

ÍNDICE

PRÓLOGO

INTRODUCCIÓN

CAPÍTULO I.

NOCIONES SOBRE NUEVAS TECNOLOGÍAS, CIBERESPACIO Y CIBERDELINCUENCIA

1. APROXIMACIÓN HISTÓRICA A LA INFORMÁTICA MODERNA Y LAS NUEVAS TECNOLOGÍAS
2. LA REVOLUCIÓN DE INTERNET Y EL CIBERESPACIO
 - 2.1. Internet
 - 2.1.1 Internet: Evolución y precisiones terminológicas
 - 2.1.2. El funcionamiento de Internet: Los protocolos TCP/IP
 - 2.2. Redes sociales y ciberespacio: Un concepto de relación entre seres humanos
3. CIBERDELINCUENCIA
 - 3.1. Evolución de la ciberdelincuencia
 - 3.2. Situación actual de la ciberdelincuencia
 - 3.3. Conceptualización y principales características de la ciberdelincuencia
 - 3.4. Evolución normativa de la ciberdelincuencia

CAPÍTULO II.

CIBERVIOLENCIA SEXUAL.

1. CIBERVIOLENCIA SEXUAL EN EL SIGLO XXI: UN NUEVO FENÓMENO QUE ATENTA CONTRA LA LIBERTAD E INDEMNIDAD SEXUAL
 - 1.1. Conceptualización de la ciberviolencia sexual y principales características
 - 1.2. Ciberviolencia sexual: Características y su necesario reconocimiento como delito de género o contra las mujeres
 - 1.3. Aproximación estadística a la ciberviolencia sexual
2. ANÁLISIS DE LOS PRINCIPALES CIBERDELITOS SEXUALES
 - 2.1. Sexting o imaged-based sexual abuse (art. 197.7 CP)
 - 2.1.1. Concepto, principales características y elementos típicos
 - 2.2.2.1. Subtipo agravado del sexting
 - 2.2.2.2. El sexcasting
 - 2.2. Sextorsión o sextortion (art. 171 y 172 CP)
 - 2.2.1. Concepto y principales características
 - 2.2.2. Elementos típicos
 - 2.3. Cyber-stalking
 - 2.3.1. Concepto de stalking
 - 2.3.2. Delimitación conceptual y elementos del cyber-stalking
 - 2.3.3. Nueva modalidad atenuada en el ámbito del cyberstalking

CAPÍTULO III:

LA INVESTIGACIÓN DE LA CIBERVIOLENCIA SEXUAL.

1. INSTITUCIONES ENCARGADAS DE LA PRÁCTICA DE LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICAS EN CIBERVIOLENCIA SEXUAL
 - 1.1. Fiscalía: La Unidad coordinadora de criminalidad informática
 - 1.2. Las FCSE con competencias en la investigación de la ciberviolencia sexual.
 - 1.3. Instituciones policiales a nivel europeo e internacional.

- 2.1. Interceptación de las comunicaciones telefónicas y telemáticas
 - 2.1.1 Concepto y evolución
 - 2.1.2. Disposiciones generales
 - 2.1.2.1. Requisitos genéricos para la intervención.
 - 2.1.2.2. Alcance de la medida.
 - 2.1.2.3. Duración y prórroga de la medida.
 - 2.1.2.4. Práctica de la medida y obligación de colaboración
 - 2.1.2.5. Ámbito subjetivo de la medida
 - 2.1.2.6. La regulación de los datos de tráfico de abonados y no abonados
 - 2.1.2.7. Acceso, cesión e identificación de datos de tráfico
 - 2.2. Registro de dispositivos informáticos
 - 2.2.1. Registro estático de dispositivos de almacenamiento masivo de datos
 - 2.2.1.1. Concepto de dispositivos de almacenamiento masivo de datos
 - 2.2.1.2 Autorización judicial motivada
 - 2.2.1.3. Forma de ejecución de la medida
 - 2.2.1.4. Excepción al auto judicial motivado: El consentimiento del investigado
 - 2.2.2. Registro remoto de dispositivos informáticos
 - 2.2.2.1. Delimitación legal y conceptual
 - 2.2.2.2. Requisitos en el registro estático de dispositivos
 - 2.2.2.3. Ejecución práctica del registro remoto de equipos informáticos
 - 2.2.2.4. El registro de dispositivos informáticos en Australia
 - 2.3. Ciberpatrullaje
 - 2.4. Agente Encubierto Informático
 - 2.4.1. Conceptualización
 - 2.4.2. Principales características del AEI
 - 2.4.3. Marcos de actuación del AEI
 - 2.4.4. Requisitos de procedibilidad para su aplicación en el marco del proceso penal
 - 2.4.5. Efectos procesales del AEI en la fase de instrucción
 - 2.4.6. La figura del AEI en el marco del proceso penal de South Australia
 - 2.4.6.1. Regulación jurídica del AEI en South Australia
 - 2.4.6.2. Presupuestos de procedibilidad del AEI en South Australia
 - 2.4.6.3. Efectos procesales
 - 2.5. Aplicabilidad de la IA como diligencia de investigación tecnológica
 - 2.5.1. La IA como herramienta predictiva y preventiva de la ciberviolencia sexual
 - 2.5.2. La IA como herramienta de apoyo a las diligencias de investigación tecnológicas
 - 2.6. Orden de conservación de datos: Medida de aseguramiento
 - 2.7. Hallazgos casuales y las diligencias de investigación tecnológicas
3. LA COOPERACIÓN JUDICIAL EN LA OBTENCIÓN DE FUENTES DE PRUEBA ELECTRÓNICA
- 3.1. Cooperación judicial internacional
 - 3.1.1. Convenio sobre Ciberdelincuencia
 - 3.1.2. II Protocolo Adicional al Convenio de Budapest
 - 3.1.2.1. Principios generales aplicables a cualquier procedimiento
 - 3.1.2.2. Procedimientos de cooperación directa con prestadores de servicios.
 - 3.1.2.3. Procedimientos de cooperación para la revelación de datos
 - 3.1.2.3. Procedimiento de obtención de datos en caso de urgencia
 - 3.1.2.4. Protección de DDFF afectados por el II Protocolo Adicional.
 - 3.2. Cooperación judicial en la UE
 - 3.2.1. Evolución de la cooperación judicial en la UE
 - 3.2.2. La Orden Europea de Investigación
 - 3.2.2.1. Regulación, fundamento y conceptualización
 - 3.2.2.2. Ámbito de aplicación y autoridades competentes para su emisión
 - 3.2.2.3. Tramitación, reconocimiento y ejecución de la OEI
 - 3.2.2.4. Motivos de denegación
 - 3.2.3. Reglamento Europeo 2023/1543 sobre órdenes europeas de producción y conservación de prueba electrónica
 - 3.2.3.1. Fundamento y cuestiones conceptuales
 - 3.2.3.2. Procedimiento de la EPO de prueba electrónica
 - 3.2.3.3. Procedimiento de la ECO de prueba electrónica
 - 3.2.3.4. Motivos para la denegación de órdenes y procedimiento de ejecución
 - 3.2.3.5. Obstáculos procesales del Reglamento

4. RIESGO DE VULNERACIÓN DE DERECHOS FUNDAMENTALES EN LA INVESTIGACIÓN DE LA CIBERDELINCUENCIA SEXUAL

4.1. Derecho a la protección de los datos personales

4.1.1. Derecho a la protección de datos personales en el almacenamiento y conservación de datos personales

4.1.1.1. Evolución normativa

4.1.1.2. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo: Tratamiento de datos personales por particulares

4.1.2. Tratamiento de datos personales por autoridades competentes

4.1.2.1. Normativa aplicable

4.1.2.2. Análisis de la Directiva y la LO 7/2021 de protección de datos en el proceso penal

4.2. Derecho al secreto de las comunicaciones

4.3. Derecho a la intimidad

4.4. Derecho al propio entorno virtual

CAPÍTULO IV:

PRUEBA ELECTRÓNICA EN EL ÁMBITO DE LA CIBERVIOLENCIA SEXUAL.

1. ANÁLISIS DE LA PRUEBA ELECTRÓNICA

1.1. Naturaleza y concepto de prueba electrónica

1.1.1. La prueba electrónica como nuevo medio de prueba

1.1.2. Conceptualización de prueba electrónica

1.2. Características inherentes a la prueba electrónica

1.2.1. Los metadatos en la prueba electrónica

1.2.2. Heterogeneidad

1.2.3. Manipulación y alterabilidad de la prueba electrónica

1.2.4. Ubicuidad

1.2.5. Huella electrónica

1.3. Fuentes y medios de prueba electrónica

1.4. Incorporación al procedimiento penal de las fuentes de prueba electrónica

1.4.1. Introducción.

1.4.2. La declaración del acusado

1.4.3. La prueba testifical

1.4.3.1. La declaración de testigos

1.4.3.2. La declaración de la víctima

1.4.3.3. La declaración por parte de los agentes de las FCSE

1.4.4. La prueba documental

1.4.4.1. Documento electrónico

1.4.5. La prueba pericial

1.4.5.1. La pericial informática

1.4.6. Otros medios de incorporación al proceso de evidencias digitales

1.5. Admisión de la prueba electrónica en el proceso penal

1.5.1. Cadena de custodia

1.5.2. Procedimientos de no manipulación de los datos digitales

1.5.3. Fiabilidad

1.5.4. Autenticidad y los principios anglosajones sobre prueba electrónica

1.5.5. Integridad

1.6. Procedimiento impugnatorio de la prueba ilícita.

1.7. Valoración judicial de la prueba electrónica

1.7.1. El principio de libre valoración de la prueba

1.7.2. Especialidades valorativas

1.7.3. Especialidades en la valoración de la prueba en Australia: El Jurado

BIBLIOGRAFÍA