ISSN 2684-0383

PERSPECTIVAS

Revista de Ciencias Jurídicas y Políticas

Nº 3 - Año 2020

ISSN 2684-0383

PERSPECTIVAS

Revista de Ciencias Jurídicas y Políticas

Año II, N.° 3 | Diciembre 2020

UNIVERSIDAD CATÓLICA DE LA PLATA

PERSPECTIVAS

Revista de Ciencias Jurídicas y Políticas

INDICE

Administración:

Revista *PERSPECTIVAS*
Facultad de Derecho y Ciencias Políticas
Universidad Católica de La Plata,
Calle 57 Nº 936, 1900 La Plata.
Tel. (0221) 4393100

Diseño y corrección: **Editorial Ucalp**

Dg. 73 Nº 2137, 1900, La Plata, Argentina
editorial@ucalp.edu.ar

I.S.S.N.: 2684-0383

Presentación

Culmina un año académico excepcional, en sentido amplio de la palabra. En circunstancias sanitarias extraordinarias, nuestra actividad educativa ha sido sumamente prolífica. La tecnología aplicada de manera masiva al intercambio y articulación entre alumnos y docentes ha sido protagonista en esta verdadera transición organizacional. Prueba de ello es el sitio preferencial que se asigna a la temática en este número de nuestra revista. Nos invita a reflexionar acerca de la tecnología como vehículo apto para educar, formar, transmitir valores en el marco del ideario de nuestra Casa.

Deseo agradecer de manera especial a toda la comunidad educativa su compromiso y trabajo en este ciclo que culmina. Del mismo modo, es mi intención dedicar una afectuosa despedida al Dr. Hernán Mathieu, rector saliente, y brindar una cálida bienvenida a la Dra. Rita Gajate, nueva rectora, augurando una gestión exitosa basada en su ya probada capacidad profesional y testimonio de vida. En el mismo sentido, quisiera dar un justo reconocimiento al Dr. Sebastián Piana y al equipo de colaboradores por su excelente trabajo cotidiano en los contenidos de jerarquía de esta publicación, y tareas y proyectos de investigación.

La universidad debe ser una cabal herramienta de transformación. Ser un fanal en el mundo de la cultura. Debe innovar para renovar.

En ese marco, educación de calidad y preparación de profesionales de excelencia es un objetivo, sin dudas, loable. Pero ello carecería de sustento y esencia si no se formaran personas íntegras, éticas y solidarias, comprometidas con las necesidades sociales, con su rol ciudadano y promotores y garantes del bien común.

Dr. Miguel Gonzáles Andía
Decano
Facultad de Derecho y Ciencias Políticas
UCALP

Editorial

Se publica hoy un nuevo número de nuestra revista *Perspectivas*. Lo que parecía un proyecto ambicioso va tomando forma e identidad.

Valoramos profundamente el esfuerzo sostenido para la continuidad de nuestra publicación institucional. Especialmente en este tiempo probado para la humanidad, en el que la salud, los vínculos, el trabajo y la economía han resignificado sus sentidos.

Agradecemos al equipo editorial y a los autores por sus reflexiones y productos, los cuales nos ofrecen una mirada exploratoria sobre la COVID-19 y sus consecuencias en diferentes campos. La humanidad no debe perder la gran oportunidad de repensarse, reeditarse y proyectarse conforme las nuevas «perspectivas» que el horizonte de la pandemia y pospandemia nos ofrecen.

Que este tiempo de Adviento sea de gestación de nuevos proyectos y de esperanza para el tiempo venidero.

¡Feliz Navidad!

Prof.ª Rita M. Gajate
Directora y Editora

Apátridas, el drama de no ser legalmente reconocido por ningún Estado

Delfina Avalos

Estudiante de ciencia política y relaciones internacionales. Facultad de Derecho y Ciencias Políticas. UCALP. Dirección de correo electrónico: delfinaa.avalos@gmail.com

Resumen

Se expone descriptivamente el concepto de *apátridas*, en conjunto con los factores que internacionalmente son reconocidos como los causantes de esta condición. El objetivo del trabajo es visibilizar la problemática que aqueja a millones de personas a nivel mundial. A su vez, también se busca concientizar a la sociedad con respecto a esta temática, basándonos en los diferentes intentos de cooperación internacional para planificar e implementar medidas conjuntas con el fin de ayudar a las personas que sufren de esta condición, y con la esperanza de que se pueda lograr su erradicación, para que todas las personas gocen de una nacionalidad. Concretamente, analizamos los efectos de la campaña «I belong», promocionada internacionalmente por ACNUR, y su aplicación efectiva en el marco normativo de nuestro país, así como sus resultados regionales.

Palabras claves: apátridas, nacionalidad, campaña.

Abstract

The concept of *stateless* is descriptively exposed, within the factors that are internationally recognized as the cause of this condition. The aim of this paper is to visualize this problem which ails thousands of people globally. At the same time, we are also looking forward to sensitizing society about this problematic, on the basis of the different attempts of international cooperation to plan and implement combined measures to help people suffering from this condition, hoping that we can achieve its eradication, so that everyone can have a nationality. Precisely, we analyse the effects of the campaign "I belong", internationally promoted by UNHCR, and its effective application on the normative framework of our country, as well as its regional results.

Key words: stateless, nationality, campaign.

1. La invisibilidad de un sector social

¿Alguna vez te has preguntado qué sentirías si tu familia te explicara que no puedes ir al colegio como el resto de los niños o que si te sientes mal no puedes ir al hospital?, ¿qué pasaría si quisieras entrar en una carrera universitaria para progresar social y académicamente, pero no pudieras acceder a documentación de ningún tipo? Estas son algunas de las experiencias cotidianas que atraviesa un apátrida que nace y vive como tal.

Un apátrida es una persona, como lo expresa su nombre, sin patria. Una persona que no posee derecho alguno y que no es reconocida por ningún país. Las consecuencias que conlleva esto son infinitas, por ejemplo, no poseer documento de identidad y, como consecuencia, no poder acceder al sistema de salud, ni al mercado laboral, ni mucho menos al sistema educativo.

Estas personas no pueden realizar aportes, tampoco estudiar ni conseguir un trabajo en blanco, como consecuencias primarias; pero la realidad es que estas son infinitas. Algo que nos parece tan simple como renovar nuestro documento de identidad nacional o tramitar nuestro pasaporte para salir del país puede ser una odisea para una persona que no es reconocida por ningún Estado. Es decir que, esta condición afecta tanto sus derechos socioeconómicos como sus derechos civiles y políticos. Por eso, Hanna Arendt (2014) describe a un apátrida como una persona «sin derecho a tener derechos». Lo que, como consecuencia, a gran escala, puede generar comunidades aisladas y marginadas.

Por otra parte, cabe mencionar que un apátrida no es lo mismo que un refugiado. Un refugiado es una persona que ha escapado de su país por razones de fuerza mayor, violencia, guerra o persecución y que, en caso de ser resuelto el conflicto, planea, por lo general, volver a su país, es decir, el asilo que solicita es relativamente «temporal». En cambio, la condición de apatridia es totalmente distinta, y está relacionada a problemas legales y vacíos jurídicos. Un apátrida es una persona que no tiene a donde regresar, porque no posee ninguna nacionalidad. No representa a nadie y nadie lo representa a él, puesto que, técnicamente, es una persona que no existe. De todas formas, debemos mencionar que muchas veces se pueden dar estas dos condiciones simultáneamente, ya que una de las razones por las que las personas pueden llegar a convertirse en apátridas es como consecuencia de conflictos armados, debido a que escapan de estos países en situaciones de extrema vulnerabilidad y sin ningún tipo de documentación que certifique su nacionalidad. Según ACNUR, la mayoría de las personas apátridas, a diferencia del migrante y el refugiado, «nacieron en los países en los que han vivido toda su vida» (ACNUR, 2017: p. 1). Sin embargo, una persona puede ser migrante y apátrida, o refugiado y apátrida, al mismo tiempo, por las causas anteriormente expuestas.

Por lo tanto, podríamos inferir que un apátrida no puede soñar, ni siquiera, con tener una vida normal porque automáticamente queda fuera del sistema institucional, y cualquier intento de progreso se convierte en una ardua lucha administrativa por conseguir un papel, la cual, debido a su extensa prolongación temporal, termina quebrando las esperanzas de estas personas, lo que genera que sus intentos acaben rápidamente. Es por eso por lo que

debemos promover una reducción y definitiva erradicación del estatus de apátrida, porque solo una persona definitivamente integrada a la sociedad puede actuar en favor de ella e impulsar su desarrollo, como un ciudadano regular. Es decir: «La negación de estos derechos no sólo impacta a las personas afectadas, sino también a la sociedad como un conjunto ya que la exclusión de todo un sector de la población puede provocar tensiones sociales y perjudicar significativamente el desarrollo económico y social». (ACNUR 2017: p. 1)

Como mencionamos anteriormente, la desigualdad ejercida consciente o inocentemente sobre estas personas se da por diversas razones, pero una de ellas es el desconocimiento y la desinformación; por ello, consideramos de suma importancia exponer este tema, porque los apátridas existen en nuestra sociedad, pero son invisibles. Tener una patria, un Estado, una nación que nos reconozca es un derecho humano básico y fundamental para la existencia de todas las personas.

2. «I belong» (2014-2024)

Como expusimos previamente, los motivos por los cuales una persona se convierte o nace apátrida son variados, pero, por lo general, se debe a irregularidades y vacíos legales que posee la normativa de cada país. Es por ello por lo que la ONU ha propuesto una campaña global con el fin de erradicar la apatridia en el mundo para 2024.

La ONU, más precisamente, el Alto Comisionado de Naciones Unidas para los Refugiados (ACNUR), ha comenzado una campaña en 2014, reconocida internacionalmente como «I belong», es decir, 'yo pertenezco'. Esta campaña, como se mencionó anteriormente, se propone terminar con el estatus de apátrida para 2024 promoviendo leyes en los distintos Estados con el fin de saciar los vacíos legales, para erradicar, finalmente, la existencia de esta condición (ACNUR, 2014*b*).

La finalidad de esta campaña es acabar con la marginalización sufrida por dichas personas, garantizando sus derechos humanos básicos, facilitando su integración, evitando la discriminación y apresurando los trámites burocráticos para que los individuos sean regulados inmediatamente al momento de alcanzar esta condición.

Para adentrarnos en esta cuestión, debemos establecer, principalmente, qué entiende esta organización por *apátrida*, ya que es el recurso humano básico y primordial de esta campaña.

Un apátrida «es una persona que no es reconocida por ningún país como ciudadano conforme a su legislación» (ACNUR, 2017: p. 1). Básicamente, es una persona que no tiene la nacionalidad de ningún país.

Algunas personas nacen sin Estado, pero otras se convierten en apátridas; debido a ello, nos corresponde en este punto definir algunas de las diversas razones por las cuales una persona puede alcanzar esta condición. Según ACNUR[1], las cinco causas de la apatridia son:

[1] https://www.acnur.org/acabar-con-la-apatridia.html

1. La discriminación (por ejemplo, racial, religiosa o de género), el conflicto y los vacíos en las leyes de nacionalidad. Ser indocumentado no es lo mismo que ser apátrida. Sin embargo, la falta de registro de nacimiento puede poner a las personas en riesgo de apatridia. Además, en muchos países, la regulación para adquirir la nacionalidad suele ser muy discriminatoria, y, por lo general, las minorías étnicas, raciales y religiosas son las que se ven más afectadas en consecuencia.

2. El desplazamiento: cuando las personas se desplazan de un país a otro, independientemente de las causas, el reconocimiento de su nacionalidad se dificulta si no posee documentación alguna. Un niño nacido en un país extranjero puede correr el riesgo de convertirse en apátrida si ese país no permite la nacionalidad basada únicamente en el nacimiento y si el país de origen no permite que un padre transmita la nacionalidad a través de los vínculos familiares.

3. La discriminación de género: las poblaciones significativas de personas apátridas también viven en los países alrededor del mundo que no les permiten a las madres transmitir su nacionalidad a sus hijos en condiciones de igualdad con los padres. Esto puede ocasionar que los niños queden en condición de apatridia cuando sus padres son desconocidos, desaparecidos o fallecidos. Según el informe[2] «Gender discrimination and childhood statelessness» de ACNUR, las leyes de 25 países no permiten que las mujeres trasmitan su nacionalidad.

4. Disolución, división y aparición de nuevos Estados: las minorías étnicas, religiosas y raciales suelen ser las más afectadas en este sentido, debido a que la legislación, muchas veces, solo permite el traspaso de la nacionalidad cuando un miembro de la familia posee nacionalidad de origen.

5. Por la pérdida o la privación de la nacionalidad: muchas personas pueden perder su nacionalidad o ser privados de ella por cuestiones discriminatorias, como mencionamos anteriormente, o de otra índole.

Cualquiera sea la causa que genere en una o en varias personas esta condición, la apatridia tiene graves consecuencias para todas las personas y todos los países, porque, a pesar de ser un problema oculto, se encuentra en todas partes del mundo. Y en este sentido, lo que se pretende con estas campañas es visibilizar su existencia y, finalmente, erradicarlo.

Para llevar a cabo la finalidad de esta campaña, la ONU propuso un «Plan de Acción Mundial para Acabar con la Apatridia». Este se basa en la definición de 10 acciones que deberán llevar a cabo los Estados, con el apoyo de ACNUR y de otras organizaciones. El objetivo principal de este plan es «resolver las principales situaciones de apatridia existentes y prevenir el surgimiento de nuevos casos» (ACNUR, 2017: p. 2), a través de un marco estratégico comprendido por diez acciones colectivas para proteger mejor a las personas apátridas. Estas acciones son:

[2] https://www.unhcr.org/ibelong/gender-discrimination-and-stateless-children/#sect4

1. Resolver las principales situaciones existentes de la apatridia.

2. Asegurar que ningún niño nazca apátrida.

3. Eliminar la discriminación de género en las leyes de nacionalidad.

4. Prevenir la denegación, pérdida o privación de la nacionalidad por motivos discriminatorios.

5. Prevenir la apatridia en los casos de sucesión de Estados.

6. Conceder el estatuto de protección a los migrantes apátridas y facilitar su naturalización.

7. Garantizar el registro de nacimientos para prevenir la apatridia.

8. Expedir documentación de nacionalidad a aquellos que tienen derecho a ella.

9. Adherirse a las Convenciones de las Naciones Unidas sobre la Apatridia.

10. Mejorar la cantidad y calidad de los datos sobre las poblaciones apátridas.

Como resultado de la implementación de esta campaña a nivel internacional, podemos aportar varios datos que contribuyen a destacar el trabajo realizado durante estos 5 años.

Según datos de ACNUR[3] (2018), desde el comienzo de esta campaña en 2014, más de 166.000 apátridas han logrado alcanzar la nacionalidad. Y una gran cantidad de Estados han adoptado convenciones internacionales relacionadas con esta cuestión, así como muchos países han modificado su legislación para erradicar la apatridia definitivamente. Si bien se cree que los apátridas son aproximadamente 10 millones alrededor del mundo, ACNUR explica que no se puede determinar una cifra exacta, lo cual complejiza aún más su erradicación. Aunque se hace referencia a que cada 10 minutos nace un nuevo apátrida, para que podamos comprender la magnitud de este problema.

Más precisamente,

> … desde que se lanzó la Campaña, 20 Estados se han adherido a una o ambas Convenciones de las Naciones Unidas sobre la Apatridia, 2 Estados han eliminado la discriminación de género de sus leyes de nacionalidad, 9 Estados han introducido procedimientos de determinación de apatridia, y 10 Estados han tomado medidas concretas para resolver situaciones prolongadas de apatridia. (ACNUR, 2019: p. 1)

Si queremos evaluar su implementación regionalmente, debemos mencionar lo siguiente:

En cuanto a la región Latinoamericana y el Caribe, cabe destacar la cumbre «Cartagena +30», en la cual 28 Estados junto con 3 territorios se comprometieron a adoptar la declaración y el Plan de Acción de Brasil, el cual desarrollaremos en profundidad más adelante para realizar un análisis regional.

[3] https://news.un.org/es/story/2018/11/1445531

En cuanto a la región asiática y el pacífico, podemos mencionar que, en una conferencia organizada por ACNUR, se reunieron en Bangkok 44 Estados que adoptaron una declaración ministerial para establecer el registro civil universal. Con la intención de prevenir la apatridia.

Por otra parte, en África, los Estados que forman parte de la Comunidad Económica de África Occidental (CEDEAO), junto con ACNUR, organizaron la primera conferencia sobre apatridia en la región, adoptando la Declaración de Abiyán sobre la eliminación de la apatridia, su protección e identificación y la posterior erradicación de esta condición.

Por último, la Unión Europea adoptó las primeras conclusiones del Consejo de la UE sobre la apatridia, alentando la adopción de la campaña «I belong» que realiza la ONU previamente descripta (ACNUR, 2019).

3. La cuestión a nivel regional: el Plan de Acción de Brasilia

En el marco global de la crisis de refugiados más grande desde la Segunda Guerra Mundial, y, sobre todo, enfrentando la crisis migratoria más importante de la región en los últimos tiempos, esta campaña es fundamental e imprescindible en el continente americano para hacer valer los derechos humanos de las personas apátridas.

Como mencionamos anteriormente, América Latina y el Caribe, en el marco de la campaña «I belong» del ACNUR, han adoptado, durante la cumbre «Cartagena +30» en Brasilia, un plan de acción común para acabar con la apátrida en 2024, siendo la primera región del mundo en comprometerse a este grado. Esta cumbre se llevó a cabo en 2014, a inicios de la campaña de la ONU, lo cual nos permite comprender el nivel de compromiso por parte de estos países y esta región para, realmente, ser la primera en eliminar la apatridia. Incluso en esta ocasión se celebraba el 30.° aniversario de la declaración de Cartagena sobre refugiados de 1984, lo cual hace aún más significativa la adhesión al plan.

Esta cumbre estuvo conformada por la mayoría de los Estados regionales, de los cuales 28 países y 3 territorios de América Latina y el Caribe (Antigua y Barbuda, Argentina, las Bahamas, Barbados, Belice, Bolivia, Brasil, Islas Caimán, Chile, Colombia, Costa Rica, Cuba, Curazao, El Salvador, Ecuador, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, Santa Lucía, Surinam, Trinidad y Tobago, las Islas Turcas y Caicos, Uruguay y Venezuela) adhirieron a la Declaración y al Plan de Acción de Brasilia, «acordando trabajar juntos para mantener los estándares de protección más altos a nivel internacional y regional, implementar soluciones innovadoras para las personas refugiadas y desplazadas, y ponerle fin a la difícil situación que enfrentan las personas apátridas en la región» (ACNUR, 2014*a*: p. 1).

Brasil fue uno de los impulsores de este proceso a nivel regional con este plan de acción, en el marco de la campaña global, el cual se basa en tres ejes: la prevención, la protección y la solución.

El plan establece una serie de objetivos que alcanzar (ACNUR, 2014*a*: p. 12):

a. Promover la erradicación de la apatridia a nivel regional y nacional, a través de la implementación de las acciones relevantes del Plan de Acción de Brasil.

b. Fomentar el trabajo interinstitucional, la programación conjunta y el desarrollo de proyectos de bajo costo e impacto rápido, con el apoyo técnico y financiero del ACNUR y la cooperación internacional.

c. Realizar un monitoreo conjunto, sistemático y permanente a nivel nacional del programa de erradicación de la apatridia, evaluando los avances registrados y desafíos subsistentes.

Esta declaración es «Un Marco de Cooperación y Solidaridad Regional para Fortalecer la Protección Internacional de las Personas Refugiadas, Desplazadas y Apátridas en América Latina y el Caribe» (ACNUR, 2014*a*: p. 1), en la cual los países miembros se comprometen a «mantener los más altos estándares de protección, reconoce los retos humanitarios que actualmente afectan a la región y hace propuestas innovadoras para abordarlos» (ACNUR, 2014*a*: p. 1).

> Estos principios se han convertido en programas específicos contenidos en el Plan de Acción de Brasil «Una Hoja de Ruta Común para Fortalecer la Protección y Promover Soluciones para las Personas Refugiadas, Desplazadas y Apátridas en América Latina y el Caribe dentro de un Marco de Cooperación y Solidaridad». (ACNUR, 2014*a*: p. 7)

Este Plan está conformado por programas estratégicos, que serán implementados por los respectivos gobiernos. Entre los principales programas (ACNUR, 2014*a*), podemos destacar:

- Asilo de calidad.
- Fronteras seguras y solidarias.
- Repatriación voluntaria, integración local y reasentamiento solidario.
- Movilidad laboral.
- Observatorio de DD. HH. para el desplazamiento, prevención y transito digno y seguro.
- Solidaridad regional.
- Erradicación de la apátrida.
- Cambio climático y desastres naturales.
- Cooperación regional.
- Implementación y seguimiento: implementación de mecanismos en los distintos países de evaluación y seguimiento, incluido un informe de ACNUR sobre la situación cada 3 años.

«La Declaración de Brasil subraya que toda persona tiene derecho a una nacionalidad y que la apatridia supone una violación de ese derecho individual cuando la prerrogativa estatal para regular la nacionalidad infringe los límites fijados por el derecho internacional» (ACNUR, 2014*a*: p. 8); ello indica que existen importantes desafíos para la región en este sentido.

En vistas de estos retos, el programa de acción se encarga de recomendar a los Estados ciertos puntos que seguir, si su voluntad es realmente erradicar la apatridia. Entre ellos, podemos mencionar (ACNUR, 2014*a*: p. 8):

(a) adherir a las convenciones sobre apatridia;

(b) promover la armonización de la normativa y práctica interna sobre nacionalidad con los estándares internacionales;

(c) facilitar la inscripción universal de nacimientos;

(d) establecer procedimientos justos y eficientes para determinar la apatridia;

(e) adoptar normativa interna de protección que garantice los derechos de las personas apátridas;

(f) facilitar la naturalización de las personas apátridas en contexto migratorio

(g) confirmar la nacionalidad a través de la expedición de documentación pertinente;

(h) facilitar la restitución automática de la nacionalidad como remedio para la privación arbitraria de la nacionalidad, así como la adopción de legislación y políticas inclusivas para la recuperación de la nacionalidad.

Además, va a establecer que los Estados deben definir qué programas y acciones entienden como prioritarios, y cuáles son las que se aplican más adecuadamente a su país, en el contexto civil y político, estableciendo también distintos mecanismos de evaluación e implementación para determinar la efectividad de la normativa. Para llevar esto a cabo, el plan promueve que cada Estado (ACNUR, 2014*a*: p. 9):

a. defina qué programa es relevante a nivel nacional;

b. determine qué acciones son relevantes a nivel y, en casos de ser varias, cuáles son las acciones prioritarias;

c. diseñe proyectos específicos para implementar actividades orientadas a realizar las metas/acciones;

d. dé seguimiento y evalúe a nivel nacional el avance.

Por último, ACNUR (2014*a*) considera que este plan de acción es beneficioso[4] tanto para los Estados como para la región en general, lo cual permite establecer indicadores que engloben a todos los países, destaca la acción de los países que mejor apliquen

[4] Los beneficios están establecidos con un mayor detalle en ACNUR (2014*a*: p. 10).

este plan, puntuándolos y dándoles prestigio en la esfera internacional, e incluso es beneficioso porque fomenta el debate de políticas públicas sobre esta cuestión y otras, presenta un problema relativamente «invisible» para la política como para la sociedad y permite identificar las acciones adecuadas para cada Estado que tenga la finalidad de erradicar la apatridia. ACNUR se encargará de realizar informes de evaluación cada 3 años y un informe final sobre la implementación de este plan. «Hacia Cero Apatridia» es un mecanismo de evaluación del programa. «La evaluación comprenderá el análisis de la legislación, y las políticas y prácticas estatales sobre nacionalidad y apatridia, así como aquellas que son relevantes, tales como las relativas a la inscripción de nacimientos y otorgamiento de documentación de identidad» (ACNUR, 2014*a*: p. 12).

La metodología que se utiliza para la evaluación es el establecimiento de indicadores, que se renovarán cada 3 años. ACNUR, además, proveerá los recursos financieros necesarios para el sustento, al menos en parte, de los proyectos políticos nacionales de todos aquellos países que adopten las convenciones sobre apatridia y otras cuestiones legales, así como también el apoyo técnico para el diseño de proyectos de bajo costo, rápida implementación y alto impacto.

La implementación de este plan de acción global en la región se tradujo en importantes programas de los Estados para acelerar los procesos de acceso a la nacionalidad de las personas apátridas. Por ejemplo, se encuentra el caso de Chile, con el programa «Chile reconoce», o el de Costa Rica, con el programa «Chiriticos». Pero para acercarnos a un caso más representativo, debemos mencionar qué consecuencias tuvo esta campaña a nivel nacional; es por ello por lo que nos corresponde hablar sobre la aprobación de la Ley 27.512 en nuestro país.

4. La repercusión de la campaña en nuestro país: la Ley N.° 27.512

Según ACNUR (2017), los Estados son los encargados de establecer las reglas para la adquisición, el cambio y la pérdida de la nacionalidad como parte de su poder soberano. En la Argentina, esta cuestión se rige por dos tratados de derechos humanos que poseen categoría constitucional, la Convención sobre el Estatuto de los Apátridas de 1954 y la Convención para Reducir los Casos de Apatridia de 1961. Debido a su carácter constitucional, «prevalecen sobre la normativa legal vigente aplicable a los extranjeros en general, salvo respecto a aquella que sea más favorable a la persona apátrida» (Boletín Oficial, 2019). La primera de estas convenciones (1954) es el primer régimen internacional y el más importante en relación a esta cuestión, ya que establece la definición de apátrida y fomenta y asegura las normas mínimas de tratamiento para las personas apátridas; garantiza sus derechos para evitar la marginalización de esta población, entre ellos podemos mencionar el derecho a la educación, el empleo, la vivienda, etc. Y en la segunda convención, que está destinada a reducir los casos de apatridia (1961), se establece una serie de obligaciones específicas que deben cumplir los Estados miembros para prevenir

y disminuir dicha condición. Además, se pueden tener en cuenta también, dentro de este marco normativo, los tratados regionales, los cuales complementan estas convenciones y establecen obligaciones adicionales a los Estados partes. Y, por último, no podemos dejar de mencionar los tratados internacionales de derechos humanos que nuestro país ha adoptado, para enmarcar aún más esta cuestión.

Entonces, se podría considerar que el problema estaría resuelto, ya que existen todos estos instrumentos y mecanismos internacionales para la protección y erradicación de la apatridia, algunos incluso con rango constitucional. Pero este compromiso formal no es sustancial. Según Piscetta (2018), «ese pacto nunca se reglamentó ni se ajustó a la normativa local. En la actualidad se desconoce cuántos apátridas migrantes hay. No existen números ni cifras estimadas porque faltan los mecanismos para identificarlos».

Es por este motivo que fue necesaria la formulación de la Ley General de Reconocimiento y Protección de las personas apátridas (N.° 27.512) en nuestro país. Porque la implementación de estos pactos, evidentemente, no fue eficiente ni suficiente para enfrentar la cuestión a nivel nacional.

Esta ley tiene como finalidad facilitar los procesos legales para que todas las personas apátridas puedan naturalizarse, así como también garantizar sus derechos humanos básicos y hacer visible esta cuestión, dándole entidad para, finalmente, erradicarla. La autoridad que aplica esta ley es la dirección nacional de migraciones (DNM), en conjunto con la Comisión Nacional de Refugiados (CONARE).

Según el artículo 4 de esta ley, un apátrida es «toda persona que no sea considerada como nacional suyo por ningún Estado, conforme su legislación» (Boletín Oficial, 2019). Esta definición es compatible con la convención de 1954. El caso de nuestro país conlleva una particularidad en cuanto a esto. Según Karina Banfi, diputada nacional por la provincia de Buenos Aires (miembro de partido Cambiemos) autora y promotora de la ley:

> Argentina, de acuerdo a su ley de Nacionalidad no «genera» apátridas. Esto se da porque tenemos ambos sistemas de adquisición de nacionalidad, *ius solis* (si naces en el territorio, independientemente de tus padres, sos argentino) y *ius sanguinis* (si cualquiera de tus padres es argentino, tenés derecho a la nacionalidad). A su vez, Argentina se ha adherido a la Convención sobre el Estatuto de los Apátridas de 1954 y a la Convención para Reducir los casos de Apatridia de 1961. Ambos instrumentos regulan la condición de apátrida en el sistema internacional. Sin embargo, nuestro país no tiene una ley específica que establezca un procedimiento de determinación de las personas apátridas. (Infobae, 2018)

Los incentivos que impulsan esta ley en nuestro país y en nuestra región son, evidentemente, la crisis regional que trajo al país a miles de extranjeros provenientes de Venezuela, muchos de ellos en condiciones de irregularidad y sin la documentación necesaria. Es importante destacar que, durante este año, los ciudadanos provenientes de Venezuela se convirtieron en el mayor grupo migratorio que actualmente reside en nuestro país. De todas formas, esta normativa también está relacionada con migraciones irregulares provenientes de Centroamérica, como de todas partes del mundo. Ya que

nos encontramos en un marco global de crisis de refugiados internacional, por lo cual, acciones concretas deben llevarse a cabo de una vez y para todas, si no queremos que esto termine siendo un problema aún más grave de lo que actualmente es.

Más allá de que nuestro país posee estas características legislativas y no sea un gran generador de apátridas a nivel global, no debería interesarnos precisamente la cantidad de personas apátridas, sino, más bien, una sola historia es suficiente para comprometernos con un régimen legal que resuelva estos problemas. Es por eso por lo que, a continuación, exponemos un caso nacional que refleja la complejidad de la situación.

5. Casos nacionales: una sola historia es suficiente

Para expresar con mayor detalle las consecuencias de la compleja regulación jurídica de esta cuestión, podemos mencionar distintos casos que evocan a lo más profundo de nuestra sensibilidad, ya que los papeles cambian cuando les damos un nombre.

Cabe mencionar el caso de Elsa Saint Girons, madre y abogada argentina que tuvo que sufrir un proceso bastante complejo para lograr el reconocimiento de la nacionalidad de su hija, que técnicamente nació apátrida. Elsa buscó ampliar los alcances de su petición utilizando medios masivos característicos de un mundo globalizado como es el internet. «No sin mi hijita» es la petición que realiza esta madre en change.org para que su hija, nacida como producto de una gestación subrogada en 2012, no quede apátrida.

Este hecho se da como consecuencia de que la legislación de los países de los cuales provienen los padres, España y Argentina, no querían reconocer la nacionalidad de esta niña.

Para estos países, la niña legalmente es india, ya que nació en ese país y su madre biológica es de la misma nacionalidad. En cambio, para la legislación india, la madre es Elsa, por lo cual no le correspondería la nacionalidad india, sino más bien la de alguno de sus padres. Estos vacíos legales llevaron a que esta niña nazca apátrida.

Casos como este nos permiten vislumbrar que, aun pudiendo categorizar las causas de la apatridia, de todas formas, existen miles de casos y se pueden dar por diversas cuestiones, muchas veces impredecibles. Debido a esta razón, es indispensable que exista una legislación que permita cubrir la mayor cantidad de casos posibles, sin observar como principal factor las causas.

Finalmente, este caso fue resuelto, y esta niña hoy tiene su respectiva nacionalidad e identidad. Pero esto fue gracias a que sus padres se encuentran en una posición de conocimiento de la cuestión y, de todas formas, han tenido que superar un arduo proceso para su resolución. Las personas que no tienen estos recursos, que están marginalizadas, se quedan sin identidad, se quedan apátridas.

Conclusión

En un mundo libre, en el que día a día la lucha de diversos sectores por la ampliación de derechos correspondientes a las más diversas cuestiones se ve acrecentada, no se puede adoptar una postura de indiferencia. Se deben romper los mecanismos culturales y legales que omiten la existencia de un determinado sector social. La apatridia es evidencia de las falencias del derecho internacional. Sus fallas y vacíos legales son motivos suficientes para que la comunidad internacional esté incentivada a actuar colectivamente para solucionar dicha cuestión. Cada país debe construir un cuerpo normativo que evite estos vacíos y, en conjunto, a través de la cooperación internacional, lograr un derecho internacional capaz de brindar una mayor protección a la comunidad internacional que se encuentra en constante cambio.

En conclusión, apelamos a que los Estados profundicen estas medidas, implementando nuevos mecanismos de eliminación de la discriminación y la marginalización, a fin de evitar que ni una persona más se convierta en apátrida en el mundo y fomentar que América Latina y el Caribe se conviertan en la primera región del mundo en erradicar esta condición definitivamente.

Ser apátrida es no tener identidad, no tener identidad es no tener derechos, es ser invisible, es no existir. Ser apátrida es un mecanismo de tortura social, y lo debemos erradicar para siempre.

Bibliografía

ACNUR (2014*a*). América Latina y el Caribe adoptan una hoja de ruta común para responder a las nuevas tendencias del desplazamiento y poner fin a la apatridia en la próxima década. Obtenido de: https://www.acnur.org/cartagena30/antecedentes-y-desafios/

ACNUR (2014b). #IBELONG: Campaña para acabar con la Apatridia. Obtenido de: https://www.acnur.org/ibelong-campana-para-acabar-con-la-apatridia-5b32bf224.html

ACNUR (2017). ¿*Qué es la apatridia?* Obtenido de https://www.acnur.org/fileadmin/Documentos/BDL/2017/10996.pdf?file=fileadmin/Documentos/BDL/2017/10996

ACNUR (enero de 2018). *Plan de Acción de Brasil. Programa* «*Erradicación de la Apatridia*». *Mecanismo de Evaluación y Seguimiento* «*Hacia Cero Apatridia*». Obtenido de https://www.acnur.org/5b97e7ce4.pdf

ACNUR (2019). Segmento de Alto Nivel sobre Apatridia. Obtenido de https://www.unhcr.org/ibelong/es/segmento-alto-nivel-apatridia/

Arendt, H. (2014). *Los orígenes del totalitarismo.* Madrid: Harcourt Brace Jovanovich.

Banfi, K. (2018). Apátridas, venciendo las barreras. *Telam*, 1.

Boletín Oficial (2019). Ley general de reconocimiento y protección de las personas apátridas. Buenos Aires.

Girons, E. S. (2012). No sin mi hijita: ayúdanos a traer a casa a nuestra pequeña. Obtenido de: https://www.change.org/p/no-sin-mi-hijita-ay%C3%BAdanos-a-traer-a-casa-a-nuestra-peque%C3%B1a

Piscetta, J. (16 de noviembre de 2018). El drama de «no existir»: qué es la apatridia y por qué el Congreso avanza con una ley para regularla. *INFOBAE*, pág. 1.

Presente y futuro en las relaciones chino-africanas. ¿Beneficio mutuo o renovada expresión de neocolonialismo?

Sofía Aristegui y Alejandra Oyola Arias

Alumnas de 3.er año de la Licenciatura en Ciencia Política y Relaciones Internacionales de la Universidad Católica de La Plata. Trabajo realizado en el marco de la Cátedra de Análisis Político. Correo electrónico: sofia.aristegui@outlook.com.ar - alejandra.oyola75@gmail.com

Resumen

El propósito del presente trabajo es analizar el proceso por medio del cual se ha ido incrementando en las últimas décadas la presencia de China en África, en base a un modelo alternativo de relaciones bilaterales centrado en la cooperación y el beneficio mutuo que se aparta, al menos retóricamente, del modelo clásico de explotación por parte de las tradicionales potencias coloniales. Sin embargo, en la práctica, algunos aspectos de estas relaciones parecen alejarse del modelo inicial, estableciéndose situaciones de explotación de recursos naturales y dependencia económica en los países de la región que podrían ser causa de una serie de problemas o desafíos en dichas relaciones a futuro.

Palabras clave: Política exterior china, África, Relaciones chino-africanas, neocolonialismo, cooperación.

Abstract

The purpose of this paper is to analyze the process by which China's presence in Africa has been increasing in recent decades based on an alternative model of bilateral relations focused on cooperation and mutual benefit that departs, at least rhetorically, from the classic model of exploitation by the traditional colonial powers. However, in practice, some aspects of these relationships seem to move away from the initial model, establishing situations of exploitation of natural resources and economic dependence in the countries of the region that could be the cause of a series of problems or challenges in these relationships in the future.

Keywords: Chinese foreign policy, Africa, Chinese-African relations, neocolonialism, cooperation.

1. Antecedentes de la relación China-África

En las últimas décadas, la presencia de China en África ha crecido escalonadamente producto de la intensificación de las relaciones entre el gigante asiático y los países del continente. Si bien estas relaciones no son históricamente nuevas, ya que se han registrado vínculos entre ambas regiones desde el siglo xv; si hacemos referencia a la historia del siglo xx, hay que tener en cuenta la importancia decisiva que tuvo para el afianzamiento de aquellas la Conferencia Afroasiática de Bandung en 1955, que significó para la República Popular China una primera oportunidad para estrechar relaciones con las naciones africanas recientemente independientes, con el objetivo político de ser reconocida internacionalmente como la China legítima, en desmedro de la República de China situada en la isla de Taiwán. Posteriormente, en 1971, la mayoría de estos países africanos aliados votaron a favor del retorno de la República Popular China como único representante legítimo de ese país a la Organización de las Naciones Unidas (González Aspiazu, 2016).

Desde el punto de vista comercial, la presencia inversora de China en el exterior se fortaleció con su ingreso a la Organización Mundial del Comercio (OMC) en 2001. El 4 de septiembre de 2018, el presidente chino Xi Jinping, en el discurso de apertura de la Cumbre del Foro de Cooperación China-África (FOCAC) en Beijing, reiteró los principios de cooperación que han guiado las relaciones chino-africanas desde sus comienzos con el objetivo de constituir un modelo de desarrollo alternativo al modelo clásico de explotación por parte de las tradicionales potencias coloniales. Estas cinco abstinencias consisten en no interferir con los países africanos en su exploración de caminos de desarrollo acordes con sus condiciones nacionales, no intervenir en los asuntos internos de África, no imponerles su propia voluntad, no añadir ninguna condición política a las asistencias a dichos países y no procurar intereses egoístas políticos en las inversiones y la financiación para el continente (Observatorio de la Política China, 2018).

2. La presencia actual de China en el continente africano

Durante los cincuenta años transcurridos desde los votos de apoyo en la ONU de 1971, los lazos políticos entre China y África han cambiado notoriamente, de manera tal que gran parte del continente africano está, en la actualidad, alineado política y económicamente con el gigante asiático. Esto se debe, principalmente, a que China ha invertido enormes sumas de dinero en África.

El modelo de interacción chino-africano se basa en la ganancia mutua o *win-win*. Por un lado, África necesita de China para desarrollarse tanto económica como socialmente y las inversiones que el gigante asiático ha hecho en África fomentan la explotación mineral, las industrias, la construcción y los servicios. Su contribución a la infraestructura reduce

los déficits y promueve el desarrollo del continente. Además, a pesar de ser la mayoría de los países africanos los peores candidatos para atraer inversiones debido a sus graves casos de corrupción e inestabilidad política, China les ha otorgado facilidades financieras a modo de préstamos a muy largo plazo y con intereses mínimos, para, de esta manera, poder seguir apostando a su desarrollo y mejorar la calidad de vida de los africanos. Por todos estos motivos, casi dos tercios de los africanos perciben su relación con China como algo positivo (Moral, 2019).

Por otro lado, China se encuentra desabastecida de recursos naturales y con un excedente de sobreproducción, por lo cual necesita a África para proveerse de materias primas y de mano de obra barata, así como de un mercado al alza de potenciales consumidores y oportunidades de negocio que puedan absorber esa sobreproducción. Con respecto a los recursos naturales, África cuenta con un tercio de las reservas minerales del mundo, las cuales hoy en día son materias primas esenciales en la era digital del siglo xxi. Hay importantes reservas de petróleo y gas en países como Egipto, Nigeria, Angola, Libia y Argelia; uranio en Níger y Namibia; oro en Ghana, Sudáfrica y Sudán; y los muy codiciados platinoides (esenciales para catalizadores, discos duros, bujías, fibras ópticas, pilas de combustible de última generación, etc.) se encuentran en Sudáfrica y Zimbabue. Dicho esto, no sorprende en absoluto que China se encuentre interesada en los principales minerales que mueven la economía digital del siglo xxi, de los cuales se ha podido abastecer en más de una ocasión como medio de pago por parte de los países africanos sin capital, a cambio de infraestructura (Rodríguez-Rata, 2020).

Un proyecto actual muy significativo es la Iniciativa de la Franja y la Ruta propuesta por China en 2013, que está en proceso y se ha convertido en una de las plataformas más prometedoras para la cooperación internacional, forjando un nuevo camino hacia la globalización inclusiva que produce beneficios compartidos. Esta iniciativa tiene como objetivo construir una red de comercio e infraestructura que conecte a Asia con Europa y África a lo largo de las antiguas rutas comerciales de la Ruta de la Seda para buscar desarrollo y prosperidad comunes.

Sin embargo, la crisis sanitaria causada por la pandemia del coronavirus (COVID-19) durante este año ha alterado considerablemente la relación entre China y África. En un comienzo, la coyuntura le ha brindado a China la posibilidad de reafirmar su presencia en la región africana, a la cual decidió asistir, en primer orden, donando toneladas de materiales sanitarios y de asistencia médica a la totalidad de los 54 países africanos, y prometiendo alivianar sus deudas económicas. Pero, a pesar de la ayuda y de las promesas, con el paso de los meses, comenzaron a desgastarse las bases que constituyen la relación en cuestión, y esto se debe, principalmente, al debilitamiento de la economía china, la cual se verá imposibilitada de sostener más préstamos masivos frente a la suba de la tasa de desempleo y al riesgo de quiebra de las empresas pertenecientes al gigante asiático (Chimbelu, 2020).

3. Perspectivas futuras de las relaciones chino-africanas

Como examinamos en el apartado anterior, la política exterior china en la región africana puede ser percibida como un novedoso plan de cooperación y beneficio mutuo. Sin embargo, dicho plan no puede dejar de enmarcarse en la estrategia de China, como potencia emergente en ascenso, de consolidarse como un nuevo *hegemón* en un orden internacional cambiante. Desde este punto de vista, el protagonismo chino puede ser visto como una manera de generar alianzas políticas y diplomáticas con países africanos en el marco del conflicto geopolítico, comercial y tecnológico con Estados Unidos. Según el internacionalista S. Walt, la lógica de la rivalidad chino-americana no se encuentra vinculada a factores ideológicos, sino con una estructura del sistema internacional en la cual Estados Unidos es la principal economía del mundo y China la segunda, lo que hace inevitable que se perciban mutuamente como una potencial amenaza. Más allá del liderazgo retóricamente agresivo de Donald Trump, el carácter sistémico de este conflicto no permite vaticinar un gran cambio con las elecciones americanas del 3 de noviembre, aún con la llegada de Joe Biden a la Casa Blanca. Para S. Walt, «… los Estados Unidos seguirán centrados en China, la reacción contra la globalización continuará y la oposición a las "guerras eternas" no desaparecerá. La política exterior de los EE. UU. se gestionará de manera más competente, pero no cambiará tanto como mucha gente cree» (Darío, 2020). Como sostiene el economista chileno Osvaldo Rosales (2019), la inversión china en el exterior es un elemento clave de su política exterior que se expresa no solo en la Iniciativa de la Franja y la Ruta, sino también en su creciente inversión en recursos naturales (energía, minerales y alimentos) tanto en África como en América Latina, ya que son cruciales para sostener su elevado ritmo de crecimiento económico y para atender las crecientes demandas de consumo que le plantea su demografía.

Pero algunos especialistas indican que, más allá de este aparente beneficio mutuo, las relaciones comerciales chino-africanas plantean algunos problemas o desafíos por afrontar en el mediano y largo plazo.

Un primer punto que señalar es que, más allá de la potencia retórica que tienen los cinco principios de la diplomacia china esbozados en el primer apartado, la irrupción de su plan de desarrollo en África no deja de ser controvertido, al menos en dos aspectos. Muchos analistas ya han señalado que las deudas acumuladas a lo largo del tiempo por los países africanos (Zambia, Nigeria, Tanzania, Mozambique, entre otros) son impagables y la pandemia no ha hecho más que agravar esta crisis de deuda. Como respuesta, el presidente chino Xi Jinping prometió cancelar una pequeña porción de los préstamos a los gobiernos de África solicitando a los bancos estatales que revisen la deuda comercial de los prestatarios de la región (Hill, Ng'Wanakilala y Soto, 2020). Un segundo aspecto es que la aplicación irrestricta de este financiamiento es contradictoria, desde el punto de vista del *soft power*, con el declamado principio de no intervención de la potencia asiática, que pareciera utilizar, como vimos anteriormente, la dependencia económica de los débiles

países africanos para beneficiarse con la explotación de recursos naturales y fortalecerse geopolíticamente en la región (Gómez Díaz, 2020).

Un segundo factor de conflicto, vinculado al racismo, ha encendido las alarmas en las relaciones chino-africanas durante la actual pandemia, ya que se han producido numerosas denuncias en el país asiático de xenofobia y discriminación contra ciudadanos africanos, principalmente en el territorio chino de Guangzhou, a quienes se culpa de traer una segunda ola de contagios por COVID-19. Esta situación ha provocado tensiones diplomáticas, como la condena de varios embajadores africanos de los incidentes y la presión al gobierno chino para que se pronuncie al respecto, debilitando un vínculo que se creía fortalecido al inicio de la pandemia (Doğru, 2020).

4. Reflexiones finales

A modo de conclusión, podemos decir que, más allá de que las relaciones entre China y los países africanos se plantearon inicialmente en el marco de un modelo de cooperación fundado en principios igualitarios, a primera vista, la potencia asiática pareciera verse más beneficiada por el intercambio. Sin embargo, el resultado final de la incursión de China en el continente continúa siendo una cuestión abierta y, como examinamos, no exenta de dificultades. El tiempo dirá si la balanza logra en los hechos inclinarse definitivamente a favor de relaciones bilaterales de beneficios compartidos, alejándose así del peligro latente de los tradicionales modelos de saqueo de los recursos naturales al que han sido sometidos los países africanos históricamente. Como advierte N. Rabbia (2015):

> Como sea, el predominio de la lógica extractiva de dichos modelos de vinculación no se ha modificado. Adicionalmente, las condiciones en que se realizan los contratos de asociación sino-africanas parecen ofrecer un panorama no tan optimista… La seductora propuesta china yace en la falta de condicionamientos y reparo a la hora de llevar adelante negocios y procesos de cooperación, y el continente africano puede una vez más encontrar en ello la semilla de su propia devastación. (p. 7)

Bibliografía

Chimbelu, C. (9 de junio de 2020). La pandemia de COVID-19 transformará las relaciones entre China y África. *Deutsche Welle*. Recuperado de: https://www.dw.com/es/la-pandemia-de-covid-19-transformar%C3%A1-las-relaciones-entre-china-y-%C3%A1frica/a-53753555

Darío, L. (8 de julio de 2020). Stephen Walt: «La pandemia ha dañado más a Estados Unidos que a China». *Diario Perfil*. Recuperado de: https://www.perfil.com/noticias/internacional/entrevista-a-stephen-walt-dijo-la-pandemia-ha-danado-mas-a-estados-unidos-que-a-china.phtml

Doğru, A. (13 de abril de 2020). Países de África instan a China a detener discriminación por COVID-19. *Agencia Anadolu*. Recuperado de: https://www.aa.com.tr/es/mundo/pa%C3%ADses-de-%C3%A1frica-instan-a-china-a-detener-discriminaci%C3%B3n-por-covid-19/1803291#

Gómez Díaz, D. (2020). China y la construcción de relaciones estratégicas con países de África. Estudio de caso: su postura contradictoria frente al principio de no intervención. *Desafíos*, 32(1), 144-182. Recuperado de: https://revistas.urosario.edu.co/xml/3596/359662515006/html/index.html

González Aspiazu, I. (2016). *La ayuda para el desarrollo de China en África. ¿Una alternativa a las relaciones de cooperación tradicionales?* [Tesis de Grado en Relaciones Internacionales]. Madrid, España: Universidad Complutense de Madrid, Facultad de Ciencias Políticas y Sociología. Recuperado de: https://eprints.ucm.es/48098/1/21-2017-12-21-CT09_Iratxe%20Gonazalez.pdf

Hill J., Ng'Wanakilala F. y Soto A. (10 de septiembre de 2020). El dinero chino le salió muy caro a África. *El Financiero en alianza con Bloomberg*. Recuperado de: https://www.elfinanciero.com.mx/bloomberg-businessweek/el-dinero-chino-le-salio-muy-caro-a-africa

Moral, P. (1 de septiembre de 2019). China en África: del beneficio mutuo a la hegemonía de Pekín. *El Orden Mundial*. Recuperado de: https://elordenmundial.com/china-en-africa/

Observatorio de Política China (5 de septiembre de 2018). *Texto íntegro del discurso de Xi Jinping en la apertura de la Cumbre del Foro de Cooperación China-África*. Galicia, España. Recuperado de: https://politica-china.org/areas/politica-exterior/texto-integro-del-discurso-de-xi-jinping-en-apertura-de-la-cumbre-del-foro-de-cooperacion-china-africa

Rabbia, N. (2015). El continuo y creciente interés chino en África. *Anuario en Relaciones Internacionales del IRI, 2015*. Recuperado de: http://www.iri.edu.ar/publicaciones_iri/anuario/anuario_2015/Africa/5%20El%20continuo%20y%20creciente%20inter%C3%A9s%20chino%20en%20%C3%81frica.pdf

Rodríguez-Rata, A. (15 de abril de 2020). China teje una telaraña sobre el África negra. *La Vanguardia*. Recuperado de: https://www.lavanguardia.com/vanguardia-dossier/20200415/473659844715/china-telarana-recursos-africa.html

Rosales, O. (2019). El conflicto US-China: nueva fase de la globalización. *Estudios internacionales*, *51*(192), 97-126. DOI:10.5354/0719-3769.2019.52820.

—ARTÍCULO—

La política de seguridad estadounidense y el escenario posterior al 11-S: terrorismo, narcotráfico y migraciones (2002-2017)[1]

Dr. Juan Cruz Tisera (UCALP/USAL)

Doctor en Relaciones Internacionales, Universidad del Salvador. Docente titular del Seminario de Doctorado en Metodología de las Ciencias Sociales, del Doctorado en Relaciones Internacionales y del Doctorado en Ciencia Política. Universidad del Salvador. Docente asociado de Relaciones Internacionales I. UCALP. Correo electrónico: jctisera@gmail.com

Resumen

¿Qué ha significado el 11-S para la seguridad internacional? La amenaza terrorista modificó las características de las amenazas transnacionales y generó oportunidades de políticas rigurosas basadas en el miedo. Las diversas estrategias de seguridad aplicadas por las tres administraciones suscitaron la formulación de un proceso de securitización en torno a la lucha contra el terror; de ahí que el narcotráfico, las migraciones, entre otros factores, fueran elevados a la agenda de seguridad. De esta manera, el interrogante por dilucidar plantea: ¿Cómo interactúan las amenazas que forman y articulan la agenda de seguridad de los Estados Unidos? Buscamos responder a nuestro interrogante señalando la implementación de un trinomio de seguridad con relación a los factores: terrorismo-migraciones-narcotráfico. Para ello, utilizaremos las herramientas que nos brindan el constructivismo y la teoría de los complejos de seguridad.

Palabras clave: seguridad internacional, terrorismo, narcotráfico, migraciones.

Abstract

What has 9/11 meant for international security? The terrorist threat modified the characteristics of transnational threats, generating opportunities for rigorous policies based on fear. The various security strategies applied by the three administrations caused the formulation of a securitization process around the fight against terror; hence drug trafficking, migration, among other factors,

[1] El presente ensayo se estructura como resultado parcial y a partir de la asistencia de investigación desarrollada para el proyecto titulado, «Seguridad internacional: crimen transnacional organizado. Debates y propuestas de acción para América Latina». Unidad ejecutora: VRID: 1947. Período: 2019-2021. Facultad de Ciencias Sociales (USAL). Instituto de Investigaciones Científicas y Sociales (IDICSO). Vicerrectorado de Investigación y Desarrollo. Dirección de Investigación.

were elevated to the security agenda. In this way, the question to be clarified rises: How do the threats that form and articulate the United States security agenda interact? We seek to answer our question by pointing out the implementation of a security trinomial in relation to the factors: terrorism-migrations-drug trafficking. For this we will use the tools that Constructivism and the theory of Security Complexes provide us.

Keywords: international security, terrorism, drug trafficking, migrations.

1. Introducción

Debido a las limitaciones de los paradigmas tradicionales y su imposibilidad por explicar la aparición de amenazas transnacionales, hemos decidido utilizar los enfoques reflectivistas que nos permiten la incorporación de una serie de actores a las agendas de seguridad de los Estados. En este punto, es necesario hacer una serie de consideraciones que nos den la posibilidad de ordenar correctamente la instrumentación de nuestra investigación:

1. La primera consideración que tener en cuenta, y que ha sido desarrollada anteriormente, es la clasificación de las amenazas no tradicionales o mal llamadas *nuevas amenazas*. En este caso, tanto el terrorismo como el narcotráfico y las migraciones no tienen nada de nuevo, sino todo lo contrario. «Sí es novedosa su jerarquía dentro de la Seguridad Internacional, en términos comparativos con épocas anteriores de predominio conceptual estadocéntrico» (Bartolomé, 2006: p. 162).

2. A partir de los atentados del 11-S, la seguridad se transformó en un factor decisivo de la política migratoria efectuada por los EE. UU. Siguiendo el trabajo realizado por Fernández de Castro (2006), podemos aseverar que se ha establecido un nuevo paradigma en la relación seguridad-migraciones, a través de tres argumentos: el primero de ellos hace referencia al abandono de la lógica económica y la adopción de las medidas de seguridad; el segundo, sostiene la necesidad de un sistema migratorio ordenado y legal con base en el control fronterizo y su militarización; por último, la restructuración de la administración gubernamental y las reformas al sistema de seguridad nacional.

3. Nuestra tercer aclaración es producto del trabajo realizado por James Rosenau (1997) en torno a la noción de la *confusa frontera*[2], en la que se sostiene la idea de que la separación entre lo doméstico y lo internacional se vuelve confusa y problemática. De esta manera, debemos considerar a las fronteras un asunto problemático, pero, a su vez, un campo de acción.

4. Una cuarta consideración nos obliga a entender las amenazas transnacionales como lógicas interconectadas entre sí, más allá de la intención y del propio Estados Unidos por vincular al terrorismo con otras amenazas; debemos considerar a las amenazas transnacionales productos complejos y no situaciones individuales. Ejemplo de ello,

[2] Denominados *política de fronteras* o *política transversal*, debido a que se abarcan diversos conflictos que traspasan sus límites; a partir de la frontera y no del sistema de Estados es donde se ordenan y resuelven las contradicciones que presenta el sistema internacional (Rosenau, 1997).

lo encontramos en la delincuencia transnacional organizada. El tráfico de personas o aquellas redes que se dedican a pasar inmigrantes de manera irregular; los deterioros de los indicadores socioeconómicos son factores determinantes de expulsión y pobreza; los conflictos estatales o intraestatales generan flujos masivos de migración (a través de los refugiados).

5. La quinta aclaración que tener en cuenta es que, desde la década de los noventa, existía un temor y una necesidad de vincular a los diversos ataques terroristas y las políticas contra los extranjeros: en 1993 el primer atentado contra el World Trade Center; en 1995 la bomba contra el Murrah Federal Building de Oklahoma. Para continuar con los ataques del 11-S, con posterioridad observamos respuestas tendientes a reforzar las leyes fronterizas, lo cual ha aumentado el número de detenciones y deportaciones.

6. Por último, se sitúa en cuanto a la jerarquización de las amenazas. En los Estados Unidos la valoración de las amenazas surge a partir de los enfoques clásicos (realismo), y post 11-S, el terrorismo domina la jerarquía de las amenazas en relación a su peligrosidad directa. Con la administración Trump, asistimos a un realismo 2.0[3].

Los enfoques clásicos determinaron que, en las relaciones internacionales, la seguridad se encontraba atada a la imagen del Estado. Por su parte, los estudios críticos permitirán cruzar la línea del Estado como único actor: en primer lugar, nos centraremos en la participación de los Estados, las sociedades y los individuos en relación con la aparición de amenazas no militares y la construcción de complejos de seguridad regional, y, en segundo lugar, la lucha contra el terrorismo, la securitización de las migraciones y el narcotráfico en torno a la amenaza terrorista.

De esta manera sostenemos que,

> … la seguridad se toma por la búsqueda de la libertad y la capacidad de los Estados y las sociedades para mantener su identidad independiente y su integridad funcional contra las fuerzas del cambio, que consideran hostil. En la línea inferior de la seguridad está la supervivencia, pero también incluye una gama razonablemente substancial de preocupaciones por las condiciones de la existencia. Muy a donde esta gama de preocupaciones deja de merecer la urgencia de la etiqueta de "seguridad" (que identifica amenazas como suficiente para justificar una acción de emergencia y medidas excepcionales incluyendo el uso de la fuerza significativa) y pasa a formar parte de las incertidumbres de la vida cotidiana resulta en una de las dificultades del concepto. (Buzan, 1991: pp. 432-433)

En este sentido nos permitimos hacer referencia a Waltz (1993) cuando sostuvo que se extrañaría a la Guerra Fría en cuanto a su simplicidad, es decir, más allá de los temas económicos, políticos y de seguridad, todos se encontraban atados a las lógicas establecidas por Estados Unidos y la Unión Soviética. Lo predecible también fue señalado por Condoleezza Rice (2001) y la peligrosa inestabilidad actual, ante la estabilidad que

[3] El 17 de diciembre de 2017, la actual Administración daba a conocer su Estrategia de Seguridad Nacional (ESN), en la que volvía a resonar las palabras de Tucídides, quien sostenía que los Estados van a la guerra movilizados por el miedo y sus intereses.

se mantenía en un mundo bipolar. De esta forma, en materia de seguridad, la dimensión que han adquirido las amenazas no tradicionales señala el marco de complejidad que posee el estudio de la seguridad. Claramente no hay temas que prevalezcan y logren una simplificación de las relaciones internacionales. En determinado momento, la agenda está compuesta por el terrorismo; en otros, las amenazas provienen de las armas de destrucción masiva y su proliferación; por momentos, las migraciones masivas y descontroladas se posicionan al tope de las agendas, o el narcotráfico es el tema por combatir. En el caso de los Estados Unidos, y luego del 11-S, ha intentado instalar al terrorismo como el enemigo de antaño, el enemigo que enfrentar por parte del mundo civilizado, y a la lucha contra el terror como el instrumento para contrarrestar a ese enemigo. De esta manera, EE. UU. no observó (o no quiso ver) los diversos problemas que proliferan en las agendas de seguridad. La subordinación de otros tipos de amenazas (migraciones y narcotráfico) a la lucha contra el terror será el eje que dilucidar, es decir, cómo EE. UU. ha articulado los demás factores en su agenda de seguridad.

La política de seguridad empleada por Estados Unidos ha legitimado una política de prevención y de ataque unilateral. «Frente a este contexto, se ofrecen también nuevas estrategias y diferentes justificaciones en las políticas del narcotráfico y la migración» (Chávez, 2008: p. 70). Como resultado de esto, proponemos, en primer lugar, señalar el proceso de securitización regional como producto de la extensión del perímetro de seguridad estadounidense; en segundo lugar, las prácticas estadounidenses señaladas en las diversas ESN, y el condicionamiento del narcotráfico y las migraciones en torno a la lucha contra el terrorismo; en tercer lugar, haremos referencia a la política de seguridad estadounidense señalando sus diversas reformas a partir de cinco grandes áreas; por último, propondremos la retórica propuesta por los Estados Unidos a través del trinomio de seguridad terrorismo-migración-narcotráfico.

2. El perímetro de seguridad de los Estados Unidos y los complejos de seguridad regional (RSCT por sus siglas en inglés)

En palabras de Buzan, el problema de la seguridad «nacional» resulta ser un problema de seguridad sistémica en el que los Estados, las sociedades, los individuos y el sistema juegan un papel fundamental (2007: p. 368). A partir de aquí, nos encontramos en condiciones de sostener que factores económicos, societales y ambientales son tan importantes como las cuestiones políticas y militares, o quizás más. Partiendo de la perspectiva integradora que nos proporciona el estudio de los RSCT, los niveles, sectores y regiones parecen más útiles como plataformas de observación, es decir, como áreas independientes.

Un complejo se define como, «un grupo de unidades cuyos procesos de securitización, desecuritización, o ambos, están tan interconectados que sus problemas de seguridad no pueden ser razonablemente analizados o resueltos en forma separada» (Buzan, Waever y De Wilde, 2008, citado en Bartolomé, 2006: p. 212). Nuestra intención será analizar el

ámbito estatal, centrado en la articulación de la agenda de seguridad estadounidense y en el establecimiento de un perímetro de seguridad regional post 11-S. «La idea central de los RSCT es que, dado que la mayoría de las amenazas viajan más fácilmente sobre corta distancia, la interdependencia de seguridad normalmente se modela en el nivel regional basado en grupos: los complejos de seguridad» (Buzan y Waever, 2003: p. 4).

Durante el siglo xx y el inicio del siglo xxi, América del Norte se constituyó como un RSCT atípico, donde los Estados Unidos son el poder clave en la configuración de los asuntos por securitizar de la región; pero, en general, el país no pensó en términos regionales y actuó principalmente en sus preocupaciones en el ámbito estatal. De ahí que la conformación de un complejo regional fuese un subproducto de sus preocupaciones a nivel estatal e interestatal. Frente a las diversas amenazas y la complejidad del sistema internacional, los EE. UU. necesitaron reconocer a la región como el primer punto de vulnerabilidad hacia su territorio. Esta postura no es para nada nueva, al contrario, la podemos rastrear a diversos mecanismos que ha implementado, por ejemplo, la aplicación de la doctrina Monroe[4], o el Tratado de Asistencia Recíproca[5]. En la actualidad, el condicionante principal es el terrorismo y la aplicación de la doctrina de la guerra preventiva[6]. De esta manera, los demás asuntos forman parte de la extensión del perímetro de seguridad para enfrentar los problemas de seguridad que afectan a la región.

El establecimiento de un área de riesgo permite la configuración adoptada por los EE. UU. en lo que Tokatlian (2004) definió como el *mare nostrum*; de esta manera, se confecciona un perímetro de defensa. Históricamente, se estableció en virtud de la aparición de gobiernos autoritarios o asociados a factores ideológicos (cercanos a la Unión Soviética); en otras etapas, la acción de defensa se convirtió en una intervención como mecanismos para afianzar su propia seguridad (el caso de las intervenciones militares en

---

[4] La doctrina Monroe es un principio jurídico inscripto en el derecho internacional, creado por el presidente James Monroe en 1823 y sintetizado en la famosa frase «América para los americanos». La doctrina sostenía el principio de no intervención de los Estados europeos en los países de América, presentándose como parte de defensa ante los procesos de independencia de los países del continente americano. Debemos aclarar que, en nuestra opinión, esta doctrina es más bien un acto político unilateral, en lo que Carl Schmitt denomino como el «imperialismo moderno» ejercido por los EE. UU. (Schmitt, 2001: p. 197).

[5] La Resolución VIII de la Conferencia Interamericana sobre Problemas de la Guerra y de la Paz recomendó la celebración de un tratado destinado a prevenir y reprimir las amenazas y los actos de agresión contra cualquiera de los países de América; a fin de perfeccionar los procedimientos de solución pacifica de sus controversias, se proponen celebrar el Tratado sobre «Sistema Interamericano de Paz», previsto en las Resoluciones IX y XXXIX de la Conferencia Interamericana sobre Problemas de la Guerra y de la Paz, donde la obligación de mutua ayuda y de común defensa de las repúblicas americanas se halla esencialmente ligada a sus ideales democráticos y a su voluntad de permanente cooperación para realizar los principios y propósitos de una política de paz. El Tratado Interamericano de Asistencia Recíproca fue adoptado en Brasil en 1947. Para el texto completo, ver: Departamento de Derecho Internacional: OEA, versión *online* www.oas.org.

[6] La doctrina de la guerra preventiva (*Preemptive Action Doctrine*) surge con posterioridad a los ataques terroristas del 11-S en contra del terrorismo; consiste en atacar en primera instancia al más mínimo de sospecha ante evidencias de que hay grupos terroristas dispuestos a atacar a los Estados Unidos. A su vez, se considera del mismo modo a aquellos Estados que patrocinen a estos grupos, considerándolos enemigos (Estrategia de Seguridad Nacional de los Estados Unidos, 2002).

Centro América y el Caribe); en la actualidad, «los temas de seguridad y vulnerabilidad de Latinoamérica se edifican desde construcciones de amenazas erigidas a partir del terrorismo» (Chávez, 2008: p. 100). A partir de esta definición, podemos aseverar la percepción de los Estados Unidos en relación con lo que establecen como la conjunción entre terrorismo y narcotráfico (narcoterrorismo) y terrorismo e inmigración.

El establecimiento de un complejo de seguridad regional no implica necesariamente el involucramiento directo, pero sí «la implementación de una soberanía efectiva» (Bagley, 2006: p. 64). De esta manera, EE. UU. pretende ejercer un control efectivo, ya sea a través de asistencia o de intervención directa. Es decir que la instauración de un perímetro de seguridad busca lograr un control efectivo de la región. En virtud de lo señalado, visualizamos dos puntos centrales que nos permiten especificar la expansión del perímetro de seguridad a partir del establecimiento de un complejo de seguridad regional: el primero de los casos lo encontramos en la conjunción entre terrorismo y narcotráfico. La política contra el narcoterrorismo se visualiza en tres zonas de la región; el más lejano en el tiempo es Colombia y la necesidad de intervención en la región para evitar el efecto contagio; post 11-S, dos zonas se enfocaron en la mira, la triple frontera entre Argentina, Brasil y Paraguay, y la posible existencia de grupos terroristas; la última zona es la frontera entre México y los Estados Unidos, y la potencial relación entre el crimen organizado y los grupos terroristas.

El segundo de los casos se establece en relación con la percepción de la amenaza que implica el ingreso de inmigrantes indocumentados en fronteras totalmente porosas: espacios no gobernados o zonas grises como posibles mecanismos de utilización por parte de grupos terroristas.

La contribución de Buzan al estudio de la seguridad regional nos permite comprender cómo Estados Unidos ha intentado establecer, a partir de su política de seguridad regional, un complejo regional de seguridad con la intención de atender temas y securitizar asuntos regionales con repercusiones globales. A partir de aquí, podemos señalar el propósito de los diversos gobiernos estadounidenses por aquello que denominamos *el trinomio de seguridad*: terrorismo-migraciones-narcotráfico. Para poder definir adecuadamente la noción de seguridad regional, debemos considerar nuevamente los aportes de Buzan, quien sostiene que «la seguridad es un fenómeno relacional. Dado que la seguridad es relacional, no se la puede entender sin comprender el patrón internacional de la interdependencia en el sector de seguridad, la cual está incrustado» (2007: p. 187).

En el análisis de la seguridad regional y cómo esta afecta al conjunto, Buzan nos permite visualizar algunos conceptos sumamente interesantes y pertinentes para nuestra investigación. La primera de ellas es la relación entre «Amistad» y «Enemistad» entre Estados (2007: p. 189). De esta manera, podemos afirmar que las relaciones entre los Estados se pueden representar a través de una amistad que es traducida en una alianza (la cual podría ser establecida por el temor o el miedo).

Ahora bien, ¿cuáles serían los problemas que pueden afectar estos sentimientos? Si nos situáramos en un contexto de guerra fría, el ideológico fue el sentimiento que

posibilitó el establecimiento de complejos de seguridad tanto de un lado como del otro. Pero en la actualidad, estos sentimientos se encuentran atados a las cuestiones de fronteras y territorios, y esto es importante para conducirnos a la definición de los complejos de seguridad regional, entendidos como «un grupo de Estados cuyas preocupaciones de seguridad se encuentran lo suficientemente cerca que sus valores nacionales no pueden ser considerados de manera realista distanciados uno del otro» (Buzan, 2007: p. 190).

La intención de un complejo de seguridad regional es la unificación bajo intereses compartidos. Estos complejos pueden ser útiles de dos maneras: la primera de ellas guarda una intencionalidad política, como marco de las presiones por resolver temas cruciales y que se encuentran en el debate de seguridad actual; la segunda, como marco de discusión a partir de temas endémicos propios de la región. A partir de aquí, la política de seguridad estadounidense ha pretendido encontrar la solución dentro del contexto de un complejo de seguridad regional. El problema surge en el establecimiento de las jerarquías del problema de seguridad que se encuentra estrechamente ligado entre lo doméstico y lo global.

3. Las estrategias de seguridad nacional de Estados Unidos en el contexto de las amenazas transnacionales (2002-2017)

Históricamente, las estrategias[7] de seguridad nacional (ESN) reflejan una visión general más allá de las visiones de ambos partidos; se instituyen como mecanismos que establecen las líneas centrales para orientar la política de seguridad de los EE.UU. Cuando se señala la política exterior de seguridad nacional, debemos marcar que ella es llevada a cabo a través de doctrinas o estrategias de seguridad. En este sentido:

> Una doctrina de seguridad nacional es un conjunto de enunciados que expresa las visiones generales que los líderes políticos tienen acerca de cuáles son las oportunidades y amenazas que enfrenta el país y propone un conjunto desagregado de estrategias para hacer frente a ese escenario. (Calle y Merke, 2005: p. 125)

Es decir, de manera simplificada, las estrategias proponen una «imagen del mundo» que delimitan los temas por tratar.

[7] Es fundamental realizar una definición del término estrategia para la comprensión de dicho concepto y señalar el objetivo de este, es decir, preservar la seguridad nacional. David Abshire sostiene que «originalmente fue una materia militar concerniente al uso de los instrumentos de guerra para alcanzar la victoria. Hoy, sin embargo, las dimensiones de la estrategia se han expandido y debe ser una preocupación de tiempo de paz... Mucha gente piensa que una estrategia es simplemente un plan. […] El término fue derivado del griego *strategos*, que significaba el 'arte' del general, no el "plan" del general. Arte es el arreglo de elementos de una manera tal que crea un todo que es mayor que la suma de sus elementos. Esto es tan verdadero para estrategias en tiempo de paz como en las de guerra. Un plan, si es fijo y estereotipado, es en realidad lo opuesto a una verdadera buena estrategia. Estrategia incluye tener un concepto, prioridades y una dirección —una que sea flexible y adaptable a situaciones cambiantes— para la distribución racional y disciplinada de recursos para alcanzar objetivos específicos» (Abshire, 1988). Como sostiene John Gaddis (1982), la estrategia es «simplemente el proceso por el que los fines son relacionados a los medios, intenciones a las capacidades y objetivos a recursos».

3.1. La administración Bush y las ESN de 2002 y 2006

George W. Bush, en el año 2002, estableció su ESN[8] teniendo como principal antecedente a los atentados del 11-S, por lo que el interés que motivó y ocupó prácticamente toda la escena de dicho documento fue este hecho, su evolución y su posterior tratamiento. Podemos decir que, así como en otros años[9], la estrategia del 2002 definió sus intereses en términos de amenazas.

La estrategia basada en la guerra contra el terror constará de nueve secciones, donde ocho de ellas se establecen en torno a la necesidad de luchar contra el mal, contra el terrorismo, contra aquellos (Estados patrocinadores) que presentan una amenaza para la seguridad nacional e internacional, pues la necesidad de continuar siendo los guardianes del orden y erigirse como los «paladines de la humanidad» se encuentran como instrumentos presentes en todo el documento; podemos sostener esto en frases como: «la causa de nuestra nación ha sido siempre más grande que la defensa de nuestra nación [...]. Debemos eliminar estas amenazas a nuestra nación, a nuestros aliados y amigos […]. Estados Unidos debe defender la libertad y la justicia porque estos principios son justos y verdaderos para la gente de todas partes». (ESN, 2002: p. 20).

El compromiso que se establece en el documento es la defensa de la nación contra sus enemigos, a través de dos grandes estrategias:

- La primera de ella es con relación al ámbito internacional. El establecimiento de la doctrina de la guerra preventiva; en términos prácticos, ante la mínima sospecha de recibir un ataque, la acción deberá ser la rápida respuesta militar.

---

[8] Respecto al diseño de las diferentes estrategias de seguridad, ellas se elaboran por parte del «Consejo de Seguridad Nacional para traducir la visión presidencial en objetivos concretos para orientar el planeamiento y ejecución del resto de los actores diplomáticos, económicos o militares del sistema de seguridad. La coordinación de los planeamientos no es fácil porque cada uno de los diferentes sistemas tiene su propia visión de los intereses y objetivos nacionales de seguridad de acuerdo con su tradición y papel corporativo, además de las diferencias de ideología que ostentan sus líderes. La diversificación de las lógicas según su adscripción al realismo o al neoconservadurismo, al unilateralismo o el multilateralismo, no sólo afecta a los niveles superiores de decisión, sino que se van entremezclando en los escalones inferiores. Por otro lado, la capacidad de planeamiento cuenta a la hora de influir en la estrategia final y, por eso, la Casa Blanca se ha ido apoyando en la mayor capacidad de planeamiento estratégico del sistema de defensa, sobrecargando el sistema en su propio perjuicio y postergando a otros departamentos, con el consiguiente distanciamiento de los procesos de planeamiento entre agencias. Como alternativa, los expertos recomendaron generar e integrar las capacidades de previsión a largo plazo de los sistemas de planeamiento no militares, de forma que se tengan en cuenta sus opiniones en la fase de definición de la propia estrategia de seguridad antes de promulgarla. Por esa razón, la NSS de 2006 propone reforzar la capacidad de planeamiento de todas las agencias y departamentos, orientándola hacia los resultados y facilitando la cooperación entre ellos. Si se aplican bien estas medidas, no sólo mejorará el diseño inicial, sino que su ejecución encontrará menos resistencias y, sobre todo, se evitará que algún miembro del sistema se sienta excluido del planeamiento» (Arteaga, 2006: p. 2).

[9] «En el año 1950 la amenaza a la seguridad, la libertad y la democracia provenía del comunismo, el cual debía ser contenido. En el 2002 la amenaza viene del eje del mal, el cual deber ser combatido. Así como la estrategia de contención de Kennan sufrió modificaciones a través del NSC68, el marco estratégico y conceptual que fue desarrollando los EE. UU. en la década posterior al fin de la guerra fría fue sustancialmente acelerado y readaptado a partir del 11/9» (Calle y Merke, 2005: pp. 127-128).

- La segunda es la reforma administrativa más amplia de los últimos años y se da en la esfera doméstica. En el año 2002, se creó el Departamento de Seguridad Interna (DHS, por sus siglas en inglés), que incorpora 22 agencias federales.

En la Introducción de la ESN del 2002, se presenta a los Estados Unidos en relación con su poderío militar y su influencia política y económica, y dejan en claro que «en un mundo a salvo de peligros, la gente estará en condiciones de mejorar sus propias vidas», por eso lucharán y defenderán la paz «contra los terroristas y los tiranos […] redes oscuras de individuos pueden traer gran caos y sufrimiento a nuestras costas por menos de lo que cuesta comprar un solo tanque» (ESN, 2002: Introducción). Las doctrinas de las diferentes estrategias han girado a través del péndulo teórico realismo-idealismo; en virtud de esto la política exterior gira alrededor de principios morales o en términos de relación de poder militar. En esta estrategia, encontramos una fuerte carga con relación al poder militar; el discurso de la administración Bush se encargó de que así fuera.

La administración Bush consideró que es condición necesaria para derrotar esta amenaza la utilización de cada herramienta disponible, ya sea: «el poderío militar, la defensa mejorada de nuestro territorio nacional, la aplicación de la ley, la recopilación de inteligencia, y gestiones vigorosas para cortarles el financiamiento a los terroristas» (ESN, 2002: p. 24). Bush en este documento dejó expuesta su postura frente a este tema señalando que los Estados Unidos contribuirá y ayudará a todos aquellos países que estén dispuestos a combatir el terrorismo, así como hará responsable a todos aquellos que den refugio a terroristas o estén comprometidos con su causa, «porque los aliados del terrorismo son enemigos de la civilización» (ESN, 2002: Introducción).

Una frase muy interesante dentro de este documento es la que planteó el presidente Bush en relación con la autodefensa y los Estados considerados frágiles, al señalar que Estados Unidos actuará contra esas amenazas en surgimiento antes de que estas terminen de formarse. Los Estados Unidos de América libran una guerra contra terroristas esparcidos por todo el mundo. El enemigo no es un régimen político, persona, religión o ideología aislados, sino el terrorismo premeditado, la violencia por motivos políticos perpetrada contra seres inocentes. Esto es utilizado para definir quién es el enemigo, marcando un punto de justificación frente a las invasiones que se estaban dando y las que vendrían con posterioridad: Afganistán, considerada como la cuna de los terroristas y culpable de los atentados del 11-S; e Irak, supuesto poseedor de armas de destrucción masiva. Es importante, acerca de la propuesta de nuestra investigación, considerar cómo el enemigo ha dejado de ser un Estado para pasar a un conjunto de actores de naturaleza no estatal conformado a partir de redes que penetran las fronteras de los Estados; esto refuerza el carácter transnacional de las amenazas en el actual contexto internacional.

La administración Bush reflejó en este documento la necesidad de «adaptar el concepto de amenaza inminente a las capacidades y objetivos de los adversarios de hoy» (ESN, 2002: Parte V). Si bien coincidimos en que es sumamente necesario que se readapten los

distintos conceptos, en especial el término de amenaza, resulta, al mismo tiempo, un arma de doble filo, pues, si bien, por un lado, permitiría un pronto accionar al atacar la causa de raíz y no dar lugar al desarrollo evolutivo, por otro, otorgaría libertad de acción cuando se considere la percepción de una amenaza. Y este es el punto que se pregonó en relación con las estrategias presentadas por la administración Bush: el establecimiento del enemigo, el terror, la utilización del eje del mal.

En el marco de la guerra contra el terror, en el año 2006 surge una nueva versión de la ESN, de tinte continuista, y agregando los riesgos, productos de la globalización y de un sistema internacional sumamente complejo en el que hay situaciones derivadas del crimen organizado como el narcotráfico, el tráfico de personas, desastres naturales, pandemias y en el que el terrorismo continúa siendo la principal amenaza de los Estados Unidos. En palabras de Bartolomé (2004), pasamos de un tablero de juego de corte realista a la incorporación de una agenda de seguridad caracterizada por las nuevas amenazas de naturaleza transnacional.

A la utilización de los instrumentos militares y la acción unilateral, se le agrega una combinación entre instrumentos no militares y acciones multilaterales, sobre todo en virtud de las consecuencias de una guerra larga y con fuertes críticas del orden internacional. Más allá de esto, se mantiene la doctrina de la guerra preventiva señalada en la anterior estrategia, «con el objetivo de prevenir actos hostiles y en ejercicio de la legítima defensa» (ESN, 2006: p. 10). La diferencia sustancial de esta estrategia señala que, más allá del rol del terrorismo, existen varias amenazas, como la inmigración indocumentada, el narcotráfico y gobiernos autoritarios. Como hemos sostenido anteriormente, la ampliación de las amenazas, referidas a la lucha contra el terror, no impide —y en la práctica sucede— que los EE. UU. vinculen a la amenaza terrorista con el aumento de la inmigración masiva e indocumentada y la lucha contra el narcotráfico.

En relación con América Latina, la ESN de 2006 recorre tres escenarios de interés, de los cuales uno de ellos hace referencia al contexto creciente de la inmigración indocumentada, sobre todo aquella proveniente de México. Se señala como una preocupación (amenaza) que debe ser atendida en lo que respecta a la lucha contra el terrorismo. Los otros dos puntos harán referencia al escenario del narcoterrorismo en Colombia y al efecto contagio del presidente de Venezuela Hugo Chávez en un escenario de ideario tiránico y prácticas populistas.

1. «Tenemos que seguir trabajando con nuestros vecinos en el hemisferio para reducir la inmigración ilegal» (ESN, 2006: p. 37). En lo concerniente a la inmigración, la ESN de 2006 hace referencia al carácter «ilegal» de la inmigración y la amenaza que esto implica para el territorio estadounidense, de ahí la necesidad y la continuidad en la extensión del perímetro a través de su frontera sur.
2. En Colombia, país democrático y aliado de los EE. UU., se encuentra luchando contra terroristas y narcotraficantes. Luego del 11-S se observó en las diferentes ESN el vínculo entre terrorismo y narcotráfico que determinaba «el surgimiento de una gra-

ve amenaza, el narcoterrorismo, que debe ser enfrentada por medio del instrumento militar» (Vega y Miccinilli, 2007: p. 69).

3. «En Venezuela se intenta socavar la democracia, tratando de desestabilizar la región» (ESN, 2006: p. 15). La preocupación señalada en la ESN de 2006 por el caso de Venezuela se encuentra relacionada a una posible extensión de gobiernos populistas y autoritarios, producto del efecto contagio de Venezuela ante discursos antiestadounidenses.

3.2. La administración de Barack Obama y la ESN de 2010 y 2015

El deterioro de la política aplicada por la administración Bush y la fuerte condena por las invasiones de Irak y Afganistán se presentaron como los dos ejes de la nueva ESN de 2010. En su discurso inaugural, el presidente Obama sentó las bases de lo que sería su mirada internacional y su desempeño como máxima autoridad del país. Las dos guerras iniciadas —Afganistán e Irak—, la preocupación por las armas de destrucción masiva (ADM), la lucha contra el crimen organizado y las migraciones «ilegales» sentaron las bases para la elaboración de la ESN durante el primer mandato de Obama. En mayo de 2010, fue anunciada la nueva ESN, rompiendo con las anteriores al señalar que los EE. UU. habían dejado de estar en guerra. El documento propuesto por la administración generó estrategias basadas en la comprensión global de las nuevas amenazas y la no centralización en la guerra. Según González (2010), se establece la idea de transición sobre nuevos poderes emergentes, enfrentados al viejo orden económico en crisis, lo cual provoca una disminución de la centralidad del instrumento militar, y se señala el énfasis en el uso de las instituciones internacionales.

Es sumamente interesante para nuestra investigación cuando esta estrategia sostiene la necesidad de construir una base sólida para el liderazgo dentro de las fronteras; se prevé una mayor seguridad, un mejor compromiso y una mejor efectividad de la frontera hacia afuera, pues nuestra seguridad comienza por casa, y la fuerza viene desde adentro (ESN, 2010: p. 4).

Entre las prioridades que establecen los Estados Unidos en este documento y que nos permitimos destacar, se encuentra la siguiente: renovar el liderazgo a largo plazo. Este enfoque se encuentra presente en toda la ESN.

> Estados Unidos sigue siendo la única nación capaz de proyectar y sostener las operaciones militares a gran escala en distancias extensas […]. Mantener capacidades superiores para disuadir y derrotar a los enemigos y para garantizar la credibilidad de las asociaciones de seguridad que son fundamentales para la seguridad regional y global. Nuestro ejército continúa apuntalando nuestra seguridad nacional y el liderazgo global, y cuando lo usamos adecuadamente, se refuerzan ambos. (2010: p. 20)

La seguridad del pueblo estadounidense se estableció a partir de dos ejes: en primer lugar, evitar la proliferación de las ADM,

> … más naciones han adquirido armas nucleares. Los terroristas están decididos a comprar, construir o robar un arma nuclear. Nuestros esfuerzos para contener esos peligros se centran en un régimen de no proliferación mundial […]. No obstante, "mientras existan las armas nucleares, los Estados Unidos mantendrán un arsenal nuclear seguro y eficaz, tanto para disuadir a adversarios potenciales como para asegurar a aliados de Estados Unidos y otros socios de seguridad de que pueden contar con Estados Unidos. (ESN, 2010: p. 25)

En segundo lugar, la seguridad consiste en desmantelar y derrotar a Al Qaeda y sus aliados a través de una estrategia global sostenida e integrada.

3.3. La administración Donald Trump y la ESN 2017

El 17 de diciembre de 2017, la administración Trump anunció su nueva ESN, una estrategia que apunta a un realismo 2.0. Rememorando a Tucídides (460 a. c.) cuando afirmaba que los Estados van a la guerra movilizados por el miedo, el orgullo y los intereses, la actual estrategia trae nuevamente al gran historiador y padre histórico del realismo clásico. McMaster señaló cómo la actual administración percibe las amenazas y las posibilidades del sistema internacional que les toca enfrentar.

La estrategia de seguridad nacional de Trump pretende recuperar el concepto de fronteras seguras. En seguridad interior, aparece la necesidad de un muro en la frontera con México para abordar la masiva llegada de inmigrantes indocumentados, el endurecimiento de los controles migratorios y la reforma de los flujos de migración legal. Estos puntos forman parte de lo que fue su campaña electoral y que la actual administración advierte en relación con la amenaza más cercana, aquella que se encuentra fronteras adentro.

> La Estrategia busca pasar de «liderar desde atrás» a involucrarse en una dura competición global en la que EE. UU. buscará recuperar terreno en el ámbito de las nuevas tecnologías y la innovación, y adaptarse a la competición que ha llegado al ciberespacio y el espacio. Y siempre tratando de priorizar los intereses de EE. UU. bajo el concepto de «América primero» y de competir más que de colaborar. (García Encina, 2018: p. 3)

La ESN se determina a partir de tres apartados que señalan diversos retadores a la seguridad de los Estados Unidos:

1. Poderes revisionistas; es sumamente interesante este concepto pues hace alusión a adversarios ideológicos que «buscan dar formas a un mundo antiético a nuestros intereses y valores» (ESN, 2017: p. 2), y aquí se incluye a China y Rusia.
2. Regímenes deshonestos, refiriéndose a «Estados fallidos»: aquellos que brindan apoyo a grupos terroristas.

3. Organizaciones terroristas internacionales, donde la lucha contra el ISIS se establece como la más importante amenaza a su seguridad.

Dentro de su estrategia, el ciberespacio, y de forma ampliada la ciberseguridad, ocupa una posición relevante; en este sentido, se observa una mirada hacia el realismo político al afirmar que los Estados Unidos necesitan retomar el dominio del espacio. El documento establece que el uso de ciberherramientas ha permitido que Estados y actores no estatales dañen a los Estados Unidos (ESN, 2017). Podemos destacar que la visión de la actual administración sobre las actividades que se desarrollan en el ciberespacio puede y debe ser utilizada para derrotar a los grupos terroristas. Se necesita abordar el reto que supone internet, entendida como el refugio de los terroristas que usan plataformas para evadir su detección.

Cabe destacar que estos apartados se determinan a partir de una mirada claramente realista por parte de la actual administración. Subrayamos que la ESN de 2017 es realista porque reconoce el papel central del poder internacional, definiendo claramente sus intereses nacionales en términos de poder; a su vez, anuncia el avance de los principios americanos de difusión de paz y prosperidad. Nos parece interesante cuando Federico Merke (2018) señala que «la estrategia de seguridad parece orientarse por un realismo de principios que combina, ante todo, una mirada basada en el interés nacional, aunque acompañada de valores que defiende la sociedad norteamericana».

El *American First* continúa presente, pero reinventado en premisas del pasado que buscan construir un orden global basado en reglas. Trump sostiene que las actuales reglas son un obstáculo a la primacía de los Estados Unidos. Durante su ESN, se observa un análisis material basado en un juego de suma cero. «Su poder militar debe prevalecer frente al resto, mejorando las capacidades tecnológicas, humanas y organizativas para defender el territorio norteamericano y sus intereses en el exterior, ya sea de ataques directos o cibernéticos de actores estatales y no estatales» (Llenderrozas, 2018: p. 16).

Como conclusión, la actual estrategia pretende resolver problemáticas estructurales y que se plantean a largo plazo. Ahora, ¿el retorno al realismo político es la solución? En este sentido, tomamos el último ensayo de Allison (2017), en el que repasa 16 momentos y casos donde las principales potencias de cada etapa histórica tuvieron que enfrentar desafíos políticos, económicos y militares de un competidor de gran peso. El autor hace una clara referencia a China como ese adversario, sosteniendo que, en 12 oportunidades, la tensión derivó en grandes guerras por la hegemonía. Ese repaso histórico busca moderar la posibilidad de que, en las próximas décadas, el caso 17, o sea, Estados Unidos contra China, pase a ser el número 13. Un número de mala suerte en la cultura popular norteamericana; no así en China, donde es el número 4. Si de cábalas se trata, 13 y 4 dan 17.

3.4. Medidas para fortalecer la seguridad post 11-S

Siguiendo la línea de Rafael Fernández de Castro (2006), el autor se pregunta por qué las autoridades migratorias estadounidenses no interceptaron a los terroristas y, de alguna manera, le permitieron perpetrar sus ataques dentro del territorio norteamericano. El informe de la Comisión del 11-S concluye que las autoridades migratorias no tenían en mente el aspecto seguridad; por el contrario, su principal preocupación estaba en evitar la entrada de indocumentados en busca de empleos. En EE. UU., la política migratoria y los criterios para pensarla y formularla tienen un antes y un después del 11-S. Antes, el radar de las autoridades migratorias no abarcaba la seguridad nacional. A partir del 11-S, la seguridad se convirtió en un factor decisivo de la política migratoria de EE. UU. En otras palabras: el objetivo primordial de la autoridad migratoria dejó de ser el de impedir el ingreso de los trabajadores no autorizados; la nueva meta es impedir la entrada de terroristas (2006). En general, vamos a destacar cinco grandes áreas en relación con las medidas de seguridad post atentados de 2001[10]:

• **Restructuración del sector administrativo:** este primer punto de reforma se da a partir del aumento de asignaciones presupuestarias con referencia al personal de las patrullas fronterizas, controles más estrictos en los puntos de ingreso, la necesidad de coordinación entre las diferentes oficinas. Dentro de este punto, se estableció, a partir del Acta de Seguridad Interna en 2002, uno de los mayores movimientos de restructuración burocrática. La primera política de seguridad fue la creación del Departamento de Seguridad Interna (DHS). Esta oficina reunió para su control y centralización 22 agencias, entre las que destacamos al Servicio de Ciudadanía e Inmigración, encargado de la expedición de visas, pedidos de asilo y de refugiados; la Patrulla Fronteriza, orientada a la detención de terroristas y con aplicación en contra de inmigrantes (que es lo que sucede en la realidad); el Servicio de Aduanas, a cargo del control en la entrada de personas y mercancías, y la Guardia Costera.

• **Sistemas de información e identificación:** se introdujeron nuevos sistemas de identificación a través de documentos y pasaportes con códigos electrónicos, además del uso de técnicas biométricas. «La introducción de estos nuevos sistemas implica, también, una vasta recolección y compilación de datos por diversas entidades de control» (Artola, 2005: p. 138). En el 2003, se empezó a aplicar el escaneo digital y el uso de la fotografía para ampliar la información personal del viajero y brindar, de esta manera, una mayor información al oficial de aduana. Este desplazamiento desempeña un papel fundamental, ya que permite obtener de manera anticipada información acerca de las personas que tienen intenciones de ingresar al país.

• **Aumento del control en las fronteras:** la implementación y determinación de las amenazas transnacionales posibilitó la aplicación de medidas de control y anticipación

[10] Parte I: Panorama General de la Estrategia Internacional de Estados Unidos (2002).

como herramientas claves en el ingreso por fronteras sumamente porosas. En el 2017, la actual administración firmó la orden ejecutiva titulada «Seguridad Interna y Mejoramiento de la Vigilancia Migratoria» (Office of the Federal Register, 2017, Executive Order 13767). Lo más relevante en esta orden, además de la construcción del muro (sección 2, apartado a), es que se establece un escalamiento en la remoción de quienes hayan violado leyes migratorias o de cualquier otro orden, ya sea federal o estatal (sección 2d, 2c; sección 5b y 5c).

• **Controles migratorios internos:** a las diferentes medidas, se debe agregar la ejecución de restricciones en la obtención de visados, residencias, trabajadores temporales, refugiados y aquellos que solicitan asilo. Un ejemplo de esta situación se refiere a la orden ejecutiva de 2017 conocida como «Mejorando la Seguridad Pública en el Interior de Estados Unidos» (Office of the Federal Register, 2017, Executive Order 13768), la cual establece de manera preocupante un discurso que permite la criminalización de la migración indocumentada.

• **Cooperación regional:** la seguridad puertas adentro de cualquier Estado no puede realizarse sin entender el contexto regional**.** En marzo de 2005, los tres países firmaron La Alianza para la Seguridad y la Prosperidad de América del Norte (ASPAN); sin embargo, estos no reflejaron una política de seguridad regional. En la actualidad, la cooperación se ha vuelto netamente doméstica en relación a cooperar con las autoridades locales, estableciéndose acuerdos federales-estatales para aplicar leyes migratorias.

Tras los ataques terroristas del 11-S, mutó la visión del gobierno estadounidense sobre la inmigración indocumentada, fundamentalmente ante la posibilidad de que grupos terroristas se sirvan de las rutas fronterizas para internarse en el territorio de los EE. UU. La reacción inmediata del gobierno de G. W. Bush fue la de establecer un proceso de securitización del fenómeno migratorio a través de diferentes medidas que se fueron ampliado durante la administración Obama, profundizas con el presidente Trump. Durante la actual administración, se estableció un aumento del presupuesto de defensa en más de 54000 millones de dólares, lo que constituyó el mayor aumento presupuestario del Pentágono desde los atentados del 11-S (Manassero y Tisera, 2019).

Las estrategias utilizadas por las administraciones estudiadas luego de los ataques terroristas nos permiten visualizar acciones claras y definidas: en primer lugar, la reacción inmediata a través de la doctrina de la guerra preventiva (Bush); en segundo lugar, una política doméstica cuya acción principal es desarrollada por el DHS a partir del desarrollo del concepto de seguridad hemisférica (continuada por Obama). Dentro de este punto, es interesante observar cómo los Estados Unidos han militarizado su frontera. Con respecto a esta situación, Timothy Dunn sostiene la aplicación de la doctrina Low-intensity conflict (LIC)[11], visualizada a partir de acciones específicas, como el empleo de drones de vigilancia, mallas metálicas, el aumento de estaciones de control por parte de la patrulla

[11] Para un mayor análisis sobre este punto, ver ESN (2017).

fronteriza, la participación de la Guardia Nacional; en definitiva, la militarización de la frontera. Por último, se construyó un discurso que se materializa, a partir del binomio terrorismo-migraciones (Trump), en una propaganda que señala al inmigrante como enemigo, amenaza y riesgo para la seguridad y para la vida pública.

4. Trinomio de seguridad terrorismo-migración-narcotráfico

¿Qué ha significado el 11-S para la seguridad internacional? La amenaza terrorista modificó las características de las amenazas transnacionales y generó oportunidades de políticas rigurosas basadas en el miedo. La aplicación de la doctrina Bush provocó la formulación de un proceso de securitización en torno a la lucha contra el terror; de ahí que el narcotráfico y las migraciones fueran elevados a un nivel superior de la agenda de seguridad. Por ello y de acuerdo a nuestro planteo del problema, mostramos cómo interactúan las amenazas que conforman la agenda de seguridad de los Estados Unidos.

Proponemos el análisis a partir del denominado trinomio de seguridad. En álgebra un trinomio es definido como la suma indicada de tres monomios distintos, es decir, un polinomio con tres términos que no pueden simplificarse más. Algunas consideraciones a tener en cuenta a partir de esta definición: cuando hacemos referencia a los tres factores de seguridad, claramente nos estamos refiriendo a amenazas transnacionales, pero manifiestamente de naturaleza diferente. A su vez, cuando se hace referencia a términos que no pueden simplificarse más, debemos considerar que no estamos ante una ciencia dura; un cambio en la estrategia podría sacar a uno de los factores de la agenda de seguridad.

La fórmula propuesta para realizar un mejor análisis de las ESN pretende una simplificación de esta complejidad y puede ser vista como Tx + Mx + Nx = ESN, donde T = terrorismo, M = migraciones, N = narcotráfico, x = amenazas transnacionales.

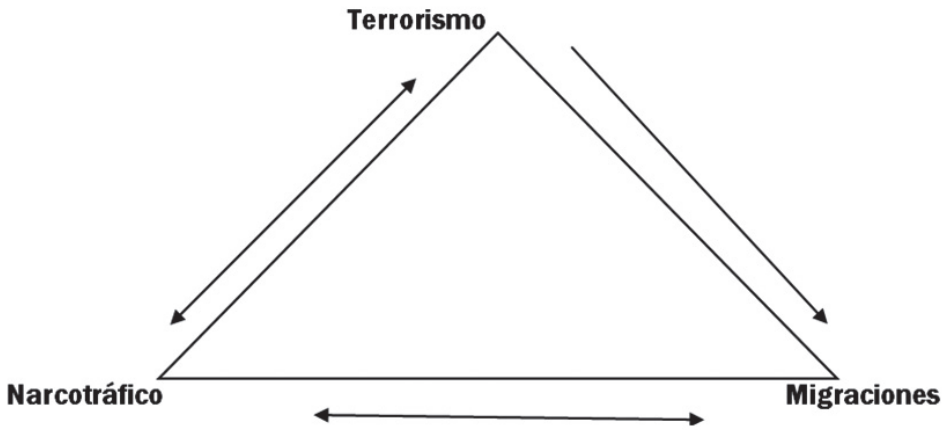
A partir de la ESN de 2002, observamos cómo los EE. UU. establecieron una misma estrategia de seguridad en relación con la guerra contra el terrorismo, es decir, una simplificación de monomios, que permiten, por ejemplo, que se trate de la misma manera a terroristas, narcotraficantes e inmigrantes. Para aclarar aún más esta situación, podemos observar que, desde la consideración del propio EE. UU., el posicionamiento de las FARC como grupo terroristas que utiliza la venta de drogas para su financiamiento genera el llamado *narcoterrorismo*, lo cual permite a los Estados Unidos considerar como lo mismo a las FARC o al ISIS; esto nos deja entender la simplificación de la estrategia de seguridad.

En este complejo de securitización, encontramos diversos elementos por considerar: en primer lugar, la percepción por parte del gobierno o las sociedades de una amenaza a partir de ciertos criterios que permiten su securitización, legitimando, de esta manera, acciones contra estas amenazas. «La construcción de amenazas de seguridad no necesariamente implica la utilización de mecanismos militares y el uso de la fuerza; sin embargo, en las reflexiones desarrolladas se evidencian un alto componente militar» (Chávez, 2008: p. 72). En segundo lugar, y desde el prisma del Estado, se articulan políticas que son elaboradas

desde el DHS, la Secretaría de Estado y las diversas oficinas de inteligencia. En tercer lugar, nos encontramos en el espacio del discurso traducido en la práctica a partir de relatos securitizadores. Por último, y acerca del punto anterior, la referencia a un trinomio de seguridad que se encuentra condicionado a definiciones, objetivos, causas y efectos que no guardan relación alguna más allá del efecto securitizador.

La vinculación de estas tres amenazas nos permite visualizar la extensión del perímetro de seguridad de los Estados Unidos en América Latina. El Gráfico 1 nos permite señalar la triangulación existente entre estos tres factores.

Gráfico 1: Triangulación Terrorismo, Narcotráfico e Inmigración



Fuente: Tisera (2016: p. 195).

Este triángulo de seguridad se encuentra determinado por el factor terrorismo, a partir de aquí se establecen una serie de relaciones y vinculaciones. «Los sucesos del 2001 redefinen las prioridades de la política exterior estadounidense» (Chávez, 2008: p. 73). El terrorismo se encuentra en la cúspide de las políticas de seguridad, establece supuestas relaciones con los factores señalados en la base de la pirámide. A través del vínculo terrorismo-narcotráfico, se construye la aparición del narcoterrorismo; en la relación terrorismo-migraciones, se halla la posibilidad de que grupos terroristas utilicen los canales de ingreso de la inmigración indocumentada; y, por último, el binomio narcotráfico-migraciones relaciona el tráfico de drogas y la utilización de los inmigrantes indocumentados como transporte a los Estados Unidos.

En nuestra investigación, proponemos ver tres casos de prácticas migratorias que guardan una relación directa con los atentados terroristas de 2001 y que nos permite visualizar un ejemplo del denominado triángulo de seguridad:

1. La Ley Patriota aprobada por el presidente Bush expandió el poder del Ejecutivo y las diferentes agencias de inteligencia que involucró la violación de libertades civiles a partir de escuchas telefónicas, violación de los correos electrónicos, allanamientos sin autorización de los jueces, entre otras acciones. ¿En qué sentido perjudica

esto a la inmigración? Al respecto de la inmigración, esta ley busca la ampliación de ciertas categorías a las cuales se las puede acusar de amenazas a los EE. UU. Y, de esta manera, se puede prohibir su ingreso o su deportación: «La Ley Patriota se configura como uno de los mayores cambios en la ley de Inmigración y Nacionalidad» (Chávez, 2008: p. 89). En este sentido, es de suma importancia la explicación de dos de sus secciones[12]: la sección 411 de la Ley Patriota permite la deportación de inmigrantes indocumentados aunque no se les hubiese comprobado vínculos con grupos terroristas. La sección 412 continúa con la criminalización del inmigrante, al sostener que, si un inmigrante es considerado una amenaza para el Estado, la sociedad o los individuos, se les pueden adjudicar cargos criminales. La Ley Patriota, en general, es una clara violación a las leyes migratorias de los Estados Unidos; por ejemplo, esta ley permite a las policías locales la detención de inmigrantes sospechosos de ser indocumentados.

2. Una segunda práctica cotidiana luego de los atentados de 2001 se estableció con relación a los visados, su control y una profunda reestructuración de los bancos de inteligencia utilizados por las embajadas y la participación directa de las aerolíneas. Las diferentes agencias que quedaron bajo la esfera del DHS contienen información acerca de las personas que pretenden ingresar a los Estados Unidos. Cuando una persona tiene la intención de viajar y presenta sus papeles para la obtención de un visado, es utilizada la inteligencia provista por las diferentes agencias y oficinas. En el año 2002, se aprobó la Ley Enhanced Border Security and Visa Entry Reform, que establecía la utilización de pasaportes electrónicos y sus respectivas visas; en este sentido, el programa US-VISIT permite la utilización de los mecanismos generados por las fronteras inteligentes en cuanto a cooperación de inteligencia.

3. El tercer caso al cual referenciamos es en relación con la Oficina de Aduana y Protección Fronteriza. La Patrulla Fronteriza se encargaba hasta el 11-S del cumplimiento de las leyes migratorias; luego su objetivo mutó respecto de la lucha contra el terrorismo, vinculándose a la lucha contra la inmigración indocumentada. De esta manera, destacamos tres objetivos de acción: el terrorismo, el combate de las drogas y la inmigración indocumentada como estrategias conjuntas. Cuando se observa el accionar de esta oficina, podemos sostener que «la interdicción de inmigrantes ilegales es imperativo posterior a septiembre 11 más por sus connotaciones terroristas que por sus implicancias económicas o sociales» (Chávez, 2008: p. 92).

5. Conclusión

La política de seguridad analizada durante las tres últimas administraciones se circunscribe a los efectos de la guerra contra el terror que se inicia post 11-S. Desde esta

[12] Para un mayor análisis de esta ley y de las dos secciones que utilizamos para referenciar el caso de nuestro estudio, ver: Ley Patriota.

matriz, la territorialidad y sus fronteras se constituyen como zonas de alta complejidad; en este sentido, se formulan políticas en el ámbito estatal con repercusiones sobre el complejo de seguridad hemisférico (regional) sumamente rigurosas. Para los EE. UU., su frontera sur se encuentra demasiado permeable a aquellos que quieren ingresar para hacer daño a la nación, de ahí la necesidad imperiosa por establecer límites en la lucha contra el terror. En virtud de esto, podemos observar como, luego de los atentados, el Congreso sancionó el *USA PATRIOT Act*, reforzando la aplicación de la ley en la frontera y habilitando la detención y deportación dentro del propio Estados Unidos. La aplicación de la ley fuera de la línea de las fronteras no es nueva; la fusión de la guerra contra el terrorismo incremento su aplicación.

Por su parte, las ESN surgen de una amenaza para su creación, es decir, el documento se elabora teniendo en cuenta cuál es el mayor «peligro» en ese momento, y, a partir de allí, se reelaboran y adaptan los distintos elementos y estrategias necesarias para contrarrestar dicha amenaza. Poco importa si los Estados fallidos guardan relación con grupos terroristas, o si tienen acceso a armas de destrucción masiva, o si en definitiva existe una relación directa entre los grupos terroristas, el narcotráfico o los flujos migratorios. En pocas palabras, las estrategias de seguridad nacional se presentan lo suficientemente flexibles como para determinar las potenciales amenazas en función del interés nacional del gobernante de turno. De ahí la necesidad de realizar un análisis de estas para poder entender las políticas posteriores al 11-S y el establecimiento del trinomio de seguridad que se acentúa con la administración de Trump.

Variados son los ejemplos que podríamos analizar en relación con el establecimiento del trinomio terrorismo-migraciones-narcotráfico. Ante esta situación, estamos en condiciones de aseverar la existencia de una realidad establecida por el *hegemon* con fuertes implicancias en nuestro fenómeno de estudio. Por ello, la militarización del combate contra las drogas y su posterior securitización en torno a la retórica narcoterrorista, junto al vínculo inmigratorio como un desafío a la seguridad de los Estados Unidos en relación al terrorismo, se establece como el eje central de las estrategias de seguridad estadounidense. De esta forma, en una agenda de seguridad donde predomina el miedo a la amenaza terrorista, se determina el incremento en la utilización del poder duro ante otras amenazas que no poseen el mismo riesgo directo que el terrorismo. En este sentido, los diversos programas de gobiernos (Bush, Obama y Trump), con un fuerte apoyo de la opinión pública, nos sirvieron para comenzar a responder nuestra pregunta-problema: ¿Cómo interactúan las amenazas que forman y articulan la agenda de seguridad de los Estados Unidos? Surge un acto discursivo que pretende la securitización de los tres temas, de ahí, que hablemos de un trinomio de seguridad. Si bien los tres componentes representan amenazas, ellas no pueden ser consideradas desde una misma naturaleza. Esta simplificación es producto de un *continuum* en las diversas ESN de los Estados Unidos y que, según ellas, es producto de la instrumentación de políticas de poder militar a través del control de las fronteras y la extensión del perímetro de seguridad regional; en

definitiva, el establecimiento de un trinomio de seguridad que se presenta como el factor securitizador de la agenda de seguridad estadounidense.

Bibliografía

Abshire, D. (1988). Preventing World War III: A realistic Grand Strategy. *Armed Forces Journal International*; vol. 126 n.° 11.

Allison, G. (2017). *Destined for War: Can America and China Escape Thucydides's Trap?* Houghton Mifflin Harcourt.

Arteaga, F. (2006). La Estrategia de Seguridad Nacional de Estados Unidos de 2006. *Real Instituto Elcano*. Área: Seguridad y Defensa/EE. UU. y Diálogo Transatlántico- ARI Nro. 71.

Artola, J. (2005). Debate actual sobre migración y seguridad. *Migración y desarrollo*, 2.° Semestre, N.° 5. México: Red internacional de Migración y Desarrollo.

Bagley, B. (2006). La Agenda de Estados Unidos. En Ministerio de Relaciones Exteriores del Ecuador. *Relaciones Ecuador-Estados Unidos: Situación Actual y Perspectivas*. En PLANEX 2020: *Plan Nacional de Política Exterior 2006-2020*. Quito: Ministerio de Relaciones Exteriores del Ecuador.

Bartolomé, M. (2004). El empleo del instrumento militar frente a las Nuevas Amenazas. ¿Es extrapolable la experiencia de la OTAN al Hemisferio Americano? *Air & Space Power Journal.* Third Quarter Volume.

Bartolomé, M. (2006). *La seguridad internacional en el siglo xxi, más allá de Westfalia y Clausewitz*. Chile: Academia Nacional de Estudios Políticos y Estratégicos. Ministerio de Defensa Nacional.

Buzan, B. (1991). New Patterns of Global Security in the Twenty-first Century. *International Affairs*, 67(3).

Buzan, B. (2007). *People, States and Fear: an agenda for international security studies in the post-cold war era*. 2nd ed. Colchester: ECPR Press.

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

Buzan, B.; Waever, O. y De Wilde, J. (1998). *Security: a new framework for analysis*, Lynne Rienner Publishers, Boulder (CO), pp. 5-16. En Bartolome, M. (2006). *La Seguridad Internacional post 11S: Contenidos, Debates y tendencias*. Buenos Aires: Instituto de Publicaciones Navales del Centro Naval.

Calle, F. y Merke, F. (2005). La Estrategia de Seguridad Nacional de EE. UU. en la Era Bipolar. *Agenda Internacional*, Año 1, N.° 3, diciembre 2004. Enero/Febrero.

Chávez, N. (2008). Cuando los mundos convergen: Terrorismo, narcotráfico y migración post 9/11. FLACSO, Ecuador.

Dunn, T. (1996). The militarization of the US Mexico Border, 1978-1992: Low-Intensity Conflict Doctrine Comes Home. *The Center for Mexican American Studies*. Texas: University of Texas.

Estrategia de Seguridad Nacional de los Estados Unidos (ESN) (1993). Departamento de Estado de Estados Unidos. Recuperado del sitio web del Departamento de Estado. Recuperado de: www.usinfo.state.gov

Estrategia de Seguridad Nacional de los Estados Unidos (ESN) (2002). National Security Strategy, The White House. Recuperado del sitio web del Departamento de Estado. www.usinfo.state.gov

Estrategia de Seguridad Nacional de los Estados Unidos (ESN) (2006). Departamento de Estado de Estados Unidos. Recuperado del sitio web del Departamento de Estado. www.usinfo.state.gov

Estrategia de Seguridad Nacional de los Estados Unidos (ESN) (2010). Departamento de Estado de Estados Unidos. Recuperado del sitio web del Departamento de Estado. www.usinfo.state.gov

Estrategia de Seguridad Nacional de los Estados Unidos (ESN) (2017). President Donald J. Trump Announces a National Security Strategy to Advance America's Interests. ESN de 2017. Recuperada de:https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-announces-national-security-strategy-advance-americas-interests/?source=GovDelivery

Fernández de Castro, R. (2006). Seguridad y migración. Un nuevo paradigma. *Foreign Affairs,* Edición en español, octubre-noviembre.

Gaddis, J. L. (1982). *Strategies of Containment.* New York: Oxford University Press [paperback].

García Encina, C. (2018). *La Estrategia de Seguridad Nacional de la Administración Trump.* Documento de trabajo 6/2018, España: Real Instituto El Cano.

González, R. (2010). *La Estrategia de Seguridad Nacional de los Estados Unidos*. Publicado en el Consejo Argentino para las Relaciones Internacionales. Recuperado de: www.cari.org.ar

Llenderrozas, E. (2018). *La Estrategia de Seguridad Nacional de los Estados Unidos*. Argentina: Universidad Nacional de Buenos Aires. Cece.

Manassero, M. S. y Tisera, J. C. (2019). *Terrorismo Internacional. La percepción de la amenaza en el escenario de la seguridad internacional.* Ciudad Autónoma de Buenos Aires: Almaluz.

Merke, F. (marzo de 2018). ¿Nada nuevo bajo las estrellas? *Revista Nueva Sociedad.* Opinión.

Obama, B. (2009). Discurso Inaugural del Presidente. Reproducido en el *Diario El País*, consultado el 6/9/2020. Disponible en https://elpais.com/internacional/2009/01/20/actualidad/1232406016_850215.html

Office of the Federal Register (2017). Executive Order 13767. Disponible en: https://www.federalregister.gov/documents/2017/01/30/2017-02095/bordersecurity- and-immigration-enforcement-improvements

Office of the Federal Register (2017). Executive Order 13768. Disponible en: https://www.federalregister.gov/documents/2017/01/30/2017-02102/enhancingpublic

Rice, C. (2001). La promoción del interés nacional. *Foreign Affairs* en español. México, ITAM, vol. 1 N.° 1, primavera.

Rosenau, J. (1997). *Along the domestic foreign frontier. Exploring Governance in a Turbulent World*. Cambridge: Cambridge University.

Schmitt, C. (2001). El Imperialismo Moderno en el Derecho Internacional. En Héctor Orestes Aguilar, (ed.) *Carl Schmitt, Teólogo de la Política*. México: Fondo de Cultura Económica.

Tisera, J. C. (2016). *Latinoamérica: ¿En los Estados Unidos? El dilema de la seguridad societal y el reto hispano*. Ciudad Autónoma de Buenos Aires, Argentina: Editorial Almaluz.

Tokatlian, J. G. (2004). Colombia: U.S. Security policy in the Andean Region the Specter of a Regionalized War. En Brian Loveman, (ed.) *Strategy for Empire: U.S. regional security Policy in the Post-Cold \War era*. Lanham: SR Books.

Tucídides (460 a. c.) *Guerra del Peloponeso*. Traducción de Diego Gracián Estudio preliminar de Edmundo O' Gorman. Edición: Enero, 2007. Madrid: Biblioteca Clásicos Grecolatinos.

Vega, J. M. y Miccinilli, M. (2007). ¿Qué Occidente se perfila luego de la renovada Estrategia de Seguridad Nacional de los Estados Unidos? *Argentina Global* 16, mayo-agosto. Buenos Aires: Centro Argentino de Estudios Internacionales.

Waltz, K. (1993). The emerging structure of international politics. *International Security*, vol. 18, N.° 2.

—ARTÍCULO—

Análisis de los aspectos jurídicos generales de las plataformas digitales de videoconferencias y, en particular, de ZOOM

Por Mauro F. Leturia

Procurador, abogado y escribano. Esp. en Docencia Universitaria. Doctorando de la Facultad de Ciencias Jurídicas y Sociales, UNLP. Prof. Derecho Civil III, Introducción al Pensamiento Científico y Derecho Marítimo y Aeronáutico y Prof. de posgrado de la Esp. en Documentación y Registración Inmobiliaria, UNLP. Prof. titular de Prácticas Profesionales II y Derecho de la Navegación, UCALP. Prof. Derecho Penal I parte general y Derecho Marítimo y Aeronáutico, Universidad del Este. Prof. de Metodología de la Investigación, Facultad de Diseño y Comunicación, Universidad del Este. Docente invitado en la Universidad Complutense de Madrid. Prof. de posgrado de la Universidad Austral. Oficial de la Justicia Federal Argentina. Becario doctoral del Ministerio de Educación de la Nación. Secretario de Extensión y de Investigación, Facultad de Derecho, Universidad del Este. Correo electrónico: mfleturia@hotmail.com

Adrián E. Gochicoa

Abogado. Auxiliar docente de Contratos Modernos, Tecnicatura de Martillero y Corredor, Facultad de Ciencias Jurídicas y Sociales, UNLP. Ayudante ad honorem en Civil/Privado III e Introducción al Pensamiento Científico en la Facultad de Ciencias Jurídicas y Sociales, UNLP. Correo electrónico: adrian_gochicoa@hotmail.com

Victoria Antonella Mongelos

Procuradora. Ayudante en Civil/Privado III e Introducción al Pensamiento Científico en la Facultad de Ciencias Jurídicas y Sociales, UNLP. Correo electrónico: vamongelos@gmail.com

Facundo Cerdá

Procurador y abogado. Recibido de la Universidad Católica de La Plata (2019). Curso del derecho de autor en el siglo xi en la Universidad Complutense de Madrid (2019). Ayudante de la Cátedra de derecho Marítimo y Aeronáutico. Correo electrónico: facundocerdaa@gmail.com

Resumen

El presente trabajo tiene como finalidad realizar un análisis de cómo se desarrollan las nuevas plataformas digitales con el avance de la pandemia mundial de COVID-19, en particular los distintos contratos que surgen en la utilización de cada aplicación, tal como Zoom. Se realizará una descripción de los aspectos jurídicos más relevantes de la herramienta principalmente utilizada para la enseñanza del derecho, y sus proyecciones con relación a cómo es el manejo de datos personales, la protección de los derechos de autor y las relaciones contractuales existentes.

Palabras claves: Derechos Intelectuales- contratos- ZOOM – COVID-19.

Abstract

The purpose of this work is to carry out an analysis of how new digital platforms develop with the advance of the global pandemic of COVID-19, in particular the different contracts arising in the application of each application, such as Zoom.

A description of the most relevant legal aspects of the tool used for law teaching, its projections in relation to how personal data is managed, the protection of copyright, and the existing contractual relationships will be carried out.

1. Introducción

El marco del presente artículo es determinado y motivado por el contexto que, en general, implica la pandemia por COVID-19 y su desarrollo, en particular, en este estado de la sociedad denominado «sociedad de redes» o «sociedad de la información» o «sociedad del conocimiento»1 donde el conocimiento e información, la tecnología e Internet, el «Internet en las cosas» son los ejes central de nuestras vidas, de nuestros sistemas de salud, educación, de nuestro sistema de producción, distribución y consumo de bienes y servicios (Castells, 2000). La información cobra, en el estado actual, vital importancia, produciéndose así una verdadera revolución con la aparición de la tecnología de la información y las comunicaciones (TIC).

Desde el inicio de esta pandemia, y el establecimiento de un confinamiento preventivo y obligatorio, hemos observado un crecimiento exponencial de las conexiones con los servicios digitales, como son Netflix, Zoom, Spotify, Google Meet, Cisco Webex Meetings, Microsoft Teams, etc. Esta nueva «realidad» llevó a que la era digital se instale de forma tal que, en la actualidad, todos estamos conectados a todas horas de todos los días, convirtiéndose esta situación en el establecimiento de los nuevos paradigmas mundiales aplicados a la educación, a la investigación y hasta para las relaciones sociales y familiares.

[1] Cumbre Mundial sobre la Sociedad de la Información. Unión Internacional de Telecomunicaciones (UIT) ONU. Declaración de Principios. Documento WSIS-03/GENEVA/4-S, 12 de mayo de 2004.

Debe entenderse que este aislamiento social decretado en la Argentina, en cierto modo, aceleró lo que ya se verificaba como un proceso lento que venía ocurriendo, como es la digitalización e informatización o conexión de muchos aspectos de nuestras vidas.

Respecto a la COVID-19, el plexo normativo se puede sintetizar señalando, por un lado, que se dispuso la emergencia sanitaria (Conf. Ley 27.541 y Decreto 260/2020) y, frente a esto, se dictó el aislamiento obligatorio a quienes revistan la condición de «casos sospechosos» (Conf. DNU 260/2020) y un aislamiento social preventivo y obligatorio para todos los habitantes del país y quienes se encuentren temporalmente en la Argentina (Conf. DNU 297/2020, Decretos Nros. 325/20, 355/20, 408/20, 459/20 y 493/20, y recientemente por el DNU 520/20 y sucesivas prórrogas), con dispensa de la obligación de asistir al lugar de trabajo para todas las actividades no exceptuadas (las actividades exceptuadas fueron enumeradas en el DNU 297/2020 y fueron ampliadas por Resolución MTEYSSN 233/2020 y las Decisiones Administrativas del Jefe de Gabinete de Ministros Nros. 429/2020, 450/2020, 467/2020, 468/2020 y 524/2020, entre otras).

Recientemente, el DNU 520/2020 dispuso la medida de «distanciamiento social, preventivo y obligatorio», y quedó prohibida la circulación de las personas alcanzadas por estas medidas por fuera del límite del departamento o partido donde residan, prorrogándose el aislamiento social preventivo y obligatorio (Decreto No. 297/20 y sus prórrogas), anteriormente señalado exclusivamente para las personas que residan o se encuentren en los aglomerados urbanos y en los departamentos y partidos de las provincias argentinas que no cumplan positivamente los parámetros epidemiológicos y sanitarios previstos.

En virtud de lo cual, en nuestro país, coexisten en diferentes territorios medidas de aislamiento social y de distanciamiento social.

La aparición y el uso de herramientas digitales e informáticas o de las TIC para diversas actividades productivas, académicas y hasta de entretenimiento no resultan actuales ni nuevas. El pasaje de la utilización de Internet para acceder al conocimiento al «Internet de las cosas» que permite simplificar o automatizar procedimientos, tareas, como también procesos productivos está en desarrollo hace años[2].

En este contexto, ciertas herramientas informáticas (*software*), como también ciertas redes sociales, lo que se denomina TIC, se tornaron de vital importancia tanto para el trabajo, la actividad comercial como para la enseñanza. Nos referimos a aquellas que permiten realizar videoconferencias en vivo y en simultáneo o videollamadas grupales, siendo las plataformas digitales más conocidas las de Zoom, Jitsi Meet, Microsoft Teams, Google Meet, Cisco Webex Meetings, entre otras.

[2] En nuestro país, a través de la Ley 23.877 (Ley de promoción y fomento de innovación tecnológica), la Ley 26.270 (Ley de promoción del desarrollo y producción de la biotecnología moderna) y la reciente Ley 27.506 (que establece, a partir del año 2020, un régimen de promoción de economía del conocimiento que se suma a las anteriores).

No puede dejar de señalarse que las empresas titulares de los derechos económicos sobre estas plataformas en este contexto mundial se han beneficiado y han aumentado su valor en el mercado[3].

Si bien estos modelos de negocios fueron desarrollados desde las plataformas de entretenimiento, hoy llegan hasta videoconferencias laborales, las cuales, a raíz de lo que estamos viviendo, sirven para mantener conectados a los usuarios sin límite de tiempo alguno y, ante cualquier circunstancia, su ingeniería jurídica es construida en función de reglas de ordenamientos jurídicos de origen anglosajón, mediante las cuales se ofrecen muchas veces en forma gratuita; ello no resulta fácil de compatibilizar con nuestras reglas jurídicas. Así, torna válida la realización de algunas preguntas, tales como: ¿A cambio de qué estas empresas facilitan la utilización de estas aplicaciones? ¿Son los contratos que establecen estas plataformas beneficiosos para los consumidores? ¿Qué es lo que en definitiva obtienen directa o indirectamente de nosotros como usuarios?

Podemos ver que estas nuevas formas contractuales poseen muchas características de los llamados «contratos leoninos», en los cuales solo una parte impone las condiciones de cómo va a ser el vínculo contractual, mientras que la otra las acepta o no se le permite utilizar la herramienta. El usuario está obligado a aceptar las bases y condiciones sin posibilidad de discusión alguna. Por lo general, en todos los casos incluye con ello que el usuario brinda sus datos y permite su utilización, convirtiéndose así «el uso de datos personales, en distintas formas sin ningún tipo de control ni regulación al respecto, en la principal contraprestación que exigen estas empresas a cambio de permitir el uso de sus plataformas»[4]. Esta actividad queda librada a la voluntad de las empresas propietarias de los derechos sobre estas aplicaciones, las cuales manejan un caudal de información cada vez más grande y completa sobre nuestras necesidades, gustos o preferencias; ejemplo claro es el algoritmo que utiliza Netflix o Spotify para determinar que género de música o películas nos gusta a cada uno con base en selecciones previas por parte de cada uno.

En concreto, nos centraremos en las plataformas que permiten una comunicación electrónica instantánea, ya sea a través de una computadora o de un teléfono móvil. Como herramientas se pueden utilizar con fines diversos jurídicamente relevantes: Para trabajar (teletrabajo), para realizar negociaciones contractuales, permitir la comunicación familiar, realizar ciertos actos procesales en el marco de un juicio (audiencias), para la enseñanza (aula virtual), entre otras.

El presente artículo tiene como finalidad realizar una descripción de los aspectos jurídicos más relevantes de una de las herramientas hoy principalmente utilizada para

---

[3] https://www.infobae.com/economia/2020/03/25/zoom-la-app-que-es-exito-economico-en-medio-de-la-pandemia-vale-casi-el-doble-que-twitter-y-tiene-5-veces-mas-usuarios-que-el-mes-pasado/

[4] De los términos y condiciones de Zoom, se extrae textualmente: «Información de registro. Puede que se le solicite información personal para registrarse y/o utilizar determinados Servicios. Usted reconoce que dicha información debe ser veraz. También se le puede pedir que elija un nombre de usuario y contraseña. Usted es completamente responsable de mantener la seguridad de su nombre de usuario y contraseña, y acepta no divulgar dicha información a terceros» (ZOOM, 2020).

la enseñanza del derecho, como son el manejo de datos personales, la protección de los derechos de autor y la relación contractual existente.

2. Acerca de Zoom y su marco general regulatorio

Centrándonos en las plataformas que permiten una comunicación electrónica instantánea, ya sea tanto a través de una computadora como de un teléfono móvil, puede describirse una de la más promocionadas, como se señaló: Zoom[5].

Siguiendo la distinción tradicional que realiza la doctrina (Sylvester, 2018; Lipszyc, 2005; Altmark y Quiroga, 2012) y que ha tomado el proyecto de ley de los senadores Fellner-Pinedo para regular la responsabilidad en Internet[6], pueden diferenciarse, principalmente, diferentes operadores en Internet, como son los proveedores de contenidos de Internet[7], los proveedores de servicios de Internet[8], los operadores de servicios web[9] y los proveedores de red o de nube[10].

Resulta dificultoso tratar de encuadrar a las plataformas que permiten una comunicación electrónica instantánea, ya que uno de los problemas que se presenta es que, en esta materia, toda conceptualización es provisoria y arbitraria, atento a la constante

[5] De los términos y condiciones que impone dicha aplicación: «USO DE LOS SERVICIOS Y RESPONSABILIDADES QUE USTED ASUME. Solo puede utilizar los Servicios de conformidad con los términos del presente Acuerdo. Usted es el único responsable del uso de los Servicios por su parte y por parte de sus Usuarios finales, y deberá cumplir y garantizar el cumplimiento de todas las leyes relacionadas con el uso de los Servicios por su parte y por parte de cada uno de los Usuarios finales, incluidas, entre otras, las leyes relacionadas con las grabaciones, la propiedad intelectual, la privacidad y el control de las exportaciones. El uso de los Servicios no es válido donde esté prohibido» (ZOOM, 2020)

[6] Dictamen en los proyectos de ley de la senadora Fellner y el senador Pinedo por el que se regula a los proveedores de servicios de enlace y búsqueda de contenidos alojados en Internet (S-1865/15 y S-942/16).

[7] Son los que realizan, producen, cargan un contenido digital en Internet o disponen de él, incluidos los usuarios.

[8] Son, en general, los intermediarios que existen entre el que realiza, produce o dispone de un contenido digital y los que adquieran, descarguen o utilicen esos contenidos. Pueden distinguirse entre aquellos que permiten el acceso del usuario a Internet (proveedor de acceso a Internet); los que permiten el almacenamiento o la publicación directa del contenido, ya sea en forma temporal o bien en forma permanente (proveedor de alojamiento); aquellos que intermedian mediante una plataforma en la realización de operaciones o transacciones comerciales de terceros (proveedores de servicios de comercio electrónico), y aquellos que brindan el servicio de enlazar y buscar contenidos alojados en otros proveedores de alojamientos (proveedores de servicios de enlace y búsqueda de contenidos).

[9] Son aquellos que proporcionan medios y espacios para intercambiar informaciones, mensajes y también contenidos.

[10] Son aquellos que suministran la infraestructura técnica, tanto en forma física a través de líneas telefónicas, de cable, antena, satélite, como en forma virtual a través de la «nube».
En este último caso, se los denomina *proveedores de nube*, pues suministran, a través de un espacio o entorno digital —o sea, en forma virtual—, una infraestructura (almacenamiento, redes, etc.), así como también plataformas y *software* para proveer servicios de Internet o web. En ambos casos, la finalidad es la conexión entre el usuario con o a través de un proveedor de servicios de Internet y otros usuarios, proveedores de Internet, operadores de servicio web, que actúan o no como proveedores de contenido.

evolución tecnológica existente. Los servicios hoy prestados a través de Internet ya no se limitan al alojamiento o buscadores de contenidos, sino que incluyen telefonía, *streaming*. Así, en la actualidad, se utilizan computadoras como dispositivos que permiten el acceso a internet y también teléfonos móviles o celulares. La infraestructura para prestar estos servicios ya no es solo física, sino que además lo es en forma virtual.

Lo cierto es que, descriptivamente, centrándonos en Zoom, puede señalarse que, al igual que las otras TIC antes mencionadas, es una plataforma (*software*) que presta servicios de Internet, tales como la posibilidad de realizar a través de ella videoconferencias o conferencias web, como también comunicaciones telefónicas y por medio de chat. En sí, se trata de una plataforma que unifica a través de Internet los servicios de telefonía, audio y video o imagen, intercambio de datos, y chats. En todos los casos, permite una comunicación plena en tiempo real entre todos los que participan de ella, posibilitando su grabación. En virtud de esto, puede entenderse que resulta ser un proveedor de servicios por Internet de intermediación en la que se comunican los usuarios mediante videoconferencias principalmente.

La plataforma Zoom pertenece a Zoom Video Communications, Inc. (NASDAQ: ZM), utiliza para prestar sus servicios la «nube o *cloud*» como estructura de red y como almacenamiento también. Presta los siguientes servicios: reuniones y chat (reuniones en línea); seminarios web por video (eventos de *marketing* y foros abiertos organizados por la empresa); salas de conferencias; sistema telefónico, y *marketplace*[11].

Estos servicios se estructuran a través de dos grandes prestaciones: Zoom Meetings y Zoom Video Webinars, donde mientras en la primera permite un debate o interacción (hasta 1000 participantes), la última aplicación está diseñada para eventos multitudinarios donde los asistentes se unen sin activar su audio ni su video.

Los servicios se ofrecen en mayor intensidad según los costos de la licencia que se adquiera, partiendo desde su versión gratuita. En tal caso, aumenta el número de participaciones permitidas, la posibilidad y capacidad tanto de almacenar las grabaciones en la nube como de traducirlas principalmente[12].

Por último, puede señalarse que, en su funcionamiento, se distingue un usuario con licencia (anfitrión) y los participantes; los primeros deber estar registrados y son los que pueden generar las reuniones.

Profundizando y puntualizando en Zoom como TIC (tecnologías de la información y las comunicaciones), debe señalarse que, en nuestro país, encuentran el marco general de

[11] https://zoom.us/

[12] De los términos y condiciones de ZOOM se extrae textualmente: «Grabaciones. Usted es responsable del cumplimiento de todas las leyes de grabación. El anfitrión puede optar por grabar las reuniones y los seminarios web de Zoom. Al utilizar los Servicios, Usted otorga su consentimiento a Zoom para guardar grabaciones de cualquiera o todas las reuniones o seminarios web de Zoom a los que se una, en caso de que dichas grabaciones se almacenen en nuestros sistemas. Recibirá una notificación (visual o de otro tipo) cuando se habilite la grabación. Si no otorga su consentimiento para que se le grabe, puede abandonar la reunión o el seminario web».

su regulación en la Ley 27.078[13]. Dicha ley define a las TIC como « el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permitan la compilación, procesamiento, almacenamiento y transmisión de información, como por ejemplo voz, datos, texto, video e imágenes, entre otros » (art. 6), estableciéndose en dicha ley que se declara « de interés público el desarrollo de las Tecnologías de la Información y las Comunicaciones, las Telecomunicaciones, y sus recursos asociados, estableciendo y garantizando la completa neutralidad de las redes » (art. 1) y como tal «… tienen como finalidad garantizar el derecho humano a las comunicaciones y a las telecomunicaciones…».

Ahora bien, en lo que nos interesa resaltar, la citada ley señala que

> … el Servicio de TIC comprende la confluencia de las redes tanto fijas como móviles que, mediante diversas funcionalidades, proporciona a los usuarios la capacidad de recibir y transmitir información de voz, audio, imágenes fijas o en movimiento y datos en general…

y que

> … el Servicio Básico Telefónico, sin perjuicio de su particularidad normativa, reviste especial consideración dentro del marco de la convergencia tecnológica. Es por ello que la efectiva prestación del servicio debe ser considerada de manera independiente a la tecnología o medios utilizados para su provisión a través de las redes locales, siendo su finalidad principal el establecimiento de una comunicación mediante la transmisión de voz entre partes (art. 55)

estableciéndose la neutralidad de red por la cual «se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación…» y, a consecuencia de ello,

> los prestadores de Servicios de TIC no podrán: a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario. b) Fijar el precio de acceso a Internet en virtud de los contenidos, servicios, protocolos o aplicaciones que vayan a ser utilizados u ofrecidos a través de los respectivos contratos. c) Limitar arbitrariamente el derecho de un usuario a utilizar cualquier *hardware* o *software* para acceder a Internet, siempre que los mismos no dañen o perjudiquen la red.

[13] Excluyéndose la aplicación de la Ley 26.522 referida a la regulación de los servicios de comunicación audiovisual (televisión, radio, etc.) y también la ley nacional de telecomunicaciones, Ley N.º 19.798 (telégrafo, telefonía fija y móvil, etc.) por cuanto no abarca a los servicios de Internet, las TIC o todos los prestados por Internet regulados por la Ley 27.078. Encuentran varios puntos de contacto en cuanto las actividades reguladas por aquellas hoy son prestadas a través de Internet y por medios de plataformas digitales (telefonía electrónica, por ejemplo) y cuyo desarrollo se refiere al concepto de convergencia digital que tiende a que todos los servicios sean prestados a través de redes o Internet: voz, imagen, datos, audiovisual mediante la integración de telefonía, televisión, radio e Internet en una sola plataforma de usuario.

Además, no se excluye la aplicación del régimen de defensa del consumidor (Ley 24.240 y modif. y C. C. y C. N.) cuando resulte aplicable. En ese sentido, conforme el art. 4, se establece la jurisdicción federal (Fuero Contencioso Administrativo Federal) sobre las actividades reguladas por dicha ley cuando existan incidencias que, de modo directo o indirecto, pudiera surgir o derivar de la aplicación de ella, con excepción de las relaciones de consumo. En este último caso, corresponderá la jurisdicción ordinaria o la federal según los casos caigan en una u otra, en razón de las personas o territorio. Por lo tanto, la utilización de las TIC como medio de comunicación puede desarrollarse en el marco de una relación de consumo, lo que implica que se proyecte el orden público protectorio sobre aquella.

3. La inviolabilidad de las comunicaciones

Uno de los temas centrales que plantea toda comunicación es la referida a su confidencialidad, privacidad e inviolabilidad. Dos son las cuestiones por considerar, ya que no solo se trata de los datos personales que las plataformas manejan o usan de los que las utilizan, sino del contenido en sí de la comunicación.

Por un lado, en este punto debe señalarse que las TIC, y en especial Zoom, permiten en cualquier momento la grabación y el almacenamiento de información o expresiones vinculadas a la vida privada de las personas, como asuntos confidenciales. Por lo cual el contenido en sí puede verse afectado por una divulgación o difusión indebida o no autorizada.

Desde el artículo 18 de la Constitución Nacional, se proclama que la correspondencia como los papeles privados son inviolables. Más allá que la correspondencia sea una forma de comunicación, y que se incluya tanto la epistolar como la electrónica (*email*) en la protección constitucional y penal en los art. 153 y 155 del Cod. Penal, esta no se extiende a todas las TIC principalmente referidas a las de comunicación.

Sí resulta más amplia la protección civil en el art. 318 del C. C. y C. y la propia correspondiente al derecho a la privacidad e intimidad con fundamento en el art. 19 de la Constitución Nacional que abarca a toda comunicación. Por su parte, el art. 5 de la Ley 27.078 señala:

> La correspondencia, entendida como toda comunicación que se efectúe por medio de Tecnologías de la Información y las Comunicaciones (TICs), entre las que se incluyen los tradicionales correos postales, el correo electrónico o cualquier otro mecanismo que induzca al usuario a presumir la privacidad del mismo y de los datos de tráfico asociados a ellos, realizadas a través de las redes y servicios de telecomunicaciones, es inviolable. Su interceptación, así como su posterior registro y análisis, sólo procederá a requerimiento de juez competente

En concreto sobre este tema, la plataforma Zoom manifiesta, mediante la declaración de privacidad que debe suscribirse, que no se hace responsable por el contenido del

cliente (quien es titular de la cuenta Zoom) ni de los actos tales como las grabaciones o transcripciones de reuniones o llamadas porque el cliente (el titular de la cuenta de Zoom) es quien controla cómo se procesa el contenido[14]. Específicamente, se manifiesta la existencia de un sistema de cifrado del audio, videos y uso de la pantalla, firma de audio, capturas de pantalla con marca de agua, almacenamiento en la nube de las grabaciones bajo contraseña, almacenamiento de archivos enviados mediante el chat, entre otras.

Por otro lado, en cuanto al manejo de datos personales proporcionados por los usuarios a la plataforma Zoom, resulta de aplicación principalmente la Ley 25.326, la cual garantiza los derechos a los titulares de los datos como los de actualización, rectificación y supresión. El art. 59 inc. f de la Ley 27.078 señala que: «El usuario de los Servicios de TIC tiene derecho a […] la protección de los datos personales que ha suministrado al licenciatario, los cuales no pueden ser utilizados para fines distintos a los autorizados, de conformidad con las disposiciones vigentes».

En específico, Zoom señala qué datos utiliza de los titulares de una cuenta con empresas, organizaciones o personas fuera de Zoom, entre otros, para transacciones corporativas y fines comerciales, además de la finalidad de *marketing*.

En los términos y condiciones del servicio de Zoom, se establece como obligación de la plataforma que «… mantendrá medidas de seguridad físicas y técnicas razonables para evitar la divulgación o el acceso no autorizado al Contenido, de acuerdo con las normas del sector»[15].

Puede notarse que no existe una regulación específica para el manejo de los datos mediante plataformas en Internet ni referida al control del contenido generado o transmitido a través de él. La regulación principal, en cuanto a esta temática, se encuentra en la ley de protección de datos personales (Ley 25.326), además del marco regulatorio general en la Ley 27.078; pero entendemos que no resulta suficiente: no solo están en juego los datos personales de los participantes, sino ciertos contenidos que son almacenados en la nube propiedad de Zoom, cuya vigilancia en cuanto a seguridad sí recae en esta empresa, siendo en general y en particular en el caso de ZOOM empresas multinacionales que residen en otro país y establecen como condiciones la prórroga de la jurisdicción, cláusulas de exclusión y/o limitación de responsabilidad, entre otras.

4. Zoom y los derechos de autor

Otra problemática vinculada al uso de las plataformas que permiten videoconferencias y transferencia de datos, como Zoom, es el que se refiere a los derechos de autor sobre las obras intelectuales.

[14] https://zoom.us/es-es/privacy.html

[15] https://zoom.us/es-es/terms.html

El contenido en sí de la comunicación mediante Zoom puede constituir una obra objeto de protección de la Ley 11.723, la cual abarca «… toda producción científica, literaria, artística o didáctica sea cual fuere el procedimiento de reproducción », entendiendo que: «… la protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí ». También pueden, en el marco de una videoconferencia, utilizarse obras intelectuales de terceros sin la autorización de estos.

Esta arista plantea, por un lado, la cuestión sobre la autoría de la obra y la titularidad de los derechos económicos sobre ella (cuando esta plataforma sea utilizada en el marco de un contrato de trabajo o empleo público, o institucionalmente para organizaciones o empresas), como la utilización de obras intelectuales de terceros fuera de los fines permitidos por dicha ley. Por otro lado, la posibilidad de grabación de la comunicación, su almacenamiento y posibilidad de posterior difusión por alguno de los participantes o de un tercero puede implicar una infracción y afectación de esos derechos.

En los términos y condiciones del servicio de Zoom[16], se establece que el titular de la licencia es el único responsable del contenido enviado, o transmitido, o mostrado, o cargado al utilizarlo, debiendo garantizar el cumplimiento de todas las leyes relativas a dicho contenido, incluidas, entre otras, las leyes que requieren que obtenga el consentimiento de un tercero para utilizarlo. Expresamente, señala que el titular de la licencia « mantiene el derecho de propiedad intelectual y otros derechos que ya posea sobre el Contenido que envíe, publique o muestre en los Servicios o a través de los mismos » y que el titular se compromete a no utilizar ni permitir el uso de los servicios para «… transmitir a través de los Servicios cualquier material que pueda infringir la propiedad intelectual u otros derechos de terceros…».

5. Aspecto contractuales

Importa caracterizar el contrato existente entre el titular de una licencia de Zoom y esta empresa, principalmente, a efectos de señalar las implicancias de cierto contenido contractual que surge de «los términos y condiciones» que deben aceptarse para utilizar la plataforma.

La relación existente entre Zoom y el titular de una licencia para su uso es de origen contractual por tratarse de un acuerdo de voluntades con la finalidad de crear relaciones jurídicas patrimoniales (art. 957 del C. C. y C.), teniendo aun en su versión gratuita un

[16] De los términos y condiciones de Zoom, se extrae textualmente: «DERECHOS DE PROPIEDAD INTELECTUAL. No le está permitido publicar, modificar, distribuir o reproducir de ninguna manera el material con derechos de autor, las marcas comerciales, los derechos de publicidad u otros derechos de propiedad sin obtener el consentimiento previo por escrito del titular de tales derechos de propiedad. Zoom puede denegarle el acceso a los Servicios a cualquier usuario que presuntamente haya infringido los derechos de propiedad intelectual de otra parte. Sin limitar lo anterior, si cree que se han vulnerado sus derechos de propiedad intelectual, notifíquelo a Zoom siguiendo las instrucciones aquí indicadas».

objeto susceptible de valoración pecuniaria (art. 1003 del C. C. y C.). Puede caracterizarse como gratuito u oneroso según se adquiera la versión gratuita o una suscripción paga (art. 967 del C. C. y C.), unilateral o bilateral según las obligaciones de las partes (art. 966 del C. C. y C.), no formal (art. 969 del C. C. y C.) e innominado (art. 970 del C. C. y C.).

Interesa destacar que dicha relación contractual puede implicar una relación de consumo (art. 3 de la Ley 24.240 y 1092 del C. C. y C.) en virtud de un contrato de consumo cuando tenga por objeto la adquisición, uso o goce de servicios por parte de los consumidores o usuarios, para su uso privado, familiar o social (art. 1093 del C. C. y C.). Pero, además, en cuanto a la forma de contratación, se trata de un contrato celebrado por adhesión o cláusulas generales predispuestas (art. 984 y 985 del C. C. y C.), sea que se trate de un contrato paritario o de consumo, ya que la empresa Zoom inc. fija los términos y contenidos del contrato mediante la aceptación de estos a modo de condición previa a registrarse como usuario de una licencia de Zoom en cualquiera de sus versiones.

Frente a esto, resulta necesario analizar ciertas cláusulas de los términos y condiciones que plantean conflictos con la regulación que se establece en el C. C. y C. y en la Ley 24.240, según corresponda:

- Cláusulas relativas al precio, en cuanto se establece la facultad para Zoom de modificar los precios en cualquier momento, lo que incluye cambiar de un servicio gratuito a uno de pago y cobrar servicios que se ofrecieron previamente sin coste alguno. Se establece además que Zoom puede cobrar intereses equivalentes a la opción menor entre 1,5 % por mes o el importe más alto permitido por la ley sobre cualquier cantidad que no se pague cuando corresponda. En tal caso, pueden resultar abusivas en los términos del art. 988 del C. C. y C. y 37 de la Ley 24.240.

- Cláusulas de elección del derecho y prorroga de jurisdicción, en cuanto se establece que el acuerdo se regirá y se interpretará de acuerdo con las leyes del Estado de California, EE. UU., como se aplica en los acuerdos que los residentes de California celebran y ejecutan en California. Y que las partes aceptan el fuero exclusivo de los tribunales estatales del Condado de Santa Clara, California (EE. UU.) y los tribunales federales del Distrito norte de California.

Si se trata de un contrato de consumo estas cláusulas, entran en conflicto tanto en la jurisdicción como en cuanto al derecho por aplicar con la normativa que regula el régimen de protección del consumidor, que es de orden público y, como tal, no puede ser excluida su aplicación y con la regulación que en materia de aplicación del derecho internacional privado realiza el C. C. y C. en los arts. 2.654, 2.655 para esta clase de contratos. El primero de los artículos excluye expresamente los acuerdos sobre el foro, y el segundo señala aplicable el derecho argentino tanto cuando el contrato es celebrado en el domicilio del consumidor como cuando se cumple en el mismo lugar, por lo cual, conforme al art. 988, puede resultar abusiva la cláusula que imponga la renuncia de una normativa protectora.

En virtud de ser celebrado por adhesión, aun cuando no fuera de consumo, puede entrar en conflicto con las limitaciones del citado art. 988 del C. C. y C.

- Cláusulas de exclusión y/o limitación de responsabilidad, donde se establece que tanto Zoom como sus filiales o proveedores, revendedores no serán responsables de ningún daño contractual o extracontractual ni de ningún daño especial, incidental, indirecto, ejemplar o consecuente (lo que incluye, entre otros, daños por pérdida de beneficios comerciales, interrupción comercial, pérdida de información comercial o cualquier otra pérdida o daño monetario). Y, en el caso de ser responsable, limita su responsabilidad al importe realmente abonado por el usuario (si corresponde) en los doce (12) meses anteriores al evento o a la circunstancia que provocó tales reclamaciones. Al igual que en los casos anteriores, puede resultar abusiva esta cláusula en los términos del art. 988 del C. C. y C. y 37 de la Ley 24.240.

6. Conclusión

Realizada una descripción de los aspectos jurídicos más relevantes de una de las herramientas hoy más utilizada para la enseñanza del derecho, entendemos que el fenómeno de Internet y, en general, los nuevos desafíos que impone el desarrollo tecnológico e informático propio de la denominada *sociedad del conocimiento* requiere de una normativa más específica.

Es cierto que puede construirse una respuesta normativa en cuanto a la regulación de este fenómeno a partir, principalmente, de la Ley 27.078 y del resto de las regulaciones citadas, pero su delimitación y eficacia ante la falta de una regulación especial de estas circunstancias se ira construyendo sobre la base de la resolución judicial de situaciones conflictivas y abusivas.

Resulta, desde la práctica, una herramienta útil, en especial para la enseñanza a distancia física o ante la imposibilidad de presencialidad en las aulas, pero que permite una relación temporalmente inmediata o sincrónica; sin embargo, las plataformas digitales como Zoom, tanto como otras aplicaciones similares de Internet, y los servicios que por ella se prestan suponen la exposición y entrega de datos personales, imagen y sonido, así como de derechos que requieren un control mayor ante este fenómeno mundial.

7. Bibliografía

Altmark, D. y Quiroga, E. (2012). *Tratado de derecho informático*. 1.a ed. Buenos Aires: La Ley.

Castells, M. (2000). *La era de la información: economía, sociedad y cultura. Volumen I. La Sociedad red*. Versión castellana de Carmen Martínez Gimeno y Jesús Alborés. 2.a ed. Madrid: Alianza Editorial, S. A.

Lipszyc, D. (2005) Responsabilidad de los proveedores de servicios en línea por las infracciones del derecho de autor y derechos conexos en el entorno digital: análisis de la jurisprudencia

internacional. *XI Curso Académico Regional OMPI/SGAE sobre derecho de autor y derechos conexos para países de América Latina*. Asunción: OMPI, SGAE, Ministerio de Industria y Comercio de la República del Paraguay.

Sylvester, P. (2018). La responsabilidad de los ISP en la jurisprudencia de los tribunales argentinos (según el derecho de los caballos). En *El Derecho,* 278. Buenos Aires.

ZOOM (2020). Términos del servicio de ZOOM. Disponible en: https://uws.zoom.us/es-es/terms.html

8. Legislación

Cámara de Senadores: Dictamen de los proyectos de ley sobre la regulación a los proveedores de servicios de enlace y búsqueda de contenidos alojados en Internet. (S-1865/15 y S-942/16).

Congreso de la Nación Argentina: Ley de solidaridad social y reactivación productiva. Ley N.º 27541. Publicada en el Boletín Oficial n.º 34268 el 23-dic-2019, p. 1.

Congreso de la Nación Argentina: Ley de promoción y fomento de innovación tecnológica. Ley N.º 23.877. Publicada en el Boletín Oficial n.º 27001 del 1-nov-1990.

Congreso de la Nación Argentina: Ley de promoción del desarrollo y producción de la biotecnología moderna. Ley N.º 26.270. Publicada en el Boletín Oficial n.º 31205 del 27-jul-2007, p. 1.

Congreso de la Nación Argentina: Régimen de promoción de la economía del conocimiento. Ley N.º 27.506. Publicada en el Boletín Oficial n.º 34132 del 10-jun-2019, p. 3.

Congreso de la Nación Argentina: Servicios de comunicación audiovisual. Ley N.º 26.522. Publicada en el Boletín Oficial n.º 31756 del 10-oct-2009, p. 1.

Congreso de la Nación Argentina: Tecnologías de la Información y las Comunicaciones. Ley N.º 27.078. Publicada en el Boletín Oficial n.º 33034 del 19-dic-2014, p. 1.

Congreso de la Nación Argentina: Defensa del consumidor, Ley N.º 24.240. Publicada en el Boletín Oficial n.º 27744 del 15-oct-1993, p. 34.

Congreso de la Nación Argentina: Código Civil y Comercial. Ley N.º 26.944. Publicada en el Boletín Oficial n.º 32985 del 8-oct-2014, p. 1.

Congreso de la Nación Argentina: Código Penal Argentino. Ley N.º 11.179. Publicada en el Boletín Oficial n.º 8300 del 3-nov-1921, p. 826.

Congreso de la Nación Argentina: Ley de protección de datos personales. Ley N.º 25.326. Publicada en el Boletín Oficial n.º 29517 del 2-nov-2000, p. 1.

Congreso de la Nación Argentina: Ley de Propiedad Intelectual. Ley N.º 11.723. Publicada en el Boletín Oficial n.º 11799 del 30-sep-1933, p. 1.

Poder Ejecutivo Nacional: Ley Nacional de Telecomunicaciones. Dec-Ley n.º 19.798. Publicada en el Boletín Oficial nº 22489 del 23-ago-1972 Página: 2

Poder Ejecutivo Nacional: Aislamiento Social Preventivo y Obligatorio Coronavirus (COVID-19). DNU n.º 297/2020. Publicada en el Boletín Oficial n.º 34334 del 20-mar-2020, p. 3.

—ARTÍCULO—

La actividad aeronáutica en tiempos de pandemia de COVID-19

Matías Barone

Abogado y Docente Universitario Autorizado, UNLP. Especialización en Derecho de la Navegación y Comercio Exterior, UBA. Profesor Titular Asociado de la Cátedra de Derecho Marítimo y Aeronáutico de la UCALP y Profesor Adjunto Ordinario de la Cátedra I de Derecho de la Navegación de la UNLP.

Paolo Marino

Ingeniero Aeronáutico y Docente Universitario. Ayudante Diplomado en las cátedras de Aeropuertos y Operaciones de Vuelo y en Planificación y Diseño de Estructuras Aeroportuarias en la carrera de Ingeniería Aeronáutica de la FI-UNLP, Asesor del Grupo de Transporte Aéreo de la Facultad de Ingeniería, UNLP, Profesor del Postgrado Interdisciplinario de Derecho Aeronáutico de la UCA, Bs. As, Asesor de la Dirección Nacional de Seguridad Operacional en la Administración Nacional de Aviación Civil, Facilitador en FF. HH.

Resumen

La pandemia de COVID-19 produjo un fuerte impacto en la actividad aeronáutica en general con graves consecuencias para las empresas explotadoras, pasajeros, actividades conexas al servicio de transporte aéreo, como resultado de la paralización o la significativa disminución de las actividades. Las proyecciones de aumento de la actividad experimentada años anteriores se ha visto severamente afectada, por lo que tanto las autoridades aeronáuticas locales como la propia OACI han tomado intervención dictando normas, reglamentaciones, planificaciones de trabajo, y elaborando informes y estadísticas para una mejor comprensión del problema y para intentar mitigar las inevitables consecuencias. El presente artículo pretende, sucintamente, describir el estado de situación y analizar las acciones llevadas a cabo por las instituciones y organismos públicos, haciendo especial referencia a lo ocurrido en nuestro país.

Palabras clave: Pandemia, COVID-19, Servicio de Transporte Aéreo, Trabajo Aéreo, Seguridad Operacional, Autoridad Aeronáutica, OACI.

Abstract

The COVID-19 pandemic produced a strong impact on aeronautical activity in general with serious consequences for operating companies, passengers, activities related to the air transport service, as a result of the stoppage or significant decrease in activities. The projections of increased activity experienced in previous years have been severely affected; hence, both the local aeronautical authorities and the ICAO itself have taken action by issuing standards, regulations, work plans and the preparation of reports and statistics for a better understanding of the problem and so as to try to mitigate the inevitable consequences. This article intends, succinctly, to describe the state of affairs and analyze the actions carried out by public institutions and agencies, making special reference to what happened in our country.

Keywords: Pandemic, COVID-19, Air Transport Service, Aerial Work, Aviation Safety, Aeronautical Authority, ICAO.

1. Introducción

Sin lugar a dudas, la irrupción de la pandemia provocada por la COVID-19 ha generado una crisis de enorme envergadura, principalmente en cuestiones humanitarias, sanitarias, sociales y económicas, con una paralización de las diversas actividades, el transporte, en general, y la actividad aeronáutica, en particular. Dicha actividad no ha sido ajena a la situación colectiva; de hecho, ha colaborado radicalmente en la propagación de la enfermedad por contagio como consecuencia de las bondades que otorga el servicio de transporte aéreo, vinculada a la rapidez del desplazamiento de las personas para llegar a destino, trasladándose de un extremo al otro del planeta en cuestión de horas[1].

La mencionada crisis, como consecuencia de la situación epidemiológica mundial, se traduce en la casi total paralización de la actividad aeronáutica que nuclea el servicio de transporte aéreo: funciona parcialmente lo que se conoce como trabajo aéreo[2] y vuelos

[1] Hay dos elementos clave que diferencian a la pandemia de COVID-19 de las anteriores: el mayor grado de contagio: tiene aproximadamente el doble de propagación comunitaria que el virus de la gripe común. El SARS-CoV-2 es muy infeccioso y contagioso; a su vez, puede transmitirse por el aire. Además, la vida media del virus en diversos materiales de uso común (acero, plásticos, papel, madera, aluminio, etc.) es, en general, superior al de otros tipos de virus. Finalmente, tiene una elevada propagación y replicación con portadores asintomáticos, lo que hace más difícil su detección temprana y posibilidad de prevención. También hemos de mencionar la velocidad con la que se diseminó por el planeta: en una semana se había extendido a más de cuarenta países. Esto no tiene precedentes, y está claro que la mayor conectividad desde la actividad aeronáutica es uno de los factores que hicieron posible esta velocidad y modelo de expansión del virus (Lombardo, 2020: p. 3).

[2] Como lo señala Juan A. Lena Paz al explicar el concepto de trabajo aéreo: «El Código define por exclusión al trabajo aéreo, expresando que comprende toda actividad comercial aérea, con excepción del transporte (art. 92, párr. 2). El codificador ha recurrido a este temperamento por cuanto, dice, la definición del trabajo aéreo en sentido positivo parece imposible, teniendo en cuenta la variedad de actividades comprendidas en

autorizados, específicamente por ser considerados esenciales o de soporte a actividades esenciales, por expresa disposición de la normativa dictada al efecto por las autoridades nacionales; por lo tanto, ha sido autorizada para continuar su desarrollo con habitualidad, cumpliendo con los protocolos sanitarios establecidos al efecto.

Planteada la coyuntura, el presente trabajo tiene como objetivo describir el estado de situación actual de la actividad aeronáutica tanto en nuestro país como a nivel internacional, con especial énfasis en el servicio de transporte aéreo, analizando la normativa que se ha dictado al efecto por las autoridades nacionales y también aquellas acciones que ha efectuado la Organización de Aviación Civil Internacional (OACI) conjuntamente con otros organismos de Naciones Unidas; asimismo, pretendemos formular algunas consideraciones como proyecciones a futuro del posible desarrollo de la actividad aeronáutica en la etapa pospandemia, ya que, entendemos, la actividad aeronáutica no será igual a partir de este momento hasta tanto no se logre erradicar definitivamente los efectos de esta enfermedad.

2. Principales consecuencias de la pandemia sobre la actividad aeronáutica en general

La declaración de pandemia por parte de la Organización Mundial de la Salud (OMS) respecto de la COVID-19 debe retrotraerse al día 11 de marzo de 2020[3], al considerar la situación como una emergencia de salud pública con preocupación internacional casi un mes y medio antes —el día 30 de enero de 2020—, momentos en que los contagios ya se encontraban en más de 114 países.

En ese marco pandémico y de incertidumbre sanitaria, el desconocimiento del origen de la enfermedad o de un tratamiento adecuado, la propagación del contagio a diversos lugares del planeta y los numerosos decesos que se iban incrementando conforme las informaciones oficiales de los países generaron estupor en la población mundial, lo cual ha tenido considerables repercusiones en la aviación civil a nivel mundial, y no escapa a ello el propio escenario local con las particularidades propias de nuestro país, tanto en el

la expresión. Entre dichas actividades podemos mencionar, por ejemplo: la fumigación de campos desde aviones para combatir las plagas de la agricultura, la fotografía aérea, etc.» (Lena Paz, 1987, p. 118). Como ejemplos, pueden citarse: la publicidad aérea, fumigación, fotografía, búsqueda y salvamento, etc.

[3] Conforme el anuncio del Director General de la Organización Mundial de la Salud (OMS), Tedros Adhanom Ghebreyesus, quien señaló que la nueva enfermedad por el coronavirus 2019 (COVID-19) puede caracterizarse como una pandemia; expresó: «La OMS ha estado evaluando este brote durante todo el día y estamos profundamente preocupados tanto por los niveles alarmantes de propagación y gravedad, como por los niveles alarmantes de inacción. Por lo tanto, hemos evaluado que COVID-19 puede caracterizarse como una pandemia». Además añadió que «describir la situación como una pandemia no cambia la evaluación de la OMS de la amenaza que representa este virus. No cambia lo que está haciendo la OMS, y no cambia lo que los países deberían hacer». En estos momentos, hay más de 118.000 casos en 114 países, y 4291 personas han perdido la vida. Información publicada por la Organización Panamericana de la Salud, disponible en el sitio https://www.paho.org/es/noticias/11-3-2020.

ámbito sanitario —si bien tardíamente, en comparación con otros países— como en el económico, político y social.

Para poder considerar el impacto de la pandemia en la actividad aeronáutica, es necesario precisar algunas ideas previas, debiendo entender que la aviación civil en nuestro país, por una cuestión geográfica, tanto de ubicación global como de superficie y distribución, es un caso particular muy distinto a los posibles escenarios que plantean otros países que se toman como modelo. En dichos casos, por ejemplo, los países de la Comunidad Europea, fuera de cualquier aspecto socioeconómico, la principal diferencia radica en la cuestión de superficie de los territorios —repárese, por citar algún ejemplo, que, en estos países, el transporte aéreo compite con los trenes de alta velocidad—, y también en cuestiones vinculadas a la capacidad o en términos aeronáuticos, envergadura del sistema, si tomamos como referencia al sistema aeronáutico de los Estados Unidos respecto de la operatividad y la infraestructura.

Ahora bien, los efectos negativos de la pandemia sobre las actividades conexas con el transporte aerocomercial y, sobre todo, las actividades proveedoras de bienes y servicios para aquella son evidentes, por cuanto las proyecciones previas a la pandemia nos evidenciaban tasas de pasajeros transportados en continuo crecimiento, con mayor cantidad de frecuencias a destinos, especialmente teniendo en cuenta la situación actual del transporte aerocomercial (en particular, el caso de las líneas aéreas).

Tales ideas surgen del análisis efectuado respecto del período comprendido entre mediados de marzo y la fecha de desarrollo del presente trabajo de este año 2020, donde se avizora, según declaraciones del Ministerio de Transporte, un retorno de los vuelos aerocomerciales para mediados o fines del octubre del corriente año[4]; sin embargo, aún no sabemos si podrá efectivamente retomarse la actividad en su plenitud, ni a qué alcance de vuelos hacen especial referencia los anuncios de las autoridades, sean estos vuelos internacionales o nacionales —cabotaje—, ni en qué proporción de la ocupación de la aeronave, por la expectativa o confianza de los pasajeros por querer viajar o por alguna disposición de las autoridades en cuanto a una utilización limitada y autorizada de las aeronaves.

Respecto de esto último, se considera como criterio la tasa de ocupación de la aeronave para que el vuelo resulte económicamente factible (*breakeven*, conforme su identificación en la lengua inglesa), incluida así la cobertura total de gastos que insume la actividad de transporte para que el vuelo resulte rentable para el explotador de la aeronave, además

[4] Los anuncios de las autoridades nacionales respecto del reinicio de los vuelos comerciales nacionales –cabotaje– sufrieron varias prórrogas, debiendo tener presente que se había autorizado inicialmente a las aerolíneas la venta de pasajes a partir del 1 de septiembre del presente año, con lo cual se presumía esa fecha como el comienzo de la actividad, pero la expansión de la enfermedad y el aumento de contagios en nuestro país implicó su postergación hasta el 13 de octubre pero comenzando efectivamente los vuelos recién el día 22, apertura que no incluyó todos los destinos nacionales. Cronista Comercial, Suplemento Apertura – Negocios (2020, 13 de octubre), "Levantan la cuarentena aérea y las compañías se preparan para volver a volar el 19 de octubre", recuperado el 13 de octubre de 2020 de https://www.cronista.com/apertura-negocio/empresas/Levantan-la-cuarentena-aerea-y-las--companias-se-preparan-para-volver-a-volar-el-19-de-octubre-20201012-0012.html.

de tener presente otras variables, como el tipo de vehículo, su configuración, tipo de operación, ruta operada, etc., cuyo cálculo es estimado por la Asociación Internacional de Transporte Aéreo (IATA)[5] en un 79 %[6], para que las líneas aéreas no sigan perdiendo dinero.

Como se observa, la paralización total no solo genera la correspondiente pérdida, teniendo presente gastos de mantenimiento de aeronaves, sino también los gastos correspondientes a las remuneraciones de personal[7], o, por ejemplo, una modalidad contractual típica de la actividad aeronáutica, como ser el «leasing de las aeronaves» con su correspondiente obligación de pago, sin la posibilidad de obtener ingresos por la paralización de la actividad para hacer frente a dichos gastos.

Estimamos que el porcentaje arriba indicado, considerando la situación económica de nuestro país, aun sin el marco de la pandemia y la consabida dolarización de insumos —con los aumentos o fluctuación de dicha divisa y sin haber llegado a una devaluación de peso que es referida en la opinión pública—, sumado a los costos propios de la operativa aeroportuaria en general, debería ser sin dudas mayor.

De esta manera, teniendo presente los costos fijos de una aerolínea para mantenerse operativa, la paralización de todos los vuelos por casi siete meses, la autorización de una menor cantidad de vuelos atento a que no todos los puntos del país han logrado la conectividad implicará el desempeño de una situación claramente deficitaria para el sector, contemplando que necesariamente deberán subirse las tarifas o bien el coeficiente de ocupación, por lo que, al hacer una predicción racional, puede asumirse que el retorno a las operaciones no será tan voluminoso como pudo haberse pensado durante los primeros meses de este «parate operativo».

Como dato estadístico, en el 2015, el *breakeven* en la Argentina estaba en un 70%, época donde comienzan a surgir las inversiones para el desarrollo de las *low cost*[8]; al cierre

---

[5] La Asociación de Transporte Aéreo Internacional (IATA) es la asociación comercial mundial del sector de las líneas aéreas internacionales. Fue fundada en La Haya, en 1919, por 57 miembros fundadores mayormente de Europa y Norteamérica. En la actualidad presenta a unas 290 aerolíneas de más de 120 países, que mueven el 82% del tráfico aéreo mundial. Disponible en https://www.iata.org/en/about/.

[6] Recuperado de https://www.iata.org/en/iata-repository/publications/economic-reports/downgrade-for-global-air-travel-outlook/.

[7] La empresa Aerolíneas Argentinas aplicó a 7.500 trabajadores el régimen de suspensión regulado por el art. 223 Bis de la LCT durante el plazo de duración de la inhabilitación de las actividades –suspensión del contrato de trabajo– a partir del mes de mayo de 2020. De esta manera se abonó una suma no remunerativa equivalente el 75 % de las remuneraciones percibidas por el personal aeronavegante en la actualidad. Infobae, Suplemento Economía (2020, 31 de mayo), "Aerolíneas Argentinas suspenderá por dos meses a 7.500 de sus 12.000 empleados", recuperado el 31 de mayo de 2020 de https://www.infobae.com/economia/2020/05/31/con-una-caida-de-97-en-sus-ingresos-aerolineas-suspendera-por-dos-meses-a-7500-de-sus-12000-empleados/.

[8] También suelen denominarse compañías de bajo coste (CBC) o bien *low cost carriers* (*LCC´S*). «Los servicios aéreos "low cost" son los prestados por transportadores que, elaborando estrategias comerciales de estricta reducción de gastos, y amplio aprovechamiento de sus recursos, compiten en el mercado aerocomercial cumpliendo sus servicios de bajo costo y ofreciendo prestaciones básicas a precios sensiblemente inferiores a los regulares de los transportadores tradicionales» (Balián, 2011: p. 14).

del 2019 en nuestro país, debido a los valores de las tarifas y los costos operativos, ese valor sumó indefectiblemente 10 puntos.

De acuerdo a los datos publicados por la OACI y la IATA, se han evidenciado resultados del transporte aéreo mundial relativos al ejercicio 2018, que muestran que el transporte aéreo era cada vez más accesible y más eficiente. En particular, el informe elaborado mediante el Comunicado 45 de la IATA (2019) señala que:

- 4400 millones de pasajeros volaron en 2018.
- Se alcanzó un máximo de eficiencia con un 81,9 % de asientos ocupados.
- La eficiencia en consumo de combustible mejoró más de un 12 % respecto al año 2010.
- 22000 pares de ciudades están conectadas en la actualidad por vuelos directos —1300 más que en 2017 y más del doble respecto a las 10 250 que había en el año 1998—.
- El sector de aerolíneas identificadas como low cost continúa superando al sector de transporte regular. Debe tenerse presente que no se trata de aeronaves con otras características, sino que el plan de negocios prescinde de muchos de los servicios de una aerolínea tradicional, con el afán de abaratar costos, seduciendo primero a los pasajeros y luego a las propias aerolíneas tradicionales.
- 4100 millones de pasajeros transportó la industria aeronáutica en el año 2017, que aumentó en 300 millones en el año siguiente.

Las referencias efectuadas en cuanto al desarrollo de la actividad aeronáutica en los años anteriores nos permiten comprender con mayor claridad el impacto negativo que ha tenido la pandemia en el sector, sobre todo teniendo en cuenta la expansión de la actividad aeronáutica. Es decir, es más evidente cuando la actividad año tras año demostraba un crecimiento nunca visto.

Al considerar la situación deficitaria descrita, en un reciente artículo, Horacio M. Pratto Chiarella describe el proceso concursal de la empresa Latam Airlines Group en los Estados Unidos y el salvataje otorgado por Alemania a Lufhtansa, empresas que habían sufrido el impacto de la pandemia en forma exponencial utilizando estas herramientas jurídicas para lograr su subsistencia en lugar de su extinción; el autor precisa:

> Por ello, cuando vemos que tal o cual firma entró en bancarrota y pidió acogerse al Capítulo 11 de la Ley de Quiebras del país del norte, no debemos pensar en la desaparición de la misma o el cese de sus operaciones inmediatas, sino en la reestructuración económico-financiera de la firma con el objeto de que la misma pueda salir adelante sin necesidad de la intervención necesaria de un síndico, como ocurre en el régimen jurídico de la República Argentina… Ahora bien, el impacto económico-financiero que tiene el COVID-19 sobre las empresas de transporte aéreo primordialmente se encuentra relacionado con el flujo de efectivo o *cash flow* que se ve drásticamente menguado, por no decir prácticamente eliminado, del giro comercial de estas empresas. Por tanto, esta falta de liquidez, entendida por la imposibilidad de hacer frente a sus obligaciones de corto plazo, así como los

> compromisos asumidos en materia de adquisición y financiamiento de aeronaves, fuerzan a las compañías aéreas a caer en lo que se conoce como estado de cesación de pagos, supuesto esencial para lograr el acogimiento de la empresa bajo la Ley de Quiebras de USA, sea en su Capítulo 7 u 11, dependiendo del estado financiero de la firma, el objetivo de la compañía de continuar con sus operaciones y el interés del Estado Nacional o de potenciales inversores de adquirir participaciones en la compañía… (Pratto Chiarella, 2020: p. 2)

Es evidente que el impacto de la pandemia de COVID-19 se ha producido, por lo menos, en cuatro aspectos que visualizamos fundamentales: la actividad aeronáutica, el turismo, el comercio y la economía.

Repasemos algunos datos estadísticos efectuados que nos permitirán ilustrar aún más la situación, teniendo presente que se comparan con el año anterior.

2.1. Tráfico de pasajeros aéreos

Se ha observado una reducción general del tráfico de pasajeros aéreos, incluidos los servicios de transporte aéreo nacionales e internacionales, entre el 60% y el 62% en lo que va del año 2020 —obviamente, dicho porcentaje estará en ascenso hasta tanto se normalice la actividad— si se lo compara con el año 2019, según lo ha informado en el Comunicado 45 de la IATA (2019).

2.2. Aeropuertos

Obviamente, la paralización de la actividad implicó la falta de utilización de los aeropuertos y aeródromos; se estima una pérdida aproximada del 60% del tráfico de pasajeros y el 61% o más de USD 104 500 millones de ingresos por actividades aeroportuarias en 2020, en comparación con los negocios habituales —según el Consejo Internacional de Aeropuertos (ACI)— (como se citó, Comunicado 45 de la IATA (2019).

2.3. Explotadores de aeronaves: las aerolíneas

En la mayoría de los países, se determinó la prohibición de venta de pasajes en los primeros meses de la pandemia por cuanto no se contaban con protocolos sanitarios específicos para evitar los contagios —tampoco se conocía tanto sobre la enfermedad—, con lo cual las empresas explotadoras del servicio de transporte aéreo tuvieron una disminución del 54,7 % en los ingresos por pasajeros/kilómetros (RPK)[9], tanto para vuelos

[9] *RPK* (*revenue-passenger-kilometers*): cantidad de pasajeros transportados multiplicado por la distancia recorrida. ASK (available-seat-kilometers): cantidad de asientos disponibles para la venta multiplicado por la distancia recorrida. PLF (*passenger-load-factor*): el factor de ocupación se obtiene dividiendo los RPK entre los ASK.

nacionales como internacionales, en el año 2020, en comparación con el año anterior, conforme IATA; Comunicado 45 (2019).

En cuanto a esta cuestión, tanto en nuestro país como a nivel internacional, han sido los organismos internacionales o las autoridades sanitarias de cada uno de los países que forman parte de la OACI los que han determinado la suspensión de los vuelos fundados en la necesidad de aislar a las personas como único medio conocido —o mejor dicho, efectivo— para evitar los contagios; de esta manera, las determinaciones de los órganos especializados (nacionales o internacionales) dictaron sus normas con el fundamento sanitario respectivo.

2.4. Turismo

La imposibilidad de traslado de los turistas implicó una reducción en los ingresos por turismo internacional de entre USD 910 y 1,170 billones en 2020, frente a los 1,5 trillones de dólares generados en 2019, con el 100% de los destinos turísticos mundiales con severas restricciones de viaje (por la Organización Mundial del Turismo [OMT]; Comunicado 45 de la IATA (2019).

2.5. Comercio y economía mundial

Si bien el comercio ha experimentado algunas transformaciones (por ejemplo, el claro incremento en el comercio de la industria alimenticia y, obviamente, en el comercio electrónico), en términos generales dicha actividad tuvo una caída del volumen del comercio mundial de mercancías de un 9,2% en 2020 en comparación hasta 2019 (por la Organización Mundial del Comercio; Comunicado 45 de la IATA (2019).

Todo ello ha significado que la economía mundial tenga una retracción proyectada —lógicamente, dado el nivel de incertidumbre de inversores o consumidores— del -4,4% al -5,2% del PIB mundial en 2020, mucho peor que durante la crisis financiera de 20082009 (por el FMI y el Banco Mundial; Comunicado 45 de la IATA (2019) Informe 2019 WATS); a su vez, si bien las estadísticas no resultan a la fecha fiables, se está analizando si la crisis actual para el caso de la Argentina supera la crisis del año 2001.

Como pudo observarse el transporte aerocomercial y la conectividad en el mundo, en general, conforme los datos referenciados, y en la República Argentina, en particular, se vieron fuertemente afectadas producto de las medidas tomadas para evitar la propagación por vía aérea y ralentizar el desarrollo de la pandemia de COVID-19, lo cual ha dado como resultado una reducción drástica de la actividad.

Brevemente se ha comentado el impacto en la actividad aerocomercial en lo que se refiere a cantidad de vuelos, y en los próximos párrafos nos referiremos a las consecuencias en las aeronaves, las tripulaciones y el personal aeronáutico.

Como se sabe, la aviación es el medio de transporte más seguro, y quizás poco se sabe de por qué puede afirmarse esa frase. En las próximas líneas, trataremos de explicarlo enfocándonos en las aeronaves y el personal aeronáutico.

Debido a la urgente necesidad de reducir los riesgos relacionados con la pandemia de COVID-19 por medio del transporte aéreo y como resultado de las prácticas de aislamiento/distanciamiento social, al cierre de los espacios de trabajo y a otras medidas de intervención de salud pública, varios Estados están tomando diversas acciones para habilitar a los proveedores de servicios y personal para mantener la validez de sus certificados, licencias y otras aprobaciones de carácter operativo en el marco de la pandemia.

En ese sentido, los Estados han implementado acciones que pueden incluir cambios temporales a las regulaciones nacionales, o «atenuaciones» necesarias para mantener las operaciones de aviación durante la pandemia del COVID-19. Estas atenuaciones se refieren a diferencias temporales según lo dispuesto en el artículo 38 del Convenio sobre la Aviación Civil Internacional de 1944 (Convenio de Chicago), y exenciones y excepciones temporales, como se describe en el Manual de Vigilancia de la Seguridad Operacional10 (Doc. OACI 9734).

Por último, y dentro del ámbito del derecho privado y del contrato de transporte aéreo, la cancelación de vuelos ha provocado las sucesivas reprogramaciones y reexpediciones de ticket o billetes de pasajes, ofreciendo las aerolíneas la devolución del dinero abonado —debe tenerse presente el valor de un pasaje adquirido en nuestro país hace un año— o el ofrecimiento de un vuelo de las mismas características que el contratado sin cargos extra.

El incumplimiento del contrato de transporte de pasajeros por vía aérea presentaba el alea de la fuerza mayor y fue motivo de muchas consultas al inicio de la pandemia, pero la cuestión fue resuelta en buenos términos con acuerdos entre pasajeros y aerolíneas. A la fecha, no se conocen fallos sobre incumplimiento contractual y la posible alegación de la eximente fuerza mayor[11].

---

[10] Según OACI, «el estado donde la posibilidad de dañar a las personas o las propiedades se reduce y mantiene al mismo nivel o debajo de un nivel aceptable mediante el proceso continuo de identificación de peligros y gestión de riesgos de la seguridad operacional», recuperado de https://www.anac.gov.ar/anac/web/uploads/ssp-sms/doc_oaci_9859.pdf. Es por ello por lo que la gestión del riesgo es un proceso social complejo que conduce al planeamiento y aplicación de políticas, estrategias, instrumentos y medidas orientadas a impedir, reducir, prever y controlar los efectos adversos sobre la población, los bienes y servicios y el ambiente.

[11] Lena Paz nos enseñaba respecto de esta eximente de responsabilidad al tratar el tema de la responsabilidad del transportador aéreo: «Se trata de una cuestión de hecho que deberá ser apreciada según las circunstancias del caso, en función del ejercicio normal de la profesión y no "in abstracto". La correspondiente evaluación deberá ser hecha, a nuestro juicio, prescindiendo de los conceptos de imprevisibilidad, irresistibilidad e inimputabilidad, que caracterizan la fuerza mayor del Derecho Civil, por cuanto, de lo contrario, podría colocarse al transportador en situación de no poder acreditar la imposibilidad de haber tomado las medidas conducentes para evitar el daño, contrariándose con el espíritu de la legislación aeronáutica —internacional e interna— de otorgar al transportador en materia de responsabilidad contractual, un régimen más favorable que el contenido en el derecho común» (Lena Paz, 1987: p. 240).

3. La regulación de carácter excepcional en nuestro país para el tratamiento de la pandemia de COVID-19

El estado de situación descripto implicó el dictado de normativas de carácter general y particular, de lo cual resultó como norma principal el Decreto del PEN 260/2020 (B. O. del 12/3/2020), que dispuso la ampliación de la Emergencia Sanitaria que había sido declarada con anterioridad por el art. 1 de la Ley 27.541 (B. O. del 23/12/2019), prescribiendo en su art. 9, la «suspensión temporaria de vuelos» al referirse a los vuelos internacionales de pasajeros provenientes de las zonas afectadas por la pandemia, medida que, originariamente, se adoptó por un término de 30 días. De esta forma, han sido las autoridades sanitarias las que han efectuado las recomendaciones para evitar la propagación de los contagios, comunicando a los órganos de contralor especializados para proceder a dictar la respectiva normativa.

La misma norma delega en la autoridad de aplicación (en este caso, el Ministerio de Salud de la Nación) la facultad de «prorrogar o abreviar el plazo dispuesto, en atención a la evolución de la situación epidemiológica». Como se observará seguidamente, la repentina expansión de los contagios a nivel mundial y el desconocimiento de la enfermedad provocaron que las primeras normas establecieran plazos reducidos, pensándose, quizás, que la situación epidemiológica podría ser superada a la brevedad, pero esto, lamentablemente, no ha ocurrido.

Además, se permitió la posibilidad de disponer diversos casos de excepción para facilitar el regreso de personas residentes en nuestro país (repatriación), debiendo cumplir en su caso con medidas preventivas y protocolos de seguridad una vez arribados a nuestro territorio (el aislamiento preventivo por un lapso de 14 días).

En forma complementaria, el Decreto del PEN 274/2020 (B. O. del 16/3/2020) dispuso la prohibición del ingreso al territorio nacional por un lapso de 15 días corridos a los extranjeros no residentes en el país a través de los aeropuertos (la medida también incluía puertos, pasos internacionales, centros de frontera y otros puntos de acceso). Dicha determinación ha sido adoptada por la mayoría de los países, y es conocida como un cierre de fronteras que a la fecha persiste.

Por su parte, el Ministerio de Transporte, dictó la Resolución 64/2020 (B. O. del 18/3/2020) que dispuso la suspensión total de los servicios de transporte aéreo de cabotaje comercial y de aviación, en general. Claramente, la norma hace referencia al servicio de transporte aéreo y no al trabajo aéreo (ver nota 2), servicio este último que se continúa prestando en la actualidad.

A los fines de dar cumplimiento a la normativa emanada del PEN, el mencionado Ministerio dicta la Resolución 71/2020 (B. O. del día 20/3/2020), mediante el cual se instruye a la Administración Nacional de Aviación Civil (en adelante ANAC[12]) para que «establezca las excepciones a aplicarse respecto del transporte aerocomercial, por razones

[12] La ANAC es la autoridad aeronáutica nacional. Es un organismo descentralizado dentro de la órbita del Ministerio de Transporte de la Nación, fue creada por Decreto 239/2007 (B. O. del 19/3/2007).

de carácter alimentario y/o humanitario y/o necesarias para el cumplimiento de tareas esenciales en el marco de la emergencia decretada (art. 8)».

Respecto de esto último, debe recordarse que, con fecha 15 de abril de 2020, partió con destino a China una aeronave Airbus 330-200 de Aerolíneas Argentinas en búsqueda de insumos médicos críticos para el tratamiento de la COVID-19, como ser termómetros digitales, trajes de bioseguridad y kits de detección temprana. La aeronave retornó a nuestro país tres días más tarde con más de 13 toneladas de los insumos descriptos. A este primer vuelo, se le sumaron unos 35 vuelos más hasta fines de octubre, transportando 887 toneladas de materiales e insumos médicos, y se prevén 6 vuelos más, lo cual totaliza 41 vuelos y 1040 toneladas en total para fines de noviembre.

La suspensión de los vuelos fue prorrogada hasta el día 31 de marzo de 2020 mediante el art. 2 de la Resolución del Ministerio de Transporte 73/2020 (B. O. del día 24/3/2020). Más allá de la prórroga, es importante destacar que el articulo siguiente reglamenta dentro de las excepciones a las suspensiones aludidas «al transporte de pasajeros para el traslado de personas que presten servicios o realicen actividades declarados esenciales en el marco de la emergencia pública declarada»; de esta manera, la actividad aeronáutica queda reducida al trabajo aéreo y al servicio de transporte aéreo de excepción (vuelos sanitarios e INCUCAI), de ahí nuestra mención de la casi total paralización de la actividad que formuláramos *supra*.

La normativa en su totalidad determina una situación general de suspensión, pero, en función del análisis de la actividad en particular, comienzan a autorizarse actividades que son consideradas esenciales para el desarrollo de tareas mínimas o de mantenimiento.

Por su parte, mediante la Resolución 99/2020 de la ANAC (B. O. del 18/3/2020) dispuso la creación de un comité especializado para el tratamiento con el nombre de Comité de Crisis Prevención COVID-19 en el Transporte Aéreo, cuyas funciones principales resultan ser: brindar conocimiento sobre las principales medidas de prevención para las personas usuarias del sistema, capacitar al personal de las distintas áreas de trabajo, establecer sistemas de detección de contagios e intervención en el caso concreto, elaboración de métodos de mitigación de la enfermedad, etc. (art. 4).

La labor del Comité de Crisis Prevención COVID-19 en el Transporte Aéreo, mediante la elaboración de estudios e informes, permitió desarrollar recomendaciones, protocolos y procedimientos, realizando actividades en forma conjunta con el Ministerio de Salud y la ANAC, como dan cuenta los protocolos existentes para los vuelos autorizados en el mes de octubre.

A su vez, uno de los temas recurrentes durante los primeros meses de la pandemia, en la opinión pública nacional, abarcó la situación de los ciudadanos argentinos o extranjeros residentes en nuestro país que se encontraban «varados» en otros países con motivos de viajes realizados a dichos destinos con anterioridad a la sanción del plexo normativo que se está analizando. Varios fueron los vuelos autorizados por la ANAC para cumplir con dicho cometido, debiendo cumplimentar los requisitos que establece la Resolución 100/2020 (B. O. del día 17/3/2020) dictada por el organismo.

En resumen, y como surge de esta última resolución administrativa, a los fines de acceder a la excepción, se deberá acreditar que el vuelo cuya autorización se solicita responde a razones humanitarias de repatriación de ciudadanos argentinos o residentes del país de bandera o del transportista extranjero. Para el caso de vuelos nacionales, deberá demostrarse que la solicitud obedece a razones de carácter sanitario, humanitario o que deviene necesario para el cumplimiento de tareas esenciales en el marco de la emergencia.

La norma siguiente, también emanada de la ANAC (Resolución 101/2020, B. O. del día 20/3/2020), resultó de suma importancia por cuanto procedió a prorrogar las licencias, por un plazo de 90 días, a todas las habilitaciones y certificados otorgados por la Parte 61 de las Regulaciones Argentinas de Aviación Civil (RACC) (art. 1). Por un mismo plazo, se prorrogaron las «Licencias para miembros de la tripulación, excepto pilotos» (Parte 63 del RACC), los «Certificados de competencia de tripulante de cabina de pasajeros» (Parte 64 del RACC), las «Certificaciones Médicas Aeronáuticas (CMA)» otorgadas de acuerdo con lo establecido en la Parte 67 de las RAAC, todas las autorizaciones de operación y aprobaciones de cursos emitidas bajo la Parte 141 «Centros de Instrucción de Aeronáutica Civil (CIAC)» y la Parte 142 «Centros de Entrenamiento de Aeronáutica Civil (CEAC)» de las RAAC, entre otros. Esta última resolución, que fue prorrogada efectivamente, es de suma importancia, ya que el reglamentarismo es uno de los caracteres del derecho aeronáutico[13], y justamente, mediante tales directrices, se determina y optimizan las medidas de seguridad de los vuelos, que no solo implica el mantenimiento y la habilitación de las aeronaves, sino también la capacitación y habilitación del personal aeronáutico.

Teniendo presente las suspensiones indicadas y sus prórrogas, la ANAC emitió las Resoluciones 143 y 144 (ambas publicadas en el B. O. del día 27/4/2020), por medio de las cuales autorizó a las diversas líneas aéreas que operan el servicio de transporte aéreo desde, hacia o dentro del territorio nacional a reprogramar y comercializar los pasajes aéreos, estableciendo una fecha estimativa de inicio de operaciones a partir del 1 de septiembre de 2020, que, como se verá, fue prorrogada hasta mediados de octubre del mismo año. De esta manera, la situación continúa extendida hasta esa fecha[14].

[13] Conforme Videla Escalada: «El reglamentarismo del Derecho Aeronáutico […] proviene de una necesidad de adaptación permanente a las exigencias de la técnica que imponen su movilidad y, al mismo tiempo, exigen la multiplicación de los preceptos positivos, de manera tal que no basta la simple sanción de leyes generales, sino que los textos deben acumularse hasta el detalle, circunstancia que exige al legislador delegar, en buena medida, sus facultades en el poder administrativo, para que proceda por vía de reglamentaciones complementarias (Videla Escalada, 1978: p. 20-21)».

[14] Como se dijo, luego de las prórrogas a la suspensión de vuelos dispuesta por las autoridades nacionales, originariamente se había estimado el comienzo de actividades para el 1 de septiembre de 2020. Más tarde, se indicó que comenzarían el día 12 de octubre, pero la actividad comenzó parcialmente a partir del día 22 de octubre. Las aerolíneas han definido los cronogramas para sus vuelos, dependiendo de su aprobación por la ANAC y de que, obviamente, exista un acuerdo en última instancia que cada una de las provincias que pretendan recibir vuelos. Ya han manifestado su intención de recibir vuelos Corrientes, Iguazú, Mendoza, Tucumán, Ushuaia, Córdoba y Rio Negro. Por otro lado, y para el caso de vuelos internacionales, la autorización de los vuelos corre exclusivamente por la determinación de cada país. En Europa, especialmente España, solo se permite el ingreso a personas que tenga doble ciudadanía, residencia o permisos de trabajo o para realizar estudios, no así a los turistas, manteniendo entonces el régimen de «frontera cerrada», salvo excepciones. Diverso es el caso de Brasil y Estados Unidos, donde se permite la

Como normas de carácter general mediante las cuales fue prorrogada o ampliada la Emergencia Sanitaria establecida originalmente por el Decreto 260/2020, podemos citar los Decretos 297/2020, 313/2020, 325/2020, 331/2020, 355/2020, 365/2020, 408/2020, 459/2020 y 714/2020. Si bien estos hacen referencia a una variedad de actividades, en todas se reitera la cuestión vinculada a la actividad aeronáutica.

Reiterando lo ya expuesto, vinculado a la necesidad de mantenimiento de las aeronaves, mediante la Decisión Administrativa de la Jefatura de Gabinete de Ministros 810/2020 (B. O. del 15/5/2020), se amplió el listado de actividades y servicios considerados esenciales, autorizando así a los trabajadores de la actividad, desprendiéndose del artículo 1, apartados 2 y 3, que pueden prestar servicios (es decir, se encuentran exceptuados de cumplir con el Aislamiento Social Preventivo y Obligatorio —ASPO—), las actividades y servicios de mantenimiento y reparación de material de aeronaves (apartado 2) y la fabricación y provisión de insumos y repuestos indispensables para la prestación del servicio de transporte «… aéreo y cualquier otro que sea necesario para el mantenimiento de […] aeronaves (apartado 3)».

Teniendo en cuanta que la actividad de trabajo aéreo continuó operando con alguna normalidad, la Resolución 205/2020 de la ANAC (B. O. del 22/7/2020) autorizó a prestar servicio a aquellas empresas de trabajo aéreo que realicen actividades en la especialidad agroaéreo.

Tras meses de labor, análisis estadísticos e informes especializados, mediante la Resolución 221/2020 del Ministerio de Transporte (B. O. del 14/10/2020), se establece que, para la reanudación de los servicios de transporte aéreo de cabotaje comercial y aviación general, todos los operadores de servicios de transporte aéreo deben contar con procedimientos y protocolos elaborados por el Ministerio de Salud. La implementación de ellos será fiscalizada por la ANAC, debiendo requerir este organismo la intervención o informes al Comité de Crisis Prevención COVID-19 en el Transporte Aéreo.

En consecuencia, la ANAC dicta la Resolución 304/2020 (B. O. del día 15/10/2020), mediante la cual —derogando alguna normativa anterior— se aprobó el Anexo I de «Requisitos a cumplimentar por las líneas aéreas para obtener autorización para la realización de vuelos de cabotaje» (art. 2). El artículo siguiente refiere que las empresas de transporte aéreo regular y no regular[15] deberán contar con procedimientos y protocolos elaborados de conformidad con los lineamientos y condiciones del Ministerio de Salud.

circulación, con el debido cumplimiento de los requisitos impuestos con anterioridad a la pandemia: en el último caso, las visas y billete de pasaje con retorno como requisito para posibilitar el ingreso.

[15] «Entonces, la característica de toda línea aérea regular es que se ejecute dentro del espacio aéreo de un país, países limítrofes o no, pero que ella pueda ser utilizada por el usuario en general, que tenga un horario que cumplir, tarifas prefijadas y que sus vuelos sean ejecutados con frecuencia... En cambio, la denominada aviación libre o irregular se asienta en la ausencia de tales requisitos. No está sometido a aquellas condiciones de subsistencia, su trabajo se desarrolla cuando existe un trasporte de carga o de pasajeros, conviniendo libremente su prestación, recorrido y tarifas» (Foglia y Mercado, 1976: p. 46).

La Resolución ANAC 305/2020 (B. O. del día 21/10/2020) es una norma de carácter similar a la resolución comentada, pero establece los requisitos que deben cumplimentar las empresas de transporte aéreo no regular.

La descripción mencionada, que a todo evento devino necesaria para comprender el estado de situación excepcional, contiene las normas más importantes del PEN, del Ministerio de Transporte y, especialmente de la ANAC; estas demuestran en su conjunto el impacto de la pandemia y el dictado de normas sucesivas, observando la evolución de la situación sanitaria y epidemiológica sobre la población; todo ello conforme el asesoramiento de expertos en materia sanitaria. Finalmente, culmina con la autorización parcial del servicio de transporte aéreo cuando se observe el cumplimiento de todas las medidas y protocolos sanitarios presentados al efecto.

4. La labor de la OACI en el contexto internacional

El derecho aeronáutico y también el derecho de la navegación tienen caracteres similares, entre ellos, la internacionalidad y la uniformidad. Sin entrar en definiciones de orden académico, nos demuestran en la práctica que la actividad de los organismos internaciones (OACI, Organización Marítima Internacional [OMI], UNCTAD, por citar algunos de ellos) responden en forma inmediata a los sucesos ocurridos —algún profesor universitario solía enseñarnos que los Convenios Internacionales OMI-OACI siguen la *siniestrología*—, intentando regular la novel situación que, hasta el momento, era desconocida y en ese marco en el cual podemos afirmar que dichos caracteres surgen de manifiesto con motivo de la pandemia de COVID-19 y la respuesta inmediata a los fines de atenuar su impacto.

La Organización de Aviación Civil Internacional (OACI)[16], en este contexto, ha realizado diversas actividades, que seguidamente se detallarán, muchas de ellas en cooperación con otros órganos de Naciones Unidas, en el caso en análisis, preponderantemente con la OMS, para atenuar los efectos de los contagios del COVID-19. Se estableció así una sinergia en cuestiones de cooperación, comunicación de datos respecto de cuestiones sanitarias, estudios o prácticas de la actividad —incluidos los procesos de suspensión de

[16] Respecto de la Organización de Aviación Civil Internacional (OACI) y en un sentido eminentemente práctico, podemos sostener que actúa de foro mundial para los Estados; mediante grupos expertos, equipos especiales, desarrolla políticas y normas, realiza auditorías de cumplimiento, brinda asistencia y crea capacidad de aviación a través de muchas otras actividades, con la cooperación de los Estados miembros y partes interesadas, para lograr el crecimiento sostenible del sistema de aviación civil mundial. Presenta ante los gobiernos los mejores resultados y asesoramiento posibles para que sean ellos quienes, en un proceso colectivo y diplomático, establezcan las nuevas normas y métodos recomendados para la aviación civil internacional. Aprobados por consenso diplomático el alcance y los detalles de una nueva norma, es adoptada por los mismos países, que, de esta forma, armonizan mundialmente sus reglamentos nacionales para contribuir a la seguridad y sostenibilidad de las operaciones aéreas con un alcance y efecto verdaderamente mundial.

actividades, como se mencionó en el punto anterior para nuestro país— que, como bien nos señala Marina Donato:

> Toda adopción de medidas como, por ejemplo, la suspensión de servicios aéreos, debe realizarse previa consulta con la OMS y las autoridades de salud del Estado donde se produce la emergencia, o el origen de la misma, y teniendo en consideración que se trata de casos de excepcional alcance. Las medidas restrictivas siempre en línea con lo dispuesto por la OMS, deben basarse en determinados principios tales como la disponibilidad de evidencia científica del riesgo a la salud o bien cuando tal deficiencia resulta insuficiente, la disponibilidad de información proporcionada por la OMS o bien otro relevante organismo intergubernamental… (Donato, 2020: p. 5)

Ahora bien, indicada la forma de acción mancomunada entre los diversos organismos de Naciones Unidas para el tratamiento de la pandemia, seguidamente se analizarán en particular las acciones específicas que ha desarrollado la OACI en esta etapa de pandemia.

El primer punto que tratar resulta ser la *gestión de riesgos de seguridad operacional de la aviación relacionada con la COVID-19 para las autoridades de aviación civil* (CAA, por sus siglas en inglés), por cuanto, como fuera expuesto a lo largo de este artículo, a causa de esta situación excepcional y de las restricciones de movimiento en general que se impusieron a nivel internacional, analizada la cuestión aeronáutica y en consenso con la OACI, se establecieron reducciones temporales a los estándares de los Anexos al convenio, Anexo I capítulo 1, Anexo 6 capitulo 3, 7 y 9, con su correlación con las RAAC 61, 63, 64, 65, 67, 91, 121, 135, 141, 142, 147.

En este orden de ideas y estando estrictamente vinculado a la seguridad de la navegación aérea, que se traduce en las adecuadas gestiones de toda operación aérea, de manera de detectar debilidades y poner barreras para reforzar las operaciones, se desarrolló —publicación mediante— el Manual para las Autoridades de la Aviación Civil (en el caso de nuestro país, la ANAC arriba descripta) sobre la gestión de los riesgos de seguridad operacional de la aviación relacionados con COVID-19 (Doc. OACI 10.144, de fecha 11/5/2020), conformando los expertos el Panel de Gestión de la Seguridad Operacional de la OACI.

Los Estados pueden aplicar la guía según sus niveles de implementación del Programa Estatal de Seguridad Operacional (SSP, por sus siglas en inglés), apoyándose en ejemplos prácticos y herramientas que allí se plasman, de manera tal de poder brindar la información con la mayor claridad posible. Teniendo en cuenta la excepcionalidad que provoca la pandemia (la «nueva normalidad», como suele decirse), los documentos OACI siempre se hicieron conocidos mediante la publicación de un documento adecuado; en este caso, el Doc. OACI 10.144 fue presentado en un seminario web (en fecha 14/5/2020) donde los participantes podían formular preguntas en la forma que permitiera la plataforma. En el futuro, habrá que observar si estos cambios son momentáneos o definitivos por cuanto, prácticamente desde la pandemia de COVID-19, todos los documentos e informes se publicitan mediante plataformas informáticas «al estilo tutorial» y se genera ese *feedback*

de contenido, impensado en años anteriores cuando se estaba a la espera de la información mediante el documento impreso o escrito.

Continuando con el análisis de este documento, se están identificando y desarrollando informaciones prácticas y herramientas para complementar el Manual; se ha desarrollado un formulario digital vía web para facilitar la recopilación de toda la información. El mencionado formulario se encuentra a disposición —puede descargarse— en la nueva página web dedicada a COVID-19 Safety Risk Management en el sitio Safety Management Implementation (SMI) (icao.int/SMI-COVID19SRM).

Por otro lado, la OACI además propuso un plan de trabajo que implicó la implementación y coordinación de todos los cambios, y procedió a realizar las publicación del caso haciendo uso de la herramienta que puso a disposición de los Estados: el CCRD[17] (COVID-19 Contingency Related Differences, concepto sobre el cual volveremos); se trata de un subsistema creado que complementa el sistema existente de presentación electrónica de diferencias (EFOD) para capturar cualquier discrepancia con las normas de la OACI sobre certificación y concesión de licencias que puedan surgir de las medidas de mitigación debido a la pandemia de COVID-19. Este sistema y los lineamientos para subir la información fueron notificados por la OACI mediante la carta a los Estados AN 11/55-20/50.

Como medidas provisionales para apoyar las operaciones continuas durante las etapas iniciales de la pandemia, a nivel nacional algunas actividades, como el trabajo aéreo o servicio de transporte aéreo en forma muy reducida o local, continuaron prestando servicios con las restricciones que efectivamente dispusieran las autoridades sanitarias.

Entendiendo que estas reducciones no pueden mantener operaciones seguras de forma indefinida, ya que el uso continuo de atenuaciones diluye décadas de experiencia en aviación, incluso con mitigaciones implementadas y con el avance de la situación pandémica, se publicaron para implementación de estos alivios unas Guías de Referencia Rápida (Quick Reference Guides18 [QRG]) para estandarizar su aplicación.

En este contexto excepcional, OACI sostiene y propone que tales alivios se deben retirar lentamente y deben ser reemplazados por herramientas de planificación, enfoques y orientación para la reanudación de operaciones de acuerdo con los requisitos de los SARPS.

Esta aseveración de OACI refiere al impacto que genera esta diminución o casi parálisis de la actividad aérea en el personal aeronáutico y en los equipos, esto se explica abordando

[17] Diferencias relacionadas con contingencias de COVID-19 (CCRD).

[18] Las Guías de referencia rápida (QRG) fueron desarrolladas por la OACI, con el apoyo de expertos en la materia, para brindar orientación sobre un área temática en particular al abordar los riesgos relacionados con COVID-19 para la continuidad de los negocios y las operaciones por parte de los Estados; consideran atenuaciones, al tiempo que se garantizan que también se aborden los riesgos de seguridad introducidos por cualquier cambio que estas atenuaciones pudieran producir por diferencia temporal. Las QRG se han agrupado según áreas operativas específicas y se presentan en la web de OACI para que cualquier Estado pueda descargarlas y utilizarlas como orientación cuando desarrolle atenuaciones específicas en su propio reglamento.

la temática de seguridad operacional y factores humanos (SegOp y FF. HH.19). Si bien no se pretende en el presente artículo hacer un estudio de factores humanos, este concepto se considera fundamental para comprender por qué y cómo las habilidades o desempeño humanos se ven afectados tanto por el exceso como por la falta de operación y práctica; y con relación a las aeronaves.

Como otra herramienta para acompañar a los Estados a fin de compartir experiencias ganadas —teniendo presente que algunos países no paralizaron la actividad como el nuestro— o promover la estandarización temporal, la OACI desarrolló una serie de Seminarios Web COVID-19, donde presenta actualizaciones e información sobre las diversas formas en que el organismo está apoyando, actualmente, a la comunidad de la aviación civil durante la crisis pandémica. La información es completamente gratuita y está a cargo de destacados expertos internacionales en cada una de las especialidades; es de fácil acceso desde la página web de la OACI (www.icao.int).

Además de las descripciones de las actividades desplegadas por la OACI en el marco de la pandemia, ha cobrado notoriedad un plan que la organización hace tiempo ha puesto a disposición de los Estados en la plataforma web: es el denominado *iPack*, donde se proponen algunas herramientas informáticas para tratar temas específicos; tiene también un módulo dedicado a la gestión de riesgos de seguridad operacional de la aviación relacionada con COVID-19 para las autoridades de aviación civil (CAA). Este paquete de implementación (de ahí si denominación *iPack)* fue pensado con el propósito de apoyar, facilitar y guiar a las CAA en la aplicación de los principios de gestión de riesgos de seguridad operacional para mejorar la toma de decisiones en cuanto a los desafíos planteados por la COVID-19 y respaldar operaciones de aeronaves seguras. El *iPack* comprende material de orientación estandarizado, capacitación, herramientas y apoyo de expertos en formato *online* que tiene como objetivo facilitar y guiar la implementación de las disposiciones de la OACI para las entidades estatales. La OACI organizó el primer seminario web el 5 de agosto de 2020 para presentar el *iPack* y sus contenidos.

En el afán de lograr el acceso a los contenidos disponibles para todos los Estados, al momento de escribir estas líneas, se están desarrollando cursos virtuales de un día de duración sobre «Gestión de Riesgos de Seguridad Operacional de la Aviación», relacionados únicamente al tema COVID-19 para las CAA.

---

[19] En un sistema donde interactúan el hombre y la tecnología, el error debe ser entendido como parte normal en esa interacción. En el estudio de los factores humanos, se desarrolló un modelo que se conoce como «el modelo SHELL», que describe las múltiples interacciones en un sistema y entre sus elementos, donde se hace hincapié en el ser humano y en las interfaces humanas con otros componentes del sistema de aviación, aeronaves, aeropuertos, espacio aéreo, procedimientos, personal aeronáutico. El modelo SHELL, desarrollado por primera vez por Elwyn Edwards (1972) y luego modificado en una estructura de «bloques de construcción» por Frank Hawkins (1984), lleva el nombre de las letras iniciales de sus componentes en inglés y se representa lo siguiente: *Software*: recursos no materiales relevantes para la operación; reglamentación, manuales, procedimientos, listas de chequeo, sistemas de señalización, etc. *Hardware*: estructura física del ámbito de trabajo; equipos, herramientas y maquinarias. *Environment*: condiciones internas y externas del entorno de trabajo. Liveware: otras personas con las que interactúo en mi lugar de trabajo. *Liveware* (central): la persona.

Con relación a la temática que trata la medicina de aviación (MED), se cuenta con el *Manual de Medicina Aeronáutica Civil* (Doc. OACI 8984). Los SARPS relativos a las disposiciones médicas sobre requisitos de aptitud física de los titulares de licencias figuran en el Anexo 1, y los relativos a la prevención y gestión de enfermedades transmisibles se desarrollan a través del programa «Arreglo Colaborativo para la Prevención y Gestión de eventos de salud pública en la Aviación Civil» (CAPSCA, por sus siglas en inglés), contenidos en los Anexos 6, 9, 11, 14, 18 de la OACI y los PANSATM. El CAPSCA trabaja en la elaboración de SARPS apropiados y material de orientación para facilitar y armonizar la planificación de eventos de salud pública que afectan la aviación, como enfermedades transmisibles graves, accidentes radionucleares y químicos.

Ahora bien, referidas las principales funciones que cumple la OACI en este régimen excepcional de pandemia, suele darse la situación de diferencias reglamentarias entre los diversos Estados parte, lo que genera la necesidad de gestionar esta situación de manera tal de proveer información y conocimientos necesarios para todos, dados los avances que se obtienen, como fuera antes referido.

A fin de garantizar las operaciones y poder lidiar con estos inconvenientes a nivel mundial, y en consenso con OACI, los estados establecieron reducciones temporales a los estándares de los Anexos. Ello generó diferencias en lo que a cumplimiento de estándares se refiere; además, de acuerdo a lo previsto, tales diferencias deben ser informadas a la OACI para conocimiento y publicación.

Siendo este el caso de las diferencias relacionadas con contingencias de COVID-19 (CCRD por sus siglas en inglés), la OACI remitió a los Estados contratantes la carta estatal AN 11/55-20/50, donde informa la creación de un subsistema CCRD en el sistema existente de presentación electrónica de diferencias (EFOD) para capturar cualquier discrepancia con las normas de la OACI sobre certificación y concesión de licencias que puedan surgir de las medidas de mitigación debido a la pandemia de COVID-19.

Los estándares a informar en el CCRD se han clasificado como «básicos» y «ampliados». El CCRD básico contiene estándares originales identificados para capturar cualquier diferencia con los estándares de la OACI sobre certificación y concesión de licencias. El CCRD ampliado contiene normas adicionales, según lo soliciten los Estados, para capturar cualquier otra diferencia con las normas de la OACI.

El CCRD del sistema EFOD permitirá a los Estados presentar una diferencia temporal y, al mismo tiempo, indicar lo que considerarían aceptable para facilitar las operaciones internacionales y cumplir con las obligaciones del Artículo 40 del Convenio para Normas Específicas. Así quedan notificadas y publicadas todas las medidas provisionales que apoyan las operaciones continuas durante las etapas iniciales de la pandemia de COVID-19.

En este proceso de evolución y avance del tratamiento de la pandemia y pensando en una pronta reactivación del sistema mundial de aviación civil, se conformó el Equipo Especial para la Recuperación de la Aviación (en inglés: Council's Aviation Recovery Task Force [CART]), que desarrolló un documento titulado: *El despegue: Orientaciones para el transporte aéreo durante la crisis sanitaria causada por la COVID-19*. Este documento

proporciona un marco de acción para hacer frente al impacto de la pandemia de COVID-19 actualmente en curso en el sistema mundial de transporte aéreo. El apéndice contiene las medidas de mitigación necesarias para reducir el riesgo sanitario para el público usuario de la aviación y su personal, con el fin de fortalecer, de esa manera, la confianza del público viajero, la cadena mundial de suministros y los gobiernos.

Se espera que tales medidas contribuyan a acelerar la demanda de transporte aéreo esencial y no esencial, que se ha visto afectada por la COVID-19. Con la ayuda y orientación de la comunidad de aviación civil, la OACI recomienda avanzar gradualmente para permitir que la industria recupere sus altos volúmenes de público usuario y carga en los servicios de cabotaje e internacionales en condiciones seguras. Este enfoque propone una serie de medidas centrales para conformar un protocolo básico de seguridad sanitaria en la aviación dirigido a proteger al público usuario y al personal del área frente a la COVID-19.

5. Conclusiones finales

El impacto en el transporte aéreo mundial de la pandemia de COVID-19, sin lugar a dudas, no tiene precedentes; generó un estado de incertidumbre inicial que implicó que tanto las autoridades nacionales e internacionales suspendieran inmediatamente el tráfico aéreo hasta tanto avanzaran los conocimientos médicos sobre el tratamiento de esta enfermedad.

Paulatinamente, fueron autorizándose algunas actividades, ya sea por la necesidad o por la declaración de su carácter «esencial o necesario» (el trabajo aéreo, vuelos sanitarios, el mantenimiento de aeronaves, fabricación, mantenimiento de repuestos o elementos para aeronaves, etc.), hasta llegar al día de hoy, cuando se permiten algunos vuelos de cabotaje, dejando librado la autorización a una suerte de acuerdo entre autoridades provinciales, nacionales y sanitarias en conjunto.

Es por ello por lo que no llama la atención los diversos cambios en las autorizaciones efectuadas por los organismos competentes por cuanto destinos autorizados para el tráfico aéreo en momentos en que en otras zonas se encontraba vedadas debieron restringirse —en algunos casos prácticamente con el incurrimiento de prohibiciones—, atento al aumento de las tasas de contagio de la enfermedad, tomando en consideración la cantidad de habitantes del territorio.

Esta inestabilidad de la situación epidemiológica, cambios constantes de conocimientos y gestión sanitaria determinó el dictado de normas de excepción a nivel nacional —las que fueron desarrolladas exhaustivamente—. Dichas disposiciones no emanaban únicamente de las autoridades aeronáuticas, sino de un trabajo consensuado con otros organismos estatales —especialmente los sanitarios— a fin de reglamentar, así, la actividad en esta denominada «nueva normalidad».

El modelo de gestión de la pandemia y la actividad aeronáutica a nivel nacional reflejan la acción internacional llevada a cabo por la OACI —también descripta sucintamente para no incurrir en excesivos tecnicismos—. Se observa, sin embargo, el cambio en la actuación de este organismo internacional para llegar de manera inmediata con las recomendaciones y los conocimientos de todos los sucesos que ocurren en los Estados parte.

De más está decir que la actividad en general ha sufrido pérdidas millonarias en toda su cadena de desarrollo, como ser en los aeropuertos, con una disminución del tráfico de pasajeros en el primer trimestre de 2020 cerca del 28,4%, por citar algún dato estadístico que se replica en todas las intervenciones de la actividad[20].

En este estadio, será fundamental la capacidad de adaptación de todos los actores y los órganos nacionales e internacionales especializados en la actividad aeronáutica para enfrentar los efectos en el periodo pospandemia y lograr que, en estas nuevas condiciones, se encausen nuevamente las proyecciones de expansión de la actividad aeronáutica en el futuro, como estábamos acostumbrados.

6. Bibliografía

Balián, E. N. (2011). Aspectos jurídicos del transporte aéreo «low cost». *Revista Ateneo del Transporte*, Nro. 56, 14-32.

Donato, M. (2020). La labor de la OACI ante la pandemia del COVID-19. *Revista Latino Americana de Derecho Aeronáutico*, Nro. 54, 1-12.

IATA (2019). Comunicado 45. Mayor conectividad y eficiencia- Estadística del transporte aéreo mundial 2018. Disponible en https://www.iata.org/contentassets/f8d2fbbfe2664612a1e4e65a22422dc3/2019-07-31-01-sp.pdf

Foglia, R. A. y Mercado, A. R. (1976). *Derecho Aeronáutico*. Buenos Aires, Argentina: Ed. Abeledo Perrot.

Lombardo, V. A. (2020). La aeronáutica y la salud. Una nueva perspectiva. *Revista Latino Americana de Derecho Aeronáutico*, Nro. 55, 1-13.

Lena Paz, J. A. (1987). *Compendio de Derecho Aeronáutico*, 5.a ed, Buenos Aires, Argentina: Ed. Plus Ultra.

Pratto Chiarella, H. M. (2020). Las aerolíneas y el COVID-19. Su reorganización a la luz del Capítulo 11 de la Ley de Quiebras de los Estados Unidos de América y alternativas de salvataje. *Revista Latino Americana de Derecho Aeronáutico*, Nro. 57, 1-4.

[20] Las primeras previsiones apuntan a que los volúmenes de tráfico (interior e internacional) cierren el año 2020 con un retroceso del 50,4 % respecto de las cifras de 2019. La OACI estima que, por efecto de la COVID-19, para el final de 2020 se contabilizarán reducciones que podrían llegar al 71% en capacidad (asientos) y 1500 millones de pasajeros en todo el mundo. Líneas aéreas y aeropuertos prevén que las pérdidas de ingresos en 2020 alcancen los USD 314 000 millones y USD 100000 millones, respectivamente.

Videla Escalada, F. N. (1978). *Manual de Derecho Aeronáutico.* Buenos Aires, Argentina: Ed. Zavalia Editor.

7. Legislación

Administración Nacional de la Aviación Civil: Comité de Crisis Prevención COVID-19 en el Transporte Aéreo – Creación: Resolución 99/2020. Publicada en el Boletín Oficial n. 34.332 el 18-mar-2020, p. 8.

Administración Nacional de la Aviación Civil: Dispensa restricción impuesta por el Decreto 260/2020. Resolución 100/2020. Publicada en el Boletín Oficial el 19-mar-2020, p. 1.

Administración Nacional de la Aviación Civil: Prorroga de certificaciones y habilitaciones aeronáuticas. Resolución 101/2020. Publicada en el Boletín Oficial n.º 34.335 el 21-mar-2020, p. 9.

Administración Nacional de la Aviación Civil: Comercialización de servicios regulares de transporte aéreo. Resolución 143/2020. Publicada en el Boletín Oficial n.º 34.366 el 27-abr-2020, p. 27.

Administración Nacional de la Aviación Civil: Autorización de Transporte de pasajeros. Resolución 144/2020. Publicada en el Boletín Oficial n.º 34.366 el 27-abr-2020, p. 30.

Administración Nacional de la Aviación Civil: Exclusión del ámbito de aplicación de la normativa excepcional a las empresas de Trabajo Aéreo que realicen la especialidad Agroaéreo. Resolución 205/2020. Publicada en el Boletín Oficial n.º 34.433 el 24-jul-2020, p. 9.

Administración Nacional de la Aviación Civil: Modificación Resolución 100/2020. Resolución 304/2020. Publicada en el Boletín Oficial n.º 34.498 el 16-oct-2020, p. 13.

Administración Nacional de la Aviación Civil: Aprobación de los requisitos a cumplimentar por las Empresas de Transporte Aéreo no Regular y bajo las reglas de vuelo y operación genera para obtener autorización para realizar operaciones que tengan origen o destino puntos situados fuera del Territorio Nacional. Resolución 305/2020. Publicada en el Boletín Oficial n.º 34.503 el 22-oct-2020, p. 18.

Congreso de la Nación Argentina: Ley de Solidaridad Social y Reactivación Productiva. Ley N.º 27541. Publicada en el Boletín Oficial n.º 34268 el 23-dic-2019, p. 1.

Jefatura de Gabinete: Ampliación Listado de actividades y servicios exceptuados en el art. 6 del Decreto 297/2020 y sus normas complementarias, en todo el Territorio Nacional, con excepción del AMBA. Decisión Administrativa 810/2020. Publicada en el Boletín Oficial n.º 34.382 el 16-may-2020, p. 13.

Ministerio de Transporte: Servicio de Transporte – Cantidad de Pasajeros: Resolución 64/2020. Publicada en el Boletín Oficial n.º 34.332 el 18-mar-2020, p. 4.

Ministerio de Transporte: Esquemas para la prestación de servicios: Resolución 71/2020. Publicada en el Boletín Oficial n.º 34.334 el 20-mar-2020, p. 4.

Ministerio de Transporte: Modificación art. 1 de la Resolución 71/2020: Resolución 73/2020. Publicada en el Boletín Oficial n.º 34.338 el 25-mar-2020, p. 19.

Ministerio de Transporte: Modificación de la Resolución 64/2020: Resolución 221/2020. Publicada en el Boletín Oficial n.º 34.497 el 15-oct-2020, p. 21.

Poder Ejecutivo Nacional: Administración Nacional de la Aviación Civil – Creación. Decreto 239/2007. Publicada en el Boletín Oficial n.º 31.118 el 19-mar-2007, p. 1.

Poder Ejecutivo Nacional: Emergencia Sanitaria (Coronavirus) COVID-19 Disposiciones. Decreto 260/2020. Publicada en el Boletín Oficial n.º 34.327 el 12-mar-2020, p. 1.

Poder Ejecutivo Nacional: Prohibición de ingreso al Territorio Nacional. Decreto 274/2020. Publicada en el Boletín Oficial n.º 34.330 el 16-mar-2020.

DOSSIER:
DERECHO, TECNOLOGÍAS Y PANDEMIA

Tengo el honor de presentarles este dossier especial sobre "Derecho, tecnologías y pandemia", fruto de un arduo trabajo realizado durante estos meses de confinamiento, que implicó un desafío conjunto entre docentes de distintas universidades. El logro obtenido, nos reconforta y esperamos sea de vuestro agrado.

Confiamos en que la temática propuesta concitará vuestro interés, teniendo en cuenta que la nueva normalidad ha demostrado hasta qué punto el mundo digital ya forma parte de nuestra vida cotidiana.

El Derecho no puede permanecer al margen de estos cambios.

Teniendo en cuenta que todos somos por igual ciudadanos del mundo digital, hemos pensado este Dossier, sujeto a referato, con el aporte de producciones de destacados docentes de diferentes nacionalidades: así podrán encontrar artículos de los Profesores españoles Luis López Lema –de la Universidad de Valencia– y Lucana Estevez –de la San Pablo SEU de Madrid–, así como también de Profesores locales, Mauro F. Leturia, Adrián E. Gochicoa Victoria Antonella Mongelos, Facundo Cerdá –de la Universidad Nacional de La Plata–, y Mariano Refi en conjunto con quien escribe estas líneas –ambos docentes de esta alta Casa de Estudios–. Confiamos que los artículos seleccionados abordan temas de indudable vigencia e interés, y les permitirán profundizar en sus conocimientos, incentivando la reflexión, y el debate.

Me permito unas últimas palabras. La magnitud de este aporte hubiera sido imposible sin la participación de varios actores. Mi más sincero agradecimiento a quienes contribuyeron a este feliz término.

Joselina Pastorini
Profesora de Derecho Penal
UCALP

La gestión de la información durante etapas de teletrabajo en la época de la COVID-19

Luis López Lema

Licenciado en Derecho por la Universidad de Valencia. Magister en Sistemas y Servicios en la Sociedad de la Información por la Universidad de Valencia. Delegado de protección de datos por el IVAC-INSTITUTO DE CERTIFICACIÓN S.L. Consultor de Nuevas Leyes y Tecnología, S.L. (LEYNET CONSULTORES). Docente de la Universidad Internacional de Valencia y de la Universidad de Florida de Valencia.

Resumen

La aparición de la COVID-19 ha cambiado nuestras vidas, desde los hábitos de higiene, las interacciones sociales y hasta la forma de trabajar dentro de las organizaciones. El nuevo cambio de paradigma ha obligado a la mayoría de las organizaciones a implantar sistemas de teletrabajo para poder tener continuidad de negocio durante los periodos de confinamiento. Ello ha generado nuevos estilos de trabajo, nuevos problemas de ciberseguridad, y, por tanto, cualquier organización debe replantearse tanto sus sistemas de información como las medidas de seguridad que venían aplicando para reducir los riesgos cibernéticos derivados del trabajo en remoto.

Palabras clave: Ciberseguridad, COVID-19, Teletrabajo, Privacidad, Protección de Datos.

Abstract

The emergence of COVID-19 has changed our lives, from the hygiene habits, social interactions, and even the way of working within organizations. The new paradigm shift has forced most organizations to implement teleworking systems in order to have business continuity during periods of confinement. This has generated new work styles, new cybersecurity problems, and therefore any organization must rethink both its information systems and the security measures that have been applied to reduce the cyber risks derived from remote work.

Keywords: Cibersecurity, COVID-19, Remote Work, Privacy, Data Protection.

1. Binomio formado por la información y la seguridad

La información es un activo vital que, como otros activos comerciales importantes y estratégicos, es esencial para el negocio de una organización y, en consecuencia, necesita ser protegido adecuadamente. En la Figura 1, se muestra de forma gráfica cómo un dato se convierte en un elemento de valor dentro de cualquier organización, tanto a nivel privado como público.

Figura 1. Cadena de valor de la información.

Fuente: elaboración propia.

Según la norma UNE ISO 27002 (2017) «La información es un activo que, al igual que otros activos del negocio, es esencial para la organización, y por lo tanto debe ser protegido de forma adecuada». (p. 9).

Por ello, es vital garantizar su seguridad, pero lograrla no es tarea fácil. Spafford (citado en Dewdney 1989), profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que:

> El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él. (p. 110)

En general, en la actualidad, podemos entender que un sistema de información es seguro si podemos garantizar los tres pilares que se muestran en la Figura 2:

Figura 2. Pilares de la seguridad.

Fuente: Observatorio Tecnológico (2012).

La confidencialidad, la integridad y disponibilidad son los principales pilares de la seguridad porque ayudan a sacarle el máximo rendimiento de la información con el mínimo riesgo. Si alguno de estos pilares se debilita, se perderá seguridad, y, por tanto, la organización queda expuesta a ataques. Para comprender el alcance de cada uno de estos pilares, se debe conocer en detalle cuál es su función:

a) Confidencialidad: hace referencia a la necesidad de mantener el secreto de determinada información o recursos. Su objetivo es prevenir la divulgación no autorizada de la información.

Para garantizar la confidencialidad se pueden implementar, principalmente, las siguientes medidas técnicas:

- Sistemas de autenticación de usuarios
- Gestión de privilegios
- Sistemas de cifrado y encriptación

b) Integridad: hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es prevenir modificaciones no autorizadas de la información; por ende, la integridad abarca tanto la propia información como su origen. Es importante hacer hincapié en la integridad del origen, ya que puede afectar su exactitud, su credibilidad y la confianza que las personas ponen en la información.

Para garantizar la integridad, se deben considerar las siguientes actividades:

- Sistemas de monitorización del tráfico de red para descubrir posibles intrusiones
- Sistemas de control de registros
- Sistemas de control de cambios

c) Disponibilidad**:** hace referencia a la accesibilidad del sistema y de los recursos del sistema de información. El objetivo de la disponibilidad es prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

Para garantizar la disponibilidad, se pueden implementan las siguientes medidas:

- Firmar un acuerdo de nivel de servicio (o SLA por su acrónimo en inglés: *Service Level Agreement*).
- Balanceadores de carga.
- Sistemas de copias de seguridad.
- Disponer de recursos alternativos a los primarios.

Toda organización debe mantener el equilibrio entre estos tres pilares, debiendo ponderar las medidas de seguridad para que se consigan los tres sin que alguno de ellos sufra. Por ejemplo, no tiene sentido conseguir la confidencialidad a toda costa para un

archivo si después ni siquiera el usuario administrador puede acceder a él, ya que, en ese caso, se está negando la disponibilidad.

La propia UNE ISO 27002 (2017) determina que existen tres fuentes donde obtener los requisitos de seguridad que nos ayuden a velar por la integridad de estos tres pilares:

- Primera fuente: es el análisis de riesgo realizado por la propia organización. Como veremos en el capítulo siguiente, a través de una evaluación interna, se podrán averiguar las amenazas y su probabilidad de materialización, lo que ayudará a identificar las medidas de seguridad idóneas.
- Segunda fuente: es el cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales a los que la organización se encuentre sometida. Por ejemplo, la normativa de protección de datos de carácter personal, que se explicará más adelante.
- Tercera fuente: son los propios objetivos y requisitos del negocio que la organización se ha establecido como necesarios para dar soporte al tratamiento de la información. Es decir, las medidas internas que la organización se haya autoimpuesto.

1.1. Aproximación al concepto de seguridad de la información

Antes de la aparición de la COVID-19 en nuestras vidas, la tecnología ya había transformado nuestro día a día. De hecho, nadie concibe un día sin enviar un correo electrónico, conectarse a una red social, escuchar música o ver una serie a través de plataformas en línea. Y, por otra parte, en el mundo de la empresa, no se podría trabajar sin transacciones electrónicas o la utilización de servicios *cloud* para reducir costes y mejorar la productividad. Pero, indistintamente de un uso corporativo o personal, la utilización de la tecnología lleva aparejado un uso responsable y seguro de ella.

Voutssas Marquez (2010) expone que, para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen. Se relacionan a continuación:

- Recursos informáticos: el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como «activos informáticos».
- Amenaza: fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización.
- Impacto: la medida del efecto nocivo de un evento.
- Vulnerabilidad: característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.

- Riesgo: la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.
- Principio básico de la seguridad informática: la seguridad informática no es un producto, es un proceso.

La seguridad informática se encarga de la seguridad del medio informático. Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y, sobre todo, que tenga disponibilidad. La seguridad de la información no se preocupa solo por el medio informático, se preocupa por todo aquello que pueda contener información, por ejemplo, todos los soportes físicos.

Actualmente, la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y, en muchos casos, más complejo de manejar, ya que los procesos, en ocasiones, no son tan visibles para los involucrados.

La principal tarea de la seguridad informática es la de minimizar los riesgos, que, en este caso, provienen de muchas partes: puede ser de la entrada de datos, del medio que transporta la información, del *hardware* que es usado para transmitir y recibir, de los mismos usuarios y hasta de los protocolos que se están implementando; pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes:

- Usuarios: considerados el eslabón más débil de la cadena, ya que las personas pueden cometer un error y olvidar algo o tener un accidente, y este suceso puede comprometer la información y que terceros puedan acceder a ella.
- Información: compuesta por la interpretación de todos los datos introducidos en el sistema, es el principal objetivo de la seguridad informática, ya que es lo que se desea proteger y lo que tiene que estar a salvo; en otras palabras, se dice que es el principal activo.
- Infraestructura: entendiéndose como todos los recursos necesarios para albergar, tratar y transmitir la información; puede ser uno de los medios más controlados para segurizar todos los procesos.

Y es en este punto donde los proveedores de servicios y tecnología relacionados con la ciberseguridad están cambiando las prioridades para respaldar las necesidades actuales: continuidad del negocio, trabajo remoto y planificación para la transición a la siguiente normalidad.

1.2 Los elementos vulnerables de un sistema de información

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que, no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de niveles de seguridad, ya que la seguridad absoluta no es posible. En adelante, entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener niveles altos de seguridad.

La seguridad es un problema integral; los problemas de seguridad informática no pueden ser tratados aisladamente, ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo. Por otra parte, existe algo que los *hackers* llaman *ingeniería asociada*, que consiste simplemente en conseguir, mediante un engaño, que los usuarios autorizados revelen sus contraseñas. Por lo tanto, la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

En vista de estas manifestaciones, hay tres elementos principales que proteger en cualquier sistema informático: el *software*, el *hardware* y los datos.

- Por *hardware* entendemos el conjunto de todos los elementos físicos de un sistema informático, como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc.
- Por *software* entendemos el conjunto de programas lógicos que hacen funcionar el *hardware*, tanto sistemas operativos como aplicaciones.
- Por datos, el conjunto de información lógica que maneja el *software* y el hardware, por ejemplo, paquetes que circulan por un cable de red o entradas de una base de datos.

Por ende, y en conclusión, tenemos que ser conscientes de que las medidas de seguridad que deberán establecerse en cualquier sistema de información comprenderán y tendrán repercusión sobre el *hardware*, el sistema operativo, las comunicaciones y los soportes físicos.

2. Riesgos en la seguridad de la información

Debemos entender como riesgo cualquier posibilidad de que se materialice una amenaza o situación que provoque un ataque a los sistemas de información y produzca el quebrantamiento de alguno de los pilares comentados anteriormente.

Según Voutssas Marquez (2010), el riesgo es la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto perjudicial en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto.

La dependencia informática tan fuerte a la que las organizaciones se encuentran sometidas, junto con la inexorable evolución de las telecomunicaciones para interactuar en Internet y compartir información, ya había cambiado el paradigma de la seguridad y la expectativa de privacidad de la información de las organizaciones, pero, a raíz de la aparición de la COVID-19, dicho paradigma se ha visto incrementado.

La pandemia no solo ha supuesto un riesgo y peligro para la salud de los humanos, sino que también resulta un riesgo para la seguridad de los sistemas informáticos, ya que han aumento los ataques de *phishing*, *malspams* y de *ransomware,* utilizando precisamente el reclamo de la COVID-19 como cebo para hacerse pasar por marcas de productos de protección individual frente al virus a fin de infectar el terminal.

También las aplicaciones relacionadas con ayuda sobre la COVID-19, o incluso las mismas aplicaciones gubernamentales publicadas para controlar a nivel nacional el virus, están siendo suplantadas para infectar de *ransomware* a los usuarios.

Y es que, con el solo hecho de abrir un correo electrónico o realizar una transacción en línea, podemos poner en riesgo la seguridad corporativa de toda la organización. Por ello, todo usuario debe concienciarse sobre la importancia de la seguridad informática, ya que el factor humano es el eslabón más débil en lo que respecta la integridad de la información.

2.1. La incidencia de la COVID-19 en la seguridad de la información

La estimación de Cybersecurity Ventures en su informe de 2020 establece que los costes de daños por delitos cibernéticos podrían potencialmente duplicarse durante el período del brote de coronavirus y no solo por las estafas de *phishing*, sino también por los ataques de *ransomware*, debido al acceso remoto inseguro a las redes corporativas, por la falta de formación de los trabajadores remotos que exponen las credenciales de inicio de sesión de sus terminales con el resto de miembros de su núcleo familiar, así como por la utilización de los equipos informáticos por parte de todos los miembros de su núcleo familiar y, por ello, comprometer los archivos e informaciones de la compañía.

Actualmente, las principales situaciones que comprometen la seguridad de la información donde el factor humano es determinante son las siguientes:

a) El trabajo remoto

La COVID-19 ha llevado a que una gran cantidad de empleados en todo el mundo sean enviados a casa para trabajar de forma remota. La gran mayoría de ellos, al trabajar desde fuera de su entorno empresarial o institucional, tienen recursos mínimos de seguridad informática en comparación con los que normalmente tienen a su disposición cuando trabajan en su puesto de trabajo habitual.

Por otra parte, la forma tan repentina y precipitada con las que las organizaciones han optado por el teletrabajo no ha permitido capacitar a los empleados remotos

sobre cómo detectar y reaccionar ante estafas de *phishing* y otros tipos de ataques cibernéticos.

b) Uso incorrecto de la tecnología

Hemos pasado de tener solo el ordenador en el puesto de trabajo dentro de la oficina a llevarlo en el bolsillo y estar constantemente conectados a él. Y es que, aunque no lo parezca, los teléfonos móviles son pequeños ordenadores. Los dispositivos que nos rodean y que se utilizan de forma cotidiana para el desempeño de las tareas empresariales permiten tener la conectividad total de tal forma que, actualmente, se puede estar controlando una empresa desde cualquier parte del mundo sin necesidad de estar conectado en un puesto fijo dentro de una oficina. Pero el uso inadecuado de estas características también puede poner en riesgo nuestra información. Por ejemplo, conectarse a una red wifi no segura puede permitir que terceros accedan al contenido del dispositivo; instalar *software* ilegal puede facilitar un ataque informático; no tener actualizados los sistemas operativos podría derivar en una brecha de seguridad por no tener los últimos parches de seguridad instalados, etc.

Además, la falta de conciencia de seguridad puede implicar también el no realizar copias de respaldo o de seguridad. O realizarlas de forma poco segura, como almacenarla en el propio ordenador, con lo que, al final, si este resultara afectado, la copia de respaldo también quedaría afectada.

En definitiva, ser prudentes con la tecnología y hacer un uso consciente siempre garantizará un nivel de seguridad de la información.

c) Virus, códigos maliciosos y engaños

La información está expuesta constantemente a virus, códigos maliciosos, troyanos, etc., bien porque llegan a través de correo electrónico, por la descarga e instalación de *software* ilegal, por la navegación por sitios poco seguros, por la introducción de dispositivos de almacenamiento externo, etc.

Sin ir más lejos, un troyano se puede autoinstalar en un ordenador gracias a una memoria extraíble USB. Las memorias extraíbles pueden ser útiles, pero también son una gran fuente de contagio, por lo que siempre que sea posible, en una organización, no deberían aceptarse dispositivos ajenos para el traslado de información.

Este tipo de amenazas pueden provocar la pérdida definitiva de la información, su secuestro o incluso que monitoreen la actividad realizada por el usuario para descubrir contraseñas, números de tarjeta de crédito o cualquier otra información sensible para la comisión de alguna actuación cibercriminal.

Gran parte de estas amenazas se pueden evitar o incluso se podrían eliminar a través de un buen *software* antivirus y sistemas de cortafuego. Pero tener un antivirus no

es garantía total de no ser infectado, ya que, dependiendo de las actividades que realicemos, vamos a estar más o menos expuestos ante este tipo de amenazas.

Por ello, y al hilo del punto anterior, hace falta tener un buen criterio analítico a la hora de gestionar el correo electrónico, debiendo evitar descargar archivos adjuntos de correos electrónicos de personas o entidades desconocidas. Pero, sobre todo, asegurarse de que el emisor es quien dice ser, ya que, en muchos casos, se reciben correos electrónicos supuestamente de la entidad bancaria con la única finalidad de engañar al usuario para conocer sus claves personales con fines delictivos.

Sin embargo, no solo se debe tener cuidado con los correos electrónicos, sino también con las redes sociales, ya que, en ocasiones, se puede recibir un mensaje directo de un desconocido, que indique el acceso a un determinado enlace. Ese *link* puede conducir a un portal web infectado con *malware* que termine infectando el ordenador o el teléfono móvil.

Todos los días, Gmail[1] bloquea más de 100 millones de correos electrónicos de *phishing*; ha llegado a detectar 18 millones de correos electrónicos de *phishing* y *malware* diarios relacionados con COVID-19. Esto se suma a más de 240 millones de mensajes de *spam* diarios relacionados con COVID. Ante esta situación, el servicio de correo electrónico de Google ha evolucionado sus sistemas para comprender y filtrar estas amenazas, y, con ello, poder lograr el bloqueo de más del 99,9 % del *spam*, el *phishing* y el *malware* para que no lleguen a sus usuarios.

d) Externalización de gestiones

Las soluciones *cloud computing* han propiciado el desarrollo de plataformas que permiten mejorar el almacenamiento de la información de las organizaciones, bien teniendo más capacidad para guardar información, bien teniendo herramientas que mejoran su tratamiento. A pesar de las potenciales ventajas que supone la tecnología en la nube, es evidente que delegar la gestión de la información en terceros entraña cierto riesgo, puesto que deja de estar bajo la propia gestión.

A veces, en la contratación de estos proveedores, prima más la oferta económica que la seguridad. Por ejemplo, pongamos el caso de servicios de alojamiento de datos, donde, en la mayoría de las situaciones, se puede optar por un servicio gratuito. No debemos dejar de lado el hecho de que muchos de estos proveedores, a cambio de sus servicios, utilizan los datos proporcionados por los propios usuarios para compartirlos con terceros y, de esta forma, ofrecer productos y servicios de acuerdo a sus hábitos.

Además, en la mayoría de las situaciones en las que se contrata este tipo de servicios, no se realiza una lectura detenida de los términos y condiciones publicados en el

[1] https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

portal web del potencial proveedor para conocer de forma detallada cómo se van a manejan los datos y las medidas de seguridad que aplican.

e) Robo, pérdida y extravío de dispositivos

De todas las situaciones descritas anteriormente, esta puede ser la más difícil de controlar, ya que muchas veces dependerá del azar. Por ese mismo motivo, se deben de adoptar medidas preventivas, por ejemplo, un sistema de bloqueo remoto para que ningún tercero pueda ver la información o implantar medidas de rastreo y geolocalización para poder localizar los dispositivos.

2.2 Análisis de vulnerabilidades y metodología

Para la correcta conjugación de los elementos anteriores, se requiere implementar una metodología de análisis de vulnerabilidades con la finalidad de tratar de mitigar o reducir los riesgos detectados dentro de los sistemas de información. Todo ello, bajo un proceso que el INCIBE (2017) —siglas del Instituto Nacional de Ciberseguridad de España— plantea en las fases ilustradas en la Figura 4.

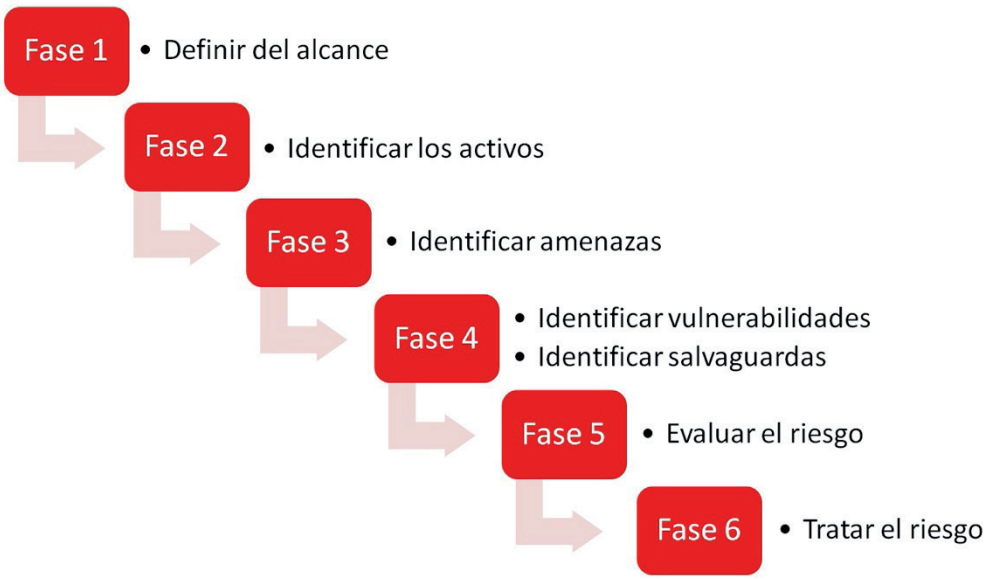


Figura 4. Fases de un sistema de gestión de riesgos.

Fuente: INCIBE (2017).

Fase 1. Concreción de que se quiere analizar

El punto de partida para un correcto análisis de riesgo es saber sobre qué parte de la organización se va a realizar, es decir, si afecta a la seguridad de la información de un determinado departamento, de un determinado proceso, de un sistema en particular, etc.

Fase 2. Identificar los activos

Teniendo claro qué se quiere analizar, se deben identificar los recursos que conforman ese sistema de información que guardan relación con el departamento, proceso o sistema objeto del estudio. Para mantener un inventario de activos sencillo, puede ser suficiente con hacer uso de una hoja de cálculo o tabla, como la que se muestra a continuación en la Figura 5.

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Figura 5. Modelo de inventario de recursos.

Fuente: INCIBE (2017).

Fase 3. Identificación de las amenazas

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Como se puede imaginar, el conjunto de amenazas es amplio y diverso, ya que pueden producirse por diferentes elementos tantos externos como internos de la organización, por lo que se debe realizar un exhaustivo esfuerzo en poder identificar todas las amenazas.

Siguiendo la terminología de la normativa ISO 31000, la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) responde a lo que se denomina *proceso de gestión de los riesgos* y lo implementa dentro de un marco de trabajo para que las organizaciones tomen las decisiones oportunas, teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. De forma ilustrativa, se muestra en la Figura 6 cómo se integra esta metodología dentro del proceso de gestión de riesgos.

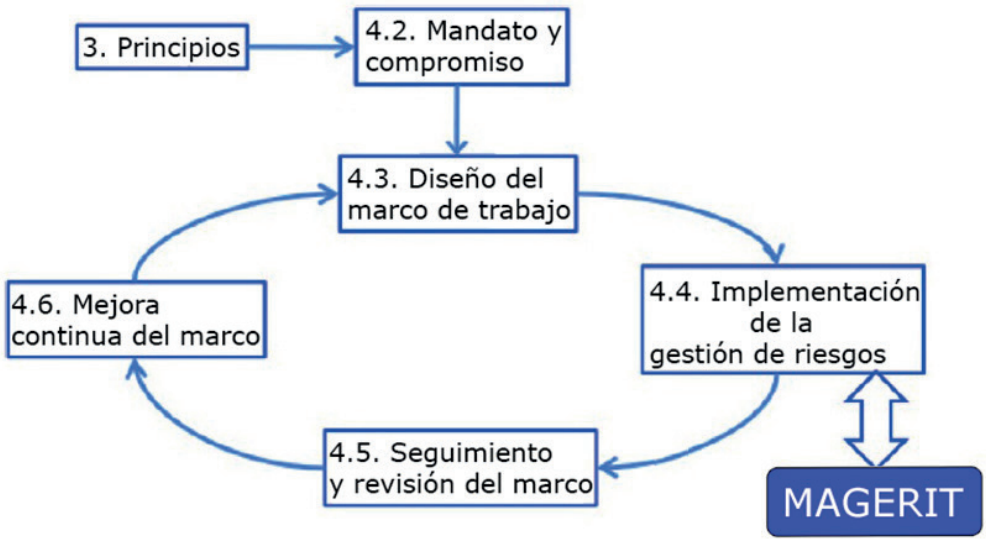


Figura 6. Relación de la metodología MAGERIT en un proceso de gestión de riesgos.

Fuente: adaptado de Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012).

Fase 4. Identificación de las vulnerabilidades

Los recursos inventariados en la primera fase deben ser auditados para identificar sus puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser que los ordenadores no tengan instalados los últimos parches de seguridad o que cuenten con sistemas operativos desactualizados.

Fase 5. Evaluación del riesgo

Con toda la información obtenida hasta el momento, se establecerá la probabilidad de que una amenaza se materialice y el grado de impacto que produciría dentro de la organización. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos, tal como se aprecia en la Figura 7.

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Figura 7. Clasificación cuantitativa y cualitativa de los riesgos.

Fuente: INCIBE (2017).

La elección del criterio cuantitativo o cualitativo definirá el cálculo del riesgo. Cabe destacar que ambos criterios no son excluyentes, sino complementarios. De tal forma que la combinación de ambos criterios aporta mayor valor a la hora de combatir y reducir los riesgos dentro de la organización.

Si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores de probabilidad e impacto, como se refleja en la Figura 8.

PROBABILIDAD * IMPACTO = RIESGO

Figura 8. Cálculo del riesgo bajo el criterio cuantitativo.

Fuente: elaboración propia.

Si, por el contrario, se quiere optar por un análisis cualitativo del riesgo, se deberá elaborar una matriz de riesgo como la que se muestra en la Figura 9.

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Figura 9. Matriz para clasificar el riesgo de forma cualitativa.

Fuente: INCIBE (2017).

Debemos poner en relación las vulnerabilidades detectadas en la anterior fase y relacionarla con esta matriz. Con ello, se podrá estimar la probabilidad y el impacto teniendo en cuenta las salvaguardas con las que cuenta la organización.

Fase 6. Gestión del riesgo

Para gestionar los riesgos seleccionados, existen cuatro estrategias:

- Transferir el riesgo a un tercero: por ejemplo, contratando un proveedor que tenga mejor capacidad técnica que nuestra organización para realizar un proceso, o bien contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.

- Eliminar el riesgo: por ejemplo, eliminando un proceso o el recurso que está expuesto al riesgo.
- Asumir el riesgo: por motivos de negocio, por ejemplo, porque el coste es desproporcionado o el estado de la técnica aún no es estable, la organización puede asumir el riesgo; sin embargo, dicha decisión siempre deberá estar justificada.
- Mitigar el riesgo: aplicando medidas de seguridad que ayuden a reducir la consideración del riesgo.

En cualquier caso, a la hora de elegir una u otra opción la organización debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del recurso y el nivel de criticidad del riesgo.

3. Ciberseguridad y protección de datos de carácter personal

A priori, el marco jurídico más cercano aplicable y afectado por la gestión de la información se compone por el conjunto de normas que regulan el uso y tratamiento de datos personales. Desde el 25 de mayo de 2018, se encuentra en vigor el Reglamento General de Protección de Datos (en adelante, RGPD), aprobado el 18 de abril de 2016, y, por otra parte, en España se encuentra en vigor desde el 5 de diciembre de 2018 y en España la Ley Orgánica de 3/2018 sobre Protección de Datos y Garantía de los Derechos Digitales (conocida también como LOPDGDD).

El art. 5.1.f del RGPD establece que los datos personales serán tratados de tal manera que se garanticen su confidencialidad y seguridad: Lo que implica que se deberán adoptar las medidas de seguridad necesarias acorde al tipo de datos, medios de tratamiento y el estado de la técnica, tal como recoge el art. 32 del RGPD. Es por ello por lo que existe tan estrecha relación entre gestión de datos personales y seguridad de la información, y por ello, la necesidad de aplicar procedimientos de gestión de riesgos para evaluar y definir las medidas más óptimas para garantizar un tratamiento de datos seguros conforme a lo visto en los apartados anteriores.

Por otra parte, en 2013, la Comisión Europea presentó una propuesta de directiva relativa a las medidas para garantizar un elevado nivel común de las redes y la información de seguridad en toda la Unión. En 2015, el Parlamento y el Consejo acordaron en el texto de la Directiva de Red y Seguridad de la Información (conocida como NIS por sus siglas).

Esta directiva tiene como objetivo la mejora de las capacidades de ciberseguridad en los Estados miembros de la Unión Europea; establece el vehículo jurídico para un ciberespacio más abierto, seguro y resiliente. Con ello, se pretende crear una Unión Europea más protegida, y desarrollar recursos tecnológicos e industriales de ciberseguridad e implementar un mercado interno de productos y servicios de ciberseguridad.

Todo ello generará un espacio donde se contará con una mayor colaboración entre los países y las empresas de la Unión Europea, lo que permitirá reducir el cibercrimen, evitar la fragmentación de planes nacionales de ciberseguridad e incrementar la armonización entre Estados miembros en la protección frente a incidentes NIS, riesgos y amenazas. Consecuentemente, se mejorará de forma considerable la protección al consumidor, el negocio y el gobierno en el ámbito de la Unión Europea.

Pero la preocupación legislativa de un tratamiento seguro de datos personales no solo es una cuestión europea. De hecho, en Canadá se promulgó La Ley de Protección de Información Personal y Documentos Electrónicos (también conocida como PIPEDA por sus siglas en inglés), que determina las reglas que cualquier organización debe seguir al recopilar información personal; entre ellas, se establece que se debe tratar de forma segura.

El mismo principio de seguridad se expande por las legislaciones de todo el mundo, como ocurre en normativas tan dispares geográficamente como es la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Ley n.º 8968 de Costa Rica y la Privacy Act 1988 de Australia.

3. Conclusiones

La aparición de la COVID-19 cambiará nuestras vidas para siempre con nuevos estilos de trabajo, nuevos problemas de ciberseguridad, nuevas políticas propuestas, higiene personal, etc.

Todos los gobiernos del mundo han implantado y potenciado el distanciamiento social y los confinamientos (totales o parciales) como medidas preventivas claves para la propagación y contención de la COVID-19.

Gracias a la tecnología y a la hiperconexión con internet, cualquier persona puede continuar su vida profesional y privada de forma virtual. Sin embargo, con los enormes aumentos en el número de personas que trabajan de forma remota, es de vital importancia cuidar también *la higiene cibernética.*

Una incidencia de seguridad puede terminar en un ataque reputacional, en perdida de la continuidad de negocio, en un coste elevado para restaurar el sistema a un punto anterior, etc.; por todo ello, es imprescindible establecer y analizar los riesgos a los que se encuentra expuesta la organización.

Reducir los riesgos sobre la nueva gestión de la información en los nuevos contextos, como el teletrabajo, no es solo es problema y responsabilidad para la organización, sino un esfuerzo conjunto de todos, tanto de la organización como de los trabajadores y proveedores de tecnología. Porque tan solo con una visión y fuerzas conjuntas, se podrán plantear, diseñar y repensar nuevas medidas de gestión que reduzcan los riesgos cibernéticos y sus consecuencias.

Debido a ello, para mantener un nivel adecuado de seguridad informática en épocas de teletrabajo, se deberían seguir los siguientes consejos:

A) Recomendaciones para las organizaciones: cualquier empleador, bien sea una institución pública o bien sea una institución privada, deberá velar por implantar medidas de seguridad. Para ello, entre otras acciones, deberá:

- Realizar un análisis de riesgo detallado, así como el protocolo pertinente para efectuar análisis periódicos con el fin de detectar nuevas vulneraciones.
- Asegurarse una conexión segura entre el dispositivo del usuario y el sistema de información de la organización. Para ello, es recomendable contar con redes VPN (de sus siglas en inglés Virtual Private Network) corporativas que admitan una gran cantidad de conexiones simultáneas y con la finalidad de conectarse a uno o más ordenadores de una red privada utilizando Internet.
- Establecer un listado de aplicaciones y software autorizado por la organización, para evitar que el personal decida e instale soluciones informáticas que puedan comprometer la información corporativa. Además, es importante que el departamento de informática se encargue de realizar dichas instalaciones.
- Establecer sistemas de acceso con protocolos de identificación y autenticación con claves robustas (mezclando mayúsculas, minúsculas, números y símbolos) para acceder a los sistemas de información corporativos. Y, además, obligar su modificación de forma periódica.
- Proporcionar, cuando sea posible, ordenadores o dispositivos informáticos al personal que lo requiera, asegurándose de que tengan el sistema operativo y *software* de seguridad.
- En el caso de que no sea posible proporcionar dichos recursos, se deberá establecer políticas BYOD (concepto que deriva de sus siglas en inglés Bring Your Own Device) que regulen el uso de los dispositivos particulares de los empleados que se autorizan para un uso corporativo. En dicha política, se establecerá, entre otros aspectos, en qué condiciones se permiten su uso, cómo se accede a la información corporativa, qué configuraciones de seguridad serán necesarias para poder utilizarlos, etc.
- Formar al personal sobre principios básicos y fundamentales de seguridad de la información, así como establecer un programa de formación continua para reforzar e instruir a todo el personal ante los nuevos riesgos y amenazas que aparezcan.
- Definir una política para responder a incidentes y violaciones de seguridad.
- Asignar una dotación presupuestaria para reforzar la seguridad informática de la organización.

B) Recomendaciones para el personal para realizar sus funciones fuera de las dependencias de la organización: cualquier trabajador debe aplicar las medidas de seguridad idóneas o sustitutivas a las que aplica durante el desempeño de su trabajo

para garantizar la confidencialidad de la información que maneja. Para ello, entre otras acciones, deberá:

- Utilizar preferiblemente equipos informáticos corporativos, en vez de utilizar equipos personales, a menos que la organización haya establecido una política BYOD. Y, en la medida de lo posible, no mezclar en el mismo dispositivo el trabajo y las actividades de ocio.
- No compartir el dispositivo con el resto de personas que residan en el mismo domicilio.
- Conectarse a Internet a través de redes seguras, evitando las redes abiertas/libres, y mucho menos utilizar de forma fraudulenta redes wifi. Con una conexión insegura, las personas que se encuentren conectadas a la misma red pueden tener acceso al tráfico que se genera allí. Por ello, deberán activar un protocolo seguro o cifrado.
- Evitar el intercambio de información corporativa confidencial (por ejemplo, por correo electrónico) a través de conexiones posiblemente inseguras, como las redes wifi de cafeterías, vecinos del mismo edificio, etc.
- En la medida de lo posible, utilizar los recursos de la intranet corporativa para compartir archivos de trabajo. Por un lado, esto garantiza que los archivos de trabajo estén actualizados y, al mismo tiempo, se evita el intercambio de información confidencial entre dispositivos locales.
- Tener especial cuidado con la apertura de correos electrónicos, sobre todo, aquellos que hacen referencia a productos o comunicaciones referentes a la COVID-19, ya que pueden ser intentos de phishing o estafas. También, mantener especial atención a la dirección completa del emisor del correo electrónico y comprobar la identidad en aquellos casos en los que se requiera un pago o transferencia bancaria. En caso de duda sobre la legitimidad de un correo electrónico, comunicarlo al responsable de la organización.
- Tener el sistema operativo, antivirus y de las aplicaciones utilizadas actualizadas a la última versión disponible para reducir los fallos de seguridad y contar, en la medida de lo posible, con todos los parches de seguridad oportunos.
- Bloquear la pantalla al ausentarse del ordenador si se trabaja en un espacio compartido.
- No compartir las URL de las reuniones virtuales en las redes sociales u otros canales públicos para evitar que personas ajenas a la organización o terceros no autorizados pueden acceder a reuniones privadas.

C) Recomendaciones para los proveedores tecnológicos: cualquier proveedor de tecnología deberá implantar medidas proactivas para anticiparse y detectar los riesgos en una primera fase incipiente.

Bibliografía

Aguilera, P. (2011). *Redes seguras (Seguridad informática)*. Madrid, España: Editex.

Australian Government - Federal Register of Legislation. (n. d.). *Privacy Act 1988*. Recuperado de: https://www.legislation.gov.au/Series/C2004A03712

Cybersecurity Ventures (2020). *Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021*. Recuperado de: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Dewdney, A. (1989). Computer Recreations. *Scientific American, 260*(3), pp. 110-113. Recuperado de: http://www.jstor.org/stable/24987184

INCIBE (2017). *Clasificación cuantitativa y cualitativa de los riesgos*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2017). *Fases de un sistema de gestión de riesgos*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2017). *Matriz para clasificar el riesgo de forma cualitativa*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2017). *Modelo de inventario de recursos*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2019). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2019). *Herramienta de Autodiagnóstico*. Recuperado de: https://adl.incibe.es/

Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. Ley n.º 8968 Publicada en La Gaceta num. 170. San Jose 7 de julio de 2011.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado núm. 294. Madrid 6 de diciembre de 2018, páginas 119788 a 119857.

Observatorio Tecnológico (2012). *Pilares de la seguridad*. [Figura]. Recuperado de: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?showall=1

Observatorio Tecnológico (2019). *MONOGRÁFICO: Introducción a la seguridad informática*. Recuperado de: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?showall=1

Ramió Aguirre, J. (2006). *Libro electrónico de seguridad Informática y Criptografía*. Madrid, España: Universidad Politécnica de Madrid.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, publicado en el *Diario Oficial de la Unión Europea* núm. 119. Bruselas, 4 de mayo de 2016, pp. 1 a 88.

Personal Information Protection and Electronic Documents Act (2000). S.C. 2000, c. 5. Ontario, 13 de abril de 2000.

UNE (2017). ISO 27001. *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.* Madrid, España: Aenor.

UNE (2017). ISO 27002. *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información*. Madrid, España: Aenor.

Voutssas Marquez, J. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica 24*(50), pp.127-155.

Violencia de género digital: Nuevos desafíos para el Sistema Penal Argentino

Joselina Pastorini

Profesora adjunta de Derecho Penal I y II de la Universidad Católica de La Plata. Becaria de Investigación del programa Becas Iberoámerica Jóvenes Profesores Investigadores 2018-2019, en la Universidad San Pablo CEU Madrid, enero-marzo 2019, «Ciberdelitos: España-Argentina».

Mariano Refi

Profesor adjunto de Derecho Procesal Penal y Practicas I de la Universidad Católica de La Plata. Jefe de Trabajos Prácticos de Derecho Penal I de la Universidad Católica de La Plata. Colaborador en libro Las Redes del Delito de Ed. Astrea (2017).

Resumen

El avance de las nuevas tecnologías está modificando dramáticamente la dinámica de nuestras sociedades. El derecho, como ciencia social, no puede permanecer indiferente frente a este fenómeno.

Han surgido novedosas amenazas para los bienes jurídicos que demandan la intervención penal a través de la tipificación de nuevos comportamientos delictivos y también nuevas formas para cometer, a través de medios digitales, infracciones que ya se encuentran tipificadas. Y es aquí donde surge un nuevo tipo de afectación de bienes jurídicos, y que, cuando tengan como víctima a las mujeres, denominaremos: *violencia de género digital*.

La presente comunicación propone indagar respecto de este nuevo fenómeno, así como también analizar su tratamiento en el Sistema Penal Argentino y su impacto ante la pandemia de COVID-19.

Palabras claves: nuevas tecnologías, violencia de género digital, Código Penal Argentino, pandemia.

Abstract

The development of new technologies is dramatically modifying the dynamics of our society. As a result the Law cannot remain indifferent to this phenomenon.

New threats have emerged for legal rights that demand criminal intervention through the classification of new criminal behaviors and also new ways to commit offenses by using digital means that have been already classified. This is the point where a new type of legal rights violation

arises. As a matter of fact, when they have women involved as victims we will classify them as *digital gender violence*.

This article proposes to inquire into this new phenomenon, as well as to analyze its treatment in the Argentine Criminal System, and its impact during the COVID-19 pandemic.

Key words: new technologies, digital gender violence, Argentine Criminal Code, pandemic.

1. Introducción

El avance de las nuevas tecnologías de la información ha dado surgimiento a nuevos tipos de delitos, así como también a la comisión de delitos tradicionales —como los cometidos contra la integridad sexual— mediante el uso de las TIC[1].

Las nuevas tecnologías constituyen un desafío para los conceptos jurídicos existentes y los procesos de investigación que se llevan adelante en todo el mundo. Los desarrollos tecnológicos impactan en todo el derecho, pero crean mayores dificultades en algunas ramas de las ciencias jurídicas que en otras.

El incremento de los dispositivos móviles y de la creación de innumerables redes sociales, más aún en el contexto de pandemia, complica la situación para regularizar las prácticas virtuales e interacciones entre los usuarios, lo que les permite adentrarse en vivencias y experiencias desconocidas que a menudo pueden terminar de manera violenta o agresiva y que se desarrollan a través de los medios electrónicos.

La violencia de género no es un tema novedoso, pero sí es un problema que se sigue agrandando en la medida en que no contamos con los elementos suficientes para afrontarlo ni terminamos de entender su magnitud.

En una época en el que el coronavirus ha expuesto descarnadamente la existencia de otra pandemia —violencia de género—, más silenciosa e invisibilizada —con un aumento de un 39 % de denuncias durante el aislamiento social obligatorio—, pensamos en la idea de realizar la presente comunicación a través de un breve recorrido que vislumbre cómo atraviesa la perspectiva de género dentro del ámbito digital.

2. Violencia de género: marco normativo y conceptual

Como una primera aproximación a lo que actualmente entendemos por *violencia de género*, el art. 1 de la Convención sobre eliminación de todas las formas de discriminación contra la mujer, llevada a cabo por la Organización de Naciones Unidas en Nueva York

[1] Las tecnologías de la información y la comunicación (TIC) son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos (computadoras, teléfonos, portátiles de audio y video, etc.).

en 1979, nos refleja un primer acercamiento conceptual sobre el tema. Así, el artículo referido establece por discriminación contra la mujer:

> Cualquier distinción, exclusión o restricción hecha en base al sexo que tenga el efecto o propósito de disminuir o nulificar el reconocimiento, goce y ejercicio por parte de las mujeres, independientemente de su estado civil, sobre la base de igualdad del hombre y la mujer, de los derechos humanos y libertades fundamentales en las esferas política, económica, social, cultural, civil o en cualquier otra esfera.

Si bien la citada Convención no fue la primera en referirse a cuestiones vinculadas a los derechos fundamentales de las mujeres, siendo que su antecedente es la Declaración sobre la eliminación de la discriminación contra la mujer, proclamada por la Asamblea General de Naciones Unidas del año 1967, esta no esboza concepto alguno al respecto, sino que, principalmente, se centra en establecer qué acciones deben tomarse para dar fin a la discriminación contra la mujer.

Esta Convención de 1979 fue firmada por nuestro país el 17 julio 1980, ratificada el 15 julio de 1985 e incorporada a nuestro ordenamiento con jerarquía constitucional, conforme lo establece el art. 75 inc. 22 de nuestra Carta Magna (en 1994).

Ya vinculado directamente al concepto de *violencia de género*, dentro de la Conferencia Mundial de Derechos Humanos celebrada en Viena en 1993, la Asamblea General de Naciones Unidas aprobó la —referida— Declaración, lo que constituyó un nuevo punto de partida en la cuestión a nivel internacional, ya que, por primera vez, se abordó la violencia de género dentro del ámbito de los derechos humanos.

En dicho instrumento, se estableció el concepto de violencia contra la mujer en el art. 1, estableciendo:

> Todo acto de violencia basado en la pertenencia al sexo femenino que tenga o pueda tener como resultado un daño o sufrimiento físico, sexual o psicológico para la mujer, así como las amenazas de tales actos, la coacción o la privación arbitraria de la libertad, tanto si se producen en la vida pública como en la privada. (ONU, 1993)

De la definición que brinda Naciones Unidad, se desprenden los primeros tres tipos de violencia que pueden sufrir las mujeres por el hecho de pertenecer al sexo femenino: física, sexual y psicológica. Con el paso del tiempo, como veremos más adelante, los tipos de violencia han ido variando y aumentando.

A nivel interamericano, nos encontramos con la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, conocida también como la Convención Belém do Pará, por la ciudad en la que se desarrolló el 9 de junio de 1994, al poco tiempo de celebrada la Asamblea de Naciones Unidas.

Este instrumento internacional toma la definición elaborada por la ONU y, en su art. 1, establece lo que se va a entender por violencia de género: «… cualquier acción o conducta,

basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado» (OEA, 1994).

De esta manera, reconoce los mismos tipos de violencia: física, sexual y psicológica. En el artículo segundo, expone, en tres incisos, los lugares donde estos tipos de violencia se pueden desarrollar. En el primero, describe aquella violencia que se de en el seno familiar, unidad doméstica, la cual engloba «cualquier relación interpersonal». El segundo refiere a la que tenga lugar en la comunidad y sea perpetrada por cualquier persona, incluida la que se da «… en el lugar de trabajo, así como en instituciones educativas, establecimientos de salud o cualquier otro lugar…». Por último, el tercer apartado se refiere a la que sea realizada o tolerada por el Estado o sus agentes, sin importar dónde ocurra.

La Argentina incorporó al sistema normativo la Convención Belém do Pará en el año 1996 a través de la Ley 24.632. Posteriormente, en el año 2009, se aprobó la Ley 26.485 de Protección Integral para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres en los ámbitos en que desarrollen sus relaciones interpersonales, la que plasmó en su contenido los conceptos y el espíritu de la Convención.

Así, en su artículo cuarto, nuestra legislación aborda el concepto de violencia de género de forma más acabada y precisa, al establecer:

> Se entiende por violencia contra las mujeres toda conducta, acción u omisión, que, de manera directa o indirecta, tanto en el ámbito público como en el privado, basada en una relación desigual de poder, afecte su vida, libertad, dignidad, integridad física, psicológica, sexual, económica o patrimonial, como así también su seguridad personal. Quedan comprendidas las perpetradas desde el Estado o por sus agentes.
>
> Se considera violencia indirecta, a los efectos de la presente ley, toda conducta, acción omisión, disposición, criterio o práctica discriminatoria que ponga a la mujer en desventaja con respecto al varón.

Tal como surge de esa definición, nuestra legislación modifica y extiende el concepto de *violencia de género*, si bien toma de los instrumentos internacionales conceptos allí reflejados, incorpora el término *omisión*, abarcando así más conductas que pueden ser cometidas por el varón, como contraposición a la acción. En igual sentido, refiere a la violencia como directa e indirecta.

Asimismo, incorpora la terminología *relación desigual de poder*, estableciendo así la condición que se tiene que verificar para considerar que nos encontramos frente a un caso de violencia de género; se desprende de ello que no toda afectación de derechos de la mujer será cometida en un contexto de ese tipo, sino aquellos desarrollados en la desigualdad mencionada.

Nuestra ley, en su último párrafo, hace mención especial a la violencia indirecta, no tratada en los instrumentos internacionales; la considera toda conducta, acción, omisión, disposición, criterio o práctica discriminatoria que coloque a la mujer en desventaja con respecto al varón.

Si bien se marcaron las incorporaciones realizadas por nuestra ley, por otro lado, de la definición original se conserva el ámbito donde se puede desarrollar este tipo de violencia: el público y el privado; y abarca la violencia que es perpetrada desde el Estado o por intermedio de sus agentes.

3. Tipos de violencia de género

Como se indicó, la Ley 26.485 sobre protección integral de las mujeres nos brinda, en su artículo quinto, una clasificación de los diferentes tipos de violencia que pueden sufrir las mujeres, tomando como referencia las tres clases identificadas a nivel internacional, y añade la violencia económica y patrimonial, como así también la simbólica.

- **Violencia física:** la que se emplea contra el cuerpo de la mujer y produce dolor, daño o riesgo de producirlo, y cualquier otra forma de maltrato o agresión que afecte su integridad física.
- **Violencia psicológica:** la que causa daño emocional y disminución de la autoestima, o perjudica y perturba el pleno desarrollo personal, o que busca degradar o controlar sus acciones, comportamientos, creencias y decisiones, mediante amenaza, acoso, hostigamiento, restricción, humillación, deshonra, descrédito, manipulación o aislamiento. Incluye también la culpabilización, vigilancia constante, exigencia de obediencia, sumisión, coerción verbal, persecución, insulto, indiferencia, abandono, celos excesivos, chantaje, ridiculización, explotación y limitación del derecho de circulación o cualquier otro medio que cause perjuicio a su salud psicológica y a la autodeterminación.
- **Violencia sexual:** cualquier acción que implique la vulneración en todas sus formas, con o sin acceso genital, del derecho de la mujer de decidir voluntariamente acerca de su vida sexual o reproductiva a través de amenazas, coerción, uso de la fuerza o intimidación, incluida la violación dentro del matrimonio o de otras relaciones vinculares o de parentesco, exista o no convivencia, así como la prostitución forzada, explotación, esclavitud, acoso, abuso sexual y trata de mujeres.
- **Violencia económica y patrimonial:** la que se dirige a ocasionar un menoscabo en los recursos económicos o patrimoniales de la mujer, a través de la perturbación de la posesión, tenencia o propiedad de sus bienes, pérdida, sustracción, destrucción, retención o distracción indebida de objetos, instrumentos de trabajo, documentos personales, bienes, valores y derechos patrimoniales. Asimismo, establece dentro de este tipo de violencia a la limitación de los recursos económicos destinados a satisfacer sus necesidades, la privación de los medios indispensables para vivir una vida digna, la limitación o control de sus ingresos, así como la percepción de un salario menor por igual tarea, dentro de un mismo lugar de trabajo.

- **Violencia simbólica:** La que, a través de patrones estereotipados, mensajes, valores, íconos o signos, transmita y reproduzca dominación, desigualdad y discriminación en las relaciones sociales y naturalice la subordinación de la mujer en la sociedad, siendo un claro ejemplo de ello algunas campañas publicitarias reproducida tanto por medios gráficos como de televisión.

Tal como lo hemos analizado, la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer de 1994 (Convención de Belém do Pará) define la violencia contra las mujeres como «... cualquier acción o conducta, basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado» (artículo 1).

Si bien dicha Convención implicó un hito en materia de regulación y reconocimiento de los derechos hacia la mujer, cuando fue escrita y adoptada —a principios de la década de 1990—, la «esfera pública» no incluía «el mundo en línea», y por tal han quedado desprotegidos ciertos ámbitos —como el ciberespacio— en donde la violencia hacia la mujer se vislumbra con habitualidad y crece de forma exponencial.

Por su parte, a nivel nacional, la Ley 26.485 de protección de violencia hacia las mujeres también contempla diversos tipos y modalidades —doméstica, institucional, laboral, obstétrica, etc.—, pero nada «dice» respecto a la «violencia digital». Y esto se debe, nuevamente, a que es una ley de hace diez años, y por tal, tiene mucho para recorrer, para actualizarse y ampliarse, y si bien el derecho nunca va por delante de la tecnología, en este caso en particular, ha quedado por demás atrás de camino.

La sociedad ha cambiado radicalmente en los últimos veinticinco años, y nuestras identidades, actividades e interacciones en línea son un componente cada vez más importante de nuestra vida cotidiana pública.

A pesar de que las TIC son recursos de gran impacto favorable en el ejercicio de los derechos de las mujeres, también lo son para su desvalorización y deslegitimación, porque el entorno virtual es un espejo de las relaciones de poder en la sociedad y de los comportamientos y ejercicios discriminatorios y violentos en sus múltiples manifestaciones.

Gran cantidad de clases y modalidades de violencia de genero están fuera del debate, porque no se conocen o se subestiman. En el marco de la violencia de género, esto no resulta ajeno: existen situaciones en el ámbito digital, ya sea a través de las redes sociales, foros, chats y otros recursos semejantes, en las que mayormente los hombres ejercen violencia contra la mujer.

La violencia de género es la misma, lo digital es el soporte. Como una primera aproximación, podemos definir violencia de género digital como «toda aquella agresión psicológica realizada por un hombre a través de las nuevas tecnologías (correo electrónico, WhatsApp, RR. SS.) contra una mujer con el único objetivo de discriminación, dominación o intromisión sin consentimiento en la intimidad de la víctima» (OEA, 2019).

Según un reciente informe publicado por la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires en *Violencia contra la mujer en el entorno digital*, la violencia de género en línea

> … son aquellos actos cometidos, instigados o agravados, en parte o totalmente, por el uso de las tecnologías de la información y la comunicación, a través de teléfonos móviles, internet, plataformas de redes sociales, correo electrónico o cualquier otro medio de transmisión de datos. (Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires, 2019, p. 4)

4. Violencia de género, ciberespacio y pandemia

Imaginemos que nos encontramos en un auditorio colmado de gente —bastante impensado en este año atípico de pandemia— y pedimos a los presentes que cierren sus ojos y piensen en un caso de violencia de género. Seguramente, la mayoría —en primera instancia y casi cual acto reflejo— pensaría en el ejemplo de una mujer víctima siendo golpeada, violada, etc.; se imaginan sangre, moretones. Este no es un ejemplo errado, nadie dudaría de que eso se trata de violencia de género, pero creemos que dicho caso hipotético es simple y escueto con relación a lo que es la violencia de género, que no solo es física o sexual, sino que también hay muchos tipos de violencia que están invisibilizados, a tal punto de haberse casi «normalizado».

¿Es posible hablar de violencia de género en el ciberespacio? Claramente no resulta simple poder brindar una respuesta. Pensemos que, al nuevo mundo de las tecnologías, que nos atraviesa, en el que nos encontramos inmersos e interactuamos gran parte de las horas de nuestros días —aún más en esta «nueva normalidad»—, tenemos que combinarlo con la «perspectiva de género», la cual tiene esa similitud, que también nos atraviesa, la escuchamos todo el tiempo, estamos inmersos, se imponen pautas distintas y aun así tampoco sabemos mucho de qué va.

Y es aquí donde nos permitimos afirmar la existencia de una nueva modalidad de violencia de género en el ciberespacio, la cual apareció como un torbellino con el fin principal de afectar la reputación digital de las mujeres y su desenvolvimiento en el ámbito virtual.

La violencia de género en el ciberespacio se ha «puesto de moda» en tiempos de pandemia, y esto se debe a que muchos individuos disponen de más tiempo para amedrentar la psiquis de exparejas, aprovechando la gran variedad de plataformas digitales de intercambio —y exposición social—, como Facebook, Instagram, TikTok y a las aplicaciones de mensajería instantánea, como WhatsApp, Telegram, etc.

Los mecanismos de violencia incluyen no solo posteos con comentarios despectivos y agraviantes hacia el género y la víctima propiamente dicha, sino también el «likeo» de sus fotografías en redes sociales, con solución de continuidad. A través de la modalidad

de «likeo ininterrumpido de imágenes», el violento demuestra, con signos inequívocos, que está presente en la vida de la víctima, la que probablemente pudo haber obtenido una orden de restricción física que no incluyó a las redes sociales en particular.

La llegada de la pandemia obligo a trasladar muchas actividades al ámbito digital: videollamadas, reuniones virtuales, clases en línea y *home office*. Las redes sociales e Internet, en general, son una extensión del debate público y que, de la misma manera en la que las mujeres sufren violencia de género en las calles o en sus casas, la sufren en las redes sociales, por lo cual la violencia digital *no es un tipo de violencia nueva, sino una forma diferente en la que esa violencia se manifiesta*.

Un claro avance en la cuestión es un reciente precedente judicial del 22 de junio pasado, dictado por la doctora Guillermina Leontina Sosa, a cargo del Juzgado de Familia número 2 de Comodoro Rivadavia, quien sentenció que la colocación de distintos «me gusta» —pulgar para arriba— por parte del victimario a publicaciones efectuadas por la víctima en su perfil de Facebook importa el incumplimiento de las medidas de no comunicación y contacto dispuestas en sede judicial.

5. Violencia de género digital en el Código Penal Argentino

El Código Penal Argentino data de 1921. Por un lado, sin mayor esfuerzo, podemos inferir que el legislador de aquella época no previó ni podría haber previsto acciones típicas que captaran conductas delictivas relacionadas con la informática y las demás tecnologías que se han desarrollado a lo largo de este siglo. Por otro, si bien nuestro Código Penal ha experimentado diversas modificaciones relacionadas a la protección de la mujer víctima, poco ha incluido en lo atinente a esta nueva modalidad de violencia a través de los medios informáticos. En esa línea, sostiene la Dra. Lorena Bicilic (2015) que nuestro ordenamiento aún no contempla expresamente la violencia digital, salvo en el caso de menores de edad contemplado en el art. 128 del C. P. en la figura del *grooming*.

Si bien dichas falencias legislativas pueden ser justificadas por la tan mencionada frase «el derecho nunca va por delante de la tecnología», en este caso en particular resulta llamativo dicho «desinterés regulatorio», puesto que las estadísticas actuales han demostrado que, anterior a escenarios que han derivado en femicidios o ataques brutales hacia una mujer, por lo general se ha constatado situaciones de violencia o persecución previas y que, en muchos casos, esta se ejerce a través de medios tecnológicos —Facebook, WhatsApp, Instagram, etc.—.

No obstante ello, si bien no existe, aún en nuestro país, una regulación ni tratamiento específico a esta nueva modalidad de violencia hacia las mujeres con la utilización de medios tecnológicos, analizaremos las figuras delictivas —algunas actualmente incluidas en nuestro derecho interno— en donde las TIC son utilizadas como medio o como fin, para allí poder analizar si ellas también pueden ser analizadas con perspectiva de género.

6. Delitos de violencia de género informática como medio o como fin

En este apartado, no analizaremos cada tipo penal en particular, siendo que es materia propia de la parte especial de nuestro Derecho Penal y dista del objeto que persigue el presente trabajo. Haremos referencia a algunos delitos en particular que, conforme la experiencia que nos dio la práctica profesional y judicial, son delitos que con mayor frecuencia resultan ser cometidos a través de medios digitales.

6.1. Amenazas, desobediencia y otros delitos

Con el avance de la tecnología y los medios de comunicación, se han ampliado enormemente las posibilidades de lograr el contacto entre dos (o más) personas, y si bien, como ya se dijo, dicha evolución tecnológica trae innumerables beneficios, tiene como contracara su empleo como medio para cometer una gran cantidad de delitos.

En relación con el contexto de género, en la práctica tribunalicia observamos que muchas de las amenazas proferidas de un varón hacia una mujer son efectuadas por medio de servicios que proveen aplicaciones como WhatsApp, Messenger de Facebook y de Instagram, y cualquier otro servicio de mensajería instantánea, como los mensajes de texto. De este modo, una persona puede llegar a contactar a otra en cuestión de segundos y, según el contenido del mensaje y el efecto que produzca en la persona que lo recibe, puede verse configurado el delito de amenazas o de coacción, conforme lo normado por los arts. 149 bis y 149 ter del Código Penal.

La imposibilidad de control respecto de este tipo de comunicaciones aumenta su impunidad. Es normal que, en algunos casos en que el hostigamiento es constante, por más medida que tome la víctima, el resultado final sea el cambio de número telefónico por parte de esta, ya que el agresor utiliza distintos medios para lograr su cometido; no basta la posibilidad que alguna de las aplicaciones mencionadas ofrecen de poder «bloquear» o imposibilitar el contacto de este agresor. En algunos casos con los que se ha tenido contacto, la víctima ha llegado a cambiar cinco veces de número telefónico debido al hostigamiento que recibía por parte del agresor.

Otro de los delitos que comúnmente se comete por medio de los servicios de mensajería es la desobediencia. Este tipo penal se configura una vez que el agresor, sobre quien pesaba una medida judicial (normalmente dictada por un Juzgado de Familia o un Juzgado de Paz) de cesar el hostigamiento, no mantener trato con la víctima (hostil o no), la incumple y se contacta de esa manera, produciéndose así el delito tipificado en nuestro art. 150 del Código Penal.

Las medidas judiciales referidas, en los últimos años y con el avance de la tecnología, al establecer las normas de conducta que debe cumplir el agresor, incorporaron la frase «por cualquier medio», lo que amplía los canales de comunicación por los cuales el

sujeto agresor puede, en su caso, incumplir la medida de comportamiento que el juez interviniente había estimado razonable, lo cual acarrea la comisión de ese delito.

En la faz práctica, a los fines de colectar material de prueba para acreditar los extremos que estos tipos penales exigen, se realizan pericias informáticas sobre el teléfono tanto de la víctima como del agresor en caso de lograr secuestrarlo. De ese modo, se logran extraer las conversaciones mantenidas entre ellos, como así también toda evidencia digital que sea útil a la investigación: imágenes o videos. Asimismo, se incorporan capturas de pantalla en formato de imagen donde lucen las comunicaciones mantenidas y que fueron extraídas de los teléfonos analizados.

Con base en la acreditación de la autoría responsable, se piden informes de titularidad respecto de los números telefónicos intervinientes a las compañías correspondientes; también a las redes sociales en caso de que hayan sido utilizadas como medio comisivo de estos delitos.

De público conocimiento es que, producto de la pandemia ocasionada por la COVID-19, a las personas privadas de su libertad en la provincia de Buenos Aires se les posibilitó el acceso a teléfonos celulares para que pudieran mantener la comunicación con sus afectos, ello en razón de que tenían vedadas las visitas y el contacto con el mundo exterior. Si bien nos parece una medida satisfactoria en cuanto se tiene que garantizar este derecho a las personas privadas de su libertad, esta medida ha aumentado los contactos de aquellas personas encarceladas por delitos de violencia de género con sus víctimas, situación que, antes del otorgamiento de teléfonos celulares, no era habitual.

6.2. *Stalking* u hostigamiento digital

El *stalking*, también conocido como «ciberacoso u hostigamiento digital», se verifica cuando una persona persigue a otra de forma obsesiva y dicha intromisión se lleva adelante mediante medios informáticos, sea llamadas telefónicas, mensajes, redes sociales.

Si bien podemos relacionar tales comportamientos con los delitos analizados —desobediencia y amenazas—, por el medio y fin con el que se realizan, se ha dado un tratamiento y regulación específica a nivel mundial, y ya el concepto de *stalking* se instaló en nuestra sociedad.

En la Argentina, algunas prácticas *online* que ocasionan graves daños en sus víctimas no están tipificadas como delito por el Código Penal. Actualmente, nuestra legislación no contempla de forma expresa este delito[2], y por tal, en caso de que se verifique una situación de hostigamiento a través de medios digitales, deberíamos recaer —para su encuadre jurídico— en las figuras delictivas tradicionales (ej., amenazas).

[2] Para muchos autores, el *stalking* se podría inferir del primer inciso del delito de *grooming* —hoy, en el art. 131 del C. P.— en donde luce: «… tomare contacto con una persona menor de TRECE años mediante relatos o conversaciones de contenido sexual». De afirmarlo, nuestro actual Código Penal contemplaría la figura del *stalking* cuando la finalidad sea «sexual» y cuando la víctima sea menor de edad.

Por tal, y al no ser delito en nuestro país, las mujeres que lo sufren son víctimas de persecuciones constantes y molestia sistemática. Al no tener marco legal, no existe la posibilidad de plantear una denuncia por vía judicial, al menos en fuero penal. Solo en la Ciudad Autónoma de Buenos Aires, se instituyó como contravención, y la pena supone el pago de una multa. Así, el Código Contravencional de la Ciudad Autónoma de Buenos Aires, en su art. 71 ter, regula el hostigamiento digital y sanciona a quien *intimide u hostigue a otro mediante el uso de cualquier medio digital, siempre que el hecho no constituya delito* (texto introducido por la Ley N.° 6.128).

España visualizó la importancia de regular en su derecho interno este delito (2018). En el año 2015, incluyó la figura del *stalking* en su art. 172 ter, el cual establece:

> Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:
>
> 1.ª La vigile, la persiga o busque su cercanía física.
>
> 2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.
>
> 3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.
>
> 4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.
>
> Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

Por su parte, el Código Penal Italiano, también reguló —desde el año 2009— el delito de *stalking*, en su art. 612 BIS, regulado por Decreto Ley 11/2009 del 23 de febrero, convalidado por el Parlamento italiano mediante Ley 28/2009; aquel establece lo siguiente:

> A menos que el acto constituya un delito más grave, cualquier persona que, con una conducta repetida, amenace o acose a alguien de una manera que cause un estado de ansiedad o temor severo y persistente, será castigada con prisión de seis (6) meses a cinco (5) años. Un temor fundado por la seguridad de uno mismo o de un pariente cercano o de una persona conectada a él por una relación afectiva o que lo obligue a alterar sus hábitos de vida.

6.3. El ciberacoso como forma de violencia de género en los jóvenes

Como se mencionó, el uso de las nuevas tecnologías se está masificado entre la población, en especial entre la más joven, un grupo necesariamente importante en la tarea

de erradicar la violencia de género, que tiende a actuar en la vida con mayor ingenuidad. En la juventud, concebida como una etapa de suma vulnerabilidad, el trabajo preventivo resulta esencial para desarrollar la igualdad entre hombres y mujeres, y evitar que «la sociedad del mañana» siga ejerciendo violencia contra ellas por razón de género (España - Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del gobierno para la violencia de género, 2014).

El ciberacoso como vía de ejercer violencia de género es una forma de limitación de la libertad que genera dominación y relaciones desiguales entre hombres y mujeres que tienen o han tenido una relación afectiva. El ciberacoso para ejercer la violencia sobre la pareja o expareja supone un dominio sobre la víctima mediante estrategias humillantes que afectan la privacidad e intimidad, además del daño que supone a su imagen pública.

Este acercamiento se produce, generalmente, sin que haya contacto físico; la reiteración se convierte en la estrategia de invasión de la intimidad más utilizada por los acosadores. Por ejemplo, la insistencia en el envío de mensajes o las peticiones recurrentes para conseguir determinada conducta se convierten en la fórmula para acosar a la víctima.

Este acoso debe ser repetitivo, no consentido, suponer una intromisión en la vida privada de la víctima, y el motivo, estar relacionado en alguna medida con la relación afectiva que tienen o tuvieron acosador y acosada. Esta definición se aplica a la población juvenil, dado que es este grupo el que asume de manera cotidiana y pasa gran parte del día utilizando las TIC, en general, y, especialmente, Internet, las redes sociales, de lo cual deriva que este sea el segmento social más expuesto a dicho fenómeno.

Es normal que la juventud, que nace en la era digital, presente una percepción muy baja de los efectos negativos que trae el ciberacoso: en un comienzo tienden a ser molestias irrelevantes o inocuas. Internet y las redes sociales constituyen un ámbito en el que la población más joven se encuentra muy cómoda y en el que desarrolla sus capacidades y relaciones sin las limitaciones impuestas en otros ámbitos. Por ello, determinados patrones de uso de Internet, que pueden ser interpretados como prácticas de riesgo, tales como intercambiar información o imágenes privadas, no se perciben como un peligro.

6.4. *Sexting*. «Pornovenganza». Sextorsión

Otro de los conceptos que tomó «relevancia» —más aún luego de un comunicado por parte del Ministerio de Salud de la Nación— en el contexto de pandemia es el de *sexting*, el cual se refiere al envío de imágenes o videos de contenido sexual a otra/s persona/s a través de distintos servicios de mensajería, por medio de dispositivos móviles.

Si bien para la concreción de la conducta debe haber, por lo menos, dos personas (emisor y receptor), la eventual y posterior circulación de dicho material puede derivar en su publicación (en un sitio web, por ejemplo) o ser viralizada sin el consentimiento de su titular, y es lo que comúnmente se conoce —de forma errónea— como *revenge porn o pornovenganza*.

A su vez, también ha surgido la figura de la *sextorsión*, donde parecería —a simple vista— no existir diferencias entre un delito u otro. La sextorsión es un tipo de chantaje a través del cual se amenaza a la persona destinataria con revelar información íntima de carácter sexual, a cambio de nuevo material, dinero u algún otro requerimiento.

La principal diferencia entre uno y otro consiste en que, en la sextorsión, el chantajista pide dinero para no materializar la amenaza, mientras que, en la *pornovenganza,* ese material es utilizado como objeto de extorsión y amenazas, con el alegato de que, si la mujer no hace lo que él pide, publicará las imágenes.

Cabe destacar, según lo sostiene Elizabeth Castillo Vargas (2015), que el término *pornovenganza* está mal utilizado, ya que la idea de «venganza» se asocia con que la mujer hizo algo malo, por lo que estaría «sufriendo las consecuencias».

Desde el punto de vista legal, en nuestro país, si bien hubo mejoras relativas en el sistema judicial, todavía no es considerado un delito.

Por su parte, el ordenamiento jurídico español regula el delito de *pornovenganza o revenge porn* en su art. 197, de forma similar a la redacción que pretende incorporar nuestro país y tampoco contempla la necesidad de que el autor del delito actúe por «venganza o despecho».

En un reciente fallo —de total interés—, del 24 de febrero de este año, el Tribunal Supremo de España[3] condenó la difusión de imágenes privadas vía mensajería instantánea. En dicha sentencia —suscripta por el Magistrado Manuel Marchena Gómez—, consideró que «obtiene la imagen quien fotografía o graba el video en el que se exhibe algunos aspectos de la intimidad de la víctima, valiéndose de cualquier medio convencional o de un programa de mensajería instantánea que opera en redes telemáticas» (Diario *La Vanguardia*, 2020); allí se destaca que *obtener* es sinónimo de *alcanzar*, *conseguir*, *lograr algo*, *tener*, *conservar* o *mantener*.

A su vez, lo más relevante de dicha resolución es que sentó postura al afirmar:

> … no se puede sustentar la teoría la cual da cuenta que fue la propia víctima la que creó el riesgo de su difusión obviando su autoprotección, remitiendo su propia foto al acusado a través del programa de mensajería. Ello, toda vez que quien remite a una persona en la que confía una foto expresiva de su propia intimidad, no está renunciando anticipadamente a ésta como tampoco está sacrificando de forma irremediable su privacidad, ya que constituye un gesto de confianza, entrega y selectiva exposición a una persona cuya lealtad no cuestiona.

7. Estadísticas: Violencia de género digital en números actuales

Desde fines de marzo, cuando el presidente Alberto Fernández decretó el aislamiento social preventivo y obligatorio, la línea 144 en la ciudad recibió 32.000 llamadas, de las

[3] ATS 1890/2019' ECLI: ES:TS:2019:1890 A

cuales un 45 % fueron por razones de violencia de género, maltrato y afines. El año 2019, durante el mismo período, se recibieron 23.000 consultas y el 35 % de ellas eran por esos motivos, informaron desde el área de Mujer que depende del Ministerio de Desarrollo Humano y Hábitat de la Ciudad (Argentina, 2020).

Del total de consultas que recibió la ciudad sobre violencia de género, el 59 % de las mujeres fue objeto de mensajes sexuales y misóginos, el 45 % decidió suspender el uso de las redes sociales por el acoso que sufría, el 34 % recibió mensajes con lenguaje o comentarios abusivos, y el 26 % recibió amenazas directas o indirectas de violencia psicológica o sexual en las redes (Centro de Protección de Datos Personales, Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires, 2019).

Con respecto a la violencia digital, de las 32000 comunicaciones que hubo en estos seis últimos meses, solo 157 fueron por esa cuestión; no obstante, ese número casi triplicó las inquietudes sobre ese tipo de agresión expresadas en otros años (Musse, 2020).

En el ámbito europeo, una de cada diez mujeres declaró haber sufrido ciberacoso desde la edad de 15 años, lo que incluye haber recibido correos electrónicos o mensajes SMS no deseados, sexualmente explícitos y ofensivos, o bien intentos inapropiados y ofensivos en las redes sociales. El riesgo es mayor para las mujeres jóvenes con edades comprendidas entre los 18 y los 29 años (Unión Europea, 2014).

8. Conclusión

El siglo xxi exige otro tipo de herramientas para garantizar persecución de los delitos «no convencionales», entre los que se ubican los ciberdelitos sexuales, y eso solo es posible con una política criminal integral, seria, y comprometida en el combate de estas nuevas formas criminales.

Un primer paso al cumplimiento de esos fines resulta ser la modificación o modernización legislativa de los delitos contra la integridad sexual cometidos a través de los medios informáticos.

Actualmente, bien lo ha dicho Marcelo Riquert (2008), la Argentina, en materia penal sustantiva, se encuentra por debajo de los parámetros internacionales que regulan la cibercriminalidad —Convenio de Budapest—. El anteproyecto de reforma del Código Penal Argentino propone varias modificaciones o incorporaciones relacionados a los ciberdelitos sexuales, al modernizar la actual redacción de nuestro Código Penal —del año 1921— e incorporar tipos penales, que actualmente carecen de regulación.

Si bien esta no resulta ser la solución para el combate de este nuevo fenómeno criminal, dado que la ley nunca va por delante de la tecnología, resulta, al menos, un primer avance en la materia, la cual debe ir acompañada de otro tipo de medidas, en especial preventivas o educativas.

Por otro lado, en relación a los delitos cometidos en un contexto de violencia de género, hemos visto como ellos han aumentado en la medida en que las nuevas tecnologías

de la información y comunicación han ido avanzando con el tiempo. A ello se le suma la característica que presentan aquellos: la dificultad de control por parte del Estado y de la víctima.

Estos medios de comunicación han presentado un gran obstáculo en cuanto a la posibilidad de detener dichos delitos; procuran además la impunidad por parte de quien los lleva a cabo y dificultan el cese de estos tipos de contacto en razón de la cantidad de medios que existen en la actualidad y a través de los cuales el agresor puede procurar un fácil contacto con la víctima. En el caso de que este último sea «bloqueado», existe también la posibilidad de crear falsos usuarios o cambiar de plataforma para continuar con el hostigamiento.

El desafío por parte del Estado, si bien resulta claramente dificultoso, debe ser tomado con seriedad y urgencia, con la finalidad de poner un punto final en estas nuevas modalidades delictivas.

Para finalizar, no queríamos dejar de citar al gran Castells, quien, con gran sabiduría, ha señalado que «todas las tecnologías pueden utilizarse tanto para la opresión como para la liberación» (2012: p. 412).

9. Bibliografía

Argentina (2020). Información estadística del sitio web argentina.gob. Recuperado de: https://www.argentina.gob.ar/generos/linea-144/informacion-estadistica

Argentina (8 de mayo de 1985). Ley N.º 23.179, Convención sobre la eliminación de todas las formas de discriminación contra la mujer.

Argentina (11 de marzo de 2009). Ley N.º 26.485 de Protección Integral a las Mujeres.

Bicilic, L. (2020). Violencia de género en el marco de la violencia digital. Recuperado de: https://www.cibercrimen.org.ar/2020/02/15/violencia-de-genero-en-el-marco-de-la-violencia-digital/

Castells, M. (2012). Redes de Indignación y Esperanza. Los Movimientos Sociales en la Era de Internet. Madrid: Alianza Editorial.

Castillo Vargas. E. F. (2015). *Violencia contra las mujeres y TIC (VCM y TIC)*. Fundación Karisma. Documentos 3. Recuperado de: https://karisma.org.co/wp-content/uploads/2014/12/VCMyTIC.pdf

Centro de Protección de Datos Personales, Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires (2019). Informe institucional producido por el Observatorio de Derechos en Internet.

Ciudad Autónoma de Buenos Aires, Código Contravencional de la Ciudad de Buenos Aires, Ley N.° 6.128, Publicación en el BOCBA N.° 5531 del 7/1/2019. Disponible en: http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley6128.html

Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires (2019). *Violencia contra la mujer en el entorno digital. Derechos, conceptos y recomendaciones*. Disponible en: http://cpdp.defensoria.org.ar/wp-content/uploads/sites/5/2019/03/Violencia-contra-la-mujer-Cuadernillo.pdf

El Supremo confirma que es delito reenviar la foto de alguien desnudo porque afecta gravemente su intimidad. (26 de febrero 2020). Diario *La Vanguardia*. Disponible en: https://www.lavanguardia.com/vida/20200226/473798822980/el-supremo-confirma-que-es-delito-reenviar-la-foto-de-alguien-desnudo-porque-afecta-gravemente-su-intimidad.html

España - Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del gobierno para la violencia de género (2014). El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento. Recuperado de: https: //violenciagenero. igualdad. gob.es /violencia EnCifras /estudios /colecciones/pdf/Libro_18_Ciberacoso.pdf

España (2018). *Sociedad Digital y Derecho*. Publicación Boletín Oficial del Estado, Madrid. Dirección de Tomás de la Quadra-Salcedo Fernández del Castillo y José Luis Piñar Mañas. Ref: NIPO BOE: 786-18-069-0

Italia. Modificación al Código Penal, decreto-legge 23 febbraio 2009, n. 11. Disponible en: https://www.gazzettaufficiale.it/eli/id/2009/04/24/09A04793/sg

Musse, V. (2020). Durante la pandemia, crecieron las consultas por violencia de género digital en la Ciudad. Diario *LA NACIÓN*, 17 de septiembre de 2020. Recuperado de: https://www.lanacion.com.ar/seguridad/durante-pandemia-crecieron-consultas-violencia-genero-digital-nid2452993

OEA (9 de junio de 1994). Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer "Belem do Para", aprobada por Ley 24.632, 13 de marzo de 1996. Belem Do Para.

OEA (2019). *Combatir la violencia en línea un llamado a la protección*. Recuperado de: https://www.oas.org/es/sms/cicte/docs/20191125-ESP-White-Paper-7-VIOLENCE-AGAINST-WOMEN.pdf

ONU (18 de diciembre de 1979). Convención sobre Eliminación de todas las formas de discriminación sobre la mujer. Nueva York.

ONU (1993). Declaración sobre la eliminación de la violencia contra la mujer, 20 de diciembre de 1993. Viena.

Riquert, M. A, (2008). Legislación contra la delincuencia informática en MERCOSUR. En *Revista General de Derecho Penal*, dirigida por los Dres. Ignacio Berdugo Gómez de la Torre y José R. Serrano-Piedecasas, con referato, N.º 9 de mayo de 2008, Sección Apuntes de Derecho Comparado, España. Versión electrónica disponible en: www.iustel.com

Unión Europea (2014). Agencia de los Derechos Fundamentales. Violence against women: an EU-wide survey.

Inteligencia artificial y violencia contra las mujeres: ¿funcionan los sistemas automatizados de evaluación del riesgo?

Lucana M.ª Estévez Mendoza

Profesora colaboradora y doctora de Derecho Procesal. Universidad CEU San Pablo.

Resumen

Este trabajo presenta un análisis reflexivo de la violencia contra la mujer basado en la valoración automatizada del riesgo mediante sistemas informáticos que hacen uso de algoritmos de inteligencia artificial. Se toma como punto de partida la Sentencia de la Audiencia Nacional de 30 de septiembre de 2020, que condena al Ministerio del Interior español a pagar una indemnización en concepto de responsabilidad patrimonial del Estado por un error de cálculo. Se estudia el sistema de valoración empleado en España (VioGen) con perspectiva crítica.

Palabras clave: inteligencia artificial, violencia contra las mujeres, análisis de riesgos, proceso penal.

Abstract

This work presents a reflective analysis of violence against women based on computer-mediated automated risk assessment using artificial intelligence algorithms. A Judgment of the National Audience dated 30 September of 2020, which condemned the Spanish Ministry of the Interior to pay a compensation due to a calculation error, is the starting point of the research. The Spanish risk assessment system applied to gender-based violence cases (VioGen) is studied from a critical perspective.

Keywords: Artificial intelligence, gender-based violence, risk assessment, criminal procedure.

1. Introducción

Durante los últimos meses, la pandemia generada por el virus SARS-CoV-2 ha supuesto que multitud de países hayan estado o estén aún en situación de confinamiento, con millones de personas recluidas en sus hogares, a salvo de la enfermedad. Esta medida

de protección, de carácter sanitario, si bien se muestra como adecuada para refugiarse de la infección que rodea al mundo, conlleva otros efectos y situaciones de crisis distintas a la sanitaria, como la económica, política e incluso social. En este contexto, según la ONU Mujeres, entidad de las Naciones Unidas para la igualdad de género creada en 2010, otro peligro mortal prolifera la violencia contra las mujeres, lo que ha sido denominada «la pandemia en la sombra» (2020).

Este tipo de violencia, según el Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica —Convenio de Estambul de 2011—, se refiere a lo siguiente:

> Una violación de los derechos humanos y una forma de discriminación contra las mujeres, y designar todos los actos de violencia basados en el género que implican o pueden implicar para las mujeres daños o sufrimientos de naturaleza física, sexual, psicológica o económica, incluidas las amenazas de realizar dichos actos, la coacción o la privación arbitraria de libertad, en la vida pública o privada. (Artículo 3 a)

Distinta connotación tiene el término, comúnmente empleado como sinónimo, de *violencia de género o violencia ejercida contra las mujeres por razón de género*, que, según el párrafo d) de la misma disposición, se aplica a «toda violencia ejercida contra una mujer porque es una mujer o que afecte a las mujeres de manera desproporcionada», es decir, a actos que tienen como sujeto pasivo a la mujer por el mero hecho de serlo.

Según fuentes oficiales, 243 millones de mujeres y niñas, con edades comprendidas entre los 15 y los 49 años, han sufrido violencia sexual o física por parte de un compañero sentimental, en el último año, a nivel mundial (ONU Mujeres, 2020). Estas cifras se hayan en aumento a raíz del encierro domiciliario al que nos hemos visto avocados, pues se convierte para muchos en el escenario ideal para que afloren comportamientos violentos, controladores, de nerviosismo, ansiedad y discusiones. Estos terminan materializándose y afectando a los seres más cercanos, los convivientes, familiares o no, adultos o menores, con independencia del sexo, si bien, ciertamente, parece que se agudiza sobre el sector femenino. Muestra de ello son los siguientes datos.

En la provincia de Hubei, el corazón del brote inicial de coronavirus, los informes de violencia doméstica de la policía se triplicaron; solo en un condado durante el cierre de febrero, pasaron de 47 del año anterior a 162 (Graham-Harrison, Giuffrida, Smith y Ford, 2020). En Singapur, en el mes de marzo, la asociación AWARE recibió 619 llamadas, la mayor cantidad registrada en un mes en los 29 años de su historia (AWARE, 2020).

En el continente europeo, en Francia, la violencia de género aumentó un 30 % desde el inicio del confinamiento en apenas un mes (*Euronews*, 2020); en Reino Unido, las llamadas a la línea de ayuda contra el abuso doméstico se incrementaron en un 25 % a finales de marzo1 y, en España, si bien el número de denuncias de los dos primeros trimestres del año fue de 34 196 y 34 659, con una leve disminución respecto al mismo período del año

[1] Mohan, M. (31 March 2020): Coronavirus: I'm in lockdown with my abuser, BBC. Recuperado de: https://www.bbc.com/news/world-52063755

anterior (34 256 y 34 297, respectivamente), aumentó el número de llamadas al Teléfono de Atención a la Mujer, lo cual alcanzó las cifras más altas del último año: 6273 en marzo, 8692 en abril y 8414 en mayo (*Epdata*, 2020), y el primer caso de violencia contra la mujer tuvo lugar el 19 de marzo, apenas 5 días después de decretarse el estado de alarma.

En el continente africano, el confinamiento ha hecho proliferar una práctica, habitual en la zona pero que constituye un atentado contra las mujeres, como son las mutilaciones genitales (Plan Internacional, 2020).

Al otro lado del mundo, el panorama es similar. Si bien en Norteamérica los datos son sectoriales, en el sur, por ejemplo, en la Argentina, se constata que se incrementó el número de consultas por cuestiones relacionadas con la violencia contra la mujer en un 39 %, y se registraron 19 feminicidios desde que comenzó el aislamiento2. En condiciones de normalidad, menos del 40 % de las mujeres que sufren violencia solicitan ayuda o denuncian el delito, y menos del 10 % recurren a la policía (ONU Mujeres, 2020).

Las circunstancias creadas por el virus complican esta actuación, en tanto que el contacto estrecho con los agresores dificulta el acceso a teléfonos de atención y las formas de hacer uso de los sistemas de denuncia, obstaculizadas además por la alteración del régimen normal de trabajo de policía, órganos judiciales y servicios sociales. Si bien ante tal situación muchos servicios y colectivos de asistencia han modificado su forma de actuar durante la pandemia —sirva de ejemplo la iniciativa Mascarillas-19, del Colegio Oficial de Farmacéuticos de Canarias, de gran acogida en el resto del país, o su equivalente en Perú, Mascarillas Violetas, impulsado por el Programa de las Naciones Unidas para el Desarrollo (PNUD), los servicios policiales y judiciales no lo han hecho.

En este contexto es donde adquiere relevancia el hecho de que el comportamiento social haya cambiado durante el confinamiento y, sin embargo, el sistema de denuncia de delitos y el mecanismo para evaluar el riesgo, basado en una aplicación informática, no se haya modificado ni adaptado a las circunstancias derivadas de la pandemia.

2. El sistema de valoración del riesgo a la luz de un caso concreto de violencia de género

2.1. Análisis de la Sentencia de la Audiencia Nacional núm. 2350/2020, del 30 de septiembre

Esta Sentencia de la Audiencia Nacional (AN) resolvía el recurso contencioso administrativo 2187/2019, presentado contra la resolución del secretario general técnico del Ministerio del Interior de 9 de septiembre de 2019, en que se desestimaba la reclamación de responsabilidad patrimonial del Estado derivada del asesinato de Stefany

[2] DIARIO 21TV (22 de marzo de 2020). Durante la cuarentena, aumentaron un 25 % los llamados al 144 por violencia de género. Recuperado de: http://www.diario21.tv/notix2/movil2/?seccion=desarrollo_nota&id_nota=132124

González Escarramán, a manos de su esposo, tras haber solicitado la víctima una orden de protección ante la Guardia Civil, que fue denegada.

Los hechos que dan origen a esta resolución datan del 17 de septiembre de 2016, cuando Stefany se persona, de madrugada, en un puesto de la Guardia Civil, con un parte médico de urgencias en que se certifica una agresión y solicita una orden de protección contra su marido, de acuerdo con el artículo 544 ter de la Ley española de Enjuiciamiento Criminal. Horas más tarde, es citada ante el Juzgado de Primera Instancia e Instrucción para celebración de juicio rápido (Libro IV, Título III, Artículos 795 y ss.), fruto del cual se dicta auto que deniega la orden solicitada ese mismo día. La motivación esgrimida en esta resolución judicial es la siguiente:

> La existencia de versiones contradictorias entre ambos esposos, ambos dicen haber sido agredidos por el otro y presentan ambos parte de lesiones, en la carencia de antecedentes penales del denunciado e indica «siendo el riesgo calificado por los agentes de "NO APRECIADO", circunstancias por las cuales no se considera que exista una situación objetiva de riesgo para la denunciante que justifique la adopción de la medida». (Fundamento de Derecho 3) (*Europa Press*, 14 de octubre de 2020)

La resolución de 9 de septiembre de 2019, contra la que se interpone el recurso, desestimó la reclamación de responsabilidad patrimonial de la Administración, presentada al amparo de las Leyes 39/2015 y 40/2015, de 1 de octubre, una vez constatado el requisito de la existencia de un nexo causal entre la muerte y el funcionamiento anormal de la Administración, reflejado en el informe de bajo riesgo elaborado por las autoridades policiales en que no se apreciaron todos los indicadores que reflejaban el peligro existente para la entonces denunciante (Antecedente de Hecho 1).

La sentencia de la AN estima el recurso en cuanto a la concesión de la indemnización destinada a reparar el daño causado por la muerte de Stefany a sus padres e hijos sobre la base de que, si bien las autoridades policiales actuaron de forma correcta, siguiendo el Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad y de coordinación con los órganos judiciales para la protección de las víctimas de violencia doméstica y de género aprobado por la Comisión Técnica de la Comisión Nacional de Coordinación de la Policía Judicial el 28 de junio de 2005, tras haberse adaptado el anterior Protocolo a las modificaciones de la LO 1/2004, de Medidas de Protección Integral contra la Violencia de Género, erraron al realizar la estimación inicial de la situación del riesgo, asignando el nivel más bajo de «no apreciado», que resultó inadecuado a la vista del asesinato de la denunciante, hecho que los protocolos tratan de evitar.

Esta decisión se apoya, además, en el voto particular formulado por la presidenta y tres consejeros al Dictamen del Consejo de Estado, trascrito de manera parcial en la propia Sentencia, que critica dos extremos:

- Por un lado, la inadecuada valoración policial del riesgo, a la luz del contenido del parte de lesiones de la mujer (cuando el marido no aporta ninguno); de la existencia de conductas similares acontecidas con anterioridad, ya que constaba la existencia

de un presunto delito de amenazas aunque la denuncia presentada había sido retirada posteriormente; y de la declaración de la víctima de haber sido obligada a mantener relaciones sexuales con su marido, lo que podría ser constitutivo de un delito contra la libertad sexual.

- Por otro lado, la inaplicación y seguimiento del Protocolo para valorar el nivel de riesgo de violencia de género, dado que no se cumplió el sistema establecido para analizarlo, al no tener en cuenta las autoridades policiales todos los parámetros señalados en este, pues no consta que se indagaran y valoraran los factores relativos a la violencia sufrida por la víctima. En este sentido, no se buscaron testigos ni se recabaron sus posibles testimonios, las relaciones mantenidas con el agresor (posibles relaciones sexuales no consentidas), los antecedentes del propio agresor y su entorno (cuando parece que los tenía, aunque fuera de la jurisdicción española, en República Dominicana, país de origen de la mujer), las circunstancias familiares, sociales, económicas y laborales de la víctima y su agresor (carecía de familiares distintos a los hijos menores en España y sólo comenzó a trabajar poco antes de los hechos), así como la retirada de la denuncia (que constaba), entre otras.

Ello justifica la condena al pago, por parte de la Guardia Civil perteneciente al Ministerio del Interior, a cargo del patrimonio de la Administración del Estado español, de una indemnización por la incorrecta valoración del riesgo a los familiares de la víctima, cuya cuantía se ha cifrado en un total de € 180 000, de los cuales corresponden € 20 000 a cada uno de los progenitores y € 70 000 a cada hijo (Fundamento de Derecho 4).

2.2. Valoración automatizada del riesgo

España cuenta, desde el 2007, con un sistema de evaluación policial del riesgo de reincidencia en casos de violencia de género (Sistema VioGen) que se fundamenta sobre una aplicación informática, que ha incorporado funcionalidades basadas en inteligencia artificial (La Vanguardia, 2020). Se creó para dar cumplimiento al artículo 32 de la Ley 1/2004, de 28 diciembre, de medidas de protección integral contra la violencia de género[3], por Orden INT/1911/2007, de 26 de junio, siendo posteriormente actualizado por Orden INT/1202/2011, de 4 de mayo, como sistema dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior.

La finalidad de este sistema se concreta, por un lado, en realizar valoraciones policiales del riesgo y, en función del riesgo determinado, efectuar un seguimiento y establecer medidas de protección a las víctimas, válidas para todo el territorio nacional, diseñando, en caso necesario, un plan de seguridad con medidas de autoprotección personalizadas,

[3] Esta disposición señala: los poderes públicos elaborarán planes de colaboración que garanticen la ordenación de actuaciones en la prevención, asistencia y persecución de los actos de violencia de género, que deberán implicar a las administraciones sanitarias coma la Administración de Justicia, las fuerzas y cuerpos de seguridad y los servicios sociales y organismos de igualdad.

y, por otro lado, en aglutinar a las diferentes instituciones públicas con competencia en materia de violencia contra las mujeres, integrando la información de interés considerada relevante (Garrido, M. J., 2012). Con ello se persigue hacer frente a la violencia de género con «técnicas policiales de carácter preventivo y anticipativo» (Ministerio del Interior, 2020).

El Sistema VioGen es una plataforma web que se apoya, según afirma López-Osorio en 2016, «en un algoritmo de valoración del riesgo que opera con Inteligencia Artificial y *Big Data*» al que, en su última versión, se sumó otro que elabora una escala predictiva construida a través de datos de homicidio (*La Vanguardia*, 2020). Se trata, de un «sistema informático *online* y multiagencia» al que se conectan miles de usuarios de forma simultánea (González Álvarez, 2016).

La aplicación se encuentra integrada en la intranet de la Administración Pública española, denominada Red SARA (Sistemas de Aplicaciones y Redes para las Administraciones)[4], y enlazada, mediante otros servicios web, con sistemas de información criminal de carácter policial, como el Sistema Integrado de Gestión Operativa, Análisis y Seguridad Ciudadana (SIGO) de la Guardia Civil y el fichero de datos SIDENPOL de la Policía Nacional. Además, se integra a nivel judicial con el Sistema de Registros Administrativos de apoyo a la Administración de Justicia (SIRAJ) y a nivel penitenciario con el Sistema de Gestión de Información Penitenciaria (SIP) y el Sistema de Información Social Penitenciario (SISPE).

VioGen se basa en el análisis permanente del riesgo, lo que implica valorar la peligrosidad de los agresores, la vulnerabilidad de las víctimas y las circunstancias que los rodean de manera individualizada y continuada en el tiempo. La información relativa a estos extremos ha de ser incluida en el sistema para que el mecanismo de inteligencia artificial actúe, para lo cual es necesario cumplimentar los formularios normalizados diseñados al efecto, que se concretan en dos.

El punto de partida lo constituye el primer cuestionario de valoración policial del riesgo de violencia contra la mujer (VPR), que contempla factores de riesgo de tipo histórico, es decir que, por haber ocurrido en el pasado, sirven de base para realizar estimaciones a futuro. Este, a modo de diagnóstico inicial, contempla 39 indicadores de riesgo agrupados en cuatro dimensiones (González Álvarez, 2016, p. 111). El cuestionario debe ser cumplimentado por las autoridades policiales que instruyan las diligencias del caso, nunca por la víctima, siendo el momento de hacerlo, en principio, cuando se denuncian los hechos por primera vez, una vez tomada declaración a la denunciante. El agente de policía ha de indagar, pero sin formular preguntas directas o tendenciosas, sobre los factores de riesgo con los implicados en el caso, es decir, la víctima, el agresor, los testigos, técnicos, facultativos, entre otros. Si por las circunstancias del hecho la instrucción pudiera llevar tiempo, es posible realizar otro VPR tras la finalización de las investigaciones necesarias

[4] La Red SARA es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las administraciones públicas españolas e instituciones europeas y facilita el intercambio de información y el acceso a los servicios.

para dar por finalizadas las diligencias del atestado, pero intentando que entre ambas valoraciones transcurra el menor tiempo posible.

Una vez cumplimentado el VPR, la aplicación VioGen resume las respuestas señaladas y asigna automáticamente uno de los cinco niveles de riesgo previstos, que se clasifican en «no apreciado», «bajo», «medio», «alto» o «extremo», según el riesgo de que se repita a corto plazo un acto de violencia contra la mujer denunciante (Instrucción 4/2019, de 13 de marzo, de la Secretaría de Estado de Seguridad), preguntando al agente si está conforme o no con el resultado automático alcanzado. Este interrogante se plantea dado que esa evaluación puede ser modificada, al alza, por las autoridades de policía que han cumplimentado el cuestionario, si aprecian indicios de riesgo no reflejados en los indicadores del sistema, para lo cual deberá rechazar el resultado indicado y proceder a asignar el nivel que él considera apropiado.

En este sentido, se ha querido afirmar que la estimación del riesgo no descansa en una mera máquina:

> A sabiendas de que es imposible construir en unas pocas frases o indicadores toda la posible casuística que se puede dar entre las decenas de miles de víctimas de agresores y de contextos de pareja, desde su origen en 2007, el protocolo de valoración policial del riesgo no ha pretendido sustituir a los agentes por una máquina, sino facilitarles una herramienta que les ayude en su trabajo diario, asumiendo la importancia que tiene la experiencia profesional, como en cualquier oficio. (González Álvarez, 2016)

El nivel de riesgo asignado determina también el estado en que se encuentra un caso, entendiendo por tal término el que contiene toda la información que relaciona a una víctima con un único agresor, incluidas tantas denuncias como se han registrado (Ministerio del Interior, 2020). Así, el caso estará activo cuando el nivel de riesgo sea «bajo», «medio», «alto» o «extremo», siendo objeto de seguimiento policial. Sin embargo, un caso estará en situación de inactivo cuando se haya calificado como con riesgo «no apreciado», lo que implica que no está siendo objeto de seguimiento policial, al menos temporalmente.

Un caso activo puede pasar a inactivo con independencia del nivel de riesgo con que haya sido calificado si concurren circunstancias que lo promuevan o aconsejen, por ejemplo, la muerte de una de las partes (víctima o agresor) o la salida acreditada, durante un período de tiempo, de alguno de ellos del territorio nacional. A la inversa, un caso inactivo puede activarse si las autoridades son informadas o tienen conocimiento de hechos o circunstancias nuevas o sobrevenidas que lo hagan necesario.

Conviene señalar que el resultado del VPR se debe incluir en el atestado policial en un informe automatizado, haciéndolo constar por diligencia (Fundamento de Derecho 3 de la Sentencia de la AN), con la información relativa a los factores de riesgo apreciados en el caso de que se trate, además de otras circunstancias que hayan podido resultar determinantes en la valoración. Se incluyen también las demás diligencias policiales efectuadas y se comunica a la autoridad judicial correspondiente y, si procede, al Ministerio Fiscal.

Además, el nivel de riesgo establecido supone la puesta en marcha de medidas de protección concretas, adecuadas a este, siguiendo las indicaciones establecidas en el anexo de la Instrucción INT 7/2016, de 8 de julio.

El segundo test de valoración policial de evolución del riesgo (VPER), sobre la base de 43 indicadores, de los cuales 34 son de riesgo y 9 de protección, agrupados en 5 dimensiones (González Álvarez, 2016, p. 112), permite monitorizar los cambios, tras haber presentado una denuncia y durante el seguimiento de la situación de la víctima. Este formulario presenta dos modalidades:

- «Sin incidente», que exige la cumplimentación del cuestionario en unos períodos de tiempo tasados en función del nivel de riesgo determinado en el VPR inicial; oscilan entre las 72 horas para los casos de nivel «extremo», un máximo de 7 días en los supuestos de nivel «alto», cada 30 días cuando el riesgo es «medio» y cada 60 cuando es «bajo», mientras que se puede realizar al año, en la práctica, cuando el nivel de riesgo se calificó como «no apreciado».

- «Con incidente», supone que se ha producido un nuevo hecho violento contra la misma víctima o se ha tenido conocimiento de circunstancias que puedan resultar relevantes a los efectos de los hechos anteriores, si bien también puede solicitarse que sea cumplimentado a instancia del juez o del Ministerio Fiscal.

Únicamente se dará de baja a un caso del sistema, procediendo a suprimir los datos del agresor, cuando se haya dictada sentencia absolutoria firme respecto a este, auto de procesamiento firme, auto firme de archivo de la causa (en fase policial) o sentencia condenatoria firme si la condena ya ha sido ejecutada y ha transcurrido el plazo para proceder a la cancelación de antecedentes penales.

En definitiva, el sistema VioGen, como herramienta de valoración de riesgo, está destinado a realizar, de manera científica, el pronóstico de reincidencia de un agresor identificado y a no cometer errores de valoración, aunque lo que hace, en realidad, son estimaciones (*La Vanguardia,* 2019).

3. Pros y contras del sistema español de valoración del riesgo

Un sistema de valoración de riesgo como VioGen no es perfecto ni está libre de críticas, de ahí que presente ventajas e inconvenientes derivados de su utilización.

Con carácter general, entre sus virtudes se encuentran las propias de utilizar una herramienta basada en tecnología de la información en la lucha contra la violencia de género, por cuanto implica la centralización de información y, por ende, de esfuerzos, la monitorización de las circunstancias que rodean a las víctimas, la combinación de fuentes diversas a la hora de actuar (policiales, judiciales, forenses, sociales) y disponer de análisis de tipo predictivo y preventivo (Cano et al., 2018, p. 2).

De manera más concreta, los defensores de VioGen destacan que se trata de una herramienta cuyo sistema está en continuo proceso de perfeccionamiento, que determina

un nivel de riesgo de agresión sobre la base de unos formularios «de corte más actuarial que de juicio clínico» (Muñoz y López Osorio, 2016) y que integra una «fórmula automática de corrección que pretende reducir la subjetividad de las decenas de miles de evaluadores que lo utilizan», como apunta González Álvarez, añadiendo además el hecho de que España es el único país del mundo en que se utilizan dos formularios de valoración del riesgo (2016, p. 113), lo cual constituye el elemento diferenciador de este sistema de valoración respecto a otros protocolos y permite, así, hacer un seguimiento de los casos a más largo plazo.

La asociación entre la valoración del riesgo y la existencia de un catálogo de medidas de protección de carácter policial, obligatorias y complementarias, si bien no son la clave del sistema, suponen una ventaja añadida en la lucha por hacer frente a la violencia contra las mujeres.

La utilización de este sistema a nivel nacional, es decir, por parte de todos los cuerpos y fuerzas de seguridad de ámbito local, autonómico y estatal, además de contar entre sus usuarios con jueces y fiscales, personal de instituciones penitenciarias, de institutos de medicina legal, de las oficinas de asistencia a las víctimas, de servicios sociales y de organismos de igualdad autonómicos, supone también un valor significativo para tener en cuenta.

Como contrapartida a estos extremos, se pueden señalar diversas críticas. Desde el punto de vista del ámbito de empleo, el hecho de que ni los Mossos d´Esquadra catalanes ni la Ertzaintza policía automática del País Vasco-, por sus peculiares sistemas de competencias, trabajen con este sistema (*La Vanguardia*, 2019) merma la uniformidad pretendida en el entono estatal.

Desde el punto de vista de la técnica para la evaluación de riesgos que se realiza, resulta que es, sin duda, una valoración sofisticada, fundada en muchos parámetros que, si bien resultan útiles, plantean, entre otros, dos inconvenientes.

Por un lado, hay parámetros incluidos en el sistema que carecen de repercusión directa en el riesgo, a la luz de los fallos que las circunstancias han puesto de manifiesto (en el caso de autos, por ejemplo). Si bien los indicadores contenidos en los formularios VPR y VPER no son accesibles, se puede comparar con los utilizados por otros sistemas policiales predictivos sí publicados, como el de Reino Unido, denominado *DASH*. Respecto a este, sustentado sobre un total de 24 preguntas de «sí / no / no sabe», se ha demostrado que no todas las preguntas son requeridas para predecir la revictimización o reincidencia. Según los estudios de Turner, Medina y Brown, sino que la relevancia está, por un lado, en responder «sí» a las preguntas 27 y 9, sobre antecedentes penales del abusador y embarazo reciente de las víctimas; «no sé» a las preguntas 19, sobre comentarios del abusador o comportamientos de naturaleza sexual y 8, sobre el control del comportamiento del abusador; mientras que, si las víctimas responden «sí» a la preguntas 7 o 12, relativas a la existencia de conflicto por el contacto con niños y a si el abusador ha intentado lastimar a niños o dependientes, parece que la predicción se inclina a un menor riego de reincidencia (2019, p. 1027). En definitiva, quizás el empleo de formularios más simples pero centrados en los indicadores correctos podría resultar más eficaz (Dressel y Farid, 2018, p. 3). Por

otro lado, el empleo automático del sistema puede desembocar en artificialidad, como indica el dato, constatado, de la conformidad de los agentes con el resultado automático facilitado por VioGen que suele ser muy alto, en torno al 95 % (Zurita, 2014).

Según este comportamiento, se plantea la duda de si realmente se está dejando el peso de la valoración del riesgo a una máquina, por la rapidez o automatización que supone, quedando relegadas las comprobaciones que deberían realizar las autoridades policiales a un número muy escaso de casos. La literatura científica ha destacado que no debe olvidarse que la evaluación de riesgos está destinada a permitir a los profesionales priorizar los casos de alto riesgo, asignando recursos adicionales donde más se necesita (Turner, Medina, y Brown, 2019, p. 1013).

En este sentido, debe recordarse que, según expresa López Osorio[5], «VioGen no juzga ni los hechos ni a los denunciados ni evalúa ninguna denuncia, simplemente analiza un nivel de riesgo y aconseja las medidas de protección que se han considerado oportunas en función de los datos que tiene. Nada más» (*La Vanguardia*, 2019).

Teniendo en cuenta todo esto, no podemos más que criticar la labor de las autoridades policiales en este extremo; su aparente automatismo al confirmar la valoración del riesgo puede hacer que la toma de decisiones sobre la protección o no de una víctima se sustenten solo en el reporte generado por VioGen. No procede discutir en este trabajo los motivos que puedan ocultarse tras dicho automatismo, pero sí parece oportuno señalar que no todos se deben a una falta de interés de las autoridades policiales, como podría pensarse tras el fallo de la Sentencia de la AN. Ni mucho menos, sino que se encuentran también entre las razones para reflexionar cuestiones como la falta de recursos humanos y materiales, la escasa formación recibida por los encargados de cumplimentar los formularios, el volumen normal de trabajo de las unidades policiales en determinadas zonas territoriales, la presión generada por las horas de trabajo, la necesidad de poner en marcha medidas de protección complejas y costosas según el nivel de riesgo determinado, la cantidad de denuncias falsas que en este tema se interponen, entre otras.

Ahora bien, tampoco podemos pasar por alto que, en el caso de autos, tampoco las autoridades judiciales se percataron de que, a pesar del nivel de valoración del riego determinado por la Guardia Civil, otros datos derivados de las diligencias practicadas en la sesión del juicio podrían hacer pensar que el peligro que corría Stefany era mayor que el indicado en el informe de VioGen. Aunque la Sentencia de la Audiencia Nacional no se refiere a ello, se podría considerar que también sería reprochable la conducta del juez de instrucción, ya que existían indicios que, de haberse valorado, podrían haber dado lugar a una actuación distinta por parte de la judicatura y la fiscalía, quienes parecen haberse limitado a seguir a pies juntillas el resultado del informe automatizado por la herramienta como único mecanismo de valoración. Quizás, en un arrebato de osadía, habría que recomendar la lectura de la propia Sentencia de 30 de septiembre, que dispone lo siguiente:

[5] López-Osorio, J.J., González Álvarez, J.L., y Andrés-Pueyo, A. (2016). Eficacia predictiva de la valoración policial del riesgo de la violencia de género. *Psychosocial Intervention*, 25, 1-7

> El sistema de medición de la intensidad del nivel de riesgo, aunque se trate de la evaluación inicial, da una predicción no sólo para aplicar las medidas de protección policial adecuadas a cada nivel de riesgo, sino que proporciona información relevante a la autoridad judicial […]. La medición policial del riesgo no es decisiva para el juez, pero es información especializada de asesoramiento útil para la valoración de la situación objetiva de riesgo para la víctima que exige la ley procesal en la adopción de medidas cautelares de protección, junto con otros instrumentos de valoración. (Fundamento de Derecho 3)

Todo ello se ve, además, ensombrecido por el hecho de que el uso de esta herramienta, desde su implantación, no parece haber hecho disminuir los incidentes de violencia género, aunque se hayan reducido en algo los casos de reincidencia por este tipo de delitos cometidos por un mismo agresor, dato que, por otro lado, no es fruto únicamente de la valoración del riesgo, sino también de la concurrencia de otras circunstancias, como detenciones, condenas y muertes.

4. Reflexiones pospandemia y conclusiones

Las circunstancias descritas invitan a una reflexión, ya que son aplicables al sistema de valoración del riesgo en cualquier momento temporal, es decir, tanto antes o después de la primera ola de la pandemia de COVID-19 como durante ella. No obstante, con perspectiva retroactiva, me preocupan diversas cuestiones relacionadas con el empleo del sistema VioGen en el período pospandemia.

En primer lugar, si en situaciones de normalidad, a la luz de la Sentencia de la Audiencia Nacional que se pronuncia sobre hechos ocurridos antes de la crisis sanitaria, la actuación policial y judicial adolece de los defectos indicados, desde el levantamiento del confinamiento y de la suspensión de los plazos procesales, se incrementa la tendencia de conductas automáticas de los agentes en el uso de la aplicación informática, amparada, de manera justificada o no, en el volumen de trabajo que la COVID-19 ha generado para la función pública.

En segundo lugar, el propio sistema de valoración del riesgo no incluye, entre sus parámetros de evaluación, indicadores que se refieran a situaciones de crisis generales, pues, como reflejan los datos con los que hemos comenzado este trabajo, queda patente que las consecuencias de una crisis de esta envergadura deberían ser tenidas en cuenta de alguna manera.

En tercer lugar, en España podría trabajarse en una revisión del sistema de valoración del riesgo de violencia de género, actualizando los parámetros de los VPR y VPER, con un doble fin. Inicialmente, se trataría de estudiar los indicadores que tras más de una década de funcionamiento, se hayan mostrado como más determinantes, y, posteriormente, dar cabida a aquellos relacionados con situaciones de confinamiento, limitaciones de movilidad o crisis de carácter más general. Tomando las virtudes arrogadas a la aplicación

VioGen, como una herramienta informática en constante evolución, se podría introducir una o varias variables que pudieran activarse en las situaciones anteriores y permanecer inactivas o fuera de valoración en condiciones de normalidad, quizás procediendo a una especialización de los formularios disponibles.

En cuarto lugar, no se ha previsto, en medio de este contexto, al menos en España, un mecanismo que facilite el acceso efectivo de las víctimas a los sistemas de denuncia. Es cierto que es posible presentar cierto tipo de denuncias por vía electrónica a través de los portales de la Policía Nacional y de la Guardia Civil, como han estudiado Estévez y Cano (2020). Si bien *a priori* podría pensarse que ello constituye una vía para las mujeres en situación de vulnerabilidad, a pesar de tener cerca al agresor, no se ha adaptado el sistema procesal para evitar que las denunciantes tengan que salir posteriormente de sus domicilios para ratificar sus denuncias electrónicas, tal como exige el artículo 268 LECrim.

En definitiva, la necesidad de combatir la violencia contra las mujeres es una prioridad absoluta e irrenunciable de la era actual, sobre la que existe un consenso social y político unánime. Es más, desde todos los niveles, incluida Naciones Unidas, se ha instado a los gobiernos a que hagan de la prevención y la gestión de la violencia contra las mujeres una parte fundamental de sus planes de respuesta nacionales. La crisis sanitaria de este 2020 ha agudizado las lagunas existentes en los sistemas de protección en casos de violencia de género, ahora bien, esto puede servir de motor para actuar en el futuro a corto y medio plazo de forma más eficaz.

5. Bibliografía

Audiencia Nacional. Sentencia 2350/2020, de 20 de septiembre, Sala de lo Contencioso-Administrativo, Sección 5. ECLI: ES:AN:2020:2350.

AWARE (2020): AWARE launches chat service to better support survivors of abuse and violence, Gender-based Violence, News, press Release, May 8th. https://www.aware.org.sg/2020/05/aware-launches-chat-service-to-better-support-survivors-of-abuse-and-violence/

Cano, J. et al. (2018). People-centered system for providing security against gender violence. International Conference for eDemocracy and eGovernement, abril, Quito, Ecuador.

Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica (11 de mayo de 2011). Estambul. BOE núm. 137, de 6 de junio de 2014.

Dressel, J. and Farid, H. (2018). The Accuracy, Fairness and Limits of Predicting Recidivism, Science Advanced, 4, 1-5.

DIARIO 21TV (22 de marzo de 2020). Durante la cuarentena, aumentaron un 25 % los llamados al 144 por violencia de género. Recuperado de: http://www.diario21.tv/notix2/movil2/?seccion=desarrollo_nota&id_nota=132124

Epdata (2020): Violencia de genero. Datos y estadísticas. Recuperado de: https://www.epdata.es/datos/violencia-genero-estadisticas-ultima-victima/109/espana/106

España, Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. BOE núm. 260, de 17/09/1882.

Euronews (28 March 2020). Domestic violence cases jump 30% during lockdown in France». Recuperado de: https://www.euronews.com/2020/03/28/domestic-violence-cases-jump-30-during-lockdown-in-france

Europa Press (14 de octubre de 2020). La Audiencia Nacional condena a Interior por no proteger debidamente a una mujer que fue asesinada por su marido. Recuperado de: https://tinyurl.com/y6gyrqa2

Garrido, M. J. (2012). *Validación del procedimiento de valoración del riesgo de los casos de violencia de genero del con mayúscula Ministerio del Interior de España* [tesis de doctorado]. Facultad de psicología, Universidad autónoma de Madrid, España.

González Álvarez, J. L. (2016). Sistema de Seguimiento Integral de las víctimas de violencia de género, VIOGEN, *IX Jornadas ATIP*, 102-120.

González Álvarez, J. L.; López-Osorio, J. J. y Muñoz Rivas, M. (2018). La valoración policial del riesgo de violencia contra la mujer en pareja en España, Ministerio del Interior, 1-120. Recuperado de: http://www.interior.gob.es/documents/642012/8791743/Libro+Violencia+de+Género/19523de8-df2b-45f8-80c0-59e3614a9bef

Graham-Harrison, E., Giuffrida, A., Smith, H., y Ford, L. (28 March 2020). Lockdowns around the world bring rise in domestic violence. *The Guardian*. Recuperado de: https://www.theguardian.com/society/2020/mar/28/lockdowns-world-rise-domestic-violence

Instrucción 10/2007, de 23 de julio, de la Secretaría de Estado de Seguridad, por la que se aprueba el Protocolo Para la versión policial del nivel de riesgo de violencia contra la mujer en los supuestos de la Ley Orgánica 1/2004 de 28 de septiembre y su comunicación a los órganos judiciales y al Ministerio Fiscal. Recuperada de: https://tinyurl.com/y3n52lu4

Instrucción 7/2016, de 8 de julio, de la Secretaría de Estado de Seguridad, por la que se establece un nuevo Protocolo para la valoración policial del nivel de riesgo de violencia de género y de gestión de la seguridad de las víctimas. Recuperada de: https://tinyurl.com/y2vr7t4k

Instrucción 4/2019, de 6 de marzo, de la Secretaría de Estado de Seguridad, por la que se establece un nuevo Protocolo para la valoración policial del nivel de riesgo de violencia de género (Ley Orgánica 1/2004) y de gestión de la seguridad de las víctimas y seguimiento de los casos a través del sistema de seguimiento integral de los casos de violencia de género (Sistema VioGen). Recuperada de: https://sicol.es/instruccion-numero-4-2019-de-la-ses-sistema-viogen/

La Vanguardia (19 de mayo de 2019). Algoritmos contra la violencia machista. Recuperado de: https://www.lavanguardia.com/tecnologia/20190519/462147339117/viogen-violencia-de-genero-violencia-machista-inteligencia-artificial-algoritmos.html

La Vanguardia (4 de junio 2020): La violencia contra las mujeres: la consecuencia invisible de la pandemia. Recuperado de: https://www.lavanguardia.com/vida/junior-report/20200602/481576160749/violencia-genero-aumenta-coronavirus-pandemia.html

Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. BOE núm. 313, de 29 de diciembre de 2004.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. BOE núm. 236, de 2 de octubre de 2015.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. BOE núm. 236, de 02 de octubre de 2015.

López-Osorio, J. J.; González Álvarez, J. L., y Andrés-Pueyo, A. (2016). Eficacia predictiva de la valoración policial del riesgo de la violencia de género. *Psychosocial Intervention*, 25, 1-7.

Ministerio del Interior (2007). Memoria ejecutiva de situación. Sistema de Seguimiento Integral de los casos de Violencia de Género, 26 de octubre, 1-24.

Ministerio del Interior (2020). Sistema de Seguimiento Integral en los casos de Violencia de Género (Sistema VioGen), enero, 1-20.

Mohan, M. (31 March 2020): Coronavirus: I'm in lockdown with my abuser, BBC. Recuperado de: https://www.bbc.com/news/world-52063755

Muñoz, J. M. y López-Osorio, J. J. (2016). Valoración psicológica del riesgo de violencia: alcance y limitaciones para su uso en el contexto forense. *Anuario de Psicología Jurídica*, 26,130-140.

ONU (20 de abril de 2020). La ONU y Argentina luchan con la otra pandemia del coronavirus, la violencia de género. *ONU Noticias*. Recuperado de: https://news.un.org/es/story/2020/04/1473082

ONU Mujeres (2020). Violencia contra las mujeres: la pandemia en la sombra, 6 de abril, https://www.unwomen.org/es/news/stories/2020/4/statement-ed-phumzile-violence-against-women-during-pandemic#notes

Plan Internacional (21 de mayo 2020): Aumentan los casos de mutilación genital femenina «puerta a puerta» en Somalia durante el confinamiento. Recuperado de: https://plan-international.es/news/2020-05-21-aumentan-los-casos-de-mutilacion-genital-femenina-puerta-puerta-en-somalia-durante

Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad y de coordinación con los órganos judiciales para la protección de las víctimas de violencia doméstica y de género. Recuperado de: https://tinyurl.com/yyzpp6cy

Orden INT/1911/2007, de 26 de junio, por la que se crea el fichero de datos de carácter personal «Violencia doméstica y de género», en el Ministerio del Interior. BOE núm. 155, de 29 de junio de 2007.

Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior BOE núm. 114, de 13 de mayo de 2011.

Turner, E., Medina, J. y Brown, G. (2019). Dashing Hopes? The predictive accuracy of domestic abuse risk assessment by police, *British Journal of Criminology*, 59, 1013-1034.

Zurita, J. (2013). La lucha contra la violencia de género. *Seguridad y ciudadanía. Revista del Ministerio del Interior*, 9, 63-127.

Zurita (2014). *Violencia contra la mujer. Marco histórico evolutivo y predicción del nivel de riesgo* [tesis de doctorado]. Facultad de Psicología, Universidad Autónoma de Madrid, España.