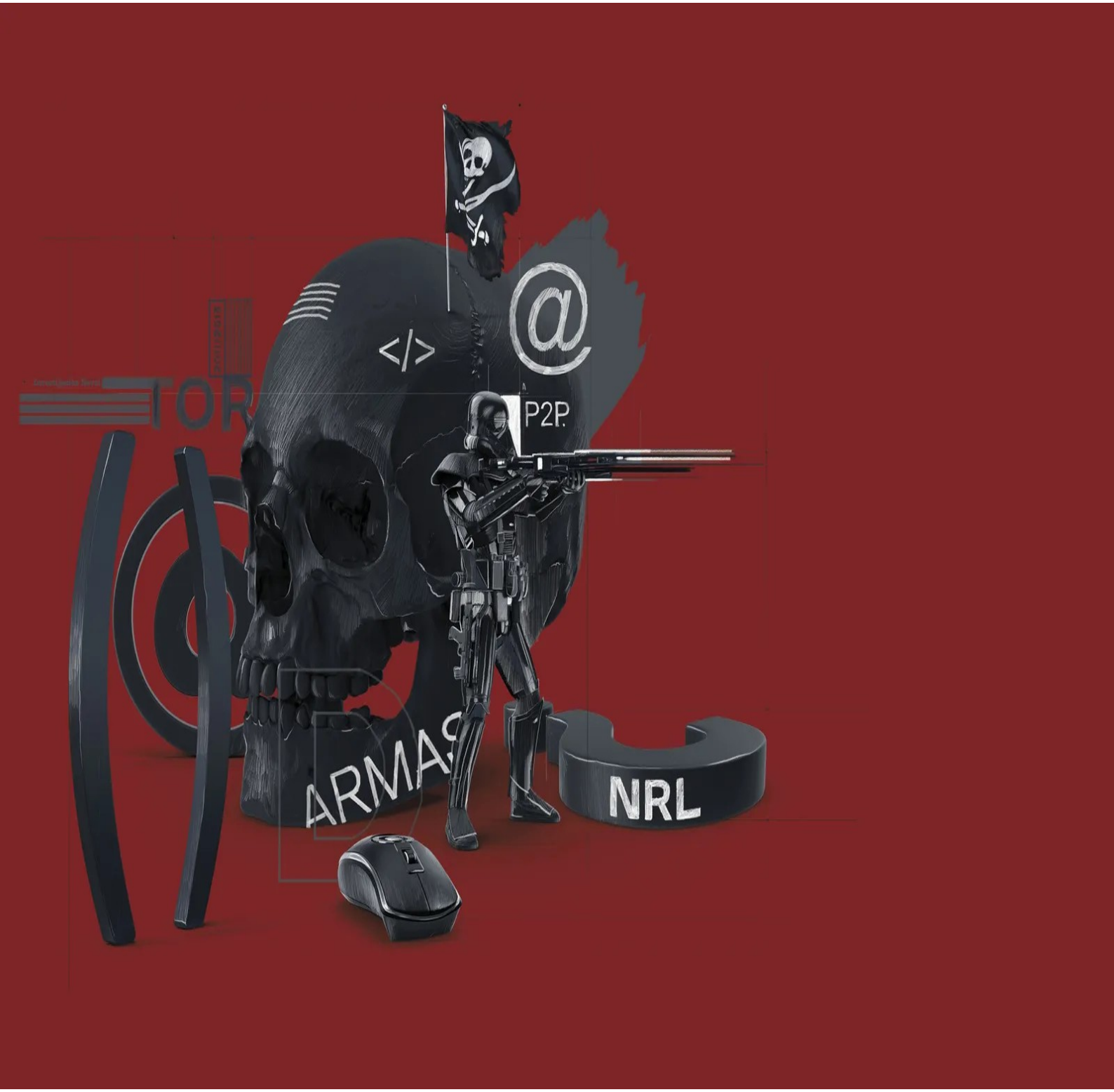
USO DE LA DARK WEB POR LA POLICÍA, INVESTIGUEMOS LA RED.

AUTOR :
ANGEL RODRÍGUEZ PÉREZ



AUTOR Y EDICIÓN:

Ángel Rodríguez Pérez

Policía Local de Maracena (Granada)

DEPÓSITO LEGAL: GR-1534-2022
ISBN-978-84-09-45126-5

COLABORA Y DISTRIBUYE

EJEMPLAR DE DISTRIBUCIÓN GRATUITA

Esta publicación electrónica se divulga y distribuye con la colaboración de S.P.L.G. Sindicato Independiente de Policía Local de Granada, con la intención de reciclar y perfeccionar en esta materia a los diferentes Policía Locales tanto de nuestra Comunidad Autónoma, así como el resto de Comunidades. Se publica electrónicamente como publicación electrónica en la página web del Sindicato Independiente de Policía de Granada S.I.P.L.G, de interés policial, estando disponible para su visualización e impresión de cuantos usuarios estén interesados en sus contenidos.

INDICE:

Indice de Figuras:

Indice de Tabla:

Resumen

La internet ha generado un desborde en el conocimiento pero también ha generado una avidez por tener ciertos aspectos bajo un resguardo no solo desde la apariencia de la seguridad informática sino también desde conocer que es lo superficial, lo profundo y por último lo más oscuro a nivel de la propia internet.

Esta investigación se centró en poder desde un arte consolidado de los conceptos de Surface Web, Deep Web y Dark Web consolidar los elementos para abordar el uso de la Dark Web por los cuerpos policiales y los resultados que estos han obtenido en esta materia y por último desde la perspectiva de marco legislativo que se ha podido construir en pro de mejoras y de controles de los delitos informáticos que han encontrado resguardado dentro de la Internet Profunda y Oscura.

Palabras claves: Delitos Informáticos, ciberespacio, Surface Web, Deep Web, Dark Web

Introducción

La internet siempre ha sido un objeto desde su nacimiento de estudio y precisamente en estos tiempos donde existe una tendencia a determinar que es lícito o legal y que no lo es.

La aparición de conceptos de ciberdelicuencia y de los delitos informáticos a hecho que exista una notoria preocupación en todos los ámbitos precisamente por el compromiso que existe en el resguardo de la información personal, corporativa y por consiguiente el evitar la proliferación de los delitos informáticos que se ven favorecidos por ambigüedades o vacíos en las diferentes legislaciones.

En esta investigación abordaremos los siguientes aspectos:

- Conceptualizar la Dark Web y términos similares para tener un estado del arte propio.

- Analizar el impacto de la Dark Web desde la perspectiva policial.

- Determinar el impacto de la legislación en cuanto al uso de la Dark Web por parte de los cuerpos policiales

Permitiendo precisamente que nos otorgue un panorama en tópicos que aun pareciendo muy comunes y hasta triviales no lo son y que han ocasionado en muchos confusiones y por consiguiente vacíos que favorecen muchos de los llamados delitos informáticos.

Objetivos

- Conceptualizar la Dark Web y términos similares para tener un estado del arte propio.

- Analizar el impacto de la Dark Web desde la perspectiva policial.

- Determinar el impacto de la legislación en cuanto al uso de la Dark Web por parte de los cuerpos policiales.

Marco Metodológico

Esta investigación empleó la técnica de recopilación documental y bibliográfica que permitió jerarquizar la información encontrada, posteriormente se realizó un proceso de análisis e interpretación que permitió lograr un análisis y síntesis adecuado y por último se realizó la redacción y presentación de todo lo que fue tratado y analizado.

o RECOPILACIÓN DE LA INFORMACIÓN

Para recopilar y seleccionar a información pertinente para esta investigación se empleó la técnica de recopilación documental y bibliográfica la cual consiste en la revisión de diferentes tipos de documentos que permitan o representen aportes para la investigación. Se tomó en consideración las fuentes para la recolección de la información empleando la recopilación documental y bibliográfica:

Libros – Documentos - Informaciones: Recopiladas en diferentes repositorios que sean vinculantes a la investigación.

Trabajos de investigación: Tesis de grado entre otros.

o ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN

Empleando la síntesis y el análisis de lo anteriormente recopilado se procedió a construir los diferentes hilos de saberes a través de una redacción adecuada y congruente. Se empleó también el uso de tablas y figuras que permitieron de alguna manera la fácil comprensión e interpretación de la información que se recopiló y que efectivamente luego se derivó en la redacción y presentación de la investigación

o REDACCIÓN Y PRESENTACIÓN DE LA INVESTIGACIÓN

Realizando de una manera sistemática, organizada y sobre todo comprensible se presentó los resultados de la investigación en donde se plasmó la posición del investigador y por supuesto fijando criterios que permiten justamente apuntalar lo investigado hacia una perspectiva o arista tomando en consideración los diferentes autores consultados.

Desarrollo

Conceptualizar la Dark Web y términos similares para tener un estado del arte propio

Es preciso concretar o establecer las diferentes terminologías similares o no en cuanto a la Dark Web para precisamente tener precisado que involucra un aspecto como el que se está estableciendo en este momento

Daniels (2021) establece el concepto de Dark Web como:

> una parte oculta de la world wide web a la que no se puede acceder usando navegadores como Microsoft Edge, Mozilla Firefox y Google Chrome. Las páginas de la dark web tampoco se encuentran indexadas por los motores de búsqueda como Google. En otras palabras, necesitas un navegador especial (como el navegador Tor) y una idea de lo que quieres buscar cuando visitas la dark web. (p.1)

Fernández (2021) establece que la Dark Web: “Es una porción de Internet intencionalmente oculta a los motores de búsqueda, con direcciones IP enmascaradas y accesibles sólo con un navegador web especial.” (p.1)

Kapersky (2022) define la Dark Web:

> es el conjunto oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet privada y en el anonimato, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien algunos la utilizan para evadir la censura del gobierno, también se sabe que se utiliza para actividades altamente ilegales. (p.1)

Aguirreburualde de Dios (2022) establece que:

> los usuarios pueden acceder a este tipo de redes (Dark Web o internet oscura) mediante ciertos buscadores anónimos, pero también, una vez accedido al navegador, se mantiene una navegación de manera confidencial y anónima, ya que estos navegadores usan servidores proxy (equipo informático que hace de

> intermediario entre las conexiones de un servidor y un cliente, filtrando los paquetes entre ambos) para que su IP sea casi imposible de rastrear. (p.27-28)

Para Daniels (2021), Fernández (2021), Kapersky (2022) y Aguirreburualde de Dios (2022) la Dark Web (Internet Oscura) es prácticamente un aspecto que genera mucho recelo y por consiguiente una inclinación precisamente a ser censurado y juzgado por el simple hecho de que todo está envuelto en un “halo de misterio”. El tan simple hecho de que su acceso no sea tan fácil o dicho de otra forma sea accesible para todo el mundo hace que uno se formule las siguientes interrogantes:

- ¿hay evasión de una censura previa por un determinado gobierno?
- ¿se emplea para actividades ilegales en un amplio porcentaje?
- ¿se emplea la confidencialidad o el anonimato para ocultar actividades que no son legales?

Existe otro concepto asociado a la Dark Web que es el denominado Deep Web (Internet Profunda).

Daniels (2021), conceptualiza la Deep Web como:

> La deep web es la parte de internet que contiene información muy específica. La mayoría de nosotros no tendremos acceso a esta información, y tampoco es accesible a través de los buscadores. En otras palabras, una búsqueda convencional en Google no mostrará páginas de la deep web. En su mayoría, son páginas y bases de datos que solo están destinadas a un determinado grupo de personas dentro de una organización. Para obtener acceso, debes conocer la dirección web exacta (URL). En algunos casos también necesitas una contraseña. (p.1)

Fernández (2021):

> Imagínate por ejemplo una página a la que accedes escribiendo una dirección web convencional, pero a cuyo contenido no puedes acceder si no pagas una determinada cuota o una mensualidad. Eso es Deep Web. También lo es la página que se genera cuando estás utilizando un buscador de viajes. Es una web única configurada con los datos que has introducido, y a la cual no se puede acceder de forma directa. (p.1)

Kapersky (2022) conceptualiza a la Deep Web:

> Se encuentra debajo de la superficie y representa aproximadamente el 90 % de todos los sitios web. Esta sería la parte de un iceberg debajo del agua, mucho más grande que la web superficial. De hecho, esta web oculta es tan grande que es imposible determinar con exactitud cuántas páginas o sitios web están activos en un momento dado. Siguiendo con la analogía, los grandes motores de búsqueda podrían considerarse como barcos de pesca que solo pueden “atrapar” sitios web cerca de la superficie. Todo lo demás, desde revistas académicas hasta bases de datos privadas y más contenido ilícito, está fuera de alcance. Esta web profunda también incluye la parte que conocemos como la web oscura o dark web. (p.1)

Aguirreburualde de Dios (2022) define la Deep Web: “es todo el contenido de Internet que no puede ser indexado por los buscadores comunes públicos, como pueden ser Yahoo, Google, etc” (p.31)

Sintetizando a los cuatro autores mencionados hay aspectos relevantes en el concepto de Internet Profunda:

- Contiene información específica.
- Mayoría de las veces es pago el contenido por tanto también su acceso
- No se indexa en buscadores públicos comunes.
- Priva el criterio de privacidad de forma autenticada (contraseñas).

El concepto denominado Surface Web (Internet Superficial), es primordial tener claro su definición y su ámbito.

Daniels (2021), lo conceptualiza como:

> La web superficial, junto a la deep web, es la parte de Internet que la mayoría de nosotros usamos todos los días. Es accesible a través de navegadores normales como Chrome, Safari, Firefox, etc. Puedes acceder a él desde cualquier lugar y en cualquier momento, siempre y cuando tengas una conexión a Internet y un navegador. Otras webs, incluyendo las tiendas en línea y de negocios, también forman parte de la web superficial. Esta es la parte de la web a la que se puede llegar a través de motores de búsqueda como Google. Si visitas una web como visitante habitual, no verás todas y cada una de las partes de la web. Solo verás la superficie. Cuando navegas por Amazon sin iniciar sesión, por ejemplo, te

> encontrarás con innumerables productos, pero solo podrás ver la web como cliente, no como vendedor o administrador. Para poder ver «entre bambalinas», necesitarás un nombre de usuario y una contraseña. Una vez lo tengas, podrás conseguir pasar de la web superficial a la deep web. (p.1)

Kapersky (2022) define la Internet Superficial como:

> La web abierta o la web superficial es la capa superficial “visible”. Si continuamos visualizando toda la web como un iceberg, la web abierta sería la parte superior que está sobre el agua. Desde un punto de vista estadístico, este conjunto de sitios web y datos constituye menos del 5 % del total de Internet. Aquí se encuentran todos los sitios web disponibles al público a los que se accede a través de los navegadores tradicionales como Google Chrome, Internet Explorer y Firefox. Los sitios web se suelen identificar con operadores de registro como “.com” y “.org” y pueden localizarse fácilmente con los motores de búsqueda más populares. La localización de sitios web superficiales es posible porque los motores de búsqueda pueden indexar la web a través de enlaces visibles (un proceso llamado “rastreo” debido a que el motor de búsqueda recorre la web como una araña). (p.1)

BLOG DE SEAS, CENTRO DE FORMACIÓN TÉCNICA EN MODALIDAD ONLINE (2017) puntualiza: “Las páginas Web por las que navegamos a diario son solo una minúscula parte de lo que realmente hay en la red, a esta parte de la red visible se le conoce como Surface Web. Esta parte de la red solo representa aproximadamente un 4% del total.” (p.1)

Kapersky (2022) caracteriza a la Surface Web:

> Imagina un iceberg. Una pequeña parte puede ser vista por todos, mientras que más de la mitad está sumergida. Así se pueden comparar las diferentes capas de Internet.
>
> Como se ha indicado anteriormente, la Web de superficie es toda la parte de Internet indexada por un motor de búsqueda común como Google, Bing o Firefox, lo que permite al público tener libre acceso a la información allí publicada, a menos que se requiera un inicio de sesión o una contraseña. Por su definición, sería el antónimo de la Deep Web. Se calcula que ya hay más de 130 billones de páginas indexadas y se encuentran fácilmente en los servicios de búsqueda. Al acceder a estos contenidos, el ordenador o dispositivo se conecta a un servidor que identifica la IP del usuario. (p.1)

En la Figura N° 1 podemos apreciar de forma sencilla lo que es cada uno de los tres conceptos desarrollados:

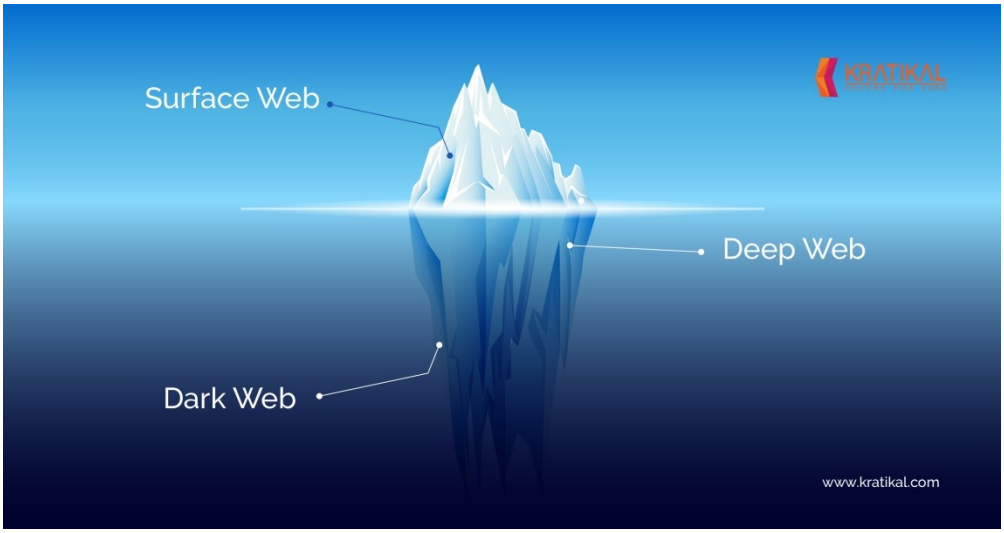


Figura 1.- Surface Web - Deep Web - Dark Web

Fuente: Kratikal (2020)

En lo más superficial precisamente está la Surface Web (Internet Superficial) seguido de la Deep Web (Internet Profunda) y por último la Dark Web (Internet Oscura)

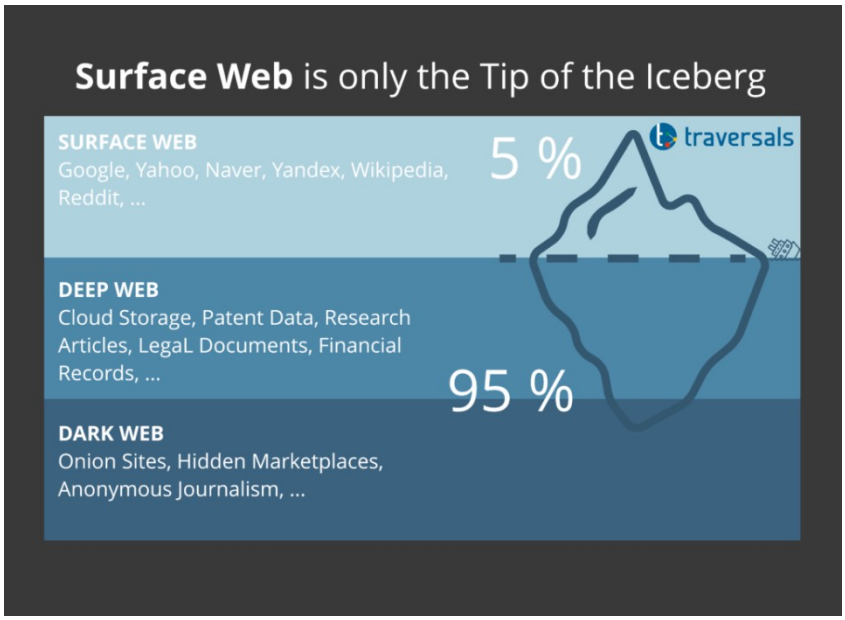


Figura 2.- Porcentajes representativos del Surface Web, Deep Web y Dark Web

Fuente: Traversals (2020)

Precisamente Traversals (2020) establece unas consideraciones propias que se derivan de la Figura N° 2 que se consideran importantes:

- “La World Wide Web está compuesta por tres capas: Surface Web, Deep Web y Darknet.” (p.1)
- “Surface Web cubre solo el 5 % de la World Wide Web.” (p.1)
- “Deep Web incluye todo tipo de servicios web y constituye una fuente de datos muy interesante para las investigaciones OSINT”. (p.1)
- “Solo se puede acceder a Darknet mediante el uso de tecnología dedicada, como TOR o I2P”. (p.1)
- “Darknet no solo se utiliza para actividades ilegales, sino también para acciones en las que el anonimato juega un papel, como el periodismo en zonas de crisis.” (p.1)

A continuación desarrollaremos en forma tabular en la Tabla N° 1 los elementos básicos que tienen en común los conceptos Deep Web y Darknet pero a su vez establecen diferencias relativas y significativas:

Tabla 1.- Aspectos relevantes de la Surface Web - Deep Web - Dark Web

	Surface Web	Deep Web	Dark Web
Concepto	la Web de superficie es toda la parte de Internet indexada por un motor de búsqueda común como Google, Bing o Firefox, lo que permite al público tener libre acceso a la información allí publicada, a menos que se requiera un inicio de sesión o una contraseña	es todo el contenido de Internet que no puede ser indexado por los buscadores comunes públicos, como pueden ser Yahoo, Google, etc	es el conjunto oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado
Porcentaje dentro de la web	5	95	
Ámbito	Público	Privado	Privado (Red Clandestina)
Actividades Legal o ilegal	Legal – Ilegal	Legal - Ilegal	Ilegal
Accesibilidad	Libre	Cualquier navegador con las credenciales adecuadas	Navegador Tor y otros navegadores especializados solamente
Controles Reglamentarios	Controles de contenido establecidos por el ISP y el país de origen del usuario	Controles de contenido establecidos por el ISP y el país de origen del usuario	No regulado
Anonimato	Fácil rastreo (aún cuando	ISP y otras entidades	Muchos navegadores hacen

	emplean los cookies)	rastrean regularmente la actividad	que el acceso sea menos rastreable pero no verdaderamente anónimo
Indexado por los motores de búsquedas	Si	No	Requiere de motores especiales de búsqueda
Uso de VPN	No	Preferencia del usuario	Muy recomendable
Uso de antivirus	Recomendado	Recomendado	Necesario
Dominios más empleados	.com, .net, .org o .es	Sin definir	.onion
Recomendación en la seguridad y protección en la internet	Debe resguardarse por sus propios medios		

Fuente: History-Computer (2022), Traversals (2020), Kapersky (2022), Aguirreburualde de Dios (2022), A2secure (2019), González (2015), Fernández (2020), Academia Geopol (2022), Test de Velocidad (2016)

La Figura N° 3 clasifica por así decirlo en una forma más sencilla que es lo que involucra cada concepto a nivel de los contenidos que pueden encontrarse allí

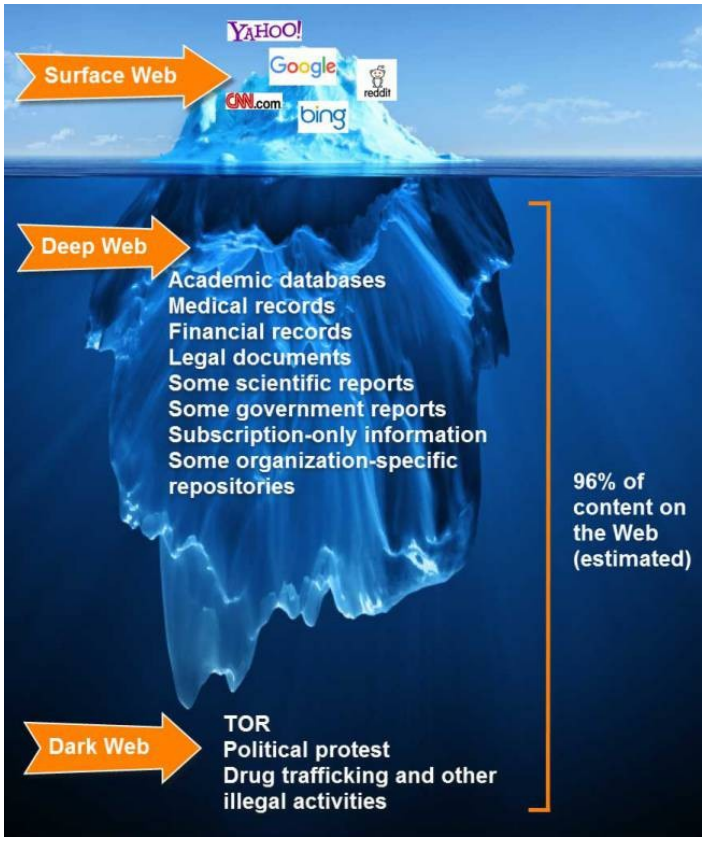


Figura 3.- Contenidos que pueden ser encontrados en la Surface Web - Deep Web - Dark Web

Fuente: Otero (2022)

Analizar el impacto de la Dark Web desde la perspectiva policial

Bajo la conceptualización desarrollada anteriormente la Dark Web o Internet Profunda como también se le denomina presenta una serie de elementos que hace precisamente sea un objeto de interés amplio y profundo por los cuerpos policiales:

- “Compraventas de datos personales y/o corporativos”. (Carmiel, 2022, p.1)
- “Embriones de ciberataques”. (Carmiel, 2022, p.1)
- “Entorno de reunión de cibercriminales”. (López, 2021, p.1)
- “Ciberestafas”. (López, 2021, p.1)
- “Sextorsion” (López, 2021, p.1)

- “Pornografía infantil y grabaciones snuff (asesinatos, violaciones, torturas, etc.)“ (López, 2021, p.1)
- “Tráfico de drogas” (López, 2021, p.1)
- “Infracción de derechos de propiedad intelectual” (López, 2021, p.1)
- “Infracción de derechos de Propiedad Industrial” (López, 2021, p.1)
- “Usurpación de identidad” (López, 2021, p.1)
- “Venta de objetos robados” (López, 2021, p.1)

Tanto Carmiel (2022) como Ecija (2021) han enumerado precisamente estos elementos que se consideran importantes desde la arista policial, todo lo nombrado son delitos lo que nos hace inferir que la Dark Web precisamente por sus características de anonimato y su forma tan “peculiar” de acceso favorece este tipo de actividades ilícitas, no obstante también promueve el desarrollo de las mismas, convirtiendo la Internet Profunda el lugar perfecto para cobijar o resguardar a este tipo de delincuencia que se clasificaría como ciberdelicuencia.

Tomando como referencia la pandemia de COVID-19 para Carmiel (2022), muchas organizaciones efectuaron migraciones hacia la nube, si bien es cierto que es una actividad diaria en el ámbito de la seguridad informática, muchas organizaciones lo realizaron de una forma muy desorganizada y sin un protocolo que permitiera un efectivo resguardo de la información que se estaba manejando, favoreciendo que por este “descuido”, información personal y corporativa fuera a dar a manos de ciberdelicuentes que precisamente operan en la Dark Web, recordemos que la línea de separación entre la Deep Web y la Dark Web es mínima.

Zarzalejos (2019) puntualiza que muchos cuerpos policiales han tenido que realizan cambios dentro de su propia estructura organizativa y crear estructuras que permitan responder y apoyar a las víctimas de la Dark Web. Es por eso que se nombra comúnmente **Unidades, Divisiones o Cuerpos de Ciberdelicuencia** dentro de los organismos policiales que ya conocemos. Zarzalejos (2019) plantea que estas subdivisiones encargadas de la delincuencia cibernética es precisamente tratar de convertir o revertir el cómo opera la Dark Web al servicio de personas que por diversos factores van a dar allí y se convierten en ciberdelicuentes o son víctimas.

Carmiel (2022) toma dos aspectos que se consideran los bastiones de operaciones dentro de la Dark Web como son: **anonimato** e **impunidad**, debido a ellos las operaciones ilícitas se ven favorecidas y sobre todo acogidas con un manto de “protección” . Desde el punto de vista informático el anonimato es precisamente para poder “navegar” o “andar” sin dejar rastros, que mejor forma de realizar actividades donde se compromete la misma integridad y seguridad de las víctimas bajo la figura del anonimato.

Ecija (2017) menciona:

> En este nuevo mundo virtual, global y carente de fronteras, el poder judicial ve acotado su eficacia y legitimación, lo que ha provocado nuevos intentos del legislador por aprobar normas que intenten poner orden jurídico y así hacer prevalecer su poder. (p.1)

¿Qué nos hace pensar esta mención?. Hay una disposición en poder crear o modificar el marco jurídico vigente para poder dar respuestas a lo que esta sucediendo desde el ciberespacio, un ámbito que precisamente al parecer en un principio no ameritaba esas regulaciones, pero debido al auge de lo que hemos venido desarrollando es preciso.

Bajo las debidas amparaciones (caso español reciente modificación de la Ley de Enjuiciamiento Criminal [LECrim], que en sus artículos 282 , y 588 quinquies , sexties y septies) nace el concepto de **Ciberpolicías**.

Ecija (2017) describe las competencias de estos ciberpolicías (bajo el ámbito de España):

- “Tienen un fin claro: los controles de seguridad en Internet.” (p.1)
- “La policía comenzaría a utilizar herramientas tecnológicas para la defensa-ataque cibernética. De esta forma nacerían las ciberarmas.” (p.1)
- “Las ciberarmas pueden ser ciberaplicaciones utilizadas para atacar y causar un daño cibernético o ser ciberherramientas de defensa” (p.1)
- “las ciberarmas se podrían definir como «las ciberaplicaciones utilizadas para atacar y causar un daño cibernético» o como ciberherramientas de defensa..” (p.1)

En España bajo la LECrim hay una tipificación clara y precisa en su artículo 588 cuales son los delitos que pueden ser considerados investigados y por ende los ciberpolicias a través de sus ciberarmas pueden operar:

- Delitos cometidos en el seno de organizaciones criminales. (Ecija, 2017, p.1)
- Delitos de terrorismo. (Ecija, 2017, p.1)
- Delitos cometidos contra menores o personas con capacidad modificada judicialmente. (Ecija, 2017, p.1)
- Delitos contra la Constitución, de traición y relativos a la defensa nacional. (Ecija, 2017, p.1)
- Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. (Ecija, 2017, p.1)

Desde el punto de vista policial, los ciberpolicías trabajan pudiéndose entender con un debido protocolo, Zarzalejos (2019) lo señala:

- **Vigilancia constante:** No solamente accede ciberdelicuentes la Dark Web sino cualquiera que pueda o tenga conocimientos mínimos de uso del TOR, bajo esta categoría cuando se emplea el Dark Web para evasión de la censura (caso de periodistas o usuarios que acceden a información previamente censurada por gobiernos en determinados países). La vigilancia se realiza a través de servidores que monitorean (estando propiamente inmersos en la Dark Web) y cualquiera que pueda ser objeto de alarma cae bajo la “lupa” de los ciberpolicías.

- **Encontrar la dirección:** Bajo la figura del anonimato todo el mundo se resguarda y en la Dark Web, previo a esto hay el aspecto de como llego a la dirección en cuestión es decir a la página que de alguna manera esta dentro de la internet profunda. Los foros que generalmente se encuentran en la red en donde se “reúnen” virtualmente muchos usuarios son otro foco de atención de la ciberpolicía porque precisamente allí es donde está el origen o orígenes de las direcciones de Dark Web.

- **Buscar el fallo en el sistema:** Con la dirección ubicada y precisada “entramos” al foro, como se crean desconociendo protocolos de seguridad, se emplea eso, por tanto se obtiene de allí la información necesaria y luego se cierra el foro y se procede a rastrear las direcciones.

- **Infiltrarse:** Muchas veces entrar a los foros no es sencillo, debido a la misma naturaleza de lo que estamos manejando (internet profunda), es necesario muchas veces una forma de “infiltrarse” dentro de los foro. Infiltrarse es un proceso largo y tedioso que puede ocupar un período de tiempo largo.

- **Identificar a los miembros: “**El resultado ideal de una operación de vigilancia dentro de la dark web culmina cuando se traza la identidad hasta una IP fiable” (p.1). La naturaleza de la Dark Web muchas veces hace que los cuerpos policiales empleen en el tipo de vigilancia métodos más tradicionales en el mundo físico como, por ejemplo, comprobar que el sospechoso se conecta a la misma hora que su identidad online.

Un aspecto relevante es precisamente la realización de una operación denominada Dark Hun TOR (Cazador Oscuro), Iniseg (2021) señala elementos importantes de esta operación:

- **¿Qué es la Operación Dar Hun TOR?:**

  > En un complejo operativo mundial, en el que han participado conjuntamente nueve países, logrando dar un nuevo golpe contra la Dark Web, la ya conocida versión clandestina de Internet, se realizó la denominada “Operación Dark HunTor“. Esta operación, cuya investigación duró 10 meses, fue planeada específicamente para desbaratar la venta ilegal de drogas, armas, bienes y servicios ilícitos que operan en la red, y fue posible organizarla en el marco de la EMPACT (Plataforma Multidisciplinaria Europea contra las Amenazas Criminales). (p.1)

“Esta operación, conocida como Dark HunTOR, se compuso de una serie de acciones separadas pero complementarias en Alemania, Australia, Bulgaria, Estados Unidos, Francia, Italia, los Países Bajos, el Reino Unido y Suiza, con esfuerzos de coordinación dirigidos por Europol y Eurojust”. (p.1)

“Para el DOJ (Departamento de Justicia de Estados Unidos) un esfuerzo internacional coordinado en tres continentes para interrumpir el tráfico de opioides en la red oscura”. (p.1)

> Aunque aún se siguen llevando a cabo varias investigaciones, esta acción ha provocado un total de 150 personas detenidas, de las cuales 65 arrestos fueron en Estados Unidos, 3 en Francia, 47 en Alemania, 4 en los Países Bajos, 24 en el Reino Unido, 4 en Italia, 2 en Suiza y 1 en Bulgaria. También se logró confiscar alrededor de 26,7 millones de euros, tanto en monedas virtuales como en efectivo, 152 kg de anfetamina, 27 kg de opioides, más de 25,000 píldoras de éxtasis, así como también 45 armas. En Italia, la policía ya había logrado cerrar los mercados “Berlusconi” y “DeepSea”, arrestando a 4 operadores e incautando 3,6 millones de euros. Ambos sitios contaban con más de 100.000 anuncios de productos ilegales. (p.1)
>
> Para Jean-Philippe Lecouffe, subdirector de operaciones de Europol señaló: “El objetivo de operaciones como esta, es advertir a los delincuentes que operan en la Dark Web, que la comunidad policial dispone de los medios y los socios globales para desenmascararlos y hacerlos responsables de sus actividades ilegales, incluso en áreas de la Dark Web”. (p.1). Por su parte, Christopher A. Wray, director del FBI indicó; “El FBI continúa identificando y llevando ante la justicia a los traficantes de drogas que creen que pueden ocultar su actividad ilegal a través de Darknet”

- **¿Cómo se gestó el golpe a la Dark Web?:**

  En enero de este año, (2021) la policía alemana logró capturar al responsable y desmantelar la “DarkMarket”, el mercado en línea más grande del mundo para tráfico de ventas ilegales, tales como dinero falso, drogas, datos de tarjetas de crédito robados, malware, documentos falsos y tarjetas SIM anónimas, entre otros. (p.1)

  Se trataba de un australiano de 34 años, que fue detenido en la frontera entre Dinamarca y Alemania. La investigación fue llevada a cabo por policías de diversos países, teniendo un desenlace extraordinario, ya que fueron confiscados más de 20 servidores que se encontraban ubicados en Moldavia y Ucrania, y que contenían registros de 320.000 transacciones, por un valor cercano a los 140 millones de euros, y cuyo pago se hacía con criptomonedas, (4.650 Bitcoins y 12.800 Moneros transferidos). Se pudo verificar que existían más de 2.400 vendedores y también más de 500.000 usuarios. (p.1)

  La infraestructura criminal proporcionó a los policías de todo el mundo un notable cúmulo de pruebas, que han servido para perseguir y acusar a los culpables, así como facilitar las complejas investigaciones posteriores. El EC3 (Centro Europeo de Ciberdelincuencia) también ha estado trabajando con esta información, a fin de identificar los objetivos clave. Producto del trabajo de inteligencia de las distintas unidades policiales, se logró la detención de las ya mencionadas 150 personas. (p.1)

- **Otros aciertos en la lucha contra la Dark Web:**

  En mayo de 2019 fue desmantelada en Alemania la que ha sido considerada la segunda mayor plataforma global de venta en la Darknet, arrestando a tres sospechosos. Se trataba del mercado en línea que funcionaba bajo el nombre de “Wall Street Market”. En aquella oportunidad los agentes de la Oficina Federal de Investigación Criminal (BKA) lograron incautar más de 550.000 euros en efectivo, criptomonedas Bitcoin y Monero (criptomoneda de código abierto), en una cantidad de centenares de miles y varios vehículos de gama alta. Los servidores de la plataforma registraban al menos 400.000 ventas, y su oferta contaba con más de 63.000 productos, tales como drogas de todo tipo, datos confidenciales, documentos falsificados y software maligno. (p.1)

  En septiembre de 2019, y tras cinco años de investigación, fue desmantelado en Alemania un centro de procesamiento de datos ubicado en un antiguo búnker de la OTAN en Traben-Trarbach, siendo detenidas 13 personas. Este centro alojaba numerosas plataformas ilegales en la red Darknet, utilizadas para la venta de drogas, de documentos y datos. Sin embargo, el mejor acierto fue que lograron desbaratar los ciberataques que se ejecutaban desde ahí, así como también la difusión de pornografía infantil. (p.1)

  En septiembre de 2020, fueron detenidas 179 personas consideradas presuntos vendedores ilícitos. Los arrestos se produjeron en Alemania, Estados Unidos, Países Bajos, Reino Unido, Austria y Suecia, como parte de un vasto operativo mundial contra delincuentes de la Darknet. Se incautaron más de 5,5 millones de euros en efectivo y monedas virtuales, 60 armas y alrededor de 500 kilogramos de drogas. (p.1)

A continuación haré mención de ciertas operaciones más pequeñas pero que reflejan precisamente el resultado de actividades de cuerpos policiales (a nivel de ciberdelicuencia)

- **Compraventas de datos personales y/o corporativos**:

  el robo de 100 millones de contraseñas de Linkedin en 2012 y 2016; el incidente que sufrió Wallapop en noviembre de 2019; la sustracción de los datos de más de 5 millones de clientes de la cadena hotelera Marriot en marzo de 2020; la copia de contraseñas de Zoom y Nintendo en abril de 2020, en pleno confinamiento por el coronavirus; o en 2021 los casos que afectaron a la aseguradora Zurich y T-Mobile. El robo se sanciona con prisión de 6 meses a 2 años y su venta o cesión con prisión de 6 meses a 2 años o multa de 3 a 18 meses (artículos 197 bis y ter del Código Penal). (p.1)

- **Ciberestafas:**

  realizadas mediante mails con todo tipo de argumentación (supuestas herencias, servicios profesionales, contactos para pareja, etc.), para que los destinatarios hagan disposiciones económicas; o mediante “phishing”, mails con la apariencia de ser de una entidad bancaria, usando bases de datos con números de tarjetas bancarias y cuentas de PayPal, sus claves y sus códigos CVV. Se sanciona con la pena de prisión de 6 meses a 3 años cuando exceda de 400 € (artículos 248-2-b) y 249 del Código Penal). (p.1)

- **Sextorsion:**

  mediante el uso de bases de datos robadas para lanzar spam indiscriminado mediante bots, enviando mails que incluyen la contraseña del destinatario para darle credibilidad, y se le amenaza con enviar una supuesta grabación sexual a sus contactos si no accede a pagar la cantidad que se le exige en bitcoins. Se sanciona como delito de coacciones con prisión de 6 meses a 3 años o con multa de 12 a 24 meses (artículo 172 del Código Penal). (p.1)

- **Pornografía infantil y grabaciones snuff (asesinatos, violaciones, torturas, etc.):**

  mediante la descarga de contenidos o indicación de los nombres de los archivos para descargarlos con programas de intercambio de archivos P2P (eMule, µTorrent, etc.). La venta y/o intercambio de material pedófilo se sanciona con prisión de 5 a 9 años y libertad vigilada, que se ejecutará tras la pena privativa de libertad, de 5 a 10 años (artículos 189-1-b) y 2 y 192-1 del Código Penal). La tenencia o adquisición para propio uso de pornografía infantil se castiga con 3 meses a 1 año de prisión o con multa de 6 meses a 2 años y libertad vigilada, que se ejecutará tras la pena privativa de libertad, de 1 a 5 años (artículos 189-5 y 192-1 del Código Penal). (p.1)

- **Tráfico de drogas:**

  que se envían por correo postal o servicios de mensajería y reciben el pago mediante bitcoins. En 2015 la Corte Federal de Nueva York impuso la cadena perpetua a Ross Ulbricht, de 30 años de edad, creador de la web conocida como “Ruta de la seda” (“Silk Road”) en la Dark Web, en la que se vendían drogas y otros productos ilegales, como culpable de narcotráfico, blanqueo de dinero, violación informática y otros cuatro cargos criminales. La sentencia fue confirmada en 2017 al desestimarse el recurso de apelación. El tráfico de drogas está sancionado con la pena de prisión de 6 meses a 3 años y multa de 6 a 12 meses, e inhabilitación especial para profesión o industria por tiempo de 6 meses a 2 años (artículo 359 del Código Penal). (p.1)

- **Infracción de derechos de propiedad intelectual:**

  permitiendo la descarga de contenidos audiovisuales (películas, series, música, etc.), libros (ebooks en distintos formatos) y software y contraseñas para el pirateo de videojuegos o accesos a plataformas online. Cuando se haga con el ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, y

no se limite a un tratamiento meramente técnico, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios, se sanciona con prisión de 6 meses a 4 años y multa de 12 a 24 meses (artículo 270-2 del Código Penal). (p.1)

- **Infracción de derechos de Propiedad Industrial:**

  ofreciendo productos falsificados (relojes, gafas, ropa, bolsos, material deportivo, etc.) que imitan los signos distintivos registrados por sus titulares sin su autorización. La distribución al por menor de productos que incorporen un signo distintivo idéntico o confundible con uno registrado se castiga con 6 meses a 3 años de prisión (artículo 274-2 del Código Penal). (p.1)

- **Usurpación de identidad:**

  ofreciendo el acceso, espionaje o toma de control de perfiles de redes sociales (Meta-Facebook, Linkedin, Twitter, Instagram, TikTok, etc.) o sistemas de mensajería instantánea (WhatsApp, Line, etc.) de terceros. En el supuesto del acceso al perfil, se sanciona como delito de violación de secreto de las comunicaciones y la intimidad con prisión de 1 a 4 años y multa de 12 a 24 meses (artículo 197-2 del Código Penal); y en el caso de que se controle el perfil, se castiga como delito de suplantación de identidad con prisión de 6 meses a 3 años (artículo 401 del Código Penal). (p.1)

- **Venta de objetos robados:**

  como vehículos (normalmente robados en la Unión Europea y “legalizados” en otros países), productos tecnológicos (smartphones, tablets, ordenadores, etc.), obras de arte sustraídas, etc. Con independencia de la pena que pueda corresponder a quien robó los objetos, el hecho de venderlos está sancionado como delito de receptación con prisión de 6 meses a 2 años (artículo 298-1 del Código Penal). En el caso de expolio de obras de arte, la pena es de

prisión de 6 meses a 3 años o multa de 12 a 24 meses (artículo 323 del Código Penal). (p.1)

Determinar el impacto de la legislación en cuanto al uso de la Dark Web por parte de los cuerpos policiales

Antes de abordar la legislación y por ende poder establecer el impacto de la misma por el uso de la Dark Web por parte de los cuerpos policiales, definamos **Ciberespacio**

- "Un entorno donde no existe espacio físico o territorio. El Derecho se ordena en el territorio, mar territorial y aire… el espacio o universo se escapa y el ciberespacio también, al ordenamiento jurídico conocido actualmente." (Ecija, 2017, p.1)
- "Existe el tiempo, no el espacio." (Ecija, 2017, p.1)
- "Un mundo virtual al que se accede a través de fronteras o ISP y estas info-pistas conectan los dos mundos." (Ecija, 2017, p.1)
- "Una acción en Internet puede afectar a las personas físicas y una acción en el mundo físico puede afectar al mundo virtual." (Ecija, 2017, p.1)
- "En este mundo nacen conductas antisociales que perjudican a otros (ciberdelitos, ciberterrorismo, ciberprivacidad, dinero virtual sin tributar…)" (Ecija, 2017, p.1)
- "Conviven los siguientes agentes: ciberorganizaciones y ciberciudadanos. No están los Estados, aunque están intentando «colonizarlos» a la fuerza, EEUU, Israel y China un claro ejemplo de ello." (Ecija, 2017, p.1)
- "La red es ideal para incumplir normas tras el anonimato que te brinda de forma sencilla y barata**."** (Ecija, 2017, p.1)

El marco legal o de legislación de cada país en función del uso de la Dark Web debe una claridad desde el punto de que ampara a los ciberagentes y por consiguiente cuales son los elementos que pueden ser considerados o no a la hora del manejo de todo lo concerniente en la materia legal.

En el caso español, el LECrim (en sus modificaciones respectivas) otorga un marco regulatorio en donde podemos desglosar algunos aspectos relevantes:

- **Definición del concepto ciberpolicías:**

  En sus artículos 282, y 588 quinquies , sexties y septies, establece dicha figura definidiendola de la siguiente manera:

  > los ciberpolicías pasan a ser los funcionarios que, habilitados por normas territoriales con rango de Ley, realizarían controles de ciberseguridad en internet, como por ejemplo, vigilancia pro activa o actuaciones reactivas y defensivas, para mantener el orden civil, evitar ciberconflictos y mitigar riesgos. En definitiva, intentar conseguir una mayor seguridad en el ciberespacio. (Ecija, 2017, p.1)

- **Definición del concepto ciberarmas:**

  El artículo 588 septies a., establece:

  > El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
  >
  > a) Delitos cometidos en el seno de organizaciones criminales.
  >
  > b) Delitos de terrorismo.
  >
  > c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
  >
  > d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación (Ecija, 2017, p.1)

Por supuesto queda establecido que las ciberarmas son: “como «las ciberaplicaciones utilizadas para atacar y causar un daño cibernético» o como ciberherramientas de defensa” (Ecija, 2017, p.1)

Para Ecija (2017) existen elementos a favor y en contra de los ciberpolicías los cuales por supuesto otorgan consideraciones que deben ser tomadas en cuenta:

a Argumentos jurídicos a favor de los ciberpolicías

- Por motivos de Seguridad Nacional y Ciberseguridad, el Estado debe ser el habilitado para realizar funciones de vigilancia pública para evitar problemas de seguridad, en vez de dejar el control de estos elementos en manos privadas.

- El ciberespacio plantea unos desafíos a los Agentes y Cuerpos y Fuerzas de Seguridad del Estado, que se ven desbordados con las herramientas actuales, y se necesita un marco normativo claro y habilitante para perseguir los ciberdelitos de una forma más eficaz.

En esto se desprende que efectivamente es responsabilidad del Estado realizar dicha vigilancia y que es un trabajo arduo porque precisamente (en el caso español) la normativa debe ser más clara para lograr efectivamente un trabajo apegado a la legislación en cuanto a la ciberdelicuencia.

Se ha mencionado que la LECrim ha sufrido modificaciones apuntando a poder otorgar un panorama jurídico bien determinado y establecer elementos que amparen conceptos como ciberpolicías y sus ciberarmas, lo que da pie a precisamente que los cuerpos policiales deban crecer y redefinirse y tener

cuerpos, unidades o divisiones únicamente y exclusivamente para manejo de la ciberdelicuencia.

b Argumentos jurídicos en contra de los ciberpolicías

- Esta ciberfigura y las actividades de cibervigilancia afectan a las libertades individuales de las personas que navegan por el ciberespacio, excediendo ampliamente el papel de garante de la ciberseguridad que se les supone.

- Esta ciberfigura no aboga por la ciberlibertad o libertad en un nuevo entorno virtual. Desde este punto de vista, el Estado se presenta como una amenaza y como un «Ciberbigbrother» sin ver limitado su poder

Producto de las ambigüedades y efectivamente su consecuente afectación a todo lo que eso implica, se observa que hay como la existencia o que pudiera existir o crearse la figura de un “SupraPoder” que no tendría limites o mejor dicho no tendría delimitado hasta donde deba llegar.

Es importante señalar que efectivamente es un trabajo a nivel legislativo (marco jurídico o legal) establecer todos esos aspectos sin que se afecten derechos o libertades de los ciudadanos al respecto.

Si tomamos ahora la legislación en un nivel más arriba es decir tomando ya ámbitos más amplios se tendría que hablar de:

- **La Cooperación Penal Internacional:** Jiménez (2018) señala que:

  > está involucrada en la persecución penal a nivel global para la regulación y sanción de las actividades ilícitas que puedan ser realizadas en Internet. Los cuerpos normativos emitidos por distintas organizaciones y Estados son necesarios para combatir los ataques

cibernéticos hacia los sistemas de información que forman parte de las comunidades virtuales. (p.35)

Esto implica que bajo el Derecho Internacional Penal:

> La cooperación judicial es la parte del Derecho Internacional Penal que se ocupa de establecer y regular los mecanismos a través de los cuales los Estados se prestan asistencia con el fin de favorecer el desarrollo de un proceso penal o la ejecución de una sanción. (Jiménez, 2018, p.36)

Agregando efectivamente que esta cooperación se enmarca en: a) con el procedimiento penal que se desarrolla en otro Estado; b) con el fin de ejecutar una sanción impuesta por otro Estado y c) con el fin de establecer qué ordenamiento resulta mejor situado para llevar a cabo un determinado proceso.

- **Convenios Internacionales:**
  A través de ellos la cooperación internacional tiene normativas que pueden ser efectivas y por ende favorecen la sanción en materia los ciberdelitos:

  - **Convenio de Budapest:** Este convenio nace el 23 de noviembre de 2001 a través del Consejo de Europa, se le conoce también como el Convenio de Ciberdelicuencia. Por tanto las conductas ilícitas que regula dicho convenio son: acceso ilegal, interceptación ilegal, interferencia de los datos, interferencia del sistema uso erróneo de dispositivos, falsificación del ordenador fraude del ordenador y pornografía infantil. (Jiménez, 2018, p.38), este convenio es lo suficientemente amplio y cualquier país puede tomar de referencia estando o no adherido a mismo y hacerlo cumplir y precisamente ha servido para aquellos países donde hay vacíos en su normativa legal en cuanto a estos temas y en especial los de la Internet Profunda.

- **Convenio No. 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las Personas con respecto tratamiento automatizado de datos de carácter personal:** Tomando su artículo número 1 donde se establece su objetivo y fin:

> Garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos). (Jiménez, 2018, p.39)

Aun cuando es una normativa que tiene muchos años y precisamente en la década de los 80 los delitos de esta naturaleza estaban por así decirlo sin una aparición formal, dio inicio a una regulación en esta materia y aún se toma para establecer parámetros iniciales que son perfectamente válido en las legislaciones

- **Decisión Marco 2005/222/JAI:** Nace el 24 de febrero de 2005 y fue firmado por la Unión Europea en Bruselas en dicha fecha. Tiene como finalidad el reforzamiento en la cooperación internacional entre las autoridades judiciales en los ámbitos de ejecución penal a los ilícitos informáticos. Los Estados miembros en armonía hacia la búsqueda del bien común en la red involucran una aproximación de sus normas penales para la regulación de la materia. Jiménez (2018) puntualiza que:

> De acuerdo con el Considerando II del cuerpo normativo en cuestión, su promulgación genera una vinculación de los sistemas de persecución penal hacia los ataques de los sistemas de información como consecuencia de la amenaza de la delincuencia organizada frente a las probabilidades de existir ataques terroristas hacia los Estados miembros poniendo en peligro la realización de una sociedad de la

información segura. Asimismo, unifica criterios para definir delitos informáticos, entre ellos, el acceso ilegal, intromisión ilegal de datos e información. Cabe señalar que los Estados que suscriben la decisión de señalar penas efectivas distinguiendo la gravedad de los ilícitos cometidos. (p.40)

- **La Organización de las Naciones Unidas (ONU) y la Prevención del Delito Informático:** Por su parte la ONU ha desarrollado lo siguiente en esta materia:
    - **Declaración de Viena sobre la Delincuencia y la Justicia frente a los retos del siglo XXI:** Bajo la sesión plenaria 81ª de fecha 04 de diciembre de 2000 aprueba la resolución número 55/59 sobre delincuencia y justicia frente a los retos del siglo veintiuno. Además agrega, que este instrumento tiene como punto de reflexión o de partida la preocupación de los Estados miembros con respecto al impacto, gravedad y cantidad de delitos de trascendencia internacional, la delincuencia organizada, la necesidad de generar políticas comunes de prevención y sanción de este tipo de ilícitos (Jiménez, 2018, p.41). La propia Asamblea General de la ONU en su cuerpo normativo de esta resolución establece:

        Decidimos formular recomendaciones de política orientadas a la acción para la prevención y el control de los delitos relacionados con la informática e invitamos a la Comisión de Prevención del Delito y Justicia Penal a que emprenda trabajos a este respecto, teniendo en cuenta la labor en curso en otros foros. Nos comprometemos también a esforzarnos por aumentar nuestra capacidad de prevenir, investigar y enjuiciar los delitos de alta tecnología y relacionados con la informática (Jiménez, 2018, p.41)

- **Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos:** Este documento recoge en esencia la definición y magnitud de los delitos informáticos y su impacto hacia la comunidad internacional, por tanto señala que los causales son: falta de acuerdos globales acerca de qué conductas tipo deben constituir delitos informáticos, falta de leyes especializadas en materia procesal, sustantiva, así como de investigación. el carácter transnacional de delitos cometidos mediante el uso de computadoras, ausencia de tratados de extradición, de acuerdos y de mecanismos sincronizados que permitan la plena eficacia de la cooperación internacional. (Jiménez, 2018, p.41)

  > Garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos). (Jiménez, 2018, p.39)

- **Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) Sobre el Derecho de Autor:** La OMPI nace el 20 de diciembre de 1996 con la finalidad de desarrollo un sistema de propiedad intelectual, en función del Convenio de Berna los países que suscribieron dicho tratado, se orienta hacia protección de las obras y los derechos de sus autores en el entorno digital.

- **Territorialidad y Alcance de la Ley Penal:** Este es un aspecto que merece atención y por ende ser tomado en cuenta. Jiménez (2018) destaca que la determinación espacial de validez de la Ley Penal es el resultado de un conjunto de principios jurídicos que fijan el alcance de la validez de la ley penal del Estado con relación al espacio, siendo más amplio que el territorio como como concepto jurídico, ya que está limitado por fronteras. Por tanto

a validez de las leyes penal de un Estado se circunscribe a un concepto de fronteras o límites físicamente establecidos queriendo decir con esto el ámbito de la misma. Por el mismo hecho de los conceptos de ciberespacio pareciera que esta queda fuera de este ámbito, ahora aplicando el concepto de territorialidad

> La territorialidad entra como principio determinante para explicar qué alcance merece la ley penal en cierto territorio y es que esta se atribuye a los límites del territorio del Estado que la emite. (Jiménez, 2018, p.44)

Esto abre una ventana de que cada Estado dentro de su normativa legal establece como debería interpretare de alguna forma esto, pero lejos de crear confusiones y ambigüedades, debe existir el espíritu de establecer lo que pueda ser mejor para establecer de alguna forma controles o sanciones en cuanto a la materia de ciberdelicuencia.

La legislación o marco legal por la cual se rige los diversos países como puede apreciarse tiene ciertos aspectos desde lo más interno (normativas del propio país), subiendo paulatinamente hasta llegar al tope donde está el ámbito internacional en donde hay un marco regulatorio en donde muchos países se han afianzado para poder establecer elementos de base para ayudar a los funcionarios como también apoyar a las víctimas y establecer las sanciones que hubiera lugar en cuanto a la materia de Dark Web se refiere.

Conclusiones

Esta investigación pueda consideró como puntos focales

- Un estado de arte que convino precisamente en delimitar los conceptos de Surface Web, Deep Web y Dark Web. Para muchos los dos últimos son lo mismo cuando realmente no lo son. Tomando el ejemplo de un iceberg lo más visible o somero es la Surface Web (Internet Superficial), la Deep Web es precisamente todo aquello que no se puede ubicar fácilmente por ende se denomina Internet Profunda y el concepto central que es Dark Web o Internet Oscura es lo que precisamente esta sumamente oculto y que tiende a ser totalmente ilícito y efectivamente se ha convertido en un resguardo de ciberdelicuentes en la actualidad.

- Al hablar del uso de la Dark Web por parte de los cuerpos policiales, se destacó precisamente el nacimiento de los cuerpos policiales cibernéticos y por consiguiente como ha sido empleando la misma Dark Web como se ha venido desmantelando poco a poco las diversas organizaciones que la emplean de forma ilícita. Operaciones con participación de muchos países han podido asestar golpes certeros en pro de un saneamiento de esta parte de la Internet.

- En materia de legislación se observó que existe la tendencia de adecuación del marco regulatorio de los países hacia la ciberdelicuencia pero también se ve el avance en materia a nivel internacional lo que ha podido de alguna forma ayudar a muchos países cuyo marco legal está débil en la materia de ciberdelitos apoyarse y poder establecer sanciones a los responsables de estos ilícitos.

Referencias Bibliográficas

A2secure. (2019). *Diferencias entre Surface web, Deep web y Dark web.* https://www.a2secure.com/blog/diferencias-entre-surface-web-deep-web-y-dark-web/

Academia Geopol. (2022). *Surface Web, Deep Web y Dark Web - Tema 39.* https://academia-geopol.es/surface-web-deep-web-y-dark-web-tema-39/

Aguirreburualde de Dios, A. (2022). *Internet oscura e internet profunda.*[Trabajo de fin de grado para Criminología y Seguridad]. Universitat Jaume. http://repositori.uji.es/xmlui/bitstream/handle/10234/198155/TFG_2022_AguirreburualdedeDios_Ainara.pdf?sequence=1&isAllowed=y

Algardata. (2022). *Surface Web, Deep Web y Dark Web: Los peligros de la web oscura.* https://www.algardata.com/es/blog-es/ciberseguridad/surface-web-deep-web-y-dark-web-los-peligros-de-la-web-oscura/

BLOG DE SEAS, CENTRO DE FORMACIÓN TÉCNICA EN MODALIDAD ONLINE. (2017). *Qué es Surface Web, Deep Web y Dark Web.* https://www.seas.es/blog/informatica/que-es-surface-web-deep-web-y-dark-web/

Carmiel, D. (2022). *Los cibercriminales han visto en la Dark Web el entorno ideal.* https://www.redseguridad.com/entrevistas/los-cibercriminales-han-visto-en-la-dark-web-el-entorno-ideal_20220318.html

Daniels, N. (2021). *La Dark Web: ¿Qué es exactamente y qué puedes encontrarte?.* https://vpnoverview.com/es/privacidad/navegacion-anonima/web-oscura-dark-web/

Ecija, A. (2019). *Ciberespacio, Dark Web y Ciberpolicía*https://noticias.juridicas.com/conocimiento/articulos-doctrinales/11763-ciberespacio-dark-web-y-ciberpolicia/

Fernández, Y. (2020). *Deep Web, Dark Web y Darknet: éstas son las diferencias.* https://www.xataka.com/servicios/deep-web-dark-web-darknet-diferencias

Fernández, Y. (2021). *Qué es la Dark Web, en qué se diferencia de la Deep Web y cómo puedes navegar por ella.* https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella

González, G. (2015). *Surface web, Deep web y Darknet: ¿en qué se diferencian?* https://blogthinkbig.com/surface-web-deep-web-darknet-se-diferencian

History-Computer. (2022). *Comparación completa entre Deep Web vs Dark Web.* https://history-computer.com/deep-web-vs-dark-web/

Iniseg. (2022). *Operación "Cazador Oscuro": nuevo golpe a la Dark Web.* https://www.iniseg.es/blog/ciberseguridad/operacion-cazador-oscuro-nuevo-golpe-a-la-dark-web/

Jimenez R., J. (2018). *El contexto jurídico de la Deep Web.*[Tesis de grado para]. Universidad Rafael Landívar. http://recursosbiblio.url.edu.gt/tesiseortiz/2018/07/01/Jimenez-Jose.pdf

Kapersky. (2022). *¿Qué es la Deep Web y la Dark Web?.* https://www.kaspersky.es/resource-center/threats/deep-web

Kratikal. (2020). *Surface Web y Dark Web: exploración de capas de Web.* https://kratikal.com/blog/surface-web-and-dark-web-exploring-layers-of-web/

López, J. (2021). *Delitos en la Dark Web.* https://revistabyte.es/legalidad-tic/delitos-en-la-dark-web/

Otero, C. (2022). *Los tres tipos de Internet que debes conocer: Web normal, Deep Web y la Dark Web.* https://as.com/meristation/2018/08/21/betech/1534888271_939768.html

Test de Velocidad. (2016). *Deep Web vs Dark Web ¿cuál es la diferencia?.* https://www.testdevelocidad.es/2016/10/07/deep-web-vs-dark-web/

Traversals. (2020). *Surface Web es solo la punta del iceberg.* https://traversals.com/blog/surface-web/

Zarzalejos, A. (2019). *Qué hace exactamente un policía para vigilar la dark web y localizar a los cibercriminales que pretenden ser 'invisibles' en Internet.* https://www.businessinsider.es/como-vigila-policia-dark-web-identificar-criminales-500365