

CIBERTERRORISMO Y DELITO DE ODIO MOTIVADO POR IDEOLOGÍA

MARÍA CONCEPCIÓN GORJÓN BARRANCO



VNIVERSIDAD
DSALAMANCA

tirant lo blanch

Valencia, 2019

Índice

INTRODUCCIÓN.....	15
-------------------	----

Capítulo I

CONCEPTO: CIBERODIO POLÍTICO VS CIBERTERRORISMO

I. REVOLUCIÓN TECNOLÓGICA Y CRIMINALIDAD TRASNA- CIONAL.....	21
1. De los delitos informáticos a la cibercriminalidad	23
2. Gobernanza global y grupos minoritarios.....	26
3. ¿Universalismo cosmopolita en el ciberespacio?	30
II. INSTRUMENTOS INTERNACIONALES SOBRE ODIO POLÍ- TICO Y TERRORISMO	33
1. Naciones Unidas	34
1.1. El odio y la discriminación	34
1.2. Terrorismo.....	37
2. A nivel europeo	40
2.1. Odio y Discriminación.....	40
2.2. Terrorismo.....	45
III. CONCEPTOS.....	49
1. Origen del delito político.....	49
1.1. Delitos mixtos	53
1.2. Cibercriminalidad política actual.....	56
2. Ciberodio político	58
2.1. Libertad de expresión y discurso de odio político	60
2.2. Modelos de tipificación: El ciberodio político como delito	66
2.3. Delitos odiosos	71
3. La necesidad de un concepto restringido de terrorismo	76
3.1. La existencia de una estructura.....	78
3.2. Delitos graves y finalidad del Terrorismo	82
4. La especificidad del terrorismo global islamista	85
4.1. ¿Un componente político en el terrorismo islamista?	85
4.2. Internet y Yihad 2.0.....	88
5. Toma de postura	92

Capítulo II

FENOMENOLOGÍA Y CLASIFICACIÓN: PREVENCIÓN

I. DATOS	97
1. Instrumentos para medir los delitos de odio	97
1.1. Comisión Europea contra el Racismo y la Intolerancia (ECRI)	97
1.2. Observatorio español del racismo y la xenofobia	98
1.3. Anuario Estadístico del Ministerio del Interior	100
1.4. Memoria de la Fiscalía General del Estado	102
2. Sobre el terrorismo	104
2.1. La Oficina de las Naciones Unidas de Lucha contra el Terrorismo	104
2.2. Europol	106
2.3. Observatorio Internacional de Estudios sobre Terrorismo (OIET)	109
II. DESCRIPCIÓN DE LOS FENÓMENOS	111
1. Ciberodio como delito	111
2. Propaganda ciberterrorista	112
3. Proceso: ¿de la radicalización a la acción?	113
4. Ataques a sistemas informáticos: Hacking y Sabotaje informático	116
4.1. Hacking	118
4.2. Sabotaje informático	119
III. CIBERVÍCTIMAS Y CIBERDELINCUENTES	121
1. Cibervíctimas	122
2. Ciberagresores o distintos agentes en internet. Hechos conocidos	125
2.1. Terroristas	127
2.2. Estados	129
2.3. Hacktivistas	134
3. Toma de postura	138
IV. PREVENCIÓN: TEORÍAS CRIMINOLÓGICAS APLICADAS AL ESPACIO VIRTUAL	138
1. Arquitectura del ciberespacio	142
1.1. Características intrínsecas. Espacio y tiempo	143
1.2. Características extrínsecas	144
2. Oportunidad criminal. Teoría o enfoque de las actividades cotidianas	146
3. Prevención situacional del delito	152
V. ALGUNAS CONSECUENCIAS DE LA PREVENCIÓN SITUACIONAL EN EL CIBERESPACIO: LA CREACIÓN DE UN NUEVO PANÓPTICO	155
1. La prevención situacional proporciona soluciones a los síntomas, pero no a las causas	156

2. Desplazamiento del delito.....	157
3. Implicaciones éticas y morales: no mordazas en internet, no vigilancia.....	159
4. La prevención en el caso español. Toma de postura	161

Capítulo III

CIBERTERRORISMO EN SENTIDO ESTRICTO: LAS TIC COMO OBJETO. ATAQUES DEL ART. 573.2 CP

I. CUESTIONES COMUNES.....	170
1. Justificación internacional	170
2. Bien jurídico.....	172
3. Agentes	175
4. Finalidades	177
II. ACCESO NO CONSENTIDO Y ATAQUES A SISTEMAS.....	183
1. Acceso ilícito o intrusismo informático del art. 197 bis 1 CP....	183
1.1. El origen en los instrumentos internacionales	183
1.2. Regulación española.....	187
2. Interceptación de comunicaciones y de transmisiones no públicas de datos informáticos, art. 197 bis 2 CP	192
2.1. El origen en los instrumentos internacionales	192
2.2. Regulación española.....	194
3. Interferencia en los datos, art. 264 CP.....	197
3.1. El origen en los instrumentos internacionales	197
3.2. Regulación española.....	198
4. Interferencia en el sistema, art. 264 bis.....	202
4.1. El origen en los instrumentos internacionales	202
4.2. Legislación española	202
5. Abuso de los dispositivos, art. 197 ter y 264 ter	205
5.1. El origen en los instrumentos internacionales	205
5.2. Legislación española.....	207
6. Toma de postura	208

Capítulo IV

RESPUESTA PENAL AL DISCURSO POLÍTICO: LAS TIC COMO INSTRUMENTO DEL DELITO

I. CUESTIONES COMUNES.....	212
1. Justificación internacional	212
2. Bien jurídico. ¿Derecho penal antidiscriminatorio o paz pública?.....	215
3. Sujetos pasivos del delito: ¿tutela de minorías?.....	220
4. Elemento subjetivo	223

5. La relevancia de internet. Retirada de contenidos	225
II. LA CRIMINALIZACIÓN DEL DISCURSO POLÍTICO EN INTERNET	227
1. La agravante genérica del art. 22.4 CP: motivación política	229
1.1. Fundamento de la agravante.....	230
1.2. Casos.....	233
2. Análisis del art. 510 CP	236
2.1. Casos: Aplicación antes y después de 2011	237
2.2. La reforma de 2015. Especial referencia al art. 510. 2 CP..	240
3. Delito de enaltecimiento del Terrorismo y humillación de las víctimas, art. 578 CP	246
3.1. Casos sobre enaltecimiento del terrorismo.....	252
3.2. Casos sobre humillación a las víctimas del terrorismo	257
4. Propaganda terrorista en internet	259
4.1. Adoctrinamiento o radicalización activa, art. 577.2 CP	260
4.2. Adoctrinamiento o radicalización pasiva, art. 575 CP	263
5. Toma de postura	269
III. PROPUESTAS DE <i>LEGE FERENDA</i>	271
1. El punto de partida: La Recomendación general número 35 del Comité de Naciones Unidas para la eliminación de la discriminación racial de 2013	271
2. Propuestas diferentes a la criminalización.....	275
3. Propuesta para una criminalización restrictiva en el marco penal.....	279
BIBLIOGRAFÍA.....	287