Consideraciones conceptuales sobre conflictividad, policiamiento, tecnología y cibercriminalidad

Tobías J. Schleider (UNMDP-UNS-ILSED) y Matías I. González (UNMDP)

Los conflictos sociales atraviesan cambios constantes. Pero más allá de cómo muten, persiste la obligación estatal de minimizar la afectación de derechos y libertades de personas. De esto se deriva en un deber político de actualización, por parte del Estado y de sus instituciones, de los conocimientos y los instrumentos necesarios para encauzar los conflictos sociales de la manera más efectiva que esté a su alcance.

La policía es una de las instituciones con un rol significativo en la vigencia de la seguridad ciudadana. Sin embargo, no es inusual que, en muchos países de la región, una parte de los recursos humanos policiales se destinen a tareas administrativas, no dirigidas a la prevención[1] o la investigación de conflictos que devienen en delictivos (Saín 2010). Y cuando este no es el caso, suelen prevalecer enfoques tradicionales del desempeño policial, con dificultades en su eficacia y eficiencia (González, Montero y Sozzo 2010).

Las tendencias institucionales que caracterizaron a las fuerzas policiales latinoamericanas durante las últimas décadas y la fuerte influencia política han dado forma a un tipo de profesionalismo policial tradicional que dificulta los cambios institucionales (Salomón 2004)[2]. Desarticular esta maraña de

[1] Las estrategias preventivas son las que buscan intervenir de manera temprana en la base fáctica del conflicto: proponen amplificar o reducir los efectos de ciertos factores sociales o culturales que puedan favorecer o disminuir la probabilidad de su manifestación violenta. Las estrategias reactivas se proyectan para ser instanciadas con simultaneidad o posterioridad a la manifestación física del conflicto, y aspiran a reaccionar de manera eficiente y efectiva para contenerlo y encauzarlo, reduciendo sus consecuencias negativas. La investigación posterior sobre hechos violentos sucedidos es una de las tantas acciones reactivas que el sistema de seguridad ciudadana puede llevar adelante. Consultar, al respecto, Clarke 1983, Ayos 2014, Sozzo 2000 y Selmini 2014

[2] El profesionalismo policial es un atributo institucional constitutivo de toda organización policial compleja que se asienta en dos dimensiones fundamentales: la *simbólica*, constituida por los valores, concepciones y el marco de referencia cultural predominantes entre sus integrantes, y la *organizacional*, conformada por la estructura orgánico-funcional de la institución, así como el

obstáculos es una tarea compleja. Para reformular los aspectos relevantes del policiamiento es crucial una transformación profunda en la formación y capacitación de los aspirantes y los miembros de las policías, acompañada de un esfuerzo institucional que priorice el trabajo basado en evidencia[3]

Entre las múltiples opciones que pueden proponerse, y sin perjuicio de la actualización de temáticas imprescindibles para la prestación del servicio policial, parece promisoria la incorporación de conocimientos en áreas no asociadas históricamente a la actividad policial. Por ejemplo, en gestión comunitaria, en comunicación pública, en capacidades de debate sobre los contornos del conflicto social y las problemáticas que se derivan de él y, sobre todo, en aquellas temáticas relacionadas al análisis estratégico y táctico, la prevención de tipos de violencias y delitos específicos y en los usos de herramientas tecnológicas (Dammert 2020, Ortega 2016, Buvinic, Alda y Lamas 2005).

Uno de los discursos sociales en boga respecto del alcance operativo de las nuevas tecnologías aplicadas a todo tipo de problemas resalta su supuesta imparcialidad y eficiencia. La *tecnofilia* está, en muchos casos, sobredimensionada. Las nuevas tecnologías no garantizan la toma de decisiones perfectas ni objetivas salvo, en algún sentido, en tareas limitadas, en un campo de acción reducido y, usualmente, no aplicado a disciplinas sociales. Cuando se aplica en estos dominios, la tecnología muestra deficiencias y casos de sobre y subdeterminación en las conclusiones que arrojan. El funcionamiento de las nuevas tecnologías no es independiente de muchos de los defectos que los seres humanos poseen, justamente, porque quienes se encuentran detrás de esas herramientas son hombres y mujeres. Los sesgos y los valores permean cada etapa de su creación. La idea distorsionada de la imparcialidad tecnológica se conoce como *"machine bias"* (Schleider, Balmaceda y Pedace 2021).

---

régimen profesional de los agentes –el escalafón y sus respectivos agrupamientos y especialidades; los grados jerárquicos; el régimen de superioridad; la estructura de los cargos orgánicos; el sistema de promociones y ascensos; el sistema de retribuciones; el sistema previsional; y el régimen laboral–, su sistema de formación y capacitación; y el régimen disciplinario y los mecanismos y dispositivos de control policial. El tipo de profesionalización policial está dado por el grado de desarrollo y el nivel de complejidad alcanzado por una institución policial en las dimensiones referidas. Ver, por todos, Salomón 2004.

[3] Una experiencia interesante al respecto, aunque limitada al nivel local, fue la Escuela Municipal de Seguridad del Partido de General Pueyrredon (Mar del Plata, Argentina). Sus características pueden consultarse en https://www.mardelplata.gob.ar/documentos/policia/presentacion%20emsl.pdf.

En estos términos puede pensarse el impacto de la tecnología en el sistema de seguridad ciudadana, en general, y en el subsistema policial, en particular. Debe concebirse a los instrumentos tecnológicos como herramientas para gestionar conflictos y para mejorar las técnicas y métodos válidos y útiles para este fin, pero no puede asumirse que su actuar no debería ser monitoreado y que siempre será acertado. Si no se asume este enfoque, no será raro encontrar Estados que recurren a la tecnología de forma indiscriminada e irrestricta. Tampoco deberían considerarse a los artefactos tecnológicos como armas en una guerra contra un supuesto enemigo *extrasocial*. Estas falencias en las distinciones conceptuales se traducen en *malas prácticas tecnológicas*. La preconcepción bélica de la criminalidad lleva a ignorar las consecuencias que las intervenciones estatales y policiales tienen en la sociedad y en los derechos de sus integrantes, en general; y esto se exacerba cuando entra en el juego la tecnología en alguna de sus tantas formas (Balmaceda, Schleider y Pedace, 2021).

Este error conceptual también guía a los Estados a soslayar el interés por la evidencia sobre la utilidad de las herramientas tecnológicas. El sentimiento de urgencia causado por la presión mediática y política se traduce en un proceso continuo de prueba y error, sin análisis previo, de uso de instrumentos tecnológicos. Lo más grave es, tal vez, que en ocasiones ni siquiera se tiene en cuenta la efectividad de las medidas que se adoptan, en tanto se consiga transmitir una idea difusa de control y de expansión de la operatividad estatal. Lo importante, según este entendimiento, es ampliar la presencia estatal, al menos de manera ostensiva; dar una imagen de eficiencia, aunque, en los hechos y en los casos concretos, no exista una influencia positiva en la gestión de los conflictos y el abordaje de la seguridad (Schleider, Balmaceda y Pedace 2021).

Por el contrario, bajo la concepción de la seguridad ciudadana que nos mueve, se realza la relevancia de la utilización de herramientas cuya efectividad para los fines perseguidos ha sido demostrada. En otras palabras, el elemento paradigmático de actuación estatal es el diseño de políticas públicas basado en evidencias (Frülling 2012; Chinchilla y Vorndran 2018). Antes de la utilización de una herramienta tecnológica, debe ser posible responder una serie de preguntas como estas: *¿con qué objetivo se utilizará la herramienta?, ¿hay alguna relación entre el uso de la herramienta y el objetivo planteado?, ¿de qué manera está*

probada esta relación?, ¿en alguna instancia de su utilización se violan derechos y garantías? Solo después de dar respuestas válidas a estas preguntas es que deviene viable incluir un elemento perteneciente a las nuevas tecnologías en el diseño, implementación o monitoreo y evaluación de una política de seguridad ciudadana. Pero, a pesar de ser planteadas, estas respuestas no pueden responderse si los operadores y agentes estatales no tienen los conocimientos suficientes para hacerlo.

Un ámbito en el que salen a la luz estas inadecuaciones de la operatividad, instrumentalidad y configuración estatal y policial es el de la cibercriminalidad. Puesto en pocas palabras, la cibercriminalidad es un fenómeno conformado por un conjunto de actos dañosos o delictivos que se concretan utilizando medios de la tecnología de la información y la comunicación[4] con dos objetivos posibles. En primer lugar, uno de estos objetivos puede ser, también, un activo digital o tecnológico, como, por ejemplo, datos confidenciales o información. Por otro lado, la cibercriminalidad puede hacer referencia a la facilitación en la realización de delitos tradicionales. Es posible, entonces, evocar la subclasificación de los ciberdelitos clásica, que los agrupa en ciberdelitos *dependientes*, es decir, delitos que sólo puedan cometerse utilizando dispositivos y sistemas tecnológicos[5] y ciberdelitos *habilitados* por la tecnología –es decir, delitos tradicionales facilitados por las TIC o *cyber-enabled crimes*, en inglés– (Europol 2018).

La utilización creciente de las TIC y de Internet, que se explica a partir de un incremento masivo de la conectividad global, ha venido generando oportunidades nuevas para esta problemática y para las cuales las agencias policiales no están preparadas de manera general (Miró Llinares 2011). La cibercriminalidad plantea, hace ya algunos años, desafíos para su prevención y para la aplicación a su respecto de teorías criminológicas generales. El ciberespacio ha creado nuevos fenómenos que son distintos a la mera existencia de sistemas informáticos y oportunidades de criminalidad que ofrecen las computadoras.

En el ciberespacio, las personas pueden comportarse de manera diferente a como lo hacen en el mundo físico y cometer delitos que no cometerían en el espacio físico. En el caso de la cibercriminalidad, puede haber

[4] Estas cuestiones pueden profundizarse, por ejemplo, con la lectura de Wall 2007 y Miró Linares 2012

[5] Un ejemplo de uso de esta clasificación se encuentra en Europol 2018.

una gran cantidad de objetivos adecuados debido al aumento del tiempo que se pasa en línea y el uso de aplicaciones que dependen del servicio de Internet. Esto resulta, en alguna medida, en una mayor ventana de oportunidad para quienes quieran aprovecharse de los usuarios de estos servicios (Balmaceda, Schleider y Pedace 2021).

La carencia de enfoques modernizados, de formación específica y de operatividad eficiente –que incluye, entre muchos elementos, el análisis de datos y la inteligencia criminal– en el subsistema policial se traduce en el agravamiento de las problemáticas sustantivas de la seguridad ciudadana (Dammert 2020). Al realizar un análisis teórico de la cibercriminalidad y la configuración de las agencias policiales se aprecian las tres líneas en las que aún es necesaria una modernización: en facetas de actuación preventiva, en su función reactiva y en la concepción del mismo subsistema policial.

Desde el ámbito de la prevención, no puede dejar de remarcarse que la falta de formación y de dirección especializada de las policías en estos temas lleva, en muchos casos, a una dificultad en la inclusión de datos válidos sobre la cibercriminalidad en las estadísticas oficiales. Esto se traduce en la inexistencia de un cuadro descriptivo de la situación fáctica de la cibercriminalidad. Saber cuántos delitos y violencias digitales se concretan, sus modalidades y qué conflictos subyacen a estos fenómenos es vital para comenzar a trazar estrategias de *ciberprevención* (Bekerman 2020, Branch 2001, Miró Llinares 2011, Peña y García Segura 2014).

Por otra parte, la falta de conocimiento sobre la temática hace difícil configurar un rol para la policía en el abordaje reactivo de la problemática. Sin embargo, deben tenerse en cuenta dos factores centrales para desmantelar este preconcepto. Por un lado, el policiamiento actual no ha de responder a formas tradicionales, en tanto que el paradigma de la seguridad ciudadana poco tiene de similar con las antiguas perspectivas securitarias. La policía no solo puede jugar un papel en el abordaje de la cibercriminalidad, sino que debe hacerlo. Por otro lado, la profundización en la formación específica acerca de ciertas técnicas de recuperación, investigación y preservación de evidencias digitales son fundamentales para potenciar el trabajo reactivo de la institución policial (Tuor, Kaplan, Hutchinson, Nichols y Robinson 2017; Balmaceda, Schleider y Pedace 2021).

Los dos ámbitos de acción para pensar una policía que contribuya con

estos nuevos fenómenos solo se habilitan tras la adopción de los principios de la seguridad ciudadana. La seguridad, bajo este entendimiento, no protege al Estado y a su concepto difuso de "orden"; no persigue criminales y los encierra; no mantiene a individuos – catalogados como *parasociales*– a raya para que no interrumpan el correcto funcionamiento administrativo. La seguridad ciudadana se enmarca en una labor preventiva, que proteja, de la mejor manera posible, el goce efectivo de derechos y libertades de ciudadanos concretos (Binder 2008, Ayos 2013, Mack 2005; Dammert, Mujica y Zevallos 2012). Un paso fundamental en esa tarea es el conocimiento especializado de los conflictos que pueden manifestarse de manera dañosa o violenta y limitar, así, el estado de seguridad ciudadana. Esto rige también para el ámbito de alcance de la cibercriminalidad; sirvan estos párrafos como línea de partida.

Referencias bibliográficas

Ayos, E. J. (2013). Prevención del delito y políticas sociales en Argentina: tres ejes problemáticos.
Revista de Ciencias Sociales, 135-136. DOI: 10.15517/rcs.v0i135-136.3682

Ayos, E. J. (2014). ¿Una política democrática de seguridad? Prevención del

delito, políticas sociales y disputas en el campo conformado en torno a la inseguridad en la Argentina de la última década *Reforma y Democracia. Revista del CLAD,* (58). DOI: 10.32870/espiral.v24i68.6332

Balmaceda, T., Schleider, T. J. y Pedace K. (2021). Bajo observación: inteligencia artificial, reconocimiento facial y sesgos. *ArtefaCToS. Revista de estudios de la ciencia y la tecnología. 10*(2), 21-43. DOI: 10.14201/art20211022143

Bekerman, U. (2020). Algunas medidas de ciberseguridad en Argentina, Colombia, Cuba, Egipto, Francia, Grecia, Japón, Singapur y Turquía. *Diario DPI - Suplemento Derecho y Tecnologías*, 66.

Binder, A. M. (2008). *El control de la criminalidad en una sociedad democrática.*

Edhasa. Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity.

International Organization,

75(1), 39-70. DOI: 10.1017/S002081832000051X

Buvinic, M., Alda, E. y Lamas, J. (2005). *Emphasizing prevention in citizen security.* The Inter- American Development Bank.

Chinchilla, L. y Vorndran, D. (2018). *Seguridad ciudadana en América Latina y el Caribe: Desafíos e innovación en gestión y políticas públicas en los últimos* 10 años. Banco Interamericano de Desarrollo. DOI: 10.18235/0001426

Clarke R.V. (1983). Situational Crime Prevention: its Theoretical Basis and Practical Scope.
Crime and Justice, 4, 225-256. DOI: 10.1086/449090

Dammert, L. (2020) *Reforma policial: Agenda (aún) pendiente en América Latina.* Diálogo Interamericano

Dammert, L., Mujica, J. y Zevallos, N. (2012). *Seguridad Ciudadana. Balance de Investigación en Políticas Públicas 2011-2016 y Agenda de Investigación 2017-2021.* Consorcio de Investigación Económica y Social.

Europol (2018) *Internet Organised Crime Threat Assessment.* European Union Agency for Law Enforcement Cooperation.

Frühling, H. (2012). *La eficacia de las políticas públicas de seguridad ciudadana en América Latina y el Caribe. Cómo medirla y cómo mejorarla.* Banco Interamericano de Desarrollo.

Gonzalez, G., Montero, A. y Sozzo, M. (2010). ¿Reformar la policía? Representaciones y opiniones de los policías en la Provincia de Santa Fe. En Sozzo, M. (Comp.). *Por una sociología crítica del control social. Ensayos en honor a Juan S. Pegoraro.* Editores del Puerto, 289-318.

Mack, A. (2005). El concepto de seguridad humana. *Papeles de cuestiones internacionales,* 90, 11-18.

Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista electrónica de Ciencia Penal y Criminología, 13- 07*, 07:1-07:55.

Ortega, D. (2016). Effectiveness versus legitimacy: Use of force and police training in Latin America, Brookings.

Pedace, K., Schleider, T. J. y Balmaceda, T. (2023). Inteligencia artificial y sesgos. El caso de la predicción del embarazo adolescente en Salta.

Revista Iberoamericana de Ciencia, Tecnología y Sociedad-CTS, 18(53), 9-26. DOI: 10.52712/issn.1850-0013-359

Peña, J. C. y García Segura, L. A. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. *Estudios en seguridad y defensa, 9*(18), 5-13. DOI: 10.25062/1900-8325.9.

Saín, M. F. (2010). La reforma policial en América Latina: Una mirada crítica desde el progresismo (Vol. 1). Prometeo Libros.

Salomón, L. (2004). El desempeño policial y la satisfacción de la ciudadanía. Programa de las Naciones Unidas para el Desarrollo.

Schleider, T. J., Balmaceda, T. y Pedace, K. (2021). Filosofía, tecnología y género: la predicción algorítmica del embarazo adolescente. La Ley, Suplemento Innovación y Derecho, 5, 1-8.

Selmini, R. (2009). La prevención: estrategias, modelos y definiciones en el contexto europeo. URVIO: Revista Latinoamericana de Estudios de Seguridad, (6), 41-57.

Sozzo, M. (2000). Seguridad urbana y tácticas de prevención del delito. Cuadernos de jurisprudencia y Doctrina Penal, 6(10), 17-82.

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N. y Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. ArXiv, 2017. DOI: 10.48550/arXiv.1710.00811

Ungar, M. (2011). Policing democracy: overcoming obstacles to citizen security in Latin America.

Johns Hopkins University Press.

Wall, D. (2007). Cybercrime: the transformation of crime in the information age. Vol. 4. Polity Press.