EDICIONES COMPLUTENSE

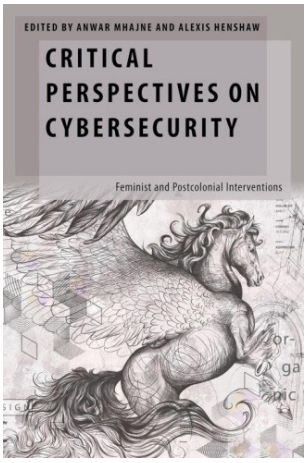
Teknokultura. Revista de Cultura Digital y Movimientos Sociales
e-ISSN: 1549-2230

RESEÑAS

Reseña/Review (Mhajne, Anwar, Henshaw, Alexis, "Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions", Oxford University Press, ISBN: 978-01-976958-8-3, 204 págs., 2024)

Bárbara Prummer Arabaolaza
Universidad Complutense de Madrid (España)

https://dx.doi.org/10.5209/TEKN.104901



Hacia una ciberseguridad centrada en las personas

El marco clásico de la ciberseguridad ha priorizado la seguridad nacional frente a la defensa de los derechos humanos (Mhajne y Henshaw, 2024). En la actualidad se está promoviendo un cambio de perspectiva que busca redefinir la ciberseguridad como «la preservación, a través de la política, la tecnología y la educación, de la disponibilidad, la confidencialidad y la integridad de la información y su infraestructura subyacente para mejorar la seguridad de las personas tanto *online* como *offline*» (Internet Free and Secure Initiative, 2024). En este sentido, las teorías críticas en el campo de las relaciones internacionales y los estudios de seguridad examinan cómo el género, la sexualidad, la raza/etnia y las divisiones entre el Norte y el Sur globales dan forma a experiencias situadas de (in)seguridad digital que, a menudo, son ignoradas desde instituciones y organismos públicos. Diversos estudios feministas han destacado que la falta de diversidad dentro del masculinizado mundo de la ciberseguridad se relaciona con la brecha de género digital (Kshetri y Chhetri, 2022; Brown y Pylak, 2020) y con la falta de medidas políticas efectivas para hacer frente a las violencias contra mujeres y minorías de género y sexuales en el ciberespacio (Slupska, 2019; Whetstone y K. C., 2024). Estas cuestiones son inseparables de los debates sobre territorialización, soberanía y gobernanza que atraviesan la red superpuesta de infraestructuras de propiedad policéntrica y bienes público-privados en disputa que constituye el ciberespacio. La multiplicidad de actores que componen la sociedad civil desafía el poder de Estados y empresas privadas sobre el dominio digital, mediante acciones de resistencia y rechazo a las crecientes violencias digitales, al abuso de los bienes comunes de la red y a la 'securitización' del ciberespacio (Whetstone y K. C., 2024).

La lectura de *Perspectivas críticas sobre ciberseguridad* es fundamental para comprender la privacidad y la protección de datos desde un enfoque feminista interseccional (Crenshaw, 1989; Hackworth, 2018) y poscolonial (Wilkens, 2017) que visibiliza la emergencia de espacios para la resistencia entre las poblaciones del Sur Global, amenazadas por nuevas formas de vigilancia, autoritarismo digital y colonialismo de datos (Thatcher et al., 2016; Mejias y Couldry, 2024). La geopolítica de la ciberseguridad dibuja un mapa de (inter)dependencias dominado por grandes potencias, como Estados Unidos, Rusia, China y países de la Unión Europea, que exportan *software* espía y herramientas de censura, al tiempo que tratan de influir en las estrategias de ciberseguridad de los países importadores del Sur Global, desde donde emergen, a su vez, algunas de las más grandes amenazas de seguridad (Mhajne y Henshaw, 2024, p. 6). En este entramado resulta clave el papel de importantes empresas tecnológicas, como Alphabet y Microsoft, que participan en iniciativas público-privadas de ciberseguridad en el Norte Global, mientras contribuyen a mantener los sistemas de censura y vigilancia de regímenes autoritarios. Con el objetivo de mitigar estas divisiones entre Norte y Sur, Erin Saltman y Dina Hussein (2024) proponen establecer normas básicas globales para la protección de datos y la privacidad de los usuarios de Internet. Las autoras del segundo capítulo

señalan cómo la hiper-localización y fragmentación de la legislación sobre la protección de datos, está generando «una forma de nuevo colonialismo» (Saltman y Hussein, 2024, p. 52) entre países democráticos y países más autoritarios, donde los gobiernos exigen el acceso a los datos de los usuarios con el pretexto de medidas de seguridad, como la lucha contra el terrorismo. Basándose en definiciones imprecisas de lo que constituye terrorismo, este tipo de legislación tiende a imponer una mayor censura contra grupos marginalizados o perseguidos, activistas de derechos humanos y periodistas críticos con el poder estatal. Precisamente, en la segunda parte del libro se examina la ciber(in)seguridad, atendiendo a particularidades regionales y nacionales diversas, a través de una serie de cinco casos paradigmáticos: Afganistán, el pueblo Uyghur, Kenia, Palestina y América Latina.

Las autoras, sin caer en el maniqueísmo de pensar en actores buenos o malos, arrojan luz sobre la complejidad de los contextos y de las posiciones y disposiciones de los múltiples actores involucrados en estas tensiones sistémicas que emergen en torno a la regulación del ciberespacio. Las diferentes miradas que se reúnen en esta colección de textos abogan por una suerte de multilateralismo co-regulatorio que defienda los derechos humanos, también en el ámbito digital. Esta posición es crítica con los dos enfoques que dominan los debates internacionales sobre la aplicación del derecho internacional al ciberespacio. Frente al institucionalismo liberal y al estatismo clásicos, se propone construir un nuevo marco de ciberseguridad centrado en las personas. Para ello, Crystal Whetstone y Luna K. C. (2024) desarrollan en el primer capítulo una interesante propuesta que conjuga derecho internacional humanitario, derecho internacional y gobernanza en materia de ciberseguridad, con una perspectiva feminista interseccional que, atendiendo a las diferencias regionales, reivindica políticas contextualizadas, para que se reconozcan y atajen los efectos desproporcionados de la ciberdelincuencia y otras formas de violencia digital 'generizada' contra mujeres y otras minorías en el ciberespacio. Basándose en los usos innovadores de la Resolución 1325 del Consejo de Seguridad de las Naciones Unidas (RCSNU) y la Agenda sobre Mujeres, Paz y Seguridad (MPS), las autoras buscan no solo «proteger a las mujeres, las niñas, las personas trans, queer y otras minorías sexuales y de género de la violencia de género en línea», sino también «promover el acceso equitativo de los grupos marginalizados a la ciberseguridad, tanto en términos de acceso a las tecnologías como de participación en la gobernanza y la formulación de políticas» (Whetstone y K. C., 2024, p. 38). No obstante, las principales críticas a la Agenda MPS señalan que la interpretación de cuestiones que tradicionalmente se han considerado ajenas a los asuntos militares y de seguridad nacional como cuestiones de seguridad, puede tener efectos perniciosos sobre los colectivos marginalizados:

> La securitización suele conducir a la justificación de la guerra y la militarización, que pueden ser dañinas para las mujeres, al tiempo que despolitiza las diferencias de poder entre los géneros en lugar de trabajar para desmantelar los procesos políticos que mantienen la jerarquía de género (Jansson y Eduards, 2016 en Whetstone y K. C., 2024, p. 26).

Desde posiciones feministas, la agenda MPS y la RCSNU han sido criticadas por su impacto sobre las mujeres al limitarlas a roles estereotipados, como el de víctimas o promotoras de paz (*peacemakers*). La falta de una mirada interseccional lleva también a ignorar otros factores de la identidad de las mujeres, como la sexualidad (Hagen, 2016). Respecto a las críticas desde posiciones poscoloniales, se ha señalado cómo la agenda MPS y los PNA (Planes Nacionales de Acción) de la RCSNU a menudo consisten en un proceso colonizador en el que la comunidad internacional excluye la participación local (Basini y Ryan, 2016). Frente a esto, se busca innovar con planes que se apliquen no solo a países extranjeros que estén en guerra o hayan sufrido una guerra, sino, internamente, en todo país donde exista violencia de género. Así, en América Latina, PNA como los desarrollados por Argentina y Brasil ya han comenzado a centrarse en algunas de las violencias contra mujeres que se producen en sus propias fronteras (Drumond y Rebelo, 2020). Una reevaluación de las narrativas dominantes en torno a las normas y leyes del ciberespacio demuestra el valor de adoptar una perspectiva crítica, situada y localmente liderada.

Resistencias digitales en las sociedades de control

Las resistencias digitales emergen en un contexto definido por Ulrich Beck (1986) como «sociedad del riesgo», donde las vulnerabilidades ya no provienen de amenazas externas, sino de los propios procesos de modernización tecnológica. En el ámbito digital, los algoritmos, infraestructuras y sistemas de vigilancia producen riesgos globales, invisibles y desiguales, generando nuevas formas de dependencia y exclusión. A la vez, como señaló Gilles Deleuze (2006), vivimos en «sociedades de control», caracterizadas por la gestión continua de los sujetos 'dividuales' o cifrables, mediante trazas digitales, flujos de datos y tecnologías de poder panóptico que trascienden las del control disciplinario clásico (Foucault, 1975).

El libro señala con claridad el conflicto entre libertad de expresión, privacidad y seguridad estatal, cristalizado en un escenario histórico polarizado, entre Norte y Sur Globales, donde se disputa la propiedad policéntrica de la Red y el carácter transnacional de sus bienes público-privados. La ONU ha reconocido el acceso a Internet como un derecho humano fundamental (UNHRC, 2011), pero ese reconocimiento convive con desigualdades sociales en el acceso y la protección de datos en un ciberespacio cada vez más dominado por el extractivismo del capitalismo de plataformas (Srnicek, 2017) y la expansión de mecanismos de control del capitalismo de vigilancia (Zuboff, 2019). La pandemia de Covid-19 y la 'infodemia' (OMS, 2020) acentuaron esta paradoja. La gestión de la emergencia sanitaria generó tecnologías de control duraderas, legitimadas mediante el miedo (Klein, 2007), en un clima que encarna lo que 'Bifo' Berardi (2021) ha denominado 'sociedad del pánico'.

Frente a la expansión de la 'securitización', el autoritarismo digital y las violencias generizadas en el ciberespacio, emergen múltiples resistencias

digitales que articulan respuestas críticas: desde el reclamo de una ciberseguridad feminista interseccional, centrada en las personas, hasta la denuncia de un 'nuevo colonialismo de datos' (Saltman y Hussein, 2024). Estas resistencias revelan que la seguridad digital no puede reducirse al control tecnocrático: solo adquiere sentido como ciberseguridad crítica, vinculada a la defensa de los derechos digitales y la justicia social.

Referencias

Basini, Helen y Ryan, Caitlin (2016). National Action Plans as an obstacle to meaningful local ownership of UNSCR 1325 in Liberia and Sierra Leone. *International Political Science Review*, *37*(3), 390-403. https://doi.org/10.1177/0192512116636121

Beck, Ulrich (1992). *Risk society: Towards a new modernity*. Sage.

Berardi, Franco (2017). *Futurability: The age of impotence and the horizon of possibility*. Verso Books.

Brown, Deborah y Pytlak, Allison (2020). Why gender matters in international cyber security. *Women's International League for Peace and Freedom and the Association for Progressive Communications*. https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security

Crenshaw, Kimberlé (1989). Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum*, *1*, 139–167.

Deleuze, Gilles. (2006). Post-scriptum sobre las sociedades de control. En *Conversaciones* (1972-1990) (pp. 233–239). Pre-Textos.

Drumond, Paula y Rebelo, Tamya (2020). Global pathways or local spins? National Action Plans in South America. *International Feminist Journal of Politics*, *22*(4), 462–84. https://doi.org/10.1080/14616742.2020.1783339

Foucault, Michel (1975). *Surveiller et punir: Naissance de la* prison. Gallimard.

Hackworth, Lucy (2018). Limitations of 'just gender': The need for an intersectional reframing of online harassment discourse and research. En *Mediating misogyny* (pp. 51-70). Springer. https://doi.org/10.1007/978-3-319-72917-6_3

Hagen, Jamie J. (2016). Queering women, peace and security. *International Affairs* (Royal Institute of International Affairs 1944-), *92*(2), 313–32. http://www.jstor.org/stable/24757887

Internet Free and Secure Initiative (2024, 14 de noviembre). *A human rights respecting definition of cybersecurity*. https://freeandsecure.online/definition/

Jansson, Maria y Eduards, Maud (2016). The politics of gender in the un security council resolutions on women, peace and security. *International Feminist Journal of Politics*, *18*(4), 590–604. https://doi.org/10.1080/14616742.2016.1189669

Klein, Naomi (2007). *The shock doctrine: The rise of disaster capitalism*. Metropolitan Books.

Kshetri, Nir y Chhetri, Maya (2022). Gender asymmetry in cybersecurity: Socioeconomic causes and consequences. *Computer*, *55*(2), 72-77. https://doi.org/10.1109/MC.2021.3127992

Mejias, Ulises, A. y Couldry, Nick (2024). *Data grab: The new colonialism of big tech (and how to fight back).* WH Allen.

Mhajne, Anwar y Alexis Henshaw (Eds) (2024). *Critical perspectives on cybersecurity: feminist and post-colonial interventions* (1). Oxford Academic. https://doi.org/10.1093/oso/9780197695883.001.0001

Saltman, Erin y Hussein, Dina (2024). Cyberspace and the nouveau colonialism'. En Anwar Mhajne y Alexis Henshaw (eds*), Critical perspectives on cybersecurity: Feminist and postcolonial interventions*. Oxford Academic. https://doi.org/10.1093/oso/9780197695883.003.0003

Slupska, Julia (2019). Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review 15*(1), 83–100. https://www.jstor.org/stable/27027755

Srnicek, Nick (2017). *Platform capitalism*. Polity Press.

Thatcher, Jim, O'Sullivan, David y Mahmoudi, Dillon (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society & Space*, *34*(6), 990-1006. https://doi.org/10.1177/0263775816633195

United Nations Human Rights Council (UNHRC) (2011). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)*. United Nations.

Whetstone, Crystal, y K.C., Luna (2024). A call for feminist insights in cybersecurity: Implementing united nations security council resolution 1325 on women, peace, and security in cyberspace. En Anwar Mhajne, and Alexis Henshaw (eds), *Critical perspectives on cybersecurity: feminist and post-colonial interventions*. Oxford Academic. https://doi.org/10.1093/oso/9780197695883.003.0002

Wilkens, Jan (2017). Postcolonialism in international relations. En *Oxford research encyclopedia of international studies, 20*. https://doi.org/10.1093/acrefore/9780190846626.013.101

Zuboff, Shoshana (2019). T*he age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.