Relaciones Internacionales
Número 40 • Febrero 2019 - Mayo 2019
Grupo de Estudios de Relaciones Internacionales
Universidad Autónoma de Madrid

Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional

Maximiliano Vila Seoane y Marcelo Saguier*

Resumen

El proceso de digitalización es un vector fundamental del capitalismo de datos, que está generando profundas implicancias en términos de nuevas formas de poder y asimetrías entre los actores de la política inter y transnacional. En Relaciones Internacionales, la ciberpolítica estudia las consecuencias de estos cambios. Mientras que en español hay pocas investigaciones sobre el tema, en inglés existe una amplia variedad de estudios, pero sin dimensionar la importancia del proceso de digitalización como parte de una nueva economía política global. En contraposición, en base a la literatura crítica de la economía política internacional en la tradición neogramsciana y de los estudios de ciencia y tecnología, argumentamos que el proceso de digitalización transforma las relaciones de producción, propiciando formas de gobernanza que expresan dinámicas de conflicto y cooperación en las que se pone en juego la construcción de nuevas configuraciones de un orden mundial digital. A partir de una revisión de la literatura en inglés, sostenemos el argumento al mostrar las dinámicas de conflicto y cooperación en cuatro áreas específicas de la ciberpolítica y las relaciones internacionales: ciberseguridad; gobernanza del comercio y de las finanzas globales; derechos humanos y ciudadanía en internet; y medioambiente.

Palabras clave

Ciberpolítica; digitalización; big data; hegemonía; capitalismo de datos.

Title

Cyberpolitics, digitalization and international relations: a critical political economy approach

Abstract

Digitalization is a fundamental vector of data capitalism, which is generating profound implications in terms of new forms of power and asymmetries between actors of inter and transnational politics. In International Relations, cyberpolitics studies the consequences of these changes. While there is little research on the subject in Spanish, in English there is a wide variety of studies, but without dimensioning the importance of the process of digitalization as part of a new global political economy. In contrast, based on the critical literature of international political economy in the neo-Gramscian tradition and the studies of science and technology, we argue that the process of digitalization transforms relations of production, fostering forms of governance that express dynamics of conflict and cooperation in which the construction of new configurations of a digital world order is at stake. Based on a review of the Anglophone literature, we support the argument by showing the dynamics of conflict and cooperation in four specific areas of cyberpolitics and international relations: cybersecurity; governance of trade and global finance; human rights and citizenship on the internet; and the environment.

Keywords

Cyberpolitics; digitalization; big data; hegemony; data capitalism.

***Maximiliano VILA SEOANE,** Becario posdoctoral de la Escuela de Política y Gobierno de la Universidad Nacional de San Martín (UNSAM), Buenos Aires, Argentina. Email: mvila@unsam.edu.ar

Marcelo SAGUIER, Investigador del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) de Argentina y Director de la carrera en Relaciones Internacionales de la Escuela de Política y Gobierno de la Universidad Nacional de San Martín (UNSAM). Email: msaguier@unsam.edu.ar

Recibido: 01/10/2018
Aceptado: 16/02/2018

Agradecemos los valiosos comentarios y sugerencias de dos de los revisores anónimos del texto.

DOI:
https://doi.org/10.15366/relacionesinternacionales2019.40.005

Formato de citación recomendado:
VILA SEOANE, Maximiliano y SAGUIER, Marcelo, "Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional", en *Relaciones Internacionales*, nº 40, 2019, pp. 113 - 131.

Introducción

Nos encontramos en un momento de transición hacia un capitalismo de datos[1], caracterizado por la acumulación de capital en base a la extracción, resguardo, análisis y (ab)uso de datos para distintos fines, liderado por pocas grandes empresas de internet especializadas en la oferta de productos y servicios[2]. El proceso de digitalización es un vector fundamental del capitalismo de datos en la medida en que la organización de la producción, las decisiones y las identidades están crecientemente ligadas a la generación, disponibilidad e interacción con grandes volúmenes de datos (conocido popularmente como *big data*) que pueden ser cuantificados y analizados para diversos fines[3]. La digitalización tiene profundas implicancias en términos de nuevas formas de poder y asimetrías entre los múltiples viejos y nuevos actores de la política inter y transnacional[4]. En efecto, estas nuevas capacidades tecnológicas se encuentran concentradas en pocas empresas líderes del sector ubicadas en Estados Unidos y China[5], y en menor medida, en Canadá, Israel, Rusia, y otros países europeos. Esta distribución desigual plantea enormes desafíos para los términos de inserción internacional de países y sociedades. Por ejemplo, se acrecienta el riesgo de profundizar históricos patrones de dependencia entre los países tecnológicamente avanzados y el resto. A esto se suman nuevas configuraciones de centro-periferia en el Sur Global, particularmente por ser China uno de los actores clave. De igual modo, la acumulación de datos por un conjunto reducido de empresas limita severamente el control ciudadano de los datos, facilitando nuevas modalidades de vigilancia y control con fines comerciales y geopolíticos, como así también de violación de derechos humanos como el derecho a la privacidad.

Debido a estos y otros aspectos problemáticos del actual proceso de digitalización, es indispensable comprender la relación entre la política y los cambios producidos por las nuevas tecnologías de la información y de la comunicación. Dos términos usualmente empleados en la literatura de ciencias sociales para referirse a esta relación son 'política de internet'[6] y 'ciberpolítica'. Si bien no hay consensos sobre el significado de este último término, que se derivan de las imprecisiones en torno a la definición de lo 'ciber', en este artículo adoptaremos ciberpolítica ya que el prefijo prevalece tanto en la literatura como en las discusiones actuales de Relaciones Internacionales. En particular, según Choucri la ciberpolítica „[...] se refiere a la conjunción de dos procesos o realidades: las relacionadas con las interacciones humanas (la política) que rodean la determinación de quién obtiene qué, cuándo y cómo, y las habilitadas por los usos del ciberespacio como un nuevo campo de discusión con sus propias modalidades y realidades"[7]. Esta definición es lo suficientemente abarcativa de las distintas contribuciones de diferentes ciencias sociales a la ciberpolítica. Sin embargo, proponemos que para las Relaciones Internacionales es importante focalizar el nivel de análisis en el conjunto de actores y procesos de cooperación y disputa de la

[1] En la literatura también se suele emplear el término 'capitalismo digital', sin embargo, optamos por este término porque hace una clara referencia al recurso central que se acumula en esta forma de capitalismo: los datos.

[2] SRNICEK, Nick, *Platform Capitalism*, Polity Press, Cambridge, 2016.

[3] MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth, *Big data. A revolution that will transform how we live, work and think*, Houghton Mifflin, Nueva York, 2013; MCAFEE, Andrew y BRYNJOLFSSON, Erik, "Big Data: The Management Revolution" en *Harvard Business Review*, Octubre, 2012.

[4] ZWITTER, Andrej. "Big Data and International Relations" en *Ethics & International Affairs*, n° 29/4, 2015, pp. 377-89.

[5] MCKINSEY & COMPANY, *Artificial Intelligence: the next digital frontier?*, MCKINSEY GLOBAL INSTITUTE, Discussion Paper, 2017: https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx [Consultado el 25 de julio de 2018]

[6] CHADWICK, Andrew y HOWARD, Phillip N (eds.), *Routledge Handbook of internet Politics*, Routledge, Londres, 2009.

[7] CHOUCRI, Nazli, *Cyberpolitics in International Relations*, The MIT Press, Cambridge, Massachusetts, 2012, p. 4.

política inter y transnacional sobre lo 'ciber'. Si bien no deja de ser una definición amplia, de esta forma se acota el objeto de estudio a las temáticas de la disciplina, excluyendo investigaciones de ciberpolítica de corte nacional.

Consideramos que las temáticas de la ciberpolítica constituyen un campo de gran importancia para la investigación académica y la política de las relaciones internacionales contemporáneas. En esta disciplina, la mayoría de la bibliografía sobre ciberpolítica es generada por investigadores e instituciones de países tecnológicamente avanzados en idioma inglés, que hace años exploran las distintas dimensiones de la agenda dinámica de la ciberpolítica, como los temas de ciberguerra o, más recientemente, la importancia de los datos[8]. La ciberpolítica también es de especial relevancia para países y sociedades dependientes tecnológicamente como es el caso en América Latina. Si bien existen varios estudios en español sobre ciberpolítica desde las ciencias políticas y la comunicación política[9], es aún escasa la investigación y publicación académica que aborde explícitamente la relación entre ciberpolítica y Relaciones Internacionales. Por ejemplo, en el caso de países de América Latina, las investigaciones existentes estudian las pocas iniciativas llevadas a cabo en la región relacionadas con la ciberpolítica, como la creación de un Marco civil de internet de Brasil y las iniciativas de ciberdefensa y ciberseguridad impulsadas por la Unasur[10]. Es decir, en la literatura hispanohablante falta desarrollo conceptual y amplitud de temas de investigación empíricos que permitan dimensionar las implicancias de los procesos de digitalización en curso, que consideramos de suma relevancia para entender las cambiantes configuraciones de poder internacional.

En este sentido, el objetivo del artículo es contribuir a este campo en gestación al realizar una revisión e interpretación de las principales áreas de debate sobre la ciberpolítica en la literatura en inglés, priorizando temáticas de interés para las Relaciones Internacionales. Entendemos que esta tarea es necesariamente exploratoria en la medida que no contamos con un campo de estudio consolidado, pero no deja de ser imprescindible para generar una agenda de investigación y de debate en español sobre ciberpolítica. En contraposición a la literatura existente que no analiza en suficiente detalle el proceso de digitalización como parte de una nueva economía política global, en este artículo argumentamos que el proceso de digitalización transforma las relaciones de producción, propiciando formas de gobernanza que expresan dinámicas de conflicto y cooperación en las que se pone en juego la construcción de nuevas configuraciones de un orden mundial digital, que son históricamente específicas de un capitalismo de datos.

Para desarrollar este argumento, en la primera sección introducimos un enfoque a la ciberpolítica basado en la literatura crítica de la economía política internacional en la tradición neogramsciana y de los estudios de ciencia y tecnología. A partir de este marco conceptual, en la segunda sección mostramos las dinámicas de conflicto y cooperación entre un conjunto de

[8] MADSEN, Anders Koed, FLYVERBOM, Mikkel, HILBERT, Martin, y RUPPERT, Evelyn, "Big Data: Issues for an International Political Sociology of Data Practices" en *International Political Sociology*, n°10/3, 2016, pp. 275-96; MAHRENBACH, Laura, MAYER, Katja y PFEFFER, Jürgen, "Policy visions of big data: views from the Global South" en *Third World Quarterly*, DOI:10.1080/01436597.2018.1509700 ; ZWITTER, Andrej. "Big Data and …, *op. cit.*.

[9] COTARELO, Ramón (ed.), *Ciberpolítica: las nuevas formas de acción y comunicación políticas,* Tirant Humanidades, Valencia, España, 2013; CHAMPEAU, Serge e INNERARITY, Daniel (comps.), *internet y el futuro de la democracia*, Paidós, Barcelona, 2012.

[10] ABDENUR, Adriana Erthal y PEREIRA DA SILVA GAMA, Carlos Federico, "Triggering the Norms Cascade: Brazil´s Initiatives for Curbing Electronic Espionage" en *Global Governance*, vol. 21, n° 3, 2015, pp. 455-74; ARANDA BUSTAMANTE, Gilberto, RIQUELME RIVERA, Jorge, y SALINAS CAÑAS, Sergio, "La Ciberdefensa Como Parte de La Agenda de Integración Sudamericana" en *Línea Sur*, vol. 9, 2015, pp. 100-116.

actores de relevancia en el campo de la ciberpolítica en cuatro áreas específicas de interés para las Relaciones Internacionales: ciberseguridad; gobernanza del comercio y de las finanzas globales; derechos humanos y ciudadanía en internet; y medioambiente, que son representativas —pero no las únicas— de las principales arenas en las que se manifiestan disputas por la construcción de un orden mundial digital. Por último, concluimos con la importancia de desarrollar el estudio de la ciberpolítica para indagar sobre sus implicancias en América Latina.

1. Marco conceptual para la ciberpolítica desde la literatura crítica de la economía política internacional

En esta sección introducimos el marco conceptual, que sugiere que el proceso de digitalización genera un profundo cambio en las relaciones de producción, tanto en término de tipos de empresas, formas de empleo como de consumo, que alteran las fuerzas sociales, propiciando nuevas formas de gobernanza y de disputas por el orden mundial digital en un capitalismo de datos.

Estos conceptos se inspiran en la literatura crítica de economía política internacional[11], que para comprender las estructuras en un período histórico determinado proponen estudiar empíricamente la relación dialéctica entre, primero, fuerzas sociales generadas por fuerzas sociales de producción, segundo, formas de estado, y tercero, diferentes tipos de orden mundial. Por ejemplo, una posible relación es que diferentes fuerzas sociales, debido a los cambios de las relaciones sociales de producción, puede llevar a antagonismos donde una clase establezca una hegemonía sobre el resto, capaz de modificar las formas de estado, y si alcanza suficiente proyección internacional, pueden alterar el orden mundial[12], que a su vez condiciona el accionar de otros estados. Según Robert W. Cox, cada nivel se puede comprender heurísticamente al analizar la relación dialéctica entre ideas, instituciones y capacidades materiales (incluyendo a las tecnológicas). En efecto, en el nivel de orden mundial, las perspectivas neogramscianas emplean el concepto de hegemonía, pero de una forma que difiere considerablemente de la visión de la perspectiva del Realismo en las relaciones internacionales, donde generalmente se trata de una cualidad de supremacía militar de un estado sobre otros. En cambio, la hegemonía en este enfoque es una forma de dominación por consenso de una fuerza social —no necesariamente restringida dentro de las fronteras de un estado-nación— sobre otras, producto de la aceptación de un conjunto de ideas, no sólo sustentadas por capacidades materiales, sino también por instituciones[13]. Por lo tanto, desde este enfoque la hegemonía tiene tanto una dimensión coercitiva como consensual. Otro aspecto importante de la relación dialéctica entre los tres niveles, es que incentiva al analista a estudiar estructuras contrahegemónicas —por más incipientes que sean— que cuestionen y tengan la posibilidad de modificar el orden hegemónico mundial[14].

Si bien la influencia de este enfoque en la literatura crítica de economía política internacional es considerable, no hay que soslayar que los conceptos empleados son también producto de un

[11] BIELER, Andreas y MORTON, Adam David, "A Critical Theory Route to Hegemony, World Order and Historical Change: Neo-Gramscian Perspectives in International Relations" en *Capital & Class*, vol. 28, n° 1, 2004, pp. 85-113; COX, Robert W., "Social Forces, States and World Orders: Beyond International Relations Theory" en *Millennium - Journal of International Studies*, vol. 10, n° 2, 1981, pp. 126-55; COX, Robert W., *Production, Power, and World Order: Social Forces in the Making of History*, Columbia University Press, Nueva York, 1987; GILL, Stephen, Power and Resistance in the New World Order, Palgrave Macmillan, Nueva York, 2008.

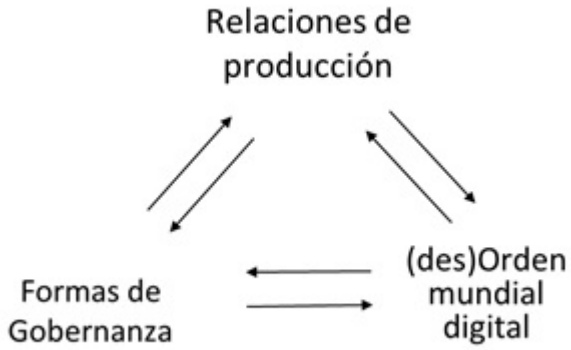
[12] COX, Rober W., Social Forces, States …, *op. cit.*, p. 138.

[13] *Ibídem*; ROBINSON, William I., "Gramsci and Globalisation: From Nation-State to Transnational Hegemony" en *Critical Review of International Social and Political Philosophy*, vol. 8, n° 4, 2005, pp. 559-74.

[14] COX, Rober W., Social Forces, States …, *op. cit.*, p. 144.

momento histórico particular. Por ende, también necesitan ser actualizados en base a las mutaciones del capitalismo. En esta dirección, en el artículo hablaremos de relaciones de producción, en vez de relaciones sociales de producción, y en formas de gobernanza en vez de formas de Estados. Estas modificaciones, que explicamos a continuación, conforman una nueva tríada de conceptos relacionados dialécticamente, ilustrados en la Figura 1, que extienden y actualizan el enfoque de inspiración Gramsciana, y que emplearemos para interpretar la literatura sobre ciberpolítica en Relaciones Internacionales.

Figura 1- Marco conceptual para comprender la literatura de Relaciones Internacionales sobre ciberpolítica.



Primero, la tecnología figura en la conceptualización original de Cox como un factor objetivo, influenciada por y que a la vez influencia a las fuerzas sociales[15], cuya dirección de cambio tecnológico es determinada por los actores con mayor 'poder social'. Sin embargo, esta conceptualización es muy limitada, pues, en línea con las tendencias en décadas previas a soslayar la importancia de la tecnología en los estudios de relaciones internacionales[16], la considera como algo externo y separado de lo social, no muy diferente de la concepción neorealista de Waltz[17]. En cambio, hace años que los estudios sociales de la ciencia y la tecnología abogan por el uso de ontologías que incluyan tanto a actores humanos, otros organismos biológicos y todo tipo de tecnologías a la par, evitando así realizar separaciones simplistas entre lo 'social' de lo 'técnico', o pensar que el grupo social con más 'poder' siempre determina la dirección del cambio tecnológico[18]. Por ende, y en línea con el creciente uso de esta literatura en relaciones internacionales[19], proponemos hablar de relaciones de producción en vez de relaciones sociales de producción, de forma tal de adoptar el abordaje empírico y relacional de los distintos enfoques de los estudios de ciencia y tecnología

[15] COX, Rober W., *Production, Power, and* …, *op. cit.*, p. 21.

[16] MAYER, Maximilian, CARPES, Mariana, y KNOBLICH, Ruth (ed.), "The Global Politics of Science and Technology: An Introduction" en *The Global Politics of Science and Technology*, Springer-Verlag, Berlin, 2014, pp. 1-35.

[17] MCCARTHY, Daniel R., "The meaning of materiality: reconsidering the materialism of Gramscian IR" en *Review of International Studies*, vol. 37, n° 3, 2010, pp. 1215-1234.

[18] BIJKER, Wiebe E., HUGHES, Thomas P. y PINCH, Trevor (ed.), *The Social Construction of Technological Systems*, The MIT Press, Cambridge, Massachusetts, 2012; FEENBERG, Andrew, *Questioning Technology*, Routledge, Abingdon, 1999; LATOUR, Bruno, *Reassembling the Social. An Introduction to Actor-Network Theory*, Oxford University Press, Nueva York, 2005.

[19] ACUTO, Michele y CURTIS, Simon (ed.), Reassembling International Theory: Assemblage Thinking and International Relations, Palgrave Macmillan, Hampshire, 2014; BALZACQ, Thierry y DUNN CAVELTY, Myriam, "A Theory of Actor-Network for Cyber-Security" en *European Journal of International Security*, vol. 1, n° 2, 2016, pp. 176-98; MCCARTHY, Daniel R., The meaning of …, *op. cit.*

en torno a las redes entre humanos y otros artefactos que se conforman en las nuevas relaciones de producción propiciadas por la digitalización.

Esta lectura del concepto de relaciones de producción es útil para investigar el accionar de los diversos dispositivos en nuestras vidas contemporáneas, que aparentan actuar de forma independiente o local, pero que en verdad son parte de vastas redes globales de elementos materiales y humanos, mantenidos por distintas prácticas, que pueden actuar a la distancia y trasladar las decisiones de política a los diseños tecnológicos[20]. Sin duda esta es la principal característica del ciberespacio[21], que no sólo incluye a internet, que suele ser definida como la red de redes entre múltiples actores, sino que también abarca a toda las infraestructuras físicas de la información y telecomunicación, códigos y protocolos de 'diálogo' entre máquinas, regulaciones e ideas sobre normativas. Esta estructura de red policéntrica y transnacional, tiene variadas implicancias para el estudio de la ciberpolítica en Relaciones Internacionales, por ejemplo, la dificultad de los estados en implementar decisiones unilaterales en el ciberespacio[22]. También es cierto que internet está enteramente construida por el ser humano[23], por ende, su estructura está en continua evolución, al igual que las amenazas transnacionales que habilita, como así también los marcos regulatorios para gobernarlo, que tienen una marcada debilidad para mantenerse actualizados.

Segundo, el concepto de formas de estado entiende al aparato burocrático estatal como ocupado en un determinado momento histórico por fuerzas sociales particulares, que pueden establecer múltiples configuraciones de relación con distintos actores sociales (por ejemplo, empresas, iglesia, medios de comunicación, etc.), y que pueden llegar a extender su influencia más allá del estado en cuestión a escala mundial[24]. Si bien esta conceptualización es superior a la idea de estado como una estructura unitaria, no es suficiente para comprender la creciente influencia en la política inter y transnacional de distintos tipos de actores y redes no estatales que se multiplicaron tras la acentuación del proceso de globalización desde los noventa, como empresas transnacionales, redes de activistas o de terroristas, etc. La especificidad de estas redes es que también construyen relaciones de forma transversal a los estados, sin necesariamente tener que alcanzar un control sobre los mismos para proyectarse a escala mundial[25]. Esto es evidente en internet, donde coexiste un gran abanico de actores 'antiguos' con nuevos, como la creación de cibercomandos por parte de los ejércitos de distintos estados o el surgimiento de empresas transnacionales de tecnología que en poco tiempo acumularon un poder y una influencia impresionante a nivel mundial. Asimismo, es importante destacar que la forma usual de entender a la gobernanza como un conjunto de reglas, normas y prácticas que incluyen, pero que van más allá del ámbito estatal, no deja de ser una visión de lo político desprovista de la dimensión tecnológica. En cambio, e inspirados también por la literatura de estudios de ciencia y

[20] NAHUIS, Roel y van LENTE, Harro, "Where Are the Politics? Perspectives on Democracy and Technology" en *Science, Technology, & Human Values*, vol. 33, n° 5, 2008, pp. 559-581.

[21] DEIBERT, Ron, ROHOZINSKI, Rafal, y CRETE-NISHIHATA, Masashi, "Cyclones in cyberspace: information shaping and denial in the 2008 Russia-Georgia war" en *Security Dialogue*, vol. 43, n° 1, 2013, pp. 3-24; MUELLER, Milton, MATHIASON, John y KLEIN, Hans, "The internet and Global Governance: Principles and Norms for a New Regime" en *Global Governance*, vol. 13, n° 2, pp. 237-254.

[22] CHOUCRI, Nazli, *Cyberpolitics in International Relations*, …, *op. cit.*

[23] BETZ, David J. y STEVENS, Tim, *Cyberspace and the State. Toward a Strategy for Cyber-Power*, Routledge, Londres, 2011.

[24] BIELER, Andreas y MORTON, Adam David, A Critical Theory …, *op. cit.*, pp. 87; COX, Robert W., Social Forces, States …, *op. cit.*, pp. 141.

[25] COX, Robert W. y SCHECHTER, Michael G., *The political economy of a plural world: critical reflections on power, morals and civilisation*, Routledge, Londres, 2002; ROBINSON, William I., "Gramsci and Globalisation …, *op. cit.*; SAGUIER, Marcelo y GHIOTTO, Luciana, „Las empresas transnacionales: un punto de encuentro para la Economía Política Internacional de América Latina" en *Desafíos*, vol. 30, n° 2, 2018.

tecnología, entendemos que la gobernanza es realizada también por intermedio de tecnologías, como algoritmos[26]. Por ende, optamos por hablar de formas de gobernanza, en vez de formas de estado, con el fin de capturar esta diversidad de configuraciones.

2. Ciberpolítica y Relaciones Internacionales

A continuación sintetizamos algunos de los principales debates de la literatura anglófona de Relaciones Internacionales en términos de ciberseguridad, gobernanza del comercio internacional y de las finanzas globales, derechos humanos y ciudadanía en internet, y medioambiente. Interpretamos la literatura a la luz de los efectos del proceso de digitalización en las relaciones de producción (tanto en término de tipos de empresas, formas de empleo como de consumo), que alteran las fuerzas sociales, propiciando nuevas formas de gobernanza y de disputas por el orden mundial. No pretendemos ser exhaustivos en la revisión, pero sí al menos examinar las expresiones de las principales tensiones en torno a un orden mundial en el capitalismo de datos.

2.1. Ciberseguridad

En términos conceptuales, la ciberseguridad, y en menor medida ciberdefensa y ciberguerra, son los términos que más se utilizan en referencia a la defensa de potenciales amenazas y/o al ataque en internet. Si bien no existen aún definiciones consensuadas sobre estos términos, ciberdefensa y ciberguerra son utilizados principalmente en contextos militares, mientras que el término ciberseguridad es más maleable, y también útil para referirse a la protección de sistemas informáticos en general. No obstante, hay una tendencia hacia una seguritización en el discurso de ciberseguridad[27], que lleva a que la perspectiva estratégica militar predomine, desplazando al ideal libertario original de los creadores de internet. En parte, esto se debe al rol pionero del ejército de Estados Unidos en adaptarse a las nuevas formas de producción propiciadas por la digitalización. Por ejemplo, en 2009, Estados Unidos creó el Cibercomando bajo el mando de la Agencia de Seguridad Nacional (NSA) para realizar operaciones defensivas y de ataque. Luego, en 2011 el Pentágono clasificó al ciberespacio como un nuevo campo de la guerra, junto con los tradicionales (aire, espacio, mar, y tierra), y en 2016 la OTAN hizo lo mismo. Por ende, las fuerzas sociales clave que analiza esta literatura de Relaciones Internacionales son los diferentes organismos militares y de inteligencia de los estados, en conjunto con las empresas y organizaciones relacionadas a la ciberseguridad, y más recientemente, a la inteligencia artificial.

La literatura en inglés sobre ciberseguridad mayoritariamente emplea un enfoque de 'resolución de problemas'[28], ya que procura contribuir al mantenimiento del orden hegemónico neoliberal[29] liderado por Estados Unidos, tanto por intermedio de técnicas de ataque y/o normas de gobernanza en internet. Por ejemplo, un tema de intenso debate es sobre si la ciberguerra ocurrirá o no[30]. Los autores de la literatura anglófona convencidos sobre el riesgo de las ciberarmas suelen

[26] ZIEWITZ, Malte, "Governing algorithms: myth, mess, and methods" en *Science, Technology, & Human Values*, vol. 41, n° 1, pp. 3-16.

[27] DUNN CAVELTY, Myriam, "From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse" en *International Studies Review*, vol. 15, n° 1, 2013, pp. 105-122.

[28] COX, Robert W., Social Forces, States …, *op. cit.*

[29] Cabe resaltar que esta aseveración es válida para la literatura previa a la asunción de Trump, que antecede a las discusiones contemporáneas sobre la crisis del orden mundial neoliberal.

[30] LYNN III, William J., "Defending a New Domain. The Pentagon's Cyberstrategy" en *Foreign Affairs*, 2010: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain [Consultado el 20 de abril de 2018]; JUNIO, Timothy J., "How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate" en *The Journal of Strategic Studies*, vol. 36, n° 1, pp. 125-133; RID, Thomas, "Cyber war will not take place" en *The Journal of Strategic Studies*, vol. 35, n° 1, 2012, pp. 5-32; VALERIANO, Brandon y MANESS, Ryan C., *Cyber*

repetir los conocidos patrones de análisis desde enfoques teóricos del Realismo, que acusan a países como China o Rusia de ser amenazas al orden mundial. Tal es el caso de Adam Segal[31], que asevera que China, con el fin de alcanzar la punta en el desarrollo tecnológico de sus industrias, apoya campañas sistemáticas de ciberespionaje contra empresas de Estados Unidos y organismos estatales para robarles su propiedad intelectual y otros datos de valor estratégico. En la misma línea, a Rusia se le atribuyen sofisticados ataques de 'guerra híbrida', que suelen contemplar una mezcla de ciberataques, campañas de desinformación, y uso de soldados camuflados, como en los casos de Estonia y Georgia[32], Ucrania, y las elecciones de Estados Unidos de 2016.

Cabe resaltar un hito que aceleró el interés por el estudio académico de la ciberseguridad desde la perspectiva de la seguridad internacional: el caso del malware conocido como StuxNet[33], un claro ejemplo de ciberarma. Este malware, supuestamente creado por los servicios de inteligencia de Estados Unidos e Israel, fue el desarrollo más sofisticado conocido hasta el momento, que logró sabotear los sistemas informáticos de la central nuclear de Natanz, Irán, sin recurrir a un ataque militar convencional. Lo original de StuxNet es que fue diseñado para atacar al software que controla procesos industriales, y específicamente centrifugadoras nucleares. Es decir que las líneas de código del malware provocaron un daño físico considerable, un hecho inédito hasta el momento. A pesar de alcanzar su objetivo, StuxNet también infectó a otras organizaciones que usaban sistemas similares a los de la central nuclear iraní, hecho que generó consternación en la comunidad dedicada a la ciberseguridad por el riesgo de provocar daños mayores más allá de sus objetivos militares iniciales.

Estas tendencias ilustran la capacidad coercitiva de la hegemonía de Estados Unidos y sus fuerzas sociales en el orden mundial del capitalismo de datos. En efecto, los riesgos de las ciberarmas son particularmente altos en las 'infraestructuras críticas', concepto impreciso que suele abarcar todo tipo de industria o sector que si sufriera un ciberataque representaría una amenaza severa al funcionamiento normal de las sociedades, ya sea civil o militar (por ejemplo, bancos, base de datos de seguridad social, plantas de energía nuclear, transporte, etc.)[34]. Ya no se trata de meros escenarios prospectivos, dado que acontecieron varios casos que demuestran el daño que las ciberataques[35] pueden causar en las sociedades contemporáneas en proceso de digitalización, como el reciente ataque mundial del ransomware WannaCry. Este malware, supuestamente creado por Corea del Norte en base a filtraciones de las ciberarmas desarrolladas por la NSA, produjo daños físicos considerables al paralizar los sistemas de empresas, reparticiones estatales, hospitales e individuos en todo el mundo.

Como toda hegemonía, el orden en internet también se basa en una dimensión de

War versus Cyber Realities: Cyber Conflict in the International System, Oxford University Press, Oxford, 2015.

[31] SEGAL, Adam, "The Code Not Taken: China, the United States, and the Future of Cyber Espionage" en *Bulletin of the Atomic Scientists*, vol. 69, n° 5, 2013, pp. 38-45.

[32] SLOAN, Elinor C., Modern Military Strategy: An Introduction, Routledge, Abingdon, 2012, pp. 88.

[33] KELLO, Lucas, The virtual weapon and international order, Yale University Press, New Haven, 2018;

[34] DEIBERT, Ron, ROHOZINSKI, Rafal, y CRETE-NISHIHATA, Masashi, Cyclones in cyberspace …, *op. cit.*; LEWIS, Ted G., *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, John Wiley & Sons, New Jersey, 2015.

[35] Cuando se habla de 'ciberarmas', los analistas se refieren a malware, que es un concepto que abarca al software con alguna finalidad maliciosa que busca provocar un cierto tipo de daño en otros sistemas o softwares. Hay varios tipos de malware, entre ellos se destacan: gusanos, ransomware, rootkits, troyanos, y virus.

cooperación o consenso. En efecto, Estados Unidos es el impulsor del modelo de múltiples partes interesadas (o en inglés *multistakeholder*) para la gobernanza de internet[36]. Esta forma de gobernanza suele ser considerada un modelo más democrático que otros (organizaciones multilaterales donde sólo intervienen estados), ya que incluye a actores estatales, privados, de la sociedad civil, organismos internacionales y comunidades técnicas, entre otros, a la par en los procesos de decisión. No obstante, no es secreto que las principales empresas y organizaciones de gobernanza de internet suelen estar localizadas en Estados Unidos, por ende, las ideas e intereses de estas organizaciones tienen una influencia superior a las de otros países en el desarrollo de internet y en los procesos de digitalización. Por ende, la promesa del modelo de múltiples partes interesadas, a pesar de su intención democrática, no altera la dinámica de poder que privilegia el rol de los estados y empresas transnacionales, en particular las de Estados Unidos[37]. El ejemplo más emblemático de esto es la internet Corporation for Assigned Names and Numbers (ICANN), una organización sin fines de lucro con base en Los Ángeles, encargada hasta 2016 de administrar los nombres de dominio de internet directamente en representación del Departamento de Comercio de los Estados Unidos. Durante años, esto fue motivo de disputa con iniciativas de otros países que buscaban transferir tal responsabilidad a las Naciones Unidas, a fin de evitar que prevalezcan las preferencias de Estados Unidos sobre las del resto de los países, tensión que persiste a pesar de los cambios recientes en ICANN[38].

Si bien Estados Unidos y sus fuerzas sociales conservan el liderazgo en la construcción de una hegemonía en el capitalismo de datos, no está exento de desafíos contrahegemónicos[39], que se acentuaron tras las revelaciones de Snowden. Cabe recordar que el ex agente de la NSA expuso programas de cibervigilancia masiva de Estados Unidos y sus aliados en cooperación con empresas transnacionales de tecnología, dejando en evidencia profundas contradicciones con el discurso de una internet libre y democrática que emana de países occidentales. No obstante, las revelaciones no produjeron cambios en estas prácticas, al contrario, en vez de prohibirlas, los cambios en términos de políticas públicas en los países occidentales fueron más bien en la dirección de legalizarlas[40]. Ante este escenario, China indirectamente acusa a Estados Unidos de tener una 'ciberhegemonía' en internet, por no respetar la 'cibersoberanía' de otros estados. En base a esta lectura, no es de extrañar que China use sus crecientes capacidades económicas y tecnológicas para competirle a Estados Unidos a la par en términos de ciberseguridad, vigilancia electrónica[41], y más recientemente, en inteligencia artificial. Otro ejemplo de esta competencia contrahegemónica es por el establecimiento de normas para gobernar los conflictos en el ciberespacio[42]. Las propuestas de la Organización de Cooperación de Shanghái para limitar el

[36] Cabe resaltar que en esta sección nuestras observaciones se limitan a la intersección entre ciberseguridad y gobernanza de internet, y no a todas las otras connotaciones que suelen ser debatidas bajo este último término. sin duda, una de las más empleadas hace referencia al proceso del Foro de Gobernanza de internet.

[37] CARR, Madeline, "Power Plays in Global internet Governance" en *Millennium: Journal of International Studies*, vol. 43, n° 2, 2014, pp. 640-59.

[38] JACKSON, Susan T., "A Turning IR Landscape in a Shifting Media Ecology: The State of IR Literature on New Media" en *International Studies Review*, 2018, DOI: 10.1093/isr/viy046

[39] EBERT, Hannes y MAURER, Tim, "Contested Cyberspace and Rising Powers" en Third World Quarterly, vol. 34, n° 6, 2013, pp. 1054-74.

[40] POHLE, Julia y VAN AUDENHOVE, Leo, "Post-Snowden internet policy: between public outrage, resistance and policy change" en *Media and Communication*, vol. 5, n° 1, 2017, pp. 1-6.

[41] VILA SEOANE, Maximiliano, "Digitalización, automatización y empresas transnacionales de seguridad privada en áreas con capacidad estatal limitada" en *Revista de Relaciones Internacionales, Estrategia y Seguridad*, vol. 13, n°2, 2018.

[42] FINNEMORE, Martha y HOLLIS Duncan B., "Constructing Norms for Global Cybersecurity" en *The American Journal of International Law*, vol. 110, n° 3, 2016, pp. 425-79.

uso de ciberarmas van en ese sentido, pero no es de extrañar que no hayan prosperado, pues Estados Unidos entiende tales normas como un límite a la libertad de expresión en internet y a su capacidad de realizar ciberataques[43]. Como respuesta a estas iniciativas contrahegemónicas, el Centro de Excelencia en Cooperación en Ciberdefensa de la OTAN ya elaboró dos versiones del Manual de Tallin, escrito con el fin de adaptar e internacionalizar su interpretación sobre derecho internacional para conflictos en el ciberespacio.

2.2. Gobernanza del comercio digital y de las finanzas

Los cambios que el proceso de digitalización genera en las formas de producción también están modificando el comercio y las finanzas, propiciando una transición a economías digitales.

Por un lado, la discusión actual es cómo regular el 'comercio digital'. Este concepto, que no tiene una definición consensuada, suele referirse al conjunto de transacciones realizadas por intermedio de portales y nuevas formas de comunicación, que gracias al incremento del flujo transfronterizo de datos y a la automatización (por ejemplo, algoritmos y robótica) aceleran el comercio internacional de bienes y servicios[44]. Cabe resaltar que las transacciones de datos son centrales en el comercio digital, pero son un tipo de transacción claramente diferente al intercambio de productos o servicios, ya que no existe consentimiento ni pagos por su flujo transfronterizo, y no obstante, tal flujo de datos es imprescindible y de enorme valor para el capitalismo de datos[45]. Si bien hay varios actores en estas cadenas de valor global, las empresas transnacionales (ETN) de tecnología de Estados Unidos (Amazon, Apple, Facebook, Gmail y Microsoft) y en menor medida de China (Alibaba, Baidu y Tencent) son los más influyentes, pues son una especie de 'infraestructura pública privatizada' y transnacional[46], pioneras en establecer las nuevas formas de producción en la era digital, y en parte, responsables por sus efectos negativos en términos de derechos humanos. Por ejemplo, la continua desterritorialización de las formas de trabajo, serían impensables sin las innovaciones de las ETN, como la oferta de servicios en la 'nube' que permite acceder a documentos, correos, y todo tipo de datos desde varios dispositivos y en cualquier momento, siempre que se cuente con acceso a internet. No obstante, el accionar de estas ETN no está exento de críticas[47]; por ejemplo, se las acusa de ser los nuevos monopolios del siglo XXI, que deben ser regulados a fin de evitar la concentración de mercado, o en particular, su tendencia a evadir impuestos.

En respuesta, las ETN responden que la concentración monopólica en el área digital es necesaria para ofrecer bienes globales que de otra forma serían difíciles de producir. Asimismo, las empresas estadounidenses realizan lobby tanto en Estados Unidos como en Europa para que

[43] MAURER, Tim, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security", Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf [Consultado el 20 de julio de 2018].

[44] LÓPEZ-GONZÁLEZ, Javier, y JOUANJEAN, Marie-Agnès, "Digital Trade: Developing a Framework for Analysis", OECD, OECD Trade Policy Paper n° 205, 2017.

[45] AARONSON, Susan, "Shifting focus to data type: How Canada can lead the global data economy", https://www.cigionline.org/events/shifting-focus-data-type-how-canada-can-lead-global-data-economy [Consultado el 5 de junio de 2018]

[46] PLANTIN, Jean-Christophe, et. al., "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook" en *New Media & Society*, vol. 20, n° 1, 2016, pp. 293-310.

[47] AARONSON, Susan, "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security" en *World Trade Review*, vol. 14, n° 4, 2015, pp. 671-700; DE FILIPPI, Primavera y MCCARTHY, Smari, "Cloud Computing: Centralization and Data Sovereignty" en *European Journal of Law and Technology*, vol. 3, n° 2, 2012, pp. 1-18.

las reglas de la economía y el comercio digital estén en sintonía con sus intereses económicos[48]. Particularmente, buscan impedir que otros estados implementen restricciones al libre flujo de datos entre fronteras (por ejemplo, requisitos de localización de datos en los países donde operan), argumentando que tales políticas restringen la libertad de acceso a internet. En cambio, los países que se inclinan por estas medidas sostienen que es indispensable implementar nuevas formas de regulación para asegurar que la digitalización propicie modelos de desarrollo en defensa de sus industrias nacionales y/o por motivos de ciberseguridad. En definitiva, lo que está en disputa son las formas de gobernanza de estas ETN, que ponen bajo presión las estrategias de desarrollo digital estatal.

Por el otro lado, el sistema financiero global también está en proceso de mutación causado por la digitalización de los procesos de producción, tendencia conocida en la industria financiera como FinTech. Las criptomonedas, como el Bitcoin, son uno de los casos más recientes de nuevas innovaciones tecnológicas en el sector. Estas monedas digitales se basan en la tecnología *blockchain*[49], que permite resguardar e intercambiar valor en redes encriptadas, descentralizadas y transnacionales, conformadas por diferentes actores, como tecnólogos, inversores, aficionados, ciudadanos, pero también evasores y criminales de todo el mundo, propiciando una nueva forma de realizar y de especular con transacciones financieras. En su expresión más radical, estas nuevas formas digitales de intercambiar valor están inspirando la creación de 'naciones sin fronteras', como Bitnation, como así también la ejecución de contratos inteligentes (*smart contracts*), que avecina una gobernanza descentralizada por algoritmos. Estos procesos de descentralización impactan directamente sobre los intermediarios dominantes de las finanzas globales (empresas como J.P. Morgan, bancos centrales y privados), ya que estas nuevas estructuras descentralizadas de flujos de dinero y de valor no están bajo su control, causando nuevos dilemas para la estabilidad del sistema financiero global y para la lucha contra el lavado de dinero[50]. Esto explica el surgimiento de iniciativas por parte de estados y empresas para apropiarse de la tecnología *blockchain*, revirtiendo así la pérdida de control causada por iniciativas transnacionales de actores civiles. En síntesis, *blockchain* ejemplifica el surgimiento de una nueva forma de gobernanza transnacional, que tiene el potencial de alterar considerablemente el orden mundial del capitalismo de datos.

2.3. Derechos humanos y ciudadanía en internet

La digitalización de las sociedades contemporáneas está provocando múltiples impactos en las ideas y prácticas preexistentes sobre ciudadanía y protección de los derechos humanos.

En términos de derechos humanos, uno de los problemas principales es la amenaza a la privacidad de los ciudadanos, provocado tanto por la inseguridad ocasionada por el cibercrimen[51], como por el excesivo uso de dispositivos capaces de producir trazas electrónicas minuciosas de

[48] AZMEH, Shamel, y FOSTER, Christopher, The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements, London School of Economics and Political Science , Working Paper Series, n° 16-175, 2016: http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf [Consultado el 5 de Mayo de 2018]

[49] DE FILIPPI, Primavera y WRIGHT, Aaron, *Blockchain and the Law: The Rule of Code*, Cambridge, Harvard University Press, 2018; DIERKSMEIER, Claus y SEELE, Peter, "Cryptocurrencies and business ethics" en *Journal of Business Ethics*, vol. 152, n° 1, 2018, pp. 1-14.

[50] CAMPBELL-VERDUYN, Malcolm. y GOGUEN, Marcel, "The mutual constitution of technology and global governance: Bitcoin, blockchains, and the international anti-money-laundering regime" en CAMPBELL-VERDUYN, Malcolm (ed.) *Bitcoin and beyond: cryptocurrencies, blockchains, and global governance*, Routledge, Londres, 2017.

[51] HOLT, Thomas J. y BOSSLER, Adam M., "An assessment of the current state of cybercrime scholarship" en *Deviant Behavior*, vol. 35, n° 1, 2014, pp. 20-40.

nuestras interacciones con otros humanos y máquinas, que les permite a las empresas generar perfiles precisos sobre consumo, preferencias políticas, desplazamientos, etc.[52]. Las fuerzas de seguridad y de inteligencia de los estados consideran que la recolección de estas grandes bases de datos - en colaboración con el sector privado - es indispensable para evitar amenazas contemporáneas, como el terrorismo o el crimen organizado, y suelen justificar a estas prácticas al afirmar que si un ciudadano no tiene nada que ocultar, tampoco tiene nada que temer del análisis de sus datos y metadatos[53]. Sin embargo, tras las revelaciones de Snowden sobre el uso indiscriminado y desproporcional de las capacidades de espionaje por parte de Estados Unidos en colaboración con otros estados, los argumentos empleados para justificar la vigilancia masiva están puestos seriamente en duda[54]. Esto no es un tema nuevo en relaciones internacionales, de hecho, ya en los noventa Der Derian[55] identificó el rol estratégico de la vigilancia para disciplinar y normalizar comportamientos de otros, pero sí lo es la variedad, velocidad y el volumen (*big data*) de datos que se pueden obtener de poblaciones enteras en el capitalismo de datos. Es decir que las prácticas actuales coercitivas de ciberespionaje y cibervigilancia confirmaron y superaron las especulaciones y preocupaciones de décadas previas.

Otro desafío tiene que ver con la regulación de los impactos del creciente poder de las empresas transnacionales de tecnología en términos de derechos económicos, políticos y sociales. En particular, estas transnacionales tienen la capacidad de hacer políticas públicas a la distancia por intermedio de algoritmos que suelen ser poco transparentes[56], y que pueden impactar en las condiciones de trabajo de sus usuarios. Por ejemplo, muchas de estas empresas coordinan la oferta y el consumo de productos o servicios de forma digital y global, sin necesariamente operar físicamente en jurisdicciones extraterritoriales, generando disrupciones considerables en sectores que hasta hace poco estaban inmunes a la digitalización. El ejemplo más contundente es la incursión de Uber en el sector del transporte, cuya rápida expansión global estuvo acompañada por un desdén a cumplir las regulaciones locales en los países donde opera, provocando conflictos con sindicatos que ven sus derechos laborales amenazados, y actores estatales que tienen una capacidad restringida de regular a estas empresas. Otro caso emblemático reciente es el de Cambridge Analytica, que en base a las laxas políticas de protección de datos de Facebook, recolectó y manipuló información personal de los usuarios para distribuir propaganda política en diferentes elecciones, como en Argentina, Kenia y el Reino Unido.

Asimismo, la creciente importancia de las empresas transnacionales en ofrecer todo tipo de servicios está teniendo impactos significativos en términos de ciudadanía. En efecto, nuestras identidades están crecientemente intermediadas por algoritmos y datos, que circulan por distintas plataformas privadas de internet, que definen la estructura tecnológica de operación de sus

[52] BALL, Kristie, HAGGERTY, Kevin, y LYON, David, (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, Nueva York, 2012.

[53] Se refiere a datos sobre los datos, por ejemplo, con qué números de teléfono se contactó una línea específica. Si bien esto no expone el contenido de las comunicaciones, sí revela la red de contactos de la línea espiada, información muy valiosa en términos de inteligencia.

[54] BERNAL, Paul, "Data Gathering, Surveillance and Human Rights: Recasting the Debate" en *Journal of Cyber Policy*, vol. 1, n° 2, 2016, pp. 243-64.

[55] DER DERIAN, James, "The (S)pace of International Relations: Simulation, Surveillance, and Speed" en *International Studies Quarterly*, vol. 34, n° 3, 1990, pp. 295-310.

[56] DENARDIS, Laura, y HACKL, Andrea M., "internet Governance by Social Media Platforms" en *Telecommunications Policy*, vol. 39, n° 9, 2015, pp. 761-770; BURKHARDT, Wolf, "Big Data, Small Freedom? Informational Surveillance and the Political" en *Radical Philosophy*, vol. 191, n° 191, 2015, pp. 13-20.

plataformas, y así influyen en las interacciones que los usuarios pueden tener[57]. Por ejemplo, los algoritmos de las redes sociales suelen presentarle a sus usuarios contenido que corrobora sus preferencias culturales, económicas, políticas, etc., con el fin de retenerlos en la plataforma. Sin embargo, esto genera las denominadas cámaras de eco (*echo chambers*), ya que los usuarios acceden mayoritariamente a contenido que confirma sus creencias, limitando la exposición a otras posiciones, y posiblemente empobreciendo el debate necesario en contextos democráticos[58]. A su vez, este fenómeno puede facilitar la distribución de noticias falsas (*fake news*), con impactos en términos de generación de identidades políticas aún por investigar[59]. Igualmente, otra particularidad de estas nuevas mediaciones, es que gran parte de los usuarios se encuentran en jurisdicciones diferentes a las de origen de estas empresas, poniendo bajo presión a la idea tradicional de ciudadanía pensada en función de nuestra pertenencia a un estado-nación en términos geográficos. Por estos motivos, la propuesta conceptual de Isin y Ruppert[60] de entender al ciudadano digital como alguien que reclama derechos, tanto de los existentes como de los nuevos, puede ser útil para indagar sobre los nuevos y cambiantes contornos de la ciudadanía digital y transnacional en el capitalismo de datos.

Estos impactos de la digitalización en la ciudadanía y en los derechos humanos están provocando distintos cambios en las formas de producción y gobernanza. Organizaciones preexistentes de derechos humanos, como Amnesty International o Human Rights Watch, han incorporado la temática a sus agendas. Igualmente, se crearon nuevas organizaciones transnacionales especializadas en derechos digitales, como Privacy International, que cuestionan las prácticas de producción a su entender poco éticas de varias empresas de internet. También es cierto que algunas de las ETN de internet están adoptando - aunque lentamente - técnicas de criptografía en sus servicios (por ejemplo, WhatsApp), que dificultan el acceso al contenido de los mensajes de sus usuarios por parte de terceros, pero que también limitan la soberanía estatal en regular el contenido por tales canales[61]. Finalmente, varios estados están legislando sobre internet y el uso de datos. Por un lado, se destacan las iniciativas para reformar las leyes de control de datos personales, como el Reglamento General de Protección de Datos de la Unión Europea, que le otorga derechos básicos a los usuarios sobre sus datos y le asigna responsabilidades a los organismos que los recolectan y procesan, aunque sin reducir todas las asimetrías entre estos dos tipos de actores[62]. Por el otro lado, otros estados están implementando políticas de censura, control y 'nacionalización' de internet, que cuestionan el modelo *multistakeholder*[63].

2.4. Medioambiente

El marco conceptual propuesto en el artículo no sólo provee herramientas para interpretar y ordenar las investigaciones preexistentes sobre ciberpolítica, sino también para entender e iniciar proyectos de investigación en otras áreas emergentes, como el nexo entre medioambiente y

[57] JACKSON, Susan T., A Turning IR …, *op. cit.*

[58] HELBING D, *et. al.*, *Will Democracy Survive Big Data and Artificial Intelligence?*, Scientific American, 2017: https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ [Consultado el 1 de septiembre de 2018]

[59] LAZER, David M. J. *et. al.*, "The science of fake news" en *Science*, vol. 359, n° 6380, 2018, pp. 1094-1096.

[60] ISIN, Engin y RUPPERT, Evelyn, *Being Digital Citizens*, Rowman & Litdefield Inc, Londres, 2015.

[61] BUCHANAN, Ben, "Cryptography and Sovereignty" en *Survival*, vol. 58, n° 5, 2016, pp. 95-122.

[62] BORELLI, Davide, "International Trading of Big Data" en *Athens Journal of Law*, vol. 3, n° 1, 2017, pp. 21-30.

[63] DEIBERT, Ron, The Geopolitics of …, *op. cit.*

ciberpolítica. Como en los casos previos, estas investigaciones se sustentan en los cambios en las formas de producción causadas por el proceso de digitalización, que generan una abundancia de datos y nuevas técnicas para analizarlos. En efecto, las técnicas de *big data* para recolectar información en tiempo real sobre el nexo entre medioambiente-humanos promete revolucionar varias áreas de investigación y de práctica, como las estrategias de mitigación y adaptación al cambio climático[64]. En esta área, una parte central de la discusión es sobre la propiedad de los datos medioambientales y/o biológicos: ¿tienen que estar bajo control privado o ser un bien público? La digitalización habilita a mayores posibilidades para la mercantilización de la naturaleza en la medida que permite estimar con mayor exactitud la disponibilidad de recursos biológicos y naturales. El lucro se facilita tanto a partir del acceso a los datos recabados como por intermedio del régimen de propiedad intelectual, que supuestamente incentiva la innovación[65]. Sin embargo, esta postura es muy problemática, ya que incita actividades controversiales, como la biopiratería o la bioprospección, que consiste en la explotación comercial de animales, plantas, microorganismos y otros recursos naturales[66]. Asimismo, se generan barreras artificiales que impiden el uso de los datos por parte de decisores de política pública, investigadores y el público en general, que podrían contribuir a democratizar la gestión, protección, y/o uso racional y sostenible de recursos naturales y biológicos. Debido a estas críticas, es entendible el surgimiento del movimiento de datos abiertos, una fuerza social que aboga por que los datos sean un bien público, con el fin de facilitar su circulación para diversos fines[67], más allá de los científicos o económicos, e inspira distintas iniciativas en esta dirección, como Resources Watch.

El marco conceptual también puede servir para investigar los cambios en curso sobre la gobernanza ambiental global y su intersección con el proceso de digitalización. Por ejemplo, tras la asunción de Trump, el interés de Estados Unidos por cuestiones medioambientales quedó relegado, fortaleciendo las iniciativas preexistentes en este campo de países como Alemania y China, que promueven formas de producción verde a nivel nacional e internacional. En efecto, tanto la transición a energías renovables (*Energiewende*) de Alemania como la transformación de China en una 'civilización ecológica' pueden ser consideradas como estrategias de *soft power*, pues sitúan a estos países y sus actores no estatales a la vanguardia de la lucha contra el cambio climático. En ambos casos, la ambición de proyectar un liderazgo global se basa en cambios a nivel estatal y en redes medioambientales nacionales, originadas por tensiones entre distintas fuerzas sociales y nuevas formas de producción en curso en cada país, sin soslayar las ventanas de oportunidad política del contexto internacional[68].

Finalmente, el foco del marco conceptual en las formas de producción puede servir

[64] FORD, James D., TILLEARD, Simon E., BERRAND-FORD, Lea, ARAOS, Malcolm, BIESBROEK, Robbert, LESNIKOWSKI, Alexandra C., MACDONALD, Graham K., HSU, Angel, CHEN, Chen y BIZIKOVA, Livia, "Opinion: Big data has big potential for applications to climate change adaptation" en *PNAS*, vol. 113, n° 39, 2016, pp. 10729-10732.

[65] LUCCHI, Nicola, "Understanding Genetic Information as a Commons: From Bioprospecting to Personalized Medicine" en *International Journal of the Commons*, vol. 7, n° 2, 2013, pp. 313-38.

[66] *Ibídem*.

[67] LEONELLI, Sabina, "Why the Current Insistence on Open Access to Scientific Data? Big Data, Knowledge Production, and the Political Economy of Contemporary Biology" en *Bulletin of Science, Technology & Society*, vol. 33, n° 1/2, 2013, pp. 6-11.

[68] BEVERIDGE, Ross y KERN, Kristine, "The Energiewende in Germany: Background, Developments and Future Challenges" en *Renewable Energy Law and Policy Review*, vol. 4, n° 1, 2013, pp. 3-12; WANG, Zhihe, HE, Huili, y FAN, Meijun, "The Ecological Civilization Debate in China. The Role of Ecological Marxism and Constructive Postmodernism—Beyond the Predicament of Legislation" en *Monthly Review*, vol. 66, n° 6, 2014, pp. 37-59.

para estudiar la incorporación de nuevas tecnologías en el área medioambiental, y sus efectos más amplios en términos de formas de gobernanza y de orden mundial digital. Un caso es la expansión de la tecnología *blockchain* al área medioambiental, donde tiene un gran potencial para resolver el problema de falta de confianza entre actores. Ya existen propuestas para desarrollar contratos inteligentes (*smart contracts*), por ejemplo, para registrar la propiedad de recursos medioambientales, o la trazabilidad de productos, entre otros[69].

Conclusiones

En Relaciones Internacionales, observamos la ciberpolítica centrándonos en el conjunto de actores y procesos de la política inter y transnacional en pugna por lo 'ciber'. El proceso de digitalización en curso es clave para entender la ciberpolítica en la medida que genera una profunda modificación de las relaciones de producción, que propician nuevas formas de gobernanza, que disputan por el establecimiento de un orden mundial en el ciberespacio. Este tema ya es prioritario en la agenda de las grandes potencias y de otros actores transnacionales, y este artículo sintetiza las principales contribuciones y temas de investigación de la literatura en inglés. En términos de ciberseguridad, detectamos que la literatura de Relaciones Internacionales está mayoritariamente orientada a mantener la hegemonía de países y de fuerzas sociales Occidentales —lideradas por empresas, agencias de seguridad y de defensa de Estados Unidos— en internet, tanto en términos de nuevas formas de llevar a cabo la ciberguerra, como en elaborar normas e instituciones que defiendan el orden neoliberal de gobernanza de internet. En términos de gobernanza del comercio digital y de las finanzas globales, identificamos dos patrones opuestos. Por un lado, desde el lado del comercio digital se observa un proceso de concentración en pocas empresas transnacionales de Estados Unidos y China, que les otorga un excesivo poder de mercado. Esto genera nuevas formas de producir valor, pero también nuevos desafíos en términos de gobernanza, y preguntas sobre qué tipo de capitalismo de datos prevalecerá en internet. Por el otro lado, en términos de finanzas globales, la tecnología de *blockchain* inició un proceso contrario de descentralización, que amenaza no sólo a los actores principales encargadas de las transacciones financieras en las últimas décadas, sino también a la estructura financiera global. De forma similar, los cambios en las formas de producción propiciados por la digitalización están generando nuevos desafíos en términos de derechos humanos y de ciudadanía, que distintos estados y organizaciones de la sociedad civil apuntan a resolver de manera dispar. Finalmente, en medioambiente destacamos la tensión existente entre las concepciones que consideran a los datos medioambientales como privados, frente a aquellas que los entienden como un bien público. También resaltamos la importancia del marco conceptual para entender cómo países como Alemania o China quieren influenciar en la gobernanza ambiental global, en base a las innovaciones alcanzadas a nivel nacional gracias a la digitalización, y el potencial de nuevas formas de gobernanza descentralizada en base a la tecnología *blockchain*.

Si bien tras las revelaciones de Snowden se intensificaron las diferencias dentro de los países occidentales, por ejemplo, en términos de protección de datos, para el resto de los países no es exagerado afirmar que se encuentran bajo una especie de imperialismo digital. Este es un orden hegemónico donde se aceptan y casi ni se cuestionan las nuevas formas de control digital, concentradas en pocos actores sociales transnacionales, que tienen influencia sobre los datos personales, biológicos, medioambientales, militares, etc., de gran parte de los países y poblaciones,

[69] CHAPRON, Guillaume, "The environment needs cryptogovernance" en *Nature*, vol. 545, n° 7655, 2017, pp. 403-405.

con un nivel de detalle inimaginable pocos años atrás. A pesar de estas nuevas condiciones de dependencia, salvo contadas excepciones, el interés académico por la ciberpolítica y el proceso de digitalización es más bien escaso en los países que experimentan estas nuevas dependencias, como los de América Latina. Consideramos que esto es un error por dos motivos. Primero, estratégicamente no se está pensando en cómo lidiar con los nuevos desafíos de las sociedades contemporáneas y del futuro, dejando a los países aún más dependientes y vulnerables de las iniciativas de actores extra regionales. Segundo, no se están investigando cómo las características y particularidades nacionales y/o regionales le otorgan especificidades a la ciberpolítica y al proceso de digitalización, complejizando nuestra comprensión de estos procesos más allá de los paradigmas usuales en Relaciones Internacionales.

Por estos motivos, es preciso contar con una agenda de investigación dinámica en Relaciones Internacionales, que aporte a entender y gobernar el proceso de digitalización y sus implicancias. Para contribuir a este objetivo, destacamos algunos temas posibles de investigación para los académicos con interés en países de América Latina. Primero, es importante estudiar las mejores estrategias para reducir las vulnerabilidades de los países de menores capacidades tecnológicas en términos de ciberseguridad. Segundo, acentuamos la importancia de entender y participar desde la óptica de la economía política internacional en los debates que definirán cómo se organizará y regulará el comercio, la economía, y las finanzas en la era digital. Tercero, es preciso investigar cómo distintos actores inter y transnacionales afectan a la protección de los derechos humanos en internet en la región, y las posibles formas de regular estas consecuencias. Por último, será estratégico indagar los efectos de la digitalización y de la automatización en los sectores basados en recursos naturales y en temas medioambientales en general, tanto en términos de distribución de riqueza, justicia ambiental, como de empleo. Si bien estos no son los únicos temas posibles, pensamos que son al menos los indispensables a cultivar de forma colectiva e interdisciplinaria a fin de comprender, y aconsejar a los actores regionales en estas temáticas. A la vez, no debemos perder de vista la postura crítica, de forma tal que los aportes académicos contribuyan a orientar el proceso de digitalización de forma más justa y soberana para los países de la región. Tal vez así se pueda alcanzar una inserción e interdependencia relativamente autónoma de la región en el marco de las relaciones internacionales en el capitalismo de datos. ●

Bibliografía

AARONSON, Susan, "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security" en *World Trade Review,* vol. 14, n° 4, 2015, pp. 671-700.

ABDENUR, Adriana Erthal y PEREIRA DA SILVA GAMA, Carlos Federico, "Triggering the Norms Cascade: Brazil´s Initiatives for Curbing Electronic Espionage" en *Global Governance*, vol. 21, n° 3, 2015, pp. 455-74.

ACUTO, Michele y CURTIS, Simon (ed.), *Reassembling International Theory: Assemblage Thinking and International Relations*, Palgrave Macmillan, Hampshire, 2014.

ARANDA BUSTAMANTE, Gilberto, RIQUELME RIVERA, Jorge, y SALINAS CAÑAS, Sergio, "La Ciberdefensa Como Parte de La Agenda de Integración Sudamericana" en *Línea Sur*, vol. 9, 2015, pp. 100-116.

AZMEH, Shamel, y FOSTER, Christopher, *The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements,* London School of Economics and Political Science ,Working Paper Series, n° 16-175, 2016: http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf [Consultado el 5 de mayo de 2018]

BALL, Kristie, HAGGERTY, Kevin, y LYON, David, (eds.) *Routledge Handbook of Surveillance Studies*, Routledge, Nueva York, 2012.

BALZACQ, Thierry y DUNN CAVELTY, Myriam, "A Theory of Actor-Network for Cyber-Security" en *European*

Journal of International Security, vol. 1, n° 2, 2016, pp. 176-98.
BERNAL, Paul, "Data Gathering, Surveillance and Human Rights: Recasting the Debate" en *Journal of Cyber Policy*, vol. 1, n° 2, 2016, pp. 243-64.
BETZ, David J. y STEVENS, Tim, *Cyberspace and the State. Toward a Strategy for Cyber-Power*, Routledge, Londres, 2011.
BEVERIDGE, Ross y KERN, Kristine, "The Energiewende in Germany: Background, Developments and Future Challenges" en *Renewable Energy Law and Policy Review*, vol. 4, n° 1, 2013, pp. 3-12.
BIELER, Andreas y MORTON, Adam David, "A Critical Theory Route to Hegemony, World Order and Historical Change: Neo-Gramscian Perspectives in International Relations" en *Capital & Class,* vol. 28, n° 1, 2004, pp. 85-113.
BIJKER, Wiebe E., HUGHES, Thomas P. y PINCH, Trevor (ed.), *The Social Construction of Technological Systems*, The MIT Press, Cambridge, Massachussetts, 2012.
BORELLI, Davide, "International Trading of Big Data" en *Athens Journal of Law,* vol. 3, n° 1, 2017, pp. 21-30.
BUCHANAN, Ben, "Cryptography and Sovereignty" en *Survival,* vol. 58, n° 5, 2016, pp. 95-122.
BURKHARDT, Wolf, "Big Data, Small Freedom? Informational Surveillance and the Political" en *Radical Philosophy,* vol. 191, n° 191, 2015, pp. 13-20.
CAMPBELL-VERDUYN, Malcolm. y GOGUEN, Marcel, "The mutual constitution of technology and global governance: Bitcoin, blockchains, and the international anti-money-laundering regime" en CAMPBELL-VERDUYN, Malcolm (ed.) *Bitcoin and beyond: cryptocurrencies, blockchains, and global governance*, Routledge, Londres, 2017.
CARR, Madeline, "Power Plays in Global internet Governance" en *Millennium: Journal of International Studies,* vol. 43, n° 2, 2014, pp. 640-59.
CHADWICK, Andrew y HOWARD, Phillip N (eds.), Routledge Handbook of internet Politics, Routledge, Londres, 2009.
CHAMPEAU, Serge e INNERARITY, Daniel (comps.), internet y el futuro de la democracia, Paidós, Barcelona, 2012.
CHAPRON, Guillaume, "The environment needs cryptogovernance" en *Nature*, vol. 545, n° 7655, 2017, pp. 403-405.
CHOUCRI, Nazli, *Cyberpolitics in International Relations*, The MIT Press, Cambridge, Massachusetts, 2012.
COTARELO, Ramón (ed.), Ciberpolítica: las nuevas formas de acción y comunicación políticas, Tirant Humanidades, Valencia, España, 2013.
COX, Robert W., "Social Forces, States and World Orders: Beyond International Relations Theory" en *Millennium - Journal of International Studies*, vol. 10, n° 2, 1981, pp. 126-55. https://doi.org/10.1177/03058298810100020501.
COX, Robert W., *Production, Power, and World Order: Social Forces in the Making of History*, Columbia University Press, Nueva York, 1987.
COX, Robert W. y SCHECHTER, Michael G., *The political economy of a plural world: critical reflections on power, morals and civilisation*, Routledge, Londres, 2002.
DE FILIPPI, Primavera y MCCARTHY, Smari, "Cloud Computing: Centralization and Data Sovereignty" en *European Journal of Law and Technology*, vol. 3, n° 2, 2012, pp. 1-18.
DE FILIPPI, Primavera y WRIGHT, Aaron, *Blockchain and the Law: The Rule of Code*, Cambridge, Harvard University Press, 2018.
DEIBERT, Ron, "The Geopolitics of Cyberspace after Snowden" en *Current History*, vol. 114, n° 768, 2015, pp. 9-15.
DEIBERT, Ron, ROHOZINSKI, Rafal, y CRETE-NISHIHATA, Masashi, "Cyclones in cyberspace: information shaping and denial in the 2008 Russia-Georgia war" en Security Dialogue, vol. 43, n° 1, 2013, pp. 3-24.
DENARDIS, Laura, y HACKL, Andrea M., "internet Governance by Social Media Platforms" en *Telecommunications Policy*, vol. 39, n° 9, 2015, pp. 761-770.
DER DERIAN, James, "The (S)pace of International Relations: Simulation, Surveillance, and Speed" en *International Studies Quarterly,* vol. 34, n° 3, 1990, pp. 295-310.
DIERKSMEIER, Claus y SEELE, Peter, "Cryptocurrencies and business ethics" en *Journal of Business Ethics*, vol. 152, n° 1, 2018, pp. 1-14.
DUNN CAVELTY, Myriam, "From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse" en *International Studies Review*, vol. 15, n° 1, 2013, pp. 105-122.
EBERT, Hannes y MAURER, Tim, "Contested Cyberspace and Rising Powers" en *Third World Quarterly,* vol. 34, n° 6, 2013, pp. 1054-74.
FEENBERG, Andrew, *Questioning Technology,* Routledge, Abingdon, 1999.
FINNEMORE, Martha y HOLLIS Duncan B., "Constructing Norms for Global Cybersecurity" en *The American Journal of International Law,* vol. 110, n° 3, 2016, pp. 425-79.
FORD, James D., TILLEARD, Simon E., BERRAND-FORD, Lea, ARAOS, Malcolm, BIESBROEK, Robbert, LESNIKOWSKI, Alexandra C., MACDONALD, Graham K., HSU, Angel, CHEN, Chen y BIZIKOVA, Livia, "Opinion: Big data has big potential for applications to climate change adaptation" en *PNAS,* vol. 113, n° 39, 2016, pp. 10729-10732.
GILL, Stephen, *Power and Resistance in the New World Order*, Palgrave Macmillan, Nueva York, 2008.
HELBING D, *et. al.*, *Will Democracy Survive Big Data and Artificial Intelligence?*, Scientific American, 2017: https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ [Consultado el 1 de septiembre de 2018]
HOLT, Thomas J. y BOSSLER, Adam M., "An assessment of the current state of cybercrime scholarship" en *Deviant Behavior*, vol. 35, n° 1, 2014, pp. 20-40.
ISIN, Engin y RUPPERT, Evelyn, *Being Digital Citizens*, Rowman & Litdefield Inc, Londres, 2015.

JACKSON, Susan T., "A Turning IR Landscape in a Shifting Media Ecology: The State of IR Literature on New Media" en *International Studies Review*, 2018, DOI: 10.1093/isr/viy046
JUNIO, Timothy J., "How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate" en *The Journal of Strategic Studies*, vol. 36, n° 1, pp. 125-133.
KELLO, Lucas, *The virtual weapon and international order*, Yale University Press, New Haven, 2018.
LATOUR, Bruno, *Reassembling the Social. An Introduction to Actor-Network Theory,* Oxford University Press, Nueva York, 2005.
LAZER, David M. J. *et. al.*, "The science of fake news" en *Science* , vol. 359, n° 6380, 2018, pp. 1094-1096.
LEONELLI, Sabina, "Why the Current Insistence on Open Access to Scientific Data? Big Data, Knowledge Production, and the Political Economy of Contemporary Biology" en *Bulletin of Science, Technology & Society,* vol. 33, n° 1/2, 2013, pp. 6-11.
LEWIS, Ted G., *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, John Wiley & Sons, New Jersey, 2015.
LÓPEZ-GONZÁLEZ, Javier, y JOUANJEAN, Marie-Agnès, "Digital Trade: Developing a Framework for Analysis", OECD, OECD Trade Policy Paper n° 205, 2017.
LUCCHI, Nicola, "Understanding Genetic Information as a Commons: From Bioprospecting to Personalized Medicine" en *International Journal of the Commons,* vol. 7, n° 2, 2013, pp. 313-38.
LYNN III, William J., "Defending a New Domain. The Pentagon's Cyberstrategy" en *Foreign Affairs*, 2010: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain [Consultado el 20 de abril de 2018]
MADSEN, Anders Koed, FLYVERBOM, Mikkel, HILBERT, Martin, y RUPPERT, Evelyn, "Big Data: Issues for an International Political Sociology of Data Practices" en *International Political Sociology, n°*10/3, 2016, pp. 275-96. https://doi.org/10.1093/ips/olw010
MAHRENBACH, Laura, MAYER, Katja y PFEFFER, Jürgen, "Policy visions of big data: views from the Global South" en *Third World Quarterly*, DOI:10.1080/01436597.2018.1509700
MAURER, Tim, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security", Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf [Consultado el 20 de julio de 2018]
MAYER, Maximilian, CARPES, Mariana, y KNOBLICH, Ruth (ed.), "The Global Politics of Science and Technology: An Introduction" en *The Global Politics of Science and Technology*, Springer-Verlag, Berlin, 2014, pp. 1-35.
MCAFEE, Andrew, and Erik BRYNJOLFSSON. 2012. "Big Data: The Management Revolution" *Harvard Business Review*, octubre, 2012.
MCCARTHY, Daniel R., "The meaning of materiality: reconsidering the materialism of Gramscian IR" en *Review of International Studies*, vol. 37, n° 3, 2010, pp. 1215-1234.
MCKINSEY & COMPANY, *Artificial Intelligence: the next digital frontier?*, MCKINSEY GLOBAL INSTITUTE, Discussion Paper, 2017: https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx [Consultado el 25 de julio de 2018]
MUELLER, Milton, MATHIASON, John y KLEIN, Hans, "The internet and Global Governance: Principles and Norms for a New Regime" en *Global Governance,* vol. 13, n° 2, pp. 237-254.
NAHUIS, Roel y VAN LENTE, Harro, "Where Are the Politics? Perspectives on Democracy and Technology" en *Science, Technology, & Human Values*, vol. 33, n° 5, 2008, pp. 559-581.
PLANTIN, Jean-Christophe, *et. al.*, "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook" en *New Media & Society*, vol. 20, n° 1, 2016, pp. 293-310.
POHLE, Julia y VAN AUDENHOVE, Leo, "Post-Snowden internet policy: between public outrage, resistance and policy change" en *Media and Communication*, vol. 5, n° 1, 2017, pp. 1-6.
RID, Thomas, "Cyber war will not take place" en *The Journal of Strategic Studies*, vol. 35, n° 1, 2012, pp. 5-32.
ROBINSON, William I., "Gramsci and Globalisation: From Nation-State to Transnational Hegemony" en *Critical Review of International Social and Political Philosophy,* vol. 8, n° 4, 2005, pp. 559-74.
SAGUIER, Marcelo y GHIOTTO, Luciana, "Las empresas transnacionales: un punto de encuentro para la Economía Política Internacional de América Latina" en *Desafíos*, vol. 30, n°2, 2018.
SEGAL, Adam, "The Code Not Taken: China, the United States, and the Future of Cyber Espionage" en *Bulletin of the Atomic Scientists*, vol. 69, n° 5, 2013, pp. 38-45.
SLOAN, Elinor C., *Modern Military Strategy: An Introduction*, Routledge, Abingdon, 2012.
SRNICEK, Nick, *Platform Capitalism*, Polity Press, Cambridge, 2016.
VALERIANO, Brandon y MANESS, Ryan C., *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford University Press, Oxford, 2015.
VILA SEOANE, Maximiliano, "Digitalización, automatización y empresas transnacionales de seguridad privada en áreas con capacidad estatal limitada" en *Revista de Relaciones Internacionales, Estrategia y Seguridad*, vol. 13, n°2, 2018, DOI: 10.18359/ries.3300
WANG, Zhihe, HE, Huili y FAN, Meijun,"The Ecological Civilization Debate in China. The Role of Ecological Marxism and Constructive Postmodernism—Beyond the Predicament of Legislation" en *Monthly Review*, vol. 66, n° 6,

2014, pp. 37-59.
ZIEWITZ, Malte, "Governing algorithms: myth, mess, and methods" en *Science, Technology, & Human Values*, vol. 41, n° 1, pp. 3-16.
ZWITTER, Andrej, "Big Data and International Relations" en *Ethics & International Affairs*, vol. 29, n° 4, 2015, pp. 377-89.