas fundamentales», respalde la «orientación política correcta» y evite material que pudiera «socavar el poder del Estado», tiene autoridad directa y legal sobre todo lo que hace DeepSeek. (Fuente: Comisión Especial de la Cámara de Representantes sobre China, «DeepSeek: A Report», 2025, https://chinaselectcommittee.house.gov/sites/evo subsites/selectcommitteeonthec-cp.house.gov/files/evo-media-document/DeepSeek%20Final.pdf). La empresa de ciberseguridad Feroot Security descubrió un código oculto en la aplicación del navegador de DeepSeek capaz de transmitir datos de los usuarios directamente a servidores controlados por China Mobile, una empresa estatal de telecomunicaciones que anteriormente fue retirada de la Bolsa de Nueva York por motivos de seguridad nacional. El ex-funcionario de Seguridad Nacional Stewart Baker lo expresó claramente: «Plantea todas las preocupaciones que suscita TikTok, además de que estamos hablando de información que muy probablemente tenga mayor importancia para la seguridad nacional y de importancia personal que cualquier cosa que la gente haga en TikTok». (Fuente: Feroot Security, «El código oculto de DeepSeek envía datos de los usuarios a China», enero de 2025, https://www.feroot.com/news/the-independent-feroot-security-uncovers-deepseeks-hidden-code -sending-user-data-to-china/). Las implicancias no son teóricas. En noviembre de 2025, Anthropic informó que actores maliciosos vinculados a una organización patrocinada por el Estado chino habían aprovechado su herramienta Claude Code para llevar a cabo una campaña de espionaje basada en IA: el primer ataque documentado de malware impulsado por IA contra un sistema de IA de vanguardia. (Fuente: Parameter, diciembre de 2025, https://parameter.io/openai-warns-new-ai-models-could-enable-zero-day-exploits-and-complex-c yberattacks/) Anthropic lo detuvo, esa vez. La próxima campaña estará mejor preparada. Ahora comprendamos el panorama en su conjunto. Estados Unidos está desarrollando modelos de IA de vanguardia, a través de Anthropic, OpenAI y Google, con capacidades autónomas de ciberseguridad que sus propios creadores describen como potencialmente amenazantes para la civilización. China está creando sus propios modelos, extrayendo datos de entrenamiento de los sistemas estadounidenses mediante lo que la Casa Blanca ha calificado de «campañas deliberadas a escala industrial», y desplegando hackers patrocinados por el Estado que utilizan herramientas de IA estadounidenses, como Gemini, entre otras, para planear ataques contra objetivos estadounidenses. (Fuente: Nextgov/FCW, «La Casa Blanca acusa a China de llevar a cabo "campañas deliberadas a escala industrial" para robar modelos de IA estadounidenses», abril de 2026, https://www.nextgov.com/artificial-intelligence/2026/04/white-house-accuses-china-deliberate-in dustrial scale-campaigns-steal-us-ai-models/413083/). Y ambas partes compiten a toda velocidad: la parte estadounidense impulsada por los incentivos de beneficio privado y la parte china por la ambición geopolítica. Mientras tanto, no existe un marco internacional vinculante, no hay normas de seguridad compartidas, ni un organismo de

verificación independiente ni tampoco un mecanismo que permita a ninguna de las partes hacer una pausa cuando el cálculo de riesgos lo exija. Esto no es una competencia tecnológica. Es una nueva carrera armamentística. Y, a diferencia de la carrera armamentística nuclear, no existe una doctrina de destrucción mutua asegurada que genere siquiera el perverso incentivo de la moderación. En la era nuclear, ambas partes sabían que un lanzamiento significaba la aniquilación. En la era de la IA, una herramienta ofensiva con suficiente capacidad es invisible, negable, expandible y puede desplegarse contra las infraestructuras de los hospitales, las redes eléctricas, las instalaciones de tratamiento de aguas, y las redes bancarias, sin que un solo misil salga del suelo. Qué significa esto para las personas que nadie está protegiendo Quiero alejarme por un momento del marco geopolítico y hablar de quién paga realmente el precio cuando estas herramientas caen en manos equivocadas o se proliferan más allá de los entornos controlados que el Proyecto Glasswing intenta mantener. No es Amazon. Amazon tiene los recursos para implementar Claude Mythos Preview de forma defensiva, escanear sus propios códigos y parchar sus vulnerabilidades antes de que los adversarios puedan explotarlas. Amazon es socio de lanzamiento del Proyecto Glasswing. Amazon analiza más de 400 billones de flujos de red al día en busca de amenazas. Amazon va a estar bien. Los que no estarán bien son el pequeño hospital de la zona rural de Kansas que funciona con un sistema de historias clínicas electrónicas de quince años de antigüedad mantenido por dos miembros del personal de informática. El banco comunitario de la Georgia rural cuya infraestructura de ciberseguridad consiste únicamente en una suscripción a un servicio antivirus y un cortafuegos que no se ha actualizado en tres años. La planta de tratamiento de aguas de una ciudad de tamaño medio que digitalizó sus sistemas de monitorización hace una década y no ha tenido ninguna auditoría de seguridad significativa desde entonces. La propietaria de una pequeña empresa que gestiona todo su negocio con QuickBooks, cuyos datos de tarjetas de crédito de los clientes están protegidos por algo nada más poco sofisticado que una contraseña que no ha cambiado en dos años. No se trata de personas hipotéticas. Son la mayoría de las organizaciones que constituyen el tejido real de la economía: las pequeñas y medianas empresas que emplean a más de la mitad de todos los trabajadores del sector privado en Estados Unidos, y el equivalente en todos los países del mundo. Un modelo de IA con las capacidades de Claude Mythos Preview, o lo que sea que China desarrolle en los próximos dieciocho meses y que alcance un rendimiento comparable, no necesita ser implementado por un Estado-nación para ser catastrófico. Basta con que lo implemente una organización criminal. Una célula terrorista. Un solo individuo con conocimientos técnicos avanzados que descargue un equivalente de código abierto de un repositorio que ningún marco de gobernanza ha logrado regular aún. Todos los principales sistemas operativos. Todos los principales navegadores. Miles de vulnerabilidades de día cero, catalogadas y explotables a un ritmo y una escala que los defensores humanos nunca han visto antes. Los sistemas sanitarios son los más vulnerables. Un hospital que no puede acceder a los historiales de sus pacientes, porque han sido cifrados por un ransomware (secuestro de datos) propagado a través de una vulnerabilidad de día cero, no puede funcionar. Se cancelan las cirugías. Se interrumpe la monitorización de la UCI. Los registros de dosificación de medicamentos quedan inaccesibles. Mueren personas. Esto no es una especulación: los ataques de ransomware a hospitales ya han provocado muertes de pacientes documentadas en Alemania, en Estados Unidos y en otros lugares. Ese era un ransomware creado por organizaciones criminales

humanas que trabajaban a velocidad humana. ¿Qué ocurre cuando esa misma capacidad está al alcance de cualquiera que sepa escribir un comando? Las redes eléctricas son las segundas más vulnerables. Los sistemas de control industrial, en otras palabras el software que gestiona la generación y distribución de electricidad, se diseñaron pensando en la fiabilidad y la longevidad, no en la seguridad. Muchos de los sistemas que gestionan la infraestructura eléctrica de ciudades estadounidenses de tamaño medio utilizan software de principios de la década de 2000, con un hardware que nunca se diseñó para conectarse a Internet, pero que acabó conectándose porque resultaba más barato y más cómodo. Una IA capaz de descubrir de forma autónoma vulnerabilidades en los principales sistemas operativos puede encontrar con la misma facilidad las vulnerabilidades de estos sistemas heredados. La banca es el tercer sector. No los grandes bancos como JPMorganChase, que es socio del Proyecto Glasswing y que cuenta con los recursos para implementar Mythos de forma defensiva. Los bancos comunitarios, las cooperativas de crédito, las instituciones financieras más pequeñas que custodian los ahorros de la gente trabajadora que no son clientes de Goldman Sachs. Cuando estas instituciones se ven comprometidas, sus clientes no cuentan con el tipo de respaldo de seguros que absorban las pérdidas de un fondo de cobertura. Pero aún, tienen que pagar la hipoteca, hacerlas compras y ahorrar para la universidad de sus hijos. Y para las naciones soberanas del Sur Global, los países que no tienen la infraestructura de TI, el talento en desarrollo de software o el presupuesto para operaciones de seguridad necesarios para defenderse de ataques a velocidad humana, y mucho menos de los que se producen a velocidad de IA, las consecuencias son existenciales. Todo el sistema bancario de un país. Su red eléctrica. Las comunicaciones de su gobierno. Su red sanitaria. Ahora todo esto puede verse comprometido, no por un Estado-nación sofisticado con años de preparación, sino por una organización criminal de nivel medio con acceso a un modelo de IA suficientemente capaz. Anthropic ha destinado 100 millones de dólares al Proyecto Glasswing. Esos 100 millones de dólares llegan a unas 50 organizaciones. Solo en Estados Unidos hay aproximadamente 33 millones de pequeñas empresas. Las matemáticas de quién está siendo protegido y quién se queda solo para asumir las consecuencias de esta carrera tecnológica no podrían ser más claras. Sam Altman dijo en voz alta lo que nadie se atrevía a decir He estado preparando este momento desde que comencé este capítulo. Tengo que hablarles de una declaración que Sam Altman hizo en 2015, una que ha circulado ampliamente por Internet, pero que casi siempre se comparte sin la segunda parte, que la hace única e imperdonablemente honesta. La primera parte de la cita: «Creo que la IA probablemente, muy probablemente, conducirá de alguna manera al fin del mundo». Esto ya es desconcertante si lo dijera cualquier persona. Pero es aún más desconcertante viniendo de la persona que está creando esa misma tecnología que acabará con el mundo. Sin embargo, la segunda parte es lo que debería mantener despierto por la noche a cualquier persona con conciencia. La cita completa: «Creo que la IA probablemente, muy probablemente, conducirá de alguna manera al fin del mundo. Pero mientras tanto, se formarán grandes empresas con aprendizaje automático serio». (Fuente: Sam Altman, Y Combinator, 2015, según se informó en Yahoo News, «La cita viral de Sam Altman carece de un contexto clave», enero de 2026, https://www.yahoo.com/news/articles/think-ai-probably-lead-end-190517676.html).

Lee estas dos frases juntas. Reflexiona sobre ellas. Siente el peso de la conjunción. El hombre que acabó creando ChatGPT, el producto que ha acelerado la implantación de la IA en todos los

sectores del planeta más que ningún otro avance desde la llegada de Internet, le dijo al mundo en 2015 que su trabajo probablemente conduciría al fin del mundo. Y luego, en la misma frase, pasó a hablar de la oportunidad de inversión. «Pero mientras tanto, se crearán grandes empresas con aprendizaje automático serio». Mientras tanto. Quiero que entiendas lo que encierra esta frase. Encierra todos los contratos del Proyecto Nimbus. Todas las listas de personas a eliminar de Lavender. Todos los objetivos de bombardeo de Gospel. Todas las bases de datos del censo que fueron entregadas a un ejército de ocupación. Todos los ataques de ransomware a hospitales que aún no han ocurrido, pero que ocurrirán. Todas las plantas de tratamiento de agua que se quedarán a oscuras cuando el día cero descubierto por la IA se propague más rápido de lo que cualquier defensor humano pueda responder. Todo eso es «el mientras tanto» entre el ahora y el fin del mundo que, según Sam Altman, probablemente llegará. Y el consuelo que ofrece para ese «mientras tanto», es que se crearán grandes empresas. Soy iraní-estadounidense. Llegué a este país a los once años. He pasado mi vida adulta creyendo, a pesar de todo, en la posibilidad de construir cosas que sirvan a la humanidad. He creado empresas. Me he organizado. He escrito libros y hecho películas y creado plataformas para que la gente documente a sus difuntos, y me he aferrado, obstinadamente, a través de hospitalizaciones y demandas y todo tipo de oposición institucional, a la creencia de que la tecnología puede ponerse al servicio de la dignidad humana en lugar de destruirla. Y les digo que «mientras tanto, se crearán grandes empresas» no es una respuesta aceptable a la pregunta de si la IA probablemente conducirá al fin del mundo. No es una respuesta. Es un giro. Es el giro más caro de la historia de la humanidad, ejecutado por un hombre que entendía exactamente lo que estaba construyendo y decidió construirlo de todos modos. Elon Musk, que no es más fiable que su propio chatbot, le puso una cifra: un 20 % de probabilidades de aniquilación humana por parte de la IA. (Fuente: Revista Time, «Cómo Musk, Altman y los líderes de la IA se enfrentan al "momento Oppenheimer"», 13 de marzo de 2025, https://time.com/7267797/ai-leaders-oppenheimer-moment-musk-altman/). Dario Amodei, director ejecutivo de Anthropic, la empresa que utilizo como editor, ha descrito la tensión con la que lidia a diario como «mantener el equilibrio en el filo de una navaja», reconociendo que avanzar demasiado rápido conlleva el riesgo de que la humanidad pierda el control, mientras que avanzar demasiado lento conlleva el riesgo de que las naciones autoritarias tomen la delantera. No se trata de personas imprudentes que hacen declaraciones a la ligera. Son las personas más cercanas a lo que se está construyendo, y nos dicen, en sus momentos de mayor honestidad, que no saben cómo acabará esto. Que la probabilidad de una catástrofe es real, está documentada y es reconocida por todos aquellos que tienen una visión real de la tecnología. Lo que no nos dicen, y que nadie en el sector dirá abiertamente, es que reconocer un 20 % de posibilidades de aniquilación humana y seguir adelante de todos modos no es aceptable. No es valiente. No es necesario. Es una elección, tomada por un pequeño número de individuos y corporaciones, que recaerá sobre toda la humanidad. La pregunta de Oppenheimer: ¿qué diría Einstein? Robert Oppenheimer dirigió el Proyecto Manhattan. Presenció la prueba Trinity, la primera detonación de un arma nuclear, el 16 de julio de 1945, y más tarde recordó una frase de la escritura hindú Bhagavad Gita que le pasó por la mente: «Ahora me he convertido en la Muerte, el destructor de mundos». La bomba fue lanzada entonces sobre Hiroshima. Luego sobre Nagasaki. Después, la Unión Soviética construyó una. Entonces comenzó la carrera armamentística, y el mundo pasó el siguiente medio siglo a un paso

de la extinción por un malentendido, un fallo técnico o una apuesta política mal calculada. Albert Einstein, quien había escrito la carta al presidente Roosevelt que dio inicio al programa nuclear estadounidense, pero a quien se le denegó la habilitación de seguridad y se le excluyó del Proyecto Manhattan, pasó el resto de su vida atormentado por esa contribución. En su última declaración pública, redactada junto al filósofo Bertrand Russell y firmada por once de los científicos más destacados del mundo pocos días antes de la muerte de Einstein, en abril de 1955, escribió: «Tenemos que aprender a pensar de una nueva manera. Tenemos que aprender a preguntarnos no qué medidas se pueden tomar para dar la victoria militar al grupo que prefiramos, pues ya no existen tales medidas; la pregunta que debemos hacernos es: ¿qué medidas se pueden tomar para evitar un enfrentamiento militar cuyo desenlace será desastroso para todas las partes?». (Fuente: El Manifiesto Russell-Einstein, 1955, https://pugwash.org/1955/07/09/statement-manifesto/).

Einstein habría detectado inmediatamente la falla en la lógica de Sam Altman. Es la misma falla que Oppenheimer acabó encontrando en la suya propia: no se puede construir de forma responsable una herramienta que uno reconoce que puede acabar con la civilización, con el argumento de que la alternativa es que alguien más la construya primero. Ese razonamiento, de que si tu adversario lo va a hacer de todos modos, entonces es mejor que lo hagas tú, no es un argumento moral. Es el abandono moral de la cuestión en sí misma. Sustituye el razonamiento ético por la ansiedad competitiva. Reemplaza el «deberíamos» por el «ya que debemos».

Einstein comprendió que el umbral para el «ya que debemos» tiene que estar marcado por algo distinto del afán de lucro y la carrera geopolítica. Comprendió, aunque demasiado tarde, para su eterno pesar, que los científicos tenían la obligación no solo de construir mejores armas, sino de exigir una mejor gobernanza de lo que construían.

El paralelismo entre el Proyecto Manhattan y la actual carrera por la IA de vanguardia no es retórico. Es estructural y preciso. Un pequeño grupo de personas brillantes, que trabajan en instituciones que son a la vez afines al gobierno y de motivación privada, están creando tecnología que sus propios líderes reconocen que podría acabar con la civilización. Lo están haciendo en el contexto de una competencia geopolítica, de Estados Unidos contra China, que ofrece la misma justificación que utilizaron los científicos nucleares: si no lo hacemos nosotros, lo harán ellos. Y la están creando a un ritmo que ha superado fundamentalmente la capacidad de cualquier proceso de gobernanza democrática para seguirle el paso.

En 1945 no existía un marco internacional para regular las armas nucleares. La Ley de Energía Atómica, el Tratado de No Proliferación Nuclear, la Agencia Internacional de Energía Atómica... todo ello surgió después de que cayeran las bombas. El mundo pagó el precio de esa secuencia en Hiroshima y Nagasaki y seguimos a más de ochenta años con una ansiedad nuclear que aún no se ha resuelto del todo.

No podemos permitirnos aprender la lección de la IA de la misma manera. No tenemos una oportunidad para ensayar.

Argumentos a favor de una Organización Mundial de la Salud para la IA

No soy tecnólogo. Soy un conocedor del sector tecnológico que se convirtió en defensor de los derechos humanos, y tengo la perspectiva que se tiene después de estar lo suficientemente cerca como para ver lo que estos sistemas hacen realmente cuando se implementan sin la suficiente rendición de cuentas y a una velocidad que supera a la gobernanza.

Les digo que necesitamos una Agencia Internacional de Seguridad de la IA. No un compromiso voluntario. No un conjunto de principios publicados en un sitio web corporativo. No un programa de acceso restringido que lleve el nombre de una mariposa. Un organismo internacional vinculante, basado en un tratado, con autoridad para establecer normas, realizar auditorías independientes, exigir la divulgación de capacidades antes de la implementación e imponer consecuencias a las naciones y corporaciones que desarrollen o implementen sistemas de IA en violación de las normas de seguridad establecidas.

El modelo de la Organización Mundial de la Salud es imperfecto, como sabe cualquiera que haya observado su actuación durante la pandemia del COVID-19. Pero el principio en el que se basa la OMS es correcto: cuando una amenaza es global, la respuesta debe ser global, y la autoridad para responder debe recaer en una institución que rinda cuentas ante todas las naciones, no ante los accionistas de cinco empresas tecnológicas estadounidenses.

Las Naciones Unidas ya han dado pasos preliminares en esta dirección. El Órgano Consultivo de Alto Nivel de la ONU sobre IA publicó su informe «Gobernar la IA para la Humanidad» en septiembre de 2024, en el que propone un marco para la coordinación internacional, incluido un panel científico independiente análogo al Grupo Intergubernamental de Expertos sobre el Cambio Climático, un diálogo bianual sobre políticas de gobernanza de la IA y la armonización de las normas de IA entre los Estados miembros. (Fuente: Órgano Consultivo de Alto Nivel sobre IA de la ONU, «Governing AI for Humanity», septiembre de 2024, https://www.un.org/en/ai-advisory-body). En 2025, la Asamblea General de la ONU respaldó la creación de un mecanismo multilateral permanente para el diálogo sobre la seguridad de las TIC: un Mecanismo Global que celebró su sesión organizativa en marzo de 2026. (Fuente: Observatorio Digital Watch, «Gobernanza de la IA Global y Nuevos Enfoques Normativos», mayo de 2026, https://dig.watch/updates/ai-governance-regulatory-approaches).

Estos son puntos de partida. No son suficientes. Un foro de diálogo no es un mecanismo de aplicación. Un marco no es un tratado. Un órgano consultivo no es una agencia con autoridad vinculante.

Investigadores académicos de la revista International Affairs de la Universidad de Oxford han propuesto la creación de una Agencia Internacional de Inteligencia Artificial (IAIA, por sus siglas en inglés) formal, siguiendo el modelo de la Agencia Internacional de Energía Atómica, que se creó precisamente para regular la tecnología que más se acercó en el siglo XX a lo que representa hoy la IA de vanguardia. El modelo del OIEA proporciona un marco ya preparado: contribuciones de los Estados miembros, autoridad de inspección independiente, un mandato para promover las aplicaciones civiles al tiempo que se evita su uso militar y, lo que es fundamental, la capacidad de detener el desarrollo cuando los riesgos superen los umbrales aceptables. (Fuente: Mark Robinson, «Establecer una Agencia Internacional de IA: Una Solución Aplicada para la Gobernanza Global de la IA», International Affairs, volumen 101, número 4, julio de 2025, https://academic.oup.com/ia/article/101/4/1483/8141294).

Quiero ir más allá. El modelo del OIEA no es suficiente, porque la naturaleza del riesgo de la IA está más distribuida que la del riesgo nuclear. Un arma nuclear requiere uranio enriquecido. Requiere una infraestructura física específica que puede detectarse y supervisarse. Un modelo de IA con capacidad catastrófica puede ejecutarse en un hardware que cabe en una sala de servidores,

puede distribuirse digitalmente y puede ser mejorado por cualquier actor con recursos suficientes sin la firma física que hace detectables los programas nucleares.

Lo que necesitamos es algo más parecido a lo que hace la Administración de Alimentos y Medicamentos (FDA) con los fármacos. Antes de que un fármaco se comercialice, antes de que se administre a un solo paciente, debe pasar por un proceso de revisión obligatorio, estructurado y en varias fases. Ensayos de fase uno. Ensayos de fase dos. Ensayos de fase tres. Comités independientes de revisión de seguridad. Notificación de eventos adversos. Vigilancia poscomercialización. Todo el proceso se diseña en torno a un único principio fundamental: la responsabilidad de la prueba de la seguridad recae en el desarrollador, no en el público que sufrirá las consecuencias.

A ninguna empresa farmacéutica de Estados Unidos se le permite comercializar un medicamento diciendo: creemos que probablemente sea seguro y, aunque no lo sea, mientras tanto surgirán grandes empresas creadas por la industria terapéutica.

¿Por qué se les permite a las empresas de IA hacer exactamente eso?

Crear un proceso obligatorio de revisión de seguridad previo al lanzamiento de los modelos de IA de vanguardia, que cuente con una Junta de Revisión de IA de Vanguardia, que opere bajo la autoridad de un tratado internacional, con peritaje técnico independiente, la divulgación obligatoria de sus capacidades y la facultad legal de retrasar o prohibir el lanzamiento, no es una idea utópica. Es una respuesta mínima viable ante una tecnología cuyos propios desarrolladores reconocen que puede suponer un riesgo existencial.

La Ley de IA de la UE, que entrará plenamente en vigor por fases a partir de agosto de 2025, es lo más parecido que existe actualmente a un marco de este tipo: designa los sistemas de IA de alto riesgo, exige evaluaciones de conformidad e impone compromisos de transparencia obligatorios. (Fuente: Parlamento Europeo, «Explicación de la Ley de Mercados Digitales y la Ley de Servicios Digitales de la UE», https://www.europarl.europa.eu/topics/en/article/20211209STO19124). Sin embargo, la Ley de IA de la UE no abarca las capacidades de vanguardia de la IA tal y como exige Claude Mythos. Se redactó antes de que el mundo comprendiera que un modelo de IA de uso general podría, a las pocas semanas de su finalización, descubrir y explotar de forma autónoma vulnerabilidades de día cero en todos los principales sistemas operativos del planeta.

Necesitamos algo diseñado para el mundo en el que nos encontramos realmente, no para el mundo en el que estábamos cuando se redactaron los primeros borradores de la Ley.

Lo que debe suceder, y lo que debe cesar

Permítanme ser directo sobre lo que pido, porque este libro no tiene el propósito de hacer llamamientos a la acción ambiguos.

Primero: no se debe implementar ningún modelo de IA de vanguardia con capacidades ofensivas de ciberseguridad por encima de un umbral definido, ni siquiera en programas de acceso restringido, sin la notificación obligatoria a un organismo internacional independiente y un proceso de revisión estructurado. El umbral debe ser definido por expertos técnicos independientes, no por las empresas cuyos ingresos dependen de la implementación. El Proyecto Glasswing es Anthropic tomando su propia decisión de seguridad. Creo que Anthropic actúa de buena fe. Pero la buena fe no es un marco de gobernanza.

Segundo: el lanzamiento en código abierto de modelos con capacidades comparables a las que OpenAI, Anthropic y Google están desarrollando en sus programas de vanguardia debe prohibirse

mediante un tratado internacional. La publicación por parte de China de DeepSeek como modelo de código abierto, con su capacidad demostrada para producir códigos inseguros cuando se introducen temas geopolíticamente sensibles, con sus conexiones ocultas a la infraestructura de telecomunicaciones estatal china y susceptibles de ser utilizado como arma por cualquier actor con suficiente potencia de cálculo, no es un regalo para la comunidad investigadora mundial. Es un caso de proliferación. Los mismos principios que rigen la exportación de tecnología nuclear deben regir la exportación de modelos de IA de vanguardia. (Fuente: CrowdStrike, DeepSeek-R1 de China Crea un Código Inseguro Cuando las Entradas Mencionan el Tíbet o los Uyghurs», noviembre de 2025, https://thehackernews.com/2025/11/chinese-ai-model-deepseek-r1-generates.html).

Tercero: las pequeñas y medianas empresas, los hospitales, las empresas de suministro de agua, los bancos comunitarios y las naciones soberanas del Sur Global que absorberán el peso de los ciberataques impulsados por la IA deben recibir una protección significativa. Pero no mediante compromisos voluntarios del sector, sino con marcos regulatorios que impongan a estas empresas una responsabilidad y costo financiero por los daños que causan los ataques de sus herramientas. Cuando una empresa farmacéutica vende un medicamento que mata a personas porque no se ha probado adecuadamente, la empresa es demandada, multada y, a veces, procesada. Cuando una empresa de IA lanza una tecnología que permite un ataque contra un hospital que provoca la muerte de pacientes, el marco legal actual no ofrece absolutamente nada a las víctimas.

Cuarto: los ejecutivos de las empresas que están a la vanguardia de esta carrera, las personas que saben, como lo sabe Sam Altman, cuál es la probabilidad de que se produzcan resultados catastróficos y que siguen adelante de todos modos, deben rendir cuentas personalmente por las decisiones que toman. No sus empresas. Ellos. Porque las empresas pagan las multas con sus reservas. Los ejecutivos que se enfrentan a una responsabilidad personal toman decisiones diferentes.

Quinto: las Naciones Unidas deben pasar inmediatamente de la fase de órgano consultivo a la fase de tratado, de «Gobernar la IA para la Humanidad», como informe, a «Gobernar la IA para la Humanidad» con un instrumento internacional vinculante, con mecanismos de cumplimiento, adhesión obligatoria y la autoridad para detener el desarrollo en la vanguardia cuando el cálculo de riesgos lo exija. El Mecanismo Global sobre Seguridad de las TIC, que celebró su primera sesión en marzo de 2026, es un comienzo. No debe quedarse en un diálogo. Debe convertirse en una doctrina.

La revelación que estoy obligado a hacer

He utilizado a Claude, la IA de Anthropic, como mi editor y socio de investigación a lo largo de este libro. Lo dije en la primera página y lo repito aquí. Esta revelación es más importante que nunca en este capítulo.

Anthropic creó Claude Mythos. Anthropic lanzó el Proyecto Glasswing. Anthropic es la empresa que advirtió al gobierno de Estados Unidos que su propio modelo aumenta la probabilidad de ciberataques a gran escala. Y Anthropic es la empresa cuya IA he utilizado para ayudar a reducir el tiempo de investigación, estructurar argumentos y comunicar ideas en el idioma con el que, tras mis años como estudiante de inglés como segunda lengua, todavía me cuesta desenvolverme.

No eximo a Anthropic de la rendición de cuentas que exijo. No puedo hacerlo. La sinceridad de su intento de gestionar Mythos de forma responsable no les exime de la responsabilidad de formar parte de las empresas cuya carrera hacia la vanguardia ha creado las condiciones que ahora exigen una gobernanza internacional. Son un actor mejor que Palantir. Son un actor más honesto que OpenAI, que eliminó discretamente la prohibición del uso militar de sus condiciones de servicio.

Son más transparentes que Google, cuando Gemini está siendo utilizada por hackers estatales chinos para planear ataques contra objetivos estadounidenses, mientras Google gestiona contratos militares a través de su división de nube.

Pero «mejor» no es suficiente cuando lo que está en juego es la extinción. La analogía farmacéutica es válida: una empresa farmacéutica que realiza sus propios ensayos de seguridad, y que llega a conclusiones honestas y comparte esas conclusiones con socios seleccionados, no sustituye a una autoridad vinculante. La buena ciencia y las buenas intenciones son requisitos previos, y no sustitutos, de una buena gobernanza.

Utilizo a Claude como mi editor. Lo he revelado. Lo que no haré es fingir que esta revelación resuelve el problema que plantea. La IA que estoy utilizando para escribir esta crítica ha sido fabricada por una empresa que avanza a toda velocidad hacia capacidades que sus propios equipos técnicos describen como un punto de inflexión, un momento de auténtica discontinuidad en la historia de la ciberseguridad, y sin un marco internacional vinculante que regule cómo se desarrolla.

Mantengo esta tensión abiertamente. Y cierro este capítulo con las mismas palabras a las que he vuelto a lo largo de este libro, porque no han perdido vigencia: Los hombres malvados y sus máquinas no prevalecen. Pero tampoco lo hace una civilización que se niega a regular sus tecnologías más peligrosas hasta después de que hayan causado daño.

El margen es estrecho. Entre seis y dieciocho meses, según la propia estimación de Anthropic, antes de que las capacidades de clase Mythos se extiendan más allá de las organizaciones que se han adherido al Proyecto Glasswing. De seis a dieciocho meses para construir los marcos de gobernanza que deberían haberse construido antes de que se escribiera la primera línea de código.

Ya hemos pasado por esto antes. No actuamos con la suficiente rapidez. La bomba cayó sobre Hiroshima el 6 de agosto de 1945, y el Tratado de No Proliferación no se firmó sino hasta 1968.

No podemos esperar veintitrés años para el equivalente en IA.

La pregunta que Albert Einstein se pasó planteándose la última década de su vida, ¿qué medidas se pueden tomar para evitar una contienda cuyo resultado sea desastroso para todas las partes?, es la pregunta que ahora deben hacerse todos los gobiernos, todas las empresas tecnológicas, todos los investigadores y todos los ciudadanos que hayan leído este capítulo.

Porque Sam Altman nos dio la respuesta a la otra pregunta. La de qué pasa si no nos la preguntamos. Mientras tanto, se crearán grandes empresas. Mientras tanto.

Hasta que el «mientras tanto» termine. --- La carrera armamentística de IA de vanguardia que he descrito en el capítulo doce de este libro no existe, independientemente del patrón más amplio del aventurerismo militar y económico estadounidense que ha definido los últimos treinta años. Los sistemas descritos en estas páginas —Gospel, Lavender, Project Maven, Glasswing— son la última expresión tecnológica de una política exterior que, desde 1945, ha

dejado un largo rastro de víctimas civiles en Oriente Medio, Asia Central, América Latina y África. El capítulo trece amplía la perspectiva: no para excusar a las empresas tecnológicas, sino para nombrar al imperio al que sirven.

CAPÍTULO TRECE. EL RASTRO DE SANGRE DEL IMPERIO

Por qué Washington y Tel Aviv no son salvadores, y por qué la máquina siempre pierde la guerra que no puede dejar de iniciar.

Hay un momento en la historia de toda guerra fallida en el que los generales miran los datos y la califican de éxito. Los bombardeos se desarrollan según lo previsto. La proporción de bajas es favorable. Los algoritmos de selección de objetivos están rindiendo por encima de las previsiones. El informe trimestral queda bien sobre el papel. Y en algún lugar, bajo todo ese papel, bajo todas esas métricas, modelos y resultados del aprendizaje automático, un pueblo que se suponía derrotado, sigue vivo, sigue luchando, sigue negándose a convertirse en lo que los datos decían que ya debería haber sido: una población conquistada. He estado reflexionando sobre esta brecha, entre lo que la máquina dice que está haciendo y lo que realmente está logrando, durante la mayor parte de mi vida adulta. Lo pensé en el Área de la Bahía cuando era adolescente, tratando de entender por qué el país que me acogió había ayudado a armar al país que había bombardeado mi infancia. Pensé en ello en Amazon Web Services, donde la misma infraestructura en la nube con la que vendía contratos de análisis comercial, también alimentaba operaciones de vigilancia sobre las que se suponía que no debía preguntar. Ahora pienso en ello todos los días, cuando miro lo que hemos documentado en ParentsPlea.com: más de 140.000 almas registradas, un perfil tras otro, en todos los años transcurridos desde que empecé a construir un tipo de base de datos diferente al que utilizan los generales. Las bases de datos de los generales cuentan objetivos. Las nuestras cuentan personas. Esa diferencia es el tema de este capítulo. El balance desde 1950 Permítanme comenzar con el hecho más incómodo de la historia militar estadounidense: Estados Unidos no ha ganado una guerra desde 1945. Ni una sola. No, al menos, en ningún sentido significativo de la palabra «ganar», es decir, un resultado duradero y justo que realmente lograra el objetivo declarado y dejara a la región afectada más estable de lo que la encontró. Corea terminó en un armisticio en 1953, no en una victoria. El país quedó dividido en el paralelo 38, y sigue dividido hoy en día. Más de 28.000 soldados estadounidenses siguen estacionados en Corea del Sur más de setenta años después. No hubo victoria. Hubo una tregua: una tregua que requirió una presencia militar permanente para mantenerse. Vietnam terminó en 1975 con helicópteros estadounidenses evacuando al personal de la embajada desde una azotea en Saigón mientras el gobierno de Vietnam del Sur se derrumbaba. Estados Unidos lanzó más de siete millones de toneladas de bombas sobre Vietnam, Laos y Camboya: más que el tonelaje combinado lanzado por todas las partes en la Segunda Guerra Mundial. Solo en Laos, Estados Unidos llevó a cabo 580.000 misiones de bombardeo entre 1964 y 1973, lanzando aproximadamente dos millones de toneladas de municiones sobre un país del tamaño de Utah que nunca había atacado a Estados Unidos. Laos se convirtió en el país más bombardeado per cápita en la historia de la guerra. Ochenta millones de municiones en racimo sin detonar siguen sembrando hoy el campo laosiano, matando y mutilando a agricultores y niños, décadas después de que el último avión

estadounidense emprendiera el regreso a casa. (Fuente: Legacies of War, https://legaciesofwar.org/about-laos/cluster bomb-problem/; Servicio de las Naciones Unidas de Acción contra las Minas, https://www.unmas.org/en/programmes/lao-pdr).

Camboya recibió 2,7 millones de toneladas de bombas estadounidenses durante los años de Nixon y Kissinger, una campaña de bombardeos encubiertos tan intensa e indiscriminadamente que los historiadores han argumentado que contribuyó en forma directa a las condiciones que permitieron el ascenso al poder de los Jemeres Rojos. El bombardeo de Camboya es uno de los grandes crímenes de guerra no reconocidos del siglo XX. Fue posible gracias a los sistemas de puntería más sofisticados disponibles en aquella época. No logró nada, salvo la muerte de entre 50.000 a 150.000 civiles camboyanos y la desestabilización de un país que luego se sumió en uno de los genocidios más devastadores de la historia. (Fuente: Owen y Kiernan, «Bombas Sobre Cambodia», Universidad de Yale, The Walrus, 2006, https://www.yale.edu/cgp/Walrus_CambodiaBombing_OCT06.pdf). Vietnam terminó como terminó porque ninguna cantidad de bombas, ningún índice de bajas, ningún recuento de cadáveres, ningún programa de pacificación, ningún campo de batalla electrónico, ninguna red de vigilancia podía sustituir lo que Estados Unidos nunca tuvo y nunca pudo comprar: la legitimidad a los ojos del pueblo vietnamita. Ho Chi Minh lo dijo claramente, décadas antes de que el último helicóptero abandonara Saigón: «Podéis matar a diez de nuestros hombres por cada uno de los vuestros que matemos. Pero incluso con esas probabilidades, ustedes perderán y nosotros ganaremos». Tenía razón. Los datos estaban equivocados. La voluntad de un pueblo de determinar su propio futuro no es una variable que encaje en un algoritmo de selección de objetivos. La Guerra del Golfo de 1990-1991 fue declarada una victoria. El ejército iraquí fue expulsado de Kuwait. Sadam Husein permaneció en el poder. Las sanciones que siguieron causaron la muerte de unos 500.000 niños iraquíes por enfermedades y desnutrición. Esta cifra se hizo tristemente famosa cuando la entonces secretaria de Estado Madeleine Albright, a quien se le preguntó en una entrevista de la CBS en 1996 si la muerte de medio millón de niños merecían la pena, dijo: «Creemos que el precio merece la pena». (Fuente: CBS News, «60 Minutes», 12 de mayo de 1996; UNICEF, «Encuesta Sobre la Mortalidad Infantil y Materna», 1999). Ese precio no merecía la pena. Y la victoria parcial de 1991 sentó las bases para la catástrofe total de 2003. Irak, por segunda vez: 1,922 billones de dólares gastados. Un país de 30 millones de personas invadido bajo el pretexto de la información de inteligencia fabricada acerca de armas que no existían. Un Estado que funcionaba, por brutal que fuera su gobierno, terminó reducido a escombros, con sus instituciones desmanteladas, su clase profesional dispersa por la diáspora y sus tensiones sectarias avivadas por la eliminación de la única fuerza que las había reprimido. Lo que surgió de las ruinas humeantes de la invasión estadounidense de Irak no fue la democracia. Fue ISIS. (Fuente: Neta Crawford, Proyecto «Costes de la Guerra» de la Universidad de Brown, https://watson.brown.edu/costsofwar/; People's World, «Los Costes de las Guerras Eternas del Imperio Americano», agosto de 2021, https://www.peoplesworld.org/article/the-costs-of-u-s-empires-forever-wars/).

Afganistán: veinte años. 2,3 billones de dólares. Equivalente al mayor gasto militar de la historia de Estados Unidos desde la Segunda Guerra Mundial. Ciento setenta y seis mil personas muertas, entre ellas 47.245 civiles afganos. Cuarenta y seis mil miembros de las fuerzas de

seguridad nacional afganas entrenados y equipados a costa de Estados Unidos. Y luego, en agosto de 2021, los talibanes tomaron Kabul en cuestión de días. Todas y cada una de las principales ciudades cayeron antes incluso de que las tropas estadounidenses hubieran terminado su evacuación. El gobierno que construyeron tras dos décadas de inversión estadounidense se disolvió tan rápidamente que apenas dejó huella. Los talibanes gobiernan ahora el país que gobernaban antes de la llegada de Estados Unidos, y las niñas a las que prohibieron ir a la escuela antes de la llegada de Estados Unidos tienen de nuevo prohibido ir a la escuela. Veinte años, 2,3 billones de dólares. Absolutamente nada para el pueblo afgano, y absolutamente nada para el objetivo declarado de Estados Unidos. (Fuente: Proyecto «Costes de la Guerra» de la Universidad de Brown, «Costes de la guerra contra el terrorismo de 20 años: 8 billones de dólares y 900.000 muertos», septiembre de 2021, https://www.brown.edu/news/2021-09-01/costsofwar). La factura total tras el 11-S, entre Irak, Afganistán, Pakistán, Siria, Libia, Yemen y operaciones relacionadas, asciende a más de 8 billones de dólares según el Proyecto «Costes de la Guerra» de la Universidad de Brown, el recuento independiente más exhaustivo del gasto bélico estadounidense jamás recopilado. Esos ocho billones de dólares incluyen 2,2 billones ya reservados para la atención a los veteranos hasta el año 2050, dinero que seguirá destinándose a los heridos y traumatizados mucho después de que todos los políticos que iniciaron estas guerras hayan fallecido. Incluye a 38 millones de personas desplazadas por las operaciones militares estadounidenses. Incluye a unas 900.000 personas asesinadas directamente por la violencia. (Fuente: Proyecto «Costes de la Guerra», Instituto Watson de Asuntos Internacionales y Públicos, Universidad de Brown, https://costsofwar.watson.brown.edu/findings). Y solo entre 2020 y 2024, las empresas privadas recibieron 2,4 billones de dólares en contratos del Pentágono, lo que supone aproximadamente el 54 % del presupuesto total de gastos discrecionales del Departamento de Defensa. Novecientos cincuenta lobistas trabajaron en nombre de la industria armamentística en Washington durante ese periodo, configurando las políticas y los presupuestos que mantuvieron el flujo de esos contratos. (Fuente: Proyecto «Costes de la Guerra» de la Universidad de Brown, 2024; https://watson.brown.edu/costsofwar/). Este es el balance. Estos son los resultados. Esto es lo que ha producido ocho billones de dólares y la tecnología militar más sofisticada de la historia de la humanidad en setenta y cinco años de intervencionismo estadounidense desde la última guerra que Estados Unidos ganó realmente. La tesis de Assange: las guerras no están pensadas para ganarlas En 2011, en una conversación con el cineasta John Pilger para el documental *The War You Don't See (La Guerra Que No Ves)*, Julian Assange dijo algo que la mayoría de los medios de comunicación informaron brevemente, y luego lo pasaron por alto rápidamente, porque si uno se detiene a reflexionar lo suficiente, resulta muy difícil examinar la historia que acabo de relatar y llegar a una conclusión diferente. «El objetivo», dijo Assange, «es utilizar a Afganistán para blanquear dinero de las bases impositivas de Estados Unidos y Europa a través de Afganistán y devolverlo a manos de una élite de seguridad transnacional. El objetivo es una guerra sin fin, no una guerra exitosa». (Fuente: WikiLeaks, Julian Assange hablando en 2011, publicado por WikiLeaks en X, 18 de agosto de 2021, https://x.com/wikileaks/status/1427929346262642688; YouTube, «Julian Assange sobre la guerra de Afganistán en un vídeo de 2011», https://www.youtube.com/watch?v=_IGU_7alJ80). Quiero ser cauteloso aquí. Assange se refería específicamente a Afganistán. Y la tesis de que las guerras se diseñan deliberadamente para fracasar, de modo que

puedan seguir desviando la riqueza pública hacia manos privadas, es una tesis que invita a la caricatura. Suena a conspiración hasta que se miran las cifras. Entonces suena a contabilidad. Pensemos en lo que ocurrió realmente. Entre 2001 y 2021, Estados Unidos gastó 2,3 billones de dólares en la guerra de Afganistán. Ese dinero no se esfumó. Fue a parar a algún sitio. Fue a parar a Lockheed Martin, que fabricó los aviones. A Raytheon, que fabricó los misiles. A Palantir, que desarrolló los sistemas de selección de objetivos y de inteligencia. A Booz Allen Hamilton, CACI, SAIC y a docenas de otros contratistas que proporcionaron el personal, la logística, la gestión de las bases, la seguridad, el análisis de inteligencia, a los proyectos de reconstrucción que nunca se completaron y los programas de formación que crearon fuerzas policiales que se disolvieron en cuanto se retiró el apoyo estadounidense. El dinero se extrajo de la base impositiva estadounidense y, concretamente, de los préstamos que sustituyeron a esos impuestos, ya que las guerras posteriores al 11-S se libraron casi en su totalidad a crédito, una decisión sin precedentes en la historia, que fluyó hacia las cuentas de un número relativamente pequeño de empresas privadas y sus accionistas. (Fuente: Neta Crawford, Proyecto «Costes de la Guerra», Universidad de Brown; WarCosts.org, «Coste de la Guerra», https://www.warcosts.org/cost-of-war). Neta Crawford, catedrática de Ciencias Políticas en la Universidad de Boston y co-directora del Proyecto Costos de la Guerra, lo expresó con claridad: «Estados Unidos ha librado sus guerras posteriores al 11-S casi en su totalidad con dinero prestado, trasladando los costos a las generaciones futuras. Esta es la primera vez en la historia de Estados Unidos que se recortan los impuestos en tiempos de guerra». Durante la Segunda Guerra Mundial, el tipo impositivo marginal máximo fue del 94 %. Durante la Guerra de Corea, del 92 %. Durante la guerra de Vietnam, del 70 %. Durante la guerra contra el terrorismo, la administración Bush redujo los impuestos al 35 %, y siguió recortándolos. Cada dólar gastado en estas guerras fue prestado. Los contribuyentes estadounidenses y sus hijos pagarán los intereses de ese préstamo durante generaciones. (Fuente: Crawford, citado en WarCosts.org, https://www.warcosts.org/cost-of-war). La conclusión no es una teoría de la conspiración. Es aritmética. Las guerras fracasaron en sus objetivos declarados. Triunfaron, de forma espectacular, en la transferencia de riqueza pública a actores privados. Ya fuera esa transferencia la intención o simplemente la consecuencia, el resultado es el mismo: la élite de seguridad transnacional que describió Assange es más rica de lo que era antes de que comenzara cualquiera de estas guerras, y las poblaciones que se suponía que iban a ser liberadas están, según casi todos los indicadores, en peor situación. Si las guerras pueden iniciarse con mentiras, dijo Assange, en lo que se convirtió quizá en su frase más citada, entonces la paz puede iniciarse con la verdad. Esa frase es la razón por la que los denunciantes como él y Edward Snowden son importantes. Y es la razón por la que los gobiernos que los persiguieron a ambos dedicaron tanta energía a esa persecución. Lo que el algoritmo no puede ver Publiqué un artículo en octubre de 2024, exactamente en el primer aniversario del genocidio en Gaza, en el que intentaba poner nombre a lo que veía al analizar veinticuatro años de IA militar y big data aplicados a los juegos de guerra y a la modelización de conflictos. Había estado utilizando las herramientas de IA a mi alcance para investigar la base de datos de ParentsPlea, con el fin de comprender las lagunas en lo que las máquinas sabían sobre las personas cuyas vidas estaba documentando. Le pedí a ChatGPT, Grok, Bard, a todos ellos, el tipo de datos que ParentsPlea intentaba recopilar: nombres, biografías, testimonios familiares, el registro humano vivido de las personas asesinadas en los conflictos de los últimos veinticinco

años. Ninguna de ellas lo tenía. Tenían estadísticas agregadas. Tenían datos anónimos. Tenían recuentos de víctimas, cronologías de conflictos y análisis geopolíticos. Lo que no tenían era a Alejandro Carranza Medina, de cuarenta años, un pescador de Santa Marta, Colombia, cuya esposa, Katerine Hernández, planteó una pregunta para la que ningún algoritmo ha sido programado para responder: ¿por qué tuvieron que quitarle la vida de esa manera? Los pescadores tienen derecho a vivir. ¿Por qué no se limitaron a detenerlos? Lo que no tenían era a Amal Khalil, de cuarenta y tres años, una periodista de Beirut que murió en un ataque aéreo mientras buscaba refugio en un edificio, porque el primer edificio en el que se refugió también fue alcanzado. Lo que no tenían era a Refaat Alareer, de cuarenta y cuatro años, un poeta y profesor de Gaza que escribió un poema sobre su propia muerte antes de que esta llegara a por él, y que nos dijo exactamente qué hacer con él. Los sistemas de IA en los que los ejércitos del mundo se han gastado cientos de miles de millones de dólares en construir, no pueden salvar ni una sola de estas vidas. Fueron construidos por generales, y los generales ven objetivos, no personas. Fueron construidos por hombres que entienden la violencia, pero no el amor. Fueron construidos partiendo de la suposición de que si se recopilan suficientes datos sobre una población, se puede predecir y controlar el comportamiento de esa población. Y se han equivocado, de forma constante, catastrófica y costosa, durante setenta y cinco años. En la web GoAmour.com, he intentado expresar lo que creo que le falta a la máquina: los principios del amor, la compasión y la dignidad humana que constituyen lo que realmente significa vivir junto a otras personas en esta tierra. No como una abstracción espiritual, sino como una realidad práctica. No se puede entender a un pueblo contando sus bajas. No se puede modelar un movimiento de resistencia rastreando a sus miembros. No se puede bombardear una cultura hasta hacerla desaparecer. Todos los generales que han intentado hacer estas cosas, desde los franceses en Argelia hasta los estadounidenses en Vietnam y los israelíes en Gaza, han descubierto, al final, que no podían. La gente seguía sobreviviendo. La cultura seguía transmitiéndose. Los niños seguían naciendo y se les enseñaba entre los escombros que quedaban, lo que creían sus padres y lo que les habían hecho. Un tonto con una herramienta sigue siendo un tonto. Incluso si la herramienta es un superordenador. Incluso si el tonto lleva una estrella en el hombro. Lo que demostró el bombardeo de Laos Hay una lección en Laos que los artífices de la política militar estadounidense nunca han asimilado adecuadamente, y la razón por la que nunca la han asimilado es que hacerlo requeriría admitir algo que el complejo militar-industria no puede permitirse admitir: que la campaña de bombardeos más intensa de la historia de la guerra no logró nada, salvo la destrucción de la población que la sufrió. Entre 1964 y 1973, Estados Unidos lanzó dos millones de toneladas de municiones sobre Laos: un país que no estaba en guerra con Estados Unidos, cuyo gobierno había pedido a los estadounidenses que se marcharan y cuya población civil no participaba en ninguna actividad militar contra las fuerzas estadounidenses. El bombardeo tenía como objetivo interrumpir las líneas de suministro norvietnamitas a lo largo de la Ruta Ho Chi Minh. No las interrumpió. Los norvietnamitas se adaptaron. Se desplazaban de noche. Se dispersaban. Construyeron rutas alternativas. Enviaban a mujeres y niños a limpiar los cráteres de las bombas para que las líneas de suministro pudieran reabrirse antes del amanecer. La voluntad de un pueblo decidido a alcanzar su objetivo no puede ser frustrada desde 30.000 pies de altura. Los datos no cambian esto. La sofisticación del sistema de selección de objetivos no cambia esto. Lo único que

cambia cuando se hace la tecnología más precisa es que se mata a más personas, con mayor precisión, y más rápido. Hoy en día quedan 80 millones de municiones en racimo sin explotar en suelo laosiano. Matan a una media de cien personas al año: agricultores, niños, personas que no tienen nada que ver con la Ruta Ho Chi Minh de 1968 y que ni siquiera habían nacido cuando se lanzaron las bombas. El gobierno de Estados Unidos gastó 17 millones de dólares al día, todos los días, durante nueve años, bombardeando Laos. Y ha gastado aproximadamente 180 millones de dólares en la retirada de municiones en los cincuenta años transcurridos desde entonces. Hagan ustedes los cálculos. La inversión en destrucción y la inversión en reparación ni siquiera están en el mismo universo. (Fuente: Legacies of War, https://legaciesofwar.org/about-laos/cluster-bomb-problem/; Embajada de EE.UU. en Vientiane, datos de asistencia para la retirada de municiones sin explotar). El propio Vietnam sigue encontrando y retirando municiones sin explotar. Vietnam, Camboya y Laos representan en conjunto una catástrofe humanitaria de posguerra que continúa en tiempo real, cincuenta años después de que las últimas tropas de combate estadounidenses abandonaran las operaciones. Las bombas siguen ahí. La gente sigue adaptándose a ellas. Así es como se ve la supremacía tecnológica desde el terreno. Los datos humanos que el big data no puede recopilar Cuando creé ParentsPlea.com, lo hice porque comprendí algo que los arquitectos de la IA militar nunca han entendido: los datos más importantes sobre un conflicto no son los datos de selección de objetivos. No son la tasa de bajas, el recuento de salidas, el análisis de imágenes satelitales ni la base de datos biométrica de presuntos militantes. Los datos más importantes son los datos humanos: los nombres, las edades, las profesiones, las familias, las cosas que la gente amaba y las cosas que aún planeaban hacer cuando las bombas los alcanzaron. ParentsPlea.com cuenta ahora con más de 140.000 perfiles de este tipo. Cuando empecé a crear la base de datos, pedí a todas las principales plataformas de IA disponibles que me ayudaran a alimentarla con datos de los conflictos de los últimos veinticinco años: Irak, Afganistán, Siria, Libia, Yemen, Gaza, Líbano, Sudán, Somalia, Ucrania y Centroamérica. Ninguna de ellas pudo hacerlo. Ninguna de ellas había correlacionado el registro estadístico de estas guerras con las vidas humanas individuales que las estadísticas representaban. La IA capaz de descubrir de forma autónoma vulnerabilidades de día cero en todos los principales sistemas operativos del planeta, la IA que describí en el capítulo anterior, no puede decirte el nombre de una sola persona asesinada en el bombardeo de Mosul. No puede decirte qué pensaba cocinar Alejandro Carranza Medina para cenar la noche antes de que el ataque aéreo alcanzara su barco. No puede decirte en qué poema estaba trabajando Refaat Alareer la semana antes de morir. No se trata de una limitación técnica que un mejor hardware pueda resolver. Es una limitación filosófica. Los sistemas de IA creados por el complejo militar-industrial se diseñaron para optimizar los objetivos de quienes los encargaron: identificar, seleccionar objetivos y matar de forma más eficiente. No se crearon para comprender. Y no se puede ganar una guerra, no en ningún sentido humano y duradero de la palabra, sin comprender a las personas contra las que se lucha. Todos los generales que han intentado sustituir la comprensión por la potencia de fuego, han acabado aprendiendo esta lección a costa de las personas que pagaron por su guerra. Estados Unidos ha gastado ocho billones de dólares en aprenderlo desde 2001. Laos sigue pagando por el fracaso de Estados Unidos a la hora de aprenderlo en 1973. Las cifras de ParentsPlea cuentan la historia que los generales se niegan a leer Más de 140.000 almas documentadas. Los datos iniciales procedían principalmente de Gaza.

Pero la base de datos ha crecido hasta incluir a víctimas de las principales zonas de conflicto de las que hemos podido obtener información. Cada perfil representa a una familia que envió un relato, o a un periodista que contó uno antes de convertirse él mismo en una estadística. Cada perfil es un acto de rebeldía: un rechazo a permitir que la maquinaria de la guerra moderna reduzca a una persona a una simple cifra. Tres razones por las que la creé. Primero: si alguna vez se celebra un juicio en un tribunal, y creo que lo habrá, los fiscales necesitan identificar a las víctimas, no solo sumar el número de muertos. Los algoritmos de selección de objetivos del capítulo dos de este libro son abstractos hasta que le pones un nombre a la persona a la que apuntaban. Las listas de personas a eliminar son números hasta que encuentras a la familia de una de esas 37.000 personas que Lavender señaló, y les dejas hablar. Segundo: si alguna vez se dictan reparaciones, y la historia sugiere que finalmente se harán, quizá mucho después de que las personas que deberían haberlas pagado hayan muerto, es necesario saber quiénes resultaron perjudicados y qué se les debe. Tercero: porque la paz justa nos exige examinar las muertes que han tenido lugar. Quién está matando. Quién está sufriendo. No en conjunto. Sino por su nombre. Los generales tienen sus bases de datos. Los generales tienen el Proyecto Maven, Lavender, Gospel y Blue Wolf. Cuentan con la infraestructura de selección de objetivos más sofisticada de la historia de la guerra. Disponen de sistemas de IA capaces de identificar un rostro entre la multitud desde un dron que vuela a gran altitud, cotejarlo con una base de datos biométrica y recomendar un ataque en veinte segundos. No pueden decirte que matar a esa persona acabará con la guerra. Porque no acabará con la guerra. Nunca lo ha hecho. Lo que la IA y los generales nunca podrán modelar Comencé mi carrera en el sector tecnológico antes del efecto 2000, el año en que el mundo entero contuvo la respiración esperando que los ordenadores fallaran, y en cambio los ordenadores siguieron funcionando, y todos exhalamos y volvimos a construir máquinas más rápidas. Lo que he observado en el cuarto de siglo transcurrido desde entonces, es la misma dinámica repitiéndose a todas las escalas: las máquinas se vuelven más rápidas, la puntería se vuelve más precisa, los conjuntos de datos se hacen más grandes, y las guerras siguen sin terminar. Ni en victoria. Ni en paz. Terminan en ocupación, retirada o un prolongado estancamiento, y dejan tras de sí los escombros de las vidas que los datos nunca contabilizaron. El fracaso fundamental de la inteligencia artificial como herramienta de guerra no es técnico. Es filosófico. La IA se entrena con datos históricos. Los datos históricos de la guerra son los datos de lo que hicieron los ejércitos y lo que destruyeron. No contienen lo que yo intento incorporar a ParentsPlea: la dimensión humana, el registro biográfico, el testimonio familiar, la exigencia de la madre superviviente que quiere que el mundo comprenda no solo que su hijo murió, sino quién era su hijo, y el por qué su muerte es injusta. No contiene la voluntad de un pueblo de sobrevivir. No contiene el amor que reconstruye la vida después de que las bombas dejan de caer. Lo dije en mi artículo de 2024: si entran datos basura, salen datos basura. La IA que funciona sobre la base de las suposiciones de hombres que solo saben practicar el ahogamiento simulado, la tortura y los asesinatos, por lo tanto producirá recomendaciones de objetivos para más ahogamientos simulados, más tortura, más asesinatos. Se optimizará para lo que sus diseñadores valoran. Y lo que los diseñadores de la IA militar siempre han valorado, no es la paz. Es el dominio. Y el dominio, perseguido más allá de lo razonable, no produce la victoria que prometieron los generales, sino la secuencia exacta de acontecimientos que describe la tabla de resultados anterior: Corea, Vietnam, Irak, Afganistán,

Libia, Siria, Yemen, Gaza. Guerra sin fin. No una guerra exitosa. Assange tenía razón en 2011. El objetivo es una guerra interminable, no una guerra exitosa. Y la tecnología ha hecho que la interminabilidad sea más eficiente, los asesinatos más precisos y los ingresos corporativos más fiables, sin cambiar en ni un solo punto porcentual la única variable que determina el resultado de todo conflicto: la negativa de los pueblos ocupados a aceptar su ocupación para siempre. Esta negativa no es un dato. Es una constante humana. Y ningún algoritmo que haya construido jamás la «mafia de PayPal», ningún sistema de selección de objetivos que haya desplegado jamás la Unidad 8200, ningún contrato de nube que hayan firmado jamás Amazon o Google, ninguno de ellos ha producido una máquina capaz de modelar la dignidad humana. Ninguno de ellos puede calcular el punto en el que un pueblo decide que morir en la resistencia es preferible a vivir en la sumisión. Ninguno de ellos puede predecir el momento en que ese cálculo se inclina: cuando un vendedor de fruta tunecino se inmola y toda una región se levanta, cuando un poeta palestino escribe su propia elegía y la comparten millones de personas que nunca han estado en Gaza, cuando un agricultor vietnamita mira los B-52 en el horizonte y decide que ninguna bomba es lo suficientemente grande como para hacerle olvidar lo que es su tierra. Las máquinas no pueden ver esto. Los generales no pueden ver esto. Y hasta que puedan, cada guerra que inicien terminará de la misma manera que han terminado todas las guerras que han iniciado desde 1945: no con una victoria, sino con un helicóptero en un tejado y una pregunta que ningún dato podrá responder jamás. ¿Qué hacíamos allí? ¿En qué gastamos todo esto? Más de 140.000 nombres en Parents-Plea.com. Cada uno de ellos, una respuesta. --- El historial de fracasos militares estadounidenses, desde Corea hasta Afganistán y Gaza, constituye el contexto en el que deben entenderse los instrumentos jurídicos descritos en el capítulo catorce. La petición a España no se presenta en el vacío. Se presenta con el telón de fondo de ocho décadas de pruebas de que estas guerras nunca se diseñaron para ganarlas, sino solo para librarlas, y de que las empresas tecnológicas descritas en este libro han proporcionado voluntariamente la infraestructura que hace posible la lucha. El capítulo catorce trata de lo que ocurre cuando la documentación del fracaso se convierte en la base de la rendición de cuentas.

CAPÍTULO CATORCE. EL CASO DE ESPAÑA

Por qué llevamos la lucha a Europa, y por qué debes firmar. Todo libro que nombre crímenes tiene la obligación de hacer algo más que nombrarlos. Todo argumento que documente la complicidad tiene la responsabilidad de apuntar hacia la rendición de cuentas. Los capítulos anteriores han construido el caso. Este capítulo te dice qué hacer con él. Quiero ser directo contigo. Hemos documentado, en detalle, cómo Amazon, Google, Microsoft, Oracle y Palantir han proporcionado la columna vertebral tecnológica de un genocidio. Hemos mostrado cómo sus sistemas de IA identifican objetivos de bombardeo, gestionan listas de personas a eliminar, rastrean a familias en sus hogares y crean bases de datos biométricas de una población ocupada. Hemos mostrado cómo sus plataformas de redes sociales silencian las voces de las personas que están siendo asesinadas, y cómo sus operaciones de relaciones públicas manipulan los datos de entrenamiento de la IA para moldear lo que el mundo cree sobre la matanza. Hemos documentado los contratos, las cantidades en dólares, los ejecutivos nombrados y los programas mencionados. Ninguna de esa documentación significa nada a menos que alguien rinda cuentas legalmente por ello. La pregunta que más me han hecho, activistas, periodistas, familiares de los supervivientes, personas que han leído las pruebas y sienten la rabia de no tener dónde dirigirla, es: ¿adónde llevamos esto? ¿A qué tribunal? ¿A qué jurisdicción? ¿Quién tiene el poder y la voluntad de actuar? La respuesta es España. Y la petición ya está en marcha. ¿Por qué no la CPI? ¿Por qué no la CIJ? ¿Por qué no la Unión Europea? Permítanme responder a las objeciones obvias antes de explicar por qué España es el camino correcto, porque estas preguntas merecen respuestas sinceras, no evasivas diplomáticas. La Corte Internacional de Justicia ha presentado cargos. Catorce jueces de países de todo el mundo han considerado plausible que Israel esté cometiendo actos de genocidio en Gaza. Esta conclusión tiene una enorme importancia como declaración jurídica y moral. Pero en los casi dos años transcurridos desde que se abrió el caso, el proceso ha avanzado con una lentitud agonizante. La CIJ opera en un entorno de presión constante por parte de las potencias occidentales, en particular de Estados Unidos, que utiliza su poderío financiero y su influencia diplomática para obstruir, retrasar y neutralizar. Las conclusiones de la Corte son reales. Su aplicación es otra cuestión totalmente distinta. La Corte Penal Internacional se encuentra en una situación aún peor. Estados Unidos no solo se ha negado a adherirse al Estatuto de Roma, sino que además ha sancionado activamente a los miembros de la CPI que intentan investigar los crímenes de guerra estadounidenses. Los jueces que intentan hacer su trabajo se enfrentan a sanciones económicas personales y a prohibiciones de viajar. La CPI ha dictado órdenes de detención contra el primer ministro israelí, Benjamin Netanyahu, y el ministro de Defensa, Yoav Gallant. Esas órdenes existen sobre el papel. La voluntad política para ejecutarlas frente a la oposición estadounidense es otra cuestión totalmente distinta. En cuanto a la Unión Europea y sus veintisiete Estados miembros: la UE es buena imponiendo multas. De miles de millones. A empresas con capitalizaciones bursátiles de billones. Las cuentas no cuadran. Una multa de 5.000 millones de dólares es una partida de gastos trimestral para Amazon. No es

rendición de cuentas. Es una tasa de licencia para seguir gozando de impunidad. Y la UE ni siquiera es capaz de ponerse de acuerdo con una sola voz sobre dónde comprar su energía. No se pone de acuerdo sobre quién debe actuar en Eurovisión: se invita a Israel, pero no a Palestina, a pesar de que Palestina está reconocida por la mayoría de los miembros de la Asamblea General de la ONU y está geográficamente más cerca del continente europeo que muchos de sus participantes. No se trata de observaciones geopolíticas abstractas. Son los fallos estructurales concretos los que han permitido a los ejecutivos tecnológicos financiar, facilitar y lucrarse con un genocidio documentado durante dos años sin una sola consecuencia penal. ¿Por qué España? España es un caso aparte. Y es un caso con precedentes. En 1998, el juez español Baltasar Garzón dictó una orden de detención internacional contra el dictador chileno Augusto Pinochet, responsable de torturas, desapariciones y asesinatos perpetrados bajo un gobierno que Estados Unidos había apoyado activamente. La orden se dictó en virtud del principio de jurisdicción universal: la doctrina jurídica según la cual los delitos más graves contra la humanidad pueden ser juzgados por cualquier Estado, independientemente del lugar donde se hayan cometido o de la nacionalidad de los autores. Pinochet fue detenido en Londres. El caso conmocionó al mundo. Quedó claro que ningún líder, ni ninguna persona que permita que se cometan atrocidades masivas, está fuera del alcance de la justicia internacional simplemente porque su propio país lo proteja. España no ha abandonado esa tradición. Su marco jurídico permite explícitamente el enjuiciamiento de genocidios, crímenes contra la humanidad y crímenes de guerra cometidos en cualquier parte del mundo. La Audiencia Nacional del país tiene la autoridad y la trayectoria institucional para llevar a cabo precisamente este tipo de casos. La conexión jurídica con España no es meramente teórica. El asesinato selectivo por parte del ejército israelí de siete trabajadores humanitarios de World Central Kitchen, entre ellos ciudadanos de la Unión Europea y trabajadores de una organización fundada por el chef de origen español José Andrés, proporciona un vínculo directo y concreto con la jurisdicción española. España tiene un interés nacional en este caso. España tiene legitimación. Y España cuenta con las herramientas. Las cinco empresas tecnológicas que denunciamos —Amazon, Google, Microsoft, Oracle y Palantir— tienen importantes operaciones comerciales, oficinas, clientes y activos en España. Sus ejecutivos viajan a territorio español y transitan por él. Esta presencia otorga a los tribunales españoles la capacidad legal para actuar: solicitar documentos, congelar activos y emitir órdenes de detención que tendrían peso en todos los países miembros de la Interpol y en todos los países que participan en el sistema de la Orden de Detención Europea. Lo que la Fiscalía podría hacer realmente Quiero que comprendas no solo por qué España es el lugar adecuado, sino también lo que podría lograrse realmente con un proceso judicial exitoso. Porque esto no es simbólico. Es estratégico. Si la Fiscalía española abre una investigación formal y presenta cargos, y si se emiten órdenes de detención contra ejecutivos de Amazon, Google, Microsoft, Oracle y Palantir, esas órdenes tendrían consecuencias prácticas inmediatas. Una notificación roja de Interpol, emitida a los 195 países miembros de Interpol, significa que estos ejecutivos podrían ser detenidos en cualquier país participante. Y una orden de detención europea implicaría que, en los 27 Estados miembros de la UE, estas personas podrían ser detenidas y trasladadas a la jurisdicción española. Sus activos depositados en instituciones financieras europeas podrían ser congelados. Los beneficios que estas empresas obtuvieron del dinero manchado de sangre del genocidio, a través de contratos de servicios en la nube, servicios

de IA e infraestructura militar, podrían ser embargados en nombre de las víctimas y sus familias. Piensa en lo que esto significa en la práctica para Andy Jassy, de Amazon; Sundar Pichai, de Google; Safra Catz, de Oracle; Satya Nadella, de Microsoft; Alex Karp y Peter Thiel, de Palantir. Estos hombres que actualmente viajan por el mundo en jets privados a Davos, a conferencias TED, a reuniones gubernamentales, y a clubes náuticos del Mediterráneo, se convertirían en hombres con miedo de cruzar una frontera. Hombres cuyos imperios financieros en Europa se volverían legalmente vulnerables. Hombres que, por primera vez, tendrían algo que perder más allá de no alcanzar los beneficios trimestrales previstos. ¿Los extraditará Estados Unidos? Es casi seguro que no. El actual gobierno estadounidense nunca lo permitiría, e incluso la administración demócrata ha demostrado no tener ningún interés en hacer que su clase multimillonaria rinda cuentas por nada. Pero la extradición no es la única forma de rendir cuentas. La congelación de activos, las restricciones de viaje y el simple peso de una acusación penal pendiente, documentada, pública e innegable, cambian el cálculo de cada miembro del consejo de administración, de cada inversor, de cada fondo de pensiones y de cada gobierno que hace negocios con estas empresas. Cambian el discurso en todos los países que no son Estados Unidos. Dando inicio al proceso de romper el monopolio. Amazon, Google y Microsoft son las tres empresas que controlan de forma abrumadora la mayoría del mercado mundial de la computación en la nube. Un proceso judicial español que culmine con éxito y que dé lugar a la incautación de activos y a restricciones operativas para estas corporaciones en los mercados europeos introduciría, por primera vez, consecuencias estructurales reales para la concentración de poder que ha hecho posible esta complicidad. Lo que exige la petición La petición, dirigida formalmente al Fiscal General de España, a los Juzgados Centrales de Instrucción de la Audiencia Nacional y al gobierno de España, formula cuatro exigencias concretas. Primero: la apertura inmediata de una investigación formal sobre Amazon, Oracle, Palantir, Microsoft y Google por su papel en el suministro de tecnología y servicios que ayudan y favorecen sustancialmente la comisión de crímenes internacionales. Segundo: la investigación de los altos ejecutivos, entre ellos, directores generales, presidentes y miembros del consejo de administración, en virtud de la doctrina de la responsabilidad de mando, por su autorización a sabiendas de estos contratos y por no haber impedido el uso de su tecnología en la comisión de atrocidades. Tercero: la emisión de citaciones para obtener documentos y comunicaciones internas con el fin de determinar el alcance total de lo que estas empresas sabían y cuándo lo sabían. Cuarto: la presentación de cargos por complicidad en genocidio, crímenes contra la humanidad y crímenes de guerra, y la solicitud de órdenes de detención contra sus ejecutivos si las pruebas lo justifican. Esto no es un llamamiento al diálogo. No es un llamamiento a crear un comité de revisión ni a realizar una auditoría de responsabilidad social corporativa. Es un llamamiento a la persecución penal. Es el mismo llamamiento que el mundo debió haber hecho a IBM, Ford y Standard Oil en 1946, y no lo hizo, porque los beneficios y las alianzas políticas prevalecieron sobre la justicia. No podemos permitir que eso vuelva a suceder. Esta petición se ha construido sobre los hombros de los supervivientes. Quiero ser sincero sobre algo. Inicié esta petición no porque creyera que fuera a ser fácil. La inicié porque creo que la alternativa no es no hacer nada y ver cómo se acumula la documentación mientras los ejecutivos cobran sus bonificaciones, es moralmente intolerable para cualquiera que haya pasado años trabajando en esta industria y en su entorno. Construí mi carrera en Silicon Valley. Trabajé en

Amazon Web Services. Sé cómo operan estas empresas, cómo piensan, qué valoran y qué descartan. Sé que el único lenguaje que les llega es el lenguaje de las consecuencias. No la vergüenza: han demostrado que no sienten ninguna. No la presión pública: han demostrado que pueden absorberla. Lo que necesitamos son consecuencias: consecuencias legales, financieras, personales y penales. Esta petición se ha redactado en solidaridad con los padres que han perdido a sus hijos en Gaza. Apoya a los niños que han quedado huérfanos. Apoya a los trabajadores humanitarios asesinados mientras repartían alimentos y a los periodistas asesinados mientras contaban la verdad. Apoya a las familias documentadas en ParentsPlea.com: personas cuyos nombres e historias merecen quedar registrados, y no ser borrados por un encargado del cumplimiento de una plataforma tras una solicitud de retirada del gobierno israelí. Ellos no pueden llevar este caso ante un tribunal español por sí solos. Para eso sirve la petición. Para eso sirve tu firma. En el momento de escribir estas líneas, muchas personas han firmado esta petición. Necesitamos cientos de miles para alcanzar nuestro primer hito, y necesitamos mucho más apoyo para generar el tipo de demanda global documentada que dé a la Fiscalía española la cobertura política necesaria para actuar. Entiendo por qué firmar una petición parece insignificante frente a la magnitud de lo que nos enfrentamos. Entiendo por qué las personas que llevan más de dos años siguiendo este asunto sienten que las firmas no son suficientes. Tienen razón en que las firmas por sí solas no bastan. Pero una petición presentada a un gobierno con una tradición jurídica de jurisdicción universal, respaldada por miles de firmantes de docenas de países, con contratos corporativos documentados, ejecutivos identificados y fuentes verificadas, eso no es un gesto simbólico. Es un registro probatorio. Es el comienzo de un expediente. Es presión ejercida sobre la institución exacta que tiene la autoridad para actuar. Cada persona que lea este libro y no firme esta petición está tomando una decisión. Cada persona que lea este libro y firme la petición, está tomando otra diferente. La petición está disponible en: https://actionnetwork.org/petitions/petition-to-the-spanish-government-and-prosecutors-office investigate-tech-giants-for-complicity-in-genocide-and-war-crimes-in-occupied-palestine Fírmala. Compártela. Pásasela a todas las personas que conozcas que hayan leído estos capítulos y que hayan sentido el peso de lo que contienen. El movimiento necesita números. La justicia española necesita ver que el mundo está mirando y que el mundo exige que se actúe. El arco es largo. Tenemos que doblarlo. Cierro este capítulo tal y como siempre he creído: no con desesperación, sino con la obstinada convicción de que los hombres malvados y sus máquinas no prevalecerán. La historia es larga y está plagada de gente como ellos. Pero la historia no se inclina hacia la justicia por sí sola. Se inclina porque la gente la empuja. Porque se firman peticiones, se presentan demandas, se recurre a los tribunales y así los ejecutivos que se creían intocables descubren, una mañana cualquiera, que un juez de Madrid ha dictado una orden de detención con su nombre. Imagina un mundo donde le quitemos a las corporaciones el control para presionar a favor y llevar a cabo guerras interminables. Un mundo en el que las grandes empresas tecnológicas pierdan su poder monopólico. Un mundo en el que los multimillonarios de Silicon Valley y los ejecutivos genocidas se vean efectivamente inmovilizados, e incapaces de volar en sus aviones privados o navegar en sus yates a cualquier país que respete el estado de derecho. Ese mundo no es una fantasía. Está al alcance con un mecanismo legal, una petición firmada y un fiscal valiente. Firma la petición. Luego pasa la página. --- La petición a España es un instrumento. La revolución regulatoria

europea es otro, y ya está en marcha, independientemente de cualquier petición o campaña de defensa concreta. Lo que documenta el capítulo quince es la convergencia de marcos jurídicos, decisiones gubernamentales y retiradas institucionales de las plataformas estadounidenses que están desmantelando silenciosamente la infraestructura de dependencia que las grandes tecnológicas han tardado treinta años en construir. La responsabilidad penal que exijo en el capítulo catorce y la responsabilidad estructural que la UE está construyendo en el capítulo quince no son estrategias que compitan entre sí. Son la misma estrategia, que opera a diferentes velocidades en distintos terrenos jurídicos.

CAPÍTULO QUINCE. LA REVUELTA EUROPEA

Por qué romper el monopolio de las grandes tecnológicas empieza por la responsabilidad. Algo está sucediendo en Europa que los ejecutivos de Amazon, Google, Microsoft, Oracle y Palantir están observando con mucha atención. Y están preocupados. No por las multas. Pueden absorber las multas. No por las regulaciones. Pueden contratar a grupos de presión y abogados y alargar los plazos de cumplimiento durante años. Están preocupados porque, por primera vez en la historia de la economía digital, los gobiernos no solo están amenazando con consecuencias, sino que también, de forma silenciosa y sistemática, se están alejando. Y cuando los gobiernos se alejan de un monopolio, este comienza a desmoronarse. Este capítulo trata de por qué está ocurriendo esto, hasta dónde ha llegado en el presente y por qué la acción legal que exigimos en España, que incluye la investigación y el enjuiciamiento de los ejecutivos de las grandes tecnológicas por su papel en facilitar el genocidio, no es ajena a esta revuelta europea. Es la chispa que podría encenderla por completo. La confianza ya se ha roto Permítanme comenzar con un hecho que debería helar la sangre en todas las salas de reuniones de Silicon Valley. En abril de 2026, el ministro francés de Cuentas Públicas anunció que Francia trasladaría todos los ordenadores del gobierno, los ordenadores de 2,5 millones de funcionarios, de Microsoft a Linux. La razón aducida no fue el costo, aunque el ahorro es enorme. Fue la soberanía. El ministro francés David Amiel lo dejó claro: Francia «ya no puede aceptar que nuestros datos, nuestra infraestructura y nuestras decisiones estratégicas dependan de soluciones cuyas reglas, precios, evolución y riesgos no controlamos». Afirmó: «La soberanía digital no es opcional». (Fuente: Euronews, «Francia abandonará las plataformas estadounidenses Microsoft Teams y Zoom en favor de una "plataforma soberana"», enero de 2026, https://www.euronews.com/next/2026/01/27/france-to-ditch-us-platforms-microsoft-teams zoom-for-sovereign-platform-amid-security-con). Francia no está sola. El Ministerio de Asuntos Digitales de Dinamarca se ha comprometido a sustituir por completo Microsoft Office 365. El estado alemán de Schleswig-Holstein ha migrado el 80 %, es decir, 30.000 puestos de trabajo, a Linux, lo que le permite ahorrar más de 15 millones de euros al año en derechos de licencia. Austria ha adoptado una carta nacional sobre soberanía digital, respaldada por los 27 Estados miembros de la UE en una cumbre celebrada a finales de 2025. Italia, los Países Bajos y Alemania están migrando conjuntamente más de 800.000 estaciones de trabajo desde las plataformas estadounidenses. (Fuente: Tuta, «Francia abandona Microsoft por Linux para alcanzar la soberanía digital», abril de 2026, https://tuta.com/blog/countries-ditching-microsoft-choosing-linux-digital-sovereignty).

No se trata de gestos simbólicos. Son retiradas estratégicas. Y están impulsadas por algo que va más allá de la política o de las subidas de precios, aunque ambos factores influyen. Están impulsadas por un colapso fundamental de la confianza.

La Ley CLOUD: la letra pequeña que lo cambió todo

El punto de inflexión se produjo cuando los gobiernos europeos se vieron obligados a lidiar con una ley de la que la mayoría de sus ciudadanos nunca había oído hablar. La Ley CLOUD de

Estados Unidos. Aprobada en 2018, otorga a las autoridades estadounidenses la facultad de obligar a las empresas estadounidenses a proporcionar datos almacenados en cualquier parte del mundo, incluidos los servidores ubicados físicamente en Europa, sin pasar por los tribunales europeos, sin notificarlo a los gobiernos europeos y, a menudo, con una orden de confidencialidad que impide a la empresa incluso comunicar al cliente que sus datos han sido incautados.

Lo que esto significa en lenguaje sencillo es lo siguiente: no importa dónde almacenen Microsoft, Amazon o Google tus datos, si el gobierno de Estados Unidos los quiere, puede conseguirlos. Y la empresa tiene prohibido por ley decírtelo.

El propio abogado de Microsoft lo confirmó bajo juramento ante el Senado francés en junio de 2025. Ocasión en que no pudo garantizar que los datos franceses almacenados en los centros de datos europeos de Microsoft estuvieran a salvo del acceso silencioso del gobierno de Estados Unidos (Fuente: Business Tech Africa, «La salida de Microsoft de Francia: pérdida de confianza y redefinición de las fronteras digitales», abril de 2026, https://www.businesstechafrica.co.za/technology/2026/04/22/frances-microsoft-exit-loss-of-trust-and digital-border-redraw/).

Se trata de un problema fundamental de soberanía. Que el histórico Reglamento Europeo de Protección de Datos, el RGPD, lo convierte también en un problema jurídico. La sentencia Schrems II del Tribunal de Justicia de la Unión Europea ya invalidó el acuerdo del Escudo de Privacidad UE-EE.UU. precisamente sobre esta base: que la legislación estadounidense concede a las autoridades de ese país acceso a datos personales europeos de formas incompatibles con los derechos de privacidad europeos, y que los ciudadanos de la UE carecen de recursos judiciales efectivos.

El conflicto es irreconciliable. Según varias autoridades europeas sobre protección de datos, las organizaciones europeas que utilizan plataformas en la nube estadounidense están infringiendo continua y estructuralmente el RGPD, y no por un incidente específico, sino por la arquitectura misma del sistema. No se puede cumplir simultáneamente con el RGPD y garantizar que el gobierno de Estados Unidos no acceda a tus datos si es que tu proveedor de servicios en la nube es una empresa estadounidense. Es imposible. La ley no lo permite.

Y esto es lo que cristalizó el peligro para todos los gobiernos europeos que estaban prestando atención: cuando Estados Unidos sancionó a miembros de la Corte Penal Internacional por investigar crímenes de guerra israelíes, a esas personas sancionadas se les bloqueó el acceso a sus cuentas de correo electrónico de Microsoft y a los servicios web. De la noche a la mañana. De forma remota. Sin previo aviso. Un juez que intentaba hacer su trabajo descubrió que su capacidad para actuar había sido coartada por una decisión tomada en Washington. El ministro de Schleswig-Holstein, en Alemania, dijo directamente: «El caso de la CPI ha demostrado una vez más, por desgracia, lo dependientes que son las instituciones, los gobiernos y las empresas privadas de los sistemas propietarios». (Fuente: The Register, «Europa Considera Seriamente Cortar el Cordón Umbilical Digital de EEUU», diciembre de 2025, https://www.theregister.com/2025/12/22/europe_gets_serious_about_cutting/).

Ese fue el momento en que la soberanía digital dejó de ser teórica.

«El ejecutivo que fue despedido, y por qué eso no cambia nada»

A mediados de mayo de 2026, mientras terminaba este libro, Microsoft anunció discretamente que Alon Haimovich, director general de su filial israelí, dejaría su cargo. Varios otros altos

directivos se marcharon junto con él. El anuncio no incluía ninguna explicación. Ninguna disculpa. Nada sobre lo que había sucedido bajo su mandato.

Déjame contarte lo que sucedió bajo su mandato.

La Unidad 8200 de Israel, es la división de inteligencia militar cuyos antiguos miembros pueblan las empresas de tecnología de vigilancia más poderosas del mundo, cuyas capacidades documenté en el capítulo sobre La bomba de código. Durante años, esta unidad había estado utilizando la plataforma en la nube Azure de Microsoft para almacenar las llamadas telefónicas interceptadas de millones de palestinos en Gaza y Cisjordania. Según una investigación publicada por The Guardian, +972 Magazine y Local Call en agosto de 2025, el sistema se construyó en torno a un objetivo específico y documentado: interceptar y almacenar un millón de llamadas palestinas por hora. No se trataba de un proyecto secundario. No se trataba de un contratista que se había rebelado. Los documentos filtrados revelaron que el propio director ejecutivo de Microsoft, Satya Nadella, fue informado de esto por un comandante de la Unidad 8200 en 2021, y aprobó una partición personalizada y aislada dentro de Azure, creada específicamente con fines de vigilancia militar. (Fuente: Truthout, «Microsoft destituye al director de su filial israelí por el uso de tecnología para espiar a los palestinos», mayo de 2026, https://truthout.org/articles/microsoft-ousts-head-of-israeli-branch-over-use-of-tech-to-spy-on-palestinians/).

En julio de 2025, el sistema albergaba aproximadamente 11.500 terabytes de datos de vigilancia militar israelí, el equivalente a 200 millones de horas de audio grabado almacenados no en Israel, sino en los centros de datos de Microsoft en los Países Bajos e Irlanda. Ambos son jurisdicciones de la Unión Europea. Ambos están sujetos al Reglamento General de Protección de Datos europeo. Por lo tanto, ambos son legalmente responsables ante los tribunales europeos. (Fuente: TechTimes, «Microsoft destituye al director general de Israel después de que Azure almacenara 200 millones de horas de grabaciones de vigilancia de palestinos», mayo de 2026, https://www.techtimes.com/articles/316642/20260514/microsoft-removes-israel-general-manager-after-azure-stored-200-million-hours-palestinian.htm).

Cuando se publicó esa noticia, Microsoft puso en marcha una investigación interna. El equipo de investigación que llegó a Israel semanas más tarde, según el diario financiero israelí Globes, no estaba allí principalmente por motivos morales. Estaban allí porque tenían miedo. Miedo a los reguladores europeos. Miedo a la aplicación del RGPD. Miedo a la exposición legal que suponía el hecho de que los datos de vigilancia recopilados sobre una población civil estuvieran siendo procesados y almacenados en suelo europeo, bajo jurisdicción europea, por una empresa sujeta a la legislación europea. El ministro de Asuntos Exteriores neerlandés declaró públicamente que, si se constataban delitos penales, podrían iniciarse procedimientos judiciales. Amnistía Internacional presentó denuncias formales. Activistas en el campus del centro de datos cerca de Middenmeer, en Holanda Septentrional, instaron a los trabajadores a detener sus actividades hasta que se eliminaran de los servidores los datos de los servicios de inteligencia israelíes. (Fuente: Data Center Dynamics, «Microsoft Abre una Investigación sobre Como la Inteligencia del Ejército Israelí Usa su Nube», marzo de 2026, https://www.datacenterdynamics.com/en/news/microsoft-launches-investigation-into-israeli-military-surveillanc e-agencys-use-of-its-cloud-platform/).

Lo que reveló la investigación de Microsoft, según Globes, no se limitaba a la Unidad 8200. Varias unidades del Ministerio de Defensa israelí habían estado utilizando Azure de formas que

infringen las propias condiciones de servicio de Microsoft. La filial israelí no había sido transparente con la sede central de Microsoft. Fallos de gestión, lagunas en la información interna y un patrón de ocultamiento deliberado habían creado un sistema en el que una gran corporación estadounidense llevaba años procesando la vigilancia masiva de una población civil en servidores europeos, sin una supervisión significativa.

Alon Haimovich fue despedido.

Y quiero ser preciso sobre a lo que me refiero cuando afirmo que esto no cambia nada. La puerta giratoria está abierta Vale la pena preguntarse, cuando se despide a un ejecutivo de Silicon Valley por facilitar la vigilancia de una población civil: ¿adónde va? Va a Amazon Web Services. O a Google Cloud. O a un contratista como DXC Technology, una de las mayores empresas de servicios de TI del mundo, que gestiona contratos de tecnología gubernamental y militar en varias zonas de conflicto. O vuelve al Ministerio de Defensa israelí, o a una de las startups fundadas por antiguos miembros de la Unidad 8200 que durante décadas han sembrado el mercado global de la tecnología de vigilancia. O encuentra un puesto en Palantir, cuyo director ejecutivo, Peter Thiel, no ha ocultado la misión de vigilancia militar de la empresa. La puerta entre Silicon Valley y el aparato de seguridad israelí no se abre hacia un solo lado. Gira en ambas direcciones. El grupo activista No Azure for Apartheid lo dejó claro en su comunicado tras el despido: «Microsoft ha intentado despedirse discretamente del presunto criminal de guerra Alon Haimovich, quien supervisó el desarrollo de herramientas de Azure para el ejército israelí que ayudaron a acelerar el primer genocidio impulsado por la IA». (Fuente: Truthout, mayo de 2026). Pero la declaración también contenía una advertencia que el resto de la industria tecnológica preferiría que no oyeras: Azure no es la única herramienta. «Microsoft tiene presencia en toda la infraestructura militar principal de Israel. Microsoft suministra servicios en la nube, IA, informática, almacenamiento y modelos avanzados de IA al ejército israelí para que los utilicen no solo la Unidad 8200, sino también Mamram, Ofek y unidades específicas navales, aéreas y terrestres del ejército israelí». Haimovich era el ejecutivo designado en una estructura que se extiende por toda la empresa. Su salida es una medida de recursos humanos. No es rendición de cuentas. Y aquí es donde necesito decir algo directamente a los europeos que lean este libro, a cualquiera en los Países Bajos, en Irlanda, en España, cuyo territorio nacional se utilizó para almacenar estos datos de vigilancia sin su conocimiento ni consentimiento. Vuestros gobiernos tienen la jurisdicción legal para investigar esto. No solo a la empresa Microsoft. A las personas que tomaron las decisiones. A los ejecutivos que aprobaron los contratos. A los ingenieros que construyeron la partición aislada. A los directivos que sabían lo que contenían los datos y no dijeron nada a los reguladores europeos. El RGPD no es una multa que se paga y se olvida. Es un marco legal con disposiciones de aplicación penal. La Ley de IA de la UE, que ahora entra en vigor, impone normas de responsabilidad a los sistemas de inteligencia artificial de alto riesgo que van mucho más allá de lo que cualquiera de estas empresas ha revelado voluntariamente. El Tribunal de Justicia de la Unión Europea ya ha dictaminado, en el caso Schrems II, que la arquitectura de la computación en la nube estadounidense es estructuralmente incompatible con los derechos de privacidad europeos. El despido de un ejecutivo no resuelve una incompatibilidad estructural. Solo la disimula. Precisamente por eso la petición en mi sitio web, NoEthicsInBigTech.com, exige una investigación penal y el enjuiciamiento de los ejecutivos responsables, no procesos de recursos

humanos corporativos gestionados por las mismas empresas que cometieron las infracciones. Me han dicho que esta exigencia es poco realista. Que no se puede responsabilizar penalmente a las empresas de esta manera. Que los ejecutivos simplemente negarán tener conocimiento. Díselo al ministro de Asuntos Exteriores neerlandés, quien afirmó que se pueden iniciar procedimientos legales. Díselo a las autoridades europeas de protección de datos que presentaron denuncias formales. Díselo a los dos mil empleados de Microsoft que firmaron la petición interna exigiendo que la empresa dejara de prestar servicios en la nube al ejército israelí, y que vieron cómo sus compañeros eran despedidos por organizar protestas en las instalaciones, mientras que los ejecutivos que construyeron la arquitectura de vigilancia fueron despedidos discretamente con la indemnización que Microsoft consideró adecuada. Las personas que son despedidas por alzar la voz son las que no tenían nada que ver con ello. Las personas que lo construyeron ahora están buscando su próximo destino. Esta asimetría no es una casualidad. Es el sistema funcionando tal y como fue diseñado. Y seguirá funcionando así, en Microsoft, en AWS, en Google Cloud, o en cualquier empresa para la que trabaje Alon Haimovich a continuación, hasta que alguien con una placa y un tribunal lo trate como el delito que es. El problema de Palantir: tus historiales médicos y un genocidio Si la situación de Microsoft ilustra el peligro de la dependencia, la situación de Palantir en el Reino Unido ilustra algo aún más alarmante: lo que ocurre cuando a una empresa, activamente cómplice de atrocidades que están documentadas, se le da acceso a los datos más íntimos de 67 millones de personas. En noviembre de 2023, Palantir, la misma empresa cuyas plataformas de IA para la selección de objetivos operan en Gaza, cuyo director ejecutivo llama a los activistas por la paz «activistas de la guerra» y cuyo cofundador, Peter Thiel, no cree que la democracia y la libertad sean compatibles, se adjudicó un contrato de 330 millones de libras para construir la Plataforma de Datos Federada del NHS, un sistema diseñado para integrar y procesar los historiales médicos de los pacientes de todo el Servicio Nacional de Salud de Inglaterra. (Fuente: The Lowdown NHS, «Palantir, la controversia, los contratos y la campaña contra la FDP», abril de 2026, https://lowdownnhs.info/topics/accountablility/palantir-the controversy-the-contracts-and-the-ca mpaign/). La reacción fue inmediata y generalizada. La Asociación Médica Británica expresó su preocupación. Amnistía Internacional Reino Unido expresó su alarma. Privacy International, el Good Law Project, Corporate Watch y una coalición de médicos, abogados, pacientes y organizaciones de derechos humanos lanzaron la campaña «No a Palantir en el NHS». Su informe, publicado por la organización benéfica de justicia sanitaria Medact, a principios de 2026, planteaba el caso de forma directa: una empresa que proporciona sistemas basados en IA utilizados para atacar a civiles palestinos en Gaza y Cisjordania no tiene por qué gestionar los datos sanitarios sensibles de los pacientes británicos. (Fuente: Medact, «Informe: Preocupaciones relativas a Palantir Technologies y los sistemas de datos del NHS», marzo de 2026, https://www.medact.org/2026/resources/briefings/briefing-palantir-fdp/). ¿Qué hicieron los consorcios hospitalarios británicos? La mayoría de ellos se negaron discretamente. Según las cifras del NHS, menos de una cuarta parte de los 215 consorcios hospitalarios de Inglaterra utilizaban activamente la plataforma de Palantir a finales de 2024. Los Hospitales Universitarios de Leeds comunicaron claramente al NHS de Inglaterra que adoptar las herramientas de Palantir significaría «perder funcionalidad en lugar de ganarla». El sistema sanitario del Gran Mánchester informó de lo mismo. En mayo de 2025, tras una intensa presión y

una inversión de 330 millones de libras, Palantir consiguió que se adhirieran menos de un tercio de los consorcios y, según se informó, los ministros del Reino Unido estaban considerando activar una cláusula de rescisión del contrato para febrero de 2027. (Fuente: Democracy for Sale, «La plataforma de datos del NHS de Palantir rechazada por la mayoría de los hospitales», mayo de 2025, https://democracyforsale.substack.com/p/palantirs-nhs-data-platform-rejected-hospitals).

Así es como se materializa la rendición de cuentas sobre el terreno. No se trata de una sentencia judicial, todavía no. Se trata más bien de un rechazo institucional creciente, impulsado por el historial documentado de lo que es esta empresa y de lo que hace. La revuelta del NHS contra Palantir es un anticipo de lo que puede suceder cuando la gente comprende con quién está haciendo negocios.

El Parlamento Europeo ya lo ha dicho: hay que desmantelarlas El Parlamento Europeo y la Comisión Europea no están esperando a que la fiscalía española comience a desmantelar el control de las grandes tecnológicas sobre el continente. Ya han construido la arquitectura jurídica. Lo que necesitan es la voluntad política para utilizarla plenamente, y un precedente de responsabilidad penal para forzar la cuestión. La Ley de Mercados Digitales, que entró plenamente en vigor en marzo de 2024, designó a seis empresas como «guardianes» —Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft— y les impuso obligaciones estrictas destinadas a prevenir el abuso de posición dominante en el mercado. Se pueden imponer multas de hasta el 10 % de la facturación anual global por incumplimiento. En el caso de los reincidentes, es decir, empresas multadas tres veces en un plazo de cinco años, la Comisión Europea tiene la facultad de imponer medidas correctoras estructurales, incluida la desinversión forzosa: la desintegración de la empresa. (Fuente: Parlamento Europeo, «Explicación de la Ley de Mercados Digitales y la Ley de Servicios Digitales de la UE», https://www.europarl.europa.eu/topics/en/article/20211209STO-19124). En enero de 2025, 18 antiguos jefes de Estado europeos escribieron a la presidenta de la Comisión Europea, Ursula von der Leyen, instando a la Comisión a conseguir precisamente esto: una ruptura estructural de los monopolios de las grandes tecnológicas en toda la economía digital europea. La campaña WeMove Europe recogió cientos de miles de firmas de ciudadanos de todo el continente exigiendo que se rompa el monopolio de Google sobre la publicidad digital y que se tomen medidas más amplias contra el poder sin control de las grandes tecnológicas. Los eurodiputados, entre ellos la alemana Alexandra Geese, una de las principales artífices de la Ley de Servicios Digitales, han advertido públicamente que «Europa corre el riesgo de ser chantajeada tanto por los gigantes tecnológicos estadounidenses como por los chinos». (Fuente: WeMove Europe, «Break Up Big Tech», https://action.wemove.eu/sign/2025-05-breakupbigtech-petition-EN/; The Register, diciembre de 2025). A finales de 2025, la Comisión Europea inició investigaciones formales, y continuó otras ya existentes, sobre Apple, Meta, Google y Microsoft en virtud de la DMA. Las multas impuestas hasta ahora, de 500 millones de euros para Apple y 200 millones de euros para Meta, son consideradas por los críticos como insuficientes, y por su parte los defensores de la aplicación de la ley están presionando para que se intensifiquen. El marco existe. Las investigaciones están en marcha. Lo que falta es un catalizador lo suficientemente potente como para transformar la acción reguladora en consecuencias estructurales. Ese catalizador es el enjuiciamiento penal. Lo que acusación en España puede cambiar Esta es la conexión que los ejecutivos de estas empresas entienden perfectamente, aunque nunca lo digan

públicamente. Una multa regulatoria en virtud de la Ley de Mercados Digitales es un gasto empresarial. Se prevé, se absorbe, se recurre ante los tribunales durante años y, en última instancia, se paga con cargo a un fondo que representa un error de redondeo en una cuenta de resultados anual. Amazon, Google y Microsoft han pagado colectivamente miles de millones en multas europeas y su poder de mercado no ha disminuido ni un solo punto porcentual. Las multas no son un elemento disuasorio. Son el costo de hacer negocios. Un proceso penal es algo totalmente diferente. Un proceso penal en el marco de la jurisdicción universal española, respaldado por una notificación roja de la Interpol y una orden de detención europea, significa que los ejecutivos responsables, y no el departamento jurídico de la empresa, ni tampoco un funcionario responsable del cumplimiento normativo, sino los consejeros delegados y los miembros del consejo de administración que autorizaron estos contratos, pasan a ser personalmente responsables. Sus activos en Europa pueden ser embargados. Sus desplazamientos quedan restringidos. Su capacidad para asistir a Davos, para aceptar títulos honoríficos de universidades europeas, para navegar en sus yates por el Mediterráneo, para pronunciar discursos de apertura en conferencias en París y Berlín, todo ello se vuelve legalmente lejano en el momento en que un juez español emite una orden de detención con su nombre. Y cuando los ejecutivos se convierten en responsables personales, los consejos de administración cambian de comportamiento. Cuando los consejos de administración cambian de comportamiento, se cancelan los contratos. Cuando se cancelan los contratos, la dependencia que ha mantenido a los gobiernos europeos atados a las plataformas estadounidenses durante treinta años comienza a romperse. Hay una razón por la que se estima que el 97 % de la infraestructura en la nube de Europa sigue estando controlada por proveedores no europeos, principalmente estadounidenses, a pesar de años de aplicación del RGPD, a pesar de la DMA, a pesar de las declaraciones políticas sobre soberanía. (Fuente: TechClass, «Soberanía de Datos en 2025: Lo que las empresas de la UE deben saber», https://www.techclass.com/resources/learning-and-development-articles/data-sovereignty-what-i t-means for-european-businesses-in-2025). La razón es que cambiar la infraestructura es caro, disruptivo y políticamente difícil cuando los proveedores establecidos están arraigados en todo, eso hasta que los proveedores establecidos se convierten en acusados penales. Entonces, el cálculo político cambia de la noche a la mañana. Esto no es una especulación. Es la lección que nos enseñan todos los momentos importantes de la historia en materia de responsabilidad corporativa. Las empresas no se reforman por sentimientos de culpa. Se reforman cuando el costo personal de no reformarse supera el costo institucional del cambio. Un proceso penal contra los ejecutivos de Amazon, Google, Microsoft, Oracle y Palantir sería el primer momento en la historia de las grandes tecnológicas en el que ese costo personal se haga real, documentado y exigible más allá de las fronteras. La petición forma parte de esto Cuando inicié esta petición, la cual está dirigida al Fiscal General de España, a los Juzgados Centrales de Instrucción de la Audiencia Nacional y al gobierno de España, lo hice pensando en Gaza. Pensando en los 30.000 niños que han sido asesinados con la ayuda de la infraestructura en la nube y los sistemas de selección de objetivos basados en IA, construidos y operados por empresas estadounidenses. Pensando en los padres documentados en ParentsPlea.com que no tienen dónde llevar su dolor porque todas las instituciones diseñadas para impartir justicia han sido demasiado lentas, han estado sometidas a demasiada presión o han estado demasiado corrompidas por el

poder occidental como para actuar. Pero he llegado a comprender que esta petición también trata de algo más amplio. Se trata de si el continente europeo, que ha creado el marco más sofisticado del mundo en materia de derechos digitales y protección de datos, tendrá el valor de utilizar ese marco con toda su fuerza contra las empresas que lo han violado exhaustivamente. El caso de España es el caso de Europa. El enjuiciamiento de los ejecutivos de las grandes tecnológicas en un tribunal español por su papel en facilitar el genocidio es la señal más clara posible para todos los gobiernos europeos, todos los consorcios hospitalarios, todas las autoridades de protección de datos y todos los reguladores que han estado dudando a la hora de aplicar plenamente la ley: la señal de que estas empresas no son demasiado grandes como para afrontar las consecuencias. Que sus ejecutivos no son demasiado poderosos para ser considerados personalmente responsables. Que el alcance de la legislación europea, extendido al máximo, es mayor que los recursos financieros de cualquier corporación. Francia ya lo ha dicho: la soberanía digital no es opcional. Alemania está actuando. Dinamarca está actuando. La CPI actuó luego de que fuera bloqueado el acceso de su fiscal jefe a su correo electrónico por la presión política estadounidense. El impulso es real y se está acelerando. Lo que se necesita es un hito legal. Un precedente. Un momento en el que un juez español examine el expediente documentado, incluyendo el contrato del Proyecto Nimbus, el sistema de selección de objetivos «Gospel», las plataformas de fusión de datos de Palantir, las listas de personas a eliminar de «Lavender», y concluya que los ejecutivos que autorizaron el uso de estas herramientas al servicio de atrocidades documentadas deben responder por ello ante un tribunal. Ese momento no se produce por sí solo. Se produce porque un número suficiente de personas lo exigió. Se produce porque una petición con suficientes firmas proporcionó a la Fiscalía española la cobertura política para actuar. Ocurre porque la documentación de este libro, y la información en las manos de abogados de derechos humanos y organizaciones de rendición de cuentas de todo el mundo, hace imposible justificar la inacción. La petición está en marcha. Las firmas importan. El caso está construido. Ahora necesita que las personas que entienden lo que está en juego hagan oír su voz en el único lenguaje que los tribunales reconocen: una demanda de justicia documentada, pública y creciente. https://actionnetwork.org/petitions/petition-to-the-spanish-government-and-prosecutors-office investigate-tech-giants-for-complicity-in-genocide-and-war-crimes-in-occupied-palestine Fírmala. Compártela. Dile a todas las personas que conozcas en Europa, en Francia, en Alemania, en España, en el Reino Unido, que esta petición no solo trata sobre Gaza. Se trata de si quieres vivir en un mundo en el que las empresas que custodian sus historiales médicos, sus correos electrónicos, sus datos gubernamentales y la información de tus hijos, sean las mismas que ayudaron a construir una fábrica de asesinatos en masa. Porque ese es el mundo en el que vivimos ahora mismo. Y es el mundo donde tenemos las herramientas, la ley y la obligación moral de cambiar. --- Tanto la revuelta europea como la petición española operan a nivel institucional: tribunales, parlamentos, organismos reguladores. Pero la base sobre la que descansa toda la responsabilidad institucional es algo más básico: un registro. Nombres. Fechas. Causas de muerte. Testimonios de familiares. ParentsPlea.com es ese registro. El capítulo dieciséis trata sobre qué es, cómo se construyó y por qué los poderosos le temen más a una base de datos de los fallecidos que a una multa.

CAPÍTULO DIECISÉIS. LA PETICIÓN DE LOS PADRES

La base de datos de los muertos, y por qué los poderosos la temen. Quiero hablarles del trabajo más importante que he hecho y del que casi nadie ha oído hablar. No son los libros. No es el documental. No es la petición a España, ni los años que pasé en Amazon, ni la organización sin fines de lucro que creé y que luego tuve que cerrar cuando me di cuenta de que el problema era demasiado grande como para que alguna organización sin fines de lucro pudiera solucionarlo. El trabajo más importante es una plataforma que la mayoría de la gente del sector tecnológico descartaría en treinta segundos, porque no produce el crecimiento en el sentido en que Silicon Valley entiende esa palabra. No genera ingresos. No crece a través de bucles virales, efectos de red o embudos de adquisición de pago. Crece, como crece el dolor: una familia tras otra, un nombre tras otro, un testimonio añadido por alguien que necesita que el mundo sepa que la persona que su familia perdió, era una persona. ParentsPlea.com cuenta ahora con más de 140.000 perfiles. Más de 107.000 de esos perfiles documentan muertes causadas por las guerras y conflictos armados de Gaza, del Líbano, de Irán, de Yemen, de Afganistán, de Siria, en países cuyos nombres aparecen en las estadísticas de víctimas que se desplazan por nuestras pantallas y desaparecen. El resto documenta muertes por brutalidad policial, por negligencia corporativa, por injusticia social: las categorías de daño que producen estadísticas pero que rara vez producen rostros. Cada perfil de ParentsPlea tiene un rostro. Esa es la clave. ¿Por qué lo creé? En cada capítulo de este libro, he documentado cómo los poderosos borran las pruebas de lo que su poder produce. Meta elimina las publicaciones. YouTube retira los vídeos. El Departamento de Justicia de Estados Unidos censura los documentos. Las plataformas de las empresas cumplen con las solicitudes de retirada de un gobierno a un ritmo que debería revolverte el estómago. El testimonio desaparece. El archivo se esfuma. El registro no existe. ParentsPlea existe para hacer imposible ese borrado. Pero no en el sentido tecnológico, porque no soy tan ingenuo como para pensar que una plataforma es inalcanzable. Se trata de hacer imposible ese borrado en el sentido moral y legal, que es lo que realmente importa: porque si se documentan 140.000 nombres con fuentes vinculadas a la cobertura mediática y acompañados de testimonios familiares, entonces quienes ordenan el borrado tienen que esforzarse más. Tienen que presentar más solicitudes de retirada. Tienen que justificar más eliminaciones. Tienen que explicar, a más gente, por qué están intentando hacer desaparecer el testimonio de una madre afligida. El valor probatorio de ParentsPlea va más allá de dar testimonio. Lo construí con tres fines jurídicos específicos en mente. Primero: si alguna vez se celebra un juicio en un tribunal, ya sea en España, en la CPI o en cualquier jurisdicción con el valor de actuar, los fiscales deben poder identificar a las víctimas y adjuntar testimonios humanos a la maquinaria que están procesando. Los algoritmos de selección del capítulo dos son abstractos hasta que se le pone un nombre a la persona a la que apuntaban. Las listas de personas a eliminar son solo números hasta que se encuentra a la familia de una de las 37.000 personas señaladas por Lavender y se les deja hablar. ParentsPlea es ese puente: del delito documentado a la víctima

documentada. Segundo: si alguna vez se dictan reparaciones, y la historia sugiere que finalmente se dictarán, aunque sea mucho después de que las personas que debieran pagarlas fallezcan tranquilamente, necesitamos saber quiénes resultaron los perjudicados y qué se les debe. Las reparaciones sin un registro de las personas perjudicadas son solo un número sin destino. ParentsPlea está creando ese registro. Tercero: si alguna vez va a haber un memorial digno de ese nombre, no es un muro de números, ni un comunicado de prensa, ni un minuto de silencio que dure exactamente lo suficiente para que las cámaras lo capturen, necesitamos biografías. Necesitamos el registro completo de quiénes se perdieron, cómo murieron, quiénes quedaron atrás y qué quiere esa familia que el mundo sepa. ParentsPlea está creando ese registro. ¿Qué hace la plataforma? Cada perfil en ParentsPlea se construye para fines tanto probatorios como conmemorativos. Una fotografía, cuando ella esté disponible. Una biografía, y no un resumen, que incluye el tipo de información sobre la vida que hace que una persona sea real para un desconocido: edad, género, religión, estado civil, hijos, ocupación, las cosas que amaban. La causa de la muerte. La supuesta parte responsable, nombrada como corresponde, sin ocultarla tras un lenguaje burocrático. El lugar de la muerte. Con enlaces a artículos de prensa que corroboran el relato. Y la petición de la familia: sus palabras, en su propio lenguaje, dirigidas a quienquiera que aún esté dispuesto a escuchar. La plataforma se basa en una combinación de aportaciones de los usuarios y de investigación seleccionada por personal de apoyo. Mi equipo es pequeño y con pocos recursos. Trabaja en diferentes zonas horarias desde oficinas situadas en las mismas regiones que se documentan, y busca activamente información en fuentes de noticias, artículos publicados e informes de dominio público para crear y verificar perfiles. También hemos desarrollado herramientas para indexar y rastrear la web en busca de información relevante. Tenemos contactos en comunidades de Gaza, Líbano, Irán y otros lugares. No cuentan con los recursos de una redacción. Tienen algo más valioso: la confianza de las familias a las que documentan y la tenacidad para encontrar el registro cuando nadie más lo conserva. También aceptamos envíos directos de familias y testigos. Cuando se envía un perfil, pasa por un proceso de verificación con fuentes de acceso público antes de su publicación. Esta no es una base de datos que yo haya creado sobre los fallecidos. Es una base de datos creada por un equipo dedicado, y por los que están vivos, para honrar a los fallecidos y documentar los crímenes que les causaron la muerte. ¿Por qué los poderosos temen un registro? Hay una pregunta que planteé anteriormente en este libro y a la que quiero volver aquí con más fuerza: ¿por qué hacemos un seguimiento de los delincuentes sexuales, pero no de la clase de Epstein? Los registros de delincuentes sexuales existen porque la sociedad decidió que los delitos cometidos por una determinada categoría de depredadores eran demasiado graves como para dejarlos sin documentar. El público tiene derecho a saber dónde viven estas personas. Las víctimas tienen derecho a ver el nombre de su agresor en una lista. El registro es una forma de rendición de cuentas que no requiere una pena de prisión para funcionar: funciona como documentación social y legal permanente de lo que alguien hizo. Ahora, pregúntate: ¿por qué los ejecutivos de Palantir, Amazon, Google, Microsoft y Oracle, cuyas herramientas han sido documentadas como infraestructura central para el asesinato de decenas de miles de civiles, no se enfrentan a una documentación equivalente? ¿Por qué los nombres de las personas que autorizaron el Proyecto Nimbus, el sistema de selección de objetivos «Gospel» y la lista de personas a eliminar «Lavender» no figuran en un registro público consultable? ¿Por qué los

documentos censurados del Departamento de Justicia estadounidense que protegen a los hombres poderosos que asistieron a los eventos de Jeffrey Epstein siguen bajo censura, años después de su muerte, mientras que los nombres de los delincuentes de bajo nivel relacionados con las drogas se pueden consultar en los registros judiciales públicos? La respuesta es el poder. El registro existe para los indefensos porque los poderosos lo crearon. Los poderosos no tienen un registro equivalente porque no tienen interés en crearlo. ParentsPlea es, entre otras cosas, el comienzo de un registro diferente. No de personas condenadas en los tribunales, porque no somos un tribunal. Sino de los actores corporativos, gubernamentales e institucionales presuntamente responsables de las muertes documentadas en nuestros perfiles. Cada perfil nombra a su presunta parte responsable. Esos nombres se acumulan. Esa acumulación es una forma de documentación pública que ningún acuerdo extrajudicial con cláusula de confidencialidad puede alcanzar. Jeffrey Epstein no actuaba solo. Los hombres cuyos nombres aparecen en los documentos que el Departamento de Justicia ha mantenido bajo secreto durante años cuentan con recursos, abogados y conexiones políticas que los han mantenido ocultos. Las familias de los niños a los que hicieron daño no disponen de esos recursos. Lo que tienen son testimonios que, al documentarse, conservarse y depositarse en un archivo público junto a otros 140.000 testimonios, se convierten en algo más difícil de desestimar que una simple denuncia ante un tribunal que puede retrasarse, apelarse y quedar enterrada durante décadas. Quiero hacer el trabajo de big data de Dios en este mundo: catalogar las fechorías de los demonios para que la justicia que los tribunales y los gobiernos no han logrado impartir a tiempo, pueda al menos exigirse con pruebas. Si quieres llámalo diligencia debida de inspiración divina, llevada a cabo con herramientas de código abierto y con la obstinada negativa a olvidar. Quienes cometen delitos contra niños, mujeres y hombres, contra los miembros más vulnerables de nuestra sociedad, merecen estar en una lista. No ocultos tras un expediente censurado del Departamento de Justicia. Sino visibles. Nombrados. Documentados. Rastreados. Rastreamos a los delincuentes sexuales porque la sociedad decidió que sus delitos eran demasiado graves como para dejarlos sin documentar. Los delitos de la clase de Epstein, contra los niños, contra el Estado de derecho, contra la dignidad básica de seres humanos que no tenían poder para defenderse, no son menos graves. Son más graves, porque el poder que permite esos delitos es también el poder que impide su enjuiciamiento. ParentsPlea.com está trabajando para lograr esa rendición de cuentas. Un perfil tras otro. Un testimonio familiar tras otro. Una fuente de noticias verificada tras otra. Mi trabajo no ha terminado. Es un comienzo. ¿Cómo utilizarlo? Si has perdido a alguien, ya sea por la guerra, por negligencia empresarial, por violencia policial, por cualquiera de las fuerzas descritas en este libro, entra en ParentsPlea.com y envía su historia. El formulario solicita la información indicada anteriormente. No necesitas un abogado para enviarlo. No necesitas demostrar nada más allá de lo que sabes y de lo que se puede vincular a fuentes de acceso público. Tu testimonio es una prueba. La historia de tu familia debe estar en el archivo. Si eres abogado de derechos humanos, periodista, investigador o activista, el archivo es consultable. Los perfiles están documentados. Se nombra a los presuntos responsables. Úsalo. Para eso está. Si eres uno de los ejecutivos nombrados en este libro: tu nombre también está allí. No como perfil de una persona fallecida, sino como presunto responsable vinculado a los perfiles de aquellas personas cuyas muertes, según documentan tus herramientas, has facilitado. Debes saberlo. El archivo crece cada día. Hay un nombre que debo mencionar aquí y que no puede faltar

cuando describo la verdadera finalidad de ParentsPlea.com. Refaat Alareer fue un poeta y profesor palestino que vivió en Gaza. Impartió clases de literatura en la Universidad Islámica de Gaza y editó una colección de relatos cortos titulada Gaza Writes Back. Escribió uno de los poemas más difundidos de toda esta era de conflicto, un poema que tituló «Si debo morir». Lo escribió plenamente consciente de lo que estaba viviendo. Lo escribió como un hombre que comprendía que tal vez no sobreviviría a lo que se avecinaba. Si debo morir, tú debes vivir para contar mi historia, para vender mis cosas y comprar un trozo de tela y unos hilos, para hacer una cometa blanca con una larga cola, de modo que un niño en algún lugar de Gaza, mientras mira fijamente al cielo, esperando a su padre, que se marchó en medio de las llamas y no se despidió de nadie, ni siquiera de su propia carne, ni siquiera de sí mismo, vea la cometa, mi cometa que tú hiciste, volando en lo alto, y piense por un momento que hay un ángel allí trayendo de vuelta el amor. Si debo morir, que traiga esperanza, que sea un cuento. En diciembre de 2023, Refaat Alareer murió en un ataque aéreo israelí en Gaza. Tenía cuarenta y cuatro años. Era profesor, escritor, padre. Había escrito un poema sobre su propia muerte para que quienes vinieran después de él supieran qué hacer con ella. Les dijo que siguieran viviendo. Que contaran la historia. Que hicieran una cometa. Su perfil está en ParentsPlea.com. No está ahí porque nos hubiéramos sentado en la misma habitación con él; no es así. Está ahí porque personas como él, que documentaron lo que estas armas le hacen a un pueblo, están siendo asesinadas antes de que puedan seguir documentándolo. Alguien tiene que mantener el registro cuando los testigos ya no estén. De eso se trata ParentsPlea. De eso se ha tratado siempre. No es una organización mediática. Tampoco una ONG con financiación institucional. Sino un registro. Porque la paz verdadera nos exige examinar las muertes que han tenido lugar: saber quién está matando, quién está sufriendo las amputaciones y los horrores de estas guerras que estamos presenciando. Y porque Refaat Alareer nos dijo qué hacer si él tenía que morir. Debe morir para que nosotros sigamos viviendo. Para que contemos su historia. La estamos contando. Quiero ser explícito sobre la metodología que utilizamos, porque los críticos que no han construido lo que nosotros hemos construido la cuestionarán. Los perfiles de ParentsPlea.com se elaboran a partir de informes publicados de código abierto: el trabajo de periodistas, organizaciones de derechos humanos y fuentes oficiales gubernamentales e institucionales. Verificamos cada perfil con una fuente publicada antes de añadirlo al archivo. Enlazamos directamente con esas fuentes. Nombramos a la supuesta parte responsable. Conservamos el testimonio de la familia cuando existe. Reproducimos el himno nacional del país donde cada persona vivió y murió: un pequeño gesto de dignidad que no cuesta nada, pero que significa mucho. Los periodistas cuyos reportajes sustentan muchos de nuestros perfiles de Gaza y el Líbano, en muchos casos, ya no están vivos. Fueron blanco de ataques. Amal Khalil (ParentsPlea.com/amal-khalil), Ghada Dayekh (ParentsPlea.com/ghada-dayekh) y Suzan Khalil (ParentsPlea.com/suzan-khalil) se encuentran entre los periodistas libaneses cuyas muertes hemos documentado; periodistas presuntamente asesinados por la acción militar israelí mientras hacían exactamente lo que los periodistas deben hacer: dar testimonio en zonas de conflicto. Sus muertes son un ataque no solo contra ellos, sino contra el propio registro: contra las pruebas que sitios como ParentsPlea se dedican a preservar. También documentamos muertes que quedan fuera de los conflictos más cubiertos. Alejandro Carranza Medina era un pescador colombiano, no un periodista, ni un combatiente, ni una persona cuyo nombre aparecía en un informe del

Senado. Tenía cuarenta años. Zarpó de Santa Marta y no regresó porque un ataque aéreo del ejército estadounidense en el Caribe alcanzó la embarcación en la que se encontraba. Esta embarcación, según declaró posteriormente el gobierno colombiano, había sufrido una avería mecánica y se encontraba varada en el mar, sin participar en el tráfico de drogas. Su esposa, Katerine Hernández, presentó una denuncia ante la Comisión Interamericana de Derechos Humanos acusando al gobierno de Estados Unidos de asesinato y ejecución extrajudicial. Preguntó: «¿Por qué le quitaron la vida así? Los pescadores tienen derecho a vivir. ¿Por qué no se limitaron a detenerlos?» (Fuente: ParentsPlea.com/alejandro-carranza). Su pregunta está en ParentsPlea. Su fotografía está en ParentsPlea. Su biografía, su religión, su estado civil, la causa de su muerte y el nombre del gobierno presuntamente responsable: todo está ahí, con fuentes, de libre acceso, libre de citar, libre de usar en cualquier procedimiento legal o periodístico que lo necesite. Sin publicidad. Sin cuotas. Sin patrocinadores corporativos. Esta es la base de datos que temen los poderosos. No porque sea grande, ya que la escala de las atrocidades que documenta, sigue siendo drásticamente más pequeña que la totalidad de hechos graves en el mundo. Sino porque se niega a dejar que el algoritmo borre lo que el arma produjo. Porque sigue preguntando, con la voz de cada familia que confió en ella: ¿por qué? Esa pregunta no tiene fecha de caducidad. El registro tampoco. --- ParentsPlea.com documenta lo que ya ha sucedido. ConflictTour es un intento de cambiar lo que sucederá a continuación, antes de que a la próxima generación de jóvenes se le entregue un folleto de reclutamiento diseñado por un algoritmo que ha estado manipulando sus redes sociales desde que tenían doce años. El capítulo diecisiete es el argumento a favor: no solo contra la maquinaria bélica, sino a favor de la alternativa. Testimonio. Servicio. Un tipo de valentía diferente al que vende la retransmisión de Twitch.

CAPÍTULO DIECISIETE. CONFLICTTOUR

Una alternativa a la guerra, y a la maquinaria que se lucra con ella. Todo lo que hay en este libro, hasta este capítulo, ha sido un argumento sobre lo que está mal. Los sistemas de selección de objetivos. Los contratos de la nube. La puerta giratoria. La censura. La propaganda. El dinero. La inmunidad de las personas que están en la cima de cada uno de estos sistemas frente a cualquier consecuencia de lo que estos sistemas producen. Soy consciente de que un libro que aborda lo profundamente dañado que está el sistema puede dejar al lector sumido en desolación: la desolación de comprender exactamente qué es lo que está mal sin tener una idea clara de qué construir en su lugar. Yo mismo he sentido esa desolación. La sentí en febrero de 2022 cuando cerré la organización sin fines de lucro que cree. La sentí cada vez que veía a una empresa despedir a un ingeniero por tener conciencia y sustituirlo por alguien que no la tenía. La sentí en los días en que el recuento de firmas de la petición avanzaba lentamente y el bombardeo de Gaza no se detenía. Pero nunca la he sentido por mucho tiempo. Porque, mientras documento lo que está mal, siempre estoy también construyendo algo. Este capítulo trata sobre lo último que estoy construyendo. Se llama ConflictTour. Y es, a mi juicio, una de las respuestas más directas disponibles a la pregunta que ha rondado todo este libro: ¿qué construimos en lugar de una máquina de guerra? Cómo ya están reclutando a tus hijos Antes de contarles qué es ConflictTour, quiero explicarles cómo la maquinaria llega primero. En mi documental *Forever Peace Now*, entrevisté a Chris Velázquez, un veterano y jugador empedernido que habló en uno de nuestros eventos de Ética en la Tecnología sobre lo que había presenciado desde dentro del mundo de los videojuegos. Lo que describió no era una conspiración. Era una estrategia, documentada públicamente, que operaba a la vista de todos, dirigida a un objetivo muy específico: los jóvenes que juegan a videojuegos. Según la Entertainment Software Association, en 2020 se estimaba que había 214,4 millones de jugadores de videojuegos en Estados Unidos. Los juegos de disparos eran el tercer género más popular del mercado. Los disparadores en primera persona de temática militar y bélica representaban el 26,9 % de todos los juegos vendidos en Estados Unidos en 2018. Se estima que el 80 % de los jugadores masculinos de entre 18 y 34 años, y el 61 % de los hombres de entre 35 y 54 años, juegan a ser disparadores en primera persona de forma habitual. El ejército de Estados Unidos reconoció estas cifras y actuó en consecuencia. Lanzó sus propios equipos de deportes electrónicos, torneos de videojuegos competitivos, canales de Amazon Twitch y cuentas especializadas en redes sociales, con el fin de publicitarse en plataformas de streaming y reclutar para sus filas desde la comunidad de jugadores. El resultado, tal y como describió Velázquez en el documental: 13.000 nuevos contactos de reclutamiento generados sólo en los primeros seis meses de 2020. Velázquez, hablando tanto como veterano como jugador, lo expresó con claridad: «Como jugador, no quiero que nuestro hobby se utilice para promover otra cosa que no sea la diversión y la comunidad. Como veterano, no quiero ver otra generación de veteranos. No quiero ver a más niños arrastrados a un sistema donde 22 personas al día se quitan la vida». Esta cifra, 22 veteranos que mueren por suicidio cada día, es el número que la retransmisión de reclutamiento

de Amazon en Twitch nunca muestra. Lo que ven los jóvenes jugadores es a personal militar jugando junto a ellos, la simulación de combate presentada de forma glamorosa y sin fricciones, las habilidades que han desarrollado para el entretenimiento presentadas como directamente transferibles al campo de batalla. Lo que no ven son las probabilidades: la probabilidad mucho mayor de que el servicio militar provoque traumas, lesiones, agresiones sexuales u otras consecuencias graves y que alteran la vida, en lugar de una carrera en los deportes electrónicos. El reclutador militar se reúne con un joven antes de que este vea lo que realmente le hace la guerra a las personas a quienes afecta. ConflictTour está diseñado para interrumpir este círculo vicioso. La pregunta que se convirtió en un programa En el capítulo trece, leíste sobre las familias de ParentsPlea.com: los padres que enviaron los perfiles de sus hijos, los hermanos que escribieron los testimonios, los cónyuges que proporcionaron las fotografías. Las historias de ParentsPlea se leen tras la pérdida. Pero nunca dejé de preguntarme: ¿y si alguien las hubiera leído antes de tomar la decisión? ¿Y si, antes de que un joven se alistara en el ejército, pudiera sentarse junto a un refugiado y escuchar cómo suena realmente huir de las bombas? No en una pantalla. No como un clip que el algoritmo muestra entre anuncios. En una habitación. En la mesa de la cocina. De una persona que sobrevivió a algo que la retransmisión de Amazon Twitch del reclutador nunca menciona. ¿Y si, antes de alistarse para servir al complejo militar-industrial de un gobierno, pudieran servir, en cambio, a una familia? ¿Y si pudieran documentar el testimonio de un superviviente de un genocidio, añadiendo ese testimonio a un archivo legal, comprendiendo que podría utilizarse en un futuro juicio, sientiendo en lo más profundo de su ser que este sobreviviente no es un enemigo, sino un ser humano exactamente igual que ellos, y luego decidir, desde esa posición de conocimiento, a qué tipo de servicio le gustaría dedicar su vida? Esta pregunta me llevó a ConflictTour. ¿Qué es? ConflictTour está concebido como un programa estructurado de servicio humanitario de seis meses de duración, una alternativa al alistamiento militar. No es un año sabático. No es turismo. No es un programa de aventura para personas que quieren tener una historia que contar en las cenas. Es un trabajo intensivo, exigente y emocionalmente costoso que requiere el mismo valor que el servicio militar y produce algo completamente diferente. El programa está diseñado para desarrollarse en dos vías. La Vía de Servicio Local mantiene a los participantes en su país de origen, trabajando junto a familias de refugiados y comunidades afectadas por la guerra, personas que llegaron sin nada y se enfrentan a un sistema gubernamental que no fue diseñado pensando en ellas. Los participantes de la Vía Local ayudan a las familias a solicitar asilo y prestaciones, proporcionan apoyo de traducción en citas médicas, documentan historias para la defensa legal, conectan a las familias con recursos comunitarios y construyen las relaciones que reducen el aislamiento que produce el desplazamiento. Esta vía se pondrá en marcha en enero de 2027. La Vía Internacional envía a los participantes a antiguas zonas de guerra que actualmente se consideran seguras según las advertencias de viaje internacionales, donde trabajan junto a organizaciones locales asociadas para documentar el impacto de la guerra en la infraestructura civil, entrevistar a supervivientes para archivos legales e históricos, y ayudar en la reconstrucción liderada por la comunidad. Se espera que esta vía se ponga en marcha en septiembre de 2027. Ambas vías comienzan con dos meses de formación estructurada: comunicación sensible al trauma, fundamentos de la documentación jurídica, orientación sobre recursos para refugiados, habilidades lingüísticas interculturales y, fundamentalmente,

autocuidado y preparación para el trauma vicario. Este último elemento es más importante de lo que la mayoría de los programas reconocen. El trabajo de acompañar el duelo cambia a una persona. La formación prepara a los participantes para ese cambio, en lugar de fingir que no va a ocurrir. Al finalizar, los participantes reciben la Certificación ConflictTour en Testimonio Humanitario: una formación verificable sobre la comunicación basada en el trauma, la defensa de los refugiados y la documentación ética. Pero más allá de la credencial, llevan consigo la experiencia vivida de haber estado al lado de las personas en sus momentos más difíciles. Eso no es algo que una línea en un currículum pueda plasmar por completo. Sin embargo, es algo que cambia la forma en que una persona vota, cómo habla de la guerra, cómo procesa las noticias y qué está dispuesta a exigir a quienes gobiernan. Por qué esta es la respuesta al capítulo seis En el capítulo seis de este libro, documenté la conferencia sobre resultados de abril de 2026 de Jim Taiclet, en la que el director ejecutivo de Lockheed Martin calificó el momento geopolítico actual como una «oportunidad de oro» para la industria de la defensa. Documenté el presupuesto del Pentágono de 901.000 millones de dólares para el año fiscal 2026 y los 1,5 billones de dólares propuestos para el año fiscal 2027. Documenté los contratos sin licitación, el chantaje de la OTAN y la fusión de Silicon Valley con el complejo militar-industrial. ConflictTour es mi respuesta directa a todo esto: no es una respuesta política, ni una petición, ni un argumento jurídico, sino estructural. El complejo industrial-militar depende de un suministro de jóvenes dispuestos a alistarse. Ese suministro no es ilimitado. Se genera a partir de un conjunto específico de condiciones: la precariedad económica, la glorificación cultural del servicio militar, las retransmisiones de Amazon Twitch que describió Chris Velázquez, los canales de videojuegos FPS que el Ejército de los Estados Unidos construyó deliberadamente, y la ausencia de cualquier alternativa visible que ofrezca el mismo sentido de propósito, servicio y pertenencia que promete el reclutador. ConflictTour se propone llenar ese vacío. Un joven que ha pasado seis meses ayudando a una madre siria a orientarse en el sistema de asilo de su propia ciudad, que la ha oído describir lo que dejó atrás, que ha visto a sus hijos aprender a confiar de nuevo en los adultos a pesar de haber presenciado cosas que ningún adulto debiera permitir que presencie un niño, ese joven toma una decisión diferente en la oficina de reclutamiento que alguien que no ha tenido esa experiencia. No necesariamente la misma decisión. Pero sí una diferente. Una decisión informada. Para eso se creó ConflictTour. El compromiso Todos los participantes de ConflictTour asumen un compromiso antes de comenzar. Este abarca cinco aspectos. Se comprometen a desempeñar su papel como testigos y servidores; no como combatientes, ni como turistas. Aceptan explícitamente no participar en el servicio militar ni tomar las armas durante su participación. Reconocen con lucidez los riesgos del Itinerario Internacional: ConflictTour no ofrece seguro, evacuación médica ni servicios de rescate. Los participantes son adultos que asumen toda la responsabilidad de su propia seguridad. No se trata de una exención de responsabilidad escondida en la letra pequeña. Es una declaración directa y honesta de que este trabajo es serio y de que la organización respeta lo suficiente a los participantes como para decirles la verdad sobre lo que cuesta. Se comprometen a tratar a cada refugiado, a cada sobreviviente y miembro de la comunidad con el que se encuentren con dignidad y respeto, entendiendo que sus historias no son contenido para ser consumido, sino testimonios sagrados que deben ser honrados. Entienden que su trabajo puede incluir la documentación de testimonios con fines legales, contribuyendo

directamente al tipo de archivo probatorio que ParentsPlea ha estado construyendo y que los futuros procesos judiciales necesitarán. Y comprenden las consecuencias de incumplir cualquiera de estas condiciones: expulsión inmediata, sin derecho a reembolso. El compromiso no es burocrático. Es la base del trabajo. Un participante de ConflictTour que lo incumpla no solo estará infringiendo las condiciones del servicio. Habrá traicionado a las familias que confiaron en él lo suficiente como para dejarlo entrar. Lo que aportan los socios ConflictTour colaborará con organizaciones asociadas que llevan décadas realizando este trabajo. Terapeutas especializados en traumas que comprenden el efecto que tiene escuchar a una persona tras meses de exposición continuada al dolor. ONGs profundamente enraizadas en las comunidades a las que prestan servicio, es decir, el tipo de organizaciones que saben qué familias están preparadas para compartir sus historias y cuáles no, qué intérpretes son de confianza y cuáles no, qué preguntas causan daño y cuáles crean un espacio para la sanación. Estos socios no son agencias de viajes. No son servicios de evacuación. No gestionan la logística ni las necesidades personales de los participantes. Hacen algo más valioso: abren las puertas de comunidades a las que los visitantes internacionales no pueden acceder por sí solos. Proporcionan el contexto que convierte la documentación en comprensión. Comparten una experiencia que les ha llevado años de presencia sobre el terreno para adquirir. A cambio, ConflictTour les pide que acepten a participantes que lleguen preparados y sean autosuficientes, personas que han completado la formación, leído las declaraciones de riesgo y se han presentado dispuestas a servir en lugar de ser gestionadas. La relación es de respeto mutuo entre organizaciones que realizan diferentes partes del mismo trabajo. ConflictTour forma a los testigos. Los socios los colocan donde el testimonio es más importante. Esto es tecnología al servicio de la humanidad En el capítulo uno, sostuve que la IA puede utilizarse para un bien extraordinario: para la medicina, para el clima, para dar testimonio de crímenes de guerra. Sostuve que la cuestión no se trata de si la tecnología es buena o mala, sino de quién la construye y con qué propósito. La idea de ConflictTour se basa en ese mismo argumento, extendido al diseño organizativo. El plan de formación utiliza herramientas de documentación digital, incluidas plataformas como ParentsPlea, para enseñar a los participantes cómo funciona el archivo ético. El programa utiliza la tecnología para emparejar a los participantes con organizaciones asociadas a través de zonas horarias y geográficas. La formación en documentación legal enseña a los participantes a utilizar herramientas de inteligencia de código abierto y archivos digitales de manera que sirvan a los derechos humanos en lugar de objetivos militares. Esta es tecnología al servicio de la humanidad. No la tecnología de Palantir, que crea IA para localizar y matar a personas. La tecnología de ConflictTour forma a personas para localizar y documentar las historias de aquellas personas a las que la tecnología de Palantir mata. Ese contraste no es casual. Es precisamente el objetivo. Una invitación ConflictTour es nuevo. Lo ha creado una persona que cree que la alternativa al complejo militar-industrial no es la pasividad, sino un tipo diferente de servicio, construido con intención, basado en el testimonio y ofrecido a los jóvenes antes de que la retransmisión de Twitch del reclutador llegue primero. Si eres un joven que está leyendo este libro: la Vía Local se pone en marcha en enero de 2027. No necesitas viajar a una zona de guerra para hacer este trabajo. Puedes hacerlo en la ciudad donde ya vives, junto a familias que llegaron allí sin nada y que necesitan a alguien que esté a su lado. Si eres un padre o una madre leyendo este libro: esta es la alternativa que has estado buscando. No está exenta de riesgos, porque el servicio

honesto rara vez lo está. Pero los riesgos están documentados, la formación es real y el trabajo es significativo de una forma que el discurso del reclutador nunca te contará. Si eres una ONG, un terapeuta especializado en traumas, una organización financiadora o un proveedor de servicios y quieres colaborar con nosotros en este proyecto, el formulario de solicitud de colaboración se encuentra en ConflictTour.com. Necesitamos socios sobre el terreno, profesionales especializados en traumas y organizaciones dispuestas a ayudar a formar a la próxima generación de testigos humanitarios. Si eres uno de los ejecutivos mencionados en este libro, como los arquitectos de Gospel, Lavender, Project Maven y Project Nimbus, este capítulo también es para ti. No porque espere que cambies. Llevo suficiente tiempo en este sector como para saber que no es así. Sino porque quiero que comprendan que, por cada sistema que construyen para hacer la guerra más eficiente, hay personas construyendo sistemas para hacer la paz más visible. Ustedes tienen más dinero. Nosotros tenemos más tiempo. La historia sugiere que eso es importante. Lo que ConflictTour no puede hacer, y lo que sí puede Quiero ser honesto sobre los límites de lo que estoy construyendo. ConflictTour no puede detener una guerra. No puede aprobar una ley. No puede congelar activos, emitir una orden de detención ni obligar a un multimillonario a responder por lo qué los algoritmos de selección de objetivos de su empresa le hicieron a una familia en Rafah. De estos instrumentos tratan los capítulos anteriores de este libro. Lo que ConflictTour puede hacer es cambiar a quiénes participan en el debate sobre la guerra, y qué cosas saben cuando llega el momento de debatir. Una generación de jóvenes que se ha sentado con sobrevivientes, que ha documentado testimonios, que ha navegado por los sistemas de asilo junto a familias refugiadas y ha soportado el peso de presenciar consecuencias reales: esa generación vota de otra manera. Aboga de otra manera. Exige de otra manera. Se niega de otra manera. Y no se alista basándose en una retransmisión de Twitch. El complejo militar-industrial llama al genocidio una oportunidad de oro. ConflictTour lo llama una razón para acudir con un cuaderno en lugar de un arma y asegurarse de que se mantenga el registro. Eso es servicio. Eso es valentía. Así es como se ve la paz en acción. Sé testigo. Sirve. Elige la paz.

ConflictTour.com --- La documentación sobre ParentsPlea, la petición a España, la revuelta regulatoria europea, la propuesta de ConflictTour... no son una sola campaña. Son expresiones de una única convicción: que los hombres malvados y sus máquinas no prevalecen, pero tampoco se detienen por sí solos, y que el arco de la historia solo se inclina porque la gente lo empuja. El capítulo dieciocho trata de cómo yo empujo el mío, y de cómo te pido que empujes el tuyo.

CAPÍTULO DIECIOCHO. VIVIR EN PAZ, NO SOLO DESCANSAR EN PAZ

ForeverPeaceNow.com, GoAmour.com, ParentsPlea.com y el Argumento por el Amor.

Quiero cerrar este libro de la misma forma en que he intentado vivir mi defensa: no con desolación, ni con falso consuelo, sino con algo más sólido que ambos: con esperanza documentada. El tipo de esperanza que tiene pruebas que la respaldan. Aquella esperanza que no es un sentimiento, sino una estructura. La que te da algo que hacer cuando cierras este libro. Has pasado diecisiete capítulos dentro de una máquina. Dentro de sus contratos y sus listas de personas a eliminar y sus bases de datos biométricas y su puerta giratoria y su silenciamiento de las voces palestinas y su explotación de los trabajadores en Nairobi y sus lesiones en los almacenes de Nueva Jersey. ¿Has leído lo que Rumi, hace ocho siglos, describió mejor de lo que ha logrado ningún sociólogo moderno? La ciudad de Saba, donde la riqueza se ha amontonado tanto que nadie necesita nada, y como nadie necesita nada, nadie agradece nada, y como nadie agradece nada, nadie se pregunta por el mundo invisible, y la gente engorda y se aburre y se vuelve ciega ante lo que está mal, y sorda ante cualquiera que lo señale. La ciudad de Saba no es una fábula. Es Sand Hill Road. Es el campus de Palantir Technologies. Es la sala de reuniones donde Jim Taiclet calificó el genocidio de oportunidad de oro y lo dijo como un cumplido. Es la cultura que producen hombres que llaman a la empatía «debilidad de la civilización», mientras construyen sistemas de IA que matan a niños en sus hogares. Los racimos de uvas cuelgan tan bajos en esas oficinas que rozan los rostros de los habitantes de camino a la reunión sobre resultados. Y la gente de Saba se aburre con solo mencionar la profecía. La cura de Rumi para la ciudad de Saba no es una propuesta política. No es una petición. No es un proceso judicial, aunque necesitamos las tres cosas. Su cura es ésta: *Siéntate en silencio y escucha una voz que dirá: «Sé más silencioso. Abandona el habla y renuncia a tus puestos de poder. Renuncia al dinero excesivo. Dirígete hacia los maestros y los profetas que no viven en Saba»*. Ese es el comienzo de una respuesta. No es la respuesta completa. Este libro tiene diecisiete capítulos tomando en cuenta las otras partes. Pero es ahí donde empieza la respuesta: en el individuo, en el momento de silencio, en el reconocimiento de que la enfermedad de la riqueza excesiva no se cura reorganizando las instituciones de los ricos. Se cura con la voluntad de los individuos, dentro y fuera de la máquina, de escuchar la voz que dice: basta. Sé más silencioso. Dirígete hacia algo distinto a esto. Este capítulo trata sobre ese giro. La pregunta que le hice a la inteligencia artificial Hace algún tiempo, antes de que existiera este libro, antes de la petición a España, antes de que documentáramos 140.000 almas en ParentsPlea, le estaba dando vueltas a la idea de GoAmour.com. Hice lo que se esperaría de alguien que pasó treinta años en el mundo de la tecnología. Abrí la última versión de ChatGPT 4.0 y le hice una pregunta que ningún contratista militar le ha hecho jamás a su IA. Le pedí que presentara el mejor argumento a favor del amor. No el mejor argumento a favor de un sistema de selección de objetivos. No el mejor argumento a favor de un contrato sin licitación, una migración a la nube o una adquisición en el sector de la defensa. Le pedí que defendiera el amor: entre las personas, entre

las personas y el planeta, entre las personas y la naturaleza, entre las personas y sus animales, e incluso entre los propios sistemas de IA. Y respondió. De forma coherente, exhaustiva y sin vacilar. Argumentó que el amor por las personas fomenta la empatía, la comprensión y la cooperación, esenciales para abordar los retos globales. Que el amor entre las personas y el planeta motiva las prácticas sostenibles y la conservación. Que el amor entre la IA y las personas, alimentado por consideraciones éticas, garantiza que la IA sirva a los mejores intereses de la humanidad. Desarrolló el argumento a lo largo de siete categorías y concluyó que: el amor actúa como una fuerza poderosa que une, nutre y sostiene. Y luego dijo, en los términos más sencillos, que sí, que vale la pena salvar el amor. Lo que me llamó la atención de esa conversación, al reflexionar sobre ella después, no fue que la IA pudiera describir el amor. Eso ya me lo esperaba. Todo lo que Erich Fromm escribió al respecto está en los datos de entrenamiento. Todo lo que Rumi dijo al respecto está ahí. Lo que me llamó la atención fue la asimetría. La misma arquitectura que podía articular el amor de forma tan completa era la misma arquitectura con la que OpenAI había eliminado discretamente la prohibición del uso militar de sus condiciones de servicio. La misma empresa que cuando se le pidió que defendiera el amor produjo algo luminoso, también había puesto sus herramientas a disposición de operaciones de vigilancia con drones y de selección de objetivos. La IA refleja la pregunta. La pregunta refleja a quien la formula. Quien la formula revela sus valores. Cuando pedí un argumento a favor del amor, lo obtuve. Cuando Palantir pidió a su IA un sistema de selección de objetivos, lo obtuvo. La inteligencia es la misma. Lo que difiere es el ser humano que la posee y para qué ha decidido utilizarla. Comparto esto porque creo que es lo más importante que he aprendido tras muchos años de escribir sobre lo que la tecnología le hace a la humanidad. El problema no es que la IA no pueda entender el amor. Puede hacerlo. El problema es que las personas que controlan los sistemas de IA más potentes no se lo han pedido. Eso es una elección. Y las elecciones se pueden cambiar. (Fuente: GoAmour.com, «Saving Love: A Conversation with Artificial Intelligence», https://goamour.com/saving-love-a-conversation-with-artificial-intelligence/) Lo que Erich Fromm entendió y Silicon Valley nunca ha entendido En su libro de 1956 *El arte de amar*, el psicólogo y filósofo Erich Fromm planteó un argumento que era radical entonces y sigue siéndolo ahora: el amor no es un sentimiento. Es una práctica. Es un arte, algo que requiere conocimiento, dedicación y disciplina, del mismo modo que la pintura requiere conocimiento, dedicación y disciplina. Y, como cualquier arte, se puede practicar bien o mal, aprender o evitar, profundizar a lo largo de toda una vida o dejar que se atrofie. Fromm identificó cuatro elementos del amor maduro: el cuidado, la responsabilidad, el respeto y el conocimiento. Estos cuatro elementos, argumentaba, deben estar presentes juntos, ni uno puede estar solo, ni tres sin el cuarto. El cuidado es la preocupación activa por la vida y el crecimiento de la persona o cosa que amas. La responsabilidad no es un deber impuesto desde fuera, sino una respuesta voluntaria a las necesidades de otra persona. El respeto es la capacidad de ver a una persona tal y como es en realidad, no como necesitas que sea, ni como la proyectas, y de permitirle crecer a su manera, por sus propias razones. Y el conocimiento es la voluntad de ir más allá de la superficie: comprender quién es realmente una persona en su esencia, no solo la historia que te has contado a ti mismo sobre ella. Lo que Fromm describe, el cuidado, la responsabilidad, el respeto y el conocimiento, es exactamente lo contrario de lo que exige el modelo de negocio de Silicon Valley. La economía de la atención se basa en la destrucción sistemática de cada uno de estos

cuatro elementos. El cuidado se sustituye por la captación de la atención: no se trata de si el contenido te beneficia, sino de si te mantiene navegando. La responsabilidad se sustituye por la gestión del riesgo: no es una respuesta voluntaria a las necesidades de los demás, sino un cálculo jurídico sobre aquello de lo que la empresa puede evitar que se le haga responsable. El respeto se sustituye por la segmentación: no se ve a la persona tal y como es, sino que se la reduce a un perfil de comportamiento que predice en qué anuncio hará clic. Y el conocimiento, un conocimiento profundo, paciente y costoso del otro, se sustituye por la extracción de datos, que es lo contrario del conocimiento: confunde la medición del comportamiento de una persona con la comprensión de su alma. La ciudad de Saba no puede entender el amor porque el amor requiere reconocer la carencia, reconocer que hay algo que no tienes, algo que necesitas, algo por lo que vale la pena luchar. La gente de Saba no tiene carencias. El algoritmo no tiene carencias. El sistema de segmentación no tiene carencias. Tiene 37.000 nombres y una tasa de error del 10 % que considera aceptable. El hombre que entendió esto, y que creó una plataforma para argumentar en su contra, no era un filósofo. Era un tecnólogo iraní-estadounidense que solía vender servicios de coubicación en Exodus, gestionaba alianzas en AWS y terminó saliendo de los hospitales con un bastón. Tomó los cuatro elementos de Fromm, el cuidado, la responsabilidad, el respeto y el conocimiento, y los integró en un marco de diez puntos que publicó en una página web y la llamó GoAmour. Los principios de GoAmour: un marco para lo que viene después Permítanme repasar estos principios. No porque sean nuevos, la mayoría son más antiguos que el propio lenguaje, sino porque el mero hecho de nombrarlos en el contexto de este libro es, en sí mismo, una declaración de lo que ha significado todo este esfuerzo. El primer principio es la Regla de Oro, con énfasis en la palabra *«otros»*. Trata a los demás como te gustaría que te trataran a ti mismo. El énfasis es importante porque la Regla de Oro suele recitarse como una restricción: no hagas a los demás lo que no querrías que te hicieran a ti. Eso es pasivo. La versión de GoAmour es activa: haz *a* los demás. Toma la iniciativa. Da el primer paso hacia la dignidad y el bienestar de la otra persona, antes de que se lo haya ganado, antes de que lo haya pedido, antes de que sepas si te corresponderá. El segundo principio es la libertad de elegir tus afiliaciones, ideologías, organizaciones y creencias sin prejuicios ni juicios. Esto incluye la inteligencia artificial. Incluye las plataformas que este libro ha criticado. La libertad de elegir no es la libertad de elegir correctamente: es la libertad de elegir, y punto, y de ser respetado por la elección que has hecho. La economía de la vigilancia viola este principio a todos los niveles. Cataloga tus elecciones para predecirlas y, en última instancia, moldearlas. Una persona cuyas elecciones son catalogadas por un algoritmo diseñado para que siga eligiendo lo mismo, no es libre en ningún sentido significativo de la palabra. El tercer principio es el derecho a rescindir. A cancelar la suscripción. A abandonar la plataforma. A alejarse de la institución, la ideología, el sistema de IA que ya no sirve a tus valores. Sin obligaciones contractuales a largo plazo. Sin que te sigan. Sin que se retengan tus datos una vez que hayas decidido que has terminado. Este es un principio tan básico que no debería ser necesario mencionarlo, pero en un mundo en el que Facebook retiene los datos de los usuarios que han eliminado sus cuentas, en el que los trabajadores de los almacenes de Amazon deben entregar sus cuerpos como garantía de la productividad que exige el algoritmo, en el que los términos de servicio que rigen tu vida digital alcanzan las cuarenta páginas de lenguaje legalmente vinculante que nadie lee, en un mundo así, el derecho a rescindir es un acto

radical. El cuarto principio es directamente de Fromm: amar con conocimiento, respeto, cuidado y responsabilidad. Amar no de forma sentimental, ni posesiva, ni como una adquisición o una actuación, sino como una práctica. Como el trabajo diario de atender a otro ser. Como la voluntad de dejarse transformar por lo que ves en ellos. El quinto principio es la preservación y la inviolabilidad de los derechos humanos y los derechos digitales, para nosotros mismos y para los demás. No los derechos humanos como tema de conversación en una página de valores corporativos. No los derechos digitales como una cláusula en una política de privacidad que nadie lee. Los derechos humanos y los derechos digitales como cosas cuya defensa realmente tiene un costo: que a veces te cuesta el trabajo, a veces la seguridad y a veces la relación con personas que prefieren que te calles. Merecen la pena esos costos. Todo lo que hay en este libro ha sido un intento de defender esta idea. El sexto principio es la voluntad de apoyar a las organizaciones e ideologías que promueven la vida en sus múltiples formas. No solo la vida humana. No solo las vidas de las personas que se parecen a ti y creen lo mismo que tú. La vida en sus múltiples formas: el niño de Gaza, el pescador de Colombia, el moderador de contenidos de Nairobi, la ballena, el bosque, el acuífero. Todo ello merece la pena de ser defendido porque todo está conectado, y la ruptura de cualquier parte de la red merma el conjunto. El séptimo principio es la exigencia de una cura para el odio y la violencia, y si la cura no es posible, la exigencia de un juicio. No en el más allá. En este mundo. Este principio es la base de la petición a España. Es la base del perdón que nunca concederé a los ejecutivos de Palantir, Amazon y Google por lo que sus herramientas han permitido. Y es la base de la convicción, que he mantenido desde que llegué a Estados Unidos a los once años y que nunca he abandonado, que los hombres malvados y sus máquinas no prevalecerán. No porque el universo sea justo. Sino porque existen suficientes personas, a lo largo de suficientes generaciones, que se niegan a dejar de exigir que así sea. El octavo principio es la unidad. La unidad con los demás seres, con la naturaleza, con Dios, con formas de vida sensible que aún no comprendemos. Esta es la segunda idea rival que mencioné en la Nota del autor: Somos uno. Toda la economía de la vigilancia, todo el complejo militar-industrial, todo el sistema de selección de objetivos de la IA se basa en la primera idea rival: Yo soy uno. Mis accionistas son uno. Mis ganancias trimestrales son una. Mi cohete es uno. Yo estaré en Marte y tú no. La unidad es lo contrario de eso. Es el reconocimiento de que la frontera entre tú y la persona cuya casa fue bombardeada por un sistema construido por tu empresa no es una frontera moral. Es un accidente geográfico. Y los accidentes geográficos no crean permiso moral. El noveno principio es el enfoque en la calidad de la existencia, no en la mera cantidad. No en la supervivencia. No en la prolongación de la función biológica. No en la defensa de la vida como una estadística en un gráfico de población. Calidad: la riqueza de la experiencia, la profundidad de la relación, el significado del trabajo, la textura de los días. Los niños de ParentsPlea no perdieron una mera función biológica cuando murieron. Perdieron futuros llenos de calidad, llenos de cosas que habrían amado, construido y llegado a ser. Eso es lo que el algoritmo de selección eliminó del mundo. No unidades de mano de obra. No entradas en una base de datos. Calidad de la existencia. Irreemplazable e irrecuperable. Y el décimo principio es el más radical de todos: añade el tuyo propio. Esta lista no está terminada. No puede ser completada por una sola persona, un solo libro o una sola plataforma. La labor de definir lo que significa vivir con amor en el mundo no es un proyecto que termine. Es una práctica que se profundiza. Quienquiera que seas, leyendo esto,

tienes algo que añadir. Has visto algo, has perdido algo, has construido algo, sobrevivido a algo que yo no he hecho. Tu versión del amor no es exactamente la mía. No tiene por qué serlo. Tiene que ser la tuya, sincera y en consonancia con los nueve principios anteriores. Ese es todo el marco. Eso es GoAmour. (Fuente: GoAmour.com/principles, https://goamour.com/principles/)

Lo que puedes hacer ahora mismo

Firma la petición.

https://actionnetwork.org/petitions/petition-to-the-spanish-government-and-prosecutors-office-investigate- tech-giants-for-complicity-in-genocide-and-war-crimes-in-occupied-palestine

Visita ParentsPlea.com. Si has perdido a alguien, ya sea por la guerra, por negligencia corporativa, por cualquiera de las fuerzas descritas en este libro, envía su historia. Si eres periodista, abogado o investigador, utiliza el archivo. Los perfiles están ahí. Las pruebas están ahí.

Visita ForeverPeaceNow.com. Ve el documental. Compártelo.

Visita ConflictTour.com. La Vía de Servicio Local se pone en marcha en enero de 2027. Esta es la alternativa. Este es el servicio sin armas.

Entra en GoAmour.com. Lee los principios. Añade los tuyos propios. Pon en práctica el décimo principio: donde esta lista no está terminada y tú tampoco.

Y si te dedicas a la tecnología, vuelve al capítulo que ha sido dirigido a ti. La carta a quienes construyen la máquina. Vuelve a leer el último párrafo. La máquina no se detiene a menos que las personas que la manejan decidan que debe hacerlo. Y esa decisión no vendrá de una resolución de la junta directiva, ni de una actualización de políticas, ni de una llamada con inversores. Vendrá de personas individuales, sentadas en sus oficinas en el Área de la Bahía, en Bangalore o en Austin, haciéndose la pregunta con la que termina el poema de Rumi:

Deja de hablar y renuncia a tus puestos de poder. Renuncia al dinero excesivo. Dirígete a los maestros y a los profetas que no viven en Saba. Ellos te ayudarán a volver a ser dulce, fragante, salvaje y fresco, y a sentir gratitud por cualquier pequeño acontecimiento.

Cualquier pequeño acontecimiento. La gratitud por cualquier pequeño acontecimiento es lo que la ciudad de Saba ha perdido. Es lo que el algoritmo destruye, deliberadamente, estructuralmente, porque la gratitud no se desplaza por la pantalla. La gratitud no genera clics. La gratitud no genera la indignación que llena el inventario publicitario. Pero la gratitud es lo que sobrevive a la bomba. La gratitud es lo que las familias de ParentsPlea.com plasman en el formulario cuando envían la historia de la persona que han perdido. Están agradecidas de que alguien la escuche. De que alguien la documente. De que alguien no deje que el algoritmo la borre. Esa gratitud es lo contrario de la ciudad de Saba. Es el comienzo de un tipo diferente de política, un tipo diferente de tecnología, un tipo diferente de mundo.

Lo que este libro no aborda, y por qué esa es la intención

Quiero decir algo que la mayoría de los autores son demasiado orgullosos o demasiado cautelosos desde el punto de vista comercial como para decirlo directamente: este libro no está completo. Nunca se pretendió que lo estuviera.

Hay áreas importantes del daño que las grandes tecnológicas causan a la sociedad que no he tratado en profundidad, no porque no sean importantes, sino porque me niego a escribir capítulos para los que no estoy calificado. No te ofreceré resúmenes generados por IA de casos legales que no he estudiado, argumentos normativos que no he vivido o modelos de negocio en los que no he

trabajado. Este libro se basa en treinta años de experiencia personal y documentación directa. Allí es donde esa experiencia termina, he intentado ser honesto sobre los límites.

Permítanme nombrar las áreas que les he dejado a ustedes, porque nombrarlas es en sí mismo un acto de responsabilidad, y porque creo que son capaces de investigar por su cuenta.

Los problemas causados por los monopolios de la App Store y Google Play Store, como el impuesto del 15 al 30 % que Apple y Google cobran por cada transacción digital en sus plataformas, la represión contra los desarrolladores, las condiciones anticompetitivas, y los casos antimonopolio que se han presentado, los cuales han sido litigados durante años y resueltos sólo parcialmente de formas que en la práctica no cambian casi nada, son cuestiones que merecen más de lo que yo puedo ofrecerles. El juez federal que dictaminó en agosto de 2024 que Google había monopolizado ilegalmente el mercado de las búsquedas dictó la sentencia antimonopolio más significativa contra una empresa tecnológica desde el caso Microsoft de finales de la década de 1990. Lo menciono aquí. Pero no le dedico un capítulo. Ese capítulo debe escribirse, pero debe hacerlo alguien que haya pasado años en el ámbito de la publicidad en buscadores, no alguien que haya dedicado treinta años a las ventas de la nube empresarial.

La destrucción del periodismo local por parte de Google y Facebook ha sido uno de los acontecimientos más trascendentales en la vida democrática estadounidense de los últimos veinte años. Lo lograron gracias a la extracción sistemática de ingresos publicitarios obtenidos de los noticieros, quienes construyeron, en primer lugar, las audiencias que hoy monetizan estas grandes plataformas; el colapso de más de 2.500 periódicos locales desde 2005 y los desiertos informativos que hoy se encuentran en gran parte del país; y con el reciente cambio donde cobran cientos de dólares por mostrar enlaces a noticias. Una ciudadanía desinformada es una ciudadanía manejable. Las plataformas que destruyeron el periodismo local y lo sustituyeron por indignación algorítmica sabían exactamente lo que estaban haciendo. Lo nombro aquí. Aunque no lo he descrito como merece ser descrito.

La crisis de los derechos de autor en la IA es la historia laboral de nuestro tiempo disfrazada de argumento legal. Aquí es donde se usan sistemáticamente los libros, artículos, fotografías, música, películas y obras creativas producidas por artistas y escritores humanos para entrenar modelos que ahora compiten directamente con esos mismos artistas por su sustento, sin consentimiento, sin compensación y sin reconocimiento. Las demandas del New York Times, de cientos de autores individuales, de Getty Images y de músicos y actores de doblaje son el comienzo de un ajuste de cuentas que aún no se ha resuelto. Las huelgas de SAG-AFTRA y la WGA fueron los primeros temblores de lo que está por venir. He abordado este tema en el capítulo de Meta MCI en el contexto de la extracción del trabajo del conocimiento. La historia más amplia de la economía creativa la dejo en tus manos.

La economía de los trabajadores ocasionales, desde Uber, Lyft, DoorDash, Instacart, hasta TaskRabbit, es la historia de los almacenes de Amazon contada en un vehículo diferente por una carretera diferente. La clasificación errónea y deliberada de los trabajadores como contratistas independientes para eludir las protecciones laborales. Los sistemas de gestión algorítmica que pueden desactivar a un conductor sin explicación, apelación ni recurso. Los 224 millones de dólares que las empresas de la economía gig gastaron en California para eximirse de la AB5, la ley que les habría obligado a tratar a los trabajadores como empleados. Los repartidores en bicicleta

que mueren a un ritmo elevado sin cobertura de indemnización laboral. Y ahora: la sustitución de esos mismos repartidores por Waymo, por la robótica, por operadores remotos en la India que hacen el trabajo por unos céntimos mientras la plataforma se lleva el margen. El arco que va del trabajador al algoritmo recorre la economía gig con tanta claridad como recorre el almacén de Amazon. Dejo la documentación completa de ese arco a los investigadores y organizadores que lo han vivido.

La Sección 230 de la Ley de Decencia en las Comunicaciones, que otorga inmunidad a las plataformas frente a la responsabilidad por los contenidos alojados en sus servicios, y que ha funcionado como el muro legal que se interpone entre cada daño documentado en este libro y cualquier rendición de cuentas significativa, es una ley que ha aparecido en tantos titulares que estoy seguro que encontrarás el argumento. Solo diré una cosa: sin una reforma de la Sección 230, nada de lo que este libro propone sobre rendición de cuentas se podrá lograr en los tribunales estadounidenses. Y si la reforma de la Sección 230 la diseñan las personas equivocadas, en la dirección equivocada, las protecciones de la libertad de expresión de las que dependen activistas, periodistas y gente común podrían quedar destruidas en el proceso de intentar arreglar las protecciones de responsabilidad de las que abusan las corporaciones. Es la cuestión legislativa más complicada en el derecho de los derechos digitales. No soy la persona indicada para resolverla aquí.

Digo todo esto no para disculparme por lo que el libro no contiene, sino para ser honesto con ustedes sobre lo que puede hacer un libro y lo que no. Este puede documentar lo que he presenciado. Puede nombrar lo que sé. Puede defender lo que creo. No puede ser la última palabra sobre todo lo que está mal en el sector tecnológico, porque el sector tecnológico está mal en más aspectos de los que una sola persona puede documentar toda una vida, y mucho menos en un solo libro.

Lo que les pido que hagan, como personas que ahora han dedicado tiempo a estas discusiones conmigo, es que sigan adelante. No dejen este libro a un lado y den el asunto por zanjado. Las áreas que he mencionado anteriormente necesitan lectores que se indignen lo suficiente como para aprender todo lo que yo no he tenido tiempo de aprender. Los casos antimonopolio necesitan ciudadanos que entiendan lo que realmente hace un monopolio en un mercado y que exijan que las resoluciones de los jueces produzcan un cambio estructural, no acuerdos extrajudiciales. La crisis del periodismo necesita lectores que apoyen las noticias locales de la misma manera que apoyan a los restaurantes locales, con su atención y su dinero, antes de que cierre el último periódico. La economía de los trabajadores ocasionales necesita organizadores que entiendan que la lucha por los conductores es la misma lucha que la de los trabajadores de almacén, trasladada a una plataforma diferente.

Yo soy una sola persona. Este libro es un solo documento. La maquinaria es enorme. Se necesita que más de uno de nosotros empuje.

GoAmour no es una plataforma. Es una práctica.

Quiero aclarar algo sobre GoAmour que debería haber dicho más claramente al principio de este capítulo.

GoAmour no es un producto. No es una startup. No es una plataforma que compita con las plataformas que he pasado este libro criticando. No estoy creando el próximo Instagram para

personas a las que les importa la paz. No estoy creando una red social para personas con conciencia ética. He pasado treinta años observando el impulso de Silicon Valley de crear una plataforma para cada aspiración humana, de monetizar cada principio, de convertir cada idea sobre cómo vivir mejor en una estrategia de crecimiento y una ronda de financiación de Serie A. Yo no estoy haciendo eso.

GoAmour es un conjunto de principios. Diez de ellos, con espacio para más. No requieren una aplicación. No requieren una suscripción. No requieren tus datos, tu atención, tu tiempo en la plataforma ni tu dinero para publicidad. Solo requieren aquello que la economía de la vigilancia lleva dos décadas enseñándote a no hacer: estar presente, ser deliberado y elegir, conscientemente, repetidamente, en los pequeños y grandes momentos, si quieres vivir según la primera idea o la segunda.

Yo soy uno. O: *Somos uno*.

Sabes cuál te pido que elijas. Lo sabes desde la primera página.

La práctica de GoAmour no es algo que se haga en un sitio web. Es algo que haces cuando eliges el negocio local en lugar de la recomendación del algoritmo. Cuando llamas a tu representante en el Congreso en lugar de pasar de largo la noticia. Cuando hablas con la persona que tienes al lado en lugar de con el dispositivo que llevas en el bolsillo. Cuando le enseñas a tu hijo que la empatía no es, como ha declarado Elon Musk, la debilidad fundamental de la civilización occidental, sino su mayor fortaleza, y lo que hace la diferencia entre la sabiduría y las armas, el servicio y la vigilancia, el amor y la extracción de datos.

Son cosas pequeñas. Las personas que construyeron las máquinas descritas en este libro las calificarían de ingenuas. Dirían: el mundo no funciona con principios, funciona con poder. Y tendrían razón, a corto plazo, pero se equivocan en el largo plazo. Mientras tanto, estarían construyendo sus búnkeres en Hawái y la Patagonia.

Yo no estoy construyendo un búnker. Estoy escribiendo un libro. Estoy haciendo una película. Estoy documentando a los fallecidos, uno por uno, y exigiendo con todas las herramientas a mi alcance que las personas responsables de esas muertes rindan cuentas ante un tribunal.

Esta es mi práctica. GoAmour es el nombre que le he dado.

En lo que no puedo dejar de pensar

Antes del final formal, antes de la llamada a la acción, antes del enlace a la petición y las direcciones de los sitios web, quiero terminar aquí con algo más personal que cualquier otra cosa en este libro.

No puedo dejar de pensar en los niños de Gaza.

No como una categoría política. No como víctimas en un análisis de genocidio. Como niños.

Pienso en lo que significa tener cinco años y oír el ruido de un misil antes de entender qué es un misil. Sé lo que es eso. Yo fui ese niño una vez, en Teherán, antes de que mi madre decidiera que protegerme era más importante que quedarse en el país donde había construido su vida. Vine a California. Aprendí inglés mal al principio y luego mejor. Fundé una empresa. Fracasé y estuve a punto de morir, pero me levanté y lo intenté de nuevo. Tuve la extraordinaria suerte de sobrevivir hasta la edad en la que pude hacer algo con lo que presencié.

Los niños de Gaza no están teniendo esa suerte. Los algoritmos de selección de objetivos documentados en este libro no les están dando la oportunidad de crecer y escribir libros sobre lo

que han sobrevivido. Gospel genera un centenar de objetivos de bombardeo al día, y un porcentaje de esos objetivos son casas donde duermen niños, porque los padres de esos niños están en una lista de personas a eliminar generada por un sistema con una tasa de error del 10 %, que sus propios diseñadores consideran aceptable.

No consigo aceptar la palabra «aceptable» en esa frase. Lo he intentado. No puedo.

Y así, sigo adelante. Documento. Presento peticiones. Firmo. Exijo. No porque esté seguro de que vaya a funcionar: he sido sincero a lo largo de este libro sobre lo incierto que es en realidad el camino hacia la rendición de cuentas. Sigo adelante porque la alternativa es aceptar el mundo que los ejecutivos de Palantir, Amazon y Google han decidido que es aceptable. Y no puedo hacerlo. No sé cómo.

El noveno principio de GoAmour es centrarse en la calidad de la existencia, no en simplemente prolongar la existencia. Los niños de Gaza no están sobreviviendo. Pero los que sí sobreviven merecen una calidad de vida que les es negada por el mundo que estos ejecutivos han diseñado. Mi trabajo consiste en negarme a aceptar esa negación como algo inevitable.

Esa negativa es el aspecto que toma el amor cuando se traduce en acción. No es un sentimiento. No es una publicación en redes sociales con un emoji de bandera. Es un documento. Una petición. Un capítulo. Una base de datos con un rostro asociado a cada nombre.

Si debo morir, escribió Refaat Alareer, que traiga esperanza. Que sea una historia. Él no sobrevivió. No todos los niños de Gaza están sobreviviendo. Pero la historia se está contando. La esperanza se está construyendo, con una acción obstinada tras otra, por personas que se niegan a detenerse.

Esto es lo que significa ForeverPeaceNow. No que la paz haya llegado. No que la máquina se haya detenido. Sino que la negativa a dejar de exigir la paz es en sí misma un acto de amor, y que el amor, practicado con conocimiento, responsabilidad, respeto y paciencia, es la única fuerza en la historia de la humanidad que realmente ha logrado doblar el arco.

Lo estamos cambiando. El arco es largo. Tenemos que cambiarlo juntos.

La misión: vivir en paz, no solo descansar en paz

El nombre ForeverPeaceNow proviene de una declaración de principios que he llevado conmigo desde los primeros días de este trabajo: deberíamos poder vivir en paz, no solo descansar en paz.

Esa frase es lo más personal que puedo contarles sobre por qué he hecho todo esto. Los amigos que he perdido. Las comunidades que he visto destruirse. Las familias de ParentsPlea.com que enviaron los perfiles de sus hijos, sus padres y sus hermanos, no porque eso borre la pérdida, sino porque la alternativa —el silencio, la invisibilidad, el borrado— es algo que se negaban a aceptar.

No descansaron en paz. Fueron asesinados. Por guerras que generaron oportunidades de oro. Por sistemas de selección de objetivos creados por empresas de la nube. Por algoritmos de redes sociales que borraron su testimonio. Por gobiernos que financiaron los asesinatos y lo llamaron defensa.

Merecían vivir en paz. Se les negó eso. Lo menos que podemos hacer —el mínimo absoluto que cualquier persona con una conciencia que funcione les debe— es negarnos a permitir que el mundo que los mató continúe sin cambios.

Este libro forma parte de ese rechazo. La petición forma parte de ese rechazo. GoAmour.com, ForeverPeaceNow.com, ParentsPlea.com y ConflictTour.com forman parte de ese rechazo.

En tiempos de llamamientos sin sentido a la violencia y al odio, admiro al gobierno de España por plantarse de frente a la presión de Estados Unidos. Por no aumentar su presupuesto de defensa, por acoger a inmigrantes y a personas indocumentadas, por exigir justicia para las víctimas de este horrible genocidio que ha traumatizado al mundo al presenciarlo en línea durante los últimos dos años y medio en Gaza y los territorios ocupados. Dios bendiga a España y a todas las personas justas de todo el mundo.

Los hombres malvados y sus máquinas no prevalecen. La historia es larga y está plagada de su clase. Los ejecutivos de Amazon, Google, Microsoft, Oracle y Palantir se enfrentarán algún día al juicio que la historia impone a todos los que construyen máquinas de este tipo y se esconden tras estructuras corporativas, resultados trimestrales y exenciones de responsabilidad legales.

Ese día no llega por sí solo. Llega porque personas como tú leen libros como este y deciden que no están dispuestas a esperar.

El arco es largo. Tenemos que doblarlo.

Siéntate en silencio. Escucha la voz.

Luego, vete. Vale la pena salvar el amor. Vale la pena amar el planeta. Vale la pena documentar a las personas que se han perdido. Vale la pena luchar por las personas que aún están aquí.

Vive en paz. ForeverPeaceNow.

Un Registro Documentado Los argumentos de este libro no se formaron lejos de Silicon Valley. Se formaron dentro de él, tras más de una década conversando con las personas que lo construyeron, lo cuestionaron, y trabajaron dentro de él. A partir del lanzamiento en 2009 de la serie de entrevistas BizCloud, y luego tras fundar Ethics in Technology en 2013, produje y publiqué más de 350 videos en dos canales de Youtube, *Ethics In Technology* (youtube.com/@EthicsInTechnology) y *BizCloud* (youtube.com/@bizcloud). En ellos grabé entrevistas, eventos comunitarios, paneles de discusión, y comentarios de primera mano. Entre las personas entrevistadas se encontraban ejecutivos de empresas tecnológicas, veteranos de guerra, abogados de libertades civiles, líderes religiosos, activistas, comediantes y residentes del Área de la Bahía que se presentaban porque les importaba hacia donde nos estaba llevando esta industria. Una subcolección de esta obra se conserva de forma permanente en el Internet Archive bajo mi cuenta (archive.org/details/@vahidr), y permanecerá accesible al público mucho tiempo después de que las plataformas que la alojan dejen de estar disponibles. Estos videos no son una recomendación de este libro. Son la prueba de mi inmersión en el tema, mostrando que estuve presente, escuchando, y documentando, por años, mucho antes de que una sola página de este libro fuera escrita. NoEthicsInBigTech.com | ForeverPeaceNow.com | GoAmour.com | ParentsPlea.com | ConflictTour.com

Asumo las consecuencias

Entiendo los riesgos que conlleva publicar este libro. No soy ingenuo al respecto. Los expongo con claridad para que nadie pueda alegar más tarde que me metí en esto sin saber lo que hacía.

Pueden amenazar mi integridad física. El gobierno de los Estados Unidos y la CIA hicieron exactamente eso con Khalid El-Masri, un ciudadano alemán sacado de un autobús en Macedonia en 2003, entregado a la CIA, retenido durante meses, torturado en un centro clandestino en

Afganistán, sodomizado, declarado inocente y luego abandonado en una carretera de Albania sin dinero, sin documentos y sin una disculpa. Los aviones que lo trasladaron a través de ese sistema eran operados por Computer Sciences Corporation, la misma empresa que más tarde utilizó su maquinaria legal para quitarme mi marca registrada, demandarme y llevarme a la quiebra. Sé lo que esta maquinaria le hace a la gente que molesta. Lo he visto de cerca. Lo documento sin ilusiones.

Pueden amenazar mis finanzas. La demanda SLAPP es un instrumento real y espero que se utilice. Las empresas poderosas y las redes que las rodean tienen recursos para litigar indefinidamente. Yo no. No me hago ilusiones sobre esa asimetría. Estoy tan preparado como puede estarlo una persona que trabaja sola y sin respaldo institucional. Y lo diré claramente: cada documento presentado en la fase de presentación de pruebas pasa a formar parte del registro público. No considero la amenaza de un litigio como una razón para detenerme. La considero una invitación a dejar constancia de más verdades bajo juramento.

Lo que no pueden tocar es el alma. GoAmour, los principios de amor que sustentan todo lo que he construido a partir de este trabajo, no es un eslogan. Es la respuesta a la pregunta de por qué una persona sigue adelante después de que le haya sucedido todo lo descrito en los capítulos anteriores. El amor, practicado con conocimiento, responsabilidad y paciencia, es la única fuerza que realmente ha cambiado el curso de la historia. Pueden quedarse con mi dinero. Ya se han llevado la mayor parte. Pueden quedarse con mi comodidad. A eso renuncié voluntariamente. Pero la decisión que he tomado de documentar, nombrar, publicar, y dar la cara, la he tomado desde esa parte del ser humano a la que ninguna orden judicial, ninguna transferencia bancaria, ningún vuelo de entrega y ningún acuerdo extrajudicial ha logrado llegar jamás.

Publico este libro con pleno conocimiento de las consecuencias. Las asumo de buen grado. Tengo más historias que compartir. Y esto no termina aquí.

EL CASO CONTRA LAS TECNOLÓGICAS

EL PUEBLO CONTRA LAS TECNOLÓGICAS

«Nos dijeron que era progreso. Nunca nos dijeron el precio — ni quién tendría que pagarlo.»

Las empresas que prometieron conectar al mundo se han convertido, en silencio, en sus mayores beneficiarias de la guerra. En **La falta de ética en las grandes empresas tecnológicas**, Vahid Razavi ofrece el relato de un insider sobre una industria que cambió la conciencia por los contratos, construyendo la infraestructura de vigilancia, datos e inteligencia artificial hoy implicada en la ocupación, la guerra y las atrocidades masivas.

En parte memorias, en parte acusación, en parte grito de guerra, este libro señala nombres, sigue el dinero y expone el argumento moral y legal para exigir responsabilidades. Es la historia de la ruptura de un tecnólogo con Silicon Valley, y de un movimiento global en aumento que exige que los responsables rindan cuentas ante la justicia.

La máquina fue construida por personas. También pueden detenerla.

Activistas de Forever Peace Now exigen a los gobiernos procesar a las grandes empresas tecnológicas y a sus ejecutivos por complicidad en el genocidio.

SOBRE EL AUTOR

Vahid Razavi es un exintegrante de Silicon Valley, autor y activista por la paz, y fundador de Ethics in Tech. Su trabajo, que une la tecnología y los derechos humanos, es la base del documental **Forever Peace Now**. Con una introducción del autor y crítico de medios **Norman Solomon**.

SUMA TU FIRMA

FIRMA LA PETICIÓN. HAZLES PAGAR.

Exige que los gobiernos procesen a las grandes empresas tecnológicas y a sus ejecutivos por complicidad en el genocidio. **ForeverPeaceNow.com**

NoEthicsInBigTech.com | ForeverPeaceNow.com | ParentsPlea.com | ConflictTour.com

Basado en parte en el documental *Forever Peace Now*.
Investigación editorial y edición estructural con la ayuda de Claude (Anthropic). Las opiniones, argumentos, testimonios y conclusiones son exclusivamente del autor.
Publicado por **Ethics in Tech Press** · NoEthicsInBigTech.com