Evidencia digital y pericia informática: desafíos estratégicos.

Por: Mario Ramón Duarte. alainet.org. 12/11/2020

Entrando en la recta final de este convulsionado 2020, un año que será recordado sin dudas, por la cantidad de hechos acaecidos alrededor del mundo y en especial, por la pandemia del coronavirus que aún seguimos atravesando y que vino a cambiar para siempre un sin número de conductas y formas en que sociabilizábamos, pero principalmente a recordarnos que todos somos iguales y que si no encaramos el futuro con coincidencias básicas a nivel global en torno a políticas de estado serias, donde el principal involucrado es el ser humano, y además en esta patriada se juega nada más y nada menos que nuestro destino como tal, no podremos aspirar a un futuro digno y acorde al ritmo con que transcurren los hechos cotidianos de esta nueva era.

En el devenir de todo este tiempo transcurrido, donde he abordado las cuestiones tecnológicas en general, buscando soluciones a las mismas, siempre desde una óptica geoestratégica, hay un tema que lo enuncié hasta el hartazgo, como también varios profesionales y expertos en el tema y del cual, al día de hoy no se ha tomado nota y cada vez es más urgente: La Regulación Global del Ciberespacio. Cuestión que sería el eje central a todas las problemáticas suscitadas del ámbito tecnológico en cualquiera de sus temáticas se tratara.

Por ejemplo, y adentrándonos en el tema al que pasare a analizar, como lo es el ciberdelito, la erradicación de éste, sin dudas que debe ser un componente básico de nuestra seguridad nacional, como también de protección de la infraestructura de la información esencial. Esto incluye en particular la adopción de una legislación adecuada contra el mal uso de las TIC, por ejemplo, aquellas que se realizan con fines delictivos, como así también de otra índole y además de las actividades destinadas a afectar la integridad de las infraestructuras nacionales esenciales.

De allí, llegamos a la conclusión que, la lucha contra el ciberdelito exige la adopción de un enfoque de amplio alcance. ¿Y porque esto debería ser así? Debería ser así, puesto que las medidas técnicas por si solas, no pueden evitar ningún delito, por eso, es impensable que organismos encargados de hacer cumplir la Ley, estén

autorizados a investigar y penalizar el delito con eficacia.

Por todo lo mencionado y descripto hasta el momento, da la pauta que indiscutiblemente, la postura que sostengo desde hace más de 5 años en torno a regulaciones, cada vez más es un imperante que no puede esperar. Si bien en esta ocasión estoy abordando solo una temática que para nada es de menor cuantía, al contrario, versa sobre la regulación en nuestro país para contar con armas para combatir los ciberdelitos, al menos con políticas reactivas, que tanto daño hacen a los usuarios y que en medio de la pandemia han aumentado en forma exponencial, especialmente en nuestro país y la región latinoamericana, como siempre lo afirmo, una de las zonas del mundo con mayor probabilidades de vulnerabilidad y sin una población preparada para el uso correcto de las nuevas tecnologías, que a pesar de los grandes esfuerzos que se llevan adelante desde el ámbito público como privado, todavía es un pendiente.

Continuando con esta problemática de suma importancia, me parece más que importante traducir dos pensamientos de grandes referentes en el tema que llevan adelante esta lucha en nuestro país:

El Dr. Marcos Salt, quien fuera uno de los pioneros que lucho por la firma y adhesión de nuestro país, al tratado internacional de Ciberdelincuencia o más conocido como tratado de Budapest, expresó: “… es necesario regular cómo se investigan los delitos informáticos. Hay que regular la parte procesal. Y es muy importante la capacitación de los operadores, para que puedan usar estas herramientas en la investigación. No solo de los delitos informáticos, sino de todos los delitos. Hay que empezar a usar eficientemente la tecnología para investigar las conductas delictivas y usarla en un marco de garantías…”.

También y en sintonía con lo esbozado por el Dr. Salt, la Fiscal de Delitos Informáticos de CABA Dra. Dupuy, primer Fiscal en el país en torno a delitos informáticos dijo: “… nos encontramos obligados a afrontar esta problemática. Los delitos informáticos, no son un catálogo cerrado; y hoy por hoy, necesitamos en todas las investigaciones recolectar Evidencia Digital. Es una obligación estar capacitados, porque el 95% de las investigaciones tocan en algún punto las nuevas tecnologías…”.

Por ello, es preciso entender además el concepto integral sobre evidencia digital y además de pericia informática, puesto que el relato de los expertos en la materia nos

conducen a lograr una comprensión total de las mismas para poder combatirlas, repito, siempre a través de políticas reactivas, hasta que en algún momento se coordine a nivel mundial, pautas y reglas claras de manera global a los efectos de combatir los delitos informáticos con políticas proactivas.

La Evidencia Digital o prueba electrónica, es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera, que una parte o toda puede ser utilizada en el juicio. Antes de aceptar la evidencia digital un tribunal determinará si la prueba es pertinente, auténtica, si es un rumor y si es aceptable una copia o es requerido el original. La evidencia digital es fácilmente manipulable; y a raíz de una falta global de regulación en cuestiones tecnológicas, es técnicamente posible falsificar desde SMS, hasta el chats de Whatsapp, correos electrónicos o publicaciones en redes sociales. Un ejemplo de ello recientemente, en la aplicación del sistema de mensajería Telegram, donde el peligroso mundo de las Deep Fakes desnuda a chicas, por supuesto sin su consentimiento con un bot que utiliza inteligencia artificial (IA), con el fin de desnudar a mujeres sin requerir conocimiento, sin dudas estamos ante otro tipo de ciberdelito que provoca quizás un daño irreparable en la victima.

Estos elementos enunciados ut-supra son sin dudas, utilizados ampliamente en la acusación dentro de numerosos procesos judiciales en todos los órdenes jurisdiccionales, y de no mediar impugnación de dichas pruebas mediante el correspondiente informe pericial informático, se asume la aceptación tácita de la autenticidad de dichos elementos de pruebas.

En referencia a nuestro país, la publicación en redes sociales de información de terceros es especialmente problemática, por lo volátil de los elementos de prueba. Una publicación que proceda a eliminarse una u dos horas después, ha podido ser vista y compartida luego por miles de personas. Ahora bien en lo que tiene que ver con nuestro ordenamiento jurídico, no están debidamente reconocidos ni los profesionales de la Ingeniería Informática que se dedican a esto, lo que provoca que alrededor del 85% de las personas que ofrecen servicios de peritajes informáticos y actúan en los tribunales de justicia no cuentan con titulación oficial en el ámbito de la informática; y esto, está más que claro que pone en riesgo derechos fundamentales de los ciudadanos y afectan gravemente el normal desempeño de la justicia, de la máxima gravedad.

Más allá de todo el proceso en que nos hallamos inmersos no podemos dejar de

reconocer que, la Prueba Informática o Evidencia Digital, tienen una gran importancia en el proceso jurídico, sin importar la rama del derecho que se presente, es decir: civil, penal, laboral, etc…

Por último, a raíz de todo lo enunciado precedentemente, podemos empezar a realizar una hipótesis y al final, comprendemos lo que ha sucedido realmente, pero lo que no podemos es saber el tiempo que ello puede llevar, al estar a merced de varias lagunas, no solos legales, sino más bien informáticas, al no contar con una regulación global del ciberespacio. Pero sin dudas el planteado aquí, es el camino a buen puerto, solo necesitamos invocar de lleno a políticas de estado urgentes en estas cuestiones que ya son parte de nuestro entorno y que al cometerse un delito nos pueden provocar daños irreversibles. Por eso a través de la Evidencia Digital, podemos evidenciar un hecho delictivo o no, que nos lleve hasta la posesión de la verdad, para esto debemos contar con ese código procedimental para la obtención de esa prueba como lo mencionaban los colegas expertos más arriba. El cual debe ser exigido por nuestras leyes para obtener la verdad de lo sucedido, y es allí donde radica el gran problema de que solucionar los delitos en entornos digitales se dificulta en demasía, cuando las normas solo están contempladas para evidencia física.

Seremos capaces de lograr y contar en un breve lapso, con los instrumentos procesales acordes para dar batalla a problemas delictuales informáticos del siglo XXI con legislaciones de siglo XXI, ese es el gran desafío estratégico que nos espera como país y como sociedad, para poder ingresar con éxito a esta nueva era tecnológica, jamás vista en la historia del mundo y la humanidad.

– Dr. Mario Ramón Duarte *es Abogado (UCASAL). Juez Administrativo de Faltas Sauce (Ctes.) M/C. Especialista Derecho Faltas y Contravencional (UCSF). Miembro Dossier Geopolítico/Cees (CBA. ARG) (CABA-ARG). Colaborador CENEGRI (RJ. BRA.. Esp. Ciberseguridad y Ciberdefensa*

Fuentes consultadas

https://hipertextual.com/2020/10/bot-telegram-desnudar-mujeres-terrible

La Evidencia Digital

Evidencia digital que es y cómo se extrae estas pruebas

https://www.dinero.com/edicion-impresa/tecnologia/articulo/la-evidencia-digital/92746

La prueba del delito como evidencia digital

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: alainet.org

Fecha de creación
2020/11/12