

Desafíos actuales en materia de seguridad y lucha contra el crimen organizado. Tres aristas: seguridad y derechos humanos, ciberseguridad y control de armas

Serie Informes Nº 07-22, 12-05-2022

por Víctor Soto Martínez

Resumen

Este trabajo tiene por objeto sistematizar una serie de problemas relacionados con la seguridad en el siglo XXI. Así, en su primera sección se fija el marco del problema, indicándose los diversos desafíos actuales en materia de seguridad nacional e internacional. Asimismo, se busca ponderar esta mirada con la óptica de los derechos humanos. La segunda sección, en tanto, analiza con mayor detalle el problema de la ciberseguridad, por tratarse de una cuestión emergente a la que los últimos gobiernos le han dedicado un gran énfasis. La tercera sección, por otro lado, se interna en el tráfico de armas y, especialmente, en el marco jurídico del control de armas en Chile, y busca identificar –a partir de la literatura existente– los flancos débiles de esta política y sus puntos críticos. Finalmente, la cuarta sección aborda principios generales para enfrentar las tres aristas señaladas: la criminalidad transnacional en general y su penetración en vastos sectores de la población a raíz de los acelerados cambios sociales de los últimos años; la ciberseguridad y el reforzamiento del Estado para enfrentar los delitos informáticos; y eventuales medidas para reforzar el control de armas y evitar su desvío.

Disclaimer: Este trabajo ha sido elaborado a solicitud de parlamentarios del Congreso Nacional, bajo sus orientaciones y particulares requerimientos. Por consiguiente, sus contenidos están delimitados por los plazos de entrega que se establezcan y por los parámetros de análisis acordados. No es un documento académico y se enmarca en criterios de neutralidad e imparcialidad política.

TABLA DE CONTENIDOS

Antecedentes.....	3
1. Nuevos desafíos en materia de seguridad.....	3
1.1. Los cambios en el escenario internacional	3
1.2. Los desafíos actuales para la seguridad.....	5
2. El desafío de la ciberseguridad	9
2.1. Marco normativo	10
2.2. Proyectos de ley en el Congreso para mejorar nuestra legislación	10
2.3. Política nacional sobre ciberseguridad	16
3. Tráfico de armas.....	17
3.1. Marco jurídico internacional	18
3.2. Marco jurídico nacional	21
3.3. Críticas a la institucionalidad chilena.....	23
4. Principios generales para enfrentar los desafíos de la seguridad pública	25
4.1. Derechos humanos y seguridad pública: una falsa dicotomía	25
4.2. Reforzamiento del Estado de Derecho y la democracia	26
4.3. Cooperación internacional	27
4.4. Enfrentar las causas del problema: la desigualdad.....	28
4.5. En materia de ciberseguridad	28
4.6. En materia de tráfico de armas	29

Antecedentes

Este trabajo tiene por objeto sistematizar una serie de problemas relacionados con la seguridad en el siglo XXI. Así, en su primera sección se fija el marco del problema, indicándose los diversos desafíos actuales en materia de seguridad nacional e internacional. Asimismo, se busca ponderar esta mirada con la óptica de los derechos humanos. La segunda sección, en tanto, analiza con mayor detalle el problema de la ciberseguridad, por tratarse de una cuestión emergente a la que los últimos gobiernos le han dedicado un gran énfasis. La tercera sección, por otro lado, se interna en el tráfico de armas y, especialmente, en el marco jurídico del control de armas en Chile, y busca identificar –a partir de la literatura existente– los flancos débiles de esta política y sus puntos críticos. Finalmente, la cuarta sección aborda principios generales para enfrentar las tres aristas señaladas: la criminalidad transnacional en general y su penetración en vastos sectores de la población a raíz de los acelerados cambios sociales de los últimos años; la ciberseguridad y el reforzamiento del Estado para enfrentar los delitos informáticos; y eventuales medidas para reforzar el control de armas y evitar su desvío.

1. Nuevos desafíos en materia de seguridad

En primer lugar, debemos hacer dos puntualizaciones. Primero, en el contexto de un mundo globalizado, no es posible resolver los problemas de seguridad con una mirada exclusivamente nacional, sino que debe incorporarse necesariamente una **mirada regional y global**. En otras palabras, para ser efectivo, el análisis de la seguridad debe ir acompañado idealmente de un *análisis geopolítico*. Esto se debe a que, más que nuevos desafíos, lo que enfrentamos en la actualidad son problemas que se vienen arrastrando desde hace varios años y que se han agudizado producto de las diversas crisis que está enfrentando el mundo –y, en particular, nuestra región–, así como por las nuevas tecnologías que han generado mayores niveles de organización del crimen transnacional.

En segundo lugar, cabe señalar que la seguridad no es un problema que pueda ser totalmente escindido o aislado de otros problemas existentes en la región, como las crisis institucionales que están atravesando los diversos países americanos y el consiguiente debilitamiento del *ethos* democrático en América Latina. Como se verá en este informe, se trata de problemas que se influyen mutuamente. En este sentido, la respuesta institucional a la crisis no puede estar centrada exclusivamente en un criterio pragmático de efectividad a corto plazo en la lucha contra la delincuencia, sino que debe articularse con una **visión ético-política** enfocada en el *desarrollo* y el *fortalecimiento institucional* de nuestros países.

1.1. Los cambios en el escenario internacional

Después de la Guerra Fría vino un periodo de reajuste de las fuerzas geopolíticas, que estuvo marcado por la presión estadounidense para pasar desde un mundo bipolar a

un mundo unipolar. Sin embargo, después del ataque a las Torres Gemelas (2001) y las subsiguientes guerras contra Afganistán e Irak, la hegemonía estadounidense empezó a debilitarse. En particular, tras la crisis económica de 2008, generada por la implosión del mercado financiero de Estados Unidos, dicho país pasó a enfocarse con mayor fuerza en sus problemas internos, lo que llevó a un reposicionamiento de las fuerzas geopolíticas. En paralelo, vino el surgimiento de nuevas potencias económicas, como Brasil, la India, China y Rusia (los llamados "BRICs") y, especialmente, el avance de China hacia posiciones hegemónicas en el ámbito económico y político, por lo que se ha sostenido que actualmente vivimos en un **mundo multipolar** o con múltiples actores¹.

Al mismo tiempo, se puede argumentar que la globalización ha pasado de ser una potencialidad a una realidad efectiva, que no sólo ha tenido consecuencias económicas sino también políticas. La globalización genera grandes desplazamientos de personas, que migran desde las economías más empobrecidas –y, por consiguiente, menos seguras- a las economías más desarrolladas. Esto se refleja especialmente en la actual **crisis de refugiados**, que no afecta sólo a países que han vivido situaciones bélicas extremas (como en el caso de Siria o, más recientemente, Ucrania), sino también a países con una deteriorada situación económica, política o social (como ocurre particularmente en Centroamérica y el Caribe o, en los últimos años, en Venezuela).

Otro factor relevante a tener en cuenta es el proceso de **cambio climático**, que también ha contribuido al empobrecimiento de vastas zonas del planeta y el consiguiente desplazamiento de grandes grupos de personas. En este contexto, se puede intuir que surgirán nuevas disputas en torno al uso de ciertos recursos naturales (por ejemplo, el agua) lo que podría redundar en posibles enfrentamientos bélicos². Esto da cuenta, además, de la crisis del sistema económico que se ha implementado en los últimos cuarenta años.

A estos factores habría que agregar, finalmente, la guerra. Por una parte la guerra que actualmente se está llevando a cabo entre Rusia y Ucrania (y que pone en entredicho el equilibrio internacional post Guerra Fría). Por otra, la soterrada **guerra comercial** entre Estados Unidos y China, que refleja las tensiones de los cambios geopolíticos apuntados más arriba, y donde los países más afectados podrían ser los países subdesarrollados o en vías de desarrollo.

¹ ROJAS ARAVENA, Francisco. "Chapter 4. Peace and Security in Latin America: New Challenges, New Directions", en el libro: OSWALD, Ursula y SERRANO, Serena (editoras). *Risks, Violence, Security and Peace in Latin America: 40 years of the Latin American Council of Peace Research (CLAIP)*, Springer International Publishing, 2018, pp. 55-59.

² Un ejemplo dramático de este desarrollo es el conflicto de Darfur, en Sudán, que se desarrolló en paralelo con la guerra civil entre el sur y el norte de dicho país, y terminó en un armisticio firmado el año 2007 (acuerdo de Doha). Una de las causas de este conflicto, además de las tensiones étnicas, fue la disputa por los recursos hídricos de la región. Es decir, aquí tenemos un ejemplo claro de una crisis multidimensional provocada, en parte, por escasez de recursos naturales.

1.2. Los desafíos actuales para la seguridad

A continuación se detallan los desafíos que conlleva el nuevo escenario mundial descrito en el apartado anterior.

1.2.1. Terrorismo³

Este ha sido un problema permanente para la política internacional, especialmente con posterioridad al ataque a las Torres Gemelas del año 2001. Así, el sociólogo Ulrich Beck ponía en su momento el acento en las nuevas características organizativas de estas redes terroristas transnacionales, de las cuales afirmaba que “son en cierto modo ‘ONGs de la violencia’. Operan como organizaciones no gubernamentales, desterritorializadamente, descentralizadamente, es decir por un lado localmente y, por otro, transnacionalmente. [...] las ONGs terroristas desbancan el monopolio estatal de la violencia, cosa que significa, en primer lugar, que esta clase de terrorismo transnacional no está ligado al terrorismo islámico, sino que puede unirse con todos los objetivos, ideologías y fundamentalismos posibles”⁴.

En vista de estas características del fenómeno, no es sorprendente que el terrorismo tenga alcances globales, en tanto ninguna zona del mundo se encuentra completamente inmune a su impacto. De acuerdo al estudio anual que realiza el *Institute for Economics and Peace (IEP)*, el terrorismo sigue siendo un fenómeno relevante, aunque su impacto global ha disminuido sostenidamente desde su *peak* el año 2015. Así, durante 2021 se contabilizaron 7.142 muertes por acciones de este tipo en un total de 44 países (es decir, un tercio menos de muertes que el año 2015 y en la mitad de países)⁵.

Pero, además, han surgido dos manifestaciones preocupantes en los últimos años. Por un lado, las guerras promovidas por la administración de George W. Bush en Estados Unidos, provocaron una reacción que amalgamó **acciones bélicas y terroristas en Oriente Medio**. Así, el Estado Islámico se constituyó en los últimos años en una fuente de riesgo para los países árabes y para Europa. Si bien actualmente –tras una larga guerra en Siria- este grupo pareciera estar neutralizado, el surgimiento de un nuevo tipo de guerra, que combina el clásico conflicto bélico focalizado territorialmente con formas de terrorismo no sujetas a un espacio territorial

³ Esta sección, al igual que el punto 1.2.3, está tomada –con las debidas actualizaciones- del trabajo de FERRERO, Mariano. *Cooperación internacional en la lucha contra el terrorismo y el crimen transnacional organizado*, Serie Informes N° 26-18, Departamento de Estudios, Extensión y Publicaciones, Biblioteca del Congreso Nacional (BCN), Santiago de Chile, 19-12-2018.

⁴ BECK, Ulrich, *Sobre el terrorismo y la guerra*, Editorial Paidós, México D. F., 2001, pp. 28-29; citado por Amar Díaz, Mauricio, *La lucha contra el terrorismo en América Latina*, Serie Informes n° 67-13, Departamento de Estudios, Extensión y Publicaciones, Biblioteca del Congreso Nacional (BCN), Santiago de Chile, 15-11-2013, pp. 2-3.

⁵ INSTITUTE FOR ECONOMICS & PEACE, *Global Terrorism Index 2022: Measuring the Impact of Terrorism*, Sydney, 2022, p. 2. Disponible en: <http://visionofhumanity.org/resources> [consultado el 11-05-2022]

determinado, plantea una preocupación para la seguridad global. Lo mismo puede decirse del conflicto que estalló en Ucrania el año 2014, que dio pie a que algunos autores hablaran incluso de una *guerra híbrida*⁶, es decir, un conflicto que puede ser conducido tanto por actores estatales como por actores no-estatales y que incorporaría “un amplio rango de modos de guerra, incluyendo capacidades militares convencionales, tácticas y formaciones irregulares, actos terroristas –entre los que se cuentan la coerción y violencia indiscriminada-, y desorden criminal”⁷. Este conflicto se encuentra entre los antecedentes de la actual guerra entre Rusia y Ucrania, que también ha sido calificado por algunos como una guerra híbrida⁸.

Por otro lado, también se ha visto el surgimiento de múltiples **acciones terroristas cometidas por supremacistas blancos**, muchos de ellos defensores de una ideología fascista o neonazi. Su expresión más dramática fueron los atentados de Noruega (2011), que terminaron en la muerte de 77 personas. Estos atentados tuvieron como motivación el rechazo al multiculturalismo y la islamofobia. En el mismo sentido, se han realizado atentados en Nueva Zelanda (2019, 51 muertos), así como varios atentados más acotados en Estados Unidos, pero que se han multiplicado en los últimos años.

1.2.2. Amenazas de la era digital y ciberterrorismo

Otro foco de preocupación es el llamado **ciberterrorismo**, es decir, el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en la población. El uso de este tipo de terrorismo podría agudizarse en los próximos años a medida que avance la tecnología y el desarrollo de la Inteligencia Artificial (IA). En particular, es de preocupación el uso malicioso de los datos privados de las personas y el *hackeo* de entidades bancarias y financieras.

Sin embargo, incluso antes de llegar al ciberterrorismo, existen amenazas concretas a la seguridad ligadas al avance tecnológico. Por ejemplo, los intentos de **manipulación política** a través de la propagación de noticias falsas, a lo que tecnologías nuevas como el *deep fake* (reemplazo de rostro en medios audiovisuales) pueden contribuir sobremanera. Igualmente, se ha constatado el **uso de los datos personales** de los usuarios de Facebook y otras redes sociales para influir en el comportamiento electoral, y la filtración de datos sensibles, como correos electrónicos,

⁶ Véase: ORTIZ, Román. “El concepto de guerra híbrida y su relevancia para América Latina”, Revista Ensayos Militares, vol. 1, N° 2, 2015, p. 136. Véase también: OVIEDO, Nicolás. “Guerra híbrida: circunvalando la lógica nuclear”, Perspectivas Revista de Ciencias Sociales, Año 4, N° 7, 2019, p. 84.

⁷ HOFFMAN, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, 2007, p. 14. La traducción es mía. Disponible en: https://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf [consultado el 11-05-2022]

⁸ BBC, “Rusia-Ucrania: qué es una “guerra híbrida” y por qué se habla de este concepto a raíz del conflicto entre los dos países” (08-02-2022), por Fernanda Paúl. Disponible en: <https://www.bbc.com/mundo/noticias-internacional-60230360> [consultado el 11-05-2022]

para atacar a candidatos opositores, entre otros⁹. Por otra parte, es de preocupación la debilidad de los algoritmos de algunas redes sociales, como YouTube, que han sido acusados de propagar la pedofilia¹⁰.

Ahondaremos en este tema cuando tratemos la ciberseguridad en Chile (punto 2).

1.2.3. Crimen organizado transnacional¹¹

En los últimos años, las organizaciones criminales han dado un salto hacia una actuación a escala mundial, aprovechando las oportunidades y rutas de negocio que se abren con los avances en los transportes y comunicaciones así como a partir de la liberalización de los mercados internacionales. De esta forma, han combinado estas nuevas oportunidades con las viejas actividades ilícitas asociadas a rutas de contrabando, y han aprovechado también la desregulación financiera para el blanqueo de dinero de las operaciones ilegales.

Ahora bien, un estudio de la Oficina de Naciones Unidas contra la Droga y el Delito (ONUDD) señala que, antes que centrarse en los grupos que cometen los hechos -que sufren frecuentes cambios en su organización y composición- habría que centrarse en "los mercados [ilegales] en los cuales ellos se involucran". En consecuencia, se entiende que, a día de hoy, el crimen organizado es, fundamentalmente, "una cuestión de un grupo de actividades ilícitas en las cuales algunos individuos y grupos están actualmente involucrados"¹².

Así, habría que poner atención en la escala, crecientemente transnacional, en que operan estos mercados ilegales a fin de entender y actuar eficazmente sobre los "problemas de crimen organizado", identificándose la operatoria de diversas actividades económicas ilegales, a saber:

a) la **trata de personas**, en que se ven involucradas en parte significativa mujeres que son trasladadas a otros países con fines de explotación sexual, pero también otras formas de explotación laboral; en términos generales, traficantes y víctimas suelen tener la misma nacionalidad;

b) el **tráfico de migrantes**, inducido por las desigualdades globales y las políticas restrictivas de migración, lleva a que organizaciones criminales presten "asistencia" a migrantes que buscan burlar los controles migratorios de países de

⁹ BBC, "Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios" (24-07-2019). Véase: <https://www.bbc.com/mundo/noticias-49093124> [consultado el 11-05-2022]

¹⁰ BBC, "El escándalo de pedofilia que afecta a YouTube tras la denuncia de Matt Watson y por el que grandes marcas están retirando su publicidad de la plataforma" (22-02-2019). En: <https://www.bbc.com/mundo/noticias-47331814> [consultado el 08-10-2019]

¹¹ Esta sección está tomada -con las debidas actualizaciones- del trabajo de Mariano Ferrero, ya citado (ver nota 3).

¹² ONUDD, *The Globalization of Crime. A Transnational Organized Crime Threat Assessment*, United Nations Office on Drugs and Crime (UNODC / ONUDD), New York / Vienna, 2010, p. 3.

destino; en las Américas, el flujo más significativo tiene lugar de América Latina a América del Norte, especialmente desde México y Centroamérica a los Estados Unidos;

c) el **tráfico de recursos medioambientales**, por una parte para el traslado ilegal de desechos peligrosos y, por otro, para recoger de manera ilícita ciertos recursos naturales como especies protegidas, madera y peces; las principales rutas estudiadas por la ONUDD no tienen relación con las Américas;

d) el **tráfico de drogas**, con sus principales productos -cocaína, heroína- cuya incidencia es particularmente significativa para las Américas en relación con la cocaína, cuyos principales flujos vinculan a América del Sur con América del Norte y a la región andina, en concreto, con Europa;

e) el **tráfico de armas** que, si bien presenta flujos más acotados, tiene como uno de sus principales mercados aquel que se genera entre los Estados Unidos, como mercado proveedor, y México;

f) el **tráfico de productos falsificados**, que constituye una forma de fraude a los consumidores, y constituye una práctica extendida a nivel global, aprovechando las técnicas propias de la deslocalización industrial; y

g) la **piratería marítima**, cuyo epicentro actual se encuentra en la zona del cuerno de África; entre otros.

Frente a esto, el principal instrumento internacional –suscrito por Chile- es la *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional* (Resolución 55/25 de la Asamblea General, de 15 de noviembre de 2000) que establece, entre otras cosas, deberes de cooperación internacional, de penalización de la participación en grupos delictivos organizados, de blanqueo de dinero y de corrupción de funcionarios públicos.

En este punto, cabe detenerse un poco en el narcotráfico, una preocupación creciente en el país¹³. El último plan nacional en la materia fue dictado el año 2014, durante el gobierno de Michelle Bachelet, y se denominó *Plan Nacional contra el Narcotráfico (2014–2020)*. El plan operó en dos niveles, microtráfico y narcotráfico, y tenía por principal objeto contener el ingreso de drogas al país y desarticular las organizaciones criminales que trafican y realizan delitos conexos como el lavado de activos¹⁴. Para ello se establecieron siete principios orientadores: coordinación,

¹³ DW, "Narcotráfico en Chile: más violencia y temor en la población" (Victoria Dannemann, 05-10-2020). Disponible en: <https://www.dw.com/es/narcotr%C3%A1fico-en-chile-m%C3%A1s-violencia-y-temor-en-la-poblaci%C3%B3n/a-55162801> [consultado el 11-05-2022]

¹⁴ GOBIERNO DE CHILE, *Plan Nacional contra el Narcotráfico (2014–2020)*, 2015. P. 7. Disponible en: https://www.subinterior.gob.cl/media/2018/03/plan_narcotrafico_FINAL_23_11_15.pdf [consultado el 11-05-2022]

cooperación internacional, territorialidad¹⁵, multidimensionalidad¹⁶, conocimiento¹⁷, evaluación y probidad, que regularon transversalmente las diferentes líneas de acción fijadas por el gobierno. Desde el término de este Plan no se han vuelto a fijar políticas nacionales en la misma línea, aunque sí se han implementado planes acotados a territorios concretos, como el *Plan anti bandas, armas y narcotráfico*, elaborado por el gobierno de Sebastián Piñera y que se concretizó en el aumento de efectivos policiales en 50 lugares críticos de la Región Metropolitana¹⁸.

1.2.4. Corrupción

Finalmente, es preciso mirar la corrupción de los gobiernos como una de las principales amenazas a la seguridad de los países. La corrupción aparece tanto como síntoma y como causa de las nuevas manifestaciones de criminalidad ya revisadas. Así, por un lado, se podría decir que se nutre de la imbricación, cada vez más evidente en el contexto neoliberal, de la política y los negocios, fomentada por las privatizaciones, la desregulación y la circulación del capital global. Por otro lado, alimenta la penetración de nuevas formas de criminalidad, y desestabiliza a las instituciones políticas que podrían hacer frente a dichos problemas: "La corrupción, en cualquiera de sus tipos, impacta negativamente los indicadores de seguridad ciudadana, porque – al debilitar, socavar, neutralizar o penetrar a las instituciones de la seguridad – contribuye al incremento de la actividad criminal y de la percepción de inseguridad"¹⁹. Este problema es particularmente agudo en la región, donde hemos presenciado últimamente la **desestabilización de diversos países**, lo cual hace retornar a su vez el fantasma del autoritarismo y el militarismo en América Latina.

2. El desafío de la ciberseguridad

Como señalamos más arriba, nos enfocaremos especialmente en este tema, ya que es una de las aristas más novedosas del problema de seguridad en el mundo, y Chile ha dado ciertos pasos para abordarlo que es preciso tener en cuenta, sobre todo en el marco de un nuevo gobierno y un nuevo ciclo legislativo.

¹⁵ *Ibíd.*, p. 9. Es entendida como adecuación al carácter nacional, regional, local o barrial del fenómeno.

¹⁶ *Ibíd.* Se busca mediante este principio abordar las diversas dimensiones que hacen al narcotráfico un fenómeno complejo, en particular sus consecuencias sociales, económicas y criminales.

¹⁷ *Ibíd.* Se refiere a la obligación de identificar, sistematizar, aprender, adaptar y evaluar las mejores prácticas llevadas a cabo en estos temas por otros países, tanto de la región como del resto del mundo.

¹⁸ El Mostrador, "Presidente Piñera presenta nuevo "Plan anti bandas, armas y narcotráfico": estará focalizado en 15 comunas de la RM" (14-10-2021), disponible en: <https://www.elmostrador.cl/dia/2021/10/14/presidente-pinera-presenta-nuevo-plan-anti-bandas-armas-y-narcotrafico-estara-focalizado-en-15-comunas-de-la-rm/> [consultado el 11-05-2022]

¹⁹ COSTA, Gino. "Seguridad ciudadana y delincuencia organizada transnacional en las Américas: situación y desafíos en el ámbito interamericano", Revista SUR, Vol. 9, N° 16, 2012, p. 146-147.

2.1. Marco normativo

2.1.1. Convenio de Budapest

En primer lugar, cabe señalar que nuestro país suscribió hace algunos años el *Convenio sobre la Ciberdelincuencia del Consejo de Europa*, conocido como el "Convenio de Budapest", que entró en vigor el 1 de julio de 2004 y que, a la fecha de suscripción por parte de Chile (2016), había sido ratificado por cuarenta y siete Estados. Este convenio fue ratificado por el Congreso y publicado, finalmente, en el Diario Oficial el 28 de agosto de 2017.

El principal objetivo del convenio es el desarrollo de una política criminal común frente al ciberdelito por parte de los diversos países suscriptores, mediante tres vías principales: a) la homologación de la legislación penal sustantiva; b) el mejoramiento de las capacidades nacionales para la investigación de este tipo de delitos, según el derecho procesal de cada país; y c) el establecimiento de un sistema rápido y eficaz de cooperación internacional.

2.1.2. Ley N° 19.223

Sin perjuicio de lo anterior, Chile cuenta con una legislación sobre la materia que, si bien en su momento fue considerada como pionera en América Latina, actualmente se encuentra bastante desactualizada, sobre todo a la luz de lo dispuesto en el Convenio de Budapest. Se trata específicamente de la ley N° 19.223, que tipifica figuras penales relativas a la informática.

En particular, dicha ley tipifica las siguientes conductas:

a) la destrucción o inutilización maliciosa de un sistema de tratamiento de información, sus partes o componentes, así como el impedimento, obstaculización o modificación de su funcionamiento;

b) la interceptación, interferencia o acceso a un sistema de tratamiento de la información realizada con el ánimo de apoderarse, usar o conocer indebidamente la información en él contenida;

c) la alteración, daño o destrucción de los datos contenidos en un sistema de tratamiento de información; y

d) la revelación o difusión maliciosa de los datos contenidos en un sistema de información.

2.2. Proyectos de ley en el Congreso para mejorar nuestra legislación

2.2.1. Mociones de parlamentarios

	N° Boletín	Fecha de Ingreso	Cámara de Origen	Etapa	Nivel de urgencia	Fundamento
1	9998-07	15 de abril de 2015	Cámara de Diputados	Primer trámite constitucional	Sin urgencia	Para solucionar el desfase de la legislación respecto del avance tecnológico se incorpora un nuevo artículo a la ley N°19.223, calificando como delito informático la producción, venta, distribución, exhibición, por cualquier medio web de material pornográfico en cuya elaboración hayan sido utilizados menores de edad, aunque el material tuviere su origen en el extranjero o fuere desconocido, y la facilitación de dichas conductas
2	10145-07	18 de junio de 2015	Cámara de Diputados	Primer trámite constitucional	Sin urgencia	Ante el desfase de la ley N° 19.223 con el desarrollo tecnológico de los últimos años, el proyecto aborda las normas penales materiales que tipifican y sancionan las acciones que

						atentan contra los derechos de las personas en materia informática, y también en algunas normas de carácter procesal penal, con el fin de facilitar y hacer más eficiente la investigación y sanción de dichos delitos.
3	10979-07	16 de noviembre de 2016	Senado	Primer trámite constitucional	Sin urgencia	Se busca tipificar el daño informático, entendido como "todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".
4	11214-07	3 de mayo de 2017	Senado	Primer trámite constitucional	Sin urgencia	La tipificación del delito de usurpación de nombre es anacrónica y no se encuentra actualizada a las nuevas maneras de relaciones interpersonales establecidas por la computación a través de

						Internet y las redes sociales.
5	11801-07	7 de junio de 2018	Cámara de Diputados	Primer trámite constitucional	Sin urgencia	A partir del caso de Katherine Winter ²⁰ , se busca incorporar a la ley N° 19.223 el delito de hostigamiento u acoso reiterado por redes sociales.

2.2.2. Mensaje del Presidente de la República, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest (Boletín 12192-25)

FICHA TÉCNICA				
N° Boletín	Fecha de Ingreso	Cámara de Origen	Etapa	Nivel de urgencia
12192-25	25 de octubre de 2018	Senado	Aprobado en tercer trámite constitucional. En vista de no haber sido objeto de observaciones por parte del Presidente de la República, se encuentra actualmente bajo control de constitucionalidad por el Tribunal Constitucional	---

Como se indica en el mensaje, este proyecto de ley deroga la ley N° 19.223, con el objeto de establecer una ley especial que contenga de manera integral las

²⁰ Adolescente que se suicidó el año 2018 por el hostigamiento que sufrió por redes sociales.

nuevas formas delictivas surgidas a partir del desarrollo de la informática. Así "se pretende llenar los vacíos o dificultades que ha tenido nuestro ordenamiento penal en la persecución de ciertas conductas que, incluso, no eran concebibles a la época de dictación de la ley N° 19.223".

En particular, se introducen las siguientes modificaciones sustantivas:

a) Se modifica el tratamiento que se entrega actualmente al **sabotaje y espionaje informático**, adecuándolos a las figuras penales reconocidas en el Convenio de Budapest, a saber: acceso ilícito a todo o parte de un sistema informático, ataque a la integridad del sistema y de los datos informáticos (arts. 2, 4 y 5 del mentado Convenio). Esto se encuentra recogido a grandes rasgos en los actuales artículos 1 y 2 del proyecto, sobre ataque a la integridad de un sistema informático y acceso ilícito, respectivamente.

b) Se agrega el delito de **interceptación ilícita**, para quien indebidamente intercepte, interrumpa o interfiera las transmisiones no públicas entre sistemas informáticos, así como la **captación ilícita** de datos transportados mediante emisiones electromagnéticas de sistemas informáticos, en concordancia con el art. 3 del Convenio de Budapest. Esto se encuentra recogido en el actual artículo 3 del proyecto.

c) Se incorpora el delito de **falsificación informática**, que comprende la indebida introducción, alteración, daño o supresión de datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos (en concordancia del art. 7 del Convenio de Budapest). Esto se encuentra en el art. 5 del proyecto.

d) Se añade el delito de **receptación de datos personales** respecto de quien "conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos" obtenidos a partir de un ataque ilícito (art. 2), interceptación ilícita (art. 3) o falsificación informática (art. 5).

e) Se incorpora, también, el delito de **fraude informático** respecto de quien manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, siempre que esto: i) cause perjuicio a otro; ii) se lleve a cabo deliberada e ilegítimamente y iii) con la finalidad de obtener un beneficio económico. Aquí se aprecia una diferencia importante con el Convenio de Budapest, introducida durante el segundo trámite constitucional, ya que, al perjuicio y al carácter indebido e ilegítimo de la acción, se añade la finalidad de obtener un beneficio económico, lo que en el art. 8 del referido convenio, sólo configura una de las hipótesis de este delito. Esto se estaría consagrando en el art. 7 del proyecto.

f) Se propone tipificar el llamado **abuso de los dispositivos**, es decir, a quien entregare u obtuviere para su utilización, importare, difundiere o realizare otra forma

de puesta a disposición un dispositivo, programa computacional, contraseña, código de acceso, o datos informáticos similares, que permitan acceder a todo o parte de un sistema informático, creados o adaptados principalmente para la perpetración de los delitos establecidos en los artículos 1 a 4 (ataque a la integridad del sistema, acceso ilícito, interceptación ilícita y ataque a la integridad de los datos informáticos). Esto está en conformidad con el art. 6 del Convenio de Budapest y se traduce en el actual art. 8 del proyecto. Cabe mencionar que, durante la tramitación legislativa, se explicitó que este delito se aplica también a propósito del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas (art. 7 de la ley N° 20.009).

Además, se agregan circunstancias modificatorias de responsabilidad penal, ya sea para atenuar o agravar la misma (arts. 9 y 10 respectivamente).

Por otra parte, se modifican algunas normas procesales, con el objeto de mejorar la persecución e investigación de estos delitos, también en la línea del Convenio de Budapest. En particular, los cambios más relevantes son:

i) Se concede **legitimación activa** al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y delegados presidenciales provinciales cuando las conductas afecten servicios de utilidad pública (art. 11 del proyecto).

ii) Se permite el uso de **técnicas especiales de investigación** (como agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones) cuando existan sospechas fundadas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley, previa autorización judicial, por cierto (art. 12).

iii) Se fija una regla especial de **comiso**, relacionada con los instrumentos del delito informático, los efectos y demás utilidades que se hubieran originado, o una suma de dinero equivalente (art. 13).

Cabe mencionar, además, que durante la tramitación se agregó un nuevo artículo 16, titulado "investigación académica", donde se establece que no será considerado ilegítimo el acceso a un sistema informático que no provoque daño o perturbación y tenga la finalidad de investigar o detectar sus vulnerabilidades, siempre y cuando quien lo realice reporte inmediatamente sus hallazgos a la autoridad competente y, de ser posible, al responsable del sistema informático. Con este artículo se subsana "uno de los puntos en discusión durante el trámite del proyecto, sobre la legitimidad de las actividades de búsqueda de vulnerabilidades del "hacking ético", siempre que se dé cuenta de los hallazgos inmediatamente"²¹.

²¹ ROBERTS, Raimundo. "Proyecto de ley sobre delitos informáticos (N° de Boletín 12192-25). Estado del proyecto de ley al 1 de diciembre de 2020", SUP 129249, Biblioteca del Congreso Nacional, 2020, p. 6.

2.3. Política nacional sobre ciberseguridad

2.3.1. Elementos de continuidad en la política pública

El año 2015 se creó el Comité Interministerial sobre Ciberseguridad (mediante decreto supremo N° 533, de 2015, del Ministerio del Interior), órgano que tiene como principales funciones asesorar del Presidente de la República en el análisis y definición de la política nacional de ciberseguridad (art. 2, a) y analizar la legislación vigente aplicable en materia de ciberespacio, proponiendo las modificaciones constitucionales, legales y reglamentarias que sean necesarias (art. 2, d), entre otras.

A partir del trabajo realizado por dicho comité, el año 2017 se dio a conocer la *Política Nacional de Ciberseguridad 2017-2022*, con medidas a corto plazo (2017-2018) y objetivos a largo plazo (2022). Estos objetivos a largo plazo son, a grandes rasgos, los siguientes:

1. Que el país cuente con una infraestructura de la información robusta y resiliente (es decir, con la capacidad de mantener una continuidad operacional a pesar de las fallas), preparada para resistir y recuperar de incidentes de ciberseguridad.

2. Que el Estado vele por los derechos de las personas en el ciberespacio, lo que implica la prevención de ilícitos y el establecimiento de prioridades en la implementación de medidas sancionatorias, entre otras medidas.

3. Desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de las tecnologías digitales.

4. Establecer relaciones de cooperación en ciberseguridad con otros actores y participar activamente en foros y discusiones internacionales.

5. Promover el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

Como se ve, se trata de objetivos generales, relacionados con la seguridad de las instituciones públicas, con bastante énfasis en la prevención y en el desarrollo de políticas de formación y sensibilización en el tema de la ciberseguridad. Sin embargo, no se incorporan medidas directas para mejorar la legislación penal (aunque el problema sí se menciona, a propósito del establecimiento de prioridades en la implementación de medidas sancionatorias²²).

Buscando cierta continuidad con la política nacional establecida por el gobierno de Michelle Bachelet, el gobierno de Sebastián Piñera desarrolló una *Estrategia Gubernamental sobre Ciberseguridad 2018-2022*²³.

²² Gobierno de Chile, Política Nacional de Ciberseguridad, p. 19. Puede consultarse en línea: <https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf>

²³ Se delinea básicamente a partir del instructivo presidencial N° 008, de 2018, sobre ciberseguridad. La estrategia puede consultarse en línea:

Entre las medidas concretas propuestas figura la tipificación de nuevos delitos informáticos en consonancia con la Convención de Budapest y la mejora procesal de la prueba del delito, lo que pudimos comprobar en el punto anterior.

2.3.2. Proyecto de ley marco

Asimismo, se mencionó el envío de un proyecto de Ley Marco sobre Ciberseguridad, que finalmente se concretizó el día 2 de marzo del presente año, mediante el Boletín N° 14.847-06. Este proyecto –actualmente bajo la revisión de la Comisión de Defensa Nacional, del Senado- establece, entre otras cosas, una serie de principios para los órganos de la Administración del Estado en materia de ciberseguridad y se incorpora el concepto de infraestructura crítica de la información, así como las obligaciones de las instituciones que poseen dicha infraestructura.

En cuanto a las innovaciones institucionales, cabe destacar también la creación de una Agencia Nacional de Ciberseguridad. Este será, de acuerdo con el texto del mensaje, un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado. Su objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en la materia de ciberseguridad, y regular y fiscalizar las acciones de los órganos de la Administración del Estado y privados que no se encuentren sometidos a la competencia de un regulador o fiscalizador sectorial que posean infraestructura crítica de la información. La Agencia se relacionará con el Presidente de la República por intermedio del Ministerio del Interior y Seguridad Pública, y tendrá su domicilio en la ciudad de Santiago, sin perjuicio de contar con oficinas en otras regiones del país. Su dirección y administración estará a cargo de un Director Nacional, y constituirá un servicio afecto al Sistema de Alta Dirección Pública. Cabe señalar, por último, que el proyecto fue desarrollado por el *Equipo de Respuesta ante Incidentes de Seguridad Informática* (CSIRT, por sus siglas en inglés), equipo dependiente de la Subsecretaría del Interior, del Ministerio del Interior, creado el año 2018 y que se encuentra regulado en la Resolución Exenta N° 5.006, de 2019²⁴.

3. Tráfico de armas

Este es un tema de gran relevancia, ya que el tráfico de armas constituye actualmente uno de los principales problemas de seguridad en el mundo y las armas de fuego “contribuyen decisivamente en la violencia, especialmente en los homicidios, cumplen con frecuencia un papel fundamental en la delincuencia organizada y amplifican la

<https://mba.americaeconomia.com/sites/mba.americaeconomia.com/files/s3e4-jorgeatton-confyn2018.pdf>

²⁴ Véase: <https://www.csirt.gob.cl/media/2019/09/RES.-EXENTA-N-5006-CREACION-DE-DIVISION-Y-UNIDAD.pdf> [consultado el 25-06-2021]

incidencia de los conflictos armados y el terrorismo”²⁵. Para dimensionar esto, cabe señalar que el año 2014 se estimaba que tan sólo la circulación global de armas pequeñas y ligeras era superior a 875 millones en 178 países, de los cuales 22.7% estaban en manos de las Fuerzas Armadas; 2.2% en manos de las Fuerzas Públicas (policías); 0.5% en manos del crimen organizado y rebeldes; y 74.6% en manos de civiles. Estas cifras, se estimaba en la época, tenderían a aumentar exponencialmente en los años sucesivos (ya que la fabricación de armas excede por mucho el número de armas destruidas)²⁶.

En su último estudio sobre el tráfico de armas de fuego, la Oficina de Naciones Unidas contra la Droga y el Delito (en adelante, UNODC), reuniendo respuestas de 81 países y otras fuentes, determinó que fueron incautadas un total de 550.000 armas de fuego en cada año de 2016 y 2017. Por cierto, como el mismo estudio aclara, la cifra real de incautaciones a escala mundial debe ser muy superior. Así, se indica que algunos de los países incluidos en dicho estudio no notificaron las incautaciones que se debían a motivos administrativos, y la calidad de los datos también varió considerablemente entre los países. Además, muchos países no proporcionaron ninguna información, incluidas algunas de las naciones más pobladas del mundo²⁷.

El elevado tráfico de armas se puede asociar con el porcentaje de delitos violentos. Así, como señala el estudio citado, “los países con los niveles de muertes violentas y homicidios más altos, en particular África y América Latina y el Caribe, tienden a incautar un mayor porcentaje de armas de fuego vinculadas con delitos violentos. Asimismo, los países que registran los niveles de tráfico de drogas más elevados también incautaron más armas de fuego vinculadas a esta actividad ilícita”²⁸.

Estos datos dan cuenta de la relevancia de que los Estados implementen políticas para minimizar el riesgo de desvío de transferencias de armas. Así, a continuación sintetizaremos los principales instrumentos internacionales en la materia (1), así como su correlato a nivel interno en Chile (2). Posteriormente, se indicarán tanto las críticas a nuestra legislación actual como las posibles medidas que podrían implementarse para mejorarla y minimizar estos riesgos (3).

3.1. Marco jurídico internacional

3.1.1. Protocolo contra la fabricación y el tráfico ilícitos de armas de fuego, sus piezas y componentes y municiones, que complementa la

²⁵ Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), *Estudio Mundial sobre el Tráfico de Armas de Fuego*, 2020 (publicación de las Naciones Unidas, No. E.20.IV.1), p. 2.

²⁶ GACITÚA, Alejandro. “Tráfico de Armas Pequeñas y Ligeras: aspectos generales, marco jurídico internacional y Proyecto de Informe de Eurolat”, Serie Minutas Nº 92-17, Biblioteca del Congreso Nacional, 2017, p. 3. Los datos están tomados de aquí: <http://www.copa.qc.ca/esp/comisiones/Democracia-Paz/documents/Presentation-Consoli-2014.pdf> [consultado el 16-11-2021]

²⁷ Oficina de Naciones Unidas contra la Droga y el Delito (UNODC). Op. Cit., p. 6.

²⁸ Ibid., pp. 7-8.

Convención de las Naciones Unidas contra la delincuencia organizada transnacional

Este es el primer instrumento de alcance universal sobre la materia, adoptado el año 2001 y aprobado por nuestro Congreso el año 2010. Tiene por objeto "promover, facilitar y reforzar la cooperación entre los Estados Parte con el propósito de prevenir, combatir y erradicar la fabricación y el tráfico ilícitos de armas de fuego, sus piezas y componentes y municiones" (art. 2).

En cuanto a la desviación de transferencias de armas, su artículo 11, referido a las medidas de seguridad y prevención, dispone la obligación de cada Estado Parte de adoptar medidas apropiadas para:

"a) Exigir que se garantice la seguridad de las armas de fuego, sus piezas y componentes y municiones en el curso de su fabricación, de su importación y exportación y de su **tránsito** a través de su territorio, y

b) Aumentar la eficacia de los **controles de importación, exportación y tránsito**, incluidos, cuando proceda, los controles fronterizos, así como de la cooperación transfronteriza entre los servicios policiales y aduaneros."

3.1.2. Tratado sobre el comercio de armas de las Naciones Unidas

Este tratado es actualmente el documento más relevante sobre la materia en el plano del derecho internacional. Fue adoptado el año 2013 y aprobado por el Congreso Nacional el año 2018.

Aquí el problema del desvío de transferencias de armas se encuentra mucho más enfatizado, ya que está incorporado en su objeto. Así, de conformidad con el artículo 1, el tratado busca: "establecer normas internacionales comunes lo más estrictas posibles para regular o mejorar la regulación del comercio internacional de armas convencionales"; y "prevenir y eliminar el tráfico ilícito de armas convencionales y **prevenir su desvío**". Acto seguido se declara que sus fines son contribuir a la paz, la seguridad y la estabilidad en el ámbito regional e internacional; reducir el sufrimiento humano; y promover la cooperación, la transparencia y la actuación responsable de los Estados partes en el comercio internacional de armas convencionales, fomentando así la confianza entre ellos.

En cuanto a las medidas específicas para prevenir el desvío, el artículo 11 establece que cada Estado parte que participe en una transferencia de armas convencionales²⁹ tomará medidas para evitar su desvío. Para ello, el Estado parte

²⁹ De acuerdo con el artículo 2, el tratado se aplica a todas las armas convencionales comprendidas en las categorías siguientes:

- a) Carros de combate;
- b) Vehículos blindados de combate;
- c) Sistemas de artillería de gran calibre;
- d) Aeronaves de combate;
- e) Helicópteros de ataque;
- f) Buques de guerra;

exportador aplicará un **sistema nacional de control**, incluida una **lista nacional** de control, evaluando el riesgo de que se desvíe la exportación y examinando la posibilidad de establecer medidas de mitigación, como medidas de fomento de la confianza o programas elaborados y acordados conjuntamente por los Estados exportador e importador. Tanto los Estados partes importadores como los exportadores, los de tránsito y de transbordo **cooperarán entre sí e intercambiarán información**, a fin de mitigar el riesgo de desvío.

Por otro lado, si un Estado parte detecta el desvío de una transferencia de armas, tomará las medidas necesarias para hacerle frente a ese desvío. Tales medidas podrán consistir en alertar a los Estados partes potencialmente afectados, examinar los envíos desviados de dichas armas convencionales y adoptar medidas de seguimiento en materia de investigación y cumplimiento.

El artículo, asimismo, alienta a los Estados partes a que compartan entre ellos información pertinente sobre medidas eficaces para hacer frente a los desvíos. Esta información podría incluir datos sobre actividades ilícitas, incluida la corrupción, rutas de tráfico internacional, intermediarios ilegales, fuentes ilícitas de suministro, métodos de ocultación, puntos comunes de envío o destinos utilizados por grupos organizados que se dedican al desvío.

El artículo 18 dispone la creación de una **Secretaría**, cuyas principales funciones son recibir, distribuir y poner a disposición de los Estados partes los informes anuales que hagan estos sobre las medidas adoptadas para aplicar el tratado, incluidas las leyes nacionales, las listas nacionales de control y otros reglamentos y medidas administrativas (art. 13), así como mantener y poner a disposición de los Estados partes la lista de puntos de contacto nacionales para intercambiar información sobre cuestiones relacionadas con la aplicación del tratado (art. 5). En este sentido, es la Secretaría la que canaliza la información que compartan los Estados partes sobre medidas eficaces para hacer frente a los desvíos (art. 11). También se hace cargo de los temas administrativos vinculados con la organización de las reuniones previstas para su implementación. Cabe señalar que este órgano ha sido establecido fuera del sistema de Naciones Unidas, por lo que ni la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA) ni la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) tienen supervisión directa sobre los tratados bajo su auspicio³⁰. Su sede se encuentra ubicada físicamente en Ginebra, Suiza³¹.

Por otro lado, se contempla la realización de conferencias de los Estados partes (art. 17), las que, en la práctica, se han ido organizando anualmente. Así, en el marco

-
- g) Misiles y lanzamisiles; y
 - h) Armas pequeñas y armas ligeras.

³⁰ OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO (UNODC). "Documento de debate: El Protocolo sobre armas de fuego y el Tratado sobre el comercio de armas: ¿divergencia o complementariedad?", Naciones Unidas, Viena, 2016, p. viii.

³¹ Véase: <https://thearmstradetreaty.org/staff-and-contact.html> [consultado el 16-11-2021]

de la Sexta Conferencia de los Estados partes, se creó el *Foro de Intercambio de Información sobre Desvíos*, un órgano *sui generis* para intercambios informales entre los Estados partes y los Estados signatarios relacionado con casos concretos de desvío detectados o sospechados, así como para el intercambio de información concreta y operativa sobre desvíos. Este órgano se reúne hasta dos veces por año y pueden asistir todos los Estados parte interesados en debatir y compartir información operativa sobre casos concretos de desvío³².

3.2. Marco jurídico nacional³³

3.2.1. Ley de control de armas. Revisión general

En Chile el control de armas está regulado en el decreto N° 400, de 1978, del Ministerio de Defensa Nacional, que fija el texto refundido, coordinado y sistematizado de la **ley N° 17.798, sobre control de armas** (en adelante, ley de control de armas). Cabe mencionar que esta ley fue modificada el año 2015 por la ley N° 20.813.

Según la ley de control de armas, la supervigilancia y el control de las armas le compete a la **Dirección General de Movilización Nacional**, órgano dependiente del Ministerio de Defensa Nacional. Este órgano actúa como **autoridad central de coordinación** de todas las **autoridades ejecutoras y contraloras** que correspondan a las **comandancias de guarnición** de las Fuerzas Armadas y autoridades de Carabineros de Chile³⁴ y, asimismo, de las autoridades asesoras que correspondan al Banco de Pruebas de Chile y a los servicios especializados de las Fuerzas Armadas, en los términos previstos en la ley y su reglamento (artículo 1°).

El artículo 2° establece que esta tutela se aplica a los siguientes elementos:

- a) material de uso bélico;
- b) armas de fuego de diverso calibre, con sus partes, dispositivos y piezas;
- c) municiones y cartuchos;
- d) explosivos y artefactos afines, de uso industrial o minero;
- e) las sustancias químicas susceptibles de ser usadas o empleadas para la fabricación de explosivos;

³² Véase: GRUPO DE TRABAJO SOBRE TRANSPARENCIA Y PRESENTACIÓN DE INFORMES DEL TRATADO DE COMERCIO DE ARMAS. "Términos de Referencia (TdR) relativos al Foro de Intercambio de Información sobre Desvíos", 2020, p. 2. Disponible en: [https://thearmstradetreaty.org/hyper-images/file/ATT_DIEF%20Terms%20of%20Reference%20\(stand%20alone\)_EN/ATT_DIEF%20Terms%20of%20Reference%20\(stand%20alone\)_EN.pdf](https://thearmstradetreaty.org/hyper-images/file/ATT_DIEF%20Terms%20of%20Reference%20(stand%20alone)_EN/ATT_DIEF%20Terms%20of%20Reference%20(stand%20alone)_EN.pdf) [consultado el 17-11-2021]

³³ Esta sección se basa y toma diversos elementos del siguiente documento de asesoría técnica parlamentaria: JARUFE, Juan Pablo. "El control de armas en la legislación nacional y extranjera", Biblioteca del Congreso Nacional, 2019.

³⁴ El Reglamento Complementario (decreto N° 83, de 2008, del Ministerio de Defensa Nacional), en su artículo 11, especifica el rol de las comandancias de guarnición de las Fuerzas Armadas o a Carabineros de Chile como entidades fiscalizadoras de lo establecido en la ley de control de armas.

- f) los fuegos artificiales, artículos pirotécnicos y otros artefactos de similar naturaleza, sus partes, dispositivos y piezas;
- g) las instalaciones destinadas a la fabricación, armadura, prueba, almacenamiento o depósito de estos elementos; y
- h) las armas basadas en pulsaciones eléctricas, tales como los bastones eléctricos o de electroshock y otras similares.

Enseguida, el artículo 3º prohíbe a las personas "poseer o tener armas largas cuyos cañones hayan sido recortados, armas cortas de cualquier calibre que funcionen en forma totalmente automática, armas de fantasía, entendiéndose por tales aquellas que se esconden bajo una apariencia inofensiva; armas de juguete, de fogeo, de balines, de postones o de aire comprimido adaptadas o transformadas para el disparo de municiones o cartuchos; artefactos o dispositivos, cualquiera sea su forma de fabricación, partes o apariencia, que no sean de los señalados en las letras a) o b) del artículo 2º, y que hayan sido creados, adaptados o transformados para el disparo de municiones o cartuchos; armas cuyos números de serie o sistemas de individualización se encuentren adulterados, borrados o carezcan de ellos; ametralladoras, subametralladoras; metralletas o cualquiera otra arma automática y semiautomática de mayor poder destructor o efectividad, sea por su potencia, por el calibre de sus proyectiles o por sus dispositivos de puntería".

El mismo acápite prohíbe la posesión, tenencia o porte de artefactos diseñados a partir de gases asfixiantes, paralizantes o venenosos; sustancias corrosivas; bombas, o artefactos explosivos o incendiarios; y armas de fabricación artesanal o que hayan sido adulterados, sin previa autorización de la Dirección General de Movilización Nacional.

La norma excluye de estas restricciones a las Fuerzas Armadas y a Carabineros de Chile. En tanto, la Policía de Investigaciones de Chile, Gendarmería de Chile y la Dirección General de Aeronáutica Civil, se encuentran exceptuadas sólo respecto de la tenencia y posesión de armas automáticas livianas y semiautomáticas, y de disuasivos químicos, lacrimógenos, paralizantes o explosivos y de granadas, hasta la cantidad que autorice el Ministro de Defensa Nacional, a proposición del Director del respectivo Servicio. El uso de estas armas y elementos debe ceñirse a lo dispuesto en el Reglamento Orgánico y de Funcionamiento Institucional.

Por otro lado, existe un tipo de armas sobre las cuales pesa una prohibición absoluta, ya que nadie está autorizado legalmente para poseer las llamadas "armas especiales", que corresponden a las de naturaleza química, biológica o nuclear. Asimismo, el artículo 6º descarta la posibilidad de que las personas porten armas de fuego sin permiso de la autoridad, salvo en el caso de los aspirantes a oficiales de Carabineros y la Policía de Investigaciones, que cursen tercer año en sus respectivas escuelas matrices; los deportistas; los cazadores; y los vigilantes privados que cumplan con los requisitos estipulados en el Reglamento de la ley.

Cabe señalar que la Dirección General de Movilización Nacional debe mantener actualizado un **Registro Nacional de Inscripciones de Armas** (art. 5). Esta inscripción faculta al titular del arma a preservar el artefacto en el bien raíz que ha declarado como residencia o sitio de trabajo. En caso de modificación de domicilio, debe avisar a la autoridad fiscalizadora correspondiente.

3.2.2. Medidas contra el desvío

Como se puede apreciar, las normas sobre tenencia de armas en Chile son bastante rigurosas, y su control se encuentra centralizado en la Dirección General de Movilización Nacional, aunque un grupo importante de las entidades fiscalizadoras (Carabineros de Chile) no se encuentra, en rigor, bajo su dependencia administrativa, sino del Ministerio del Interior.

Ahora bien, respecto del desvío de transferencias de armas, esta ley no cuenta con medidas específicas. Sin embargo, en su reglamento (decreto N° 83, de 2008, del Ministerio de Defensa Nacional) se establecen requisitos rigurosos para la adquisición y transferencia de las armas de fuego. Así, el artículo 47 de este texto legal se refiere específicamente a dichas transacciones al prohibir a toda persona natural o jurídica, la venta, compra, enajenación, adquisición, cesión o recepción en arriendo, préstamo, prenda o depósito sobre estos artefactos, sin haber obtenido con anterioridad los permisos a que se refiere dicho reglamento.

De todos modos, en caso de trato directo entre comerciantes, el artículo 49 de dicho texto reglamentario considera la opción de que la autoridad fiscalizadora conceda una **Autorización de Compra e Inscripción**, con el detalle de la clase de arma, calibre y casa comercial donde se realizará el intercambio. En tanto, el artículo 51 dispone que las ventas, consumos o compras que efectúen los fabricantes, armadores, importadores, consumidores habituales y comerciantes deban ser rebajados de los inventarios por las respectivas autoridades fiscalizadoras. La Dirección General de Movilización Nacional debe determinar los elementos sometidos a control que deberán ser informados a las autoridades fiscalizadoras mediante el **Informe Mensual de Movimiento Comercial**. Los elementos que se mencionen en dicho informe deben venir identificados. Este informe mensual debe ser entregado a la autoridad fiscalizadora durante los primeros cinco días del mes siguiente de realizadas las actuaciones (art. 52). El no cumplimiento o mal uso de estas reglas es motivo suficiente para que la autoridad fiscalizadora, por medio de una resolución fundada, suspenda, condicione o limite la autorización de inscripción otorgada, como también deniegue su renovación anual (art. 53).

3.3. Críticas a la institucionalidad chilena

Como indica la profesora de derecho Myrna Villegas, pareciera ser que el cumplimiento de las obligaciones internacionales respecto del control de armas en Chile "dista

mucho de ser satisfactorio³⁵. En este sentido, la Contraloría General de la República descubrió el año 2017 graves irregularidades en torno al control de las armas por parte de las autoridades encargadas. Así, por ejemplo, al auditar al Departamento de Control de Explosivos de la Zona de Seguridad Privada, Control de Armas y Explosivos de Carabineros (Zosepcar), detectó que las bases de armas inscritas estaban desactualizadas desde 2011 y había alrededor de 128 millones de pesos en pagos a externos³⁶.

Luego, en diciembre de 2017, la Contraloría emitió el **Informe Final de «Auditoría al proceso de control de armas y municiones destinadas al uso del personal de Carabineros de Chile»** que comprendió el periodo que abarca desde el 1 enero al 31 diciembre de 2016. En él se detectaron incumplimientos a la normativa de armas que afectan la eficacia del **control de las existencias** de armas y municiones. En particular, se denunció «una serie de diferencias entre la cantidad de elementos registrados en el sistema de inventarios de la institución y el conteo físico de las mismas» lo que motivó la instrucción de un sumario administrativo, una investigación judicial en la Sexta Fiscalía Militar de Santiago, y una denuncia ante la justicia ordinaria en la Fiscalía Metropolitana Sur³⁷.

En su síntesis de lo detectado por el informe de Contraloría, la profesora Villegas indica las siguientes falencias de control:

i) la ausencia de una numeración única y archivo exclusivo de los informes técnicos elaborados por el Departamento L.5 sobre armas particulares, lo cual no permite constatar ni identificar la cantidad de armas personales utilizadas en fines institucionales;

ii) inconsistencias en la información y la no inclusión de una copia del acta en los estados comprobatorios de consumo de munición, lo que, a juicio de la Contraloría, no permitiría «validar que el Departamento L.5 haya recibido las especies físicas informadas como utilizadas o deterioradas por parte de las unidades policiales, lo cual redundaría en información desactualizada en el inventario»;

iii) diferencias entre la información consignada en actas suscritas por la Comisión Administrativa de Armamento y Municiones de la Escuela de Suboficiales respecto de lo informado por la repartición en el estado comprobatorio;

iv) desfase entre el uso efectivo de las municiones y su confirmación a la sala de armas; entre otras³⁸.

A juicio del ente contralor, sería imposible «contar con información oportuna y completa de especies, el destacamento al cual se circunscriben y las personas a cargo de las mismas con el consiguiente riesgo de control asociado a su porte y uso» (CGR,

³⁵ VILLEGAS, Myrna. "Corrupción y criminalidad organizada. Aproximaciones al terrorismo, contraterroterrorismo y tráfico de armas", Revista de Estudios de la Justicia, N° 28, 2018, p. 70.

³⁶ *Ibíd.*

³⁷ Contraloría General de la República, Informe 532/2017. Citado En: VILLEGAS, Myrna. Op. Cit., p. 70.

³⁸ *Ibíd.*

Informe 532/2017, p. 20). Todas estas situaciones «podrían redundar en la pérdida de los bienes asignados a las reparticiones» (CGR, Informe 532/2017, p. 25)³⁹.

En otras palabras, se evidencia una falla en los registros y en los inventarios de las armas en posesión de las autoridades fiscalizadoras, lo que puede ser muy perjudicial para el cumplimiento de los objetivos de la ley, y contribuye a horadar la confianza pública en el sistema nacional de control de armas.

Por otro lado, la profesora Villegas critica una gran falencia del sistema chileno: la **falta de marcaje de las municiones** (lo que se encontraría en desavenencia con el estándar internacional). En el mismo sentido, la profesora critica que –luego de la modificación de la ley de control de armas del año 2015– la venta de municiones sea sancionada sólo con pena de multa: “La laxitud de control de armerías, municiones y la falta de marcación en las del Estado son un factor criminógeno favorable a la corrupción y al tráfico de las mismas como se demostrado en más de algún caso en el que se han visto armerías involucradas, clubes de tiro e incluso funcionarios de FF.AA.”⁴⁰.

4. Principios generales para enfrentar los desafíos de la seguridad pública

4.1. Derechos humanos y seguridad pública: una falsa dicotomía

Vistas ya las actuales amenazas a la seguridad es necesario que abordemos el problema de fondo: la relación entre la seguridad y los derechos humanos.

Aquí lo primero que debe señalarse es que ambos conceptos se necesitan mutuamente. La seguridad es parte del entramado de la defensa de los derechos humanos en cualquier sociedad. Algunos, incluso, llegan a plantearla como una precondition para el ejercicio de estos derechos⁴¹. En realidad, podríamos sostener que **la seguridad está al servicio del fortalecimiento de los derechos humanos** de las personas. Es este mismo carácter subordinado, lo que nos puede llevar a afirmar que es un contrasentido sacrificar los derechos humanos por la seguridad.

Así, es preciso advertir en contra de la falsa dicotomía que contrapone los derechos y la seguridad en los debates sobre este tema. Según algunos autores esta es una construcción mediática orientada hacia la configuración de una “política del miedo”, que tiene por objeto la hiper-inflación de las amenazas contra la seguridad para justificar el resurgimiento del autoritarismo, la restricción de las libertades y el

³⁹ *Ibíd.*, p. 71.

⁴⁰ *Ibíd.*, p. 72. La autora alude al siguiente caso: Valentina de Marval, «Efecto dominó: Testimonio de un narco llevó a destapar tráfico de armas entre ex GOPE, un militar y un civil», *The Clinic*, 28 de febrero de 2017, disponible en <https://www.theclinic.cl/2017/02/28/efecto-dominio-testimonio-narco-llevo-destapar-trafico-armas-ex-gope-militar-civil/> [consultado el 17-11-2021].

⁴¹ ROJAS ARAVENA, Op. Cit., p. 75.

debilitamiento de la democracia⁴². En el mismo sentido, Jeremy Waldron ha argumentado que muchas de las medidas lesivas hacia los derechos humanos que se aplicaron como reacción a la amenaza terrorista en Estados Unidos desde el año 2001 en adelante, tuvieron poca eficacia práctica, pero generaron “la sensación de que algo sorprendente e inusual se estaba realizando”; en otras palabras, que muchas veces las medidas lesivas a los derechos humanos sólo tienen efectividad en el nivel simbólico⁴³.

Además, la securitización en muchas ocasiones va de la mano con mayores niveles de discrecionalidad para la policía, que es justamente uno de los actores que gran parte de la población en los países latinoamericanos mira con desconfianza, sobre todo en el marco de la crisis de corrupción señalada en el apartado anterior. Por lo tanto, no parece razonable que esta sea considerada como una opción válida para el enfrentamiento de las nuevas amenazas de la criminalidad en nuestra región.

En definitiva, las medidas que se tomen para enfrentar las nuevas amenazas deberían seguir una regla básica: **circunscribirse dentro del respeto a los derechos humanos**, entre los cuales se cuentan el respeto a la intimidad y la privacidad de las personas y el debido proceso, entre otros.

4.2. Reforzamiento del Estado de Derecho y la democracia

Como se señaló en el punto 1, la corrupción socava las instituciones públicas de cualquier país. Ella no es producto de acciones aisladas sino que se nutre de un clima o un ambiente institucional de impunidad y falta de regulación. Por lo tanto, uno de los primeros problemas que se deberían abordar en esta materia es el **problema institucional**. Los países de la región deberían reforzar la ética pública y sancionar los actos que la contravengan. Pero, para que ello resulte, se debe tener en cuenta un plan que abarque desde la educación (formación ciudadana) hasta la reforma de las instituciones policiales (transparencia, profesionalización) y judiciales (aseguramiento de su independencia), con el objeto mediato de profundizar la democracia. Esto podría realizarse, además, con una mayor participación ciudadana en la gestión pública, favoreciendo la rendición de cuentas (*accountability*). En este mismo sentido, Rojas Aravena reitera la idea de reforzar el Estado de Derecho como parte clave del enfrentamiento a las nuevas formas de criminalidad. Reforzar el Estado de Derecho implica la disminución de la discrecionalidad de las autoridades, o, en otras palabras, **asegurar la estricta sujeción al derecho de policías, fiscales, jueces y funcionarios públicos** en general.

Por otra parte, a partir de los diversos acuerdos y documentos internacionales que hemos revisado en este trabajo, podemos señalar que las medidas debieran darse en

⁴² LAZARUS, Liora y GOOLD, Benjamin. “Security and Human Rights: Finding a Language of Resilience and Inclusion”, en: *Security and Human Rights (second edition)*, Hart, Oxford, 2019, p. 1.

⁴³ WALDRON, Jeremy. “Security and Liberty: The Image of Balance”, *The Journal of Political Philosophy*, Volume 11, Number 2, 2003, p. 209 y ss.

diversos niveles: i) en la prevención de los delitos; ii) en su investigación y sanción y iii) en la rehabilitación o reinserción social de los condenados. Todos estos ámbitos requieren una mirada y una atención específicas, pero incorporadas dentro de una visión de conjunto. Si tomamos como ejemplo el caso de los sobornos a funcionarios extranjeros, nuestro país ha avanzado exitosamente en la tipificación de esta conducta, pero –según el Grupo de Trabajo de la OCDE– tendría un desempeño insuficiente en su aplicación práctica en, al menos, dos de estos tres niveles⁴⁴. Así, se ha constatado, por un lado, una deficiencia en los modelos de prevención de delitos dentro de las empresas (en lo relativo al punto i), y, por otro, debilidades en la fiscalización, vacíos legales en la responsabilidad de las personas jurídicas, debilidad en la investigación por parte del Ministerio Público, pocas condenas –en realidad, un tratamiento que contrasta con la persecución de delitos comunes y genera una sensación de impunidad en cuanto a los delitos de cuello y corbata–, y poco uso del decomiso de bienes (en lo relativo al punto ii)⁴⁵. Este es sólo un ejemplo de las deficiencias institucionales actuales en materia de lucha contra la corrupción en nuestro país.

4.3. Cooperación internacional

Los diversos autores revisados son coincidentes en sostener que una medida clave para enfrentar las amenazas a la seguridad es la cooperación internacional. Efectivamente, como vimos en el punto 1, los principales problemas vienen dados por la criminalidad transnacional, por lo que la **coordinación entre diversos gobiernos y policías** vendría a ser clave en la persecución de estos delitos. Cabe señalar que esto es parte de los consensos reflejados en la *Declaración sobre Seguridad en las Américas*, de la OEA (2003), que en su punto III incluso detalló una serie de compromisos y acciones de cooperación. Sin embargo, hasta el día de hoy subsiste la dificultad de realizar una coordinación efectiva de los países de la región, lo que se ve graficado, en el caso de Sudamérica, en la debilidad del anterior órgano de cooperación internacional, UNASUR, y la falta de consenso para la configuración de un nuevo órgano en su reemplazo.

En segundo lugar, es importante **reforzar en los diversos frentes la ayuda jurídica mutua** entre los países de la región. Si bien esto también está presente en una serie de tratados y acuerdos multilaterales, como la *Convención OCDE para combatir el cohecho de servidores públicos extranjeros*, se han constatado dificultades para implementar adecuadamente estas medidas (lo que se denota, por ejemplo, en la burocracia de algunos países, la falta de coordinación de su legislación interna, la falta de capacitación de los actores encargados de la persecución de los delitos, etc.).

⁴⁴ SOTO, Víctor. *El rol del Congreso chileno en la lucha contra la corrupción: la Convención OCDE para combatir el cohecho de servidores públicos extranjeros*, Serie Minutas N° 131-19, Departamento de Estudios, Extensión y Publicaciones, Biblioteca del Congreso Nacional (BCN), Santiago de Chile, 26-09-2019.

⁴⁵ *Ibíd.*

4.4. Enfrentar las causas del problema: la desigualdad

Finalmente, llegamos a un último punto clave para el enfrentamiento de la delincuencia nacional e internacional: el **fortalecimiento de las redes de protección social de los Estados**. Se ha argumentado que muchos de los problemas que gatillan el alza de la delincuencia y la penetración del crimen organizado en las sociedades subdesarrolladas, tiene relación con la pobreza y la mala distribución del ingreso⁴⁶. Esto facilita el surgimiento de mercados informales donde se canalizan el tráfico de drogas, de inmigrantes, la trata de personas, etc.

En este mismo sentido, se ha sostenido que la **educación** es un aspecto clave para reforzar la identificación con las instituciones democráticas⁴⁷. Pero además es un factor relevante para enfrentar uno de los grandes problemas de la región: el aumento de la violencia juvenil. Se ha destacado a la desafiliación institucional como un factor que afecta particularmente a la población juvenil. Así, en el caso de aquellos jóvenes que no estudian ni trabajan -y excluyendo aquel porcentaje dedicados principalmente a labores domésticas o de cuidados- se “una situación de ruptura de los vínculos que permiten la formación de capacidades y la participación en el capital social”. Si el mercado laboral y el sistema educativo “son los espacios más importantes de inclusión, esto puede constituirse en un factor de riesgo que incrementa la propensión de los jóvenes a perpetrar algunas manifestaciones de violencia”⁴⁸.

4.5. En materia de ciberseguridad

La ciberseguridad y, dentro de este ámbito, la defensa contra los ciberdelitos, es un tema central para la seguridad del país y de los ciudadanos, sobre todo a la luz de los avances tecnológicos de las últimas dos décadas. Por eso mismo, los dos últimos gobiernos han realizado un esfuerzo para contar con una política nacional y una estrategia gubernamental en esta materia.

Uno de los puntos centrales de estas iniciativas es la adecuación de la legislación actual (ley N° 19.223) sobre delitos informáticos con los avances tecnológicos y los estándares internacionales. De ahí que, durante el gobierno de Michelle Bachelet, Chile haya suscrito el Convenio de Budapest, que es uno de los instrumentos más avanzados sobre delitos informáticos en el contexto internacional. Asimismo, esto se refleja en la estrategia del gobierno de Sebastián Piñera, que considera varias iniciativas legales para realizar dicha adecuación normativa, en particular el proyecto de ley N° 12192-25, que deroga la ley N° 19.223, establece nuevos delitos informáticos y modifica los tipos penales ya consagrados, así como la mentada ley

⁴⁶ COSTA, Gino. Op. Cit., p. 135.

⁴⁷ HONNETH, Axel. “La educación y el espacio público democrático. Un capítulo descuidado en la filosofía política”, *Isegoría. Revista de filosofía moral y política*, N° 49, 2013.

⁴⁸ SOTO, Humberto y TRUCCO, Daniela. “Inclusión y contextos de violencia”, en: TRUCCO, Daniela y ULLMAN, Heidi (editoras). *Juventud: realidades y retos para un desarrollo con igualdad*, CEPAL, Santiago, 2015, p. 126.

marco ingresada al término de su mandato, cuya tramitación le corresponderá al actual gobierno de Gabriel Boric.

Cabe señalar que también existen varias mociones parlamentarias en tramitación que también buscan adecuar y actualizar nuestra normativa. Todos estos esfuerzos son relevantes y deberían ser estudiados y profundizados, ya que, de concretarse, permitirían al país elevar sus estándares en materia de ciberseguridad.

Con todo, es importante que el enfoque de la ciberseguridad sea consistente con los principios generales que guían el actuar del Estado, en particular, los derechos fundamentales de las personas y que esto se convierta en una mirada transversal a las diversas instituciones y órganos que manejan datos personales o que tienen alguna relación con la ciberseguridad.

La ciberseguridad no se limita a su aspecto penal, procesal o incluso defensivo. Se necesita aquí, como en otras materias derivadas de la transformación tecnológica de la sociedad, enraizar el problema en una comprensión de los principios básicos que guían el actuar del Estado. Así, por ejemplo, es clave entender que la otra cara de cualquier avance en esta materia es la **protección de los datos personales** (derecho fundamental consagrado en el artículo 19, N° 4, de la Constitución).

Esto no se consigue solamente a través de medidas punitivas, que operan siempre a posteriori, sino con protocolos que pongan a resguardo los datos que los ciudadanos comparten con los organismos gubernamentales. En otras palabras, para prevenirnos de posibles ataques, es necesario enfatizar también el **control público sobre el uso de los datos de las personas**, e implementar este control como un imperativo de todos los órganos públicos. Es decir, es preciso contar con una mirada integradora, transversal y no parcializada del problema (sin perjuicio de que la forma de coordinar todo esto sea a través de una figura especializada como la Agencia Nacional propuesta).

4.6. En materia de tráfico de armas

Tras un análisis de la normativa internacional y nacional sobre el tema de las transferencias de armas, podemos extraer algunas ideas para el futuro trabajo de los parlamentos en la materia:

1. Es necesario reforzar la legislación interna de los países para contribuir a la implementación de las medidas tanto del Protocolo, de 2001, como del Tratado de Comercio de Armas, de 2013, y lo estipulado en la Convención Interamericana sobre la materia. En esta línea, una mejora en la **gobernanza** de las adquisiciones y transferencias de armas a nivel de las Fuerzas Armadas o del Estado, incluyendo **mecanismos de rendición de cuentas** o de auditoría, podría ser clave. Asimismo, se debería impulsar la obligación legal de incluir un **marcaje de las municiones** - cuestión en, como vimos, en Chile es deficitaria- y mejorar los **controles internos de**

las entidades fiscalizadoras de la ley de control de armas, particularmente Carabineros de Chile.

2. Aunque las medidas administrativas escapan al rol de los parlamentos, por lo menos en países de régimen presidencial, como Chile, sería positivo que estos reforzaran sus medidas de control político y fiscalización al poder ejecutivo sobre la materia, instándolos a implementar los cambios requeridos.

3. Finalmente, en cuanto a su rol en la diplomacia parlamentaria, los parlamentos podrían favorecer los compromisos de los Estados respecto del **intercambio de información y de buenas prácticas**, para enfrentar en conjunto el riesgo de desvío de transferencias de armas.