

SECCIÓN III – PROCESO PENAL

SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL

Propuesta de Resolución

Preámbulo

Los participantes del Coloquio Preparatorio de la Sección 3 del XIX Congreso Internacional de Derecho Penal celebrado en Antalya (Turquía), del 24 al 27 de septiembre de 2013

Considerando que

- el uso de las tecnologías de información y comunicación (TIC) genera cambios en las realidades social, cultural, económica y jurídica;
- el uso de las TIC plantea nuevos retos en los sistemas de justicia penales, tanto nacionales como transnacionales, en el ámbito de la prevención, investigación y persecución de los delitos en general, y de los delitos que se enmarcan dentro de la cibercriminalidad en particular;
- las TIC tienen potencial para incidir peligrosamente, y de una manera sin precedentes, en la esfera de los derechos humanos y en particular en el derecho a la privacidad;
- el desarrollo de las TIC han llevado a las autoridades policiales a utilizarlas ampliamente en los procesos penales, tanto en la fase de investigación penal, como en una fase preliminar de recopilación de información con fines preventivos;

Tomando en cuenta que

la AIDP ya ha abordado diversos aspectos de los retos que plantea la sociedad de la información en el campo de la detección y de la investigación penal, en especial en:

- el XV Congreso Internacional de Derecho Penal (Río de Janeiro, 1994), sobre las tendencias de reforma en el proceso penal y la protección de los derechos humanos;
- el XVI Congreso Internacional de Derecho Penal (Budapest, 1999), sobre los sistemas de justicia penal frente a los retos de la criminalidad organizada; y
- el XVIII Congreso Internacional de Derecho Penal (Estambul, 2009), sobre medidas procesales especiales y el respeto a los derechos humanos;

Con el objetivo de

- establecer principios y normas procesales aplicables para que la utilización de las TIC en el proceso penal, y en la fase preliminar de recopilación de información con fines preventivos, se ajuste a los principios del Estado de derecho y al respeto de los derechos;¹
- garantizar que el uso de las TIC en los procesos penales y en la recogida de información con fines preventivos o de inteligencia no vulnere el derecho a la privacidad y a la protección de datos;
- garantizar que el uso de las TIC no viole el derecho de defensa y el derecho a un proceso con todas las garantías;
- lograr la implementación efectiva de las nuevas tecnologías en la lucha contra formas sofisticadas de delitos graves que utilizan las TIC;

Proponen al XIX Congreso Internacional de Derecho Penal la adopción de la siguiente resolución:

¹ El término "fase preliminar de recopilación de información con fines preventivos" es una traducción libre del término acuñado en inglés *building information positions*, el cual hace referencia a la recopilación, almacenamiento, procesamiento y análisis de información con carácter proactivo o preventivo por parte de las autoridades policiales con fines estratégicos, tácticos u operativos.

A. El uso de las TIC y la protección de los derechos humanos

El uso de las TIC en el proceso penal, así como en la recogida de información con fines preventivos o de inteligencia, puede producir una importante intromisión en la esfera de los derechos humanos. Por ello, en particular, deberán seguirse los siguientes principios:

1. Cualquier restricción del derecho a la privacidad deberá estar prevista en la ley, y ser proporcional, legítima y necesaria en una sociedad democrática.
2. El uso de las TIC en el proceso penal, así como en la recogida de información con fines preventivos o de inteligencia, deberá respetar el derecho a la protección de datos de carácter personal. La intromisión en este derecho deberá ser proporcionada a la finalidad de prevención e investigación penal en cada caso.
3. El principio de que los datos personales recogidos solo pueden utilizarse para la finalidad para la que su obtención fue autorizada² deberá respetarse con carácter general y como regla, también en la transferencia de datos personales automatizados a las autoridades policiales. Los datos personales no deberán ser procesados para un fin incompatible con aquel para el que fueron recopilados.
4. El principio de la limitación del uso de los datos para la finalidad autorizada sólo podrá excluirse en casos excepcionales, cuando su transferencia a las autoridades policiales sea necesaria para la prevención o persecución de un delito grave, siempre y cuando se respete el principio de proporcionalidad.
5. La ley deberá establecer medios y límites adecuados para garantizar que el acceso y el tratamiento de datos almacenados están sometidos al control de una autoridad independiente. Las compañías públicas y/o privadas que estén sujetas a la obligación de retener datos digitales y preservar la integridad de esos datos deberán respetar el derecho a la protección de datos.
6. El uso de las TIC en los procesos penales no podrá suponer una merma del derecho de defensa, que a su vez incluye, entre otros, el derecho a un proceso público, el derecho a la confrontación contradictoria de la prueba, el derecho de acceso a los autos y el derecho a acceder a la prueba pericial especializada en medios de prueba electrónicos, con el fin de salvaguardar el principio de igualdad de armas.

B. El uso de las TIC en la elaboración de inteligencia y recogida de datos con carácter preventivo

7. La ley determinará las medidas que podrán ser utilizadas en la recogida de datos con fines preventivos o de inteligencia, así como los fines, el ámbito y los requisitos a los que quedarán sometidas esas medidas, incluidas las condiciones del almacenamiento y/o de la destrucción de los datos.
8. No se permitirá el empleo de medidas coercitivas con el fin de recopilar datos con fines preventivos o de inteligencia, salvo que así lo autorice una resolución judicial. Se requerirá también autorización judicial para proceder a la recogida de información con fines preventivos o de inteligencia a través de técnicas de rastreo y/o cotejo de datos (*data mining* y *data matching*) que no sean accesibles libremente.
9. Las medidas de vigilancia adoptadas para la obtención de información con fines preventivos o de inteligencia deberá respetar el derecho a la privacidad, así como los demás derechos fundamentales.
10. El acceso a bases de datos para recopilar datos con fines preventivos o de inteligencia deberá controlarse a través de sistemas de software adecuados. El acceso a datos sensibles deberá someterse al control de una autoridad independiente.
11. La Ley determinará en qué casos y bajo qué condiciones los datos recopilados con fines preventivos o de inteligencia podrán ser transmitidos a otra autoridad.

² El principio de limitación de fines (*purpose limitation*), o restricción del uso de los datos a sus fines, significa que los datos personales solo pueden ser recogidos con fines determinados, explícitos y legítimos, y no pueden ser tratados posteriormente de manera incompatible con dichos fines.

C. El uso de las TIC en la investigación penal

12. Las medidas de investigación que recurran a las TIC sólo estarán permitidas en los casos previstos en la ley y cuando la información requerida no pueda obtenerse por medios menos intrusivos. La ley definirá el alcance y duración máxima de cualquiera de estos actos de investigación, así como las condiciones para el almacenamiento y/o destrucción de los datos obtenidos.³
13. Las medidas de investigación que impliquen el uso de las TIC y que representen una intromisión significativa en el derecho a la privacidad, como el acceso al contenido de las comunicaciones o la interceptación y acceso de datos en tiempo real, sólo podrán acordarse, como regla general, previa autorización judicial, cuando exista una sospecha razonable de la comisión de un delito que pueda calificarse como grave y de que el destinatario de la medida está vinculado con ese hecho delictivo.
14. Las personas cuyo derecho a la privacidad se haya visto afectado por una medida investigativa vinculada a la utilización de TIC deberán ser informadas de ese acto de investigación, en cuanto ello no perjudique a los fines de la medida y/o a los resultados de la investigación penal. La ley contemplará las medidas y recursos frente a la posible ilicitud de los actos de investigación que hayan hecho uso de las TIC.
15. Aquellos que hayan sido autorizados a llevar a cabo actos de investigación que conlleven el uso de TIC que permiten el acceso a datos en ordenadores o a comunicaciones electrónicas, habrán de respetar el derecho a la confidencialidad de las comunicaciones entre el abogado y su defendido. Deberán adoptarse las medidas necesarias para prevenir el acceso y tratamiento de datos no relacionados con el proceso penal.
16. Los Estados han de asumir la obligación de proveer a las fuerzas policiales de los medios técnicos, las capacidades y la formación especializada en el uso de las TIC, no sólo para luchar de manera eficaz contra las formas sofisticadas de cibercrimen, sino también para obtener y manejar correctamente la prueba electrónica en general. Se promoverá el desarrollo de guías de buenas prácticas en el uso de las TIC con fines de investigación criminal.
17. Las empresas privadas y los proveedores de tecnología de información y comunicaciones (TIC) podrán cooperar con las autoridades policiales en la investigación criminal solamente en las situaciones previstas por la ley. La ley deberá precisar la finalidad, condiciones y requisitos de esa cooperación. El cumplimiento de dichas obligaciones legales no deberá producir responsabilidad civil en relación con los clientes de la empresa correspondiente.

D. Las TIC y la prueba

18. Debido a la naturaleza volátil de las pruebas electrónicas, la ley habrá de establecer normas que faciliten la rápida conservación y almacenamiento de los datos digitales. Para prevenir y evitar la manipulación o alteración de los datos electrónicos almacenados se emplearán las herramientas forenses adecuadas siguiendo un protocolo ordinario.
19. Si se cuestiona la fiabilidad de la prueba electrónica o bien la prueba obtenida mediante TIC, deberá acreditarse el cumplimiento de la cadena de custodia (o *evidence continuity*). Se garantizará a la defensa el acceso a los datos electrónicos de tal manera que pueda verificar su autenticidad, y presentarlos en el juicio de una manera efectiva y sin restricciones.
20. Las pruebas digitales obtenidas vulnerando directa o indirectamente los derechos y libertades fundamentales, incluyendo el derecho a un principio con igualdad de armas y con todas las garantías, serán inadmisibles.

³ La opinión mayoritaria decidió no incluir una enumeración de medidas investigativas relacionadas con las TIC. El texto original que se acordó eliminar mencionaba las medidas de: "vigilancia electrónica, geo-localización, acceso a datos almacenados o en tiempo real, investigación encubierta on-line, registro y confiscación de ordenadores, registros extensivos de redes interconectadas, órdenes para entregar datos informáticos o automatizados, utilización de instrumentos de acceso remoto y la interceptación de cualquier tipo de comunicación con fines de una investigación penal.

E. El uso de las TIC durante el juicio

21. Las salas de vistas deberán contar con el equipamiento necesario para la utilización de las TIC durante los juicios penales, para lo cual se dotarán los suficientes recursos económicos.
22. Deberá facilitarse el uso de la videoconferencia para retransmitir las declaraciones e interrogar a los testigos que por su situación vulnerable o de difícil presencia, no puedan o no deban comparecer en el juicio. La ley regulará los casos y las condiciones en las que la video-conferencia esté permitida.
23. El interrogatorio contradictorio de los niños víctimas de delitos realizado durante la fase de investigación deberá grabarse en vídeo, para evitar que deba posteriormente comparecer en el juicio oral, si ello está contraindicado por razones del desarrollo y bienestar del menor.
24. Como regla general, todo imputado habrá de estar físicamente presente durante el desarrollo del juicio. En los casos excepcionales en que se autorizara su presencia mediante videoconferencia, deberá garantizarse de tal manera que se protejan adecuadamente su derecho a la no auto-incriminación, el derecho a la asistencia letrada (incluido el derecho a comunicarse confidencialmente con su abogado) y el derecho al examen contradictorio de los testigos.