

PODERES, CONSTITUCIÓN Y DERECHO

David Sánchez Rubio, Álvaro Sánchez Bravo
y Jesús Ignacio Delgado Rojas
(editores)



David Sánchez Rubio
Pilar Cruz Zúñiga
David Vila-Viñas
Alexandre Bernardino Costa
Jesús Ignacio Delgado Rojas
Hernando León Londoño Berrío
Blanca Rodríguez Ruiz
Luísa Winter Pereira
Alfonso de Julios-Campuzano
Antonio Mesa León
Antonio Carlos Wolkmer

**PODERES,
CONSTITUCIÓN Y DERECHO**

PODERES, CONSTITUCIÓN Y DERECHO

**David Sánchez Rubio, Álvaro Sánchez Bravo
y Jesús Ignacio Delgado Rojas**
(editores)

**David Sánchez Rubio
Pilar Cruz Zúñiga
David Vila-Viñas
Alexandre Bernardino Costa
Jesús Ignacio Delgado Rojas
Hernando León Londoño Berrío
Blanca Rodríguez Ruiz
Luísa Winter Pereira
Alfonso de Julios-Campuzano
Antonio Mesa León
Antonio Carlos Wolkmer**



FACULTAD DE DERECHO

Dykinson, S.L.

No está permitida la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (art. 270 y siguientes del Código Penal).

Diríjase a Cedro (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra. Puede contactar con Cedro a través de la web www.conlicencia.com o por teléfono en el 917021970/932720407

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial
Para mayor información, véase www.dykinson.com/quienes_somos

© De la obra: David Sánchez Rubio, Álvaro Sánchez Bravo y Jesús Ignacio Delgado Rojas

© De los textos: los autores

Primera edición, 2024

Editorial DYKINSON, S.L. Meléndez Valdés, 61 – 28015 Madrid

Teléfono (+34) 91544 28 46 – (+34) 91544 28 69

e-mail: info@dykinson.com

<http://www.dykinson.es>

<http://www.dykinson.com>

ISBN: 978-84-1170-985-9

Depósito Legal: M-2655-2024

Preimpresión:

Besing Servicios Gráficos, S.L.

besingsg@gmail.com

Índice

INTRODUCCIÓN.....	13
--------------------------	-----------

David Sánchez Rubio y Jesús Ignacio Delgado Rojas

CAPÍTULO PRIMERO. SOBRE PARADIGMAS DE CONOCIMIENTO, PODERES Y TEORÍAS CRÍTICAS DEL DERECHO.....	17
--	-----------

David Sánchez Rubio y Pilar Cruz Zúñiga

1. INTRODUCCIÓN.....	17
2. TEORÍAS CRÍTICAS DEL DERECHO Y NUEVOS PARADIGMAS	21
3. ALGUNOS DISPOSITIVOS DE PODERES.....	25
BIBLIOGRAFÍA.....	37

CAPÍTULO SEGUNDO. ENTENDER EL PODER PARA INVESTIGAR SOBRE EL DERECHO. CUESTIONES DE MÉTODO Y GUBERNAMENTALIDAD	41
---	-----------

David Vila-Viñas

1. INTRODUCCIÓN.....	41
2. RACIONALIDADES JURÍDICOPOLÍTICAS HEGEMÓNICAS: UN ITINERARIO	42
3. OTROS ENFOQUES. EL DERECHO DE LAS PLANTAS ALTAS Y EL DERECHO A PIE DE CALLE.....	53
BIBLIOGRAFÍA.....	56

CAPÍTULO TERCERO. O DIREITO ACHADO NA RUA E O NEOLIBERALISMO DE AUSTERIDADE 61

Alexandre Bernardino Costa

1.	INTRODUÇÃO	61
2.	UMA IDEIA PERIGOSA	62
3.	A CONSTITUIÇÃO DE 1988 E A NOVA RAZÃO DO MUNDO	64
4.	NEOLIBERALISMO, UMA TEORIA CIENTÍFICA? QUAIS OS SUPOSTOS EPISTEMOLÓGICOS DA AUSTERIDADE?	66
5.	AUSTERIDADE – DEMOCRACIA E AUTORITARISMO	69
6.	O DIREITO ACHADO NA RUA.....	73
7.	CONSIDERAÇÕES FINAIS	77
	BIBLIOGRAFÍA.....	79

CAPÍTULO CUARTO. PODER TECNOLÓGICO Y POLÍTICAS PATERNALISTAS. LA GOBERNANZA ALGORÍTMICA A TRAVÉS DE *HYPERNUDGES* 81

Jesús Ignacio Delgado Rojas

1.	INTRODUCCIÓN.....	81
2.	BIG DATA COMO TÉCNICA DE REGULACIÓN EN EL DISEÑO PREVIO DE OPCIONES ELEGIBLES.....	82
3.	LA CRÍTICA A LOS <i>HYPERNUDGES</i>	88
4.	DE LA TOTAL TRANSPARENCIA A LA VIGILANCIA TOTALITARIA	97
5.	CONCLUSIONES	100
	BIBLIOGRAFÍA.....	101

CAPÍTULO QUINTO. PODER PUNITIVO, PENAS ILEGALES Y DEMOCRACIA 105

Hernando León Londoño Berrío

1.	INTRODUCCIÓN.....	105
2.	LAS PENAS ILEGALES EN EL MARCO DE LA EJECUCIÓN DE LA PENA DE PRISIÓN Y DE LA PRISIÓN SIN CONDENA.....	106
3.	AVATARES DE LA “PENA ANTICIPADA” O “PRISIÓN SIN CONDENA”	114
4.	CONCLUSIONES	125
	BIBLIOGRAFÍA.....	127
	JURISPRUDENCIA.....	133

CAPÍTULO SEXTO. LA AUTONOMÍA REIVINDICA SU LUGAR CONSTITUCIONAL: INCURSIONES DEMOCRÁTICAS DESDE LO ÍNTIMO 135

Blanca Rodríguez Ruiz

1.	INTRODUCCIÓN.....	135
2.	CUATRO SENTENCIAS, UNA LÍNEA JURISPRUDENCIAL	136
3.	RAMIFICACIONES DE LA AUTONOMÍA: EL SISTEMA GÉNERO-SEXO, LO ÍNTIMO, LOS CUERPOS.....	141
4.	REFLEXIONES DE CIERRE: AUTONOMÍA E INTERSUBJETIVIDAD	151
	BIBLIOGRAFÍA.....	152

CAPÍTULO SÉPTIMO. LA RISA DE ROUSSEAU. LÍMITES ONTOLÓGICOS DEL CONSTITUCIONALISMO Y DEMOCRACIA SIN CUERPOS..... 155

Luísa Winter Pereira

1.	INTRODUCCIÓN.....	155
----	-------------------	-----

2.	LA DEMOCRACIA SIN CUERPOS EN LA XIV LEGISLATURA ESPAÑOLA.....	157
3.	LA RISA DE ROUSSEAU EN EL CONSTITUCIONALISMO MODERNO/COLONIAL.....	161
4.	UNA PROPUESTA DE DEMOCRACIA CORPORAL COMO PRINCIPIO ANTIOLIGÁRQUICO	171
	BIBLIOGRAFÍA.....	175

CAPÍTULO OCTAVO. DERECHOS Y LIBERTADES EN LA CONSTITUCIÓN DE 1812 179

Alfonso de Julios-Campuzano

1.	EL TRATAMIENTO DISPERSO DE LOS DERECHOS EN LA CONSTITUCIÓN DE CÁDIZ.....	179
2.	LOS DERECHOS COMO CLAVE INTERPRETATIVA DE LA CONSTITUCIÓN.....	181
3.	EL CATÁLOGO DE DERECHOS EN LA CONSTITUCIÓN DE CÁDIZ.....	184
4.	LOS DEBERES DEL CIUDADANO	191
5.	LA FELICIDAD DE LA NACIÓN Y EL BIENESTAR DE LOS INDIVIDUOS QUE LA COMPONENTE	193
6.	TRADICIÓN Y MODERNIDAD EN LA CONSTITUCIÓN DE CÁDIZ.....	196
	BIBLIOGRAFÍA	199
	DOCUMENTOS NORMATIVOS	201

CAPÍTULO NOVENO. LA IDEA DE UNA CONSTITUCIÓN GLOBAL EN EL PENSAMIENTO DE ALEXANDRE KOJÈVE..... 203

Antonio Mesa León

1.	INTRODUCCIÓN.....	203
2.	EL CONSTITUCIONALISMO COSMOPOLITA.....	206
3.	LA PROPUESTA DE KOJÈVE: EL ESTADO UNIVERSAL Y HOMOGÉNEO	210

4. CONCLUSIONES	220
BIBLIOGRAFÍA.....	221
CAPÍTULO DÉCIMO. PARA ALÉM DO ANTROPOCENO: O DIREITO HUMANO AO FUTURO	225
<i>Antonio Carlos Wolkmer</i>	
1. INTRODUÇÃO	225
2. CENÁRIOS DO ANTROPOCENO E SEUS REFLEXOS NA CONSTITUIÇÃO DE MARCOS NORMATIVOS	226
3. DESCOLONIZAR A TRADIÇÃO UNIVERSALISTA DOS DIREITOS HUMANOS	230
4. RESSIGNIFICAR DIREITOS HUMANOS COMO DIREITOS AO FUTURO: DO ANTROPOCÊNTRICO AO ECOCÊNTRICO	232
5. CONCLUSÃO	236
BIBLIOGRAFÍA.....	237

CAPÍTULO CUARTO.

Poder tecnológico y políticas paternalistas.

La gobernanza algorítmica a través de *hypernudges*

JESÚS IGNACIO DELGADO ROJAS¹

1. INTRODUCCIÓN

La sociedad del siglo XXI está inmersa en la denominada “revolución de los datos masivos” (Mayer-Schönberger y Cukier, 2013: 6-7), lo cual implica una profunda transformación en la forma en la que se ha venido entendiendo la humanidad. Responsables de dichos cambios son los importantes avances alcanzados en diversos ámbitos como la Inteligencia Artificial, los sistemas de Big Data o la robótica. Este capítulo se centra en cómo la industria tecnológica está aprovechando dichos sistemas de Big Data para transformar los masivos datos digitales personales, obtenidos a partir de las decisiones que los individuos toman en la red, en información con un alto valor económico.

La combinación del inmenso volumen de datos procedentes de las numerosas fuentes que los generan y de las tecnologías que los almacenan, ha traído consigo innegables beneficios de diversa índole. Sin embargo, el tratamiento de dicha información y su posterior uso (con fines comerciales o estratégicos, principalmente) ocasiona injerencias en la vida privada de los individuos, lo que implica sin duda una amenaza, sobre todo, a aquellos derechos fundamentales que han de protegerla. El Big Data supone un salto cualitativo muy importante que coloca a quien dispone de los datos, y del conocimiento y técnicas para procesarlos, en una situación de ventaja competitiva sin precedentes (Pasquale, 2015). Quien tiene los datos, tiene el poder: y los individuos pasan a convertirse en una especie de *sujeto datístico* bajo el paradigma de una *data society*:

Una ‘sociedad de datos’, que no sólo se rige por los datos como en su advenimiento fue la sociedad de la información y el conocimiento, sino que está

¹ Profesor del Departamento de Filosofía del Derecho de la Universidad de Sevilla. jdrojas@us.es.
ORCID ID 0000-0002-3818-5990.

íntimamente impregnada de ellos, llegando a implicar y moldear al hombre mismo como un *data subject* (Faini, 2019: XVII).

Sostendré que la forma de conocimiento que se obtiene de los comportamientos digitales de los usuarios a través de los sistemas de Big Data es preocupante no sólo por sus implicaciones para la privacidad, sino también por la manera concreta en que esos datos se están utilizando para moldear la toma de decisiones individuales al servicio de los intereses de los gigantes tecnológicos (las llamadas *Big Tech*: sobre todo, Google, Amazon, Apple, Meta y Microsoft). Mi argumento central es que, con la tecnicidad y sofisticación de sus procesos algorítmicos subyacentes, estos sistemas tecnológicos están influyendo peligrosamente en el diseño y toma de decisiones humanas de forma paternalista: lo que se consigue a través de *hypernudges* (Yeung, 2017). Al configurar y, por tanto, personalizar el contexto informativo de elección del usuario, normalmente mediante el análisis algorítmico de flujos de datos procedentes de múltiples fuentes que pretenden ofrecer información predictiva sobre nuestros hábitos y preferencias, estos *nudges* moldean las decisiones del usuario en las direcciones preferidas por el “arquitecto de la elección” (quien tiene la responsabilidad de organizar el contexto en el que se toma la decisión) a través de procesos sutiles y discretos, pero extraordinariamente potentes. Trataré de ofrecer una aproximación por la que evaluar las problemáticas consecuencias persuasivas y manipuladoras para la autonomía personal que genera la implementación de estos *nudges* a través de técnicas de Big Data.

2. BIG DATA COMO TÉCNICA DE REGULACIÓN EN EL DISEÑO PREVIO DE OPCIONES ELEGIBLES

Las técnicas algorítmicas de Big Data, o “gobernanza algorítmica” (O’Reilly, 2013), pretenden sistemáticamente influir en el comportamiento de los individuos. Las decisiones humanas están determinadas no sólo por las deliberaciones racionales de las opciones disponibles, sino también por el diseño del entorno de elección en el que se presenta la información, que puede ejercer una influencia subconsciente en el resultado. En otras palabras, lo que se elige a menudo depende de cómo se presentan las opciones, por lo que la arquitectura de la elección altera el comportamiento de las personas de forma predecible.

La política conductual es el estudio de cómo los gobiernos logran los objetivos de política pública a través de nuevos instrumentos regulativos que promueven un mejor cumplimiento de las normas. Para mejorar así la calidad de la legislación y su grado de obediencia, los científicos conductuales exploran cómo funcionan los sesgos y atajos cognitivos, la importancia de las

emociones y la influencia de las expectativas futuras en el comportamiento del ciudadano (Güemes, 2021: 311). Con esa información se diseñan políticas públicas que tengan en cuenta tanto esta psicología humana como el papel de la neurociencia para establecer normas orientadas a ganarse un mayor apoyo y cumplimiento entre sus destinatarios.

El proceso de mejora de la legislación llevado a cabo por las políticas conductuales se compone de tres fases de trabajo: recopilación de información y supervisión; establecimiento de normas, metas y objetivos; y cambio del comportamiento para adecuarlo al requerido por la norma u objetivo establecido (Hood, Rothstein y Baldwin, 2001). Dentro de la literatura acerca de la psicología del comportamiento humano, las técnicas empleadas por los reguladores para alcanzar el resultado social deseado se distinguen según el grado de fuerza y coacción que ejercen sobre el destinatario: que van desde la mera persuasión, el consejo, la recomendación o el exhorto a fórmulas de desincentivación más contundentes como la pena de prisión (Bemelmans-Videc *et al.*, 1998). Mientras que los juristas tienden a centrarse en las técnicas tradicionales de compulsión y control, en las que la ley prohíbe u obliga a una conducta específica, respaldada por sanciones coercitivas en caso de infracción, los técnicos de las políticas conductuales han estudiado cómo funciona el “diseño previo de opciones elegibles” como instrumento regulador y orientador de la conducta humana (Clarke y Newman, 2005; Lessig, 1999; Zittrain, 2008). La regulación basada en el “diseño previo de opciones” trabaja precisamente en el momento de la elaboración de las normas, con el objetivo de que, con el cumplimiento de dichas normas, se fomenten y alcancen conductas y resultados sociales considerados deseables².

2.1. La arquitectura de la elección y el *nudge* como instrumentos para influir en el comportamiento humano

Sunstein y Thaler, desde lo que han denominado “paternalismo libertario”, se han referido con la idea de *nudges* a los impulsos que reciben los ciu-

² Este enfoque está en sintonía con la *función promocional del Derecho*, teorizada por Norberto Bobbio, que pone de relieve las “nuevas técnicas de control social que caracterizan la acción del Estado social de nuestros días y la distinguen profundamente de las del Estado liberal clásico: el empleo cada vez más difundido de las técnicas de alentamiento junto a, o en sustitución de, las tradicionales de desalentamiento”. Se puede distinguir “un ordenamiento protector-represivo de un ordenamiento promocional, diciendo que al primero le interesan sobre todo los comportamientos socialmente no deseados, por lo que su fin principal es impedir en todo lo posible su realización; al segundo le interesan sobre todo los comportamientos socialmente deseados, por lo que su fin es provocar su realización incluso entre los recalcitrantes”. Para provocar la realización de esos comportamientos que se estiman valiosos se establecen técnicas de “alentamiento” en las que “A trata de influir en el comportamiento querido (no importa si comisivo u omisivo) de B o facilitándolo o atribuyéndole consecuencias agradables” (Bobbio, 1990: 372 y 381-382).

dadanos para moldear y orientar su comportamiento. Estos “pequeños empujones” estimulan, incentivan o preparan de antemano las decisiones posibles sin querer traicionar la libertad de elección del individuo. El paternalismo libertario se basa en “la convicción de que, en general, las personas deben ser libres para hacer lo que desean, y para desvincularse de los acuerdos desventajosos si lo prefieren”; pero, al mismo tiempo, también se considera que “es legítimo que los arquitectos de las decisiones traten de influir en la conducta de la gente para hacer su vida más larga, más sana y mejor”. Un *nudge* queda así definido como “cualquier aspecto de la arquitectura de las decisiones que modifica la conducta de las personas de una manera predecible sin prohibir ninguna opción ni cambiar de forma significativa sus incentivos” (Sunstein y Thaler, 2009: 20).

El legado intelectual de Sunstein y Thaler se basa en experimentos de psicología cognitiva que tratan de comprender la toma de decisiones de los seres humanos, descubriendo considerables divergencias entre el modelo del actor racional de la toma de decisiones asumido en el análisis microeconómico (que se remonta a la perspectiva antropológica del *homo oeconomicus*) y la forma en que los individuos toman realmente las decisiones cuando emplean generalmente atajos cognitivos y heurísticos (Tversky y Kahneman, 1974; Ayres, 2010).

Basándose en estas premisas, Sunstein y Thaler destacan cómo el contexto que rodea la toma de decisiones puede diseñarse intencionadamente de forma que se pueda influir sistemáticamente en las elecciones humanas de determinada manera. Por ejemplo, para animar a los consumidores a elegir alimentos más sanos, los responsables de las cafeterías podrían colocar los productos más saludables en un lugar más destacado, situando la fruta en un sitio más visible que la tarta de chocolate (Sunstein y Thaler, 2009: 15 y ss.).

Por lo que a nosotros interesa, esta teoría de los “pequeños empujones” está en la base de distintas propuestas para la mejora de las decisiones que los usuarios adoptan en el ámbito de las aplicaciones tecnológicas: cuando la teoría de los “empujones” se ha aplicado al entorno digital en combinación con los sistemas de Big Data ha dado lugar a los llamados *hypernudges*, una novedosa técnica de guiado algorítmico para la toma de decisiones que da forma al contexto de elección en el que se mueve el usuario digital.

2.2. Los sistemas de Big Data combinados con la técnica regulatoria del *nudge*: los *hypernudges*

Para entender cómo las técnicas analíticas de Big Data utilizan los *nudges*, dando lugar a los *hypernudges*, podemos distinguir dos grandes configuracio-

nes de procesos de toma de decisiones en un entorno web basados en sistemas algorítmicos:

- (a) Procesos *automatizados* de toma de decisiones. Muchas transacciones habituales se basan en procesos automatizados, desde disponer de dinero en efectivo a través de cajeros automáticos hasta técnicas muy sofisticadas utilizadas por algunas entidades financieras que ofrecen créditos inmediatos al consumo. Estos procesos de toma de decisiones emiten automáticamente algún tipo de “decisión” sin necesidad de intervención humana más allá de la introducción por el usuario de los datos pertinentes (a través de formularios *online*). Cathy O’Neil (2018) se ha referido a estos procesos algorítmicos altamente automatizados como “armas de destrucción matemática” por su potencial destructivo e injusto para los individuos.
- (b) Procesos *digitales* de orientación de toma de decisiones. Los procesos digitales están diseñados para que no sea la máquina, sino la persona a la que se dirigen, la que adopte finalmente la decisión pertinente. Pero, aunque la elección sea humana, en el proceso de construcción de la voluntad del individuo interfieren otros factores que orientan y guían su decisión final. Estos factores son tecnologías que tratan de dirigir la decisión de la persona de manera que un algoritmo de software subyacente la identifica como óptima, ofreciendo al usuario algunas “sugerencias” destinadas a incitarle a tomar la decisión que para él o ella ha prefigurado el arquitecto web de la elección (Selinger y Seager, 2012).

En este trabajo me estoy centrando en este segundo tipo de procesos: en los que la decisión última tiene que ser adoptada por una persona, no por una máquina, aunque en el proceso de construcción de su voluntad haya recibido la interferencia que ha diseñado para ello un sistema de Big Data. Estas técnicas aprovechan los empujones o *nudges* con el fin de optimizar la elección del consumidor o hacer más atractiva su experiencia de usuario. Pensemos en el funcionamiento de los motores de búsqueda de Internet: en respuesta a una consulta que introducimos en la barra de búsqueda, las técnicas analíticas de Big Data extraen millones de páginas web a la velocidad del rayo, evalúan algorítmicamente su “relevancia” o “coincidencia” con nuestra petición y muestran los resultados por orden de clasificación. En el caso de Google, por ejemplo, los sitios más destacados son los patrocinados (lo que permite a las empresas pagar por aparecer en los primeros puestos de los resultados de búsqueda), seguidos de los enlaces web ordenados según la relevancia determinada algorítmicamente por Google.

Si bien cada persona es libre de consultar todos los resultados que desee (de los cientos que la búsqueda arroja), en la práctica es probable que el usuario sólo visite los enlaces web de la primera o de las dos primeras páginas (Pasquale, 2006). De ahí que el comportamiento del usuario esté sujeto al efecto “cebo” de elegir “lo primero”, provocado por la configuración algorítmica en el diseño de las opciones, que trata de “empujar” la decisión de hacer clic sobre los enlaces favorecidos por el arquitecto de la elección. Para Google, esto implica dirigir el tráfico web en direcciones que promuevan un mayor uso de las propias aplicaciones a su vez de Google (aumentando así el valor del espacio publicitario patrocinado por la compañía).

Aunque el concepto de *nudge* es sencillo, los análisis de Big Data que utilizan *nudges* para la toma de decisiones lo hacen de forma muy compleja. Comparemos un simple *nudge* estático en forma de badén sobre la calzada y un *nudge* dinámico y altamente sofisticado basado en Big Data como el que utiliza la función de navegación de Google Maps. En ninguno de los dos casos se obliga al conductor a actuar de la manera que el arquitecto del *nudge* considera óptima: de haber obligación o prohibición tajante, no estaríamos en el ámbito del paternalismo libertario; aquí se trata sólo de sugerir o recomendar, no de coaccionar, y de mantener en todo caso la libertad de elección (Sunstein, 2017: 39). Cuando un conductor se acerca a un badén puede estar dispuesto a soportar las molestias y asumir los posibles daños al vehículo que se deriven de pasar por encima del bache sin modificar su conducta ni reducir la velocidad. Tampoco un conductor está obligado a seguir las “sugerencias” de Google Maps sobre la mejor ruta para llegar a su destino. Si el conductor no sigue la dirección sugerida, Google Maps simplemente recalculará su itinerario en relación con la nueva ruta que ha elegido el conductor mediante el análisis algorítmico de flujos de datos a tiempo real que rastrea tanto la ubicación del vehículo como la situación del tráfico que, según cálculos predictivos (estamos, por ejemplo, en “hora punta” de salida del horario laboral), afectarán a la rapidez con la que el usuario llegará al destino deseado.

Muchas formas estáticas de instrumentos reguladores se ejecutan por sí mismos, esto es, sin automatismos (como el badén) y evitan la necesidad de intervención humana más allá del momento en el que se diseña la regulación. Ello hace que el coste de implementar la medida sea relativamente bajo y que el objetivo perseguido por la norma –la reducción de la velocidad– se cumpla en un grado adecuadamente satisfactorio (Latour, 1994: 39-40). El problema de los instrumentos estáticos es que siguen operando aunque el efecto que provocan no sea el deseado en un momento determinado: por ejemplo, pueden instalarse badenes para aminorar la velocidad en momentos de tráfico denso; pero los badenes seguirán modificando la conducta de los conducto-

res incluso cuando el tráfico sea fluido y no fuera necesario aminorar la velocidad. Este tipo de efectos indeseados es el que intentan paliar los *nudges* como herramientas dinámicas y adaptativas al contexto decisorio a través de los sistemas de Big Data: que el “empujón” sólo opere modificando la conducta del individuo en determinados momentos en los que el arquitecto así lo ha diseñado. De esta forma, los *nudges* basados en sistemas de Big Data (*hypernudges*) permiten que los efectos de los “empujones” se desplieguen de forma dinámica en función de circunstancias previamente diseñadas, y que tanto la norma como su ejecución se actualicen y perfeccionen continuamente en un entorno en red que permite la retroalimentación de datos en tiempo real que, sobre todo, puede utilizarse para personalizar resultados algorítmicos posteriores (Degli Esposti, 2014).

El uso de *hypernudges* es, por tanto, una técnica de control regulatorio ágil, discreta y muy potente, que permite modificar de forma dinámica –según circunstancias previamente diseñadas por el arquitecto de la medida– la conducta de los destinatarios del “empujón” y, a su vez, devuelve información muy valiosa al poseedor de los datos –al arquitecto: normalmente una compañía tecnológica– acerca de cómo se comportan los usuarios cuando reciben distintas recomendaciones:

La IA podría ser, y ha sido, usada para este tipo de *nudge*, por ejemplo cuando Amazon hace recomendaciones de productos que afirma que yo debería querer comprar. De forma similar, Spotify parece afirmar que me conoce mejor de lo que yo mismo me conozco cuando me recomienda una música concreta. Estos sistemas de recomendación actúan como *nudges* en el sentido de que no limitan mi elección de libros o música, pero influyen en mi compra, mi lectura y mi comportamiento como oyente en la dirección sugerida por el algoritmo (Coeckelbergh, 2023: 31).

Estas técnicas de control de comportamiento humano que aúnan *nudge* y Big Data (*hypernudging*) se basan en formas de cribado y perfilado que se realiza sobre conjuntos de personas que se toman como muestras. Fruto de esa detección de comportamientos estandarizados procedentes de universos poblacionales analizados, el algoritmo puede adecuar sus respuestas a los patrones y gustos recopilados entre millones de resultados recogidos. Esa estandarización y homologación (y, a la larga, uniformización) de las opciones elegibles que lanzan los sistemas de Big Data (opciones que se han verificado como las preferidas por miles de usuarios que las han adoptado al recibir un determinado *nudge*), puede cercenar la riqueza y diversidad de la personalidad y, por tanto, de la propia identidad individual, pues en definitiva se va empobreciendo la capacidad de apertura a lo distinto y nuevo. Progresivamente se irá cerrando nuestro abanico de opciones retirándonos el acceso a otros

productos que podrían enriquecer nuestra personalidad. La hiperpersonalización de los resultados que visualizamos crea “filtros burbuja”³ que limitan nuestro horizonte: a la manera de una cámara de eco, el algoritmo devuelve continuamente la información que agrada al individuo, reforzando sus propias creencias y omitiendo las opiniones opuestas. Algo que a largo plazo y de forma casi imperceptible puede llegar a condicionar e incluso a definir desde fuera nuestras decisiones. El cultivo de la personalidad individual habría dejado de ser un asunto de autonomía moral para convertirse en una construcción diseñada heterónomamente desde instancias digitales.

3. LA CRÍTICA A LOS *HYPERNUDGES*

Aunque las políticas paternalistas suelen justificarse haciendo alusión a las amplias cotas de autonomía que dejan a salvo, tratando de hacer ver que es el individuo el que finalmente toma la decisión, ello no implica la total ausencia de interferencias ni la plena libertad personal. Allí donde se ejerce algún tipo de injerencia externa sobre el individuo, existe el riesgo de un uso y abuso que se extralimite más allá de los fines benevolentes inicialmente previstos que buscaban el bienestar de la persona. ¿Cómo debe entonces evaluarse la legitimidad de los *hypernudges* en una sociedad liberal y democrática cuyos principios se asientan sobre el ideal de la autonomía individual?

Para realizar este análisis conviene tener en cuenta dos consideraciones previas. En primer lugar, no se puede ignorar la enorme asimetría de poder entre las grandes compañías digitales globales y los usuarios individuales de sus servicios (Zuboff, 2015). En segundo lugar, la vigilancia y obtención de datos a través de sistemas de Big Data incide sobre millones de personas. A diferencia del badén, que solo afecta directamente a unos pocos vehículos en un momento dado al cruzar por encima, un único *hypernudge* implementado por Google o Facebook puede afectar directamente a millones de usuarios al mismo tiempo. De ahí que el riesgo de manipulación sobre la autonomía individual que ejerce un *hypernudge* sea de mayor alcance y magnitud que las fórmulas estáticas de paternalismo tradicional y, por tanto, nos requiera mayor atención y preocupación.

³ Pariser (2012) define los filtros burbuja como “el ecosistema personal de información que ha sido provisto por algoritmos”. Dichos algoritmos predicen y seleccionan la información que al usuario le podría interesar basándose en su información personal (su ubicación, historial de búsquedas o enlaces en los que hizo clic en el pasado). Como resultado, los usuarios son apartados de información que no concuerda con sus puntos de vista y se mantienen aislados en su sesgo informativo generando burbujas ideológicas y culturales. Pariser advierte que estos filtros burbuja “nos vuelven más cerrados a ideas y temas nuevos, y a información importante” y “crea la impresión de que nuestros limitados intereses son los únicos que existen”.

3.1. Contra el paternalismo libertario

Las críticas al paternalismo libertario y, en concreto, a su implementación en forma de *hypernudges*, han sido múltiples y se han recibido desde diferentes frentes. En conjunto, creo que dichas objeciones podrían agruparse bajo tres grandes bloques: (a) los *hypernudges* no persiguen el fin legítimo de mejorar la decisión del individuo; (b) los *hypernudges*, aunque persigan un fin legítimo, suponen una forma de manipulación de la autonomía; (c) los *hypernudges* no son transparentes en su diseño.

(a) Los *hypernudges* no persiguen el fin legítimo de mejorar la decisión del individuo. Varios críticos temen que los *hypernudges* se utilicen con fines dudosos o que escondan estrategias e intereses más allá de su función orientada a mejorar el contexto de elección del usuario. James Williams (2021) ha propuesto una triple distinción respecto a los medios de manipulación digital que dirigen nuestra voluntad: (1) distracciones digitales de la atención respecto al *hacer*: pérdida de concentración individual por los diseños e interfaces digitales orientados a distraernos; (2) distracciones digitales de la atención respecto al *ser*: dirigidas a hacernos perder nuestros valores y a asignar atención a lo que no la merece; y (3) distracciones digitales respecto al *conocer*, lo que Williams denomina la “distracción epistémica”, afectando a la reflexión, memoria, predicción, sosiego, lógica y la fijación de objetivos. El entorno digital perturba la racionalidad humana y la percepción real de nuestro entorno a través de las noticias falsas (*fake news*), la afectación de la inteligencia y las capacidades emocionales, generando estrés y otras patologías, promoviendo la indignación moral continua y conduciendo a la deshumanización y al populismo.

Consideremos el experimento llevado a cabo por Facebook para manipular las reacciones de sus usuarios ante distintas noticias que visualizaban. Algunos periódicos así lo titularon: “La polémica por la manipulación emocional de Facebook” (BBC, 30/06/2014); “Así manipuló Facebook las emociones de sus usuarios. Un estudio revela que la red social ha manipulado datos privados para estudiar y modificar nuestras reacciones hacia la página” (El País, 30/06/2014); “Facebook manipuló las cuentas de 700.000 usuarios para hacer un experimento psicológico” (ABC, 30/06/2014).

El ensayo consistió en manipular el algoritmo que selecciona las noticias que aparecen en el “muro” de cada usuario con el objeto de observar si existe un “contagio emocional” entre la comunidad. Para ello, los ingenieros enviaban deliberadamente a un grupo de usuarios noticias positivas y alegres mientras que a otro grupo se le proporcionaban noticias cargadas de connotaciones negativas. Y constataron que, efectivamente, los usuarios publicaban

mensajes positivos o negativos en función de los contenidos a los que habían sido expuestos. Los usuarios que observaban historias menos negativas en su “muro” fueron menos propensos a escribir un mensaje negativo, y viceversa. Por tanto, la influencia social dictamina nuestro estado de ánimo. El estudio concluyó que una menor exposición a posts de contenido positivo provoca una menor transmisión y comunicación de informaciones de esta índole.

Los críticos lo calificaron de experimento masivo de manipulación emocional y acusaron a Facebook de violar directrices éticas y legales al no notificar a los usuarios afectados que estaban siendo sometidos a un experimento. Facebook defendió su actuación como un intento legítimo de “mejorar nuestros servicios y hacer que el contenido que la gente ve en Facebook sea lo más relevante y atractivo posible” (Booth, 2014). Estamos, pues, ante un caso en el que un *hypernudge* no cumplía su función legítima de mejorar las elecciones de las personas, sino que se implementó tan solo para experimentar como si de un ensayo de laboratorio se tratara, utilizando para ello a los usuarios como cobayas.

(b) Los *hypernudges*, aunque persigan un fin legítimo, suponen una forma de manipulación de la autonomía. Para algunos críticos, estos incentivos, aunque se implementen para mejorar nuestras decisiones, para hacerlas más acertadas o para descubrir nuestros “verdaderos intereses”, explotan las debilidades cognitivas del individuo y vician la construcción de una voluntad humana auténticamente libre.

Los sesgos, atajos y miserias cognitivas nos remontan al problema, ya denunciado por Aristóteles, de la denominada “debilidad de la voluntad” (*akrasia*). El ejemplo clásico sería el de un Ulises que se ata al mástil para no ser vencido por el seductor cántico de las sirenas. El paternalismo, ante circunstancias que vician la voluntad, trataría de evitar que, siendo víctimas de tentaciones y arrebatos, nos dejemos arrastrar por impulsos irracionales o deseos transitorios y vehementes. Las medidas paternalistas buscarían reforzar la autonomía débil de un individuo que no cuenta con información completa o que puede haber errado al medir las consecuencias de su conducta: la persona parecería no saber lo que en verdad quiere o podría estar equivocada al no valorar con el peso adecuado lo realmente importante para su bienestar. El estagirita señaló que es a causa de la “debilidad de su convicción por lo que los que tienen opiniones obran más contra su modo de pensar que los que tienen un conocimiento” (2011: 151 [1146b]). Al no poseer conocimiento fiable de las consecuencias de nuestras decisiones, la elección puede ser errónea. En David Hume encontramos la formulación de las causas psicológicas de la aceptación de este paternalismo y nos brinda también los remedios para combatir esa “flaqueza de carácter” (2012: 466 y 467 [536 y 537]). Y, entre los

contemporáneos, ha sido Garzón Valdés quien ha defendido este tipo de paternalismo en el que “se procura combatir la debilidad de la propia voluntad” cuando “el Estado interviene para impedir que con su comportamiento el individuo lesione intereses propios a los que reconoce como más importantes que los deseos que motivan su conducta actual” (1988: 162)⁴.

Entre los opositores a esta forma de paternalismo el más contundente ha sido John Stuart Mill. El filósofo londinense intentó mostrar que, a pesar de que determinados actos pueden ocasionar daño al propio agente que se los inflige y, por ende, alguna ayuda externa podría evitarlos, esa interferencia social y jurídica sobre su conducta afecta a su autonomía de un modo más dañino que el mal que se intenta sortear con la medida paternalista. Ya sabemos que el “principio del daño” de Mill solo justificaría una interferencia externa sobre la voluntad del individuo si con ella se evitara un daño a otro: por el contrario, tratar de evitar un daño causado a sí mismo “no es justificación suficiente. Nadie puede ser obligado justificadamente a realizar o no realizar determinados actos porque eso fuera mejor para él” (Mill, 2013: 80). En definitiva, no cabe el paternalismo ni siquiera para mejorar el propio bienestar del individuo. La autonomía es un bien demasiado valioso como para sufrir manipulaciones o engaños. Es el propio individuo el que mejor conoce sus intereses y cualquier interferencia (i.e.: un *nudge*) en la búsqueda y construcción de su personalidad se reputa como una intromisión intolerable en el ejercicio de su autonomía (Delgado Rojas, 2021). Para la teoría política liberal clásica, las medidas paternalistas, aunque persiguieran el loable fin de mejorar la vida de los individuos, suponen una manipulación indebida de la autonomía personal, lo que convertiría a las técnicas regulatorias que las utilizan en ilegítimas.

(c) Los *hypernudges* no son transparentes en su diseño. Los profesores Pasquale y Bracha han estudiado en profundidad los sesgos que los motores de búsqueda generan cuando filtran y clasifican los sitios web al arrojar los resultados de una consulta. La ordenación de los resultados sigue criterios que inevitablemente estarán estructuralmente manipulados (diseñados para “gustar” a los usuarios y mantener una ventaja competitiva sobre las empresas rivales), generando así resultados sistemáticamente encaminados a promover intereses subyacentes del arquitecto de la decisión, que ha configurado el sistema algorítmico, distorsionando a su vez las decisiones de los usuarios, pues los resultados de la búsqueda no se ajustan a los intereses de los individuos sino a lo que el sistema de Big Data muestra con preferencia en los primeros lugares. La decisión de visitar una u otra página web (hacer clic) ha recibido

⁴ Garzón Valdés mantuvo un interesante debate sobre el concepto y justificación del paternalismo con Atienza (1988: 203-214). Para un análisis general del paternalismo desde la filosofía jurídica y política, vid. Alemany (2006).

un estímulo (*nudge*) que no persigue mejorar la decisión del usuario, sino socavar el ejercicio de su autonomía individual y seleccionar la opción interesada por el arquitecto (Pasquale y Bracha, 2015).

Las preocupaciones de Pasquale y Bracha reflejan la creciente demanda de mecanismos institucionales que puedan garantizar eficazmente la “responsabilidad algorítmica”, dado que cada vez se utilizan algoritmos más sofisticados para influir intencionadamente en las decisiones de los usuarios, pero que funcionan como “cajas negras”, interesadamente opacas para el escrutinio y control externo (Rauhofer, 2015). Aunque las técnicas de *hypernudging* varían en su nivel de transparencia (Bovens, 2008), su diseño a través de sistemas de Big Data suele estar integrado por complejos algoritmos de *machine-learning* que los hace aún menos transparentes y, en todo caso, difíciles de conocer y captar por los sistemas y organismos de regulación de mercados y lucha contra la concentración oligopolista y la competencia desleal. A pesar de ello, se han dado pasos en materia de control y vigilancia en el uso de la Inteligencia Artificial y el Big Data cuando estas tecnologías, combinadas con las técnicas de *nudging*, afectan al ejercicio y disfrute de los derechos fundamentales. Por su novedad y reciente creación citaré el caso de la *Agencia Española de Supervisión de la Inteligencia Artificial*, cuyo Estatuto, aprobado mediante Real Decreto 729/2023, de 22 de agosto, encomienda a este organismo “la supervisión de la puesta en marcha, uso o comercialización de sistemas que incluyan inteligencia artificial y, especialmente, aquellos que puedan suponer riesgos significativos para la salud, seguridad, la igualdad de trato y no discriminación”. Por su parte, el Comité de Ministros del Consejo de Europa, en una Declaración de febrero de 2019, ha alertado sobre el riesgo de manipulación a través de algoritmos aquí apuntado⁵ y en el Documento titulado *Towards Regulation of AI Systems* ha señalado que:

Hay que prestar especial atención al uso potencial de la IA en la interacción hombre-máquina para aplicar estrategias de *nudging*. En este caso, debido a la complejidad y oscuridad de las soluciones técnicas adoptadas, la IA puede aumentar el papel pasivo de los ciudadanos y afectar negativamente al proceso democrático de toma de decisiones (Ben-Israel *et al.*, 2020).

3.2. La notificación y el consentimiento como aceptación de la injerencia en la autonomía

Cabría preguntarse si, a través de la emisión de alguna forma de consentimiento, se podrían superar o vencer las críticas al carácter opaco y manipula-

⁵ *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, adopted by the Committee of Ministers on 13 February 2019 at the 1337 meeting of the Ministers’ Deputies.

dor de los *hypernudges*. Me referiré a tres posibles situaciones que contestarían afirmativamente a la posibilidad de aplicar determinados “empujones” bajo ciertas circunstancias: (a) para proteger a una persona incompetente o con facultades cognitivas disminuidas; (b) para asegurar el ejercicio de la autonomía futura; y (c) para remediar situaciones voluntarias de puesta en riesgo cuyas consecuencias no han sido correctamente medidas.

(a) Fue el influyente trabajo de Ernesto Garzón Valdés *¿Es éticamente justificable el paternalismo?* el que popularizó la figura del “incompetente básico”. Si el consentimiento legitima una intervención paternalista, en determinados casos hay que presumir otorgado aquel y aplicar la medida porque el individuo “en ese momento no está en condiciones de comprender el alcance de la misma”, es decir, es un incompetente. Por “competencia” debemos entender “la capacidad de una persona para hacer frente racionalmente o con una alta probabilidad de éxito a los desafíos o problemas con los que se enfrenta” (1988: 165). Carecer de esta competencia básica sería una condición necesaria aunque no suficiente para la justificación de medidas paternalistas: junto a la incompetencia, es preciso además que la intervención tenga un interés benevolente “con miras a superar los inconvenientes que trae aparejada la incompetencia básica para el propio incompetente, es decir, procurar que no se dañe a sí mismo” (1988: 167). Estas dos condiciones –constatación de la incompetencia básica y que la medida esté orientada a buscar el bienestar del incompetente– son necesarias y conjuntamente suficientes para la justificación del paternalismo.

En la revolución tecnológica en la que nos hallamos inmersos, el incompetente básico sería equiparable a todas aquellas personas que, fruto de las brechas digitales –sobre todo las causadas por edadismo y nivel educativo–, se han convertido en lo que suele denominarse “analfabetos digitales”: personas que presentan serios impedimentos para poder navegar por Internet, acceder a contenidos multimedia, relacionarse mediante redes sociales, crear y editar documentos, discriminar información relevante de la superflua u otorgar un consentimiento significativo y válido a las actividades de intercambio y tratamiento de datos que conllevan las técnicas analíticas de Big Data. Destacan las barreras insuperables a las que se enfrentan las personas en un panorama tecnológico en rápida evolución a las que se les invita a compartir sus datos personales para poder acceder a servicios digitales básicos, como por ejemplo pedir una cita médica. La mayoría de usuarios de la red ni leen ni comprenden las políticas de privacidad *online* que deben “aceptar” antes de acceder a los servicios digitales, y se estima que si una persona realmente las leyera, ello le consumiría 244 horas al año (McDonald y Cranor, 2008). Existen serias dudas de que el consentimiento dado por un “incompetente digital” se entienda

válidamente otorgado como permiso que autoriza la injerencia en la privacidad del sujeto (por ejemplo, consintiendo el usuario la cesión de sus datos personales).

(b) Otro motivo que puede justificar la aplicación de un *nudge* consiste en apelar a la noción de consentimiento futuro (*future-oriented consent*): el destinatario de la medida, aunque hoy no expresara su consentimiento, en el futuro agradecerá que se le haya aplicado. Son políticas paternalistas que buscan el consentimiento en un momento posterior al de la ejecución de la disposición. En el caso de Stuart Mill, la única excepción que propuso a su prohibición del paternalismo fue en el supuesto en el que, de no mediar la intervención paternalista, el individuo dejara de ser libre, ya que ello vedaría todo ejercicio futuro de la propia autonomía (2013: 222). Ante un caso de entrega voluntaria en esclavitud se justificaría una intervención paternalista ya que, de lo contrario, una vez convertido en esclavo se produciría la pérdida misma de la capacidad de elección para todo momento posterior (incluso para rescindir el contrato y decidir dejar de ser esclavo).

También el filósofo oxoniense Derek Parfit intentó articular, en el marco de su teoría de la identidad personal, un paternalismo respetuoso con la idea de preservar la autonomía futura. Para Parfit, es el hecho de querer proteger nuestra identidad en el tiempo (que podamos seguir siendo mañana el mismo sujeto moral que ahora somos) lo que nos da razones para interesarnos por nuestro futuro. Bajo esta preocupación por nuestra identidad futura, se intenta justificar un tipo de paternalismo que protege al “yo futuro” contra actos lesivos de su “yo presente”:

La autonomía no incluye el derecho a imponerse a sí mismo, por ninguna razón válida, un gran daño. Debemos evitar que nadie haga a su yo futuro lo que sería incorrecto hacer a otras personas (Parfit, 2004: 560).

Una impresionante variedad de estudios empíricos sobre la privacidad demuestran que las personas experimentan una incertidumbre considerable sobre qué pasará en el futuro con la cantidad de información revelada sobre su identidad (fotos, vídeos...) una vez “subida” a la red, debido a las dificultades para determinar las posibles consecuencias de la gestión de la propia privacidad y las inconsistencias que se agregan para la construcción de un consentimiento bien informado. Los estudios indican que las decisiones que las personas toman acerca de su privacidad se ven fácilmente influidas por motivos tan espurios como el diseño de una interfaz web atractiva, o por la dependencia generalizada que los usuarios adoptan ante las economías de red (“no puede ser malo si todo el mundo acepta”) o por participar de las costumbres y normas sociales (ante el riesgo de exclusión de tu “círculo” de amigos si

no se interactúa con ellos a través de redes sociales). Así, un elevado número de juristas especializados en Derecho de la información dudan seriamente de que la aceptación individual de los “términos y condiciones” ofrecidos por los proveedores de servicios digitales, que suele otorgarse haciendo clic en el enlace de una página web, constituya una renuncia significativa a los derechos que forman parte de la privacidad informativa (Solove, 2013). Se desconfía por ello que la injerencia hoy en la autonomía (con “recomendaciones” que implican cesión de datos personales) pueda encontrar el consentimiento que justifique la medida en un momento futuro.

(c) En tercer lugar, plantearé la posibilidad de justificar el uso de *hypernudges* para evitar daños de quien irracionalmente se pone en una situación de riesgo. Todos sabemos que existen actitudes temerarias sobre las que somos propensos a hacer caso omiso de los peligros eventuales que entraña su práctica, y que a menudo el placer que nos provoca llevarlas a cabo eclipsa los riesgos que conlleva su desarrollo. Si, dadas las circunstancias, el peligro de estas actividades fuera tan evidente, parecería adecuado conceder autorización a cierto tipo de “empujones” que desincentiven la realización de estas conductas arriesgadas y perjudiciales para el propio sujeto. No me estoy refiriendo ahora a aquellas medidas benevolentes que se dirigen a proteger el interés de personas sobre el presupuesto de su inmadurez, ignorancia o incompetencia. Ninguna filosofía política ha rechazado este tipo de paternalismo sobre el sujeto que no puede valerse por sí mismo y todas ellas, en mayor o menor grado, han admitido cierto ámbito de paternalismo justificado en relación con los usuarios tecnológicos que son menores de edad (pixelado de su imagen fotográfica), los adolescentes (impidiendo el acceso a portales de pornografía), los discapacitados (necesidad de un tutor legal para realizar trámites a través de la e-Administración) y, en general, sobre adultos claramente incapaces.

Pero cuando personas que no son incompetentes asumen tales riesgos, debemos suponer que lo hacen por una razón que estiman suficiente (Lyons, 1986: 176). Cuando valoramos su capacidad de regirse a sí mismos, nos comprometemos a respetar sus decisiones autónomas. Si, en cambio, menospreciamos las razones que tengan para llevar a cabo tal conducta arriesgada, los individuos pasan a convertirse en meros objetos manipulados para cumplir unos planes de ingeniería social. Un *nudge* que limitara de forma absoluta ciertas actividades porque sean peligrosas o poco saludables atentaría contra la libertad del individuo. Como dice Gerald Dworkin, “hay algunos riesgos –incluso muy grandes– que la gente tiene derecho a asumir en sus vidas” (1990: 160).

Para el asunto que nos concierne los inconvenientes surgen ante las dificultades de calibrar el daño dispuesto a asumir durante la navegación en Internet, pues su cuantificación –sobre todo en términos de violación de derechos como la privacidad– resulta bastante confusa. Las personas tienen dificultades para tomar decisiones informadas sobre su privacidad debido a problemas de racionalidad limitada y problemas de agregación: los usuarios luchan por gestionar su privacidad en la red con los cientos de proveedores de servicios digitales con los que interactúan en línea y les resulta difícil, si no imposible, evaluar adecuadamente el riesgo de daño en una serie de transacciones aisladas, dado que muchas de las posibles lesiones a la privacidad son de naturaleza acumulativa. Un *hypernudge*, ante estas patologías en las que el consentimiento puede estar viciado por falta de conocimiento, pretendería evitar la situación de quien irreflexivamente o, sencillamente, por incompreensión del lenguaje técnico utilizado, se embarca en una decisión que él mismo, si hubiera mediado un juicio certero e informado, descartaría por resultar contraria a lo que él considera sus intereses más importantes. Se justifica así la extensión del paternalismo sobre individuos que, aun siendo competentes, resultan propensos a tomar decisiones desafortunadas para sus propios intereses.

Pensemos, por ejemplo, en las leyes de protección de datos personales. Estas leyes se basan en lo que Daniel Solove denomina un modelo de “autogestión de la privacidad”, en el que la ley otorga a las personas un conjunto de derechos para que sean ellas mismas las que ejerzan el control sobre sus propios datos personales, pudiendo decidir por sí mismas cómo sopesar los costes y los beneficios de compartir, almacenar y procesar su privacidad (Solove, 2013: 1894). Este enfoque se basa en el paradigma de la “notificación y consentimiento”: el texto de las cláusulas legales aparece en una ventana emergente al entrar en el sitio web, su lectura se intenta que sea obligatoria (normalmente obligando a deslizar hasta el final la ventana para poder cerrarla) y sólo tras aceptar y dar el consentimiento se puede continuar accediendo a la página. Ahora bien, se han tratado de idear soluciones creativas que conviertan a estos *hypernudges* en herramientas que proporcionen avisos útiles e informativos a los usuarios, pues todos los sistemas tradicionales (normalmente de aceptación vía cookies) han resultado inadecuados.

Estos modelos de “autogestión de la privacidad” aún generan más problemas en entornos de sistemas de Big Data. En primer lugar, la “paradoja de la transparencia”, como la ha denominado Helen Nissenbaum, subraya que en el complejo entramado de datos que caracteriza actualmente al universo de Internet, las personas deben estar informadas sobre los tipos de datos que se recopilan, con quién se comparten y con qué fin, para otorgar un consentimiento suficientemente significativo. Pero proporcionar el nivel de detalle

necesario para permitir a los usuarios dar un consentimiento verdaderamente informado abrumaría incluso a los usuarios más expertos, porque las propias prácticas son volátiles, indeterminadas y queridamente confusas, ya que surgen nuevos proveedores y técnicas que aumentan constantemente los flujos de datos existentes (Barocas y Nissenbaum, 2014: 59; Nissenbaum, 2011).

No se debe perder de vista, asimismo, cómo el principal modelo de negocio, a través del cual se están monetizando los macrodatos, se aprovecha directamente de lo atractivo y poderoso que resulta para las personas el consumo de servicios aparentemente gratuitos. El modelo de negocio predominante para los servicios digitales es el del “trueque”: los usuarios aceptan revelar sus datos personales a las empresas a cambio de servicios “gratuitos” en lugar de “pagar” por ellos en otras empresas o plataformas. Sin embargo, como demuestra el economista conductual Dan Ariely (2009), “el poder de lo gratuito puede llevarnos a tomar muchas decisiones insensatas”.

En consecuencia, en un entorno de Big Data no se puede confiar en el modelo existente de la “notificación y consentimiento” para proteger el derecho a la privacidad, dado que normalmente se pide a los usuarios que otorguen su consentimiento al tratamiento de sus datos personales para fines que no han podido ser contemplados en condiciones de racionalidad y conocimiento informado.

4. DE LA TOTAL TRANSPARENCIA A LA VIGILANCIA TOTALITARIA

La privacidad, ese reducto de nuestra intimidad que no resiste nada bien las injerencias de terceros, nos permite mantener o hacer valer la identidad que queremos reservar para nosotros y la identidad que queremos proyectar hacia fuera. La privacidad permite controlar mi “yo” y, a su vez, expresar el “yo” que se desea transmitir al exterior. Hay, por tanto, una dualidad entre la identidad pública (cómo nos reconocen los demás, el “yo público”) y la identidad privada (cómo nos reconocemos a nosotros mismos, el “yo privado”). La tesis que mantendré es que este “yo privado” puede llegar a ser definido, no desde la autonomía de la persona, sino heterónomamente desde instancias digitales que controlan externamente nuestra identidad.

Este control ejercido sobre la privacidad puede ser comparado con otros enfoques sobre vigilancia como el sistema carcelario del “panóptico” que ideó Jeremy Bentham, la “sociedad disciplinaria” descrita por Foucault en *Vigilar y castigar* o la distopía totalitaria que plasmó George Orwell en *1984*. Byung-Chul Han (2014), por su parte, ha contemplado como factibles estos escena-

rios, pero los adapta a lo que él denomina la “psicopolítica digital” que no niega la libertad, sino que la explota al intervenir en el pensamiento y pronosticar el comportamiento de los individuos.

El panóptico digital del siglo XXI difiere del creado por Bentham, principalmente, en la perspectiva centralizada que caracterizaba a dicho sistema. Mientras que en el sistema ideado por el filósofo utilitarista inglés el vigilante, desde su posición, podría controlar cualquier espacio de las celdas, en el panóptico digital el poder disciplinario sobre los individuos “no es ejercido desde una única atalaya, sino que es móvil, multivalente e interno al propio tejido de nuestra vida diaria” (Downing, 2008: 83). Por ello, mientras los moradores del panóptico de Bentham son conscientes de la presencia constante del vigilante, los que habitan en el panóptico digital se creen que están en libertad (Han, 2013: 89).

Esta sensación de (falsa) libertad deriva de la hipercomunicación. A diferencia de los presos del panóptico original, en el contexto digital no se impone el aislamiento a las personas, sino que se promueve la interacción continua e intensa hasta llegar a la total transparencia. Continuando la metáfora, podemos llegar a considerar también que el Big Data es el nuevo vigilante carcelario, o el actual rostro del gran hermano orwelliano –ese ojo que todo lo ve– que lejos de ser una fuerza represiva y visible, ahora esconde su dominación bajo una careta que lo invisibiliza y oculta tras una *nube*. Cuanto más transparentes seamos, más fácil será vigilarnos:

Las tecnologías digitales ofrecen nuevos medios de vigilancia y manipulación que pueden apoyar o conducir al totalitarismo. (...) La IA no solo nos observa, sino que también realiza predicciones acerca de nuestro comportamiento. La IA y la ciencia de datos pueden convertirse así en un instrumento de nuevas formas de totalitarismo en las que la IA nos conozca mejor (y antes) que nosotros (Coeckelbergh, 2023: 106-107).

Los *hypernudges* empleados por los sistemas de Big Data constituyen una forma a través de las que operan estos mecanismos de vigilancia digital. A diferencia del control disciplinario del panóptico de Bentham, el control algorítmico del Big Data opera de una manera menos visible, pero más rápida y “seductora” gracias a continuos bucles de retroalimentación basados en las interacciones constantes de los usuarios (Cheney-Lippold, 2011: 169; Boyne, 2000). La forma de control resultante es más potente y poderosa que el tipo de control disciplinario que solía asociarse a las formas de vigilancia analógicas, que se basaban en la experiencia coercitiva de vivir con la incertidumbre y el miedo a ser observado. Sin embargo, este proceso es esencial para una forma emergente de capitalismo de la información que Shoshana Zuboff (2020) ha denominado “capitalismo de la vigilancia” dominado por poderosas empre-

sas transnacionales (“capitalistas de la vigilancia”), un sistema que engendró Google de la misma manera que Henry Ford y su modelo T de producción dio lugar al capitalismo de masas. Pero, a diferencia del capitalismo industrial, en el que el poder se identificaba con la propiedad de los medios de producción y que estuvo vigente durante el siglo XX, el “capitalismo de la vigilancia” que ha emergido en los albores del siglo XXI produce una nueva forma de poder: un poder que es ejercido ahora por un vigilante digital invisible que ostenta, además, la propiedad de los medios de modificación del comportamiento humano.

Zuboff ha ejemplificado bien el funcionamiento de este capitalismo de la vigilancia a través del algoritmo *News Feed* de Facebook. Victor Lukerson ha descrito también cómo este algoritmo se ha ido perfeccionando hasta llegar a ser “el cártel más valioso de la Tierra”, mostrando su evolución desde un algoritmo bastante tosco, basado en juicios esencialmente arbitrarios de ingenieros de software que asignaban puntuaciones a diferentes características de las publicaciones de Facebook para determinar su clasificación, hasta convertirse en un complejo sistema de *machine-learning* que proporciona una experiencia de usuario mucho más individualizada, en la que el algoritmo se adapta al comportamiento de los consumidores. Por ejemplo, las personas que hacen clic en más fotos verán luego en su “muro” mayor cantidad de imágenes, y las que consultan más contenido de tipo textual recibirán más cantidad de mensajes de ese tipo (Lukerson, 2015). Debido a que el usuario promedio de Facebook tiene acceso a alrededor de 1500 publicaciones por día pero solo mira 300, la mayoría ve solo una pequeña parte de las publicaciones potenciales en su red a diario: por lo tanto, la clasificación algorítmica determina de manera crítica cómo se filtran y resaltan estas publicaciones en los “muros” de los usuarios.

Este es el “capitalismo de la vigilancia” de Zuboff, ilustrado bien por Facebook, con fines que dicen ofrecer a sus usuarios un entorno informativo altamente personalizado y significativo, pero que en realidad utiliza un algoritmo diseñado para fomentar y consolidar a la compañía como el principal proveedor mundial de servicios de networking, asegurando y ampliando así su posición privilegiada y sus pingües beneficios. Por tanto, si estos *hypermudges* están siendo implementados para definir las emociones y decisiones de los usuarios por parte de las grandes corporaciones, esto significa la instrumentalización de las personas como medios para cumplir los fines de otros y ese es el camino que conduce –como nos lo mostró Arendt– a los orígenes del totalitarismo.

5. CONCLUSIONES

He intentado argumentar que las técnicas de orientación para la toma de decisiones basadas en sistemas algorítmicos de Big Data (*hypernudges*) pueden entenderse como un instrumento de control utilizado desde el campo de las políticas conductuales, y que funcionan como una potente forma de “empujón” que llega a condicionar el ejercicio de la autonomía personal.

El análisis algorítmico de los patrones de datos configura dinámicamente el entorno de elección del individuo de forma altamente personalizada, afectando al comportamiento y las percepciones de los usuarios al moldear sutilmente la comprensión del mundo digital que les rodea. Sus cualidades claramente manipuladoras, si no directamente engañosas, surgen de la explotación deliberada de las debilidades cognitivas sistemáticas que impregnan la toma de decisiones para canalizar el comportamiento en las direcciones preferidas por el arquitecto de la elección. He intentado argumentar acerca de la inadecuación del “culto al consentimiento” (Brownsword, 2004) en los entornos digitales, haciendo hincapié en los fallos sistemáticos de los usuarios a la hora de leer o comprender el significado y alcance de las políticas de privacidad *online*, lo que convierte al consentimiento en un “constructo vacío” (Bietti, 2020: 315). De modo que la acción de hacer clic en un sitio web para indicar la aceptación del usuario suele estar muy lejos de poder considerarse la autorización informada necesaria que permite la injerencia en los derechos fundamentales. A mi juicio, el paradigma de la “notificación y el consentimiento” no logra justificar plenamente la forma en que las técnicas algorítmicas de Big Data ejercen influencia sobre el comportamiento a través de la hiperpersonalización de los entornos de elección informativa de los individuos.

Las tecnologías de orientación digital de decisiones por Big Data tipo *hypernudges* están resultando difíciles de resistir para los individuos, ya que operan mediante una persuasión sutil más que mediante una coerción patente. Esa manipulación encubierta en la toma de decisiones de los individuos amenaza la libertad entendida como autonomía personal. Nuestra creciente sobreexposición digital continua nos hace partícipes de un proceso de hipervigilancia que amenaza, en última instancia, con empobrecernos intelectualmente. Al dejarnos vigilar sutilmente de forma constante, podemos estar erosionando lenta pero inexorablemente nuestra capacidad para llevar a cabo procesos auténticos de autonomía y desarrollo personal. A medida que nos replegamos cada vez más en nuestros propios “filtros burbuja” determinados algorítmicamente, nuestra exposición a experiencias compartidas, diversas e inesperadas, que son esenciales para un desarrollo de la personalidad rico y pleno, se ve correspondientemente disminuida. Si queremos evitar unas vidas

estrechas, planas, comercialmente preparadas y determinadas por algoritmos, debemos establecer restricciones más eficaces para “domesticar” el capitalismo de la vigilancia y los excesos manipuladores de los que intentan orientar las decisiones humanas a través de sistemas de Big Data.

Justificar el empleo de *hypernudges* de forma recurrente o excesiva implicaría, a mi juicio, tener que asumir, al menos, tres consecuencias indeseables difíciles de aceptar. Primera, habría que suponer –rechazando a Mill– que el arquitecto de la elección es quién mejor conoce nuestros intereses y sabe lo que más nos conviene (quiebra del ideal de la autonomía personal). Segunda, el paternalismo podría desembocar en una sociedad atrofiada, empujeñecida e infantilizada –en un *imperium paternale* como avisó Kant (2010: 274-275 [Ak. viii, 290-291]) o en el tocquevilliano *despotismo benevolente* (2002: 405)–, en la que los gigantes tecnológicos parecen proteger a sus usuarios con cuidados y medidas en lugar de que sean ellos mismos los que dirijan autónomamente sus vidas y asuman sus decisiones con responsabilidad. Lógicamente esa prestación de cuidados por parte de las compañías no es tan “gratuita y desinteresada” como pareciera y el coste de ello se paga en términos de vigilancia y pérdida de privacidad. Y tercera, como si de una pendiente resbaladiza se tratase, se puede entrar en una espiral paternalista que no conoce límites ni distingue entre una sociedad democrática que dispone determinadas políticas públicas que buscan el bienestar de los ciudadanos, y una sociedad digital, teledirigida e ideológicamente autoritaria que solo busca el beneficio del propio imperio tecnológico.

BIBLIOGRAFÍA

- ALEMANY, Macario (2006), *El Paternalismo jurídico*, Iustel, Madrid.
- ARIELY, Dan (2009), *Predictably irrational: The hidden forces that shape our decisions*, Harper Collins, London.
- ARISTÓTELES (2011), *Ética Nicomáquea*, Gredos, Madrid.
- ATIENZA, Manuel (1988), “Discutamos sobre paternalismo”, *Doxa*, 5, 203-214.
- AYRES, Ian (2010), *Carrots and Sticks: Unlock the Power of Incentive to Get Things Done*, Bantam Books, New York.
- BAROCAS, Solon y NISSENBAUM, Helen (2014), “Big Data’s end run around anonymity and consent”, en Lane, J. (ed.), *Privacy, Big Data and the public good* (pp. 44-75), Cambridge University Press, New York.
- BEMELMANS-VIDEC, Marie Louise *et al.* (1998), *Carrots, sticks, and sermons: Policy instruments and their evaluation*, Transaction Publishers, London.

- BEN-ISRAEL, Isaac *et al.* (2020), *Towards Regulation of AI Systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law*, Council of Europe.
- BIETTI, Elettra (2020), "Consent as a Free Pass: Platform Power and the Limits of Information Turn", *Pace Law Review*, 40, 310-398.
- BOBBIO, Norberto (1990), "La función promocional del Derecho", en *Íd.*, *Contribución a la Teoría del Derecho*, Ruiz Miguel, A. (ed.), Debate, Madrid.
- BOOTH, Robert (2014), "Facebook reveals news feed experiment to control emotions", *The Guardian*. Recuperado de: <https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds> [Última consulta: 14/11/23].
- BOVENS, Luc (2008), "The ethics of nudge", en Grüne-Yanoff, T. y Hansson, S.O. (eds.), *Preference change: Approaches from philosophy, economics and psychology* (pp. 207-219), Springer, Dordrecht.
- BOYNE, Roy (2000), "Post-panopticism", *Economy and Society*, 29, 285-307.
- BROWNSWORD, Roger (2004), "The cult of consent: Fixation and fallacy", *Kings College Law Journal*, 15, 223-251.
- CHENEY-LIPPOLD, John (2011), "A new algorithmic identity: Soft biopolitics and the modulation of control", *Theory, Culture & Society*, 28, 164-181.
- CLARKE, Ronald y NEWMAN, Graeme (eds.) (2005), *Designing out crime from products and system*, Criminal Justice Press, New York.
- COECKELBERGH, Mark (2023), *La Filosofía Política de la Inteligencia Artificial. Una introducción*, Cátedra, Madrid.
- COHEN, Julie E. (2012), *Configuring the networked self*, Yale University Press, New Haven.
- DEGLI ESPOSTI, Sara (2014), "When Big Data meets dataveillance: The hidden side of analytics", *Surveillance & Society*, 12, 209-225.
- DELGADO ROJAS, Jesús Ignacio (2021), *Ciudadanía liberal y moralismo legal*, Centro de Estudios Políticos y Constitucionales, Madrid.
- DOWNING, Lisa (2008), *The Cambridge Introduction to Michael Foucault*, Cambridge University Press, New York.
- DWORKIN, Gerald (1990), "El paternalismo", en Betegón, J. y De Páramo, J.R. (eds.), *Derecho y Moral. Ensayos analíticos* (pp. 147-161), Ariel, Barcelona.
- FAINI, Fernanda (2019), *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè, Milano.
- GARZÓN VALDÉS, Ernesto (1988), "¿Es éticamente justificable el paternalismo?", *Doxa*, 5, 155-173.
- GÜEMES, Cecilia (2021), "Políticas conductuales", *Eunomía. Revista en Cultura de la Legalidad*, 20, 310-321.

- HAN, Byung-Chul (2014), *Psicopolítica: neoliberalismo y nuevas técnicas de poder*, Herder, Barcelona.
- HAN, Byung-Chul (2013), *La sociedad de la transparencia*, Herder, Barcelona.
- HOOD, Christopher, ROTHSTEIN, Henry y BALDWIN, Robert (2001), *The government of risk*, Oxford University Press, Oxford.
- HUME, David (2012), *Tratado de la naturaleza humana*, Gredos, Madrid.
- KANT, Immanuel (2010), *En torno al tópico: eso vale para la teoría pero no sirve de nada en la práctica*, Gredos, Madrid.
- LATOURETTE, Bruno (1994), "On technical mediation - Philosophy, sociology, genealogy", *Common Knowledge*, 3, 29-64.
- LESSIG, Lawrence (1999), *Code and other laws of cyberspace*, Basic Books, New York.
- LUKERSON, Victor (2015), "Here's how Facebook's news feed actually works", *Time Magazine*. Recuperado de: <https://time.com/collection-post/3950525/facebook-news-feed-algorithm/#:~:text=The%20post%2Dtype%20is%20also,it%20in%20more%20people's%20feeds> [Última consulta: 14/11/23].
- LYONS, David (1986), *Ética y Derecho*, Ariel, Barcelona.
- MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth (2013), *Big data: la revolución de los datos masivos*, Turner, Barcelona.
- MCDONALD, Aleecia y CRANOR, Lorrie Faith (2008), "The cost of Reading privacy policies", *A Journal of Law and Policy for the Information Society*, 4, 540-565.
- MILL, John Stuart (2013), *Sobre la libertad*, Alianza Editorial, Madrid.
- NISSENBAUM, Helen (2011), "A contextual approach to privacy online", *Daedalus*, 140, 32-48.
- O'NEIL, Cathy (2018), *Armas de destrucción matemática: cómo el Big Data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid.
- O'REILLY, Tim (2013), "Open Data and Algorithmic Regulation", en Goldstein, B. y Dyson, L. (eds.), *Beyond transparency: Open data and the future of civic innovation* (pp. 289-300), Code for America Press, San Francisco.
- PARFIT, Derek (2004), *Razones y Personas*, Mínimo Tránsito - Antonio Machado Libros, Madrid.
- PARISER, Eli (2012), *The filter bubble*, Penguin Books, London.
- PASQUALE, Frank (2015), *The Black Box Society: The Secret Algorithms that control Money and Information*, Harvard University Press, Cambridge.
- PASQUALE, Frank y BRACHA, Oren (2015), "Federal search commission? Access, fairness and accountability in the law of search", *Cornell Law Review*, 93, 1149-1191.
- PASQUALE, Frank (2006), "Rankings, reductionism, and responsibility", *Cleveland State Law Review*, 54, 115-138.

- RAUHOFER, Judith (2015), "Of men and mice: Should the EU data protection authorities' reaction to Google's new privacy policy raise concern for the future of the purpose limitation principle", *European Data Protection Law Review*, 1, 5-15.
- SELINGER, Evan y SEAGER, Thomas (2012), *Digital jiminy crickets: Do apps that promote ethical behavior diminish our ability to make just decisions?*. Recuperado de: <https://slate.com/technology/2012/07/ethical-decision-making-apps-damage-our-ability-to-make-moral-choices.html> [Última consulta: 14/11/2023].
- SOLOVE, Daniel (2013), "Privacy self-management and the consent dilemma", *Harvard Law Review*, 126, 1880-1903.
- SUNSTEIN, Cass y THALER, Richard (2009), *Un pequeño empujón. El impulso que necesitas para tomar las mejores decisiones en salud, dinero y felicidad*, Taurus, Madrid.
- SUNSTEIN, Cass (2017), *Paternalismo libertario*, Herder, Barcelona.
- TOCQUEVILLE, Alexis (2002), *La democracia en América*, Alianza Editorial, Madrid.
- TVERSKY, Amos y KAHNEMAN, Daniel (1974), "Judgment under uncertainty: Heuristics and biases", *Science*, 185, 1124-1131.
- WILLIAMS, James (2021), *Clics contra la humanidad. Libertad y resistencia en la era de las distracciones tecnológicas*, Gatopardo, Barcelona.
- YEUNG, Karen (2017), "Hypertext: Big Data as a mode of regulation by design", *Information, Communication & Society*, 20, 118-136.
- ZITTRAIN, Jonathan (2008), "Tethered appliances, software as service, and perfect enforcement", en Brownsword, R. y Yeung, K. (eds.), *Regulating technologies* (pp. 125-156), Hart Publishing, Portland.
- ZUBOFF, Shoshana (2020), *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, Paidós, Barcelona.
- ZUBOFF, Shoshana (2015), "Big other: Surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology*, 30, 75-89.