ENSEÑANZA DEL DERECHO INFORMATICO.EL LENGUAJE DE UN DERECHO PENAL TECNOLOGIZADO.

Horacio Enrique Maidana [1]

Innovación es la palabra que define el impacto del avance tecnológico, y que más allá de nosotros, se impone como una realidad proponiéndonos una mirada hacia el futuro a la vez que nos desafía a ampliar el campo de la enseñanza del derecho informático para incorporar un nuevo lenguaje, y nuevas herramientas tecnológicas para la investigación del cibercrimen y de los ciberdelitos.

En este contexto enseñar derecho informático, y más específicamente comprender la complejidad en la que se desarrolla y tiene lugar el cibercrimen y la ciberdelincuencia, requiere de un plus proporcionado por el conocimiento sobre el funcionamiento básico de los dispositivos más comúnmente utilizados, de sus posibilidades técnicas, de las estructuras básicas de redes y arquitecturas de hardware y software de código abierto entre otros temas, además de un conocimiento actualizado de los desarrollos más importantes en materia de tecnología

Al respecto, poco o nada se ha debatido, sobre cómo debe enseñarse el derecho informático, a pesar de la constante producción bibliográfica, no es fácil encontrar textos que se refieran a la didáctica o a la pedagogía para la enseñanza de los denominados delitos informáticos, no obstante, la realidad impone una necesaria revisión sobre las metodologías, estrategias, y objetivos planteados respecto a la enseñanza de esta disciplina.

En el caso de los contenidos, la mayoría de los programas de pos grado o especializaciones, si bien abordan la temática, lo hacen desde un plano

[1] Profesor y docente auxiliar de la materia *"Epistemología y Metodología de la Investigación"* del Profesorado en Ciencias Jurídicas, Facultad de Derecho. UBA. Resol. (D.) N° 18.113/16.Email: horacioenriquemaidana@derecho.uba.ar

meramente teórico basado en el análisis jurídico de las figuras delictivas, sin referencia directa a los aspectos técnicos que se necesitan conocer para comprender como fueron los hechos. Desde el punto de vista procesal, actualmente las pruebas tradicionales están migrando desde el papel hacia los entornos virtuales, es así que la trazabilidad de los datos se convierte en un activo de relevancia. En un caso dado, estos indicios y evidencias facilitan la determinación precisa de la ubicación, fecha y hora de inicio, mecanismos y procesos empleados como medios de comisión de un delito, así como también permiten deducir la magnitud del daño causado, el resultado final, la fecha y la hora de finalización de una acción delictiva, entre otros datos posiblespara la investigación penal, por lo que resulta conveniente hacer algunas aclaraciones.

El investigador debe saber, y para eso alguien debe enseñarle, que por su carácter altamente volátil, los datos en la memoria principal deben capturarse antes de cualquier otra actividad, como por ejemplo, antes de la adquisición del contenido del disco rígido, el que usualmente es utilizado como primer recurso para realizar la copia espejo. El análisis de la memoria principal puede ayudar a inferir el uso que se le da al equipo, o detectar indicios que soporten una hipótesis particular.

En el mismo sentido, solo si el investigador conoce las posibilidades técnicas de un dispositivo puede solicitar y enumerar puntos de pericias que coadyuven a dilucidar el caso, cuando no tenga los conocimientos mínimos, podrá estar generando solicitudes innecesarias, sobreabundantes o erróneas que pueden fácilmente ser pasibles de nulidad procesal.Como se ve, tendremos que buscar nuevas formas de escribir el derecho, necesitamos cambiar rápidamente para adaptarlo a un nuevo lenguaje, actualizarlo e intentar incorporar las herramientas disponibles desde la tecnología, para utilizarlas de forma eficiente en la investigación de los ciberdelitos y del cibercrimen.

El interrogante es el atributo intelectual que nos distingue de las máquinas, aún de las más modernas formas de inteligencia artificial, y basta con formular algunas preguntas para corroborar esta afirmación, ¿cómo puede un agente que interviene en la investigación de un ciberdelito, asesorar o proponer la

pertinencia o de una medida anticipada de prueba si desconoce las posibilidades técnicas de la evidencia digital, su carácter volátil, la facilidad de su alteración, adquisición o resguardo?, ¿Cómo podría aun hoy, desconocer el potencial de la bigdata o de las herramientas OSINT y su impacto para ser utilizadas en la investigación penal?

Ahora bien, teniendo en cuenta que, el nivel de aptitud promedio del delincuente informático, hacker o como se quiera llamar, supera, en relación al manejo de las TICs, al de muchos operadores jurídicos, (esto es un hecho, pero no por ello vamos a quedarnos sin hacer nada), se hace necesario más que nunca acortar esta brecha o superar la relación de capacidades, y ello, sin dudas es un problema que se resuelve con la capacitación de los actores involucrados.

No se cree imprescindible que el operador jurídico relacionado con los delitos informáticos tenga que ser ingeniero, pero si, que es necesario que conozca, cuanto menos, las estructuras básicas de los procesos técnicos, y las distintas posibilidades de los dispositivos comprometidos o de los utilizados como medio para la comisión de las diversas modalidades delictivas, más aún es imprescindible la comprensión del lenguaje nativo que sustenta la estructura que nos está conectando con el mundo, y que está implícito en las tecnologías de aprendizaje trascendente.

Enseñar derecho informático y en especial, el capítulo de cibercrimen y ciberdelitos requiere comprenderlos cinco temas que más impacto tienen en relación a la investigación penal en la actualidad; **a)** Deep Web, **b)** Big Data, **c)** Inteligencia Artificial, **d)** Cloud Computing, **e)**OSINT –Open Source Intelligence. Como afirma Luis Wells **(1),***"La vanguardia no existe más. Hoy el asombro viene de la tecnología, no del arte"*

---

(1) Luis Wells. Entrevista suplemento Idea del diario La Nación, 25 de septiembre de 2015.