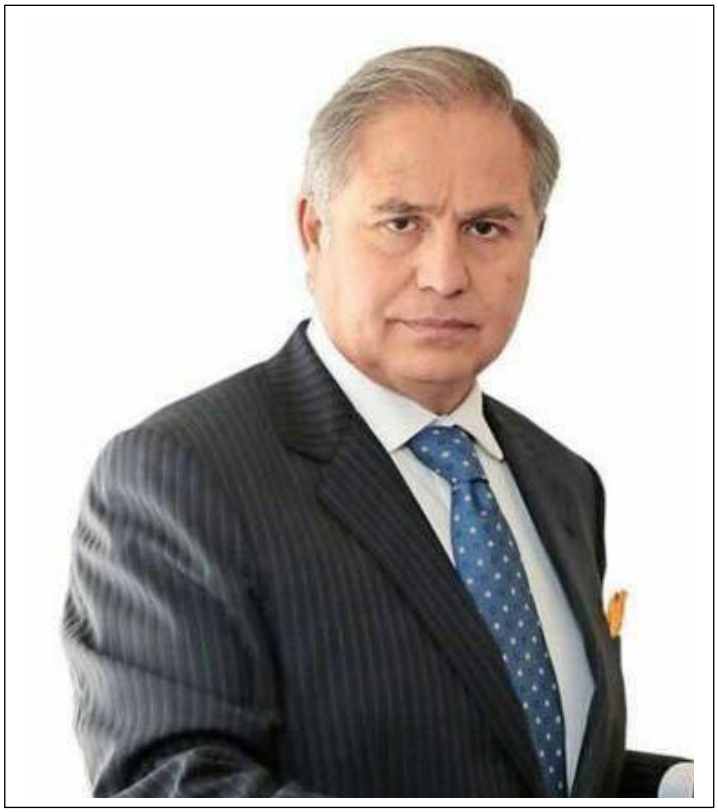
MANRIQUEZ BENAVIDES & CÍA
Abogados

PRIVACY RULES



# IA en la "predicción delictiva": Criminología y Política Criminal en base a Algoritmos. Ventajas y Riesgos.


Expert name:
Juan Carlos Manríquez
Expert position:
Founder, Partner


## Expert presentation

***LLM, Lawyer since 1991, 26 years of experience advocating & advising in Chile, Peru, Ecuador, USA and Argentina in cases of economic crime, environmental crime, tax fraud, political issues and data protection before higher jurisdictions in Chile such as the Supreme Court of Justice, the Constitutional Court and the Court of Appeals. Juan Carlos regularly lectures at national and international level, including on Strategic Litigation at the National School of Fiscal Prosecutors in Perù; at the Environment and Economic Crimes Unit of National Fiscal Prosecutors Office in Argentina; is a recurrent advisor of the Constitutional, Justice and Law Commission of the Chilean Parliament and of the Chilean Defence and Justice Ministries. He is the former President and Chairman of the Bar Association of Valparaiso; Member of the International Association of Penal Law (AIDP), and certified attendant in the Siracusa International Institute for Criminal Justice and Human Rights, within the international programme for lawyers and counsels on Human Rights protection before International Courts.***


Contact details
Firm: http://mbcia.cl/
Email: jcmanriquez@mbcia.cl
Phone number: +56 32 2231080

# IA en la "predicción delictiva": Criminología y Política Criminal en base a Algoritmos. Ventajas y Riesgos.

1. Estado del asunto.

El desarrollo de la Internet de las Cosas (IoT), que es la la capacidad interconectada de los equipos con memoria y capacidad de transmisión de la información que recolectan y almacenan sobre nuestra conducta, desplazamientos, opciones y gustos, que es la misma que llega a controladores y tratantes de las Bases de Dato que las recogen, ya sea para para comerciar con ellas o para engrosamiento del Big Data, son el "nuevo petróleo" que hace moverse a la sociedad de información.

Si ya Hoover, fundador del FBI, descubrió que la información era Poder puro, y sentó los pilares rudimentarios de los modernos sistemas de tratamiento de datos para fines de perfilamiento, hoy la tarea es enorme. Sólo decir por mínimo rigor histórico, que uno de los primeros perfiladores estadounidense fue el también agente del FBI John E. Douglas, quien tuvo un rol decisivo en el desarrollo de la ciencia del comportamiento (Jackson, JL, y Bekerian, DA (1997). Delincuente perfiles: investigación, teoría y práctica/ Chicester: Wiley.

Turvey, BE (1999). Perfiles criminales: Una Introducción al análisis de la evidencia conductual. San Diego: Academic).

Los actuales desarrolladores de métodos de Inteligencia Artificial (AI) y Algoritmos Predictivos tienen en la web y las plataformas de redes sociales una cantera casi inagotable de millones de teras de información que se genera por cada segundo a nivel global. La Net es una mina de oportunidades.

En este contexto, la predictibilidad de comportamientos delictivos nacionales e internacionales, interpretados dentro de propuesta sociológica que ya en 1986 hiciera Ulrich Beck con la "sociedad del riesgo", toma particular interés y necesidad.

PRIVACY RULES

***Headquarters:***
*3491 Forestoak Court*
*Cincinnati, Ohio 45208, United States of America*
*Website: www.privacyrules.com*
*Email: info@privacyrules.com*

Aunque como todo, hace igualmente necesario evaluar sus pro y contra, particularmente desde la óptica del balance que debe hacerse con toda política pública intensiva e intrusiva, entre seguridad y dignidad humana; entre la restricción y la libertad de las personas.

Cuando acechan nuevos peligros, que requieren de nuevas herramientas dotadas de legitimidad, se necesita que no avasallen derechos y garantías fundamentales, y que su uso justifique la restricción temporal de derechos cuando la amenaza general supera el bien individual, y se imponga el deber de ceder.

2. Estudios recientes:

El algoritmo es una herramienta de IA. Se dice que son alrededor de 10 los más conocidos, y los hay de tipos diversos. En general el algoritmo es "un conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo de problemas."

Cuando el problema es saber si por su comportamiento en la red una IP asociada a un usuario "está por cometer un delito" y justificaría la alerta de posible intervención del sistema penal, el tema es acuciante, porque el "principio del acto" o de "exteriorización", dice que sólo hay delito "cuando éste comienza a ponerse por obra" a través de un comportamiento (activo u omisivo), que es perceptible. "Cogitationis Poenam Nemo Patitur" (los pensamientos no se castigan).

Si la dirección IP es "un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop , teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.", entonces cada vez que la IP se activa y su movimiento se acerca a una tentativa delictiva, sería materia del sistema penal (arts. 1 y 7 en clave del Código Penal chileno).

En el contexto global veamos cómo se ha ido aplicando, y para qué, el modelo predictivo en base a algoritmos usados en herramientas de IA para adelantar o detectar ciertos delitos.



***Headquarters:***
*3491 Forestoak Court*
*Cincinnati, Ohio 45208, United States of America*
*Website: www.privacyrules.com*
*Email: info@privacyrules.com*

A. Delitos de fraude y robo en el sistema bancario: ensayo y error.

Los modelos predictivos algorítmicos en delincuencia económica han demostrado ser aplicables y han otorgado relevante información para mejorar los sistemas de Compliance, así como perfilar más certeramente la "anticipación de comportamientos esperados" en ciertos empleados o clientes, que por acercarse a "perfiles de riesgo" ya trazados o "adivinables" estarían más propensos a cometer lavado de activos, robos, delitos informáticos, fuga de datos, o fraudes con facturación falsa, por ejemplo.

- "Las empresas están utilizando IA para prevenir y detectar todo, desde el robo rutinario de empleados hasta el uso de información privilegiada. Muchos bancos y grandes corporaciones emplean inteligencia artificial para detectar y prevenir el fraude y el lavado de dinero. Las empresas de medios sociales utilizan el aprendizaje automático para bloquear contenido ilícito como la pornografía infantil. Las empresas están experimentando constantemente nuevas formas de utilizar la inteligencia artificial para una mejor gestión de riesgos y una detección de fraudes más rápida y receptiva, e incluso para predecir y prevenir delitos.

Si bien la tecnología básica actual no es necesariamente revolucionaria, los algoritmos que utiliza y los resultados que pueden producir sí lo son. Por ejemplo, los bancos han estado utilizando sistemas de monitoreo de transacciones durante décadas basados en reglas binarias predefinidas que requieren que la salida se verifique manualmente. La tasa de éxito es generalmente baja: en promedio, solo el 2% de las transacciones marcadas por los sistemas en última instancia reflejan un delito real o una intención maliciosa. Por el contrario, las soluciones actuales de aprendizaje automático utilizan reglas predictivas que reconocen automáticamente las anomalías en los conjuntos de datos. Estos algoritmos avanzados pueden reducir significativamente la cantidad de alertas falsas al filtrar los casos que se marcaron incorrectamente, mientras se descubren otros perdidos utilizando las reglas convencionales."

Dicen Quest, Charrie, du Croo de Jongh y Subas Roy en "The Risks and Benefits of Using AI to Detect Crime"

https://hbr.org/amp/2018/08/the-risks-and-benefits-of-using-ai-to-detect-crime



***Headquarters:***
*3491 Forestoak Court*
*Cincinnati, Ohio 45208, United States of America*
*Website: www.privacyrules.com*
*Email: info@privacyrules.com*

B. Instagram y trackeo del "Drugs Dealing".

El uso expandido de las plataformas más actuales que día a día van adecuándose a los gustos de los usuarios millenials y centenials, que los "boomers" no dominamos del todo, han ido siendo un caldo de cultivo perfecto para la adecuación del mercado delictivo más moderno, en especial para el tráfico de drogas, que a través de ellas ha ido mejorando sus canales de oferta y distribución, así como sus políticas de captación de nuevos usuarios.

Un estudio reciente sobre la red social Instagram arroja sorprendentes resultados, que se lograron aplicando herramientas de IA y de análisis de los Emoji más comúnmente usados:

- "De las 12,857 publicaciones que recopilamos, detectamos 1228 publicaciones de traficantes de drogas que comprenden 267 usuarios únicos. Utilizamos la validación cruzada para evaluar los 4 modelos, con nuestro modelo de aprendizaje profundo alcanzando el 95% en la puntuación F1 y obteniendo mejores resultados que los otros 3 modelos. También descubrimos que al eliminar los hashtags en el texto, el modelo tenía un mejor rendimiento.

Las publicaciones detectadas contenían hashtags relacionados con varias drogas, incluida la sustancia controlada Xanax (1078/1228, 87.78%), oxicodona / OxyContin (321/1228, 26.14%) y drogas ilícitas dietilamida de ácido lisérgico (213/1228, 17.34%) y 3,4-metilendioxi-metanfetamina (94/1228, 7,65%).

También observamos el uso de aplicaciones de comunicación para el presunto tráfico de drogas a través de los comentarios de los usuarios.

Conclusiones:

Nuestro enfoque utilizando una combinación de raspado web y aprendizaje profundo fue capaz de detectar vendedores ilegales de drogas en línea en Instagram, con alta precisión.

A pesar de un mayor escrutinio por parte de los reguladores y los formuladores de políticas, la plataforma de Instagram continúa recibiendo publicaciones de traficantes de drogas, en violación de la ley federal.



***Headquarters:***
*3491 Forestoak Court*
*Cincinnati, Ohio 45208, United States of America*
*Website: www.privacyrules.com*
*Email: info@privacyrules.com*

Se deben tomar medidas adicionales para garantizar la seguridad de las comunidades de redes sociales y ayudar a poner fin a este canal digital ilícito de abastecimiento."

En Medical Internet Research Jiawei Li, MS, Qing Xu, MAS, and Tim K Mackey, MAS, PhD. "A Machine Learning Approach for the Detection and Characterization of Illicit Drug Dealers on Instagram: Model Evaluation Study"https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598421/

3. Ventajas:

Como vemos, los dos ejemplos previos dan cuenta de innegables ventajas, al hacer más estricta y casi más certera la posibilidad de intervención del sistema criminal y la fortaleza probatoria en perspectiva de juicio oral.

Sin ir más lejos, en Chile dotarían más eficacia a nuestra añosa ley 19.223 sobre delitos informáticos y a la 20.009 sobre fraudes asociados a tarjetas de crédito (actualmente en modificación en el Parlamento, Boletín 11.078-03), por una parte, y por otra, pondrían más presión a real capacidad de evitación de los modelos de prevención de lavado de activos, conforme a las leyes 19.223 y 20.393, sobre responsabilidad penal de la persona jurídica.

4. Riesgos:

Pero también el uso indiscriminado y poco riguroso de estas herramientas apareja peligros graves.

A. Para la Empresa Privada:
   Pérdida de prestigio por la detección errónea de "falsos positivos" (ejemplo "aparentes" mecheros), que eran clientes distintos a los habituales, o por el despido de trabajadores que "iban" a robar etc, con o ingentes demandas civiles por difamación o daños a cuestas.

B. Para el Estado y el Sistema de Justicia Penal:

a) Sesgo y discriminacion: Reconocimiento Facial (FR) y Reconocimiento de Emociones (ER).



***Headquarters:***
*3491 Forestoak Court*
*Cincinnati, Ohio 45208, United States of America*
*Website: www.privacyrules.com*
*Email: info@privacyrules.com*

Los controles de identidad o intervención preventiva de "potenciales asaltantes" en barrios cuyas IP habitualmente no circulan por ahí, o cuyo Reconocimiento Facial no lo ubica en ese "Cuadrante", por el problema que aún tienen muchas cámaras de seguridad ciudadana en el 1:N o en movimiento, o por su alto pixelado, etc, pueden configurar una política criminal de prevención especial negativa anti democrática e inconstitucional, además de atentatoria contra el derecho internacional de los DDHH.

Hemos referido antes los estudios que denuncian al Reconocimiento de Emociones (ER) como una fuente de sesgo discriminatorio en contratación laboral de personas LGTBI+ que no develan su opción sexual o condición de minoría por miedo al rechazo. Y en contexto de psicología del testimonio, los parámetros que aporta su uso deben ser tenidos solo como un indicio más, a valorarse en el contexto, y no como una sólida "prueba independiente", al depender en alto grado del subjetivismo del interrogador o del sentenciador.

Así en https://www.bbc.com/mundo/amp/noticias-44860540

b) FR, Bases de Dato Policiales, Control de Identidad, Mapeo, GeoReferencia y Politica Criminal basada en prejuicio.

Un 96% de error arrojó el sistema de FR de la Policía Metropolitana de Londres, según un estudio de FOI (Freedom of Information).

En Chile, de la Fundación Datos Protegidos, Danny Rayman ha dicho que casos como el de Inglaterra demuestran que la tecnología de FR es un riesgo para las personas.

Señaló tiempo atrás que la PDI informó que, en las pruebas de implementación del sistema, 9 de cada 10 casos fueron identificados incorrectamente".

5. Proyección y Limites Tolerables.



***Headquarters:***
*3491 Forestoak Court*
*Cincinnati, Ohio 45208, United States of America*
*Website: www.privacyrules.com*
*Email: info@privacyrules.com*

Como vemos, si bien los avances y aportes de la IA son innegables, e imparables, su admisión y aplicación no puede estar exenta de un necesario filtro normativo, constitucional, de deberes, libertades públicas y DDHH.

Solo así se podrá configurar en el Congreso una política criminal balanceada y respetuosa de la dignidad humana y del derecho internacional y se podrá reforzar las reglas que gobiernan el Estado de Derecho 4.0 en que se asienta la web, esa que aunque a-territorial y a-espacial no es, ni puede ser, un mar de anomia e impunidad.

**Juan Carlos Manríquez R.**

***Lawyer, LLM***

***UC- UCV Professor***

***Litigator before the International Criminal Court and the IACHR***

***Member of PrivacyRules International***

***Headquarters:***
*3491 Forestoak Court*
*Cincinnati, Ohio 45208, United States of America*
*Website: www.privacyrules.com*
*Email: info@privacyrules.com*