

Reformas al Código Procesal Penal: EVIDENCIA DIGITAL

Antecedentes

- El 13 de enero de 2022 Amnistía Internacional confirmó que se había utilizado el programa Pegasus para vigilar los dispositivos móviles de periodistas y miembros de organizaciones de sociedad civil en El Salvador.
- El programa Pegasus es un software de vigilancia remota altamente invasivo, desarrollado por la empresa NSO Group, que solo se comercializa con gobiernos y sus agencias de inteligencia.
- El 11 de enero de 2022 diputados de Nuevas Ideas presentaron a la Asamblea Legislativa un proyecto de reformas al Código Procesal Penal para establecer las reglas de la evidencia digital, y su incorporación a procesos penales.
- El 1 de febrero de 2022 la Asamblea Legislativa aprobó las reformas al Código Procesal Penal.
- Las reglas sobre la evidencia digital teóricamente se basan en un control inter-institucional y filtros entre fiscalía general de la República (FGR), policía y jueces. Sin embargo, este presupuesto debe ponderarse ante el deterioro de la independencia de la FGR y del Órgano Judicial derivado:
 - a. El golpe de Estados del 1 de mayo;
 - b. Las posteriores reformas a la Ley Orgánica Judicial y a la Ley Orgánica de la Fiscalía General de la República; y
 - c. Otras acciones como el traslado y/o remoción de jueces y fiscales. De manera que no puede garantizarse que los pesos y contrapesos institucionales garanticen de forma efectiva los derechos ciudadanos.

Contenido de las reformas

- El objeto de las reformas es establecer las reglas para incorporar en los procesos penales evidencia como documentos digitales, mensajes electrónicos, imágenes, videos, datos y cualquier tipo de información que sea almacenada, recibida o transmitida a través de las Tecnologías de la Información y Comunicación o por medio de cualquier dispositivo electrónico.
- Reglas de incorporación de la evidencia digital:
 1. Acreditación de autenticidad:
 - Por medio de un testigo que intervino en la elaboración, generación o transmisión de la evidencia digital. Deberá demostrarse integridad de la evidencia con peritos.
 - Por medio de mecanismos informáticos idóneos, como la firma electrónica u otros medios semejantes. Deberá demostrarse integridad de la evidencia con peritos.
 - Por medio del perito informático que intervino en la obtención, resguardo, almacenamiento o análisis de la información.
 2. Acceso al contenido de la evidencia digital requiere orden judicial. No será necesaria orden judicial cuando se cuente con consentimiento informado de la persona cuya intimidad es afectada por el acceso a la evidencia digital.

3. Los puntos objeto de la pericia sobre la evidencia digital pueden ser establecidos por la FGR, o solicitados al juez por las partes.
 4. La reproducción de la evidencia digital se hará en la vista pública con los medios tecnológicos idóneos.
- Agente encubierto o digital:
 1. Las operaciones encubiertas son las que usan de medios engañosos con el exclusivo objeto de investigar y probar conductas delincuenciales. Están previstas en el artículo 175 del Código Procesal Penal.
 2. FGR puede autorizar a PNC que realice operaciones encubiertas digitales. Las reformas no especifican en qué consisten.
 3. Por otra parte, la PNC podrá buscar información en fuentes de carácter abierto o público, como páginas de internet, por medio de programas especializados o por búsqueda libre.
 4. La PNC y la FGR podrán celebrar acuerdos con entes públicos o privados de otros países para recibir y documentar evidencia digital.
 - Medidas cautelares:
 1. La FGR podrá solicitar al juez que ordene, hasta por un plazo de 6 meses prorrogables por otro período igual, la restricción, bloqueo de la cuenta, perfil o sitio de internet, o el aseguramiento de la información contenida en ellas, utilizados para cometer los delitos informáticos.