Convenio de Budapest

De acuerdo con la definición oficial, el convenio de budapest sancionado el 23 de noviembre de 2001 por el comité de ministros del consejo de Europa es;

El primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos del autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red.

También contiene una serie de poderes y procedimientos como la búsqueda de redes informáticas y la intercepción.

El objetivo principal de este instrumento, define en el preámbulo, es establecer una política penal común y alineada entre países, orientada a la protección de la sociedad contra la ciberdelincuencia, esto se alcanza tipificando los delitos informáticos de forma similar en todas las naciones, unificando normas procesales y a través de una cooperación internacional armónica.

En la práctica, es el único instrumento internacional vinculante sobre este tema, y pretende ser una guía para que los países desarrollen legislaciones nacionales integrales y alineadas contra el cibercriminal.

Además facilita la adopción de medidas para detectar y perseguir, nacional e internacionalmente a los ciberdelincuentes, ejemplo de ello es la creación de una red 24/7 para garantizar una rápida cooperación internacional que reaccione frente a cualquier incidente y facilite la extradición de criminales cibernéticos.

Esto es clave en la lucha global contra la ciberdelincuencia, dado el carácter transfronterizo que esta puede llegar a tener.

Cabe señalar que el tratado no define explícitamente el concepto de ciberdelincuencia pero si establece los tipos de cibercrimen que los países deben tipificar en sis legislaciones, entre estos son de gran importación por su impacto y frecuencia los delitos informáticos reseñados.

Falsificación informática, hace referencia a la introducción, alteración, borrado o supresión, deliberada y de forma ilegitima, de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos.

Fraude informático, son los actos deliberados e ilegítimos que causen perjuicio patrimonial a otro mediante la introducción, alteración, borrado o supresión de datos, o causándole interferencia en el funcionamiento de sus sistemas informáticos.

El artículo 37 establece que los estados no miembros del consejo de europa y que no hayan participado en la elaboración del tratado, pueden adherirse por invitación del comité del COE a la fecha ya son más de 50 países a nivel global los que se an adherido al tratado.

España firmo el tratado el 23 de noviembre de 2001 y lo ratifico mediante el instrumento de ratificación del convenio el 1 de octubre de 2010 en el que el país se compromete a observarlo y cumplirlo en todas sus partes.

Sin embargo las reformas al ordenamiento penal, derivadas de la ratificación solo se hicieron realidad hasta el 24 de diciembre 2010 cuando entro en vigencia la LO 5/2010 de 22 de junio.

Esta reforma fue inspirada en la decisión marco 2005/222/J AI, sustituida por la directiva 2013/40UE, que en cierta forma, impulso la reforma al código penal español de 2015 que introdujo artículos importantes para la tipificación de los diferentes tipos de cibercriminal, como el articulo 197 ter que penaliza la producción, adquisición importancia o entrega a terceros de datos de acceso o software desarrollado o adaptado con el fin de cometer delitos.

Ya en 2019 España aprobó la estrategia nacional de ciberseguridad la cual busca garantizar el uso fiable y seguro del ciberespacio, protegiendo los derechos y libertades de los ciudadanos, y promoviendo el progreso económico.

La lucha del estado contra la ciberdelincuencia es frontal, aun asi solo en 2018 se registraron 110613 ciberdelitos que costaron millones de euros a las victimas según cifras del observatorio español de delitos informáticos.