FACULTAD DE CIENCIAS HUMANAS
COORDINACIÓN DE SOCIOLOGÍA, CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES

IMPLICACIONES DE LA TECNOSECURITIZACIÓN EN LAS RELACIONES INTERNACIONALES CONTEMPORÁNEAS

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE LICENCIADO EN RELACIONES INTERNACIONALES

FÉLIX DANIEL ANDUEZA ARAQUE

DIRECTORA: PAOLA LOZADA

MAYO, 2022

Resumen

En los últimos años se ha visto una transición dentro de la sociedad hacia gobiernos mucho más permeados por la tecnología. Una de las áreas en dónde se ha visto ese incremento tecnológico es en los procesos de seguridad. Actualmente, bajo la justificación de un mundo más seguro, se da una vigilancia perpetua a la población mediante el uso de cámaras de reconocimiento facial y la recolección de datos. Por ese motivo, el presente trabajo de investigación busca explicar como los procesos de securitización se han complejizado para dar paso a una prevención subjetiva mucho más amplia de los problemas de seguridad. Esta investigación se realizó mediante un enfoque cualitativo mediante una revisión bibliográfica. Ante estos hechos, se halló evidencia de que esta forma compleja de la securitización ha llevado a que se trasciendan los actos discursivos y se termine institucionalizando esta securitización.

Palabras clave: securitización, Escuela de Copenhague, tecnosecuritización, vigilancia masiva, Big Data, reconocimiento facial

Abstract

In recent years there has been a transition within society towards governments much more permeated by technology. One of the areas where this technological increase has been seen is in security processes. Currently, under the justification of a safer world, perpetual surveillance is given to the population through facial recognition cameras and data collection. For this reason, this research work seeks to explain how securitisation processes have become more complex to give way to much broader subjective prevention of security problems. This research was carried out using a qualitative approach with a bibliographic review. Given these facts, it was found that this complex form of securitisation has led to transcending discursive acts and ending up institutionalising this securitisation.

Keywords: securitsation, Copenhagen School, technosecuritisation, mass surveillance, Big Data, facial recognition

Índice

Introducción

Actualmente se vive en la era de la información, donde los datos son claves para el desenvolvimiento de la sociedad. Desde finales del siglo XX, el progreso tecnológico ha ido aumentando al punto de que se está viviendo una nueva transición, de la revolución digital a la cuarta revolución industrial (Perasso, 2016). Esto implica una unión de tecnologías físicas, digitales y biológicas en cuestiones como la inteligencia artificial o las neurotecnologías. De esta forma, esta nueva revolución se basa en "sistemas ciberfísicos, que combinan la infraestructura física con software, sensores, (…)" (Perasso, 2016). Esta cuarta revolución tecnológica está llevando a distintos cambios productivos, así como a cambios en la salud, la educación, la vivienda, y la seguridad (CEPAL, 2019), por lo que es importante plantear cuestionamientos sobre las afectaciones que se vivirán dentro de la misma en las Relaciones Internacionales contemporáneas.

Este tipo de progreso tiene consecuencias positivas y negativas para el desarrollo social. Por ello, la postura que se debe tomar no debe irse a los extremos, por lo que se debe ser realista y considerar el futuro de una forma racional. Dentro de esto, se debe tener en claro que la tecnología no es imparcial. De esta forma, las maneras de ver el mundo de las personas que crean estas tecnologías van a terminar incidiendo en como funcionan. Por este motivo es que se puede entender como en la actualidad, con los avances de la era de la información, se ha pasado del temor de un enemigo particular a la prevención de posibles enemigos en todas partes mediante la tecnología. Es así como, en conjunto con sus innegables progresos positivos, estos sistemas ciberfísicos han permitido una vigilancia permanente a la población (Petit, 2019; Hansen y Nissenbaum, 2009).

Todo lo anteriormente planteado está enmarcado en procesos de securitización dentro de la sociedad que, con la ayuda de estos sistemas ciberfísicos, pueden plantear diferentes

retos y dificultades en el mundo moderno. Por ese motivo, es importante preguntarse sobre de qué manera incide la aplicación de la securitización en las Relaciones Internacionales en la era de la información.

Ante este cuestionamiento, dentro del presente trabajo se ha planteado la siguiente hipótesis: dados los contantes cambios y avances de la tecnología en el siglo XXI, los procesos de securitización se han complejizado para dar paso a una prevención subjetiva mucho más amplia de los problemas de seguridad. Desde este punto de vista, teniendo en cuenta que no existe un marco jurídico internacional que regule la vigilancia tecnológica, se han creado vulnerabilidades sociales y problemas de gobernanza con los que se tendrán que lidiar en las Relaciones Internacionales contemporáneas.

Con el fin de llegar a comprobar dicha hipótesis, se ha planteado el objetivo de conocer las implicaciones de la securitización en las Relaciones Internacionales en la era de la información. Para cumplir con dicho objetivo, se han establecido tres objetivos específicos, los cuales también determinaran la estructura del presente trabajo de investigación:

1. Explicar qué es la securitización y su desarrollo histórico
2. Explorar las consecuencias de la tecnosecuritización en el ámbito de la gobernanza
3. Explorar las consecuencias de la tecnosecuritización en el ámbito social

De esta manera, el primer capítulo corresponde al primer objetivo específico, por lo que se buscó explicar cómo es la evolución histórica del concepto de seguridad y su transformación en la securitización. Con eso establecido, se trató de explicar cómo ha sido su evolución y aplicación en distintas áreas dentro de las Relaciones Internacionales. El segundo capítulo, correspondiente al segundo objetivo específico, se trató de dar cuenta de los impactos que tiene esta tecnosecuritización a nivel político e institucional. Finalmente, con el tercer capítulo, que sigue la misma línea y corresponde al tercer objetivo específico, se

explicaron los impactos de la tecnosecuritización en los niveles de Derechos Humanos y de control social.

Para sustentar todo este proceso, el marco teórico de esta disertación se enmarca en la securitización expuesta dentro de la Escuela de Copenhague. Dentro de esta perspectiva se menciona como los asuntos cotidianos se politizan por parte de los Estados con el objetivo de tener mayor control sobre ellos. Al ponerlos en la esfera de la seguridad como una amenaza a la integridad nacional, se justifica el empleo de cualquier medio, incluso extraordinario, para contrarrestar los posibles "daños" que podría causar. Sin embargo, al ser todo esto una percepción de los gobernantes, muchas veces no es la visión más adecuada de lo que está pasando y termina en violaciones a los derechos de las personas (Buzan, Waever y De Wilde, 1998)

Esta securitización cuenta con un marco temporal y una población objeto sobre la que recaen las políticas de securitización. Además de esto, las políticas implementadas generalmente se dan en términos militares. Esto se puede ejemplificar de forma sencilla con migraciones, que es el tema dónde más se aplica la securitización. Dentro del contexto latinoamericano, una de las grandes migraciones que se ha vivido esta enmarcada en la crisis venezolana. Por este motivo, dentro de los diferentes países se han implementado distintas medidas para afrontar cada una de las olas migratorias. Es así que en casos como el del Ecuador, por medio del acto discursivo, se ha visto esta migración como una amenaza existencial para la estabilidad nacional, por lo que esto terminó justificando medidas de emergencia en las zonas fronterizas, donde, además de contar con personal médico, se contaba con un control militar para "evitar irregularidades" (Reyes Guzmán, 2018).

Como se estableció anteriormente, esta securitización está delimitada en cuanto a tiempo y objetivo. Sin embargo, dentro de los procesos de las sociedades actuales altamente tecnológicas, existen problemas para establecer esta delimitación. Por ello en años recientes

se amplia el concepto de la securitización con la tecnosecuritización. Dentro de esta ampliación, el control mediante la información permite a los Estados una prevención profunda ante cualquier acto "irregular". Esto, con un fin de seguridad, se hace a costa de clasificar a todo el mundo como una amenaza existencial poniéndolos en una vigilancia permanente. En este punto es que nace lo que se conoce como "*everywhere war*" (Petit, 2020)

A nivel metodológico, la presente investigación tiene un alcance explicativo sobre las implicaciones que está teniendo la tecnosecuritización en los ámbitos expuestos anteriormente. Se pretende explicar la forma en la que se dan las políticas de securitización y sus futuras implicaciones en las Relaciones Internacionales. Por este motivo, se entiende que este trabajo tiene un enfoque cualitativo, lo cual se realizó desde una revisión bibliográfica de las causas y efectos de esta tecnosecuritización en las Relaciones Internacionales contemporáneas.

Finalmente, cabe destacar la relación que tiene esta disertación con el área de estudios. Esta tesis cae dentro del campo de estudios de las Relaciones Internacionales debido a que está relacionado a las áreas de Seguridad Internacional y de Problemas Contemporáneos de las Relaciones Internacionales. De esta forma, esta investigación busca dar una perspectiva ligada a la tecnología y a la seguridad, la cual poco se ha desarrollado dentro de la academia hispana.

Capítulo 1: La Securitización

El objetivo de este capítulo es explicar qué es la securitización y cuál es su desarrollo histórico dentro de las Relaciones Internacionales. Esto se realizará mediante un desarrollo progresivo de qué implica la seguridad y cómo se ha llegado al concepto de la securitización. De la misma manera, se busca explicar cuál es el complemento y actualización que se está haciendo a la securitización mediante la "tecnosecuritización" y cómo este nuevo formato está siendo clave en las implicaciones que se van a tener por parte de la securitización en las Relaciones Internacionales de la era de la información.

1.1 Origen y Contexto Histórico

Históricamente se ha visto un gran debate sobre diferentes conceptos dentro de las Relaciones Internacionales (Robinson, 2008, p.1). Específicamente dentro de los estudios de seguridad, ha existido un debate sobre un término que, a pesar de ser esencial, no tiene un acuerdo común dentro de la academia. Este concepto es el de seguridad. Partiendo de la forma más básica, la seguridad implica la ausencia de una amenaza. Esto puede ser visto desde dos perspectivas, bien sea absoluta o relativa. Desde la perspectiva absoluta se entiende que una persona, Estado u objeto está o no seguro. Es una visión totalmente binaria del tema. Desde la perspectiva relativa, se pueden tener distintos grados de seguridad, dependiendo del grado o intensidad que tenga la amenaza. (Robinson, 2008, pp.1-2).

A pesar de que a simple vista la definición de seguridad sea sencilla, distintos académicos, especialmente dentro de los "Estudios Críticos de Seguridad", mencionan que es un concepto "esencialmente disputado" (Horowitz, Allen, Saravalle, Cho, Frederick y Scharre, 2018; Detraz, 2013; Robinson, 2008, p.2). Esta disputa se da en el marco de distintos cambios en el escenario político a nivel mundial. Históricamente los estudios de seguridad estaban determinados por el poder desde una mirada realista o liberal, sin embargo, tras la caída del Muro de Berlín, la desaparición de la Unión Soviética, el auge de los conflictos

étnicos dentro de las naciones, y de las amenazas transnacionales con actores no-estatales, se empezaron a crear distintas ramas dentro de estos estudios que buscaban ampliar el concepto a un campo más amplio de amenazas para la supervivencia humana (Munster, 2005, p.2)

Dentro de este debate por ampliar el concepto de seguridad y de ampliar la visión del Estado como único objeto referente, aparecen los enfoques feministas, posestructuralistas, poscoloniales, y de la Escuela de Copenhague. (Buzan 1983, pp.2-8; Ravelo, 2018, p.59). Del interior de este conjunto, una de las ramas que más ha sobresalido es la Escuela de Copenhague. Esto, dado que ofrece un marco claro para el análisis con preguntas específicas que ayudan a entender qué constituye un asunto de seguridad. Esto lo logran al tomar una postura intermedia entre los enfoques tradicionales de la seguridad y los enfoques más críticos, lo que también implica un punto medio entre el positivismo y el postpositivismo (Baysal, 2020, p.7; Ravelo, 2018, p. 59).

Este marco de análisis que ofrece la Escuela de Copenhague es conocido como la teoría de la securitización. Esta fue estructurada formalmente por Buzan, Waever, y De Wilde en su libro de 1998 "*Security: A new framework for analysis*". Dentro de este libro ofrecen una visión de la seguridad diferente, donde exponen que esta es principalmente sobre la supervivencia. Mencionan que la seguridad es cuando se presenta un asunto público que es puesto como una amenaza existencial para un objeto referente. Esta amenaza, al poner en riesgo la supervivencia de un ente, justifica tomar las medidas necesarias para poder lidiar con ello. En esta perspectiva, la seguridad se pone al nivel de la esfera política, siendo la securitización una forma extrema de la politización. (Buzan, Waever, y De Wilde, 1998). Cabe destacar que, dentro de esta perspectiva, el asunto a securitizar no es necesariamente una amenaza real, sino que mediante actos discursivos se presenta como una amenaza existencial. (Buzan, Waever, y De Wilde, 1998).

Esta teoría se enmarca en una visión regional de seguridad. Esto, dado que, tras los conflictos de la Guerra Fría, se determinó que era más práctico a nivel metodológico el empezar a estudiar la seguridad a nivel nacional y regional para luego hacer comparativas con otros países y regiones. Esta perspectiva se entiende con la entrada de un mundo unipolar, donde no es sencillo entender como funciona el mundo si solo se tiene en cuenta el ejercicio de poder que puede llegar a realizar el hegemón. (Buzan y Waever, 2003, p.11). A pesar de esto, el análisis no se queda de forma estricta en ese nivel. Muchos procesos de securitización alrededor del mundo tienen como base elementos que son causados por la globalización, como los problemas identitarios, de mercado negro de armas, o el terrorismo, por lo que es posible analizar como las regiones o los países interactúan con las amenazas globales, poniendo como objeto referente valores universales como el régimen económico mundial o el ecosistema planetario. (Buzan y Waever, 2003, p. 12-13)

1.2 Aplicación

Tal como fue mencionado anteriormente, la securitización puede ser vista como una forma extrema de politización. Cualquier asunto que esté localizado en una esfera diferente a la política, lo cual implica que no está sujeta al debate público, puede ser llevada al plano público. Al estar en el plano público, el gobierno o cualquier actor con legitimidad suficiente para imponer una narrativa, puede convertirlo en un asunto que más allá de requerir decisiones gubernamentales, necesite de acciones emergentes que puedan salir de los límites normativos y legales de la política. (Buzan, 1998, p.24)

La aplicación de estas acciones se da mediante el discurso político. Un argumento con una retórica y estructura semiótica particular puede persuadir de manera tan efectiva a una audiencia al grado de que esta llegue a tolerar las violaciones de las reglas comúnmente impuestas para regular el poder del Estado, es decir, lo que conocemos como el Estado de Derecho. (Buzan, 1998, p.24). Lo mencionado anteriormente tiene un punto bastante

particular, y es que, hay que tomar en cuenta que el hecho de que un discurso ponga como una amenaza existencial al objeto referente, esto no crea la securitización. El asunto termina siendo securitizado solo cuando la audiencia lo acepta como tal. (Buzan, 1998, p.25). Estos procesos discursivos son tomados de teorías lingüísticas, y se denomina acto discursivo, o "*speech act*". (Buzan, 1998, p.26)

Dentro de esta teoría, el análisis tiene que responder unas preguntas particulares que llevan a entender mejor el contexto sobre el que se está trabajando. En este caso, hay que entender quién es el que securitiza (actor securitizador), sobre qué asunto se da la securitización (cuál es la amenaza), a quién se está amenazando (objeto referente), por qué se esta dando esa amenaza y securitización, cuáles son los resultados, y en qué condiciones se está dando (Baysal, 2020, p.7).

A pesar de ser una teoría bastante particular, distintos académicos han señalado sus limitaciones iniciales, lo cual se desarrollará a continuación. La más común es relacionada a los actos discursivos, donde se dice que llevarlo netamente al terreno lingüístico limita el entendimiento a otras formas de comunicación por las que se puede transmitir el mensaje de securitización, como las imágenes o los videos. Además, expresan como es que no solo porque se exprese una idea en un discurso es que va a realizarse la securitización, sino que esto parte de la institucionalización y rutinización a través de la repetición de las prácticas de seguridad. Finalmente, se critica que esta teoría no toma en cuenta el contexto de los asuntos, ya que se piensa que en un momento particular el actor securitizador decide realizar el acto discursivo simplemente porque ve una amenaza, cuando esa construcción puede devenir de un contexto histórico. (Baysal, 2020, p.7-8). Atendiendo a estas críticas, el presente trabajo se enmarcó en la teoría de la securitización con las actualizaciones que se han venido haciendo desde 1998, como el tomar el acto discursivo como un elemento de narrativa que puede ser implementado por cualquier medio comunicativo para su aceptación pública, el tomar en

cuenta el contexto histórico que lleva a la creación de esas narrativas específicas o su implementación como en contextos digitales, como se menciona más adelante.

1.3 Uso en la Década de los 90's

Son distintos los casos que se han analizado bajo la perspectiva de la securitización a lo largo de la historia. Sin embargo, para este periodo se consideró de forma muy breve dos casos específicos: los hackers en los Estados Unidos y las FARC[1] en Colombia. Se eligieron estas dos situaciones dado que, en el primer caso, se puede empezar a visualizar la securitización en contextos tecnológicos y, en el segundo caso, se puede entender que el actor securitizador no tiene que ser necesariamente el Estado, sino un actor legítimo capaz de imponer narrativas. Para el primer caso, se puede evidenciar como un acto discursivo crea el sentimiento de una amenaza existencial cuando el Pentágono designó a los hackers como una "amenaza catastrófica" y una "seria amenaza para la seguridad nacional" (Buzan, 1989, p.40). Esto dio paso a que el gobierno de los Estados Unidos tomara medidas drásticas para enfrentar esta amenaza. Entre estas medidas estuvo la "Operación Sundevil" llevada a cabo por el servicio secreto, donde se tuvo como objetivo a grupos de hackers que eran sospechosos del uso y robo de números de tarjetas de créditos. Se rastreó a numerosos individuos que terminaron presos por sus actividades, mientras el gobierno expresaba que "la salud y bienestar de individuos, corporaciones y las agencias del gobierno quienes dependían de la infraestructura tecnológica estaban siendo amenazadas". A pesar de tener esta gran cobertura, no existe prácticamente evidencia de que estos "robos" de información fueran críticos o costosos (Halbert, 1997, p.361).

Dentro del segundo caso se puede observar el proceso de securitización que llevó a cabo el gobierno colombiano en contra de las facciones comunistas colombianas tras la era de violencia en 1960. Esto, sumado a el contexto de narcotráfico llevó a que se tuviera como

[1] Entendido como Fuerzas Armadas Revolucionarias de Colombia

actor esencial a los Estados Unidos en el proceso de securitización, al declarar que estos grupos eran una amenaza para la estabilidad regional. A pesar de esto, el proceso de securitización no se dio solo por parte del Estado como actor legitimo, sino que se extendió a los propios grupos comunistas, que en un proceso de contrasecuritización crearon guerrillas armadas como las FARC. De esta forma, ambos tenían al otro como una amenaza existencial que justificaba las medidas extraordinarias que se dieron en la década de 1980 y 1990 en Colombia, con la guerra contra las guerrillas (Baysal, 2020, p.12).

1.4 Uso en la Década de los 2000 y de los 2010

Durante los primeros años del siglo XXI se encuentran muchos más casos de securitización. Estos se ven enmarcados en áreas como la identidad, la migración, la energía, el medioambiente, la salud global o la religión (Balzacq, Léonard y Ruzicka, 2016, p.506). Sin embargo, a modo de desarrollo de los más relevantes, se explica de forma breve los procesos de securitización en el contexto de la Guerra contra el Terror y la crisis migratoria en Europa. Para el primer caso, generalmente se hace una distinción entre una guerra formal y la guerra que es creada desde el discurso de las élites. De esta forma, la Guerra contra el Terror que se genera tras los atentados de septiembre de 2001 se ve legitimada no solo por los discursos proclamados por el presidente de los Estados Unidos, sino que se articula por medio de los medios de comunicación, como los periódicos y las cadenas televisivas, donde la narrativa de una versión del conflicto se ve internacionalizada por la cobertura mediática y facilita su aceptación por parte del público (Vultee, 2010, pp. 33-37). De la misma forma, esta guerra global contra el terror utilizaba un lenguaje determinado (como el “eje del mal”) que convertía este asunto en materia de seguridad internacional. De esta forma, con una retórica de suma-cero, terminaban resurgiendo temas como la civilización versus la barbarie, que durante varios años justificaron la invasión de países en el Medio Oriente (Coşkun, 2012, pp.3-5).

Dentro del caso de migración, el problema toma un tinte histórico pues en muchas sociedades humanas se ha tenido un gran recelo hacia las influencias externas. En el caso de Europa se puede visualizar desde dos perspectivas: Grecia y Alemania. En el caso de Grecia, este país vivió un proceso de emigración entre 1951 y 1981 debido a las condiciones económicas y sociales del país. Sin embargo, para inicios y mediados de la década de 1980, este proceso se invierte y las personas empiezan a regresar por las condiciones económicas favorables que se estaban dando. A pesar de esto, el país estaba lejos de ser económicamente estable. No obstante, el final de la Guerra Fría marcó un antes y un después, dado que se produjo un gran flujo de migrantes hacia Grecia, puesto que se ofrecía trabajo a personas indocumentadas. Este flujo de migrantes generó un descontento en la población, quienes decían que "los migrantes les estaban quitando el trabajo". Ante esto, el Estado empieza a ver a estos migrantes como una amenaza, lo que se puede ver con las palabras y frases que más se repetían durante los discursos políticos, como: "problemáticos", "inundación de aliens", "invasión", "hordas hambrientas". Esto generó la introducción de una nueva ley de regulación migratoria, llamada "Ley Alien", donde todas las categorías migratorias estaban unidas bajo dicho término. (Karyotis, 2012, pp.390-395). Dentro del caso alemán, se pueden observar dinámicas similares, pues en 2015 se dio la crisis migratoria en Europa tras el conflicto de la primavera árabe. Aunque en menor medida que en Grecia, en Alemania y en gran parte de Europa se tuvo el problema de la no aceptación de la población musulmana, pues se pensaba que eran terroristas, lo que a largo plazo dificultó su integración en estos países. (Barnai y Kreide, 2017, p.908).

Dentro de esta época la securitización dio un paso importante. Esto dado que su uso se convirtió en parte fundamental de la política de los Estados, especialmente de los Estados Unidos, tras el 9/11. Esto conlleva a un uso indiscriminado de la vigilancia al "otro", el cual es enmarcado como el enemigo. Dentro de esta época, el uso de la securitización implicó una

institucionalización de la vigilancia, tanto en temas de identidad, migración, energía, religión, como en medio ambiente o salud.

1.5 Uso en la Actualidad

En la actualidad es importante tener en cuenta los problemas que se han venido desarrollando de manera histórica, así como los que empiezan a tener impactos que antes parecían poco relevantes. De esta manera, hay que poner un énfasis en como se dan los procesos de securitización en diferentes temáticas como: materia ambiental, teniendo en cuenta que el gasto excesivo de recursos naturales está llevando a problemas como la desaparición de varias islas en el Pacífico (de Jong y Gallagher, 2021); en materia de salud, teniendo en cuenta como la sociedad se ha adaptado a la pandemia del COVID-19 y como puede afrontar futuras situaciones similares (Park y Lim, 2020), y, el punto central en el desarrollo de esta investigación, como se dan los procesos de securitización en el ámbito tecnológico, teniendo en cuenta que vivimos en mundo cada vez más interconectado donde los flujos de información no solo son constantes, sino que son masivos y pueden transformar la forma en que las personas viven (Araya, 2012). De la misma forma, estamos cada vez más rodeados de dispositivos electrónicos como teléfonos, computadoras, relojes inteligentes, lentes inteligentes y demás dispositivos que nos mantienen atados al mundo digital, que cada vez se amplia más con conceptos como el del metaverso[2].

1.5.1 La Tecnosecuritización y la Cibersecuritización

Bajo la caracterización dada anteriormente, es importante especificar como se dan los procesos de securitización en el sector tecnológico. Esto puede resultar bastante amplio porque abarca diferentes elementos del mundo actual y generalmente es bastante difuso el

[2] El metaverso es entendido como una sociedad red, o una digitalización de la sociedad. Esto implica que se termina con una línea delgada entre lo real y lo virtual pues las personas van a empezar a interactuar, vivir, trabajar, etc. Dentro de estos espacios virtuales. Desde la misma palabra “metaverso” implica una forma de trascender el universo que ya conocemos y llevarlo a este plano digital. El metaverso no es una invención de Facebook, pues es algo que data de principios de siglo con plataformas como SecondLife o Habbo (Ávila, 2022; Vargas, 2022)

entendimiento que se tiene sobre el impacto de la securitización en el sector tecnológico (Balzacq, Léonard y Ruzicka, 2016, p.515), por lo que este tipo de securitización generalmente se entiende en dos grupos: cibersecuritización y tecnosecuritización.

A pesar de que ambas van a estar estrechamente relacionadas en distintos puntos, es importante caracterizarlas para dar un mayor entendimiento de como se utilizó en el presente trabajo. A muy grandes rasgos, la cibersecuritización se va a entender como la securitización realizada directamente mediante el *software*, y la tecnosecuritización mediante el *hardware*. Es decir, una implica solo las redes de computadoras y la otra implica el componente físico, como las cámaras, sensores, computadoras, y otros dispositivos tangibles.

Con esta breve explicación, se pasará a ampliar esta diferenciación. La cibersecuritización es dada en el contexto de la ciberseguridad, la cual viene siendo utilizada desde la década de los 90s para dar un entendimiento a las diferentes inseguridades que pueden verse dentro de las redes de computadoras. Este concepto está ligado a metodologías técnicas que son utilizadas dentro del campo de la informática. (Hansen y Nissenbaum, 2009, p.1155). Esta ciberseguridad se liga con la securitización porque dentro de la misma década diferentes políticos norteamericanos expresaron su preocupación por un posible "Pearl Harbor electrónico"[3] y por una posible utilización de la informática para la creación de nuevas "armas de destrucción masiva" (Hansen y Nissenbaum, 2009, p.1155). Este discurso es legitimado por el público al existir poco entendimiento de como funcionan estos asuntos, además de por la gran digitalización que se estaba creando por los procesos la tecnologización de la globalización y, además, se ve incrementado por el sentimiento de inseguridad que se derivaba del 9/11. (Hansen y Nissenbaum, 2009, p1156).

[3] Este "Pearl Harbor electrónico" implicaba un posible ataque contra la infraestructura cibernética de los Estados Unidos, lo cual les dejara en un estado de vulnerabilidad. Por ejemplo, un ataque al sistema bancario pondría en serios problemas a la estabilidad del país. Por ese motivo se buscó reforzar la seguridad electrónica en gran medida (Hansen y Nissenbaum, 2009)

Bajo el mismo orden de ideas, la cibersecuritización puede ser entendida como la forma en que la cooperación entre los ejércitos, las agencias de seguridad y las empresas se refleja en la protección de sistemas e infraestructura informática que puede ser clave para el bienestar nacional y tiene un impacto en la población al momento en que estas personas se transforman en una amenaza constante para los sistemas (Cristiano, 2020, p.1). El punto discursivo que explicaban Hansen y Nissenbaum (2009) previamente puede ser visto en la definición expresada antes sobre la forma en que se puede entender la cibersecuritización, sin embargo, puede complementarse entendiendo que en la actualidad existe un miedo constante hacia los temas informáticos al punto de que el objeto referente central, el Estado, se esta viendo en una amenaza existencial. Por este motivo, desde hace algunos años se está hablando del daño que pueden hacer las personas a los Estados o Estados a otros Estados, en situaciones como la llamada "*Web War I*", donde por primera vez en la historia se registró el ataque hacia un país por medios informáticos, en este caso Rusia hacia Estonia en 2007[4] (Ooijen, 2020, p.7).

Bajo la caracterización anteriormente dada, los objetos que pueden recaer en la inseguridad dentro de la cibersecuritización son bastante amplios y pueden ir desde individuos, negocios e, incluso, procesos electorales. (Fouad, 2019, p633). Todo esto puede ser enmarcado en lo que se puede denominar como una "sociedad del riesgo", donde en la nueva modernidad se entiende que cualquier actor puede ser construido como una amenaza ante el sistema predominante. De esta manera, existe una amenaza ante la "sociedad libre que implica economías prosperas y gobiernos transparentes" (Fouad, 2019, p635). Todo esto

[4] Dentro de este caso, Estonia responsabilizó a Rusia por los ataques que afectaron medios de comunicación, bancos e instituciones gubernamentales de Estonia (Quiñonez, 2021). Este ataque se dio tras el levantamiento de un monumento de homenaje a un héroe soviético que estaba en Estonia. Esto fue considerado como un ataque a la memoria rusa, por lo que procedieron al ataque (Ooijen, 2020). Este fue el primero de muchos ataques informáticos realizados por Rusia, los cuales han incrementado en el contexto de la guerra de Rusia contra Ucrania.

implica una legitimización de poner a la sociedad como una amenaza, lo cual es la base para todo el contexto de securitización.

Como se explicó anteriormente, esta cibersecuritización tiene una base técnica donde la población va a terminar amenazando el sistema por medio de redes, como los ataques informáticos o la vulneración de dispositivos propios. Esto da un entendimiento de como la tecnología puede tener una incidencia en la securitización. Ahora, la securitización que se va a manejar dentro del presente trabajo está más orientada a la tecnología en términos físicos (*hardware*) y al análisis de datos recolectados. En esa perspectiva entra la tecnosecuritización. Marin (2017), explica como dentro de los procesos de globalización el mundo se ha convertido en una "aldea global" donde los bienes, capitales e información circulan a través de todo el mundo. Esto implica que cualquier tipo de flujo transnacional es más común que en el siglo anterior, lo que lleva a nuevas formas de inseguridad (p133). En esa medida, los Estados, dentro de la era de la información, han implementado la tecnología para prevenir estos nuevos riesgos, entre los que se puede encontrar la vigilancia y la recolección de datos mediante procesos como el *Big Data*. (Marin, 2017, p.133).

Una forma más precisa de entender esta problemática es que desde la filtración de contenidos secretos dada por Snowden en el 2013, la sociedad ha entendido como desde agencias de seguridad como la NSA[5] se ha obtenido el acceso a grandes empresas tecnológicas como Facebook, Google o Apple. Este acceso resulta crucial pues esta información permite tener un control más cercano a las posibles amenazas que puede tener un Estado, como es el caso del terrorismo. Sin embargo, bajo este pretexto se ha puesto como amenaza existencial a todo el mundo, lo que justifica emplear cualquier medio para su control. Y más allá del peligro de tener a todo el mundo como amenaza existencial es que este proceso de securitización no tiene un marco temporal estricto donde se den las políticas

[5] La Agencia de Seguridad Nacional de los Estados Unidos, por sus siglas en inglés

de control, sino que da paso a un control permanente. Una supervisión permanente. De esta forma, se pasa de la violencia de Estado versus Estado a la del Estado versus individuos o grupos de personas, por lo que todo este proceso se denomina como "*everywhere war*" (Petit, 2020, p.8).

En este contexto, desde lo digital, existe una problemática donde el individuo se convierte en problema de seguridad nacional manejado por distintas tecnologías de vigilancia y monitoreo de la vida diaria (Lacy y Prince, 2018, p2). Esto se puede visualizar en distintos escenarios como la vigilancia de aglomeraciones como forma de contraterrorismo en Japón (Nishiyama, 2018, p2), la vigilancia de las fronteras para contener la crisis de refugiados en Europa mediante la toma de decisiones automatizada con inteligencia artificial, recolección de datos biométricos y reconocimiento facial (Sadik y Ceren, 2020, p146), hasta casos que se presentan en este trabajo como el de China, Reino Unido, Estados Unidos y Corea del Sur. Desde una perspectiva bastante amplia, todo esto está enmarcado en un disciplinamiento social, donde desde la biopolítica[6] se busca que las personas se autorregulen por la extrema supervisión con el objetivo del control de la gestión total de la vida. (Foucault, 2009; Rodríguez-Merino, 2018)

Con este capítulo se cumple el objetivo de la explicación y desarrollo del concepto de la securitización. Se puede ver como históricamente el concepto de la seguridad ha sido disputado y, dependiendo de la perspectiva, puede tener diferentes implicaciones. Por esta ambigüedad del término han surgido diferentes enfoques críticos que buscan ampliar el concepto a objetos referentes más allá del Estado. Dentro de estos nuevos enfoques surge la

[6] Según López (2013), el concepto de biopolítica es acuñado por Rudolph Kjellen a principios del siglo XX para dar un entendimiento al funcionamiento del Estado como un organismo vivo (p.112). Sin embargo, a finales del siglo XX es retomado y popularizado por Michel Foucault para dar cuenta de la forma de ejercicio del poder político que tiene como objetivo el control de la vida biológica del ser humano (Castro, 2008, p.2)

Escuela de Copenhague, la cual, mediante sus principales exponentes Buzan y Waever, traen el concepto de la securitización. Dentro de este concepto se entiende a la seguridad como un proceso discursivo que tiene efectos dentro de la población al poner un asunto como de extrema emergencia. Con esto presente, dentro de la era de la información este conflicto se ha actualizado y así se llega a la tecnosecuritización, donde los actos discursivos tienen un impacto que se termina articulando mediante diversos hardware y el análisis de datos.

Capítulo 2: La Tecnosecuritización en la Gobernanza

En este capítulo se explora cuáles son las consecuencias de la tecnosecuritización en el área de la gobernanza. Estas implicaciones estarán articuladas como las implicaciones políticas y las institucionales que puede tener esta securitización. Para demostrar esto se utilizaron dos casos: La seguridad desde la gobernanza algorítmica dentro del Reino Unido y las dinámicas de vigilancia realizadas desde la alianza de inteligencia de los "5 ojos".

2.1 Implicaciones Políticas

2.1.1 Gobernanza Algorítmica

Dentro de las formas políticas que puede tener la tecnosecuritización se puede encontrar la gobernanza algorítmica. Para esto, se debe entender como actualmente la era de la información se puede caracterizar de mejor manera como un "capitalismo de la vigilancia". Dentro de la globalización se ha gestado parte de la tercera revolución industrial que implica el desarrollo de las tecnologías de la información y la comunicación (TIC). Estas tecnologías han permitido que se cambien las dinámicas de poder en la sociedad y que el ser humano ahora tenga la capacidad de transmitir, almacenar y procesar mucha información en muy poco tiempo (Araujo, 2022, p.6). Este procesamiento de la información se da mediante algoritmos que clasifican a las personas y establecen formas de predecir su conducta (Araujo, 2022, p.2).

Sin embargo, para entender lo anteriormente expuesto es importante establecer qué es un algoritmo. Según la Real Academia Española (s.f), un algoritmo es un "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema". Con esa base, se puede entender que un algoritmo conlleva una serie de pasos para llevar a cabo una tarea. Con esa conceptualización, se puede pasar al análisis de como esos algoritmos están teniendo una influencia en la forma en como se maneja la política hoy en día. Gómez (2019) explica que actualmente se vive en la era del algoritmo o en una "algocracia" donde las matemáticas

y la informática están teniendo un impacto en la forma de moldear y guiar el comportamiento humano y la gobernanza (p.219). Dentro de este modelo, la forma en la que se concibe un algoritmo ha ido cambiando de un modelo “de arriba hacia abajo” que implicaba un establecimiento de reglas por parte de los programadores, a un sistema “de abajo hacia arriba”, donde los algoritmos tienen incorporadas reglas que les permiten aprender e instalar un orden de reglas propio (Gómez, 2019, p.220).

Entendiendo la conceptualización del algoritmo, la principal preocupación que surge en la era de la información es cuál es el rol que tienen estos algoritmos y su efecto de ordenamiento dentro de la gobernanza y las relaciones sociales. Ante esto, los algoritmos moldean acciones, procedimientos y decisiones desde sus prácticas matemáticas, lógicas y estadísticas (Katzenbach y Ulbricht, 2019, p.2; Grisenko y Wood, 2022, p.45). De esta forma, se intenta que todo tipo de decisión tenga una base totalmente lógica para poder ser lo más objetiva y eficiente posible, lo que llevaría a una gobernanza que, en el papel, parece mucho más justa porque parece predecir cuales son los problemas que van a existir en un área determinada. Sin embargo, la sociedad no puede ser medida en términos netamente matemáticos porque esto puede dar paso a problemas como la discriminación, como se desarrollará mas a profundidad en apartados siguientes.

Dentro de todo lo que significa el tener a los algoritmos en espacios sociales existen dos narrativas predominantes. Una explica como con los algoritmos la gobernanza puede ser más inclusiva y sensible a los cambios sociales, y otra que explica como la gobernanza puede ser más poderosa e intrusiva (Katzenbach y Ulbricht, 2019, p.2). Dentro del presente trabajo se entiende que ambas narrativas son complementarias y que tienen elementos que pueden ser ciertos y otros que no lo son. Por ejemplo, una mayor eficiencia puede ser significativamente importante a la hora de implementar planes de acción públicos y solventar problemáticas que pasan en el día a día. De la misma forma, en el momento en que se securitiza mediante

discursividades este asunto, puede terminar con sesgos que afecten de forma negativa a la población. De esta manera, el presente trabajo tuvo un mayor desarrollo dentro de la narrativa negativa, pues el desarrollo a nivel social de las cuestiones positivas de la tecnologización de la gobernanza es ampliamente aceptado, pero solo en años recientes se ha puesto un cuestionamiento de esta, tal como se está haciendo de los efectos de la globalización.

Actualmente, los algoritmos son parte del día a día, pero al no ser tangibles las personas no se dan cuenta de ello. Estas cuestiones se pueden ver desde los *feeds* personalizados de las redes sociales hasta como se dan las decisiones comerciales actualmente (Gritsenko y Wood, 2022, p.45). De esta manera, los datos y los dispositivos electrónicos se han convertido en elementos que son clave para la gobernanza. Al momento en que la cotidianeidad donde las personas viven se eleva en gran medida a terrenos digitales se eleva lo virtual a la categoría de nueva plaza pública (Innerarity y Colomina, 2020, p.12). De esta forma, el acceso a los datos de cualquier persona es mucho más sencillo que antaño y su control es disputado y, en muchas ocasiones, compartido entre el sector público y el privado. De este modo, el tránsito hacia la mecanización y automatización de la gobernanza pasa por distintos intereses que pueden ir en contra de los intereses ciudadanos (Innerarity, 2020, p.89).

Habiendo entendido toda esta implicación política de la gobernanza, es importante cruzarlo con el tema de la securitización. Y es que, a pesar de que, como anteriormente se expuso, la gobernanza algorítmica puede ser positiva en términos de eficiencia de políticas, la mayor parte de las veces está orientado a la seguridad. Esto dado que históricamente los Estados han tenido una motivación para sus acciones que va más allá de una eficiencia en sus procesos y es el de preservar la propia integridad. Por esta motivación es que los Estados han desarrollado distintos sistemas que buscan estar al tanto de las acciones enemigas para poder prevenir cualquier ataque. De esta manera, y como se desarrollará más adelante con la

privacidad, la tecnología ha permitido un incremento y desarrollo de estos sistemas, por lo que han aparecido diferentes sistemas que ahora son conocidos gracias a las filtraciones de Snowden. Entre estos sistemas se pueden encontrar el proyecto MINARET para espiar a figuras públicas en el contexto de la Guerra Fría, el proyecto SHAMROCK para vigilar de forma masiva los telegramas y llamadas entrantes y salientes de los Estados Unidos, el proyecto DISHFIRE que recopila millones de SMS de todo el mundo, el proyecto MYSTIC, que recopila los metadatos relacionados a llamadas en todo el mundio y el proyecto PRISM que engloba la vigilancia de todo el internet. (Medero, 2013, pp.120-121; Preibusch, 2015, P.1)

Teniendo esto en cuenta, Treguer (2019), explica como esta gobernanza algorítmica ha creado la "ciudad inteligente" que realmente puede ser vista como una "ciudad bajo vigilancia" (p.1). Se está pasando a la creación de un Leviatán[7] político mucho más poderoso con la colaboración de grandes empresas. Con el objetivo de reducir cualquier amenaza, las empresas ofrecen herramientas informáticas que son puestas en espacios públicos y tienen la capacidad de "vigilar, analizar, predecir y controlar los flujos de personas y de mercancías" (Treguer, 2019, p.1). De esta manera, la premisa de "reducir cualquier amenaza" implica que cualquier persona puede ser una amenaza y eso legitima su vigilancia perpetua. Para esto, los tecnócratas creen que, mediante los dispositivos de vigilancia y el aprendizaje que tienen los algoritmos, se pueden detectar características o patrones estadísticos desde los que se podrá "categorizar, seleccionar, anticipar, adelantar, ajustar, poner en punto de mira y reprimir" cualquier acción que pueda parecer amenazante (Treguer, 2019, p.1). De esta forma, dentro de la gobernanza algorítmica, el gobierno como actor con legitimidad suficiente para imponer

[7] El Leviatán es un concepto explicado por Hobbes dentro de su teoría del Estado. En ella explica al Estado como un Leviatán que tiene la capacidad de ofrecer seguridad a la población. De esta manera, todos los hombres renuncian a su derecho natural (la libertad), entendiendo que será una máxima para todas las personas. De esta forma, nadie puede atentar contra otra persona y, por lo tanto, el ente que se encargará de la protección es el Estado y sobre el recae el monopolio de la fuerza (Astorga, 2009, p.152). De esta forma, se entiende como es que las personas ceden su libertad en pos de la protección del Leviatán.

una narrativa, explica que el "otro" puede resultar un peligro, por lo que hay que tomar medidas drásticas. Al existir un miedo a lo diferente, las personas terminan aceptando esta vigilancia que va a mantener neutralizado al otro, pero que al mismo tiempo nos termina neutralizando a nosotros mismos. De esta manera, se termina perpetuando el concepto hobbesiano del Leviatán, donde cedemos nuestra libertad en pos de la seguridad. Solo que en este punto transitamos hacia un Leviatán tecnológico que se articula mediante medidas securitizadoras.

2.1.2 La Seguridad Desde la Gobernanza Algorítmica en el Reino Unido

2.1.2.1 Caso

Como se expuso anteriormente, dentro de los Estados contemporáneos se ha normalizado el "estado de vigilancia" o "la sociedad de la vigilancia", donde esta termina convirtiéndose en la principal forma de organización política (Wood y Webster, 2009, p.259). Con esto en mente, uno de los casos más interesantes dónde se están aplicando las medidas de la gobernanza algorítmica es en el Reino Unido, donde se están empezando a realizar cuestionamientos acerca de la ética y las implicaciones en libertad y seguridad que conlleva la nueva normalidad de estar en constante vigilancia (Wood y Webster, 2009, p.260).

Para establecer los impactos de este caso primero hay que entender cuál es su contexto. Para esto primero se puede ver como históricamente la vigilancia se ha desarrollado con tintes racistas, dado que al hablar de vigilancia se puede remontar al control que se tenía sobre las personas afrodescendientes en los barcos de comercio de esclavos, o las leyes de linternas en los Estados Unidos, que requerían a los esclavos a llevar linternas en la noche para poder reconocerlos y ubicarlos en todo momento. (Chowdhury, 2020, p.5). Estas cuestiones han sido normalizadas dentro del imaginario social mediante distintas narrativas desarrolladas a lo largo de la historia, lo que lleva a que actualmente exista una racialización de la seguridad.

El racismo institucionalizado en la sociedad ha llevado a su reflejo en distintas escalas. Por ejemplo, la comunidad BAME (Afrodescendientes, Asiáticos y otras Minorías Étnicas, por sus siglas en inglés), está sobrerrepresentada en las bases de datos, listas de vigilancia y en las prisiones. A pesar de representar el 3% de la población, son la mayoría en estos espacios, lo que hace que sea mucho más probable que se detenga a un miembro de la comunidad BAME antes que a una persona blanca (Chowdhury, 2020, pp.8-9). De la misma forma, en años más recientes, un problema social en el Reino Unido ha sido la islamofobia, donde la narrativa de prevención ante el terrorismo ha sido interiorizada dentro de la sociedad y lleva a que el 47% de los votantes conservadores y un 22% de los votantes laboristas consideren que el Islam es una amenaza para la forma de vida británica y, por lo tanto, se justifican las medidas en su contra como la vigilancia o la prohibición del porte de velos religiosos que cubran la cara (Chowdhury, 2020, p. 9; London Policing Ethics Panel, 2019)

Este problema se ve reflejado en la gobernanza algorítmica porque hay dos problemas: primero que los algoritmos terminan siendo creados por humanos y, segundo, que estos sistemas de vigilancia son alimentados con datos históricos de las cortes y de los arrestos, que al final están reflejando las prácticas discriminatorias que se realizan en el día a día del sistema penal (Smith, 2020). De esta manera, el realizar una vigilancia bajo estos parámetros no está consiguiendo una sociedad más segura, sino que solo busca el control de los que considera amenaza. Este problema de los algoritmos también se ve reflejado en como se da el reconocimiento facial, y es que las cámaras y programas están diseñados y probados por personas blancas, lo que ha causado que estos sistemas fallen a la hora de identificar a hombres afrodescendientes o asiáticos. Incluso en el caso de mujeres afrodescendientes, son más propensas a ser identificadas de forma errónea en una mayor cantidad de ocasiones (BBC News, 2019; Big Brother Watch, 2018).

Estos sesgos raciales son agravados en el contexto tecnológico contemporáneo. Actualmente esta securitización no se da solo por los circuitos cerrados de televisión o CCTV, pues estos solo toman fotos. El reconocimiento facial va más allá y toma medidas como la distancia entre los ojos, el largo de la nariz, la forma de la cara, etc. De esta forma, más que una evolución del CCTV es una evolución de la toma de huellas y el control establecido por esta (Chowdhury, 2020, p.5; Rahim, 2019; Portal, 2018). Este reconocimiento facial está manejado por inteligencia artificial, la cual cada vez toma mayor peso en la toma de decisiones y puede determinar si una persona debe ser contratada, despedida, se le debe o no otorgar un préstamo, o cuando tiempo debe permanecer en prisión (Buolamwini y Gebry, 2018, pp.1-2). Al no ser una tecnología imparcial, aquí surgen todos los problemas que se expusieron anteriormente.

A pesar de que, como se expuso anteriormente, el reconocimiento facial no es la evolución de los CCTV, si se vale de la infraestructura de estos para poder realizar sus operaciones. De esta manera, toda esta infraestructura va más allá de la reducción del crimen y pasa a ser un poder para observar y potencialmente intervenir en una amplia variedad de situaciones, sean estas criminales o no (Norris y Armstrong, 2015, p.158). Este gran poder de observación se ve incrementado por la cantidad de cámaras que están presentes en el Reino Unido. Actualmente existen más de 6 millones de cámaras, lo que por ciudadano es mayor que cualquier otro país a excepción de China (Chertoff, 2020).

Ahora, todo este problema racial se ve incrementado cuando se entiende que el Reino Unido tiene reglas y leyes muy ambiguas a la hora de regular esta vigilancia. En teoría, la vigilancia por sistemas de cámaras está regulada por el Acta de Protección de Libertades del 2012 (POFA, por sus siglas en inglés), por el Acta de Regulación de los Poderes Investigativos del 2000 (RIPA, por sus siglas en inglés) y el Acta de Protección de Datos del 2018 (DPA, por sus siglas en inglés). Para cada acta existe un comisionado que vela por su

cumplimiento y que es independiente del secretario de Estado. Sin embargo, en 2016 expresaron que no sabían cual de ellos tenía que ser el responsable por la supervisión de los sistemas de reconocimiento facial, por lo que ninguno iba a responder a las problemáticas y solicitaban la creación de un nuevo código de conducta que regule a estas tecnologías (Chertoff, 2020).

Esta ambigüedad legal lleva a que actualmente incluso las empresas privadas puedan usar este reconocimiento facial sin hacer este cambio de forma pública y sin notificarlo a las autoridades (Dearden, 2019). De esta forma, dentro del Reino Unido se vive una "epidemia" de la vigilancia, donde a cada paso que se da las personas están siendo escaneadas y están siendo sujetas a una alineación policial digital sin siquiera saberlo. En los sitios en donde hay mayor cantidad de cámaras las personas han intentado pasar ocultando su cara con alguna prenda y han sido detenidas por "disturbio del orden público" (Carlo, 2019; Big Brother Watch, 2018)

De forma más específica, algunos de los casos más sonados de los problemas de esta vigilancia perpetua son, en primer lugar, el caso del uso del reconocimiento facial en áreas con mayoría de personas pertenecientes a la comunidad BAME, como en el festival caribeño, en el carnaval de Notting Hill, además de en las zonas de Stratford y Romford en Londres. En estos lugares se reportó un alto número de detenciones, donde en muchos casos la identificación era errónea (Chowdhury, 2020; Smith 2020). En segundo lugar, se tiene el caso del ex concejal de Cardiff, Ed Bridges, quien fue detenido luego de que en su hora de almuerzo asistiera a una protesta pacífica y fuera reconocido por estas cámaras. El estar presente dentro de esta protesta pacífica fue motivo suficiente para su detención. Él realizó una demanda contra la policía alegando que se estaban violando normas británicas y la Convención Europea de Derechos Humanos. Sin embargo, el dictamen fue a favor de la policía alegando que la vigilancia era mínimamente intrusiva (Dearden, 2020; Chertoff,

2020). Finalmente, esta el caso de la Baronesa Jenny Jones quien expresó su preocupación de que la policía estaba utilizando el reconocimiento facial para identificar e interferir con las reuniones confidenciales con denunciantes con los que ella se reunía regularmente como parte de sus obligaciones parlamentarias. Ella expresó esta preocupación, pero no fue escuchada por el gobierno (Chertoff, 2020)

2.1.2.2 Actor Securitizador

Dentro de este caso se puede determinar que el actor securitizador es el gobierno del Reino Unido. Si bien es cierto que se cuestiona la legitimidad que pueden tener los políticos al tomar decisiones enmarcadas en un contexto tecnológico (Hersee, 2019, p.59), el actor ve su discurso legitimado bajo dos métricas: la narrativa de la necesidad de la seguridad ante amenazas inminentes y el racismo sistémico que presenta la sociedad británica. A pesar de que la privacidad es una cuestión preocupante para la población, la cobertura de las problemáticas relacionadas a la vigilancia es menor en los medios de comunicación en relación con las problemáticas sobre al crimen y la violencia (Barnard-Wills, 2011, p.548). Por este motivo, el discurso termina siendo aceptado por la población por cuanto apoya la vigilancia en pos de la disminución del crimen (Chowdhury, 2020, p.13).

2.1.2.3 Amenaza

La amenaza tal vez es mucho más clara. Como se había expuesto anteriormente la sociedad puede representar un peligro ya que esta puede “llevar a cabo actos terroristas” o poner en peligro a la ciudadanía mediante el crimen. El problema es que, al tener esta institucionalización del racismo, la amenaza principal para el gobierno termina siendo los miembros de la comunidad BAME y las comunidades musulmanas. Al ser percibidas como amenaza a la estabilidad y, por ende, a la existencia del Estado y los valores británicos, se termina justificando la vigilancia como medida de securitización. A pesar de esto, la

vigilancia perpetua es para todas las personas y no solo para los miembros de estas comunidades.

2.1.2.4 Objeto Referente

El objeto referente en primera instancia es el Estado mismo, pues un alto nivel de criminalidad puede llevar a una insatisfacción general que dirija a un cuestionamiento de toda la estructura que lo sostiene, por lo tanto, termina siendo el ente principal bajo la amenaza existencial. Sin embargo, por otro lado, se pueden ver los valores mismos de la nación como amenazados, pues la institucionalización del racismo ha llevado a que se piense que tanto la comunidad BAME como las comunidades musulmanas pueden cambiar la forma de vida británica.

2.1.2.5 Análisis e Implicaciones

Con los puntos anteriormente expuestos se demuestra la existencia de una securitización dentro del Reino Unido. El gobierno es un actor con la suficiente legitimidad para imponer una narrativa, la cual en este caso es que hay una amenaza que más allá de decisiones políticas requiere de acciones emergentes que terminan saliendo de los marcos legales. Esta amenaza, en este caso, se ve representada por estas comunidades que han sido históricamente discriminadas y que se ven como actores que podrían implicar un atentado contra la estabilidad y bienestar nacional. Estos temas terminan siendo aceptados por la audiencia, ya que estos están atravesados por la institucionalización del racismo que está presente en el imaginario colectivo.

Todo esto pasa al terreno de la tecnosecuritización al momento en que las acciones emergentes realizadas por el gobierno ya no son en temas militares, sino que está marcado por el reconocimiento facial enmarcado en el contexto de la gobernanza algorítmica. De esta forma, la acción extraordinaria es entendida como una presencia absoluta del gobierno para prevenir cualquier atentado contra su integridad. A pesar de estar pasando por encima de,

incluso, los Derechos Humanos, el peligro que es percibido por el gobierno es tan grande que justifica estas medidas.

Todo esto es sumamente peligroso dentro de las Relaciones Internacionales contemporáneas porque en conjunto con la tecnologización de la sociedad, se está entrando a una era donde el Estado es capaz de adentrarse cada vez más en la vida de las personas para de esta manera ejercer más control. A medida que pasa el tiempo, la tecnología se va distribuyendo en el mundo, gracias a la globalización, y así como antaño los teléfonos móviles eran poco comunes y ahora están en el día a día, la tecnosecuritización mediante el reconocimiento facial se puede hacer común. De esta manera, hay que preguntarse que medidas se pueden tomar a nivel nacional o regional para la implementación de leyes, regulaciones o prevenciones como iniciativas desde la sociedad civil para evitar que se tenga el mismo efecto que dentro del Reino Unido. Más, tomando en cuenta que dicho país es una democracia estable. Las consecuencias que esto podría tener en países con una menor calidad democrática pueden asemejarse mucho más a las historias que se han visto dentro de distopías literarias.

2.2 Implicaciones Institucionales

2.2.1 "Jurisdiction Shopping"

La tecnosecuritización también puede tener impactos significativos en cuestiones relativas a la institucionalidad o estructura de los Estados. Esto se puede enmarcar dentro de lo que se conoce como *"Jurisdiction Shopping".* Sin embargo, antes de pasar a su explicación, hay que tener varios conceptos claros. El primero de ellos es el de jurisdicción. Según la Real Academia Española (s.f) existen varias formas de entender la jurisdicción. Entre las más atingentes para el presente trabajo se pueden encontrar dos: el poder o autoridad que tiene alguien para gobernar y aplicar leyes en un territorio en particular, o el ámbito y territorio en el que se ejerce una autoridad o poder.

Esta conceptualización es importante, ya que la jurisdicción se ha construido, en conjunto con conceptos como el de Estado de Derecho o el de soberanía, como una forma de implementar el derecho como técnica de regulación y de limitación de los poderes públicos (Ferrajoli, 1997, p.3). De esta forma, la jurisdicción funciona como una garantía para asegurar la justiciabilidad de las violaciones de derechos que se puedan dar en un determinado territorio (Taruffo, 2008, p.384). De este modo, todo lo que incumbe al Estado y su accionar está delimitado en un espacio determinado donde puede obrar.

Esta jurisdicción está condicionada y ligada, como se mencionó anteriormente, a los conceptos de Estado de Derecho y soberanía que se desarrollarán de forma breve. El primero tiene que ver con una prevención ante el ciudadano de las consecuencias que puede tener vivir en un Estado absolutista. De esta forma, se busca el aseguramiento de la libertad y propiedad del individuo (Borda, 2007, p.73-73). Esto implica que el Estado de Derecho es la sujeción del Estado al derecho (García Ricci, 2015, p.23) o, en otras palabras, que el Estado puede hacer solo lo que la ley le permite, así como las personas pueden hacer cualquier cosa siempre y cuando no esté prohibido por la ley[8]. En esa misma línea, la soberanía es entendida como el poder supremo de dictar una ley y hacerla cumplir sobre un territorio determinado (Zuppi, 2002, p.19). Todo esto implica, que, para una buena institucionalidad, el Estado debe estar limitado por el correcto funcionamiento de estos elementos.

Con estos puntos en cuenta, se puede pasar a la explicación de "*Jurisdiction Shopping*". En principio, se puede entender que implica una forma de tomar beneficio de la

[8] Dentro de este punto cabe hacer una salvedad. La premisa de que el Estado puede hacer solo lo que la ley le permita y las personas pueden hacer todo lo que no esté prohibido por la ley es una forma coloquial y sencilla de entender qué es lo que implica algo como el Estado de Derecho. Sin embargo, de forma más formal, hay que entender que dentro de las relaciones sociales en Derecho se pueden encontrar el sector público y el sector privado. Dentro del derecho público solo se puede hacer lo que la ley permite, y es aquí donde entra en el accionar del Estado. En Derecho privado se puede hacer todo lo que no esté prohibido. A pesar de esto, hay personas que pueden encontrarse dentro del derecho público y otras dentro del derecho privado. De la misma forma, existen ramas como el derecho laboral que se entienden en un marco privado, pero sus intereses son públicos. Por este motivo, de forma mucho más formal, las personas no tienen una libertad absoluta de accionar, depende desde dónde se esté mirando el asunto en cuestión.

jurisdicción de un Estado en particular. Este término es usado principalmente en disputas económicas y comerciales, y en estas implica que un actor puede terminar eligiendo en que jurisdicción quiere que su caso sea sometido a juicio, cuando en muchos casos se elige el del país con leyes menos severas. Esto no es algo que se de en cualquier situación, sino que aplica cuando son conflictos transnacionales (Baumgartner, 2016; Cornell University Law School, s.f). Dentro de este sentido del término, Petit (2020) realiza una aplicación de este a las dinámicas de seguridad. De esta forma, se entiende esta *"jurisdiction shopping"* como una externalización de la vigilancia. De esta manera, este concepto describe el proceso por el cual un Estado gana acceso a la jurisdicción de otro Estado, mediante la externalización o delegación de acciones que son prohibidas dentro de la propia jurisdicción (p.11). Bajo esta visión, mediante el empleo de programas de vigilancia en jurisdicción extranjera, y con la colaboración con agencias extranjeras, se lidia con los problemas legales a los que podrían llevar los esfuerzos de la vigilancia (Petit, 2020, p.11). Esta forma de externalizar la vigilancia puede tener efectos perjudiciales dentro de las Relaciones Internacionales Contemporáneas y es una de las principales fuentes de funcionamientos de alianzas como la de los "5 ojos".

2.2.2 Vigilancia Desde la Alianza de Inteligencia de los "5 ojos"

2.2.2.1 Caso

Como se expuso anteriormente, uno de los principales ejemplos para hablar de la externalización de la vigilancia entendida desde el *"jurisdiction shopping"* es la alianza de inteligencia de los "5 ojos". Esta es una alianza de seguridad compuesta por Canadá, Australia, Nueva Zelanda, Reino Unido y los Estados Unidos. Esta alianza de cooperación en materia de inteligencia nació en la Segunda Guerra Mundial como una forma de cooperación entre el Reino Unido y Estados Unidos para compartir información que pudiera ser valiosa para la seguridad de ambos. (Cox, 2013, p.4). Esta relación entre E.E.U.U y el Reino Unido

tuvo inicio el acuerdo nombrado como UKUSA enfocado a hacer frente a la URSS. Más adelante, en 1948 se une Canadá y, en 1956, se unen Nueva Zelanda y Australia, dado que estas tres últimas seguían manteniendo vínculos institucionales, políticos y culturales con el Reino Unido bajo su concepción de dominios británicos (Pfluke, 2016, p.302). En teoría, cada uno de estos países tiene una combinación de supervisión de sus agencias de inteligencias desde el parlamento, el ejecutivo o desde entes judiciales. Sin embargo, dado los intereses estratégicos que se manejan, en muchas ocasiones estas agencias tienen una amplia libertad (Baker, Petrie, Dawson, Godee, Porteous, Purser, 2017, p.1)

A pesar de que este acuerdo está enmarcado en la vigilancia para la seguridad, no está exento de críticas. Antes de explicar sus formas de supervisión, la principal crítica deriva de su conformación y de los ámbitos a los cuales está suscrito, y es que a pesar de que tenga su origen al final de la Segunda Guerra Mundial, su existencia no fue conocida hasta el año 1999 cuando autoridades australianas declararon que tenían acuerdos de inteligencia con estos otros países. Y, aún así, muchas particularidades de este acuerdo no fueron de dominio público hasta las filtraciones de Edward Snowden en 2013. Incluso con este contexto, hoy en día, no se tiene acceso al acuerdo actualizado de forma completa. (Ruby, Goggin, y Keane, 2017)

Con estas explicaciones se puede entender que es un acuerdo bastante polémico con un potencial de alcance global, pues hasta donde se sabe cada uno de los países es responsable de recolectar información de una zona. De esta forma, Australia monitorea el Sur y el Este de Asia, Nueva Zelanda el Sur del Pacífico y el Sudeste Asiático, el Reino Unido a Europa y Rusia Occidental, Canadá a Latinoamérica, y Estados Unidos al Caribe, China, Rusia, Medio Oriente y África. (Cox, 2013, p.6). Ahora, esta alianza se encarga de la recolección de información obtenida desde diferentes formas. En principio su accionar está enmarcado en la SIGINT (inteligencia de señales, por sus siglas en inglés). Esta inteligencia

viene de la recolección y análisis de emisiones electromagnéticas transmitidas a través redes de información global (Cox, 2013, p.6). A partir de este acuerdo es que surgen divisiones de inteligencia en estos países, por lo cual la recopilación de estos datos pasa, en el caso de los Estados Unidos, de la CIA a la NSA (Ruby, Goggin y Keane, 2017). De esta forma, si de este acuerdo surgen organismos como la NSA, se puede entender que proyectos mencionados anteriormente en este trabajo como el MINARET, el SHAMROCK, el DISHFIRE, el MYSTIC, el Carnivore o, más peligroso aún, el proyecto PRISM tienen origen en este acuerdo.

Los países parte de la alianza de los "5 ojos" han adoptado medidas de vigilancia como las escuchas telefónicas, el análisis de los metadatos[9] o el análisis del internet y las redes sociales (Walsh, 2016, p.349). En este orden de ideas, la primera forma es entendida como un método de intercepción de las comunicaciones entre individuos residentes en los países parte o en países externos (Walsh, 2016, p.350). La segunda forma es entendida como el análisis de los datos generados por llamadas telefónicas, como los números de teléfono, ubicación, o el tiempo de llamada, sin tener en cuenta el contenido mismo de la llamada. Además de esto, desde las filtraciones de Snowden, se sabe que con el programa PRISM las agencias tienen acceso a una gran cantidad de datos digitales, como correos electrónicos, publicaciones de Facebook o mensajes instantáneos. Este último modo, a diferencia del solo análisis de datos de las llamadas, también implica la recolección del contenido de estas comunicaciones (Walsh, 2016, pp.351-352). La última forma, que es el análisis del internet y

[9] Los metadatos pueden entenderse como un conjunto de datos que describen información sobre otros datos (Pabón Cadavid, 2020). Esto implica que es un conjunto de datos que puede brindar información importante, como patrones de comportamiento de un individuo. Esto se entiende mejor con el ejemplo dado por Snowden en una de sus entrevistas: Si llevas un teléfono encima, el gobierno puede saber que fuiste a desayunar a un Starbucks, luego fuiste a una clínica especializada en oncología y estuviste varias horas allí, finalmente llamaste a tu madre y estuvieron una hora hablando. Estos tres metadatos empiezan a esbozar una imagen de la situación socioeconómica del individuo y de su salud. Con muchos más metadatos, ya que generamos miles día a día, el panorama de quienes somos resulta muchísimo más claro. Es la vigilancia perfecta. (LaSexta, 2016)

redes sociales, implica utilizar las redes como fuente de información para entender como se piensa colectivamente de un tema en situaciones de emergencia o crisis (Walsh, 2016, p.355).

Con todo lo expuesto anteriormente, existen diferentes visiones de los efectos que tiene esta alianza. Hay visiones que exponen los aspectos positivos y otras los negativos (Pfluke, 2016). De esta forma, entre los aspectos positivos se puede encontrar que, en primer lugar, por su carácter global se puede mantener actualizada la lista de amenazas y compartirlas con los países aliados, lo que implica una mejor prevención de desastres. En segundo lugar, esto ha permitido un mayor desarrollo de las capacidades ofensivas cibernéticas para la defensa de los actores parte (Pfluke, 2016, p.305; Gold, 2020, p.2020). Entre los aspectos negativos se pueden encontrar, en primer lugar, los atentados contra la privacidad que parten de las actividades de vigilancia. En segundo lugar, que la recolección de datos puede dar paso a brechas de seguridad sobre los mismos que lleven a una desconfianza entre los miembros. Y, en tercer lugar, que ha existido una censura a la publicación de información sobre las consecuencias de este acuerdo por parte de la Academia y de los medios de comunicación, pues al estar como documentos clasificados puede conllevar represalias legales por parte de los Estados miembros (Pfluke, 2016, pp. 305-307; Ruby, Goggin y Keane, 2017)

2.2.2.2 Actor Securitizador

Dentro de este caso, se entiende que la alianza de los “5 ojos” se posiciona bajo el rol de actor securitizador. De acuerdo con lo expuesto anteriormente, al estar enmarcada en una alianza de seguridad e inteligencia para recolectar información y prevenir un ataque externo, se esta enmarcando en un discurso de amenaza inminente. En un inicio era mucho más claro el “enemigo”, pues se planteaba una prevención desde Occidente a posibles ataques de la URSS. Sin embargo, tras la desaparición de esta última, esta concepción del “otro” enemigo también desaparece. De esta manera, surgen otras amenazas a la existencia de los miembros,

como lo puede ser el terrorismo. Por estos motivos, la vigilancia masiva realizada por la alianza podría entenderse como un discurso securitizador

2.2.2.3 Amenaza

La amenaza ha evolucionado. Estuvo entendida como la URSS por largo tiempo, pero, más adelante, se entendió esta amenaza como el terrorismo. De esta manera, esta alianza justifica la vigilancia mediante la intervención del *hardware* como forma de prevención de esta amenaza. La supervisión de todo el internet o la intervención de llamadas como forma de recolección de metadatos es entendida como esta prevención. Todo esto implica que la amenaza es la sociedad. Cualquier persona es una amenaza para el Estado y, por lo tanto, se justifica la vigilancia.

2.2.2.4 Objeto Referente

El objeto referente es el Estado. Dentro de un contexto de globalización característico de la era de la información, el Estado no solo se enfrenta a amenazas internas específicas, como movimientos sociales, o a externas, como Estados enemigos, sino que la amenaza está en cualquier parte del mundo. Esto podría ser el justificante para tener una red de vigilancia zonal que abarque a todo el mundo.

2.2.2.5 Análisis e Implicaciones

Si bien dentro de este caso se puede identificar quién es el actor, sobre qué asunto se da la securitización, a quién se amenaza, y, de cierto modo, por qué se da esta securitización, existen problemáticas para observar este hecho desde la securitización y, específicamente, desde la tecnosecuritización.

Para el primer punto, el problema es que no se está dando el acto discursivo de forma clara. Es decir, de cierta forma se puede entender que la sociedad va a terminar legitimando el control que se puede hacer por medio de los metadatos si es que tiene un incentivo para ello, como pasa con el control que existe por medio de metadatos desde las empresas, donde con

este control ofrecen contenido o productos personalizados para los clientes a cambio de su información[10]. En este caso, la legitimidad se puede dar desde el ofrecimiento de una seguridad ante los peligros del mundo como el terrorismo. Sin embargo, esta alianza ha sido confidencial por gran parte de su historia, solo expuesta a medias tras las filtraciones de Snowden, lo que implica que no existe un proceso de socialización donde la sociedad termine aceptando. A pesar de que cumple con ciertos parámetros de la securitización, es complicado realizar el análisis sin un acto discursivo.

Para el segundo punto, en apartados anteriores se explicaba la diferencia entre tecnosecuritización y cibersecuritización. El problema en este punto es que se están utilizando medios virtuales y físicos para esta securitización. Esto implica que es un cruce entre ambas concepciones. A pesar de esto, puede considerarse esta dualidad en la utilización para entender de forma mucho más profunda el caso. Aún con esta ampliación, continúa la problemática del acto discursivo. Por lo que lo que se necesitarían más elementos en la teoría para dar un análisis que abarque la totalidad de este fenómeno.

A pesar de lo anteriormente mencionado, se pueden establecer las implicaciones que este acto puede tener en las Relaciones Internacionales contemporáneas. Que los Estados puedan tener una capacidad vigilancia tan amplia puede llevar a un incremento de sociedades con tintes totalitarios. Esto es problemático porque puede darse el caso de una mayor violación de Derechos Humanos y una menor capacidad de la sociedad civil para defenderse ante estas problemáticas. De la misma forma, dentro de la sociedad actual existe un problema relacionado a la brecha tecnológica. Es decir, no todas las personas pueden acceder a la

[10] Sobre este punto, existen muchos debates sobre las razones por las cuales las personas actualmente toman la privacidad como algo sin importancia. A un nivel bastante amplio, se puede entender que las recompensas, entendidas como un servicio gratuito de una plataforma como Facebook, Google o TikTok, pueden ser positivas para las personas. Sin embargo, muchas veces no se está al tanto de la cantidad de datos personales que se están cediendo por ese servicio. Esto parte de la lógica de que nada es gratis. Esto tiene consecuencias como la manipulación mediática, tal como pasó en las elecciones de E.E.U.U donde resultó ganador Donald Trump. En el mundo actual, el espacio público aumentó y se ha atenuado el concepto de privacidad. (Muñoz, 2018)

misma tecnología. De esta manera, las personas con tecnologías más antiguas serán digitalmente más vulnerables y sus datos pueden terminar recolectándose de manera más sencilla. Otro punto, ya de manera directa con una implicación institucional, es que, como se mencionó con el concepto de *"jurisdiction shopping",* este tipo de vigilancia se puede utilizar como una forma de externalizar el control para evadir regulaciones internas. Por este motivo, sería importante contar con mecanismos de Derecho Internacional u organizaciones enmarcadas en la gobernanza global que puedan tener un cierto nivel de control, por lo menos ético o de responsabilidad, sobre las acciones que se van a realizar sobre las personas del mundo. Actualmente, los mecanismos para crear una regulación ante la vigilancia masiva han sido prácticamente nulos. Uno de los pocos ejemplos se puede encontrar en una nueva normativa dentro de la Unión Europea que indica que la vigilancia masiva solo debe ser utilizada en contextos de emergencia (Forbes, 2021; Rosemain, 2020). A pesar de esto, fuera del contexto europeo, la preocupación de los gobiernos por ejercer un control es nula.

Con este capítulo se cumplió el objetivo de explorar las consecuencias de la tecnosecuritización en el ámbito de gobernanza. Tanto a nivel político como institucional, la tecnosecuritización puede llegar a reflejarse en la manera en la que los Estados regulan la sociedad. Esto, dado que implica una deshumanización al reducir a las personas a enemigos o a datos, y esto puede llevar a una tecnificación de las Relaciones Internacionales donde se tome cada vez menos en cuenta el impacto que puede tener en las personas. Esto podría verse como una suerte de vuelta a las dinámicas estatocéntricas del primer debate de las Relaciones Internacionales. De la misma manera, esto implica un reforzamiento de la relación de poder y dominación que el Estado ejerce. Por lo tanto, el Estado va a tomar un papel cada vez más preponderante dentro de las Relaciones Internacionales[11]. Toda esta problemática está

[11] Es claro que los Estados son el actor central de las Relaciones Internacionales. Sin embargo, con el pasar de los años, más actores han entrado en el Sistema Internacional, lo que ha llevado a nuevas dinámicas de poder. De esta forma, las implicaciones de esta tecnosecuritización están enmarcadas en un retroceso del poder de estos actores nuevos y a un regreso a la preponderancia del poder y dominación del Estado.

enmarcada en como los Estados ponen un enemigo de forma discursiva y aplican medidas emergentes realizadas desde la tecnología, en otras palabras, está enmarcada en la tecnosecuritización.

Capítulo 3: La Tecnosecuritización en la Sociedad

Este capítulo busca explorar cuáles son las consecuencias de la tecnosecuritización dentro de la sociedad. Estas implicaciones estarán articuladas como las implicaciones en los Derechos Humanos y las de control social que puede tener este tipo de securitización. Para demostrar esto se utilizarán distintos casos: la vigilancia en Corea del Sur en el contexto de COVID-19, la vigilancia desde la Big Data en los Estados Unidos, y el caso de China con el control social.

3.1 Implicaciones en los Derechos Humanos

3.1.1 La Privacidad como Derecho Humano

Como se ha visto en los apartados anteriores, la tecnosecuritización puede tener un impacto en distintas áreas. A nivel social, una de las implicaciones más importantes es dentro de los Derechos Humanos, específicamente dentro de la privacidad. Para explicar esto primero se debe definir a la privacidad. De esta manera, según el Diccionario de la Real Academia Española (s.f), la privacidad es aquel "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". Esto implica que las personas deben tener el control o alguna influencia sobre la información o datos que existen sobre ellos (Bélanger y Crossler, 2011, p.1017).

En décadas anteriores, la privacidad no estaba tan en peligro como hoy en día. El desarrollo de tecnologías que se alimentan de la información y la gran conectividad a la que conlleva el internet implican un desvanecimiento de la privacidad (Barbudo, 2019, p. 141). Bajo esta problemática, es importante reconocer que, según la definición dada en el párrafo anterior, la privacidad implica una autonomía personal o una autodeterminación informativa. Es decir, tener la capacidad de elegir sobre la información que se tiene sobre si mismo. Esto, dado que muchas veces se confunde a la privacidad con intimidad o secretismo (De

Terwangne, 2012, p.54). Esta diferenciación es importante porque una de las principales críticas que se hace ante un llamado al respeto de la privacidad en internet es que las personas "no tienen nada que esconder" o que "al no ser criminales, la información no va a conllevar a ningún peligro", y en última instancia, este tipo de afirmaciones son falsas. Por más de que la información que una persona posea no sea ilegal, esta revela muchas cosas de la conducta y vida de la persona que pueden ser perjudiciales para la misma.

Dichas críticas, mencionadas anteriormente, son parte de un problema grave actual que es importante mencionar. La privacidad, así como otros conceptos tales como la presunción de inocencia o la libertad de expresión, tienen una mala reputación al considerárseles anticuadas y antiprogresistas (Cohen, 2012, p.1904). Esto es porque sus raíces están ligadas a la tradición del individualismo liberal (Cohen, 2012, p.1906). A pesar de esto, es importante romper con ese estigma pues el mundo real no tiene que ver con las islas autónomas donde solo está el individuo de las que se basa el individualismo (Cohen, 2012, p.1906). El mundo actual es uno interconectado donde incluso la afectación a la privacidad de una persona puede llevar a una afectación de todas las personas. Esto dado que, en primera instancia, permitir esta clase de intromisiones implica legitimar esta problemática y que se use contra otros, y, en segunda instancia, estas informaciones individuales pueden servir para crear modelos de comportamientos social que pueden llevar a un control de las personas, como se explicará más adelante. De esta forma, se debe tener en claro que una sociedad democrática no puede ser viable sin que sus ciudadanos tengan la capacidad de autogobernarse (Cohen, 2012, p.1905)

Con todo esto claro, se puede pasar al entendimiento de la privacidad como Derecho Humano. Y es que la misma está reconocida en el Art. 12 de la Declaración Universal de los Derechos Humanos como "*Nadie será objeto de injerencias arbitrarias en su vida privada*, su familia, su domicilio (…). Toda persona tiene derecho a la protección de la ley contra tales

injerencias o ataques" (Asamblea General ONU, 1948; las cursivas son de este trabajo). Hoy en día esta injerencia ante la vida privada es mucho más clara, dado que, con fenómenos como el internet de las cosas, el *cloud computing*, o el *Big Data*, han llevado a una revolución donde la información ha cobrado un rol significativo (Gil, 2016, p.15). Con estas tecnologías, hoy en día se crean más datos que nunca y el proceso para su recolección y almacenamiento es cada vez más sencillo (Gil, 2016, p.15).

Esta facilidad que se da gracias a la tecnología implica un peligro ya que puede llevar a una injerencia indiscriminada a la privacidad de las personas. Las empresas buscan más formas de vender sus productos y, dentro de los Estados, el temor al delito se erige como uno de los principales problemas ante los cuales la información parece dar una prevención (Malamud, 2018, p.1). Como se explicó en apartados anteriores, el Estado emplea herramientas como el posicionamiento global de una persona, cámaras con reconocimiento facial, drones, y muchos empleados encargados de las bases de datos que implican toda esta información recolectada y que es usada para moldear las políticas públicas (Malamud, 2018, p.1; Milanovic, 2015, p.81). Esta utilización por parte del Estado incrementa la clásica dicotomía entre seguridad y libertad, configurándose en este momento como seguridad versus privacidad, donde ante esta tensión existe un desbalance de poder entre quienes vigilan y quienes son objeto de esta vigilancia (Malamud, 2018, p.1)

Hoy en día, en la era de la información, existe una saturación de la información. No existen medios para prevenir la fuga de la información propia o para la recepción de informaciones falsas, tales como filtros en redes sociales, noticias falsas, o tecnologías como el *DeepFake*[12] (Larsson, Guilhem, Bustamante, Lara, Putallaz, y del Carpio, 2022, p.453). De

[12] El DeepFake puede entenderse como una serie de tecnologías que, valiéndose del machine learning y la inteligencia artificial, crean videos donde se imita a una persona. Uno de los videos más famosos sobre DeepFake muestra a Obama dando un discurso donde expresa los peligros del DeepFake. Este video, surgido en 2018, causó una gran polémica pues, a pesar de decir explícitamente que no era Obama, era muy difícil distinguir la realidad de la ficción. Actualmente se han hecho mucho más comunes y es muy común ver videos

esta forma, es necesario que dentro de los países exista una mayor regulación sobre el uso de la información o, por lo menos, un reconocimiento o llamado desde la gobernanza global a un manejo de información que es responsabilidad de todos. La violación a la privacidad puede darse desde una persona que comparte información o contenido confidencial que le fue suministrado de forma exclusiva por otra persona, hasta las acciones de empresas o Estados que se comentan en el presente trabajo.

3.1.2 Vigilancia Desde el Reconocimiento Facial en Corea del Sur

3.1.2.1 Caso

Dentro del contexto de la privacidad como Derecho Humano existen diversos ejemplos que pueden ayudar a comprender como es que hoy en día se está violando desde procesos de tecnosecuritización. El primero de los ejemplos que se expondrá será el de Corea del Sur durante la pandemia producto del COVID-19 que inició a principios del año 2020.

Dentro de Corea, el primer caso de COVID-19 fue reportado el 20 de enero de 2020 y tras ello empezó un descontrol del nivel de contagiados, tal como se pudo presenciar en gran parte del mundo (Park y Lim, 2020, p.14). Sin embargo, el caso de Corea fue especial, dado que desde 2015 este país tiene un marco legal para la supervisión tecnológica de enfermedades, derivado de los distintos casos históricos del Síndrome Respiratorio del Medio Oriente (MERS, por sus siglas en inglés). La infraestructura tecnológica autorizada para monitorear esos casos llevó a un control mucho más agresivo para buscar frenar la pandemia (Park y Lim, 2020, p.14; Inn, 2020)

Dentro de los controles establecidos dentro de Corea estaban: rastreo por GPS para un aseguramiento de las medidas de cuarentena, rastreo de contactos automatizado, divulgación pública de las rutas de casos confirmados, etc. (Park y Lim, 2020, pp.14-17). A pesar de que

---

con estas tecnologías en redes como TikTok o Instagram haciéndose pasar por celebridades (Hancock y Bailenson, 2021)

una respuesta pronta a la pandemia era necesaria para salvaguardar la vida de las personas, la implementación de este tipo de tecnologías plantea cuestionamientos alrededor de la privacidad que deben ser observados para prevenir acciones negativas en un futuro cercano.

Según Park y Lim (2020), los cuestionamientos sobre trasfondos autoritarios son falsos pues Corea ha demostrado un gran apego al Estado de Derecho y a la protección de datos y privacidad dentro de su legislación (p.18). Sin embargo, el problema es la normalización que se puede hacer sobre este estado de emergencia extrema que percibe el Estado. Muestra de esto es que en 2022 se ha extendido el uso de reconocimiento facial como forma de monitoreo y rastreo de casos, por lo que puede darse el caso de un uso indebido e invasivo si es que no tiene los límites debidos (Feeney, 2022). El monitoreo en muchas ciudades ha sido masivo, pero ha tenido limitaciones como el hecho de que las personas porten su mascarilla, lo cual limita su identificación por parte de las cámaras. Esto, más que ser un beneficio ante la invasión a la privacidad, plantea un problema pues para cumplir con el objetivo del monitoreo las autoridades deben tener una mayor cantidad de datos y fotos que permitan identificar a las personas de forma eficiente, cosa que se está realizando (Young, 2021; Najah, 2020; Ramos 2020).

3.1.2.2 Actor Securitizador

Dentro de este caso el actor securitizador el gobierno coreano. Es este quien mediante el discurso de la prevención ante el COVID-19 implementó las medidas de vigilancia. Esta vigilancia se dio mediante dispositivos de rastreo, reconocimiento y monitoreo, por lo que pueden enmarcarse en la tecnosecuritización. Un punto interesante dentro de este caso es que el discurso de prevención y, por ende, el despliegue de la tecnología es legitimado dentro de la población por ser algo anterior. Es decir, desde 2015 se tenía un marco legal para enfrentar situaciones similares, por lo que el contexto de ser un país pequeño con una densidad poblacional alta pudo llevar a la facilidad de la aceptación de este discurso

3.1.2.3 Amenaza

En principio la amenaza parece obvia, la cual sería el virus del COVID-19. Sin embargo, si se va un poco más allá, se puede observar que en si la amenaza no es el virus, sino las personas que son portadoras de este virus. Por ese motivo es que existe una restricción de movilidad y una vigilancia masiva para evitar que se reproduzca el virus con el contacto con personas no contagiadas.

Tras vivir una pandemia de la escala de la ocurrida en 2020, esta amenaza parece legítima para plantear un accionar desde la securitización. Sin embargo, si no existe una correcta regulación de ese control puede ser la base para acciones en contra de la libertad en el futuro. Dentro de esto hay que tener en cuenta que en Corea la tecnosecuritización en casos de emergencia sanitaria se encuentra en el marco legal, pero, en última instancia, el declarar algo como emergencia sanitaria no siempre responde a la opinión de la comunidad científica, lo que puede dar paso a distintos tipos de discursos que lleven a la implementación de estas acciones.

3.1.2.4 Objeto Referente

La sociedad se ve en una amenaza existencial dentro de este caso. La escalada de contagios y la cantidad de muertes se planteó como un peligro inminente que no se tenía la certeza de como manejar. Ante ese escenario se planteó la tecnosecuritización.

3.1.2.5 Análisis e Implicaciones

Con los puntos anteriormente expuestos se demuestra la existencia de una tecnosecuritización dentro del caso coreano. Dado el contexto emergente de la pandemia por el COVID-19 y por la especificidad del marco legal coreano, el gobierno se configura como un actor con la legitimidad suficiente para imponer una narrativa de protección total. El tema de la necesidad real de poner estas medidas no es menester de este trabajo, sin embargo, queda claro que

estas medidas implican una limitación dentro de los Derechos Humanos, especialmente al de privacidad.

Ante este último punto, generalmente se explica que en contextos de emergencia los Estados están justificados a limitar ciertos derechos, de ahí el surgimiento de los Estados de Excepción. Sin embargo, estos deben estar muy bien delimitados para evitar el abuso de esas limitaciones en contra de los ciudadanos. Al parecer, a inicios de pandemia, dentro del caso de Corea no hubo este tipo de abusos. Sin embargo, ya en 2022 se ve como se continua con una ampliación de la vigilancia, lo que puede tener efectos negativos a largo plazo.

Las consecuencias de las medidas de securitización empleadas durante la pandemia por el COVID-19 pueden resultar bastante peligrosas para las Relaciones Internacionales contemporáneas. Como se había visto en apartados anteriores, se está entrando a una era donde el Estado tiene la capacidad de inmiscuirse en las esferas íntimas de las personas. Bajo el justificante de la salud, esto puede incrementarse y mantenerse en el tiempo. Hoy en día, en el 2022, se está viendo una reducción en muchas regulaciones, como el uso de las mascarillas. Sin embargo, las regulaciones de movilidad siguen presentes y pueden ser funcionales a intereses políticos de los Estados.

3.1.3 La Seguridad Desde la Big Data en los Estados Unidos

3.1.3.1 Caso

Otro de los casos en relación con violaciones de privacidad, y que tal vez es mucho más conocido, es la forma en la que se utiliza la *Big Data* como herramienta de seguridad dentro de los Estados Unidos. Sin embargo, para entender esto de mejor manera hay que definir a la Big Data. Las tecnologías de Big Data describen a una nueva generación de herramientas que están diseñadas para extraer valor de largos volúmenes de una amplia variedad de análisis a alta velocidad para su posterior análisis (Matturdi, Zhou, Li, Lin, 2014, p.135; Quasim y Meraj, 2017, p.408). Actualmente, dentro de la era de la información, la cantidad total de

datos que se han generado desde el año 2005 hasta la actualidad excede la cantidad de información que se generó durante los anteriores siglos de existencia humana (Matturdi et al., 2014, p. 135). De esta forma se entiende la necesidad de crear herramientas que permitan dar un entendimiento a esta cantidad de información.

A pesar de lo expuesto anteriormente, el problema que se presenta actualmente no es de la información en sí, sino de las intenciones que se tienen para su recolección, que es lo que puede generar riesgos a la seguridad y a la privacidad. De esta forma, cada metadato va alimentando a estas tecnologías que aprenden de la vida de las personas o las terminan controlando. Por ejemplo, el motor de Google aprende los hábitos de búsqueda de las personas y, por su parte, Facebook captura hábitos, preferencias y gustos de las personas y sus contactos. De la misma forma, las operadoras telefónicas saben con quien se está hablando y, además, quien está cerca (Matturdi et al., 2014, p.135).

Dentro de las implicaciones que puede tener el uso de la *Big Data*, más allá de el abuso a los derechos de los individuos bajo vigilancia, va encaminado a lo que se explicó anteriormente como la "gobernanza algorítmica" o, en otras palabras, la gobernanza de la *Big Data*, ya que se vale de estos datos para enmarcar sus acciones. De esta manera, los problemas pueden verse en las acciones que ha realizado la NSA con su iniciativa PRISM (Park y Wang, 2013, p.516; Crampton, 2015, p.519). De la misma manera, existen otros problemas o desafíos para esta tecnología, tales como la seguridad ante filtraciones de datos, las vulneraciones de bases de datos, y el intercambio de datos a terceros actores (Schmitt, Shoffner, Owen, Wang, y Lamm, 2013, p.2).

Ya de forma más específica, el caso de los Estados Unidos se evidenció con las filtraciones realizadas por Edward Snowden, quien fue trabajador de la Agencia de Seguridad Nacional de los Estados Unidos (NSA, por sus siglas en inglés). Dentro de sus filtraciones se evidenció como los Estados y, en especial los Estados Unidos, tienen una orientación hacia la

explotación de nuevas formas de vigilancia de datos masiva y de cibervigilancia. Esto con un objetivo de recolectar la mayor cantidad posible de datos para mantener la seguridad (Hu, 2014, p.775-780). Dentro de este contexto, el primer caso conocido de la vigilancia mediante el uso de la Big Data fue el de la NSA requiriendo a la empresa de telecomunicaciones Verizon la entrega de la metadata de millones de llamadas telefónicas de los ciudadanos norteamericanos. En este caso, Verizon tenía prohibido divulgar esta información al público o de pedir permiso a los consumidores (Lyon, 2014, p.2; MacAskill, 2013). En las subsiguientes filtraciones de Snowden a los medios de comunicación también se vio como el programa PRISM daba a la NSA un acceso directo a los servidores de compañías como Apple, Facebook, Google, Microsoft o Yahoo (Lyon, 2014, p2). Esta supervisión mediante la Big Data fue reconocida por el presidente norteamericano Barack Obama el 17 de enero de 2014, cuando pidió una revisión compresiva de la privacidad y el Big Data luego de las filtraciones de Snowden (Lyon, 2014, p.4)

Tras estas filtraciones, se vivió un intenso debate sobre las implicaciones de este tipo de vigilancia. Para ese entonces Obama canceló un viaje a Moscú por la protección de Rusia a Snowden. El gobierno de Brasil canceló actos en Washington en protesta hacia los Estados Unidos. El avión presidencial de Bolivia, con Evo Morales a bordo fue forzado a aterrizar en Viena bajo la sospecha de que transportaba a Snowden. Y, el caso más directo, Ángela Merkel acusó a los Estados Unidos de espiarla, ante lo que los Estados Unidos respondieron que son acciones que no volverán a ocurrir (MacAskill, 2013; BBC News, 2014).

Ante la gran expansión del uso de la *Big Data* para la vigilancia, la NSA argumenta que, si toda esta infraestructura hubiese existido antes del 9/11, lo más probable es que se hubiesen detenido a los atacantes (MacAskill, 2013). Y, precisamente este punto, es una de las bases de la vigilancia actual: el medio al terrorismo pos-9/11. Bajo esta premisa, la NSA quebranta las leyes nacionales e internacionales cientos de veces cada año. Por ese motivo es

que se han dado casos como el de 2008, cuando un gran número de llamadas dentro de Washington fueron interceptadas por un error del sistema, donde se colocó “202” (código de área de Washington), en lugar de “20” (código telefónico de Egipto). (BBC News, 2014; BBC News, 2020).

En años recientes se ha realizado juicios para dar paso a la responsabilidad de la NSA ante la vigilancia masiva a la que ha estado sometiendo al mundo (BBC News, 2022; PoKempner, 2020; Satter, 2020). Sin embargo, el gobierno no ha cesado esta vigilancia, pues ahora agencias como la CIA se atienen a una Orden Ejecutiva (la 12333) que data de la era de Ronald Reagan, donde se ordenaba la expansión de las capacidades de recolección de datos de los Estados Unidos para poder hacer frente de manera eficiente a las amenazas extranjeras (Meyer, 2022; Beens, 2021; McCray, 2021).

Dentro de este contexto, es preocupante la violación a este Derecho Humano, ya que se hace de forma indiscriminada y solo con una justificación discursiva. De esta forma, los Estados Unidos están infringiendo los derechos de privacidad en 193 países (Amnistía Internacional, 2015). Esto puede llegar a ser más preocupante con las declaraciones del propio Snowden

> “Tenemos agencias mirando a través de las cámaras web dentro de las habitaciones de las personas, ellos están recolectando millones de locaciones de los teléfonos celulares cada día. Ellos saben a dónde tomas el bus, dónde vas a trabajar, dónde duermes y que otros teléfonos duermen contigo” (Amnistía Internacional, 2015).

De esta forma, se entiende por qué la seguridad no tiene que darse a expensas de la privacidad, ya que esto implica una transformación de las personas en simples datos (Amnistía Internacional, 2015). Mientras las agencias de seguridad están buscando criminales, las personas que están siendo supervisadas siguen teniendo el derecho a la presunción de inocencia y a la privacidad (Amnistía Internacional, 2015).

Cabe destacar que todo este problema de la vigilancia trasciende las divisiones políticas. Otra de las principales bases para la vigilancia dentro de los Estados Unidos es parte del Acta de Vigilancia de la Inteligencia Extranjera de 1978. Esta ley permitía a la NSA espiar a personas que no fueran estadounidenses fuera de los Estados Unidos. Esto se modificó para dar paso a una vigilancia total. Este cambio ha sido reautorizado bajo el gobierno de Bush en 2008, de Obama en 2012, y de Trump en 2018 (Schneider, 2018). Se espera que Biden haga lo mismo, ya que todo esto está enmarcado a la amenaza existencial que representa el terrorismo dentro de la población (Shahshahani y Gupta, 2021).

3.1.3.2 Actor Securitizador

Dentro de este caso el actor securitizador es el gobierno de los Estados Unidos. Este impone la narrativa sobre una amenaza existencial, que en este caso es el terrorismo, e implementa las acciones necesarias para hacer frente al mismo. Sin embargo, al igual que pasaba con el caso de la alianza de los "5 ojos", no existe una claridad en como el discurso se termina legitimando. Si bien es cierto que tras el 9/11 el discurso en contra del terrorismo se instaló en el imaginario colectivo, las personas realmente no dieron paso a la legitimidad de las acciones pues estas se hacían de manera secreta. No es sino hasta las filtraciones de Snowden que se empiezan a conocer las acciones reales del gobierno de los Estados Unidos.

3.1.3.3 Amenaza

La amenaza existencial, como se expuso anteriormente, es el terrorismo. Dentro de la lucha contra el terrorismo se ha justificado el realizar todo tipo de acciones para salvaguardar el "bienestar" estadounidense. Esto se puede ver desde las guerras en el Medio Oriente hasta la supervisión de su propia población para evitar cualquier atentado. Al ser percibida esta amenaza existencial, se termina justificando cualquier acción para prevenir sus consecuencias.

3.1.3.4 Objeto Referente

En primera instancia se puede pensar del Estado y la sociedad como objetos referentes. Dado que estos son los que estarían bajo una amenaza vital y, de existir un atentado, serían los más afectados. Sin embargo, también entran en juego los valores occidentales y democráticos, que en gran medida están moldeados por la ideología liberal norteamericana. De esta forma, la prevención ante el terrorismo está enmarcada en una defensa a Occidente de las problemáticas generadas por el "otro".

3.1.3.5 Análisis e Implicaciones

Con los puntos anteriormente mencionados se demuestra la existencia, parcialmente, de una tecnosecuritización en el caso de los Estados Unidos. A pesar de esto, continúa la limitación sobre el discurso. De esta forma, existen rasgos de la securitización sin uno de sus elementos claves. A pesar de esto, las implicaciones de este tipo de control son bastante graves pues demuestran una intromisión del Estado en las esferas privadas con el justificante de una amenaza existencial. En este caso se puede ver como el gobierno viola deliberadamente los derechos humanos de todas las personas, incluyendo mandatarios extranjeros. Esto, a largo plazo, puede tener un impacto fundamental dentro de las Relaciones Internacionales pues se deben plantear acciones para evitar este tipo de situaciones. Ya no solo por el bien de las personas, sino por la estabilidad de cada uno de los países del mundo.

A nivel normativo, como forma de prevención ante la violación de Derechos Humanos, tal como se había expuesto anteriormente, no hay un gran avance. Además de las nuevas normas puestas por la Unión Europea sobre la limitación para la vigilancia masiva, se puede encontrar un pronunciamiento del Alto Comisionado para los Derechos Humanos de las Naciones Unidas (2014), donde se expone que existen grandes vulneraciones a los derechos de forma arbitraria e injusta, por lo que es necesario atenerse a los principios universales de los Derechos Humanos. A pesar de eso, como se vio en los casos presentados

anteriormente, los Estados han hecho caso omiso a estas recomendaciones. Es complicado terminar obligando a los Estados a cumplir con regulaciones de este estilo, sin embargo, es necesario crear iniciativas para cambios normativos que den un inicio para la solución de estas problemáticas.

Finalmente, cabe destacar que gran parte de la vulneración a los derechos de las personas dentro de la tecnosecuritización, no se da necesariamente sobre el individuo en si, sino que se le vulnera como agregado. Es decir, es un proceso sistemático en masa que termina con la violación de los derechos de un conjunto. Esto se puede ver con el caso presentado sobre la recolección de datos por parte del gobierno con Verizon o con casos como el de Cambridge Analytica, donde se utilizaron los datos de las personas para terminar incidiendo en, entre otros temas, las elecciones de los Estados Unidos (BBC News Mundo, 2018).

3.2 Implicaciones en el Control Social

3.2.1 Evolución del Control Social de los Estados

Otra de las implicaciones de la tecnosecuritización está enmarcada dentro del control social. Para entender esta implicación es importante dar cuenta de como se ha ido desarrollando el control social dentro de los Estados. Con esto en cuenta, se puede decir que todas las sociedades han desarrollado mecanismos que permiten el control social. Estos mecanismos se utilizan para evitar la anomia y el desorden dentro de la sociedad (Barraycoa, 2017, p87). Estas formas de control pueden ser externas, lo que implica normas a seguir por parte de los individuos, y también internas, lo que da paso a la legitimidad y aceptación de estas herramientas (Barraycoa, 2017, p87). La dualidad externo/interno también puede ser entendido dentro de los paradigmas sociales, el externo está ligado a la teoría hobbesiana y al funcionalismo, el interno está ligado a la teoría weberiana y se centra en la creación de sentido para las acciones realizadas (Barraycoa, 2017, p.88; Rossi, 2018, p.1).

Dentro de estos mecanismos se debe entender al Estado de una forma particular. En principio no es un actor que permanece igual toda su historia, sino que debe entenderse como un proceso de constante definición mediante distintos hechos históricos, políticos y sociales (Salvi, 2019, p.9). De esta manera, el Estado se va trasformando a lo largo de la historia y sus modos de control y de ejercicio del poder van variando. Así mismo, la sociedad va cambiando y existen hechos, como la tecnologización del siglo XXI o las crisis como la del COVID-19, que cambian las formas de imaginar y vivir el mundo (Sagot, 2020, p107). Por este motivo, la evolución de estas formas de control será constante.

Teniendo lo anteriormente mencionado en cuenta, uno de los principales pensadores sobre el control social fue Foucault. Él mencionaba que estas formas de control fueron evolucionando hasta tener un punto importante entre los siglos XVII y XX con las sociedades disciplinarias. Estas sociedades tenían como núcleo el control en grandes centros de encierro, como la familia, la escuela, el cuartel, la fábrica, el hospital o la cárcel (Deleuze, 2006, p.1). Todos estos espacios moldean el comportamiento de las personas, tanto a nivel externo mediante la implantación de reglas, como a nivel interno, normalizando las situaciones del día a día.

Sin embargo, estos centros de encierro presentan una crisis y, por ese motivo, el mundo busca su reforma. Esta crisis se da porque la sociedad está evolucionando y la disciplina en centros cerrados no funciona en un mundo que al parecer es cada vez más abierto. Bajo ese contexto surgen las sociedades de control (Deleuze, 2006, p2). Una de las principales diferencias entre estos dos tipos de sociedades, más allá de la apertura, es que en las sociedades disciplinarias siempre se tenía que empezar de nuevo, por ejemplo, luego de la escuela se va al cuartel, y luego a la fábrica. En contraposición, en las sociedades de control nunca se termina nada, la empresa, la formación y los servicios son constantes (Deleuze, 2006, p.3). Además de esto, dentro de las sociedades de control lo esencial ya no es el

individuo como tal, sino la cifra. Existen cifras que marcan o prohíben el acceso a determinada información o espacio (Deleuze, 2006, p.3)

Todo esto no implica una desaparición total de los elementos disciplinarios dentro de la sociedad. La disciplina se ha difuminado dentro de las prácticas comunes y cotidianas, y se da por medio de redes flexibles y fluctuantes (Araya, 2012, p.20). De esta manera, las sociedades de control dan una mayor "libertad" al individuo ya que el control está interiorizado en las prácticas cotidianas. Esto implica que dentro de estas nuevas formas de sociedad la vigilancia no necesita de una institución, sino que se ejerce mediante las tecnologías electrónicas (Han, 2014, pp. 20-21; Rodríguez, 2008, p.2). Dentro de estas sociedades, ya no existe el panóptico de Foucault dentro de un espacio determinado, sino que la vigilancia se da desde la información (Rodríguez, 2008, p.2). Las sociedades de control van de la mano con algo mucho más similar a la imagen del *Big Brother* dentro de la novela 1984 de George Orwell, con el lema "*Big Brother is watching you*", ya que esto denota una vigilancia genérica donde no hay limites para la visibilidad (Rodríguez, 2008, p.2).

Estas prácticas de vigilancia están creciendo especialmente en los países del norte global (Lyon, 2010, p.107). Sin embargo, esto no implica que estas tecnologías y prácticas no se vayan diseminando por el mundo. De esta manera, mediante el avance tecnológico, se está entrando a unas sociedades de vigilancia donde cada vez es más difícil seguir, analizar o regular esta vigilancia. Esto es lo que ha llevado a que se proclame el problema del "fin de la privacidad" (Lyon, 2010, p.107). Estos nuevos modelos se han incrementado desde los ataques terroristas del 9/11 y la subsecuente declaración de la Guerra contra el Terrorismo (Whitaker, 2003, p.1).

Siguiendo el orden de ideas presentado, "la libertad y la comunicación ilimitadas se convierten en control y vigilancia totales" (Han, 2014, p.20). Esto implica que las sociedades de control no limitan la comunicación entre los vigilados, sino que buscan que estos se

comuniquen intensamente. Se busca que voluntariamente se de la información. Por este motivo, el *Big Brother digital* traspasa el poder a los reclusos, convirtiendo esta forma de sociedad en una mucho más eficiente que la disciplinaria (Han, 2014, p.21)

Este tipo de sociedad también implica una evolución del concepto de biopoder de Foucault. A pesar de que hay rasgos de este mediante el control de los cuerpos, como se mencionó anteriormente, en la actualidad se está dando paso a una psicopolítica digital. Esto implica, más allá del control de los cuerpos, la intervención en la psique de las personas para condicionarlas a un nivel prerreflexivo (Han, 2014, p.25). Y para todo esto, la herramienta por excelencia es la Big Data, ya que esta es la que permite hacer pronósticos sobre el comportamiento humano, haciendo el futuro predecible y controlable (Han, 2014, p.25). De esta manera, el papel de la información es clave para dar paso a una reducción de la incertidumbre dentro del mundo (Matterlart y Vitalis, 2015, p.131).

Con todo esto en mente, se puede entender que hoy, dentro de las sociedades del control, se vive con una vigilancia líquida, de acuerdo con lo expuesto por Bauman y Lyon (2013). De esta forma, la vigilancia se puede configurar desde cualquier dispositivo y la única intención es la recolección de datos. Por este motivo, la seguridad hoy en día está ligada totalmente a la reducción de esa incertidumbre en el mundo a forma de negocio (Bauman y Lyon, 2013, p.13).

3.2.1 Control Social Tecnológico en China

3.2.2.1 Caso

Dentro del control social a nivel tecnológico que se presenta en China hay distintas perspectivas. Dentro de este apartado se presenta una de las que puede ser considerada más "leve" en términos de violaciones de derechos, como lo es el Sistema de Crédito Social, hasta uno de los casos de control más graves dentro del mundo contemporáneo, como es la vigilancia a la población de etnia uigur.

3.2.2.1.1 Sistema de Crédito Social en China

Para comenzar se expondrá el caso del Sistema de Crédito Social. Para esto es importante primero entender qué es. En principio es un sistema de monitoreo y análisis de reputación. Esto dado que el gobierno chino había identificado una serie de problemas dentro de la sociedad que debían solucionarse, tales como fraudes en mercados, dificultades para hacer cumplir condenas judiciales, corrupción dentro del gobierno, malas prácticas profesionales e, incluso, plagio académico (Dai, 2018, p.1). De esta forma, el gobierno chino busca hacer uso de la Big Data para crear una sociedad donde los individuos, las empresas y el gobierno actúen todos con integridad para alcanzar una estabilidad económica y social (Shen, 2019, p.21).

Existen dos documentos regulatorios que definen a este sistema. El primero data del 2007 y se titula "Opiniones de la Oficina General del Consejo de Estado sobre la Construcción de un Sistema de Crédito Social". En este documento trata sobre la necesidad de crear un sistema que permita el mantenimiento de la "economía socialista de mercado", ya que existían problemas como el fraude, la evasión fiscal o la piratería de productos (Shen, 2019, p.22; Chorzempa, Triolo y Sacks, 2018, p.3). Más adelante, en 2014, se tiene el documento titulado "Nota del Consejo de Estado relativo a la expedición del Esquema de Planificación para la Construcción de un Sistema de Crédito Social (2014-2020). Este segundo documento abarca áreas más allá de lo económico y busca solucionar la falta de confianza que se da en todos los niveles de la sociedad china. Por ese motivo, se planeaba la creación de una "sociedad de reputación" (Chong, 2019; Shen, 2019, p.22).

Con lo expuesto anteriormente hay que tener una cosa en claro. La búsqueda de la reputación a nivel social puede parecer un objetivo totalmente frívolo a ojos de las sociedades occidentales. Sin embargo, todo esto se basa bajo el "Xin" (信), que puede ser entendido como crédito, reputación o confianza, y es uno de los conceptos fundamentales dentro del

pensamiento del confucianismo. (Shen, 2019, p.24). Dado que la sociedad está inmersa en comportamientos deshonestos, se crea este sistema para curar los problemas y la falta de confianza (Langer, 2020, p.1; Shen, 2019, p.24). A pesar de esto, los resultados del plan pueden plantear un reforzamiento del autoritarismo.

Teniendo en cuenta el funcionamiento, se puede entender como esto implica la construcción de un ranking moral sobre la sociedad. El no cumplimento del estándar de "buen ciudadano" dado por el gobierno puede llevar a distintas penas. Los comportamientos negativos pueden enmarcarse en cosas como la mala conducción, fumar en zonas para no fumadores, comprar demasiados videojuegos, y postear noticias falsas (Canales, 2018). El sistema asigna de partida 1.000 puntos y, por ejemplo, una multa de tráfico puede hacer perder 5 puntos. Ganar un reconocimiento de la ciudad por un acto heroico puede dar 30 puntos. De esta manera, los ciudadanos van oscilando entre un ranking "A+++" y el "D". Entre más alto en el ranking, más beneficios y reconocimiento social se tendrá. Entre más bajo, más restricciones y un mayor *public shaming* (Mistreanu, 2019).

3.2.2.1.2 Vigilancia a la población Uigur

El otro de los casos dentro del control social dentro de China es el de la vigilancia hacia la población uigur. Para esto, primero hay que entender el contexto histórico. La etnia predominante en China es la Han y, dentro de la región de Xinjiang en el noreste de China se puede encontrar a la etnia Uigur, la cual tiene raíces turcas. China ha tenido una larga historia tratando con la región de Xinjiang desde una perspectiva de seguridad. China mantiene que su gobierno ha tenido el control de la zona desde hace más de 2.000 años con los asentamientos militares en las colonias de las regiones occidentales por parte de la dinastía Han. Sin embargo, su control efectivo en la zona ha sido intermitente. Dentro de esta intermitencia, China ha visto a la región como una amenaza existencial dadas las influencias externas que poseía esta región (Trédaniel y Lee, 2018, pp-2-8). Desde la dinastía Qing hasta

los gobiernos comunistas han compartido posiciones similares en relación con la seguridad nacional que se tiene que establecer frente a Xinjiang. Sin embargo, desde 1949, se ha buscado una unidad nacional mucho más sólida, lo que implica la búsqueda de un mayor control sobre la zona para evitar cualquier intento de secesión (Trédaniel y Lee, 2018, pp. 8-9). Bajo ese contexto, han surgido distintos movimientos nacionalistas uigures que buscan reivindicar su propia identidad, pero esto ha sido reprimido por el gobierno.

Teniendo en cuenta el contexto histórico, el problema actual se remonta al año 2014, cuando empiezan los proyectos de internamiento masivo para la reeducación. Esto coincide con un repunte de atentados, según el gobierno chino, ocurridos por parte de nacionalistas uigures en 2012 y 2013. Por ese motivo, empiezan las prohibiciones más fuertes, como la prohibición del ayuno a las comunidades musulmanas y, en el mismo periodo, empieza la vigilancia masiva (Leibold, 2020, p.2; Smith Finley, 2019, p.3). Desde el año 2015 se clasifica a las personas en función de su "confianza", esto es basado en indicadores como la edad, si es o no parte de la étnica uigur, si es desempleado, si tiene conocimiento religioso o reza cinco veces al día, si posee pasaporte, si ha visitado uno de los 26 países "sensibles" (países musulmanes), si tiene familiares en países extranjeros, o si educa a sus hijos en casa. Un bajo indicador de confianza puede conllevar al internamiento en los campos de reeducación (Smith Finley, 2019, pp. 3-4). Además de las medidas de vigilancia tecnológica, otra de las formas para supervisar a las personas de la etnia uigur es mediante el incentivo a que sus familiares de la etnia Han los visiten y reporten cualquier anormalidad, o mediante el cuestionamiento a los niños sobre si es que sus padres y familiares están inmersos en actividades religiosas (Smith Finley, 2019, p.4)

Actualmente se estima que más de un millón de personas han sido detenidas en el sistema de reeducación dentro de la provincia de Xinjiang. Mientras estas personas están detenidas, el resto de las personas son controladas mediante sistemas de vigilancia, puntos de

chequeo, y fuerzas policiacas formales e informales (Kam y Clarke, 2021, p.625). El gobierno chino justifica el accionar en esta zona como una forma de bajar el extremismo y la radicalización de los uigures (Kam y Clarke, 2021, p.625; Güngör, 2020, p.80).

Briglia (2021) presenta una ejemplificación bastante clara sobre como luce un día bajo el régimen de vigilancia dentro de la provincia de Xinjiang:

> Imagina que eres uno de los once millones de uigures viviendo al noreste de China. Es viernes, el día de rezo congregacional dentro del islam, pero optas por no ir a la mezquita porque no quieres atraer la atención. Necesitas hacer las compras y tu esposo te pregunta si puedes ponerle gasolina al carro familiar mientras estas afuera. Normalmente el lo haría, pero la policía lo ha llamado a participar en un "chequeo gratis de salud" requerido por el gobierno y tiene cita hoy. Mientras estas cerca de la estación de gasolina, te encuentras con uno de los 10.000 puestos de control dentro de Urumqi, la capital de la provincia de Xinjiang. Sacas tu identificación nacional, que fuiste bastante cuidadosa de no olvidar, mientras ves a varios individuos de la etnia Han que te llaman. El oficial confirma que tu cara coincide con tu identificación y te pide tu teléfono desbloqueado. Tu fuiste también cuidadosa de traer el teléfono, ya que escuchaste que el vecino fue detenido por no tener el teléfono el mes pasado. Después de que el oficial revisó los mensajes de tu WeChat, las llamadas recientes y las fotografías, te hacen pasar el puesto de control.
>
> Al momento de entrar a la estación de servicio, un sistema vincula las placas con el registro oficial y verifica que tu seas la dueña, pero este está registrado a nombre de tu esposo. Tu identificación vuelve a ser escaneada luego de pagar por la gasolina. Unos minutos después, se te aproxima un oficial de policía para cuestionarte sobre por qué estas comprando gasolina para ese carro y dónde está tu esposo. Con tus acciones creaste una alerta en la aplicación que la policía utiliza para rastrear cada

> detalle intimo de ti y de tu familia, dado que, de acuerdo con el gobierno, comprar gasolina para un carro que está registrado con otro dueño es un comportamiento sospechoso. Eventualmente te liberan.
>
> Llegas a casa y le describes a tu esposo lo que pasó en la gasolinera y él te cuenta como el supuesto "chequeo de salud libre" en la policía conllevo a que le requirieran muestras de sangre y ADN. La policía también escaneó su cara con una variedad de expresiones, como neutra, enojado, riéndose, etc. Luego de eso, la policía le dio un periódico y lo forzó a leerlo en voz alta por tres minutos. Los oficiales no tomaron su ritmo cardiaco, ni su presión o peso. Cuando preguntó por los resultados le dijeron que no tenía derecho a ellos. Incluso en toda esta situación, eres afortunada. No estas en los centros de educación por ahora. (pp.86-88)

Esta ejemplificación da un entendimiento mucho más profundo de la vigilancia masiva que viven las personas dentro de la provincia de Xinjiang. Este tipo de situaciones se saben por las personas que han huido a Turquía o a los Estados Unidos y que cuentan como se les detuvo en estos centros.

Por este accionar, la comunidad internacional ha acusado a China de cometer genocidio y crímenes en contra de la humanidad. Existen muchos reportes de tortura, abortos obligados, esterilización masiva, etc. (Bhuiyan, 2021; Shakir, 2021). Todos estos problemas se han dado en el marco de una tecnologización de la seguridad que implica máquinas de reconocimiento facial y de emociones (Aylward, 2021), redes de video y aplicaciones de vigilancia en manos de la policía. Mucha de la tecnología empleada en estas acciones es hecha por la Corporación de Tecnología y Electrónica China (CETC por sus siglas en inglés). La tecnología abarca un nivel tal que en ciudades como Kashgar, con una población de 720.000, se tienen bases de datos con 68 mil millones de datos de las personas. Para hacer

una comparación, el FBI tiene una base de datos de registro criminal de 19 millones para todo el país (Wakefield, 2021; Buckley y Mozur, 2019)

3.2.2.2 Actor Securitizador

Dentro de este caso el actor securitizador es el gobierno chino. Este no necesariamente goza de la legitimidad para imponer las narrativas a nivel social, pero si tiene la fuerza para implantarlas al ser considerado un gobierno autoritario que sigue las políticas de su partido único. Este caso también choca con la aceptación del discurso que debe tener la audiencia, ya que en este caso no tienen la posibilidad de negarse al discurso.

3.2.2.3 Amenaza

La amenaza puede ser el terrorismo desde el caso de los uigures. Sin embargo, a nivel general, la amenaza es el atentado en contra de los valores sociales chinos, que en este caso se puede ver con la confianza / reputación. Al existir una amenaza contra sus valores, se cree que es una amenaza existencial ante la estabilidad del gobierno y de la sociedad china. De esta forma, para prevenir cualquier problema, se implementan las medidas masivas como el Sistema de Crédito Social o la vigilancia violenta que experimentan los uigures.

3.2.2.4 Objeto Referente

Principalmente son los valores y la integridad nacional. Al ser una sociedad que ha sido históricamente cerrada, esta se ha construido alrededor de una serie de valores que resultan importantes para la estabilidad de los proyectos nacionales. Por ese motivo es que se quiere recuperar la confianza social mediante el ejemplo de los “buenos ciudadanos” que se puede ver en el caso del Sistema de Crédito Social.

3.2.2.5 Análisis e Implicaciones

Este caso plantea un desafío para el análisis y es que no es posible establecer si existe una aceptación del discurso si es que no se puede disentir ese discurso. A pesar de esto, el resto de las características de la tecnosecuritización están presentes. La amenaza existencial a los

valores resulta tan grave que legitima aplicar todas estas medidas drásticas contra su propia población. A pesar de que cada sociedad necesite de un cierto nivel de orden para progresar, el llegar a este nivel resulta perjudicial para los derechos de las personas.

El planteamiento del control social mediante la tecnosecuritización dentro de las Relaciones Internacionales contemporáneas puede ser un factor clave. Como se planteó anteriormente se está viviendo una transición hacia una sociedad del control, donde este aparataje tecnológico va a ser cada vez más común. Como se veía en el caso del Sistema de Crédito Social, existe un cierto nivel de libertad para que la gente actúe, pero el objetivo es el control de la psique. El objetivo es que las personas se comporten de una forma particular que sea de agrado del gobierno. Y esto solo se puede lograr mediante la tecnología y la recolección de datos. Esta claro que el escenario de China puede parecer el más distópico, pero no existen razones para que esto no se siga distribuyendo en el mundo y cada día se haga más común. Con ejemplos como los de Estados Unidos o el Reino Unido se puede ver que es una posibilidad. Aún más, teniendo en cuenta que las sociedades de control se valen de apoyar la generación de información por parte de los usuarios, cosa que se puede ver actualmente con las redes sociales.

Con este capítulo se cumple el objetivo de explorar las consecuencias de la tecnosecuritización en el ámbito social. Tanto a nivel de los Derechos Humanos como del control social, la tecnosecuritización se puede observar en la forma en que la tecnología termina impactando en la vida diaria de las personas. Aquí se sigue con la narrativa de ver a las personas como enemigos, lo que lleva a la necesidad de seguir regulando y controlando por medio de la información. Ante esto, dentro de las Relaciones Internacionales contemporáneas, se puede ver la emergencia de sociedades cada vez más autoritarias que planteen lógicas de control. Por este motivo, hay que plantear formas de prevención que garanticen el bienestar ciudadano.

Conclusiones

La hipótesis planteada en el presente trabajo es que, dados los contantes cambios y avances de la tecnología en el siglo XXI, los procesos de securitización se han complejizado para dar paso a una prevención subjetiva mucho más amplia de los problemas de seguridad. Desde este punto de vista, teniendo en cuenta que no existe un marco jurídico internacional que regule la vigilancia tecnológica, se han creado vulnerabilidades sociales y problemas de gobernanza con los que se tendrán que lidiar en las Relaciones Internacionales contemporáneas.

Teniendo esto en cuenta, se podría establecer que la hipótesis se cumplió de forma total. Para explicar esto de manera más profunda, se pasará a un análisis desde las premisas de esta hipótesis. En primer lugar, los procesos de securitización si se han complejizado dentro del mundo actual. Esto, dado que ya no se está simplemente ante un ejercicio discursivo que se materializa con actos militares, como es el hecho de decir que los migrantes son un peligro existencial y ello conlleva a la justificación de medidas extraordinarias como la militarización de las fronteras, sino que hoy en día conllevan procesos mucho más técnicos y amplios. Estos procesos complejos ya no implican poner a un grupo minoritario dentro de la categoría de amenaza existencial, sino a toda una población o, incluso, a todo el planeta. De esta manera, los procesos de securitización de hoy en día están cruzados por el concepto de las sociedades de control, lo que implica un estado constante de conflicto. Esta nueva forma de pensar la securitización lleva a unos problemas diferentes dentro de las Relaciones Internacionales contemporáneas, ya que la prevención de sus consecuencias no está enmarcada en un respeto al Estado de Derecho liberal, sino que implican una agenda o regulaciones globales para evitar el atropello de los derechos fundamentales de las personas.

De la misma manera, la prevención que se hace sobre los inminentes peligros de seguridad es cada vez más subjetiva. A pesar de que existen amenazas reales, tales como el caso de la pandemia por el COVID-19 y sus respectivos contagios, en el resto de los casos no existe una justificación suficiente para siquiera entender a los sujetos amenazantes como amenazas. Esto se entiende dado que todo el proceso de securitización se da en el marco de una prevención total del crimen o la inseguridad desde los medios tecnológicos, lo cual termina convirtiendo a los sujetos en cifras para estimar un posible acto de inseguridad, lo que lleva a un estado de amenaza existencial constante y, por ende, a una securitización institucionalizada.

Por otro lado, si se han creado vulnerabilidades sociales y problemas de gobernanza derivadas de la vigilancia tecnológica o, de manera más amplia, de la tecnosecuritización. Esto, dado que como se ha visto en los casos, no existe ninguna regulación en la materia. Estados Unidos, a pesar de tener algunas regulaciones en materia legal, no ha tenido ningún impedimento para vigilar a millones de personas en el mundo, incluyendo a mandatarios de países aliados. Esta vigilancia no solo ha violado el derecho a la privacidad y, en última instancia, al de la presunción de inocencia en millones de personas, sino que también se ha valido de vacíos legales para ejercer su poder. Este punto de los vacíos se puede ejemplificar con el caso de la vigilancia desde la alianza de seguridad de los “5 ojos”, ya que gran parte de su funcionar implica la vigilancia en terceros países, es decir, si en uno de los países es ilegal la vigilancia a los nacionales por el propio país, es muy probable que no exista una regulación para la vigilancia a los a los nacionales por terceros países, lo que implica explotar estos vacíos para ejercer un mayor control. Del mismo modo, ni el Reino Unido, ni China, ni Corea del Sur se han visto limitados por regulaciones exteriores y, en algunos casos, incluso se ampara a la vigilancia. De esta manera, el mundo actual va progresivamente cayendo en la

gobernanza algorítmica y la vigilancia extrema de las sociedades de control, lo que genera perjuicios para todas las partes.

Finalmente, al estar hablando de que estos problemas se están transformando en un fenómeno que traspasa las fronteras y se multiplica en los países, es que se entiende como es que son problemas con los que se tendrán que lidiar dentro de las Relaciones Internacionales contemporáneas. Más adelante, incluso, se tendrá que estudiar como es que esta sociedad de control se establece en el sur global y, de la misma manera, como es que estos procesos de tecnosecuritización se establecen dentro de democracias más débiles o, incluso, dentro de regímenes totalitarios, lo que implicaría aún más problemas ante los que los investigadores tendrán que plantear soluciones.

Con todo esto en cuenta, y en forma de respaldar el cumplimento de la hipótesis presentada, se exponen las siguientes conclusiones:

- En los casos presentados parece que no es necesaria la existencia del acto discursivo para que ocurra la securitización. Dentro de la teoría, el discurso por sí solo no crea la securitización, sino que necesita de la aceptación de la audiencia. Dentro del presente trabajo se puede identificar con facilidad al actor securitizador, la amenaza, el objeto referente, etc. Lo que implica un contexto securitizador. Sin embargo, el punto del acto discursivo se presenta como una limitación, dado que, al parecer, si el Estado tiene el poder suficiente puede ejercer la securitización, incluso si no es mediante la legitimación del acto discursivo. De esta forma, parece ser que la realidad va más cerca de la crítica sobre que, más allá del acto discursivo, que es válido en ciertas situaciones, la securitización parte de la institucionalización y rutinización a través de las prácticas de seguridad y del ejercicio de poder, lo que también implica una imposición de narrativas desde el poder

- La teoría si es eficiente en la descripción de los casos. Más allá de sus conflictos para dar paso a una emancipación, o por la limitación que pueda existir por parte de la aceptación del discurso, la teoría permite entender las dinámicas de creación de amenazas existenciales, las cuales se han complejizado en el siglo XXI. Este fenómeno se da con la sociedad de control, dónde se incrementan las problemáticas de la tecnosecuritización, dado que el Estado puede tener un mayor control sobre la amenaza existencial mediante la vigilancia perpetua.
- A pesar de que la teoría permite hacer una descripción de las problemáticas, no da paso a la acción. Esta es una problemática que, más que ser de la securitización en si misma, se entiende por su adscripción al enfoque de la Escuela de Copenhague que no se entiende como una teoría emancipatoria. A pesar de esto, sería interesante plantearse como cambiar estas estructuras de poder.
- Dentro de las implicaciones políticas a las que conlleva la complejización de la securitización, entendida como tecnosecuritización, se encontró que el manejo público está cada vez menos dado por los políticos y se está tomando como alternativa a la gobernanza algorítmica. A pesar de que la tecnología pueda verse como algo superior al ser imparcial, es una premisa que termina siendo falsa. La tecnología está hecha por humanos y se alimenta de datos generados por humanos. De esta forma, el giro hacia prácticas como la gobernanza algorítmica pueden ser perjudiciales para las sociedades contemporáneas al dar paso a sesgos raciales o de género. De la misma manera, al estar en sociedades donde cada vez se rechaza más al “otro”, estas prácticas de tecnosecuritización pueden dar paso a una represión o persecución cada vez mayor hacia las minorías.
- Dentro de las implicaciones institucionales, los casos analizados reflejaron un panorama bastante complicado. Para la correcta institucionalidad de un país es

importante la sujeción a las limitaciones de su propia estructura, es decir, estar enmarcado dentro del Estado de Derecho. Sin embargo, dentro del contexto de la tecnosecuritización se brinda un poder muy amplio al Estado, donde, por una parte, se puede utilizar el "*jurisdiction shopping*" para evadir las regulaciones internas de vigilancia y, por otra parte, se otorga el poder de vigilancia perpetua mundial mediante la intervención de sistemas electrónicos. Todo esto puede resultar bastante grave dentro de las Relaciones Internacionales contemporáneas, pues ya no se ve como una amenaza existencial a un grupo, sino a toda la sociedad mundial. De esta forma, es importante la existencia de regulaciones ante el poder que abarcan entes como la alianza de los "5 ojos".

- Las implicaciones dentro de los Derechos Humanos pueden considerarse entre las más graves para la población. El hecho de que se vea a todo el mundo como una amenaza, porque desde la perspectiva de los Estados existe la posibilidad de que cualquier persona sea un criminal o un terrorista, justifica la vigilancia masiva global mediante herramientas tecnológicas. De esta forma, la tecnosecuritización implica una intromisión constante a la privacidad de las personas para controlar que no estén incurriendo en actos criminales. Además de esto, las formas de vigilancia actuales implican que se ve a las personas como sujetos culpables a los que se debe vigilar, y no como sujetos con una presunción de inocencia como Derecho Humano fundamental.
- Dentro de las implicaciones en el control social, se pudo ver que, con la tecnosecuritización en el contexto de las sociedades de control, el problema va a ir en aumento. La tecnología da la posibilidad de recolectar cada vez más información y, de esta manera, llevar a un control mucho más preciso de las personas. Con todo este aparato de información, los Estados están en la capacidad de moldear el

comportamiento de las personas. Toda esta problemática sigue estando enmarcada en la complejización de la securitización, es decir, se sigue viendo a todas las personas como una amenaza existencial y eso justifica su vigilancia, en este caso por medios tecnológicos para abarcar a más personas, lo que implica, según su visión, mucha más seguridad.

- Dado la novedad del tema tecnológico dentro de las Relaciones Internacionales, resultó importante el planteamiento desde un enfoque cualitativo con su investigación documental para dar cuenta de una problemática poco estudiada dentro del campo actual. Esto es un inicio para dar un entendimiento a futuro sobre posibles formas de prevenir los daños que conlleva la tecnosecuritización y, tal vez, plantear procesos de desescuritización desde la sociedad civil en esta materia.
- A pesar de que resultó importante el enfoque cualitativo por la novedad, si fue una limitación el no tener cifras para estimar el tamaño del impacto de las 4 implicaciones en las Relaciones Internacionales contemporáneas
- Con lo expuesto durante el desarrollo del presente trabajo se puede entender que el rol de la tecnología dentro de las Relaciones Internacionales irá en incremento con el paso de los años. Esto plantea diferentes retos dentro del campo, ya que implica una adaptación de las teorías para dar cuenta de los hechos que ocurrirán dentro de un nuevo tipo de sociedad hiperconectada. El rol que están tomando las empresas privadas, ya no solo en moldear el panorama económico de los países, sino también en brindar apoyos políticos y de seguridad y, en algunos casos, superando el poder que tienen algunos Estados (como son los casos de Facebook y Google en el mundo), son temas que se deben tomar en cuenta en los futuros estudios de las Relaciones Internacionales.

Recomendaciones

- Dada la limitación sobre los actos discursivos dentro de la complejización de la securitización, sería importante realizar un complemento actual a esta teoría. Esto puede ser basado en como dentro de las actuales sociedades de control se están dando procesos de seguridad mucho más autoritarios, pero, al mismo tiempo, mucho más silenciosos. Esto no implica una reformulación teórica, sino una ampliación para su correcta aplicación dentro de los casos actuales
- Es importante que se amplíe el análisis de las implicaciones de esta tecnosecuritización dentro de las Relaciones Internacionales contemporáneas por medio de cifras. Es decir, datos que reflejen hasta que punto realmente está existiendo un cambio sustancial en las dinámicas de securitización de hoy en día y como eso está influyendo en la sociedad. Por ejemplo, se puede medir la percepción de las personas sobre la vigilancia realizada por su gobierno o que cantidad de personas están conscientes de la información que se les está sustrayendo de sus dispositivos o de la cantidad de información que están otorgando a empresas/Estados. De esta manera se pueden establecer, de forma más precisa, los impactos de la securitización, así como también se pueden armar planes para realizar una desecuritización.
- Enmarcado en los casos presentados, sería importante establecer regulaciones sobre el accionar de los Estados o, por lo menos, visibilizar mucho más estás problemáticas para que existan iniciativas de control desde la sociedad civil. Si bien la regulación a nivel internacional no es muy útil, ya que los Estados no están sujetos a un ente supranacional que tenga la capacidad de hacer cumplir dichas regulaciones, todo esto se puede empezar a dar desde políticas internas de cada país. Actualmente en los países del norte global no existen limitaciones claras para esta tecnosecuritización, dado que en muchas ocasiones está al servicio de los intereses nacionales. De esta

forma, es importante que sea la sociedad civil quien eleve a los parlamentos muchos más cuestionamientos sobre el manejo de datos y la implementación de la gobernanza algorítmica. Actualmente abogados e ingenieros están hablando sobre implementar la *blockchain* en los sistemas públicos o privados, así como el tránsito hacia las *smart cities*. Sin embargo, se debe dejar de lado esta idealización de la tecnología y realmente plantear regulaciones para evitar más violaciones de la privacidad, más control social y más discriminación.

- Dentro del estudio general de las Relaciones Internacionales, sería importante ampliar el estudio del impacto de la tecnología en dos ámbitos: primero en la creación de especialidades y, segundo, en la ampliación de los syllabus. El primer punto dado que, incluso en Estados Unidos y Europa, se sigue teniendo el cruce entre seguridad y tecnología como un ámbito totalmente orientado a las ingenierías. Por este motivo, no se tiene una visión clara de como todas estas cuestiones pueden presentar nuevos retos dentro de las Ciencias Sociales y, en especial, dentro de las Relaciones Internacionales. El segundo punto es dado en la medida en que los syllabus actuales están enmarcados en como se han dado las Relaciones Internacionales hasta la década del 2010. Esto implica que no hay un espacio para que las nuevas generaciones, quienes nacieron y crecieron en contextos tecnológicos, entiendan como se conecta la forma en la que entienden el mundo con las Relaciones Internacionales contemporáneas.

Bibliografía

Algoritmo (s.f). En *Diccionario de la Real Academia Española*. Recuperado de: https://dle.rae.es/algoritmo?m=form

Amnesty International UK. (2015, 17 marzo). *Evidence of global opposition to US mass surveillance*. https://www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq

Araujo, J. (2022). La algoritmización en el mundo del capitalismo de la vigilancia. *OXÍMORA Revista Internacional de Ética y Política,* 1-37.

Araya, A. S. (2012). Diagramas y biopoder. Discusiones sobre las sociedades de control. *Hermenéutica intercultural: revista de filosofía*, (20), 19-55.

Asamblea General de la ONU. (1948). Declaración Universal de los Derechos Humanos (217 [III] A). Paris.

Astorga, O. (2009). *El pensamiento político moderno: Hobbes, Locke y Kant.* Ediciones de la Biblioteca de la Universidad Central de Venezuela: Caracas

Ávila, J. A. N. (2022). El Metaverso: conceptualización jurídica, retos legales y deficiencias normativas. *Erişim Tarihi*, *3*(03), 2022.

Aylward, M. K. (2021, 2 noviembre). *Turning Ghosts into Humans: Surveillance as an Instrument of Social Engineering in Xinjiang*. War on the Rocks. https://warontherocks.com/2021/11/turning-ghosts-into-humans-surveillance-as-an-instrument-of-social-engineering-in-xinjiang/

Barker, C., Petrie, C., Dawson, J., Godec, S., Porteous, H., & Purser, P. (2017). *Oversight of Intelligence Agencies: A Comparison of the'Five Eyes' Nations*. Parliamentary Information and Research Service.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization'revisited: Theory and cases. *International relations, 30*(4), 494-531.

Banai, A., & Kreide, R. (2017). Securitization of migration in Germany: the ambivalences of citizenship and human rights. *Citizenship studies, 21*(8), 903-917.

Barbudo, C. F. (2019). El nuevo concepto de privacidad: la transformación estructural de la visibilidad. *Revista de estudios políticos*, (185), 139-167.

Barnard-Wills, D. (2011). UK news media discourses of surveillance. *The Sociological Quarterly, 52*(4), 548-567.

Barraycoa, J. (2017). Despersonalización y control social en la sociedad posmoderna. *Espíritu: Cuadernos del Instituto Filosófico de Balmesiana*, *66*(153), 87-106.

Bauman, Z, y Lyon, D. (2013). *Vigilancia líquida*. Editorial Paidós: Barcelona

Baumgartner, J. (2016). Treaty Shopping in International Investment Law. *Oxford Scholarship Online*. https://doi.org/10.1093/acprof:oso/9780198787112.001.0001

Baysal, B. (2020). 20 Years of Securitization: Strengths, Limitations and A New Dual Framework. *Uluslararası İlişkiler Dergisi, 17*(67), 3-20.

BBC News. (2014, 17 enero). *Edward Snowden: Leaks that exposed US spy programme*. https://www.bbc.com/news/world-us-canada-23123964

BBC News Mundo. (2018, 21 marzo). *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. https://www.bbc.com/mundo/noticias-43472797

BBC News. (2019, 20 diciembre). *Facial recognition fails on race, government study says*. https://www.bbc.com/news/technology-50865437

BBC News. (2020, 3 septiembre). *NSA surveillance exposed by Snowden ruled unlawful*. https://www.bbc.com/news/technology-54013527

BBC News. (2022, 12 febrero). *Lawmakers allege «secret» CIA spying on unwitting Americans*. https://www.bbc.com/news/world-us-canada-60351768

Beens, R. E. G. (2021, 10 diciembre). *The State Of Mass Surveillance*. Forbes.

https://www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/?sh=2caa50a1b62d

Bélanger, F., & Crossler, R. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 1017-1041.

Bhuiyan, J. (2021, 30 septiembre). *'There's cameras everywhere': testimonies detail far-reaching surveillance of Uyghurs in China*. The Guardian. https://www.theguardian.com/world/2021/sep/30/uyghur-tribunal-testimony-surveillance-china

Big Brother Watch. (2018, mayo). *Face Off: The lawless growth of facial recognition in UK policing*.

Borda, L. V. (2007). Estado de derecho y Estado social de derecho. *Rev. Derecho del Estado*, *20*, 73.

Briglia, M. D. (2021). Big Brother XI: How China's Surveillance of the Uyghur Population Violates International Law. *George Washington International Law Review, 53*(1)

Buckley, C., & Mozur, P. (2019, 22 mayo). *How China Uses High-Tech Surveillance to Subdue Minorities*. The New York Times. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

Buolamwini, J. & Gebru, T. (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Learning Research (81)*, 1-15

Buzan, B. (1983). *People, States, and Fear.* Wheatsheaf books: Brighton

Buzan, B., Wæver, O., & De Wilde, J. (1998). S*ecurity: A new framework for analysis.* Lynne Rienner Publishers.

Buzan, B., & Waever, O. (2003). R*egions and Powers: The Structure of International Security.* Cambridge University Press: Cambridge

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge

University Press: Cambridge

Canales, K. (2018, 30 octubre). *China has started ranking citizens with a creepy «social credit» system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you*. Business Insider. https://www.businessinsider.nl/china-social-credit-system-punishments-and-rewards-explained-2018-4?international=true&r=US

Castro, E. (2008). Biopolítica: de la soberanía al gobierno. *Revista latinoamericana de filosofía, 34*(2), 187-205.

Carlo, S. (2019, 17 mayo). *Britain Has More Surveillance Cameras Per Person Than Any Country Except China. That's a Massive Risk to Our Free Society*. Time. https://time.com/5590343/uk-facial-recognition-cameras-china/

CEPAL. (2019, 24 mayo). *Revolución tecnológica: desafíos y oportunidades para la industria, el empleo, la igualdad de género y el desarrollo social en América Latina y el Caribe | Evento | Comisión Económica para América Latina y el Caribe*. https://www.cepal.org/es/eventos/revolucion-tecnologica-desafios-oportunidades-la-industria-empleo-la-igualdad-genero

Chertoff, P. (2020, 7 febrero). *Facial Recognition Has Its Eye on the U.K.* Lawfare. https://www.lawfareblog.com/facial-recognition-has-its-eye-uk

Chong, G. P. L. (2019). Cashless China: Securitization of everyday life through Alipay's social credit system—Sesame Credit. *Chinese Journal of Communication*, *12*(3), 290-307.

Chorzempa, M., Triolo, P., & Sacks, S. (2018). *China's social credit system: A mark of progress or a threat to privacy?* (No. PB18-14).

Chowdhury, A. (2020). *unmasking facial recognition an exploration of the racial bias*

implications of facial recognition surveillance in the United Kingdom. WebRoots Democracy.

Cohen, J. E. (2012). What privacy is for. *Harv. L. Rev.*, *126*, 1904.

Cornell University Law School. (s. f.). *Forum Shopping*. LII / Legal Information Institute. https://www.law.cornell.edu/wex/forum_shopping

Coşkun, B. (2012). Words, images, enemies: Macro-securitization of the Islamic terror, popular TV drama and the war on terror. *Turkish Journal of Politics, 3*(1), 37-51.

Cox, J. S. (2013). *Canada and the five eyes intelligence community*. Canadian Defence & Foreign Affairs Institute.

Crampton, J. W. (2015). Collect it all: National security, big data and governance. *GeoJournal*, *80*(4), 519-531.

Cristiano, F. (2020). Israel: Cyber-securitization as National Trademark. *Routledge Handbook of Global Cybersecurity Strategy. Abingdon: Routledge.*

Dai, X. (2018). Toward a reputation state: The social credit system project of China.

Dearden, L. (2019, 16 agosto). *Facial recognition becoming 'epidemic' in British public spaces*. The Independent. https://www.independent.co.uk/news/uk/home-news/facial-recognition-kings-cross-shopping-centres-law-epidemic-privacy-a9062956.html

Dearden, L. (2020, 13 agosto). *Facial recognition has been used unlawfully and violated human rights, Court of Appeal rules in landmark case*. The Independent. https://www.independent.co.uk/news/uk/home-news/facial-recognition-unlawful-violation-human-rights-court-of-appeal-a9664441.html

Deleuze, G. (2006). Post-scriptum sobre las sociedades de control. *Polis. Revista Latinoamericana*, (13).

De Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *IDP. Revista de Internet, Derecho y Política*, (13), 53-66.

Detraz, N. (2013). *International security and gender*. John Wiley & Sons.

de Jong, E., & Gallagher, S. (2021, 25 agosto). *«One day we'll disappear»: Tuvalu's sinking islands*. The Guardian. https://www.theguardian.com/global-development/2019/may/16/one-day-disappear-tuvalu-sinking-islands-rising-seas-climate-change

Feeney, M. (2022, 4 enero). *Keep Facial Recognition Away from COVID-19 Response.* Cato Institute. https://www.cato.org/blog/keep-facial-recognition-away-covid-19-response

Ferrajoli, L. (1997). Jurisdicción y democracia. *Jueces para la democracia*, (29), 3-9.

Forbes. (2021, 21 abril). *UE regula inteligencia artificial; deja vigilancia masiva para emergencias*. Forbes México. https://www.forbes.com.mx/ue-inteligencia-artificial-vigilancia-masiva-emergencias/

Foucault, M. (2009). *Nacimiento de la biopolítica*: curso del Collège de France (1978-1979) (Vol. 283). Ediciones Akal.

Fouad, N. (2019). The peculiarities of securitising cyberspace: a multi-actor analysis of the construction of cyber threats in the US (2003-2016). In *Proceedings of the 18th European Conference on Cyber Warfare and Security. Academic Conferences and Publishing International Limited.*

Garcia Ricci, D. (2015). *Estado de derecho y principio de legalidad.* Comisión Nacional de los Derechos Humanos.

Gil, E. (2016). Big data, privacidad y protección de datos. *Madrid: Agencia Estatal Boletín Oficial del Estado*.

Gold, J. (2020). The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'. *URL: https://ccdcoe. org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities. pdf*.

Gómez, C. (2019). Estudios críticos sobre algoritmos:¿ un punto de encuentro entre la

ingeniería y las ciencias sociales?. *Revista Iberoamericana de Ciencia, Tecnología y Sociedad-CTS, 14*(41).

Gritsenko, D., & Wood, M. (2022). Algorithmic governance: A modes of governance approach. *Regulation & Governance, 16*(1), 45-62.

Güngör, G. (2020). *Security and surveillance in Xinjiang Uyghur autonomous region* (Master's thesis, Middle East Technical University).

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society, 13(*4), 361-374.

Han, B. C. (2014). *Psicopolítica: neoliberalismo y nuevas técnicas de poder*. Herder Editorial.

Hancock, J. T., & Bailenson, J. N. (2021). The social impact of deepfakes. *Cyberpsychology, behavior, and social networking*, *24*(3), 149-152.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly, 53*(4), 1155-1175.

Hersee, S. (2019). *The Cyber Security Dilemma and the Securitisation of Cyberspace* (Doctoral dissertation, Royal Holloway, University of London).

Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018). *Artificial intelligence and international security*. Center for a New American Security..

Hu, M. (2014). Small Data Surveillance v. Big Data Cybersurveillance. *Pepp. L. Rev.*, *42*, 773.

Inn, T. L. (2020). Smart city technologies take on COVID-19. *World Health*, *841*.

Innerarity, D. (2020). El impacto de la inteligencia artificial en la democracia. *Revista de las Cortes Generales, 109*, 87-103

Innerarity, D., y Colomina, C. (2020) La verdad en las democracias algorítmicas. *Revista*

CIDOB d'Afers Internacionals, 124, 11-23

Jurisdicción (s.f). En *Diccionario de la Real Academia Española*. Recuperado de: https://dle.rae.es/jurisdicci%C3%B3n?m=form

Kam, S., & Clarke, M. (2021). Securitization, surveillance and 'de-extremization'in Xinjiang. *International Affairs*, *97*(3), 625-642.

Karyotis, G. (2012). Securitization of migration in Greece: process, motives, and implications. *International Political Sociology, 6*(4), 390-408.

Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review, 8*(4), 1-18.

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse, 8*(1), 100-115.

Langer, P. (2020). Lessons from China-The formation of a social credit system: Profiling, reputation scoring, social engineering. In *The 21st Annual International Conference on Digital Government Research* (pp. 164-174).

Larsson, M., Guilhem, D., Bustamante, C., Lara, C., Putallaz, P., del Carpio A. (2022). La privacidad: un derecho humano y un principio ciudadano. *La privacidad como derecho humano,* 451

laSexta (2016, 13 marzo). *Entrevista completa a Edward Snowden en El Objetivo (versión extendida en VO)*. LaSexta. https://www.lasexta.com/programas/el-objetivo/noticias/entrevista-completa-edward-snowden-objetivo-version-extendida_20160313572398a04beb28d446ffed10.html

Leibold, J. (2020). Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement. *Journal of Contemporary China*, *29*(121), 46-60.

London Policing Ethics Panel. (2019, mayo). *London Policing Ethics Panel final report on live facial recognition.*

López, C. (2013). La biopolítica según la óptica de Michel Foucault. Alcances, potencialidades y limitaciones de una perspectiva de análisis. *El banquete de los Dioses, 1*(1), 111-137.

Lyon, D. (2010). Surveillance, power and everyday life. In *Emerging digital spaces in contemporary society* (pp. 107-120). Palgrave Macmillan, London.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society*, *1*(2), 2053951714541861.

MacAskill, E. (2013, 1 noviembre). *NSA files decoded: Edward Snowden's surveillance revelations explained*. The Guardian. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Malamud, S. (2018). Videovigilancia y privacidad. Consideraciones en torno a los casos" Globos" y" Drones". *Revista chilena de derecho y tecnología*, *7*(2), 137-162.

Marin, L. (2017). The deployment of drone technology in border surveillance: Between techno-securitization and challenges to privacy and data protection 1. I*n Surveillance, Privacy and Security* (pp. 107-122). Routledge.

Mattelart, A., & Vitalis, A. (2015). *De Orwell al cibercontrol*. Editorial Gedisa.

Matturdi, B., Zhou, X., Li, S., & Lin, F. (2014). Big Data security and privacy: A review. *China Communications*, *11*(14), 135-145.

McCray, R. (2021, 29 septiembre). *The Privacy Lesson of 9/11: Mass Surveillance is Not the Way Forward | News & Commentary*. American Civil Liberties Union. https://www.aclu.org/news/national-security/the-privacy-lesson-of-9-11-mass-surveillance-is-not-the-way-forward

Medero, G. (2013). El ciberespionaje. *Derecom, (13)*, 9.

Meyer, D. (2022, 11 febrero). *The CIA has been conducting mass surveillance in the U.S.*

with minimal oversight—and the program's uncovering is bad news for Big Tech. Fortune. https://fortune.com/2022/02/11/cia-mass-surveillance-wyden-privacy-shield-meta/

Milanovic, M. (2015). Human rights treaties and foreign surveillance: Privacy in the digital age. *Harv. Int'l LJ*, *56*, 81.

Mistreanu, S. (2019, 23 julio). *Life Inside China's Social Credit Laboratory*. Foreign Policy. https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/

Munster, R. (2005). *Logics of Security: The Copenhagen School, Risk Management and the War on Terror.* Copenhagen, Denmark: Syddansk Universitet

Muñoz, M. M. (2018). Virtualización del espacio público y concepto débil de privacidad. Lecciones del caso Facebook-Cambridge Analytica. *Ensayos de Filosofía*, *8*(2).

Najah, R. (2020). Surveillance Technologies in the COVID-19 Era. *Policy Center for the New South*

Nishiyama, H. (2018). Crowd surveillance: The (in) securitization of the urban body. *Security Dialogue, 49*(3), 200-216.

Norris, C. & Armstrong, G. (2015). CCTV and the social structuring of surveillance. *Crime Prevention Studies, (10),* p.157-178

Ooijen, M. (2020). *Cyber securitization or cyberization of conflict? –the militarization of Cyber Security in Estonia* (Master's thesis).

Park, S., Lim, Y. (2020). Harnessing technology to tackle COVID-19: Lessons from Korea. *Data, AI Governance, and COVID-19: Medium and Long-Term Perspectives for Asia*

Park, C., & Wang, T. (2013, December). Big Data and NSA Surveillance--Survey of Technology and Legal Issues. In *2013 IEEE International Symposium on Multimedia* (pp. 516-517). IEEE.

Pabón Cadavid, J. A. (2020). Protección legal a los metadatos y la gestión digital de los

derechos de autor. *Ius et Praxis*, *26*(1), 57-76.

Perasso, V. (2016). Qué es la cuarta revolución industrial (y por qué debería preocuparnos). *BBC Mundo*, *12*.

Petit, P. (2020). 'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization. *Science as Culture, 29*(1), 30-56.

Pfluke, C. (2019). A history of the five eyes alliance: possibility for reform and additions. *Comparative Strategy*, *38*(4), 302-315.

PoKempner, D. (2020, 28 octubre). *US Government Mass Surveillance Isn't 'Secret'*. Human Rights Watch. https://www.hrw.org/news/2019/09/18/us-government-mass-surveillance-isnt-secret

Portal, B. (2018, 25 julio). *Police facial recognition system faces legal challenge.* BBC News. https://www.bbc.com/news/uk-44928792

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48-55.

Privacidad (s.f) En *Diccionario de la Real Academia Española.* Recuperado de: https://dle.rae.es/privacidad?m=form

Quasim, M. & Meraj, M. (2017). Big Data security and privacy: a short. *Technology, 8*(4), 408-412

Quiñones, R. (2021). Cyberwarfare o Ciberguerra. *Comunicación: estudios venezolanos de comunicación*, (196), 95-103.

Rahim, Z. (2019, 13 agosto). *London King's Cross estate admits using facial recognition technology*. The Independent. https://www.independent.co.uk/news/uk/home-news/london-kings-cross-estate-facial-recognition-a9055101.html

Ramos, L. F. (2020, September). Evaluating privacy during the COVID-19 public health

emergency: the case of facial recognition technologies. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (pp. 176-179).

Revelo, M. (2018). Securitization as Survival, Securitization as a Speech Act: A Critic to the Copenhagen School. *URVIO Revista Latinoamericana de Estudios de Seguridad, (22),* 58-69.

Reyes Guzmán, A. (2018). *Migración como tema de seguridad: securitización de la inmigración venezolana en el Ecuador* (Bachelor's thesis, Quito).

Robinson, P. (2008). *Dictionary of International Security*. Polity: Cambridge

Rodríguez, P. E. (2008). ¿Qué son las sociedades de control? *Revista Sociedad*, *27*, 177-192.

Rodríguez-Merino, P. (2018). China's protracted securitization of Xinjiang: Origins of a surveillance state. *E-International Relations.*

Rosemain, M. (2020, 6 octubre). *Top court rules EU states must curb mass spying on data*. Reuters. https://www.reuters.com/article/us-eu-privacy-idUSKBN26R129

Rossi, L. S. (2018). Agenciamientos en las sociedades de control. *Cultura-hombre-sociedad*, *28*(1), 177-206.

Ruby, F., Goggin, G., & Keane, J. (2017). "Comparative Silence" Still? Journalism, Academia, and the Five Eyes of Edward Snowden. *Digital Journalism*, *5*(3), 353-367.

Sadik, G., & Ceren, K. (2020). The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management. *Uluslararası İlişkiler Dergisi, 17*(68), 145-160.

Sagot, M. (2020). Muerte, control social y bienestar en tiempos de Covid-19. *Alerta global*, 107.

Salvi, N. (2019). Poder y propiedad: el gran relato del dominio y el control social. *Fuegia: Revista de estudios sociales y territorio*, *2*(2), 76-84.

Satter, R. (2020, 3 septiembre). *U.S. court: Mass surveillance program exposed by Snowden was illegal*. Reuters. https://www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK

Schmitt, C., Shoffner, M., Owen, P., Wang, X., & Lamm, B. (2013). Security and privacy in the era of big data. *The SMW, a Technological Solution to the Challenge of Data Leakage*, *1*(2).

Schneier, B. (2018, 25 enero). *How to fight mass surveillance even though Congress just reauthorized it*. Washington Post. https://www.washingtonpost.com/news/posteverything/wp/2018/01/25/how-to-fight-mass-surveillance-even-though-congress-just-reauthorized-it/

Shahshahani, A., & Gupta, A. (2021, 28 abril). *Broader US government surveillance powers won't make us safer*. Privacy | Al Jazeera. https://www.aljazeera.com/opinions/2021/4/28/broader-u-s-government-surveillance-powers-wont-make-us-safer

Shakir, O. (2021, 24 noviembre). *Mass Surveillance Fuels Oppression of Uyghurs and Palestinians*. Human Rights Watch. https://www.hrw.org/news/2021/11/24/mass-surveillance-fuels-oppression-uyghurs-and-palestinians

Shen, C. F. (2019). Social credit system in China. *City University of Hong Kong*.

Smith, A. (2020, 29 junio). *AI experts warn against crime prediction algorithms, saying there are no «physical features to criminality».* The Independent.https://www.independent.co.uk/tech/ai-experts-crime-prediction-algorithm-criminality-a9583451.html

Smith Finley, J. (2019). Securitization, insecurity and conflict in contemporary Xinjiang: has PRC counter-terrorism evolved into state terror?. *Central Asian Survey*, *38*(1), 1-26.

Taruffo, M. (2008). Leyendo a Ferrajoli: consideraciones sobre la jurisdicción.

Trédaniel, M., & Lee, P. K. (2018). Explaining the Chinese framing of the "terrorist" violence in Xinjiang: insights from securitization theory. *Nationalities Papers*, *46*(1), 177-195.

Treguer, F. (2019). La "ciudad segura" o la gobernanza por los algoritmos. *Le Monde diplomatique en español,* (284), 15.

Vargas, L. (2022) *¿Está usted preparado para ingresar al metaverso?*

Vultee, F. (2010). Securitization: A new approach to the framing of the "war on terror". *Journalism practice, 4*(1), 33-47.

Walsh, P. F., & Miller, S. (2016). Rethinking 'Five Eyes' security intelligence collection policies and practice post Snowden. *Intelligence and National Security*, *31*(3), 345 368.

Wakefield, B. J. (2021, 26 mayo). *AI emotion-detection software tested on Uyghurs*. BBC News. https://www.bbc.com/news/technology-57101248

Wood, D., & Webster, C. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research*, *5*(2), 259-273.

Whitaker, R. (2003). The Return of Big Brother? Privacy, Surveillance Technologies, and Ethics After 9-11.

Young, J. Y. (2021, 13 diciembre). *South Korean City to Test Facial Recognition to Track the Coronavirus*. The New York Times. https://www.nytimes.com/2021/12/13/world/asia/south-korea-facial-recognition-coronavirus.html

Zuppi, A. (2002). *Jurisdicción universal para crímenes contre el Derecho Internacional: El camino hacia la Corte Penal Internacional*. Ad-Hoc: Buenos Aires