Vigilancia electrónica a gran escala y listas de alerta: ¿Productos de una política paranoica? / Electronic Large-scale Surveillance and Watch Lists: The Products of a Paranoid Politics?

Didier Bigo

Dossiê: "Criminalização das migrações"

VIGILANCIA ELECTRÓNICA A GRAN ESCALA Y LISTAS DE ALERTA: ¿PRODUCTOS DE UNA POLÍTICA PARANOICA?

Didier Bigo[1]

A partir de los artículos de Richard Hofstadter, sabemos que un estilo defensivo y hasta paranoico ha impregnado de vez en cuando a la política norteamericana. Murray Edelman y Michael Rogin han desplazado la postura psicológica de esta terminología hacia una de tono político, enfocándose en cómo la noción de la construcción de un espectáculo político puede incitar histeria y paranoia para atraer la atención pública y, al hacerlo, construir una securitización que expanda los poderes ejecutivos del Estado. Rogin describió cómo el discurso político norteamericano ha enfatizado estrategias antisubversivas en la construcción de enemigos: por ejemplo, contra pueblos indígenas, comunistas y la URSS y, más recientemente, migrantes ilegales y terroristas quienes han infiltrado, supuestamente, el país. Sin embargo, las implicaciones de estas políticas han sido raramente expandidas a la política trasnacional o internacional.

El objetivo amplio de este artículo es conectar la configuración de la política mundial contemporánea con ramas interesantes de la investigación sociológica que provienen del estudio crítico de la política norteamericana. Más específicamente, el autor argumenta que la compilación de listas de alerta a partir de bases de datos trasnacionales construye la criminalización de los viajeros como migrantes ilegales y

[1] Profesor de Estudios sobre Guerra, King's College London (KCL). Profesor-investigador en Sciences-Po de Paris. Paris, Francia.

peligrosos, mientras que afecta también a todo aquel que use servicios informáticos en la nube. Los Estados usan un estilo paranoico para oponer la soberanía nacional contra sus obligaciones internacionales. Las prácticas de cada país en este aspecto constituyen una variación distintiva de la tendencia hacia la Vigilancia Global Preventiva (GPS por sus siglas en inglés) que, según la mirada del autor, se ha convertido en una forma contemporánea de un proceso trasnacional de (in)seguridad, es decir, un proceso que entrega inseguridad a través de herramientas tecnológicas destinadas a proveer seguridad.

Para sostener este argumento, el artículo muestra cómo la emergencia de listas globales de alerta está reorientando a las tecnologías de bases de datos para servir a los fines de la vigilancia electrónica masiva. Los gobiernos justifican la vigilancia masiva, a pesar de su estatus ilegal en muchos países, alegando que si todo el mundo lo está haciendo, no puede ser ilegítimo. Una deformación paranoica de la política trasnacional basada en el malestar y el miedo es entonces instrumentalizada en el nombre de la soberanía, la seguridad, la ciudadanía y la identidad nacional. Las listas de alerta, en la visión del autor, son una manifestación concreta del desarrollo, por profesionales de la seguridad, de un intercambio trasnacional de acciones de miedo, que pretende enfocarse en migrantes y controles fronterizos pero que tiene mucho más que ver con fomentar estrategias antisubversivas domésticas que con servir como una respuesta efectiva frente a las amenazas.

Palabras clave: vigilancia, seguridad, movilidad, listas de alerta, política paranoica.

Enmarcando el problema: ¿es la vigilancia de la movilidad de personas e información a gran escala una forma de políticas burocráticas trasnacionales paranoicas?

El proyecto de este artículo es conectar la configuración de políticas mundiales contemporáneas con las ramas más interesantes de la investigación sociológica provenientes del estudio crítico de la política norteamericana. El artículo argumenta que la compilación de listas de alerta (*watch lists*) desde bases de datos trasnacionales construye la criminalización de los viajeros como migrantes ilegales y peligrosos, mientras que afecta también a las personas que alrededor del mundo usan servicios informáticos en la nube. ¿Cuál es la racionalidad contemporánea que justifica tal escala de vigilancia? ¿Dónde y cómo es la vigilancia llevada a cabo, cómo es transformada en herramientas de inteligencia a través de listas de alerta, cómo se volvió tan penetrante que amenaza con transformar la vida cotidiana? Para muchos, estas preguntas tienen una respuesta simple: todo deriva del imperativo de luchar contra el terrorismo global. Argumento aquí que la conexión íntima entre vigilancia e inteligencia no es el resultado de un miedo legítimo sino de una política paranoica en el sentido que Michael Rogin le da al término cuando discute sobre el mccartismo.

Por lo tanto, la primera sección ahonda en los debates norteamericanos de sociología crítica sobre el mccartismo, donde conceptos tales como la demonología política fueron ideados. El trabajo de Richard Hofstadter[2] sobre el desarrollo de un estilo paranoico en la política norteamericana y su elaboración por Michael Rogin, quien muestra que esta política paranoica puede originarse en el aparato de seguridad del Estado, son esenciales para entender la política contemporánea de vigilancia y movilidad[3].

Aunque el análisis de estos autores estuvo restringido a la política norteamericana, la racionalidad de la vigilancia electrónica internacional contemporánea de personas e información a gran escala tiene hoy, además, un carácter decisivamente trasnacional, porque los servicios de inteligencia occidentales comparten grandes volúmenes de datos sobre movimientos, comunicaciones y contactos de las personas a través, y también dentro, de las fronteras nacionales. La segunda sección, entonces, rastrea las conexiones entre servicios de inteligencia, guardias fronterizos e iniciativas antiterroristas. Aunque actúan ahora a través de un campo de poder internacional, los servicios de los Estados Unidos son, definitivamente, "primus inter pares". A pesar de esta asimetría, ningún servicio de inteligencia puede recolectar datos globales sin colaborar con otros servicios. Estos vínculos estructurales han desafiado a las políticas nacionales y a los conceptos tradicionales de seguridad nacional. Como fue argumentado en otra parte[4], esto ha creado asociaciones trasnacionales de profesionales de la seguridad en cada país, redes obsesionadas con la tecnología y el secreto, que colaboran a través de las fronteras, justificando la recolección masiva de datos que facilitan en nombre de los peligros del "enemigo interno". Esta lógica diagonal conecta la vigilancia a gran escala en democracia con la política paranoica mejor ilustrada por la doctrina del uno por ciento de Donald Rumsfeld, el Secretario de Defensa en el gobierno de George W. Bush desde enero de 2001 a diciembre de 2006[5]. Tales estrategias están destinadas a crear conformidad en poblaciones que, de otra manera, podrían impugnar una estrategia preventiva que requiera la recolección de datos a gran escala y la vigilancia masiva. Esta sección se enfocará en dos programas específicos – aquellos concernientes a la movilidad de personas y el control fronterizo –, y al movimiento online de información y correspondencia (particularmente su intercepción, recolección, retención y extracción para elaboración de perfiles)[6].

---

[2] HOFSTADTER, Richard. *The Paranoid Style in American Politics, and Other Essays*.

[3] ROGIN, Michael Paul. *The Intellectuals and McCarthy: the Radical Specter;* ROGIN, Michael Paul. The War on Evil.

[4] BIGO, Didier. The Transnational Field of Computerised Exchange of Information in Police Matters and its European Guilds, p. 155.

[5] La doctrina del uno por ciento está explicada en este artículo. Para una mayor información sobre sus orígenes e impacto, véase SUSKIND, Ron. *One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11*.

[6] Una tercera lógica está conectada con el movimiento de capital y el congelamiento de los bienes.

A continuación, la tercera sección analiza, primero, las listas de exclusión aérea construidas a través de la vigilancia de los movimientos de personas con los Archivos de Nombres de Pasajeros (PNR por sus siglas en inglés) y segundo, la vigilancia secreta de la Agencia de Seguridad Nacional (NSA por sus siglas en inglés), el Cuartel General de Comunicaciones del Gobierno (GCHQ)[7] y otros servicios de inteligencia occidentales, del movimiento de información y correspondencia digitalizada que ha sido divulgado por las revelaciones de Edward Snowden. Argumento que estos dos programas comparten características específicas. Primero, sus iniciadores suponen que estos programas les dan un alcance global, permitiendo prevenir amenazas inesperadas a través de compartir información mediante la colaboración entre servicios de inteligencia; una suposición que no es confirmada por consultas recientes. Segundo, el compartir información crea una hibridación de las disposiciones de secreto e interés público de los servicios de inteligencia con las disposiciones de los proveedores privados ya sean las compañías aéreas y/o agencias de viajes en el primer caso, o proveedores privados de internet, en el segundo. Esto crea la tendencia a tener intereses privados involucrados en la elaboración de la seguridad nacional y genera una intrusión respecto de la vida personal que va más allá de la protección de datos e incluso de la privacidad, ya que afecta la naturaleza del régimen democrático.

Finalmente, argumento que, si la vigilancia, la inteligencia y la democracia no son, per se, incompatibles, la escala de vigilancia sin precedentes que el seguimiento por aparatos electrónicos le provee a los servicios de inteligencia (afectando la libertad de movimiento de bienes, dinero, y viaje de las personas, así como también su libertad de comunicación sobre datos de información, metadatos y rutas), ha creado una política trasnacional paranoica y burocrática dominada por los profesionales de la seguridad y sus redes a través de esferas públicas y privadas. La interconexión de bases de datos públicas y privadas, argumento, no se debe al progreso de la tecnología y el aumento de las amenazas globales, sino a la veneración de lo tecnológico que amenaza con transformar[8] la naturaleza de los regímenes democráticos.

I. ¿La sospecha generalizada a escala trasnacional? Miedo, políticas del miedo y políticas paranoicas

Esto ha sido descripto por Anthony Amicelle y Marieke de Goede. Concierne al movimiento de capitales y el congelamiento de bienes que ensambla el flujo y la capacidad de seguir al dinero "sucio" y la limitación de bienes disponibles para el crimen organizado y terroristas. Fuentes de los medios populares han buscado familiarizar al público con organizaciones que se esfuerzan para congelar los bienes de los terroristas, tales como la compañía SWIFT, la TFTP y Naciones Unidas. Además, una larga lista de organizaciones (incluyendo bancos) han recolectado información sobre individuos privados con el objetivo de detectar operaciones sospechosas.

[7] Véase el glosario.

[8] MARX, Gary. La sociétéde sécurité maximale.

I.A. Lecciones del mccartismo: política paranoica y demonología política

Analizando el mccartismo, Hofstader sostiene que una forma de pensamiento popular proveniente de los "márgenes", pero retransmitida por algunos políticos, podría cambiar la lógica del liberalismo al centrar la atención en ciertos miedos hasta el punto en que éstos se convierten en obsesiones. Se distancia de la definición psicológica de paranoia insistiendo en que su foco no está en los rasgos de la personalidad individual sino en un estilo de política. "Estilo tiene que ver con la forma en la cual las ideas son creídas y propugnadas más que con la verdad o falsedad de su contenido"[9]. Este estilo está caracterizado por la emergencia de un portavoz, varón o mujer, quien es capaz de popularizar su convicción de que todo el mundo *viene a por su país*. Él o ella canalizan esta ansiedad a través de historias sobre enemigos y conspiraciones que buscan destruir la nación y su modo de vida. Las teorías conspirativas difieren dependiendo del lugar, las circunstancias y el período histórico, pero el estilo permanece constante.

Michael Rogin, en su crítica a Hofstader, desarrolló la noción de políticas paranoicas desde un ángulo diferente[10]. Para Rogin, la política paranoica no es un efecto del populismo producido por las personas que viven en los márgenes y amenazan a los del partido liberal, sino que es producto de una política antisubversiva que construye objetos del miedo a través de políticas específicas a fin de proporcionar justificación para una serie de medidas que, de otro modo, serían rechazadas. Por ejemplo, el gobierno puede usar la retórica paranoica para justificar el aumento del presupuesto por las amenazas, percibidas como tales, contra la seguridad, liberando de este modo al poder ejecutivo de la supervisión de los organismos de control, especialmente los tribunales[11]. El mccartismo no es sino un ejemplo de esta estrategia a la que Rogin denomina demonología política[12].

Quince años después, Rogin usó un análisis similar para explicar las acciones de Ronald Reagan en la "guerra encubierta" que su administración condujo contra Nicaragua en 1986. La administración de Reagan articuló una demonología política en donde los enemigos eran terroristas y traficantes de drogas, y marcó el comienzo de la idea de una amenaza global permanente, que debía ser "retrotraída". Rogin presenta una genealogía de las políticas antisubversivas organizadas por las burocracias de la seguridad, una demonología política[13] en la política norteamericana desde la demonización inicial de los pueblos indígenas por parte del ejército, pasando por la amenaza roja promovida por el FBI, hasta la Guerra Fría y la demonización de las políticas "socialistas". Este doble

[9] HOFSTADTER, *op. cit*., p. 5.
[10] ROGIN, *The Intellectuals…*, *op. cit*.; ROGIN, Michael Paul. *McCarthyism and Agrarian Radicalism*.
[11] VILTARD Yves. *Le cas Mc Carthy. Une construction politique et savante*.
[12] ROGIN, *The Intellectuals..., op. cit*.
[13] ROGIN, Michael Paul. *Ronald Reagan, the Movie and Other Episodes in Political Demonology*.

movimiento de exclusión nos permite entender la figura del enemigo presentada no como una ideología prohibida sino como una idea foránea que se infiltra en el gobierno y que genera traidores. El período de McCarthy llevó a una marca de la política que es todavía popular en los Estados Unidos (¡y en cualquier otro lugar!), por la cual los políticos de derecha acusan a cualquier persona poderosa de la izquierda de ser antipatrióticos, o simpatizantes del comunismo o socialismo. La consiguiente caza de brujas crea muchos "falsos positivos", personas inocentes acusadas equivocadamente, y un pequeño número de casos sustanciados. Como fue documentado después, la vigilancia de los servicios de inteligencia comenzó como una reacción al mccartismo, pero la "política paranoica" fue sin embargo practicada contra los movimientos de derechos civiles en la década de 1960 y usada nuevamente para justificar las acciones de Ronald Reagan en Nicaragua a fines de la década de 1980.

I.B. ¿La guerra contra el terrorismo como mccartismo global?

Michael Rogin tuvo tiempo, justo antes de su muerte, de escribir un artículo sobre la política de la guerra contra el terrorismo de Bush en septiembre de 2002, analizando la narrativa de Bush como una continuación de aquella de Ronald Reagan, pero con la figura del terrorista sirviendo como un enemigo global, interno y externo; y la amenaza escaló a una pelea de tipo armagedónica contra "el mal". Rogin vio esto como una estrategia que uniría al ala de la derecha aislacionista y la derecha religiosa con una política intervencionista que requería un nuevo complejo militar enfocado en la seguridad interna y en el desarrollo de herramientas de vigilancia masiva[14]. Las listas de alerta mundiales pueden ser simplemente leídas, quizás, como la aceleración y acentuación de esta lógica. Sin embargo, argumentaré que la construcción de listas de alerta a escala trasnacional es evidencia de que la política paranoica al estilo norteamericano se ha hecho global, transformando en el proceso a la política burocrática trasnacional y poniendo en peligro a la democracia.

II. La doctrina del uno por ciento y la globalización de la política paranoica por parte de los profesionales de la seguridad

II.A. La justificación de la guerra contra el terrorismo y su tecnologización a través de las listas de alerta

Como sabemos por la declaración sobre la guerra contra el terror del 14 de septiembre de 2001, nuevos modos de vigilancia fueron justificados como una respuesta necesaria a los eventos catastróficos del 11-S. Sin embargo, la lista de catástrofes contra las cuales protegerse se expandió rápidamente del terrorismo hacia las armas de destrucción masiva, el ciberterrorismo (la interrupción de

[14] ROGIN, The War..., *op. cit*.

la circulación electrónica de dinero), entre otras, creando una gran narrativa amenazante de la sospecha[15]. Mientras que una narrativa de la sospecha no es nueva – el imaginario cultural ha florecido por décadas en los Estados Unidos –, la escala de la sospecha no tiene precedentes porque la imagen del sospechoso es muy vaga[16]. El mccartismo, shockeante en su momento, ahora parece haber sido un asunto a pequeña escala. McCarthy simulaba tener una lista de nombres de traidores en su billetera. Pero la lista de la que hablaba tenía alrededor de 20 personas. Ahora el director de la NSA no esgrime una lista en papel, sino que tiene un pequeño disco duro con más de 400.000 sospechosos bajo vigilancia. La administración de Obama, a pesar de algunos movimientos para bajar el tono de la retórica de la guerra contra el terrorismo, ha seguido políticas similares a las de la administración Bush: por ejemplo, declaraciones como "la pregunta no es si, sino cuándo" y "tenemos que actuar antes de que sea demasiado tarde"[17]. Varios intelectuales con inclinación hacia la derecha han reforzado esta fórmula, agregando que un futuro Armagedón no puede ser limitado por las preocupaciones sobre derechos de privacidad. Por ejemplo, Posner sostiene que en tales situaciones "los servicios de inteligencia deben lanzar una amplia red con una malla muy fina para capturar las pistas que puedan posibilitar que el próximo ataque sea prevenido"[18]. Y, como explica, los servicios de inteligencia no pueden ser los bomberos llegando luego del incendio, deben actuar preventivamente, lo que sólo puede ser logrado revirtiendo la carga de la prueba y tratando a todo el mundo como un potencial terrorista hasta que se demuestre lo contrario. El enfoque puede ser resumido así: si las consecuencias del riesgo son inmensas, incluso si la probabilidad de riesgo es sólo del "uno por ciento", es necesario prevenir las acciones siguiendo a toda la población identificada como peligrosa. Este grupo no está predefinido, emerge de la búsqueda misma, y es desafortunado, pero necesario, detener al inocente para asegurarse de que la red es lo suficientemente amplia como para atrapar al potencialmente culpable.

En esta doctrina, el miedo legítimo a un "incidente" grave (por parte del gobierno) justifica el cambio en los patrones de comportamiento de los agentes de seguridad y la remoción del principio de inocencia. Este razonamiento ha sido atribuido a Donald Rumsfeld, cuyo síndrome del uno por ciento justifica la vigilancia, no sobre las bases de las evaluaciones de riesgo sobre comportamientos pasados (el estilo de razonamiento de la aseguradoras), sino anticipando las futuras consecuencias de un solo acto catastrófico[19].

---

[15] ARADAU, Claudia, MUNSTER, Rens. *Politics of Catastrophe: Genealogies of the Unknown*.

[16] BIGO, Didier. La mondialisationde l'(in)sécurité; CEYHAN, Ayse, PÉRIÈS, Gabriel. L'ennemi intérieur: une construction politique et discursive.

[17] 26 de mayo de 2011, declaración del Presidente Barack Obama cuando firmó la PATRIOT Sunsets Extension Act de 2011, una extensión de cuatro años de las tres provisiones claves de la Ley patriótica estadounidense.

[18] POSNER, Richard. *Frontiers of Legal Theory*, p. 5.

[19] Aquíes donde yo desacuerdo con una gran parte de la literatura sobre valoraciones de riesgo que

II.B. Las consecuencias: ¿una sospecha legítima desestabilizando el principio de inocencia? ¿qué significa la prevención?

Tal como plantea un funcionario del Centro Nacional contra el Terrorismo, a quien entrevisté en el 2005, al ofrecer una de las narrativas más sólidas sobre la elección de hacer prevención que obtuve en mis series de entrevistas durante los años 2002 al 2009:

> Estamos en una época en la que si tenemos que decidir capturar a diez personas y detenerlas indefinidamente porque una de ellas está potencialmente organizando un acto terrorista, entonces las nueve personas inocentes deben admitir que sus detenciones son un efecto colateral en la búsqueda del bien del colectivo. Puede ser que la noción tradicional de justicia sea invertida, pero es justo aceptar el sacrificio de algo de libertad para el conjunto del colectivo. El mundo ha cambiado. Para responder a las amenazas globales, necesitamos nuevas herramientas para sobrevivir. Y sólo aplicamos un principio utilitarista: la prevención... Prevención significa contrastar una lista de sospechosos o conductas sospechosas con un listado más amplio tanto de personas reales o seudónimos como de categorías de personas que comparten los mismos patrones que los algoritmos han identificado como pertenecientes a un perfil común: esto es lo que llamamos listas de alerta... Éstas no son listas públicas como las listas negras, que se utilizan para las personas que ya conocemos muy bien, son para sospechosos que no han sido condenados. No los castigamos. Sólo los rechazamos ex ante, o en la frontera; y si los detenemos es por un período muy corto, y tratamos de devolverlos tan pronto como sea posible. ¿Qué hay de malo con eso?[20]

Para él, no es posible actuar como antes, bajo las normas (de la ley), ya que éstas le están "torciendo el brazo por detrás de la espalda a los miembros de los servicios de inteligencia", dando ventajas a los terroristas. Cuando la supervivencia de la nación está en juego, la aceptación de estas limitaciones ya no es posible. Los servicios de inteligencia en las democracias deben ser absolutamente confiables para las personas que han elegido al gobierno. Están trabajando para protegerlos, no para espiarlos. Y necesitan trabajar en secreto para protegerlos eficazmente. La justicia penal, la presunción de inocencia, la intimidad y la libertad tienen que ajustarse a la "nueva" situación. Los fanáticos escondidos deben ser puestos al descubierto e interrumpidos, sean cuales sean los costos para las libertades civiles.

La vigilancia a gran escala contemporánea y la creación de listas enormes de sospechosos parecen ser el resultado de este síndrome de la sospecha ampliada.

---

mezclan los dos razonamientos y crean falsas continuidades entre las lógicas del seguro descritas por François Ewald y Michel Foucault y la lógica de la catástrofe descripta por Rumsfeld. Para la explicación de la posición de Rumsfeld y su desacuerdo con otros miembros de la administración Bush, véase SUSKIND, *op. cit*.

[20] Entrevista de Didier Bigo a un funcionario de enlace estadounidense en Europa en el 2008.

Investigaciones convergentes realizadas por una serie de ONG y parlamentos, después de las revelaciones de Snowden, pero también basadas en hechos sucedidos en los últimos diez años, y especialmente las investigaciones sobre el programa Conocimiento Total de la Información, condujeron a la conclusión de que las diferentes listas funcionan como la voluntad de las burocracias y sus contratistas privados para reevaluar continuamente quién es confiable y quién no lo es. Son el producto, una forma deliberada de objetivar la sospecha encontrando algunos de los peligrosos hipotéticos o indeseables del uno por ciento que *podrían* haber sido letales para la sociedad.

Contra esta narrativa, en las siguientes secciones insisto en que este razonamiento invierte completamente la lógica del derecho penal. Mediante la eliminación de la presunción de inocencia y la construcción de una lógica del futuro perfecto (*futur antérieur*), retiene a todos como sospechosos en base a una "memoria hacia adelante" – una memoria que ya ha leído el futuro[21]. Pero esta pretensión no se justifica sobre la base de la evidencia, las predicciones sobre futuras conductas son más oráculos que ciencia.

Sin embargo, la falta de datos sobre la eficacia no es, aparentemente, ningún obstáculo. Aceptando la imposibilidad de presentar evidencia sobre complots que fueron descubiertos y bloqueados a través de estas tácticas, los gobiernos, sus servicios de inteligencia, los juzgados y las ONG que defienden los derechos humanos parecen estancados. El gobierno de Estados Unidos ya ha propuesto algunas reformas que limitarían la capacidad de la NSA para recolectar información telefónica y de internet de manera masiva. En Europa, los juzgados han criticado fuertemente la recopilación masiva de datos y la directiva de retención de datos, pero hasta ahora han sido incapaces (o poco dispuestos) para declarar ilegal la recopilación preventiva de datos. Esto puede deberse a que las redes transnacionales de agencias de inteligencia que intercambian datos sobre los sospechosos de otros servicios han argumentado poderosamente que estas prácticas son herramientas esenciales para mantener el mundo seguro. Pero esto ha creado una bolsa de intercambio de valores del miedo, donde cada organización viene con su propia lista de alerta y de rechazos de ingreso, que entran en una serie de transacciones con las demás; el resultado dependerá del poder relativo de los actores institucionales. El llamado "Grupo de cinco ojos", el Club de Berna o incluso Europol se han convertido en tales lugares[22]. Una vez construido, el sistema debe crecer, ya que este es el fundamento de estas redes. Puesto que se da por sentado que millones de aspirantes a terroristas están

[21] Que no es exactamente la lógica de la seguridad especulativa tal como la describe DE GOEDE, Marieke. The SWIFT Affair and the Global Politics of European Security; BIGO, Didier, DELMAS-MARTY, Mireille. The State and Surveillance: Fear and Control; UGELVIK, Synnove, HUDSON, Barbara. *Justice and Security in the 21st Century: Risks, Rights and the Rule of Law*.

[22] Véase el glosario.

"allí afuera", si estas listas no crecen, los gobiernos podrían sospechar que estas agencias no están haciendo su trabajo, un escenario que amenaza tanto a actores públicos como privados, e involucra pérdida de ganancias, puestos de trabajo, prestigio y perspectivas profesionales.

Además, si algunos éxitos no son publicados, es más probable que la gente reaccione contra los controles. Por lo tanto, la expansión de la lista debe ir más allá de los sospechosos obvios para incluir a aquellos que tengan sólo vínculos tangenciales, o ninguno en absoluto, con los grupos terroristas. Las listas ahora incorporan a individuos asociados con otras formas de conductas consideradas problemáticas por las autoridades, tales como los evasores fiscales, personas con documentos falsos y quienes se han excedido en la permanencia de su visa (*overstayers*)[23]. Las dinámicas en funcionamiento aumentan exponencialmente la sospecha e incrementan el número de viajeros definidos como sospechosos cuya información se intercambia y se agrega en otras listas.

III. Seguimiento y control a través de medios electrónicos: Una lógica transnacional e híbrida de lo privado y lo público que afirma tener un alcance global en contra de las amenazas a fin de prevenirlas

Dos tipos de programas preventivos basados en sospechas – donde un/a individuo debe probar su inocencia antes de viajar o de ejercitar el derecho de libertad de expresión – han sido desarrollados. Ambos se basan en la información recolectada masivamente, identificando categorías de indeseables y controlándolos a través de los distintos servicios de inteligencia. Ambas generan listas de alerta automatizadas de sospechosos que se pueden compartir a nivel internacional y funcionan en todas partes.

III.A. Seguimiento y control de la circulación de las personas: las listas de no-vuelo

El primer tipo de programa se concentra en la creación de "fronteras inteligentes", realizadas a través de la elaboración de perfiles y recolección de datos personales. En los países democráticos esta securitización de las fronteras debe ser conciliada con la economía política del liberalismo.

Las fronteras inteligentes son pregonadas por su capacidad de dejar circular a la gente "libremente" en relación a sus actividades legítimas, mientras que recopilan electrónicamente información sobre todos los pasajeros. Los programas luego comprueban la historia personal y los movimientos de cada uno para distinguir al viajero potencialmente peligroso del legítimo. Esto divide a los viajeros entre aquellos "confiables" y los "indeseables". La primera categoría

[23] Una persona a la que se le ha dado permiso limitado para entrar o permanecer en un país, pero que no ha salido del país en la fecha indicada o no ha pedido que su estadía sea extendida.

nunca verá los controles o la vigilancia a distancia; los pertenecientes a la segunda van a terminar en las listas de "no vuelo"("*no fly" lists*) y en las "listas de alerta de terroristas", no por lo que hayan hecho, sino porque coinciden con un perfil de lo que otros han hecho previamente.

Una variedad de programas de fronteras inteligentes (por ejemplo, PNR, API, CAPPS, US-VISIT o Schengen VIS y SIS, ESTA, sistemas de Entrada y Salida) existen tanto en los EE.UU. como en la UE. Las etiquetas ahora le son familiares a los viajeros frecuentes, aunque sólo los especialistas entienden las sutiles diferencias entre los sistemas de EE.UU. y de la UE, sus lógicas y fundamentos[24]. Ambos están justificados por la necesidad de combatir al terrorismo, pero las lógicas europeas también hacen hincapié en la lucha contra la migración ilegal y el exceso de permanencia. En los EE.UU., CAPPS I & II (por sus siglas en inglés) o Sistema Computarizado de Pre-monitoreo de Pasajeros, creado tras el 11-S por el Departamento de Seguridad Nacional, son los programas más importantes. El secretario de Seguridad Interior, Michael Chertoff, por ejemplo, explicó en el año 2006 que el gobierno ha puesto en marcha con los programas US-VISIT (seguidores del CAPPS II criticado por su alto número de falsos positivos) una red de computadoras interconectadas y bases de datos interoperables con capacidades de entrada biométricas en 117 aeropuertos, 16 puertos marítimos y 153 puertos de entrada terrestres. Según él, "en cuestión de segundos, podemos confirmar positivamente la identidad de una persona chequeando los escaneos digitales de dos de sus dedos con listas de alerta de terroristas y criminales y registros de inmigración"[25]. Esto ha creado nuevas controversias, no sólo acerca de su eficiencia, sino también sobre la privacidad de los ciudadanos norteamericanos y de los extranjeros que pasan por los EE.UU. en ruta hacia otros destinos. Todavía no conocemos las conexiones entre este programa US-VISIT y los registros del PNR, o la cantidad de información personal que proviene de las bases de datos no identificadas del gobierno o de fuentes comerciales. Sin embargo, algunas fuentes han sugerido que pueden estar vinculadas con la Nueva Inteligencia de Datos Masivos (NIMD por sus siglas en inglés, una iniciativa secreta de la Comunidad de Inteligencia, Investigación de Avanzada y Actividades de Desarrollo, ARDA por sus siglas en inglés) que se centra en los datos masivos, y con el Programa Multiestatal Anti-Terrorismo de Intercambio de Información (MATRIX por sus siglas en inglés), un programa a nivel estatal que cuenta con el apoyo del Departamento de Justicia norteamericano y tiene como objetivo darles a las agencias policiales en todo el país una nueva y poderosa herramienta para analizar los antecedentes tanto de criminales como de ciudadanos norteamericanos comunes. De acuerdo con un artículo publicado en el periódico *The Washington Post* el 5 de agosto de 2003,

[24] Véase el glosario.

[25] CHERTOFF, M. citado en KABATOFF, Mathew. *Subject to Predicate. Risk, Governance and the Event of Terrorism within Post-9/11 U.S. Border Security*.

este programa en particular "permitiría a las autoridades (...) encontrar al instante el nombre y la dirección de cada dueño con pelo castaño de una camioneta Ford roja en un radio de 20 millas de un caso sospechoso"[26].

Las especulaciones son altas, el conocimiento es escaso. Matthew Kabatoff, en una excelente tesis doctoral, ha explorado en detalle los tecnicismos de esta lógica de rastreo de viajeros. Como él mismo explica, el método más predominante de alto perfil de comparaciones de listas de alerta empleado por la seguridad de Estados Unidos es conocido como Lista de Alerta del Terrorismo, en virtud del cual los datos de los nombres de todos los viajeros que entran, salen y viajan al interior de los Estados Unidos por vía aérea son comparados con tres listas (que son, a su vez, compilaciones de otras listas). En primer lugar, la lista de exclusión aérea de terroristas (una lista que contiene, hasta el 2008, aproximadamente 2.000 nombres de individuos que tienen prohibido abordar un avión a cualquier destino de los Estados Unidos). En segundo lugar, la lista de "personas seleccionadas automáticamente" (una lista que contiene aproximadamente 14.000 nombres de aquellas personas que son colocadas bajo escrutinio adicional al cruzar las fronteras debido a la percepción, por parte de la inteligencia de Estados Unidos, de sus vínculos con el terrorismo). En tercer lugar, se controlan al menos otras seis listas de alerta gubernamentales de los EE.UU. que contienen nombres de personas que han cometido delitos, infracciones relacionadas a la inmigración u otros delitos menores[27].

Estas listas de alerta informatizadas son consideradas por el DHS como las líneas reales de control. La frontera física está ahí para poner en práctica la inteligencia recopilada antes de que una amenaza potencial cruce. Es una línea importante, pero es la última, no la primera. Estas listas de alerta crean la posibilidad de clasificar a la gente, requiriendo que sólo algunos sean controlados en el aeropuerto – ampliando el período de control, pero también evitando extensos cuellos de botella en el aeropuerto. Sin embargo, esto significa que todo el mundo que viaja es sometido a procedimientos de comprobación de confianza. La información complementaria, obtenida a través de controles sistemáticos de la lista de alerta, crea una categoría específica de "otros", es decir, individuos que son menos confiables que otros. Los datos de los viajeros menos fiables (que contienen números de autenticación de transacciones, cuentas bancarias, alias, direcciones de residencia, origen étnico, nacionalidad, socios y a veces, huellas dactilares) despiertan una alarma si el

[26] Cf. <http://cironline.org/reports/us-backs-florida%E2%80%99s-new-counterterrorism-database-%E2%80%98matrix%E2%80%99-offers-law-agencies-faster-access>.

[27] Bases de datos usadas por el Centro Nacional de Terrorismo (NCT por sus siglas en inglés), para los datos del registro de nombres de pasajeros (PNR por sus siglas en inglés): 1) Sistema avanzado de información de pasajeros (APIS por sus siglas en inglés), 2) Sistema de información de no-inmigrantes (NIIS por sus siglas en inglés), 3) Índice de sospechosos y violadores (SAVI por sus siglas en inglés), 4) Sistema de cruce de fronteras (BCIS por sus siglas en inglés), 5) Bases de datos de Visas del Departamento de Estado, 6) datos sobre incautaciones del TECS, y 7) Listas de alerta de terroristas; subconjuntos de la base de datos sobre Terroristas del Gobierno de los Estados Unidos. Fuente: CRS Report 7-5700.

software detecta cualquier signo de comportamientos "anormales" o vinculaciones sospechosas (por ejemplo, sentarse cerca de otro sospechoso en dos ocasiones). Estos viajeros son controlados de nuevo en el aeropuerto y enviados de vuelta si se les considera un peligro para la seguridad nacional.

Como explica Taipale – abogado, erudito y teórico social especializado en información –, la tecnología que utiliza la Fundación Markle para el desarrollo de programas de datos predictivos incluye,

> los métodos de extracción de datos que se utilizan como parte de las prácticas de lucha contra el terrorismo y la seguridad en la frontera [que están]: (i) orientados al sujeto, donde las implicaciones de un individuo son trazadas como partes de una investigación más amplia; y (ii) basadas en patrones, donde se aplica un conjunto de plantillas pre-existentes a una selección de datos, tales como plantillas que proporcionen pistas sobre el comportamiento terrorista[28].

En el segundo caso, se utiliza el procesamiento de datos preventivos o la extracción de datos de perfiles. Este es un cambio metodológico porque las estadísticas no se utilizan para el análisis retrospectivo, sino para análisis en red y análisis de patrones. Por lo tanto, mientras que los datos de un individuo específico se pueden extraer de un gran número de agentes en las redes, también puede determinarse un patrón, una trayectoria, que parece conducir a un comportamiento específico.

Sin embargo, esta pretensión de predicción o incluso de detección, no es eficaz. Si bien la combinación entre bases de datos las conecta entre sí, no necesariamente lo hace con verdaderos comportamientos o intenciones. El propio Departamento de Justicia de los Estados Unidos reconoció este problema en 2005 al afirmar que:

> Se identificaron problemas significativos. Nuestra auditoría de la etapa inicial de consolidación muestra que persistieron problemas adicionales en cómo fueron usadas las listas de no vuelo o de personas seleccionadas para comparar nombres de viajeros entre esas listas. En el nivel de la base de datos de la TSC, el D[epartamento] de J[usticia] encontró numerosos errores, tanto en cómo se llevó a cabo la transferencia de nombres de la lista de alerta y en cómo estos nombres llegaron a codificarse en términos de su nivel de amenaza. En el nivel del algoritmo y del proceso utilizado para comparar listas de viajeros aéreos con la lista de no vuelo o de personas seleccionadas, esto fue considerado también como defectuoso aunque finalmente tolerable para la Oficina de Contabilidad del Gobierno, a pesar del hecho que los algoritmos utilizados para comparar a los viajeros consistentemente produjeron altas tasas de falsos positivos. Esta aceptación de falsos positivos significa no sólo una vuelta hacia la precaución sino que, más importante, evidencia una racionalidad del gobierno que acepta daños

[28] TAIPALE, Kim. Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data.

> colaterales en relación a la prevención del terrorismo; esto es, el sacrificio de derechos individuales o protecciones con el fin de proveer el mayor bien a la seguridad conforme Posner y Vermeule[29].

La construcción de listas de alerta como el elemento práctico de una estrategia política paranoica no es puramente norteamericana, es una práctica transnacional que se aplica no sólo en las fronteras de los EE.UU. sino en la mayoría de las fronteras (aéreas) de los países occidentales. Mientras que la UE participó en la construcción de listas de alerta, la Organización Internacional de Aviación Civil ha promovido vigorosamente el desarrollo de listas de exclusión aéreas informatizadas. Dichas listas colocan a grandes segmentos de la población mundial bajo sospecha para permitir encontrar los datos que son necesarios para elaborar patrones y algoritmos de predicción y construir perfiles que tomen la forma de listas de alerta[30].

El gobierno de Estados Unidos ha sido y sigue siendo un jugador clave. La Ley de Seguridad de la Aviación y el Transporte (ATSA, 2001) requiere del DHS y el Servicio de Aduanas y Protección de Fronteras (CBP por sus siglas en inglés) que recopile y analice los manifiestos tanto de pasajeros como de tripulación de los vuelos internacionales que ingresan al territorio estadounidense. Sin embargo, las acciones de los Estados Unidos han sido seguidas, sino prefiguradas, tanto por los europeos con el Sistema de Información de Schengen como sus contrapartidas en Australia con su sistema de entrada-salida. Ambos han desarrollado recursos aún más sistemáticos de intercambio de información sobre viajeros. La historia del desarrollo de las negociaciones a nivel mundial del PNR y el API no ha sido bien documentada, sin embargo las conexiones entre investigaciones en los EE.UU., la UE, Australia y al nivel de las organizaciones internacionales demuestran que opera la misma lógica: la información proporcionada a operadores privados (tales como corporaciones) para mejorar el servicio hacia los consumidores (por ejemplo, las tarjetas de fidelidad) fue utilizada posteriormente por los organismos de control de fronteras para crear listas de alerta, entre otras cuestiones. Después del 11-S, la lógica de la doctrina del uno por ciento ha empujado a los gobiernos a ampliar el número de agencias que suministran datos y a reorganizar su recopilación a fin de predecir futuros actos de terrorismo, en vez de controlar a los individuos ya considerados sospechosos. De una herramienta útil para conocer las preferencias de los consumidores, el PNR ha pasado a transformarse en un dispositivo de seguridad que recoge estas elecciones para tratar de detectar posibles patrones de peligrosidad. Sistemáticamente, este proceso se ha presentado como un éxito para mantener al mundo a salvo del terrorismo y de la migración ilegal aunque, como muestran los siguientes ejemplos, el proceso se torna a menudo arbitrario,

[29] Departamento de Justicia de los Estados Unidos, citado en KABATOFF, *op. cit.*, p. 139.

[30] WEBER, Cynthia. Design, Translation, Citizenship: Reflections on the Virtual (De)Territorialization of the US-Mexico Border.

incompleto e inexacto. Todos estos factores – la creación del Departamento de Seguridad Nacional, el aumento en cantidad y poder tanto de los organismos dedicados al control fronterizo como de agencias de inmigración, la participación compulsiva en el control de las aerolíneas comerciales y de las agencias de viajes y la informatización total del proceso de visados y entradas a EE.UU. (a través del sistema ESTA, según sus siglas en inglés) –, han movilizado un cuantioso personal con una inversión elevada en el desarrollo y crecimiento de las industrias de vigilancia.

En el nivel institucional, los presupuestos y las ganancias de las compañías y organismos privados dependen actualmente del sostenimiento y expansión de la industria de la vigilancia. En vez de contar tanto con una lista precisa de terroristas peligrosos, identificados a través de la cooperación entre servicios, como con un objetivo específico, determinado por el entrecruzamiento de esa lista con otras listas de viajeros, hoy en día contamos con bases de datos que recogen, almacenan e intercambian información sobre viajeros con la esperanza de individualizar sospechosos – a pesar de que los perfiles de los terroristas son desconocidos. Las búsquedas de datos sobre relaciones localizadas en los sujetos han multiplicado las posibilidades de ser identificados dentro de una lista de terroristas porque solamente un criterio de sujeto es suficiente para encajar dentro de la definición general. El antropólogo Mark Maguire ha descrito en detalle la lógica de algunas de estas tecnologías antiterroristas. Por ejemplo, el programa de Tecnología de Reconocimiento de Atributos Futuros (FAST por sus siglas en inglés) intenta detectar al sujeto potencialmente peligroso a través de determinar su estado mental por medio de tecnologías que miden la reacción cardiovascular, las secreciones corporales y el movimiento ocular. Como explica Maguire, el software puede detectar certeramente el estrés, sin embargo la inferencia del impacto emocional que afecta la peligrosidad/terrorismo es altamente imprecisa, lo cual produce tasas muy altas de falsos positivos. Nadie ha sido condenado exitosamente como terrorista tras ser detenido por la máquina[31]. La mayoría de los investigadores de las ciencias del comportamiento refutan las declaraciones de éxito realizadas por las empresas de seguridad y sus clientes, en parte debido a que todas sus evaluaciones son confidenciales. Es razonable sospechar que la confidencialidad es considerada necesaria debido a que la evidencia existente no apoya el discurso de la prevención ni la lógica de la doctrina del uno por ciento.

De hecho, los analistas de seguridad utilizaron en sus evaluaciones la Teoría del Actor-Red (ANT por sus siglas en inglés), pero aplicándola sin asumir la incertidumbre radical que constituye su episteme exploratoria. En este sentido, han tratado de transformar la ANT en pruebas y argumentos explicativos para justificar

[31] MAGUIRE, Mark. Counter-Terrorism in European Airports. Véase también el trabajo sobre el aeropuerto de San Diego; BIGO, Didier. Dans les filets du contre-terrorisme global.

una lógica preventiva. Sin embargo, ANT enfatiza que las representaciones de "lo real" son meramente una de las múltiples interpretaciones visuales posibles, no la verdad, especialmente si el resultado final es tan singular que tiene correlación con un individuo específico. Evidentemente, la justicia penal y la metodología de enfoques exploratorios de la ANT no pueden ir de la mano. Los analistas de seguridad han depositado su confianza en los números, en la extracción de datos y en las representaciones visuales de las amenazas como una verdad independiente de éstos al mismo tiempo que la construían. Mientras que en privado reconocen que no se trata de una técnica confiable y que nadie puede proyectar de antemano el comportamiento futuro de una persona desconocida, los analistas de seguridad están presionados por la demanda de resultados que el discurso de las agencias de inteligencia precisa entregar. La creencia en la tecnología predictiva transforma al mundo en una tierra de fantasía poblada por máquinas inteligentes. De este modo, las máquinas basadas en el comportamiento, el *software* de las teorías de redes y la extracción de datos han replanteado la noción de terrorismo, extendiéndola a fin de encajar los métodos populares mientras se alejan de sus objetivos originales. En definitiva, ésta no ha sido una respuesta al terrorismo, sino un producto de la política del miedo al terrorismo en la que se utilizan las tecnologías de elaboración de perfiles con el objetivo de "neutralizar", de encubrir las discriminaciones causadas por la política de la sospecha. La transnacionalización, la hibridación de lo público y lo privado y el uso de bases de datos informáticas interoperables funcionan como formas de desresponsabilización de los productos de la demonología política implícita en las listas de alerta. Esto impacta aún más en el caso del rastreo y el control de la circulación de la información digitalizada.

III.B. Trazando y controlando la circulación de información en el espacio cibernético: PRISM y la vigilancia electrónica de gran escala

El segundo tipo de programa que muestra estas lógicas de sospecha es aquel relacionado al trazado, trabajo de datos en gran volumen, espionaje, retención y análisis de todos los medios de comunicación a través del intercambio electrónico de datos de cualquier persona remotamente conectada con individuos que ya se encuentran bajo vigilancia o aquellos considerados blancos útiles para propósitos de seguridad nacional. El programa, o más exactamente el conjunto de programas de interceptación de comunicaciones, fueron mantenidos en secreto durante aproximadamente una década, pero las revelaciones de Edward Snowden, publicadas por los periódicos *The Guardian* y *The Washington Post* el 6 de junio de 2013, revelaron la escala de vigilancia, la intromisión de los servicios de espionaje y la naturaleza de nuestros regímenes. Snowden mostró, en primer lugar, que las autoridades de Estados Unidos están accediendo y procesando la información personal de ciudadanos de la Unión Europea en gran escala por medio de, entre otros, interceptación electrónica sin autorización judicial de tráfico de

internet por cable (UPSTREAM), realizado por la Agencia de Seguridad Nacional (NSA), y mediante acceso directo a la información personal guardada en servidores de empresas privadas con sede en los Estados Unidos, como Microsoft, Yahoo, Google, Apple, Facebook y Skype (PRISM)[32]. Esto permite a las autoridades de Estados Unidos acceder tanto a comunicaciones almacenadas como también a realizar una recolección de datos en tiempo real sobre usuarios específicos. Sin embargo, programas de búsqueda que trabajan datos cruzados como UPSTREAM, PRISM, QUANTUMINSERT, BULLRUN, DISHFIRE y X-KEYSCORE, para nombrar seis de los programas más publicitados, representan apenas la punta del iceberg de la vigilancia de la NSA. En segundo lugar, la agencia de inteligencia del Reino Unido, el Cuartel General de Comunicaciones del Gobierno (GCHQ) ha cooperado con la NSA e iniciado acciones de interceptación bajo diferentes programas, designados con los nombres cifrados de TEMPORA y OPTIC NERVE. Nuevos reportes han surgido implicando un puñado de otros países miembros de la Unión Europea que estarían llevando adelante (Suecia, Francia, Alemania) o desarrollando (potencialmente Holanda) sus propios programas de interceptación de internet a gran escala y colaborando con la NSA en el intercambio de información. Pero esta colaboración es desigual y ciertamente no tiene la intención de crear confianza entre los diferentes servicios ya que los Estados Unidos han espiado a sus aliados más próximos al tiempo que les pedían colaboración, con el objetivo de verificar tanto lo que estaban ofreciendo espontáneamente como aquello que estaban ocultando de la NSA. Han accedido al cable que atraviesa el Medio Oriente operado por el sistema de escuchas telefónicas de la empresa francesa Orange, quien ha lanzado una demanda contra la NSA por violación de comunicaciones privadas[33]. En contrapartida, Francia ha sido acusada de desarrollar un modelo hostil de "*quantum insert*" bajo el nombre cifrado de BABAR, que se dice fue usado contra Canadá y quizás contra los Estados Unidos. Angela Merkel reclamó a la NSA cuando quedó probado que su teléfono celular ("*Handy*" en alemán) había sido intervenido durante muchos años, con la ilusión de asegurar ventaja económica y política para los Estados Unidos. Merkel comparó esta vigilancia con aquella conducida por la Stasi, el infame servicio de inteligencia operado por el gobierno de la Alemania Oriental hasta que éste fue derribado en 1989. En tercer lugar, más allá de los gobiernos de los Estados miembros, tanto instituciones de las Naciones Unidas como instituciones de la Unión Europea y embajadas y representaciones de los Estados miembros de la Unión Europea también fueron blanco de vigilancia y actividades de espionaje por parte de Estados Unidos y el Reino Unido. Por ejemplo el GCHQ del Reino Unido infiltró los sistemas de Belgacom mediante

[32] Esta parte es un extracto proveniente de mi propia contribución a la nota dirigida al Parlamento Europeo: "Programas nacionales de vigilancia masiva de datos personales en los Estados miembro de la Unión Europea y su compatibilidad con la legislación de la UE". Disponible en: <http://bit.ly/1chl2TJ>.

[33] Cf. <http://www.lesechos.fr/30/12/2013/lesechos.fr/0203214421104_nsa---orange-se-porte-partie-civile-apres-le-piratage-d-un-cable-sous-marin.htm>.

un acceso simulado en LinkedIn en lo que fue denominado en nombre cifrado (¿irónicamente o no?) como 'Operación socialista' para ganar acceso a información de instituciones de la Unión Europea (Comisión, Consejo y Parlamento). Parece por lo tanto que la NSA es frecuentemente pero no siempre la creadora de esta vigilancia a gran escala y que la mayor parte de sus operaciones son realizadas mediante redes transnacionales de agencias que cooperan con o sin el conocimiento de sus propios gobiernos. Las preguntas que conciernen a PRISM, Tempora y tantos otros programas compartidos por la NSA, GCHQ y otros servicios de inteligencia son extraordinariamente importantes para la seguridad, la soberanía, las alianzas, el derecho internacional, la obediencia, la subjetivización del ciudadano y los derechos digitales para todos los usuarios de internet independientemente de sus nacionalidades[34]. Para profundizar en esto recurriré a una investigación reciente que he llevado a cabo para el Parlamento Europeo[35].

Esta investigación puso de relieve tres características compartidas por estas operaciones de la creación de las comunicaciones. En primer lugar, son operaciones secretas que afectan directamente la vida cotidiana de toda la población que usa servicios de internet (como e-mail, navegación por la red, servicios de computación en la nube, redes sociales o comunicaciones vía Skype, ya sea mediante computadoras personales o dispositivos móviles), al transformarlos en potenciales sospechosos. Esto es especialmente problemático para aquellos que no están protegidos por derechos ciudadanos dentro del país donde se origina la vigilancia, entrando en la categoría de "inteligencia extranjera".

En segundo lugar, tienen una dimensión de "gran escala", lo que modifica su naturaleza ya que superan en gran medida a lo que alguna vez se llamó vigilancia orientada con orden judicial. Estas operaciones ahora se conectan a capacidades de inteligencia utilizando diferentes formas de vigilancia y distintas plataformas, y pueden llevar a la extracción de datos y la vigilancia masiva.

Una tercera característica, todavía más central e importante, se refiere a que son un híbrido de formas privadas y públicas de co-vigilancia. Esta característica particular es exclusiva para la vigilancia por sistemas electrónicos y cibernéticos. Una gran parte de las comunicaciones electrónicas del mundo, incluyendo cada vez más, información almacenada o procesada dentro de servicios de computación de nube (como Google Drive, Dropbox, Salesforce, Amazon, Microsoft y Oracle) pueden ser interceptadas mediante tecnologías colocadas por una red transnacional de agencias de inteligencia especializadas en recopilar

[34] BAUMAN, Zygmunt *et alii*. After Snowden, Rethinking the Impact of Surveillance.

[35] BIGO, Didier *et alii*. *Fighting Cyber Crime and Protecting Privacy in the Cloud*. Véanse las dos notas dirigidas al Parlamento Europeo: "Programas nacionales de vigilancia masiva de datos personales en los Estados miembro de la Unión Europea y su compatibilidad con la legislación de la UE"(2013), PE 493.032; "La Agencia de Seguridad Nacional norteamericana (NSA), sus programas de vigilancia (PRISM) y el Acta de Vigilancia en el Extranjero (FISA) y su impacto en los derechos fundamentales de los ciudadanos de la Unión Europea" (2013) PE 474.405.

datos, cuyo líder parece ser la NSA. La NSA lleva a cabo vigilancia mediante varios programas y colaboraciones estratégicas. Mientras que el mayor porcentaje del tráfico de internet se cree que es recolectado directamente en las raíces de la infraestructura de comunicaciones (accediendo a la columna vertebral de las redes de telecomunicaciones distribuidas alrededor del mundo), la reciente exposición del programa PRISM reveló que el tráfico restante es interceptado mediante la recolección secreta de datos y la extracción de información de nueve empresas con base en los Estados Unidos: Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL y Apple. Por lo tanto, los programas de vigilancia no sólo implican la participación de gobiernos y de una red de servicios de inteligencia, sino también la participación "forzada" de los proveedores de internet a través de una colaboración público-privada (PPP por sus siglas en inglés).

Sobre la base de las provisiones de la ley FISA de los Estados Unidos, la NSA, con una "certificación"anual de la corte FISA (FISC), puede tener como objetivo a cualquier ciudadano no estadounidense o residente legal no estadounidense radicado fuera del territorio de los Estados Unidos para su vigilancia. Estos datos, una vez interceptados, son filtrados y la información sospechosa es conservada por la NSA y GCHQ. Los datos almacenados pueden luego ser agregados a otros datos y ser inspeccionados mediante programas específicamente diseñados como el X-KEYSCORE. Además, los proveedores de acceso a internet en los Estados Unidos (y también en Europa) se encuentran bajo la obligación de guardar sus datos por un cierto periodo, para dar a las agencias policiales la oportunidad de conectar una dirección de IP con una persona específica bajo investigación. Las obligaciones legales concernientes al acceso de datos y derogación de leyes de privacidad varían de acuerdo a una serie de factores, incluyendo los proveedores de internet asociados y los servicios de inteligencia, y la nacionalidad de las personas bajo sospecha en relación a la nación que conduce la investigación.

La publicación de las revelaciones de Snowden en *The Guardian* y *The Washington Post* generó gran controversia sobre la legitimidad de esta forma de recopilar datos. Se evidenció que la recolección de datos a gran escala debe ser entendida junto con una gama de servicios de inteligencia intrincadamente vinculados e insertados en las actividades e intereses de sus contratistas privados. Primero, la recolección de datos es usada a veces en un contexto de actividades antiterrorismo o antiespionaje que siguen la lógica de la justicia criminal, pero esto está lejos de ser el panorama completo. Segundo, las actividades antiterroristas frecuentemente proceden a la identificación de personas desconocidas relacionadas a un grupo inicial de sospechosos, dentro de lo que es llamado como los tres grados de separación (o saltos). Esto es, para una persona sospechosa con cien amigos en el primer salto, la persona a cargo de la vigilancia en la NSA o uno de sus subcontratistas puede, sin orden judicial, colocar bajo vigilancia a todas

las 2.669.556 conexiones potenciales en el tercer salto[36]. Tercero, las prácticas de extracción de datos son usadas para actividades de espionaje cibernético dirigidas a grupos específicos con un enfoque de estrategia militar, las cuales no se ocupan de individuos específicos y sus datos personales, sino que recogen información anónima para discernir tendencias en el comportamiento de la población general. Finalmente, actividades de vigilancia electrónica masiva a veces son llevadas a cabo sin objetivos claros, pero son almacenadas en caso de que puedan ser útiles en el futuro, para los usos de los servicios o para información en relación a las variaciones en el consumo o las modificaciones de opinión (incluso aquellas que son políticas y religiosas).

Considerando estos usos variados y las justificaciones, se torna claro que la cuestión central es la naturaleza, escala y profundidad de la vigilancia que puede ser tolerada en y entre democracias. Aquí es donde el desplazamiento hacia una política paranoica permite que la rama del poder ejecutivo se libere a sí misma de la supervisión resulta una cuestión central, ya que afecta la naturaleza misma del régimen.

IV. Vigilancia, servicios de inteligencia y democracia

IV.A. Una vieja relación dentro de las "sociedades abiertas"

La vigilancia de ciudadanos no es un fenómeno nuevo en regímenes políticos liberales. Grupos específicos de individuos con frecuencia han sido blanco de servicios de inteligencia al ser sospechados de conducir actividades criminales (incluso violencia política). Aunque los regímenes democráticos no hayan ido tan lejos como los autoritarios, donde los cuerpos de inteligencia sistemáticamente espían a sus propias poblaciones para detectar el disenso (tales como la Stasi en la antigua República Democrática de Alemania, el Securitate en Rumania o el UDBA en la antigua Yugoslavia), tienen sin embargo una historia de vigilancia a gran escala.

Los propósitos y la escala de vigilancia están precisamente en el corazón de lo que diferencia a los regímenes democráticos de los Estados policiales. Incluso si se han producido transgresiones en el pasado, en principio los servicios de inteligencia en regímenes democráticos no recogen datos masivos de grandes grupos al interior de su población. Además, si individuos específicos comienzan a ser vigilados, ello debe estar legalmente justificado como necesario para detectar

[36] Barack Obama, siguiendo una de las 45 recomendaciones del grupo de revisión sobre inteligencia y tecnología de la comunicación, entregado el 12 de diciembre de 2013, parece dispuesto a limitar la búsqueda sin orden judicial a dos saltos (en este caso 16.340), reduciendo la escala de la búsqueda mientras mantiene el principio activo. Discurso 17/01/2014, disponible en línea en *The Guardian*: <http://www.my-rss.co.uk/feeditem.php?feed=0&word=&search=laws&item=263734> (consultado el 19/03/2014). Para una búsqueda interactiva sobre los saltos, véase: <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> (consultado el 19/03/2014).

y prevenir acciones violentas, no meramente para reunir información sobre estilos de vida u opiniones políticas. Este 'acuerdo' informal, un entendimiento compartido entre el Estado y sus ciudadanos está bien capturado en esta cita: "Nuestro gobierno en su propia naturaleza y nuestra sociedad abierta en todo su sentido, bajo la Constitución y la Carta de Derechos de los Estados Unidos automáticamente proscribe organizaciones de inteligencia del tipo que han sido desarrolladas en estados policiales"[37].

Sin embargo, cuando las defensas contra la vigilancia total no son controladas regularmente, pueden dejar de operar. En nombre del desarrollo de altas tecnologías y su posible uso por parte de 'enemigos', los servicios de inteligencia han cruzado estas fronteras para perseguir su misión. Este estiramiento excesivo de la seguridad nacional puede ser atribuido parcialmente a una frecuente redefinición de quién es el enemigo (o el sospechoso), y hasta dónde se considera que éste ha infiltrado el territorio. Sin embargo, en democracias, donde se espera que haya una separación de poderes, los excesos de los servicios de inteligencia han sido regularmente denunciados cuando sus actividades ilícitas han sido descubiertas.

Antes de PRISM, las autoridades de Estados Unidos fueron condenadas en numerosas ocasiones por vigilar e infiltrar ciertos grupos. Por ejemplo, movimientos por los derechos civiles y comunistas fueron los blancos en la década de 1950, y los movimientos contra la guerra se convirtieron en el foco en las décadas de 1960 y 1970. Programas secretos que usaban informantes, correo y llamadas telefónicas interceptadas, y actividades de piratería planificadas – tales como COINTELPRO a fines de la década de 1950, así como CHAOS y MINARET en la década de 1960 y 1970 – fueron todos condenados posteriormente como programas de vigilancia ilícitos. Todos ellos dieron origen a reglas específicas para proteger personas estadounidenses de ese tipo de vigilancia política. El tribunal de la Ley de Vigilancia a la Inteligencia Extranjera (FISA por sus siglas en inglés) fue específicamente concebido en 1978 para neutralizar estas restricciones y dar al sistema judicial el poder para supervisar actividades declaradas como "inteligencia extranjera", especialmente aquellas que se consideraba estaban afectando derechos fundamentales de los ciudadanos estadounidenses. Como se ha detallado en otro lugar, esta corte ha visto su poder constantemente debilitado, incluso con más énfasis luego del 11-S y la puesta en marcha de la guerra contra el terrorismo[38]. El objetivo de este tribunal también está limitado a la protección de ciudadanos estadounidenses; personas no-estadounidenses que son víctimas de vigilancia ilícita están excluidas. Las actividades actuales de PRISM y otras de la

[37] DULLES, Allen Welsh. *The Craft of Intelligence*, p. 4.

[38] SCHIFF, Adam, ROKITA, Todd., "Republicans and Democrats agree: Fisa oversight of NSA spying doesn't work. 'Secret law'is anathema to our democratic traditions and the rule of law. We have introduced legislation to change this". *The Guardian*, 29 de julio de 2013.

NSA, y aquellas de otros servicios de inteligencia y empresas privadas de los Estados Unidos, todos demuestran el debilitamiento de los poderes del sistema judicial ante las actividades de inteligencia. Implementar una supervisión estatal o parlamentaria sobre dichas actividades se torna más complicada dada la participación de actores y corporaciones del sector privado en iniciativas de vigilancia global.

En Europa, una serie de escándalos surgieron cuando prácticas de vigilancia policial encubierta y vigilancia de partidos políticos pusieron en riesgo libertades civiles, pero estaban más vinculadas a infiltraciones y operaciones secretas que a vigilancia masiva. En España, la creación de Grupos Antiterroristas de Liberación (GAL) para combatir el grupo separatista vasco ETA terminó en 1996 con la condena y detención del antiguo Ministro del Interior. En Francia, los *Renseignements Généraux* fueron amenazados de cerrarse luego de que una serie de actividades ilegales fueron reveladas, incluyendo escuchas telefónicas y el presunto asesinato de Pasteur Doucé, un activista gay, en la década de 1990. Más recientemente, en junio de 2013, el Primer Ministro de Luxemburgo Juncker anunció oficialmente que iba a dimitir debido a un escándalo de espionaje que envolvía escuchas telefónicas a figuras políticas, pero no lo hizo, y aún así es considerado un buen candidato para ser el próximo presidente de la Comisión Europea.

Aunque cuestionada y dificultosa, la necesidad de supervisar las actividades de inteligencia por parte de autoridades parlamentarias o judiciales ha sido ampliamente aceptada desde la década de 1990. Los servicios de inteligencia franceses aceptaron apenas recientemente un procedimiento de control externo. Los *Renseignements Généraux* han sobrevivido en parte bajo la DCRI, pero sus misiones han sido reorientadas. Estos servicios siempre insistieron en que se enfocaban en casos específicos de espionaje o violencia política, o que estaban emprendiendo encuestas de opinión que eran mejores que aquellas que investigadores o compañías privadas podían proveer. Como se detallará a continuación, la especificidad de la vigilancia a gran escala desafía estas afirmaciones supuestamente alentadoras y suscita interrogantes sobre las conexiones entre servicios a cargo del antiterrorismo y aquellos responsables de recoger datos para la vigilancia a gran escala.

La guerra contra el terrorismo fue lanzada luego de que los eventos del 11-S socavaran el frágil consenso acerca de que las democracias no realizan vigilancia masiva y que deben aceptar la supervisión judicial. En los Estados Unidos, y en menor grado en Europa, una serie de programas han sido iniciados secretamente, utilizando recursos existentes de moderna tecnología de la información. Las posibilidades de vigilancia han aumentado al mismo ritmo que aumentó la disponibilidad de datos. Los incrementos regulares en el ancho de banda han permitido nuevos usos de la internet como el almacenaje masivo y el procesamiento de datos personales, privados y gubernamentales, mediante servicios de computación en la nube. El desarrollo de dispositivos de computación

móviles (por ejemplo, *smartphones* y *tablets*) ha ofrecido un gran cúmulo de valiosa información personal y geolocalizada.

Cada vez que un escándalo tiene lugar, como los relacionados al SWIFT y TFTP y sus repercusiones en la Unión Europea y en los Estados Unidos, la demanda de supervisión sobre las actividades de inteligencia por parte de autoridades parlamentarias y/o judiciales gana más legitimidad. Claramente las modalidades e implementación de la supervisión se mantienen como problemáticas debido a que los programas de vigilancia, como he documentado en este artículo, son transnacionales y tienen un alcance global, pero también porque estos servicios envuelven sus actividades con un velo de secretismo (el argumento de 'información clasificada'). La presunta dificultad en trazar una línea entre los intereses del Estado y aquellos de un partido específico o grupo político (cuando ellos no son intereses puramente privados) sólo exacerba el problema existente. Además, cuando los programas están conduciendo vigilancia de alcance mundial sobre ciudadanos de otros Estados sin el conocimiento de estos ciudadanos, e incluso a veces sin el conocimiento de sus gobiernos, la pregunta ya no refiere a la protección de datos y privacidad individual sino sobre la sobrevivencia de la democracia en sí misma.

IV.B. La vigilancia masiva en la democracia a través de la generalización de la sospecha, la prevención y las listas de alerta: ¿un cambio de escala que afecta a la naturaleza del régimen?

Lo que debe cuestionarse aquí es la posible transformación de la vigilancia a gran escala limitada al terrorismo en lo que puede denominarse como una 'cibervigilancia masiva' que permite el acceso irrestricto a datos en una magnitud sin precedentes. Dicha vigilancia, argumento, amenaza la naturaleza del régimen político liberal.

Irónicamente fue la investigación del Parlamento Europeo acerca del programa ECHELON de la NSA la que, entre 2000 y 2001, reveló que los programas de vigilancia eran capaces de interceptar las comunicaciones globales y revisar el contenido de las llamadas telefónicas, los fax, los correos electrónicos y otros intercambios de datos. Como informó el denunciante Duncan Campbell al Parlamento Europeo, ECHELON era parte de un sistema de vigilancia global que involucraba la cooperación de las estaciones satelitales administradas por Gran Bretaña, Canadá, Australia y Nueva Zelanda. El informe de Campbell generó gran preocupación al asegurar que ECHELON se había alejado de su propósito original de defensa frente al bloque del Este y estaba siendo utilizado con propósitos de espionaje industrial[39].

[39] CAMPBELL, Duncan. Inside Echelon: the History, Structure, and Function of the Global Surveillance System known as Echelon.

Desde 2004, luego de ECHELON, se iniciaron una serie de programas en Estados Unidos y en Europa con el desarrollo de plataformas integradas, con posibilidad de romper las claves informáticas de cifrado, y con la adopción de un nuevo *software* que permite filtraciones de manera sistemática. Todo esto posibilitó que volúmenes sin precedentes de datos y metadatos puedan ser visualizados y correlacionados. Estos nuevos recursos para la vigilancia, más el uso generalizado de teléfonos móviles inteligentes y la posibilidad del almacenamiento de datos *online*, hicieron que se diluya la línea entre la 'vigilancia selectiva' – justificada por la lucha contra el crimen – y la extracción de datos generalizada, lo cual conlleva el riesgo de una vigilancia ilimitada.

Estos programas se justificaron encarnando la voluntad de proteger a la población del crimen y proporcionaron herramientas para ayudar a delinear perfiles de personas susceptibles de cometer tales delitos. Sin embargo, una vez que los datos estuvieron disponibles para su búsqueda y extracción, se usaron con otros fines. Uno de tantos intentos para ampliar el alcance de la vigilancia fue el programa Conocimiento Total de la Información (TIA por sus siglas en inglés), el cual fue rechazado en 2003 por el Congreso estadounidense al aducir la "desviación de su uso", aunque (al menos públicamente) estaba limitado al Conocimiento de Información sobre Terrorismo[40]. No obstante, se ha practicado tanto la idea de escuchas telefónicas sin orden judicial como búsqueda de datos globales. El TIA no desapareció aunque fue fuertemente denunciado por el senador Ron Wyden en el Congreso de Estados Unidos, y fue legalizado de facto en 2007 por la Ley de protección estadounidense. Es nodal el modo en que el TIA se justifica, ya que dentro de esta justificación es que subyace la política paranoica estableciendo el nexo entre la doctrina del uno por ciento y su implementación en el corazón de la producción de sistemas de bases de datos interconectados para patrones predecibles. Lo que resulta extraordinario cuando uno lee el documento del TIA es que allí se asuma una correlación equitativa entre el mundo físico y el mundo electrónico. En su núcleo yace la creencia en la capacidad del cálculo probabilístico vía algoritmos, a través de modelos de análisis predictivo que conectan el pasado, presente y futuro, a fin de hallar lo que no se puede encontrar en el mundo físico, es decir, una predicción definitiva del futuro. Esta creencia, y la política del miedo que la alimenta, se asienta sobre una imaginación política que predice el caos en el caso que la vigilancia sea limitada de cualquier manera. El caos por venir es variadísimo: el terrorista con una bomba nuclear en el equipaje, la invasión de extranjeros que se benefician de la hospitalidad de aquellos que los han recibido, la posibilidad de cambios climáticos drásticos, la destrucción de la economía de mercado y la posibilidad de una epidemia de gran escala en la que los virus pasan desde los animales a las personas. Se supone que cada uno de estos escenarios debe ser prevenido por una recolección de datos cada vez mayor. Sin embargo,

[40] HARRIS, Shane. *The Watchers, the Rise of America's Surveillance State*.

la seguridad no podría asegurarse si las organizaciones encargadas se encuentran restringidas por órdenes judiciales y limitaciones parlamentarias.

Esta creencia fue articulada por John Poindexter, quien estuvo en el corazón del escándalo del *contra-gate* en Nicaragua y más tarde fue jefe de la Oficina de Conocimiento bajo la gestión de George Bush, en el documento llamado "Información total de conocimiento" (un documento que puede ser el equivalente del panóptico de Jeremy Bentham en la era moderna). En diciembre de 2003, la propuesta de reforma de Poindexter fue bloqueada por el Congreso de Estados Unidos, aunque sus esfuerzos sentaron las bases para la vigilancia actual. Los principios que rigen esta nueva realidad son que el sistema sólo está inspeccionando objetivos específicos, quienes ya son sospechosos, asumiendo que la recolección de datos por lo general no perjudica a las personas que no tienen nada que ocultar. La libertad, por lo tanto, no está en juego, únicamente los criminales son quienes tienen que estar preocupados. El conocimiento de la información tiene que conectar todos los puntos para evitar vacíos y es por eso que es necesario el conocimiento total de la información. El *software* se está volviendo tan inteligente que los patrones emergentes de discernimiento analítico a través de los algoritmos que pueden descubrir patrones que los simples seres humanos no pueden. Las asociaciones específicas pueden ser visualizadas y usadas a fin de priorizar las amenazas.

Finalmente, el TIA fue rechazado, pero sólo porque el Congreso de los Estados Unidos no consideró ético el surgimiento de los mercados de predicción (con sus apuestas sobre en qué parte del país se producirían nuevos atentados). A pesar de esto, parece ser que el horizonte de conocimiento ha sido establecido y que cada argumento en su contra representa un modo rudimentario de resistencia al liberalismo, el cual debe ser superado. El programa Conocimiento Total de la Información se ha renombrado como Conocimiento de la Información Terrorista, limitando sus propósitos a la lucha contra el terrorismo, el crimen organizado y la seguridad nacional. Sin embargo, se han creado otros programas para eludir esta restricción y conectar puntos entre las listas negras del terrorismo y las listas de alerta y el control fronterizo además de la internet y las telecomunicaciones. Las revelaciones recientes acerca de las actividades de la NSA (por ejemplo, los programas PRISM y Xkeyscore) parecen demostrar que existe una continuidad entre los programas que precedieron y siguieron al TIA. Esto plantea una pregunta central: ¿Hasta dónde los programas PRISM (en EE.UU.) y Tempora (en el Reino Unido) siguen la lógica del TIA, del proyecto original del síndrome del uno por ciento y de una doctrina de políticas paranoicas? ¿Estos dos programas mantienen un propósito limitado al terrorismo y al crimen? ¿O los datos también se utilizan para la evasión de impuestos, para que algunas empresas privadas obtengan ventajas en su búsqueda de contratos, para tipificar las opiniones políticas de grupos considerados marginales o para elaborar escenarios sobre conflictos políticos y otras situaciones internacionales?

La preocupación se ha centrado en la percepción de que estos programas operan interconectados y que algunos servicios de los Estados miembros de la UE participan en las extracciones de datos de internet para "exploraciones" con múltiples propósitos. De hecho, Snowden afirmó que los datos recopilados por el programa Tempora son compartidos con la NSA y que no hay distinción entre la recopilación de datos de ciudadanos particulares y de sospechosos. Pero el GCHQ ha subrayado que los datos no se usaban para búsquedas generalizadas y que su utilidad era limitada a la seguridad nacional, puntualmente a la detección y prevención del crimen. Uno puede preguntar: ¿Dónde está la "línea roja" que no pueden cruzar los servicios de inteligencia en los regímenes democráticos cuando utilizan la cibervigilancia? Si esta "línea roja" es reconocida, ¿es compartida por EE.UU. y la UE? ¿Qué pueden hacer los órganos de supervisión en ambas regiones si en frente tienen una red de agencias de inteligencia y proveedores privados, es decir, una asociación a escala internacional de profesionales de la intranquilidad?

Conclusión. La vigilancia a gran escala y la vigilancia masiva: el vínculo a través de políticas paranoicas

Este trabajo insiste en que actualmente tenemos evidencia sobre las diferencias existentes entre la escala y la profundidad de los programas conectados a PRISM y FiveEyes Plus Group, en comparación con los que previamente se pusieron en práctica en nombre de la lucha contra el terrorismo y el contra-espionaje. Volviendo a la pregunta central: ¿Es esta vigilancia a gran escala una forma de política paranoica que puede poner en peligro a la democracia? No tengo la respuesta, pero este debate merece tomarse en serio en lugar de rechazarse de plano. Esto significa que una manera de ver el mundo y de expresarse está dándose a conocer a y siendo compartida por el grupo que está enmarcando estas actividades en términos de seguridad y de riesgo. Esto representa una trasformación de las políticas cotidianas. Por lo tanto, es útil establecer una comparación con otros períodos, entre ellos el surgimiento del maccartismo. Aunque esta comparación puede parecer demasiado fuerte, constituye la genealogía de las políticas paranoicas que pueden surgir de la vigilancia a gran escala. Estos "productos" son el resultado de la emancipación del control de diferentes asociaciones de profesionales de la (in)seguridad y servicios de inteligencia a través de la construcción de una demonología política que creó una figura demoníaca: el/la sospechoso/a quien tiene que ser impedido/a de actuar por medio de la anticipación y predicción de su comportamiento.

La figura del sospechoso no es específicamente la de un enemigo criminal (interno o externo). Aquí los límites de la delincuencia y el enemigo son en sí mismos desestabilizados. La imagen no es naturalizada a través del nacionalismo y el patriotismo; es una prueba que cada individuo, responsable por su propia libertad, debe pasar antes de unirse al grupo de personas confiables, quienes

tienen el derecho de ser protegidas de otras. Por lo tanto, se legitima la obtención de información sobre nuestras acciones y pensamientos a través de los servicios de inteligencia. Se afirma que esto no afecta la libertad de nadie porque la intención no es espiar, así como sucede en los regímenes no democráticos, sino verificar si la persona puede ser confiable. Por ende, esta prueba tiene que realizarse continuamente ya que la persona puede ir cambiando con el tiempo. Si se pasa la prueba (comenzando por la autenticación de la identidad por medio de la biometría y la verificación discursiva comparada con la información almacenada en las bases de datos) la persona es normalizada/certificada y se unirá a los viajeros felices que se benefician desde su casa de los servicios personalizados que ofrecen proveedores de servicios mundiales a través de internet. En caso contrario, si existen dudas, la persona será observada, a-normalizada (aunque sin transformarse inmediatamente en un enemigo o excluido), e ingresada en los datos bajo una de las tantas categorías que alertan un comportamiento que podría conducir en el futuro hacia un delito o hecho terrorista.

Es en este proceso que surge la justificación de la vigilancia a gran escala, la cual imbrica al mundo del intercambio de información con los servicios de inteligencia y los servicios de lucha contra el terrorismo. Sus capacidades para conectar lo capturado, sin intención o para otros fines, por parte de ensamblajes heterogéneos de técnicas de vigilancia y por la auto-exposición en las redes sociales es considerado normal sólo porque es tecnológicamente posible. Este esquema otorga la racionalidad para que, en vez de un diálogo cara a cara, las máquinas "inteligentes" recolecten gran cantidad de información sobre los viajeros. La "inteligencia" es un proceso de certificación técnica que le permite a la persona transformarse en confiable para evitarse así un mayor control y acelerar su viaje. Ella depende de sus datos por duplicado, porque el rechazo presupone su clasificación en una lista de alerta.

En mi opinión, es de máxima importancia comprender las técnicas utilizadas por las plataformas de integración de la información y la racionalidad bajo la cual se permite la recolección de datos personales a gran escala (tales como la localización de las personas; el mapeo de las relaciones que tienen; la identificación de sus coordenadas con un grupo específico de "sospechosos" relacionándolo con el lugar donde viajan; puntualizar dónde ellos están – o sus computadoras –, con quiénes hablan, lo que dicen y quiénes son). Esta es una forma específica de vigilancia que no es retomada por el debate académico entre la visión centralista del panóptico *versus* las herramientas descentralizadas y heterogéneas de los ensamblajes de vigilancia. Esta parece ser una discusión pasada de moda, ya que la figura del sospechoso, quien tiene que ser certificado a cada paso, y el desarrollo de plataformas de integración de datos tienen que encontrar una manera de organizarse simultáneamente a través de la noción de la recopilación de datos a gran escala para búsquedas selectivas. El estilo paranoico está actualmente

impregnando el lenguaje técnico y, aunque es menos descollante, es más profundo en términos de gubernamentalidad de las poblaciones.

Glosario

Club de Berna: Es un foro compartido entre los servicios de inteligencia de los 28 Estados de la Unión Europea (UE), además de Noruega y Suiza, llamado así por la ciudad de Berna. Es una institución basada en el intercambio voluntario de secretos, experiencias y puntos de vista así también como de debate de problemas. El Grupo Antiterrorista (CTG por sus siglas en inglés) es una extensión del Club de Berna que comparte información de inteligencia sobre terrorismo. Proporciona, asimismo, evaluaciones de las amenazas a los responsables de la elaboración de políticas de la UE y ofrece una modalidad de colaboración entre expertos. El CTG, como el Club de Berna, se encuentra por fuera de las instituciones de la UE aunque está comunicado con el ámbito comunitario europeo a través de su participación en el Centro de Análisis de Datos de Inteligencia (INTCEN, según sus siglas en inglés). Aunque está fuera de la UE, su presidencia rota en línea con la del Consejo de la UE y actúa como una interfaz formal entre el Club de Berna y la UE.

Europol (acrónimo de Oficina Europea de Policía): Es la agencia policial de la Unión Europea que se encarga de la inteligencia criminal. Europol no tiene poderes ejecutivos. Es un servicio de apoyo a los organismos del orden público de los Estados miembros de la UE y entrega análisis estratégico proveniente del intercambio de información sobre terrorismo (TESAT) y sobre crimen organizado (SOCTA). Comenzó a funcionar plenamente el 1 de julio de 1999. Europol asigna los recursos desde su sede central en La Haya: tiene 800 empleados, y de éstos aproximadamente 145 son Funcionarios de Enlace de Europol (ELOS, por sus siglas en inglés). El tamaño de Europol opaca el hecho de que hay una constante vinculación con cientos de diferentes organizaciones policiales, que a su vez cuentan con su propio apoyo individual o grupal para contribuir con las actividades de Europol. A partir de 2013, Europol abarca a los 28 Estados miembros de la UE. Con el fin de luchar eficazmente contra el crimen organizado internacional, Europol coopera con terceros países y organizaciones. Los 15 países (en orden alfabético) son: Albania, Australia, Bosnia y Herzegovina, Canadá, Colombia, Estados Unidos, Federación Rusa, Islandia, Moldavia, Noruega, Serbia, Suiza, República de Macedonia, Turquía y Ucrania.

Five Eyes: Abreviado como FVEY, refiere a una alianza anglófona que comprende a Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos. Estos países están vinculados por el Acuerdo multilateral UKUSA, un tratado de cooperación conjunta en inteligencia de señales. A fines de la década de 1990, la existencia de ECHELON fue revelada al público, desencadenando un gran debate en el Parlamento Europeo y, en menor medida, en el Congreso de Estados Unidos. Desde 2001, como parte de los esfuerzos para ganar la Guerra contra el Terrorismo, el FVEY amplió sus capacidades de vigilancia enfatizando el monitoreo de la web.

El excontratista de la NSA, Edward Snowden, ha descripto a Five Eyes como una "organización de inteligencia supranacional que no responde a las leyes de sus propios países". Los documentos filtrados por Snowden en 2013 han revelado que el FVEY ha espiado intencionalmente a cada ciudadano de los países miembros, compartiendo la información recolectada para así esquivar las restrictivas regulaciones nacionales sobre espionaje.

GCHQ: El Cuartel General de Comunicaciones del Gobierno (GCHQ por sus siglas en inglés) es la agencia de inteligencia británica responsable de proveer inteligencia vía la intercepción de señales (SIGINT por sus siglas en inglés) y garantizar con ello información al gobierno británico y las fuerzas armadas.

NSA: Es la Agencia Nacional de Seguridad de los Estados Unidos (NSA por sus siglas en inglés) responsable del monitoreo global, la recolección, decodificación, traducción y análisis de información y datos para propósitos de inteligencia y contrainteligencia en el extranjero, una disciplina conocida como inteligencia de señales. La NSA se encarga también de la protección de los sistemas de comunicación e información del gobierno estadounidense contra la infiltración y las guerras en la red.

PNR: En las industrias de las aerolíneas y de viajes, el registro de nombres de pasajeros (PNR por sus siglas en inglés) es un registro en la base de datos del sistema informático de reservas (CRS por sus siglas en inglés) que posee el itinerario de un pasajero o un grupo de pasajeros que viajan juntos. El concepto de un PNR fue introducido por primera vez por las compañías aéreas que necesitaban intercambiar información sobre las reservas en el caso de que los pasajeros necesitasen vuelos de distintas compañías para llegar a su destino ("interlíneas"). Con esta misiva, IATA y ATA han definido normas para la comunicación entre compañías aéreas del PNR y otras bases de datos a través de los llamados "Procedimientos ATA/IATA de comunicación entre aerolíneas para la gestión de reservas de pasajeros" (AIRIMP por sus siglas en inglés). No existe una norma general de la industria para el diseño y el contenido de un PNR. En la práctica, cada CRS o sistema de registro tiene sus propios estándares privados, a pesar de que las necesidades comunes de la industria, incluyendo la de cotejar fácilmente los datos del PNR con los mensajes del AIRIMP, ha dado lugar a que los principales sistemas tengan muchas similitudes en el contenido y el formato de datos. Cuando un pasajero reserva un itinerario, el agente de viajes o el usuario del sitio web de viajes creará un PNR en el sistema de reservas informático que utiliza. Comúnmente este suele uno de los grandes Sistemas de Distribución Global, tales como Amadeus, Sabre, Worldspan o Galileo, pero si la reserva se hace directamente con una aerolínea, el PNR puede estar también en la base de datos del CRS de la aerolínea. Este PNR se denomina el PNR Maestro tanto para el pasajero como para el itinerario asociado. El PNR es identificado en una base de datos específica por un localizador de registros.

SIS: El Sistema de Información de Schengen (SIS) es una base de datos gubernamental utilizada por los países europeos para mantener y distribuir

información sobre individuos y sobre bienes de propiedad que sean de interés. Los usos previstos de este sistema son para fines de seguridad nacional, control de fronteras y control policial. El SIS II, la segunda versión del sistema, está actualmente operativo bajo la responsabilidad de la Comisión Europea. En el SIS hay más de 46 millones de entradas (llamadas alertas), que incluyen principalmente documentos de identidad perdidos. Las alertas sobre personas representan alrededor del 1,9% de la base de datos (aproximadamente 885.000 registros). Cada una contiene elementos de información tales como: nombre y apellido, inicial del segundo nombre, fecha de nacimiento, sexo, nacionalidad, apodos que puedan estar usando, antecedentes sobre si la persona portó armas y/o fue violenta, motivo del alerta y la acción a tomar si la persona es encontrada.

TAN: Algunos servicios bancarios en línea utilizan el Número de Autenticación de Transacción (TAN por sus siglas en inglés) como una forma simple de garantizar contraseñas de un solo uso para autorizar transacciones financieras. Los TAN son un segundo nivel de seguridad por sobre y más allá de las contraseñas únicas tradicionales de autenticación. En caso de robo de un documento físico o ficha que contenga los TAN, éste será de poca utilidad sin la contraseña; por el contrario, si se obtienen los datos de inicio de sesión en la web, ninguna transacción puede realizarse sin un TAN válido.

Bibliografía

ARADAU, Claudia; MUNSTER, Rens. *Politics of Catastrophe: Genealogies of the Unknown.* Londres y Nueva York: Routledge, 2011.

BAUMAN, Zygmunt *et alii*. After Snowden, Rethinking the Impact of Surveillance. *International Political Sociology*, v. 8, n. 2, 2014, p. 121-144.

BIGO, Didier. La mondialisationde l'(in)sécurité. *Cultures & Conflits*, n. 58, 2005, p. 53-101.

BIGO, Didier. Dans les filets du contre-terrorisme global. *Le Monde Diplomatique*, 2008, p. 26-28.

BIGO, Didier. The Transnational Field of Computerised Exchange of Information in Police Matters and its European Guilds. In KAUPPI, Niilo; RASK MADSEN, Mikael (eds.). *Transnational Power Elites: The New Professionals of Governance, Law and Security*. Londres/Nueva York: Routledge, 2013, p. 155-182.

BIGO, Didier *et alii*. *Fighting Cyber Crime and Protecting Privacy in the Cloud.* Bruselas: Parlamento Europeo, 2012.

BIGO, Didier; DELMAS-MARTY, Mireille. The State and Surveillance: Fear and Control. In *La Clé des Langues,* 23 de septiembre 2011. Disponible en: http://cle.ens-lyon.fr/anglais/the-state-and-surveillance-fear-and-control-131675.kjsp.

CAMPBELL, Duncan. Inside Echelon: the History, Structure, and Function of the Global Surveillance System known as Echelon. *Telepolis*, 25.07.2000.

CEYHAN, Ayse; PÉRIÈS, Gabriel. L'ennemi intérieur: une construction politique et discursive. *Cultures & Conflits*, n. 43, 2001, p. 100-112.

DE GOEDE, Marieke. The SWIFT Affair and the Global Politics of European Security.

Journal of Common Market Studies, v. 50, n. 2, 2012, p. 214-230.

DULLES, Allen Welsh. *The Craft of Intelligence*. Nueva York: Harper &Row , 1963.

HARRIS, Shane. *The Watchers, the Rise of America's Surveillance State*. Nueva York: The Penguin Press, 2010.

HOFSTADTER, Richard. *The Paranoid Style in American Politics, and Other Essays*. Cambridge, MA: Harvard University Press, 1996.

KABATOFF, Mathew. *Subject to Predicate. Risk, Governance and the Event of Terrorism within post-9/11 U.S. Border Security*. Tesis doctoral (Sociología). Londres: London School of Economics and Political Science (LSE), 2010.

MAGUIRE, Mark. Counter-Terrorism in European Airports. In MAGUIRE, Mark; FROIS, Catarina; ZURAWSKI, Nils (eds.). *The Anthropology of Security: Perspectives from the Frontline of Policing, Counter-Terrorism and Border Control*. Londres/Nueva York: Pluto Press, 2014.

MARX, Gary. La sociétéde sécurité maximale. *Déviance et société*, v. 12, n. 2, 1988, p. 147-166.

POSNER, Richard. *Frontiers of Legal Theory*. Cambridge: Harvard University Press, 2004.

ROGIN, Michael Paul. *McCarthyism and Agrarian Radicalism*. Chicago: University of Chicago, 1962.

ROGIN, Michael Paul. *The Intellectuals and McCarthy: The Radical Specter*. Cambridge: MIT Press, 1967.

ROGIN, Michael Paul. *Ronald Reagan, the Movie and Other Episodes in Political Demonology.* Berkeley: University of California Press, 1987.

ROGIN, Michael Paul. The War on Evil. *Le Monde,* 11 September 2002.

SUSKIND, Ron. *One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11*. Nueva York: Simon and Schuster, 2006.

TAIPALE, Kim. Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data. *Columbia Science and Technology Law Review*, v. 5, n. 2, 2003, p. 1-83.

UGELVIK, Synnove; HUDSON, Barbara (eds.). *Justice and Security in the 21st Century: Risks, Rights and the Rule of Law.* Londres/Nueva York: Routledge, 2012.

VILTARD, Yves. Le cas Mc Carthy. Une construction politique et savante. *Cultures & Confits*, n. 43, 2001, p. 13-60.

WEBER, Cynthia. Design, Translation, Citizenship: Reflections on the Virtual (De) Territorializationof the US-Mexico Border. *Environment and Planning D: Society and Space*, v. 30, n. 3, 2012, p. 482-496.

Abstract

Electronic Large-scale Surveillance and Watch Lists: The Products of a Paranoid Politics?

We know from the articles of Richard Hofstadter that a defensive, even paranoid style has pervaded American politics from time to time. Murray Edelman and Michael Rogin have shifted the psychological stance of

this terminology to a political one, focusing on how the notion of the construction of a political spectacle can excite hysteria and paranoia to attract public attention and by so doing build a securitization that expands the executive powers of the state. Rogin described how American political discourse has emphasized counter-subversive strategies in the construction of enemies: for example, against aboriginal peoples, communists and the USSR, and more recently, illegal migrants and terrorists who have supposedly infiltrated the homeland. However, the implications of this politics have rarely been expanded to transnational or international politics.

The broad objective of this paper is to link the configuration of contemporary world politics with interesting strands of sociological research coming from the critical study of American politics. More specifically, the author argues that the compiling of watch lists from transnational databases constructs a criminalization of travellers as illegal and dangerous migrants, while also affecting everyone who uses cloud computing. States use a paranoid style to play off national sovereignty against their international obligations. Each country's practices in this regard constitute a distinctive variation of the trend toward Global Preventive Surveillance (GPS), which has in the author's view become a contemporary form of a transnational process of (in)security, i.e. a process that delivers insecurity through technological tools aiming to provide security.

To sustain this argument, the paper shows how the emergence of global watch lists is reorienting data base technologies to serve the ends of electronic mass surveillance. Governments justify mass surveillance, despite its illegal status in many countries, by claiming that if everyone is doing it, it cannot be illegitimate. A paranoid strain of transnational politics based on unease and fear is thereby instrumentalized in the name of sovereignty, security, citizenship and national identity. Watch lists, in the author's view, are a concrete manifestation of the development by security professionals of a transnational stock exchange of fears, which purports to focus on migrants and border control but has much more to do with fostering domestic counter-subversive strategies than with serving as an effective response to threats.

***Keywords**: surveillance, security, mobility, watch lists, paranoid politics.*

Recibido para publicación en 05/08/2015
Aceptado para publicación en 22/10/2015
Received for publication in August, 05th, 2015
Accepted for publication in October, 22th, 2015

ISSN impresso: 1980-8585
ISSN eletrônico: 2237-9843

http://dx.doi.org/10.1590/1980-85852503880004502