ÍNDICE

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