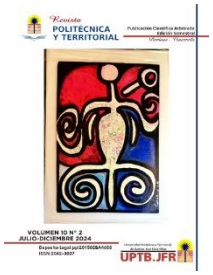
N° 2, V. 10 JULIO DICIEMBRE 2024/ Revista Científica Multidisciplinaria/
ISSN: 2542-3037 https://revistapt.edublogs.org/



ÉTICA CRIMINALÍSTICA: RESPONSABILIDAD EN LA ERA DIGITAL

CRIMINALISTIC ETHICS: RESPONSIBILITY IN THE DIGITAL AGE

Luis Vicente Regalado Sánchez[1,2]
1.Corporación Eléctrica Nacional, CORPOELEC, Venezuela 2.
regalado18756@gmail.com (https://orcid.org/0009-0006-8291-2127).

RESUMEN

Este ensayo examina los desafíos éticos que enfrenta la criminalística en la era digital y propone un modelo de "responsabilidad profesional reflexiva" para una práctica forense más ética. Se analiza la necesidad de una ética posmoderna y crítica que trascienda la deontología tradicional, fundamentándose en autores como Hans Jonas (2000, p. 33) (principio de responsabilidad), Shoshana Zuboff (2019, p. 25) (capitalismo de la vigilancia) y Michel Foucault (1975) (poder-saber). A través de una revisión crítica de la literatura, se exploran los dilemas éticos emergentes relacionados con la privacidad, el sesgo algorítmico, la manipulación digital y la encriptación. Se consideran las perspectivas de autores contemporáneos como Floridi (2020), Crawford (2021) y Buitenhuis et al. (2022). Se concluye que la formación integral, la conciencia crítica y la participación ciudadana son cruciales para una criminalística comprometida con la justicia social en la era digital.

Palabras clave
Ética criminalística, responsabilidad profesional, tecnocrimen, tecnologías digitales, justicia social.

Recibido: 2024-08-08 /Revisado: 2024-09-26/ Aceptado: 2024-10-24/ Publicado: 2024-12-28 / Páginas: 527-542

CRIMINALISTIC ETHICS: RESPONSIBILITY IN THE DIGITAL AGE

Luis Vicente Regalado Sánchez[1,2]
1.Corporación Eléctrica Nacional, CORPOELEC, Venezuela 2.
regalado18756@gmail.com (https://orcid.org/0009-0006-8291-2127).

ABSTRACT

This essay examines the ethical challenges facing criminalistics in the digital age and proposes a model of "reflexive professional responsibility" for a more ethical forensic practice. It analyzes the need for a postmodern and critical ethics that transcends traditional deontology, drawing on authors such as Hans Jonas (2000) (principle of responsibility), Shoshana Zuboff (2019) (surveillance capitalism), and Michel Foucault (1975) (power-knowledge). Through a critical review of the literature, emerging ethical dilemmas related to privacy, algorithmic bias, digital manipulation, and encryption are explored, considering the perspectives of contemporary authors such as Floridi (2020), Crawford (2021) and Buitenhuis et al. (2022). It concludes that comprehensive training, critical awareness, and citizen participation are crucial for criminalistics committed to social justice in the digital age.

Keywords
Forensic ethics, professional responsibility, techno-crime, digital technologies, social justice.

Received: 2024-08-08 / Revised: 2024-09-26/ Accepted: 2024-10-24/ Published: 2024-12-28 / Pages: 527-542

INTRODUCCIÓN

La criminalística, como disciplina científica en constante evolución, se encuentra en una encrucijada ética sin precedentes. La era digital, caracterizada por la omnipresencia de las tecnologías de la información y la comunicación (TIC), ha transformado el panorama del delito. Su alcance se ha ampliado, sus métodos se han sofisticado y han surgido nuevas formas de criminalidad (Casey, 2011, p. 35). El cibercrimen, por ejemplo, ha dado lugar a delitos como el robo de datos, el fraude online y la extorsión digital.

Estos delitos, según Casey (2011, p. 35), trascienden las fronteras físicas y plantean retos sin precedentes para la investigación criminal. Su abordaje efectivo requiere una colaboración internacional e interdisciplinaria (Maras, 2015, p. 15). La era digital también ha facilitado la comisión de delitos tradicionales, como el tráfico de drogas y la trata de personas. Las nuevas tecnologías proporcionan herramientas para la comunicación, la organización y la financiación de actividades ilícitas, abriendo nuevas posibilidades para el crimen organizado transnacional (*Saferstein,* 2015, p. 17).

La concepción tradicional de la ciencia forense como neutral y objetiva ha sido cuestionada a lo largo de la historia. Diversos casos y estudios han demostrado cómo la parcialidad, la manipulación de pruebas y las presiones externas pueden corromper la práctica pericial y afectar la administración de justicia (*Jasanoff*, 1995, p. 25). Esta crítica se alinea con las ideas de *Foucault* (1975) sobre el poder-saber, que destaca la relación intrínseca entre el conocimiento y el poder. *Foucault* argumenta que el conocimiento científico no es neutral, sino que está moldeado por las relaciones de poder y sirve para legitimarlas.

La ética criminalística ha cobrado importancia debido a la conciencia del impacto social de la prueba pericial, el avance de los derechos humanos y las garantías procesales (*Mnookin*, 2008, p. 15). Los nuevos desafíos éticos

en la era digital también han contribuido a este protagonismo. Se ha impulsado la necesidad de un marco ético sólido para guiar la práctica forense en un entorno tecnológico en constante cambio (*Garland,* 2016, p. 12).

Este ensayo estudia la compleja relación entre la ética y la criminalística en la era digital, buscando aportar al acervo científico una reflexión crítica que contribuya a la construcción de una práctica forense más responsable y socialmente justa. Su relevancia radica en abordar problemáticas que impactan directamente en la solución de problemas sociales, tecnológicos y productivos.

En el ámbito social, este ensayo analiza cómo los dilemas éticos de la criminalística digital afectan a la protección de los derechos humanos, la garantía de un juicio justo y la construcción de una sociedad más equitativa. En el ámbito tecnológico, esta indagación explora las implicaciones éticas del uso de algoritmos, la inteligencia artificial y otras tecnologías emergentes en la investigación criminal. Se abre un espacio para la reflexión sobre el diseño e implementación de estas tecnologías, considerando la creciente influencia de las corporaciones tecnológicas en el desarrollo y aplicación de la IA (Noble, 2018, p. 23).

Finalmente, en el ámbito productivo, la investigación destaca la importancia de una ética sólida en la criminalística para generar confianza en el sistema de justicia, la protección de la propiedad intelectual y la seguridad de las transacciones digitales. Estos son elementos cruciales para el desarrollo económico y social. Se propone un modelo de "responsabilidad profesional reflexiva" que integre la conciencia crítica, el diálogo interdisciplinario y la participación ciudadana.

Este modelo se inspira en las ideas de autores como *Lynch* (2008, p. 15), así como *Feeley y Simon* (1992, p. 450), quienes abogan por una visión más amplia de la justicia penal que tenga en cuenta las dimensiones sociales y éticas de la práctica forense. El objetivo es una criminalística ética, transparente y comprometida con la justicia social.

DESARROLLO

La ética criminalística como praxis transformadora

La ética criminalística no se limita a la mera aplicación de normas y códigos deontológicos preestablecidos. En un contexto de constante cambio tecnológico y social, la ética criminalística debe ser dinámica, adaptable y fundamentada en un profundo proceso de reflexión (*National Commission on Forensic Science*, 2016, p. 15). Esta necesidad de una ética dinámica se apoya en la teoría de la responsabilidad social de las profesiones.

Dicha teoría argumenta que los profesionales tienen una responsabilidad moral que va más allá del cumplimiento de sus deberes técnicos y legales, extendiéndose al bienestar de la sociedad en su conjunto (*Bayles,* 1981, p. 25). La *National Commission on Forensic Science* (2016, p. 15) argumenta que "los códigos de ética profesional deben ser dinámicos y adaptables a los cambios en la ciencia, la tecnología y las expectativas sociales".

Para que la ética criminalística pueda cumplir con este mandato de adaptabilidad, se requiere un modelo de responsabilidad profesional que sea a la vez dinámico y reflexivo. Este modelo debe incorporar elementos de la epistemología crítica (Harding, 2004, p. 15) y la ética del discurso (Habermas, 1984, p. 25).

Los componentes del modelo

Conciencia crítica: La conciencia crítica implica un proceso de autoevaluación constante por parte del perito. Implica cuestionar sus propios supuestos, reconocer los límites del conocimiento científico y analizar las implicaciones éticas de sus decisiones. La epistemología crítica proporciona un marco teórico para desarrollar esta conciencia.

La epistemología crítica, con su énfasis en la desnaturalización del conocimiento y la identificación de los intereses que subyacen a las prácticas científicas, proporciona un marco teórico para desarrollar esta

conciencia crítica en la práctica forense. *Koppl* (2005, p. 265) argumenta que:

Los científicos forenses deben ser conscientes de que su trabajo tiene un profundo impacto en la vida de las personas. Sus conclusiones pueden llevar a la condena de un inocente o a la liberación de un culpable. Por lo tanto, es crucial que actúen con la máxima integridad, objetividad y rigor científico.

Este llamado a la conciencia crítica se fundamenta en la idea de que la ciencia forense no es un proceso puramente objetivo y neutral, sino que está influenciado por factores sociales, culturales y políticos (Cole, 2001, p. 15). La creciente complejidad del tecnocrimen demanda una reflexión crítica sobre los sesgos, las limitaciones y las potenciales consecuencias del uso de las tecnologías digitales en la investigación criminal (*Buitenhuis* et al., 2022).

Actualización constante: La actualización constante se refiere a la necesidad de que los peritos se mantengan al día con los avances científicos, tecnológicos y legales en su campo. La rápida evolución de las tecnologías digitales exige un esfuerzo permanente de capacitación y aprendizaje por parte de los profesionales forenses.

La teoría del aprendizaje continuo, que enfatiza la importancia del aprendizaje a lo largo de la vida para adaptarse a un mundo en constante cambio (*Merriam & Caffarella,* 1999, p. 25), proporciona un fundamento para este componente. *Saferstein* (2015, p. 17) señala la importancia de la actualización constante en el contexto de la era digital:

La convergencia de la tecnología y la globalización ha creado un nuevo panorama de riesgos y oportunidades para la ciencia forense. Los delincuentes utilizan cada vez más la tecnología para cometer delitos, y los científicos forenses deben estar preparados para afrontar estos nuevos desafíos.

Esta necesidad de actualización se vuelve aún más crucial en el contexto de la inteligencia artificial, donde los avances en algoritmos y

técnicas de aprendizaje automático están transformando rápidamente el panorama de la investigación criminal (Interpol, 2021, p. 5).

Diálogo interdisciplinario: El diálogo interdisciplinario implica la colaboración y el intercambio de conocimientos con profesionales de otras disciplinas relevantes para la investigación criminal, como el derecho, la informática, la sociología y la psicología. La complejidad de los casos contemporáneos, especialmente aquellos que involucran tecnologías digitales, exige una perspectiva holística que solo puede lograrse a través del diálogo interdisciplinario (*Klein*, 1990, p. 25).

La teoría de la complejidad, con su énfasis en la interconexión de los sistemas y la necesidad de abordajes transdisciplinarios para comprender fenómenos complejos (*Mori*n, 2008, p. 15), proporciona una base teórica para este componente. *Casey* (2011, p. 35) enfatiza la importancia de la interdisciplinariedad en la investigación del cibercrimen:

Las fronteras nacionales se han vuelto porosas en el ciberespacio, y los delincuentes aprovechan esta realidad para operar desde cualquier parte del mundo. Esto plantea importantes desafíos para las fuerzas del orden, que deben encontrar nuevas formas de cooperar y compartir información para combatir el cibercrimen de manera efectiva.

La necesidad de colaboración interdisciplinaria se vuelve aún más relevante en el contexto del tecnocrimen, donde la comprensión de las dimensiones sociales, culturales y políticas del delito digital se vuelve crucial (*Holt & Bossler*, 2014, p. 15).

Participación ciudadana: La participación ciudadana implica la apertura al diálogo con la sociedad, la transparencia en la comunicación del trabajo pericial y la consideración de las preocupaciones y expectativas ciudadanas. La teoría democrática deliberativa proporciona un marco para este componente.

La teoría democrática deliberativa, que enfatiza la importancia de la participación ciudadana informada en la toma de decisiones que afectan a la sociedad (*Gutmann & Thompson*, 2004, p. 25), proporciona un marco

para este componente. Además, la inclusión de la perspectiva ciudadana se alinea con las ideas de la justicia restaurativa.

La justicia restaurativa busca reparar el daño causado por el delito a través de la participación de todas las partes involucradas. En la era digital, la participación ciudadana es crucial para abordar las preocupaciones sobre la privacidad, la vigilancia y el uso responsable de las tecnologías en la investigación criminal (*Roberts*, 2021, p. 25).

Dilemas éticos en la era del tecnocrimen

La convergencia de la criminalística con el mundo digital genera una serie de dilemas éticos que son abordados por diversos autores en el campo de la ética y la tecnología (*Casey*, 2011, p. 35; *O'Neil*, 2016, p. 23; *Taddeo & Floridi*, 2018, p. 296; *Solove,* 2004, p. 25):

Privacidad vs. Seguridad: El uso de tecnologías de vigilancia masiva plantea un dilema entre la privacidad individual, considerada un derecho humano fundamental, y la necesidad de garantizar la seguridad pública. La teoría del equilibrio entre la libertad y la seguridad busca encontrar un punto medio entre la protección de los derechos individuales y la seguridad del Estado (*Etzioni*, 2003, p. 25).

Se debe cuestionar la legitimidad del acceso a información personal sin consentimiento judicial y garantizar que no se use para fines discriminatorios. Este dilema se intensifica en la era digital, donde las tecnologías de vigilancia se vuelven cada vez más sofisticadas e invasivas (*Lyon*, 2018, p. 15).

Sesgo algorítmico: Los algoritmos utilizados en la criminalística, como los sistemas de predicción de la reincidencia criminal, pueden perpetuar sesgos existentes en los datos con los que se entrenan. Esto puede llevar a la discriminación de ciertos grupos sociales, violando principios de justicia distributiva y equidad (*Rawls*, 1971, p. 25).

La teoría de la justicia algorítmica, que busca identificar y mitigar los sesgos en los algoritmos para asegurar que sus decisiones sean justas e imparciales (*Barocas & Selbst*, 2016, p. 671), es fundamental para abordar

este dilema. *O'Neil* (2016, p. 23) advierte sobre el potencial de los algoritmos para perpetuar la desigualdad y la discriminación:

Los algoritmos... son opiniones incrustadas en código. Y, sin embargo, a menudo se los trata como objetivos y científicos. Los algoritmos establecen quién recibe un préstamo, quién es contratado para un trabajo, quién es admitido en la universidad y quién es considerado un riesgo para la seguridad.

Este problema se ha vuelto cada vez más preocupante, ya que los algoritmos sesgados pueden tener un impacto negativo significativo en la vida de las personas (Benjamin, 2019, p. 25).

Manipulación de la evidencia digital: La facilidad para alterar archivos digitales, como imágenes y videos, plantea un desafío para la autenticación de la evidencia. La teoría de la evidencia digital, que establece los principios y procedimientos para la recopilación, preservación y análisis de la evidencia digital (*Carrier & Spafford*, 2004, p. 25), es esencial para asegurar la integridad de las pruebas.

Se debe asegurar la autenticidad de la evidencia digital y preservar la cadena de custodia. El desarrollo de tecnologías de manipulación de imágenes y videos, como los *deepfakes*, ha intensificado este desafío, creando nuevas preocupaciones sobre la confiabilidad de la evidencia digital (*Chesney & Citron*, 2019, p. 147).

En este mismo sentido, el acceso a dispositivos encriptados: La encriptación, utilizada para proteger la privacidad de las comunicaciones y datos digitales, puede dificultar el acceso a evidencia crucial para una investigación criminal. Este dilema se enmarca en la teoría del derecho a la privacidad en la era digital, que busca equilibrar la necesidad de seguridad y la protección de la privacidad en el contexto de las nuevas tecnologías (*Kerr*, 2004, p. 501).

Se debe equilibrar la necesidad de investigar con el derecho a la privacidad y seguridad digital. *Taddeo y Floridi* (2018, p. 296) abordan la

tensión entre la seguridad nacional y el derecho a la privacidad en el contexto de la encriptación:

La inteligencia artificial está entrando en una nueva era caracterizada por la proliferación de capacidades de doble uso, que tienen aplicaciones tanto civiles como militares, y por la aceleración en el desarrollo de sistemas autónomos letales. Si no se regula adecuadamente, esta nueva era podría llevar a una carrera armamentista en la que los Estados compitan por desarrollar las armas de IA más sofisticadas.

Este dilema se ha vuelto cada vez más complejo a medida que la tecnología de encriptación avanza y se vuelve más accesible (*Abelson* et al., 2015, p. 25).

El principio de responsabilidad y el capitalismo de la vigilancia

La era digital nos sitúa ante una encrucijada ética. El principio de responsabilidad de *Hans Jonas* (2000, p. 33) cobra vigencia. Este principio, basado en la ética de la responsabilidad, enfatiza la responsabilidad de proteger a las generaciones futuras de las consecuencias de nuestras decisiones tecnológicas:

Actúa de tal modo que los efectos de tu acción sean compatibles con la permanencia de una vida humana auténtica en la Tierra.

En criminalística, este principio implica reflexionar sobre el impacto a largo plazo del uso de nuevas tecnologías. El capitalismo de la vigilancia reclama unilateralmente la experiencia humana como materia prima gratuita para traducirla en datos de comportamiento. Estos datos son computados y empaquetados como productos de predicción que se comercian en un nuevo mercado de futuros conductuales.

Implicaciones para la práctica forense

Conciencia del poder de la tecnología: Los criminalistas deben ser conscientes del poder de las herramientas que utilizan y del impacto de sus decisiones. Deben reconocer la capacidad de las tecnologías digitales para

afectar la vida de las personas y la sociedad (*Goodman & Flaxman*, 2017, p. 25; *Floridi*, 2020, p. 15).

Evaluación crítica de los algoritmos: Se deben identificar y mitigar los posibles sesgos en los algoritmos. Se debe asegurar que su uso en la investigación criminal se realice de forma justa, transparente y responsable (*O'Neil*, 2016, p. 23; *Crawford*, 2021, p. 15).

Goodman y Flaxman (2017, p. 25) defienden el derecho a la explicación en el uso de algoritmos que toman decisiones que afectan a las personas. Argumentan que la transparencia y la rendición de cuentas son fundamentales para garantizar la justicia y la equidad.

Protección de la privacidad: Se deben recopilar y analizar datos con apego a la ley y respeto a la privacidad. Se debe reconocer el derecho a la privacidad como un derecho humano fundamental (*Zuboff,* 2019, p. 25; *Solove*, 2004, p. 25; *Schneier*, 2015, p. 15).

Responsabilidad por las consecuencias: Se debe asumir la responsabilidad por el impacto del trabajo, incluyendo las consecuencias a largo plazo. Se debe reconocer que las decisiones tomadas en el ámbito forense pueden tener un impacto duradero en la vida de las personas (*Jonas,* 2000, p. 33).

Promoción de la justicia social: Se deben utilizar las ciencias forenses para proteger a los vulnerables, combatir la discriminación y promover la equidad. Se debe asegurar que la aplicación de la ciencia forense contribuya a la construcción de una sociedad más justa (*National Commission on Forensic Science,* 2016, p. 15).

HALLAZGOS

El análisis de la literatura sobre ética criminalística en la era digital revela los siguientes hallazgos:

Necesidad de una ética posmoderna: La ética criminalística tradicional, basada en la deontología y el rigor metodológico, se queda corta ante la complejidad de los desafíos éticos planteados por el tecnocrimen.

Importancia de la responsabilidad profesional reflexiva: Un modelo de responsabilidad profesional que integre la conciencia crítica, la actualización constante, el diálogo interdisciplinario y la participación ciudadana se vuelve crucial para asegurar una práctica forense ética en la era digital.

El principio de responsabilidad como guía: El principio de responsabilidad de *Hans Jonas* ofrece un marco ético fundamental para considerar las implicaciones a largo plazo del uso de nuevas tecnologías en la investigación criminal.

Los peligros del capitalismo de la vigilancia: El modelo económico basado en la extracción masiva de datos para la vigilancia y el control del comportamiento plantea serios desafíos éticos para la privacidad, la autonomía y la justicia social.

CONCLUSIONES

La ética criminalística en la era digital exige un cambio de paradigma que vaya más allá de la simple aplicación de códigos deontológicos. Este ensayo aporta al debate sobre la ética profesional al destacar la necesidad de una "responsabilidad profesional reflexiva" que sea dinámica, contextualizada y crítica.

La "responsabilidad profesional reflexiva" se configura como un modelo necesario para afrontar los dilemas éticos generados por el tecnocrimen. Este modelo, basado en la integración de la conciencia crítica, la actualización constante, el diálogo interdisciplinario y la participación ciudadana, busca revitalizar la teoría de la responsabilidad social de las profesiones (*Bayles*, 1981, p. 25) en el contexto de la criminalística digital.

La formación de los criminalistas debe integrar la ética, la tecnología y las ciencias sociales para promover una práctica forense consciente, crítica y socialmente responsable. Este ensayo aporta a la teoría educativa al destacar la necesidad de una formación integral que equipe a los futuros criminalistas con las herramientas necesarias para navegar los desafíos éticos de la era digital. Se toman en cuenta las perspectivas de la

epistemología crítica (*Harding*, 2004, p. 15) y la ética del discurso (*Habermas*, 1984, p. 25).

La participación ciudadana y el debate público son fundamentales para asegurar que el desarrollo y la aplicación de las ciencias forenses se realicen de manera ética y contribuyan al bienestar de la sociedad. Este ensayo contribuye a la teoría democrática deliberativa (*Gutmann & Thompson*, 2004, p. 25) y la justicia restaurativa (*Zehr,* 2002, p. 15) al enfatizar la importancia de la participación ciudadana informada en la configuración de la práctica forense.

Posibles investigaciones a partir de los aportes del estudio:

- Estudios empíricos sobre la implementación del modelo de "responsabilidad profesional reflexiva" en la formación y la práctica de los criminalistas.
- Análisis comparativo de los marcos legales y éticos para la investigación del cibercrimen en diferentes países.
- Desarrollo de herramientas y metodologías para la detección y mitigación de sesgos en los algoritmos utilizados en la criminalística.
- Investigación sobre la percepción pública de la ética criminalística en la era digital y su impacto en la confianza en el sistema de justicia.
- Estudios sobre las implicaciones éticas del uso de tecnologías emergentes, como la inteligencia artificial y el *blockchain,* en la investigación criminal.

REFERENCIAS

Abelson, H., Ledeen, K., & Lewis, H. (2015*). Keys under doormats: Mandating insecurity by requiring government access to all data and communications*. MIT Press.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104, 671-732.

Bayles, M. D. (1981). Professional ethics. *Wadsworth Publishing Company*.

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new jim code.* Polity.

Buitenhuis, H., van der Hof, S., & van der Sloot, B. (2022). Responsible AI in criminal justice: Towards a framework for assessment and implementation. *AI and Ethics*, 2(4), 1-14. https://doi.org/10.1007/s43681-022-00211-4

Carrier, B., & Spafford, E. H. (2004). *Getting physical: A forensic approach to investigating computer crime.* Addison-Wesley Professional.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3.a ed.). *Academic Press.*

Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147-155.

Cole, S. A. (2001). *Suspect identities: A history of fingerprinting and criminal identification. H*arvard University Press.

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

Etzioni, A. (2003). *The limits of privacy*. Basic Books.

Feeley, M. M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, 30(4), 449-474.

Floridi, L. (2020). *The ethics of information*. Oxford University Press.

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

Garland, D. (2016). *The culture of control: Crime and social order in contemporary society* (2.a ed.). Oxford University Press.

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation". *AI Magazine*, 38(3), 50-57.

Gutmann, A., & Thompson, D. (2004). *Why deliberative democracy*? Princeton University Press.

Habermas, J. (1984). *The theory of communicative action*. Beacon Press.

Harding, S. (2004). *The feminist standpoint theory reader: Intellectual and political controversies.* Routledge.

Holt, T. J., & Bossler, A. M. (2014). *Cybercrime and digital forensics: An introduction*. Routledge.

Interpol. (2021). *Artificial intelligence for law enforcement*. New York: autor

Jasanoff, S. (1995). *Science at the bar: Law, science, and technology in America.* Harvard University Press.

Jonas, H. (2000). *El principio de responsabilidad: Ensayo de una ética para la civilización tecnológica*. Herder Editorial.

Kerr, O. S. (2004). A user's guide to the law of internet surveillance. *The Journal of Criminal Law and Criminology,* 94(2), 501-546.

Klein, J. T. (1990). *Interdisciplinarity: History, theory, and practice*. Wayne State University Press.

Koppl, R. (2005). How to improve forensic science. *European Journal of Law and Economics,* 20(3), 255–286.

Lynch, M. (2008). *Truth machine: The contentious history of DNA fingerprinting.* University of Chicago Press.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity.

Maras, M. H. (2015). *Cybercrime and cyberterrorism: Investigating internet crimes and criminals.* ABC-CLIO.

Merriam, S. B., & Caffarella, R. S. (1999). *Learning in adulthood: A comprehensive guide* (2.a ed.). Jossey-Bass Publishers.

Mnookin, J. L. (2008). *The search for certainty: Confronting the limits of knowledge and the search for absolute truth*. W. W. Norton & Company.

Morin, E. (2008). *On complexity*. Hampton Press.

National Commission on Forensic Science. (2016). *Report on Professional Ethics Codes for Forensic Science Providers*. U.S. Department of Justice.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism.* NYU Press.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishers.

Rawls, J. (1971). *A theory of justice*. Harvard University Press.

Roberts, H. (2021). *Technology, ethics and the everyday*. Routledge.

Saferstein, R. (2015). *Criminalistics: An introduction to forensic science* (11.a ed.). Pearson Education.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world.* W. W. Norton & Company.

Solove, D. J. (2004). *Digital person: Technology and privacy in the information* age. NYU Press.

Taddeo, M., & Floridi, L. (2018). *Regulate artificial intelligence to avert cyberarms race. Nature,* 556(7701), 296-298. https://doi.org/10.1038/d41586-018-05449-3

Zehr, H. (2002). *The little book of restorative justice*. Good Books.

Zuboff, S. (2019). *La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder*. Paidós.