SECCIÓN IV – DERECHO PENAL INTERNACIONAL

SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL

RELACIÓN GENERAL

André KLIP*

1. El derecho penal internacional en la sociedad de la información

1.1 Conectar el mundo físico con el mundo virtual

El cambio provocado por las nuevas tecnologías informáticas y de las telecomunicaciones para nuestra sociedad es enorme y al mismo tiempo, no es exagerado afirmar que tienen consecuencias dramáticas para los diversos aspectos de la legislación penal y procesal penal. Esto justifica una renovada atención a este problema en nuestra Asociación. No es la primera vez que la AIDP aborda el tema del Derecho a la información, aunque hace ya algunos años, y las cosas han cambiado drásticamente[1].

La globalización de nuestra sociedad tiene como consecuencia que la conducta humana puede tener efecto en muchos más lugares que aquel en el que ha actuado el sujeto. Google Earth, Street View, Facebook y Hyves nos dejan claro que para muchos hay poco que otros no puedan ver. Cada vez más personas están *online* todo el tiempo con los teléfonos celulares, iPads o sistemas de navegación. Finalmente el Gran Hermano nos está mirando ahora, dejamos huellas dondequiera que vayamos.

El mundo del delito sigue (o algunos incluso dicen que va por delante de) el mundo jurídico. Las nuevas tecnologías, como las telecomunicaciones, la informática y la World Wide Web pueden ser una herramienta útil y también un objetivo interesante para cometer un delito. Los hackers pueden acceder a una red o a un equipo individual ubicado en un Estado desde un ordenador al otro lado del mundo. El discurso del odio que se pronuncia a través de Twitter, correo electrónico o Youtube tiene una expansión global. Los ataques cibernéticos pueden demoler o inutilizar redes de información, sistemas de banca online y servidores públicos.[2]

Con respecto a las investigaciones sobre los delitos cometidos en los tiempos modernos, la nueva sociedad de la información plantea nuevas cuestiones jurídicas. La investigación de una red internacional de producción de pornografía infantil y la difusión de sus productos puede requerir visitar sitios, entrar en sus áreas protegidas, buscar en buzones de correo electrónico, analizar grupos de debate y de noticias e identificar las direcciones IP individuales de los ordenadores. La computación en la nube[3] plantea la cuestión de qué datos están almacenados y qué legislación es aplicable.[4] También la comunicación inalámbrica plantea nuevos problemas a las agencias de aplicación de la ley, porque la transmisión de datos puede implicar varios Estados u organismos internacionales. La persona que usa un teléfono celular en un Estado puede conversar con una persona en otro Estado. Sin embargo, el satélite que transmite la conversación puede ser propiedad de otros Estados o sujetos privados y encontrarse en el espacio. ¿Qué significa esto para las posibilidades de interceptar la conversación?

En momentos en los que existen diversas situaciones en las que es importante tener una cierta posición informativa (*information position*) que permita al Estado evitar o responder a los ataques terroristas, los Estados han concluido los llamados acuerdos sobre el registro de nombres de pasajeros. Además, los Estados han desarrollado bases de datos (comunes) que se pueden ser consultados directamente y sin la interferencia del Estado que haya facilitado la información. Por ejemplo, entre los Estados miembros de la Unión Europea, las

---

* Catedrático de Derecho penal, procesal penal y aspectos transnacionales del Derecho penal. Universidad de Maastricht (Holanda). Trad. Isidoro Blanco Cordero y J.L.de la Cuesta Arzamendi.

[1] Ver la Relación general por Cole Durham, The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm, 64 RIDP 1993, p. 79-117.

[2] Ver los diversos ejemplos mencionados en Francia 2.

[3] Se define la computación en nube como "un modelo que facilita un servicio de acceso por red ubicuo, conveniente y a demanda a un conjunto compartido de recursos configurables (p.e. redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente suministrados liberados con un mínimo esfuerzo de gestión o de interacción con el suministrador del servicio". Peter Mell and Timothy Grance, The NIST definition of Cloud Computing 2011, Special Publication 800-145, National Institute of Standards and Tecnología.

[4] Ver Laviero Buono, the Global Challenge of Cloud Computing and EU Law, Eucrim 2010, p. 117-124.

bases de datos de ADN permiten la consulta directa para comprobar si una nueva muestra coincide con los perfiles de ADN ya presentes en las bases de datos nacionales de otros Estados.

Por lo tanto ahora, a pesar de la presencia desde hace bastante décadas ya, la emergencia del ciberdelito no ha dado lugar a una gran actividad legislativa a nivel internacional. Los principales documentos son el Convenio sobre la Ciberdelincuencia[5] y su Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Los redactores de la Convención sobre la Ciberdelincuencia relatan la necesidad del acuerdo por la evolución del conjunto de la sociedad[6]. El ciberdelito es considerado como un problema común. En nuestros tiempos no habrá muchos temas que tengan una dimensión internacional inherente y, por tanto, va a ser difícil para los Estados actuar y legislar individualmente.

Las definiciones contenidas en el art. 1 de la Convención sobre la Ciberdelincuencia se utilizan en este informe. Además, el ciberdelito comprende la conducta criminal que afecta intereses asociados con el uso de tecnología de la información y la comunicación (TIC), como el funcionamiento adecuado de los sistemas informáticos y de Internet, la privacidad y la integridad de los datos almacenados en o transferidos a través de las TIC, o la identidad virtual de los usuarios de Internet. El denominador común y lo característico de todos los delitos informáticos y la investigación del cibercrimen se pueden encontrar, por un lado, en su relación con los sistemas informáticos, redes informáticas y datos informáticos y, por otro, en los sistemas cibernéticos, redes cibernéticas y datos cibernéticos. El ciberdelito comprende delitos relativos a los ordenadores tradicionales, así como al ciberespacio en la nube y a las bases de datos cibernéticas.

Sin levantar el velo demasiado pronto en este informe, ya se debe mencionar que existe una preocupación general entre los ponentes nacionales por considerar su legislación nacional insuficiente en relación con los problemas que plantea el ciberdelito[7]. El informe brasileño expresa esto en su declaración de la siguiente manera: "A pesar de que la importancia de Brasil en el mundo es cada vez mayor y que el país está cada vez más integrado en las relaciones internacionales y las actividades económicas globales, la legislación penal brasileña en materia de crímenes informáticos es reciente y aún incipiente".[8] En el informe francés se reclama una legislación más moderna, adaptada a las necesidades de nuestros tiempos: "Frente a la globalización de los riesgos, no es ciertamente inconcebible imaginar una globalización de la respuesta y la instauración de una especie de *lex paenalia electronica*. ¡Pero estamos lejos de ello! Sea lo que sea, las normas destinadas a encuadrar las actividades que se desarrollan en el ciberespacio son perfectibles. Y no están por otra parte sólo «territorializadas». Están cada vez más « internacionalizadas»."[9]

La evolución en el mundo jurídico siempre ha tenido consecuencias paralelas en el mundo del crimen y las formas de luchar contra el crimen. Esencialmente, el tema principal de este Informe General es: ¿cuáles son las implicaciones para el derecho penal internacional de una sociedad global que se ha convertido en una sociedad de la información? Esto se hará con respecto a los diversos aspectos relevantes y con la estructura siguiente. En primer lugar, se abordarán las cuestiones relativas a la competencia jurisdiccional y al *locus delicti*, pues estas determinan si el derecho penal sustantivo de un Estado es aplicable a la conducta (apartado 2). Posteriormente se examinarán las posibilidades de investigar en el mundo del ciberespacio, especialmente en vista a determinar

[5] Budapest, 23 noviembre 2001, ETS 185, 39 ratificaciones a fecha de 26 de mayo de 2013. La mayoría de los Estados que han presentado un Informe nacional son partes. Fue ratificado por Bélgica, Dinamarca, Finlandia, Francia, Alemania, Italia, Japón, Países Bajos, España, Suiza y los EE.UU. Sólo firmado por Polonia, Suecia y Turquía. El Protocolo Adicional había recibido 20 ratificaciones a fecha de 26 de mayo de 2013. De los Estados que han presentado informe ha sido ratificado por Dinamarca, Finlandia, Francia, Alemania y los Países Bajos. Bélgica, Italia, Polonia, Suecia y Suiza todavía sólo han firmado el Protocolo Adicional.

[6] En el preámbulo del Convenio sobre Ciberdelincuencia la necesidad de legislación internacional en una sociedad de información global se describe con los siguientes argumentos: "Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional; Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas; Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes; Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información; En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;"

[7] La propuesta de resolución núm.1 tiene que ver con este problema: "Los Estados deberían desarrollar una respuesta coherente a los desafíos del ciberdelito, en particular, manteniendo su legislación y práctica en continua revisión con el fin de asegurar que su Derecho penal, su Derecho procesal penal y los regímenes de auxilio legal mutuo respondan a las necesidades del actualmente interconectado mundo globalizado."

[8] Brasil 1.

[9] Francia 13.

si estas medidas son de carácter nacional o con una dimensión transnacional (apartado 3). El apartado 4 se centra en la asistencia judicial en materia penal. ¿Hasta qué punto puede la asistencia entre los Estados afrontar o hacer uso de los nuevos desarrollos? Las dificultades de aplicación del Derecho penal en la nube constituyen el tema del apartado 5. La tecnología moderna puede también tener consecuencias para la forma en que los procesos penales se llevan a cabo en los tribunales. El apartado 6 explora las prácticas actuales y las posibilidades para el futuro. El apartado 7 identifica los problemas que surgen para garantizar los derechos humanos en el ciberespacio. Las observaciones finales se hacen en el apartado 8.

Adjunto al proyecto de Informe General están las Resoluciones que fueron aprobadas por los participantes en el coloquio preparatorio celebrado en Helsinki los días 9 a 12 de junio de 2013. Se hace referencia a cada texto individual en la resolución de este Informe General en aras de una mejor comprensión. Las resoluciones deben ser interpretadas en el contexto de este Informe General.

1.2 Propósito del Informe general

La tarea del Informe General es identificar las cuestiones más importantes. ¿Qué temas relacionados con la sociedad de la información en el derecho penal aparecen en el horizonte? Esta imagen contribuirá a hacer un análisis de los diversos aspectos de la sociedad de la información y el derecho penal internacional, para plantear otras cuestiones que incentiven el debate y sugieran soluciones. La sección IV de la AIDP es la sección en la que tradicionalmente los diversos elementos de las otras tres secciones se unen. El Relator General es consciente de la posible superposición con los temas tratados en cada una de las otras tres secciones. Sin embargo, este es un aspecto inherente a este tema.

Siguiendo la metodología ya seguida en la AIDP, el Relator General obtiene su información de los informes nacionales presentados por los grupos nacionales que han nominado a sus relatores nacionales. Los informes nacionales fueron estructurados de acuerdo con el cuestionario elaborado por el Relator General en consulta con el Comité Científico de la AIDP. En varias reuniones todos los Relatores Generales, Emilio Viano, Thomas Weigend, Johannes Nijboer[10] y André Klip discutieron los proyectos de cuestionario intensamente. Me gustó mucho el alto nivel del debate y la inspiradora atmósfera. El Relator General expresa su agradecimiento a todos los ponentes nacionales por el tiempo y el esfuerzo invertidos en la entrega de los informes con tan elevada calidad, que ofrecen una amplia variedad de enfoques y dan mucho que pensar. La colección de los informes nacionales es una fuente de inspiración a explorar. Ofrece una perspectiva comparativa enriquecedora en varios sistemas jurídicos de todo el mundo.

Redactar este informe ha sido un reto, pero también una agradable tarea, ya que los informes nacionales ofrecen mucho que aprender. En este contexto, me remito al Informe francés, que distingue tres enfoques para el ciberdelito: un enfoque semántico, un enfoque criminológico y un enfoque jurídico. En esencia se centra en el tema que es central en este informe: "uno de los aspectos en el corazón de la problemática del derecho penal de internet: ¿en qué medida este derecho tiene en cuenta a la vez la ubicuidad y la inmediatez que caracterizan a los flujos de información en la Web?"[11]

El presente Informe General se ha beneficiado de las aportaciones de diecisiete informes nacionales de los siguientes Grupos nacionales: Argentina,[12] Bélgica,[13] Brasil,[14] China,[15] Dinamarca,[16] Finlandia,[17] Francia,[18] Alemania,[19] Italia,[20] Japón,[21] Países Bajos,[22] Polonia,[23] España,[24] Suecia,[25] Suiza,[26] Turquía,[27] y los Estados

[10] En abril recibimos la triste noticia del fallecimiento de Hans Nijboer, el 13 de abril de 2013. Era un colega inspirador y encantador, que muchos echamos de menos.
[11] Francia 1.
[12] Javier Augusto De Luca, Marcelo Riquert, Christián C. Sueiro, María Ángeles Ramos y Francisco Figueroa.
[13] Gert Vermeulen y Lynn Verrydt.
[14] Carlos Eduardo Adriano Japiassú y Rodrigo de Souza Costa.
[15] Guo Jing.
[16] Jørn Vestergaard.
[17] Karri Toltilla.
[18] Jacques Francillon.
[19] Florian Jeßberger.
[20] Mariavaleria Del Tufo y Tommaso Rafaraci.
[21] Takeshi Matsuda, Tadashi Iwasaki y Megumi Ochi.
[22] Anne-Marie Smit.
[23] Arkadiusz Lach.
[24] Patricia Faraldo Cadana y María de los Ángeles Catalina Benavente.
[25] Nils Rekke y Anna Graninger.
[26] Sabine Gless, Anna Petrig, Dario Stagno y Jeannine Martin.
[27] Murat Önok, Baris Erman y Güçlü Akyürek.

Unidos.[28] Cuando se hace referencia a los informes nacionales, se mencionarán el país, así como la página del formato original presentado al Relator General.

2. Jurisdicción y *locus delicti*

Principios jurisdiccionales

En sus respuestas al cuestionario, los informes nacionales afirman por lo general que sus Estados aplican los principios generales relativos a la competencia jurisdiccional. Los Estados aplican los principios clásicos tales como el principio de territorialidad, el de personalidad activa y pasiva / nacionalidad, el del domicilio y el de jurisdicción universal. Los Estados no han desarrollado nuevos principios jurisdiccionales en relación con los delitos informáticos y aplican los principios ya existentes.[29] Parece que el único país que ha modificado sus principios jurisdiccionales en relación con los delitos informáticos es Dinamarca[30]. El art. 9 bis del Código Penal crea la jurisdicción sobre un acto penal online que tiene una relación con Dinamarca. Mientras que los EE.UU., en principio, no aplican sus leyes fuera de su territorio, contemplan explícitamente la jurisdicción extraterritorial en algunos casos, incluido el ciberdelito.[31] En el informe de los EE.UU. se alude a la *USA Patriot Act*, que da jurisdicción si el delito está relacionado con un dispositivo de acceso relevante para entidades en los Estados Unidos. Por lo demás, parece que se aplican los principios jurisdiccionales existentes de los Estados. La mayoría de los relatores informan de que, dada la amplia jurisdicción existente, su Estado no se enfrenta a graves dificultades para declararse jurisdiccionalmente competente.[32] Esta es una observación interesante, pues los principios jurisdiccionales se desarrollaron para aplicarse a la conducta física que causa efectos en las inmediaciones. Al parecer, se pueden utilizar fácilmente para los contactos digitales a larga distancia.

Sólo unos pocos Estados aplican la jurisdicción universal y, en su caso, sólo para algunos ciberdelitos. Se ha informado de que la lista de delitos por los que se aplica la jurisdicción universal es muy extensa en Turquía.[33] Los Países Bajos tienen jurisdicción universal sobre el hacking cuando es considerado como delito de terrorismo. Además, en relación con unos pocos delitos se ha establecido una jurisdicción específica.[34] Italia informa de que una vez que un tratado obliga al Estado a aplicar el principio de jurisdicción universal, tiene efecto inmediato en Italia.[35]

Locus delicti

Con la creciente importancia de los desarrollos técnicos los viejos conceptos jurídicos pueden tener dificultades para mantener el ritmo. Mientras que en el pasado era relativamente fácil ubicar un comportamiento en un lugar específico de comisión (*locus delicti*), se hace cada vez más difícil localizar la conducta en el ciberespacio. Algunos autores se refieren a este fenómeno como "pérdida de ubicación"[36]. En el Informe nacional italiano aparece el término "a- territorialidad".[37] Términos similares se pueden encontrar en el Informe francés: "Se trata en efecto de conciliar el carácter espacio-temporal –delimitado y estable– de la norma de derecho penal con el carácter global del espacio virtual."[38]

Se aprecian muchas diferencias en la manera en la que los Estados determinan el lugar del delito. Los Estados pueden considerar que un delito ha sido cometido en su territorio si produce efectos en él.[39] La dirección IP domicilia un punto de ordenadores en una dirección física.[40] Suecia informa de que si no se puede determinar el *locus delicti* a ciencia cierta, pero hay motivos para creer que el delito fue cometido en Suecia, este país es competente.[41] Ley jurisdiccional danesa tiene una amplia comprensión de la conexión con Dinamarca: "Un ciberdelito relacionado con las imágenes, sonido o texto difundido desde otro país pero accesible para un grupo indeterminado de usuarios de Internet, se considera que también se ha cometido en Dinamarca si el material

[28] Bruce Zagaris.
[29] Argentina 3, Suecia 1, Turquía 1, Finlandia 3, Polonia 3, Países Bajos 7 y 12, Italia 1, Brasil 2, Dinamarca 1, Bélgica 1, España 1, Alemania 2, Francia 5, Suiza 8, Japón 1, China 2.
[30] Dinamarca 2.
[31] EE.UU. 2 y 3.
[32] Suecia 1.
[33] Turquía 5.
[34] Países Bajos 14 y 15.
[35] Italia 5.
[36] Bert-Jaap Koops, Ronald Leenes, Paul De Hert y Sandra Olislaegers, Misdaad en opsporing in de wolken, Knelpunten en kansen van cloud computing voor de Nederlandse opsporing, Tilburg Institute for Law, Tecnología y Society 2012, p. 7.
[37] Italia 6.
[38] Francia 4.
[39] Argentina 1, Suecia 1, EE.UU. 3, Italia 3, Brasil 2 y 3, Dinamarca 1, Alemania 2, Francia 9. Ver también propuesta de resolución 6: "Las infracciones penales pueden tener más de un lugar. Los Estados pueden establecer un *locus delicti* si la conducta tiene lugar o causa sus efectos en el marco de sus fronteras."
[40] Argentina 1, Suecia 1.
[41] Suecia 1.

tiene algún tipo de relación específica con Dinamarca, por ejemplo, si está en danés o se ocupa de cuestiones relacionadas con un grupo específico de personas que viven en Dinamarca".[42] El Informe nacional belga señala que no existe una teoría específica para determinar el *locus delicti* de los delitos en el ciberespacio. Lo que es necesario es establecer si existe un elemento constitutivo de la infracción que tuvo lugar en Bélgica.[43]

Turquía informa de que cualquier contenido al que se puede acceder por cualquier persona en Turquía, posiblemente, puede ser descrito como un delito cometido en Turquía.[44] Esto parece crear una jurisdicción muy amplia, ya que también se refiere a los contenidos cargados en el país y almacenados en los servidores de Turquía. Es interesante ver que en relación con el criterio de que el contenido se puede acceder desde Turquía se considera irrelevante la distinción entre "tecnología pull" (descrita como cualquier método de acceso en función de la voluntad del usuario) y "tecnología push" (que se describe como cualquier método de acceso en función de la voluntad del proveedor o de quien lo hospeda).[45] En esencia, la ubicación de la información no es relevante para la determinación de la competencia jurisdiccional de Turquía. Es importante señalar que, si el *locus* se puede determinar en Turquía, esto tiene el efecto de que no se requiere ni la doble incriminación ni se aplica el *ne bis in idem* transnacional. Uno de los problemas con la aplicación de un principio de territorialidad basado en el acceso en el territorio del Estado podría ser que el autor no puede conocer todas las particularidades de la legislación nacional específica.[46] Siendo esto cierto, sin embargo, se podría refutar con el argumento de que los autores que utilizan Internet para sus actividades crean el riesgo de que su conducta pueda estar dentro de los límites de una disposición penal. Los que patinan en el hielo fino, no deben sorprenderse si se caen al agua. En este sentido, es valiosa la propuesta del Informe de Turquía, de que el nexo con el territorio también debe depender de la voluntad del autor.[47] Volveremos sobre esto al final de este párrafo. Una observación similar se hace en el Informe de Finlandia. Si la declaración de discriminación se hace en finlandés, fácilmente se puede suponer que se dirige al público finlandés.[48] El Informe francés usa un término diferente, que al parecer tiene un significado similar, "el enraizamiento social del delito".[49] Se trata de un concepto desarrollado sobre la base de la jurisprudencia relativa a los derechos de autor en la que el delito se ubica ya sea en el lugar donde tiene su domicilio el propietario de los derechos de autor o en Francia cuando el delito tiene impacto en el orden público francés.[50]

Sobre la base del art. 8 de su Código Penal, Suiza aplica la teoría del resultado para determinar la ubicación[51]. Sin embargo, el Informe nacional también critica el concepto por falta de claridad: "interpretar un lugar de comisión en Suiza sobre la base de la teoría del resultado sólo es posible para los delitos de resultado -pero no para los delitos de mera actividad, que no cuentan con un resultado previamente definido y de los que, como consecuencia, un lugar de la comisión sólo puede ser ubicado en Suiza sobre la base de la teoría de la acción". Según la ley suiza, es relevante identificar la naturaleza del delito como delito de resultado o de simple actividad. Esto significa que para los delitos de mera actividad, Suiza sólo tiene jurisdicción si la conducta puede ser ubicada en Suiza. Para los delitos de resultado, las cosas son diferentes y se declara competente si el resultado se produce en Suiza.[52] Debido a la distinción que se hace entre los resultados y los delitos de conducta bajo la ley suiza, es absolutamente necesario que se identifique el lugar de comisión. También el Derecho japonés hace una distinción entre la conducta y el resultado. El Informe nacional establece que: "La doctrina dominante afirma que el Código Penal japonés se puede aplicar de conformidad con el principio de territorialidad (art. 1), cuando uno de los elementos del delito, en particular, la "conducta" o el "resultado" del delito se produce dentro del territorio. Sin embargo, algunos autores afirman que el lugar de la comisión no sólo se debe especificar por la "conducta" del delito y que se requiere que el "resultado" se produzca en el territorio con el fin de aplicar art.1 del código".[53]

---

[42] Dinamarca 1.
[43] Bélgica 2. Similarmente España 1.
[44] Turquía 1.
[45] Turquía 2.
[46] La propuesta de resolución 7 recoge la esencia de este pensamiento: "Los Estados deberían restringir la aplicación de la teoría del resultado en situaciones en las que el efecto no ha sido "empujado" por el autor hacia el Estado, sino que ha sido "atraído" hacia él por un individuo de ese mismo Estado."
[47] Turquía 7.
[48] Finlandia 5, Dinamarca 1 y 2.
[49] Francia 9. Ver además: "Según esta tesis, la competencia judicial vendría determinada por el lugar del hecho generador (la emisión del mensaje en estos supuestos), la competencia legislativa por el lugar de producción del resultado (la recepción del mensaje) cuando se cumplan por lo menos ciertas condiciones." Francia 12.
[50] Francia 10. El Relator nacional apunta al peligro de que pueda violarse el principio de legalidad. Cómo puede saber el autor si hay indicadores suficientes de que la conducta se dirige a la sociedad francesa.
[51] Suiza 11.
[52] Suiza 12 y 13.
[53] Japón 1.

Para los Estados Unidos la ubicación del lugar de la comisión no es esencial.[54] Varias leyes de este país prescinden de la determinación del *locus delicti*, mientras que otras requieren que se demuestre que los equipos implicados han sido utilizados en o afectan al comercio interestatal o extranjero y a los ordenadores utilizados por el gobierno federal y las instituciones financieras.[55] Esto es especialmente relevante en lo que respecta a un "equipo protegido", un término jurídico de la *Computer Fraud and Abuse Act*. Con respecto a los "ordenadores protegidos" es irrelevante desde dónde accede el autor al ordenador.

La ley de los Países Bajos establece el requisito específico de que el lugar del delito debe ser mencionado en la acusación. Sin embargo, por otro lado, no necesita ser descrito con gran precisión.[56] El Relator nacional holandés plantea la cuestión de si en el futuro se podría omitir la determinación del *locus delicti* en los casos de delitos informáticos, ya que no tiene ningún valor añadido.[57] Este parece ser un punto delicado. Mientras que la mayoría de los sistemas sostienen que la determinación del lugar es importante, también han encontrado formas creativas para identificar un *locus* dentro de sus fronteras. Es más pertinente la manera en la que los Estados han hecho que la cuestión de la determinación de la ubicación siga siendo relevante. La creatividad que los Estados manifiestan en su práctica de la localización de un delito dentro de sus fronteras ha tenido principalmente dos consecuencias. La primera es que la conducta criminal puede tener más de un *locus delicti*. La segunda es que hay numerosos conflictos de jurisdicción.

Algunos delitos son más vulnerables en este sentido que otros. Probablemente van a aparecer *loci delicti* múltiples con un delito como la incitación pública a un delito: donde el mensaje ha sido escrito, donde el mensaje se hizo público y donde se ha causado el peligro de comisión del delito.[58] O dicho de una manera diferente: "un delito se comete en un lugar en el que el autor haya actuado u omitido el hecho al que estaba obligado, o cuando se produjo o se intentó producir el resultado del delito descrito en el tipo penal".[59] La ley de los Países Bajos exige un nexo de conexión, pero es bastante indulgente en cuanto a lo que califica como tal.[60] La teoría de la ubicuidad se aplica en muchos Estados, lo que requiere un vínculo relevante.[61] Aplicado a definiciones amplias de delitos o colectivos de autores (crimen organizado, blanqueo de dinero, terrorismo), da lugar a una jurisdicción muy amplia.

También hay una amplia jurisdicción en Alemania, donde el delincuente actúa en cualquier lugar en el que realiza una actividad con miras a la materialización de los elementos del delito.[62] Esto puede tener un gran impacto. El Informe nacional alemán hace referencia a la "decisión histórica del 12 de diciembre de 2000" ("*Toeben*"), el Tribunal Supremo Federal (Bundesgerichtshof, BGHSt 46, 212) consideró que el delito de "incitación al odio" (Volksverhetzung , Sección 130), como delito de "peligro abstracto–concreto o potencial" (*abstrakt-konkretes oder potenzielles Gefährdungsdelikt*), puede ser calificado como un delito cometido en el territorio ("*Inlandstat*"), incluso si el delincuente actuó físicamente en Australia".[63] Sin embargo, por otro lado, se sugiere que, dado el alcance universal del ciberespacio, se debe adoptar un enfoque restrictivo con respecto a los delitos de peligro abstracto. El mero hecho de que los datos se suban a internet no crea un vínculo territorial con Alemania. Se informa de que la jurisprudencia aún no da una respuesta explícita a la cuestión de cuándo se puede considerar que el delito ha producido el resultado en Alemania.[64]

Con respecto a la cuestión de si el sistema nacional de justicia penal puede funcionar sin una determinación del *locus*, la mayoría de los relatores niegan que esto pueda ser así, a menos que el delito estuviera sometido a la jurisdicción universal.[65] Los Relatores belgas se oponen a la jurisdicción universal, ya que aumentaría la probabilidad de conflictos de jurisdicción.[66] Mientras que en Alemania la determinación exacta del lugar no puede ser importante en los casos de jurisdicción universal, el hecho de que el *locus* se encuentre fuera de Alemania tiene consecuencias procesales específicas. Con base en el art. 153c del Código de Procedimiento Penal alemán se aplica el principio de oportunidad en materia de persecución y no el principio de legalidad, el cual obliga a la

[54] EE.UU. 2, Polonia 2. Similarmente en Finlandia. El Relator Nacional indica que no está claro dónde se comete un ciberdelito (Finlandia 2).
[55] EE.UU. 3.
[56] Países Bajos 10. Similarmente Italia 4, Brasil 2 y 3 y España 1.
[57] Países Bajos 10.
[58] Finlandia 5, Suiza 10, refiriéndose también a la decisión del Tribunal Supremo que dejó abierta la cuestión de si el lugar donde está el servidor puede ser considerado el *locus* del delito.
[59] Polonia 1, Países Bajos 7, China 1 y 2. Alemania 3 alude a una disposición explícita del art. 9 del Código Penal alemán.
[60] Países Bajos 8.
[61] Francia 5 y 6, Suiza 9.
[62] Alemania 3.
[63] Alemania 3.
[64] Conforme al Derecho alemán, para la determinación de la competencia jurisdiccional no es relevante si los datos pueden ser localizados, lo relevante es dónde se produjeron los efectos de esos datos. Ver Alemania 4.
[65] E.g. Argentina 2.
[66] Bélgica 3.

fiscalía a enjuiciar todos los delitos cometidos en Alemania.[67] El Informe alemán se opone a una aplicación gratuita de la localización de jurisdicción, tanto por razones teóricas como de orden práctico. Los fundamentos teóricos se refieren a la soberanía y a la elusión de los tratados de asistencia mutua; las razones prácticas a las opciones selectivas en la aplicación, la sobrecarga de las autoridades alemanas y los conflictos de jurisdicción entre Estados.[68] El Informe alemán señala que el hecho de que la ubicación del ciberdelito pueda ser difícil de determinar no es una razón para aplicar el principio de jurisdicción universal.

En Suiza se ha debatido la cuestión de si la jurisdicción universal debería aplicarse a los ciberdelitos. El Informe nacional lo describe de esta manera: "se ha argumentado que el juez suizo debe ser elevado a una posición de "juez del ciberespacio" -un espacio al que es ajeno el concepto de fronteras (nacionales)- con competencia universal para juzgar los ciberdelitos".[69] Sin embargo, actualmente no existen propuestas y se espera que la jurisprudencia suiza amplíe los principios jurisdiccionales existentes, así como la noción de resultado.[70]

Es justo concluir que el principio más importante de la competencia jurisdiccional respecto de los ciberdelitos es el principio de territorialidad. Puesto que los Estados interpretan la territorialidad de manera muy amplia y la aplican en el sentido de que un delito se comete donde se dejan sentir sus efectos, la mayoría de los delitos no plantean ningún problema de competencia.[71] No hay evidencia de que alguno de los otros principios jurisdiccionales jueguen un papel importante en la práctica, ni que sea necesario cambiar o ampliar los principios de jurisdicción. El hecho de que en muchos casos se aplique el principio de territorialidad es también importante por otras razones. Pues este es el principio más fuerte de la competencia y su aplicación es indiscutida en el derecho internacional. Sin embargo, como yo interpreto el informe francés, se trata de una posición elegida por la falta de alternativa. Los Estados están obligados a declararse competentes de manera que se llega a la competencia universal, sin decirlo así.[72] Por otro lado, mediante la ampliación de sus nociones de territorialidad y *locus delicti* a primera vista, eluden las posibles controversias y disputas sobre la soberanía.

Concurrencia de jurisdicciones

Los Estados generalmente tienen tendencia a evitar que la conducta pueda ser competencia de la jurisdicción de otro Estado y, por lo tanto, han extendido cada vez más el ámbito de aplicación de su legislación penal.[73] Aunque hay poca evidencia de casos en que los Estados hayan reclamado la competencia en la práctica, pero no pudieron como consecuencia de la falta de jurisdicción, la mayoría de los Estados han ampliado su jurisdicción durante años. Tenían la intención de resolver el problema potencial de que no haya ningún Estado capaz de aplicar su legislación penal a determinadas conductas y que produzcan un efecto secundario. Además, la naturaleza transfronteriza de la infracción como tal ha incrementado la competencia jurisdiccional múltiple. Como consecuencia de la práctica de la ampliación de la aplicación extraterritorial de la ley penal, en teoría existen numerosos conflictos positivos por definición.[74] Se pueden plantear varias preguntas como consecuencia de ello. ¿Esto se debería evitar? ¿Es esto un problema? ¿Lleva a problemas reales en la práctica, o es, esencialmente, una cuestión académica?[75] Mi conclusión de los informes nacionales es que la superposición de jurisdicciones es actualmente un gran problema en teoría, pero no es un problema real en la práctica entre los Estados. Llama la atención que, con la excepción de Francia, muy pocos informes nacionales mencionan la jurisprudencia sobre los delitos informáticos, aluden solo los conflictos de competencia. El Relator francés llama la atención sobre un aspecto diferente, y se refiere a los problemas que derivan de la aplicación de la legislación divergente para el ciudadano, para quien es imposible saber qué norma es aplicable a su conducta: "se supone que todos los derechos penales del mundo son aplicables al contenido de la comunicación –pero muchas veces se contradicen entre sí– y ¡hay que presumir que todos los actores tienen conocimiento de todas sus prescripciones y se encuentran por consiguiente obligados a respetarlas!"[76]

---

[67] Alemania 5.
[68] Alemania 5 y 6.
[69] Suiza 21 y 22.
[70] Suiza 22.
[71] Como afirma el Relator alemán esto lleva *de facto* a la aplicación universal del Derecho nacional, ver Alemania 4.
[72] Francia 7, ver también Suiza 22 y 23.
[73] No emplearé el término comúnmente usado "conflicto negativo de competencia", que considero no es una fórmula apropiada para esta situación. No hay conflicto alguno cuando ningún Estado es competente sobre determinada conducta. En ausencia de Derecho penal aplicable no hay ni infracción penal.
[74] Todos los informes nacionales reconocen la existencia de numerosos conflictos de competencia, ver por ejemplo Bélgica 2.
[75] En un studio comparado encargado por el Ministerio de Justicia de los Países Bajos, Klip y Massa concluyen que no hay casi procedimientos de persecución por crímenes con un *locus delicti* externo al territorio del Estado. Ver André Klip y Anne-Sophie Massa, Communicerende grondslagen voor extraterritoriale rechtsmacht, Maastricht University 2010 http://www.wodc.nl/onderzoeksdatabase/vestiging-rechtsmacht.aspx?cp=44&cs=6802
[76] Francia 8.

El Informe de Turquía señala que el principio jurisdiccional de complementariedad surgió para evitar conflictos negativos de competencia en la Convención Europea sobre la validez internacional de las sentencias penales[77]. De acuerdo con los relatores nacionales turcos, en materia de ciberdelitos los conflictos positivos plantean más problemas que los conflictos negativos. Los Países Bajos ofrecen más de una reglamentación específica para hacer frente a la solución de los conflictos de jurisdicción, la legislación ha sido adoptada tanto a nivel europeo como a nivel nacional.[78] Los informes nacionales de Estados de la UE se refieren a Eurojust[79], la Decisión marco 2009/948 y, en ocasiones, al Convenio europeo sobre transmisión de procedimientos en materia penal de 1972 como mecanismo para resolver los conflictos de jurisdicción. Además, se mencionan las disposiciones sobre el *ne bis in idem.*[80] Italia también se refiere al art. 22, párrafo 5 del convenio sobre la Ciberdelincuencia que proporciona una herramienta de consulta.[81]

La legislación brasileña prevé una regulación relativa a un conflicto positivo de competencia en el caso de la jurisdicción sobre los delitos cometidos fuera de Brasil debido a las obligaciones de una convención, así como a la jurisdicción sobre un extranjero que haya cometido un delito contra un nacional brasileño fuera de Brasil[82]. En los Estados Unidos la jurisprudencia ha desarrollado normas sobre prevención o resolución de conflictos de jurisdicción[83]. En esencia, se da preferencia al Estado con el vínculo más fuerte, salvo contraindicaciones que lo hagan irrazonable.

La ausencia de normas relativas a la solución de los conflictos positivos de competencia debe considerarse como una indicación de que en la práctica se han enjuiciado relativamente muy pocos delitos y que, si esto sucede, no han atraído la atención de otro Estado. No se han reportado casos en los que los conflictos positivos hayan provocado problemas. Los sistemas regionales creados en la UE y el Consejo de Europa son de carácter general para todos los delitos y no dan normas específicas para los ciberdelitos. La ciberdelincuencia pertenece a los delitos en los que es una característica específica es la superposición de jurisdicciones.[84]

Aspectos de asignación supranacional y de soberanía

Otra forma de enfocar las cosas podría ser que para ciertos delitos, para los que el *locus delicti* es difícil de encontrar o delitos que impliquen concurrencia de jurisdicciones, debería existir una asignación supranacional. La ventaja podría ser que un tribunal supranacional tendría el poder para resolver el conflicto de competencias de manera vinculante para los Estados involucrados. Además, un tribunal y una persecución más especializada podrían hacer frente a determinadas formas de delincuencia transnacional, que superan las posibilidades de las autoridades policiales y judiciales nacionales.

A excepción de Turquía, ninguno de los Informes nacionales se refiere al tema.[85] Esto es comprensible a la luz de lo que se describe anteriormente, la ausencia de un entendimiento de que la superposición de jurisdicciones es problemática. También indica que no se apela a algo que los Estados no pueden manejar por sí mismos. Sin embargo, la cuestión que debe plantearse es en qué medida los Estados pueden ampliar su jurisdicción sin menoscabar la soberanía de otros Estados. Algunos informes se refieren a la sentencia del caso Lotus del Tribunal Permanente de Justicia Internacional de 1927, que se entiende que hace una distinción entre la competencia del derecho penal sustantivo y la competencia para aplicar e investigar. Mientras que la jurisdicción extraterritorial puede ser fácilmente establecida, esto es diferente para los elementos del procedimiento. En el contexto de la aplicación de su legislación penal nacional sobre los delitos no se menciona frecuentemente la soberanía en los informes nacionales. Esto puede relacionarse con dos factores: el hecho de que la mayoría de los Estados ubican el ciberdelito en su propio territorio y el hecho de que los Estados tienen la tendencia a ser menos sensibles con una violación de la soberanía de los demás que a su propia soberanía.

Delitos que tienen una dimensión transnacional

El Informe francés distingue entre los delitos que tienen como objetivo dañar los diversos sistemas informáticos y aquellos en los que la tecnología informática es un medio para cometer un delito que, en teoría, también puede ser cometido por medios físicos. Esta ambigüedad se explica por el hecho de que algunos relatores mencionan muchos delitos,[86] mientras que otros informan de que la definición de las infracciones no tiene elementos

[77] Turquía 6.
[78] Países Bajos 15.
[79] España 2, Alemania 6.
[80] Italia 5, Suiza 20.
[81] Italia 5.
[82] Brasil 4.
[83] EE.UU. 4.
[84] Ver Propuesta de resolución 4: "Los Estados deberían restringir el establecimiento de vías de competencia extraterritorial, con el fin de prevenir los conflictos de competencia más que confiar de manera primaria en su resolución cuando se produzcan."
[85] Esto no debería llevar a la creación de una instancia supranacional, Turquía 10.
[86] Suecia 2, EE.UU. 3 y 6, Alemania 7.

jurisdiccionales.[87] Algunos afirman que es imposible enumerar todos los ciberdelitos con una dimensión internacional.[88] Los Relatores japoneses señalan: "Todos los ciberdelitos pueden tener una dimensión transnacional, porque el ciberespacio no tiene fronteras. Sin embargo, no significa necesariamente que todos los ciberdelitos en realidad tengan una dimensión transnacional: los ciberdelitos pueden tener lugar también a nivel nacional".[89] Una expresión similar sobre los diversos aspectos de la delincuencia informática se puede encontrar en el informe chino: "Es controvertido decir que el ciberdelito es transnacional. Algunos creen que todos los ciberdelitos son de carácter transnacional. Algunos creen que los delitos contra la información en Internet son transnacionales por el hecho de que internet no tiene fronteras, mientras que los delitos tradicionales cometidos mediante herramientas cibernéticas no tienen carácter transnacional".[90]

Hay una amplia variedad de delitos que son reportados como teniendo una dimensión transnacional:[91] pornografía infantil,[92] interferencia con correo electrónico,[93] acceso ilegal a un sistema de información,[94] publicación de correspondencia sin autorización,[95] revelación de secretos,[96] delitos relativos a datos protegidos,[97] falsedad electrónica,[98] demolición,[99] interrupción y obstaculización de comunicaciones,[100] interferencia con pruebas,[101] difamación pública de personas / discursos de odio,[102] denigración de la nación turca,[103] incitación a un grupo de personas a animosidad contra otra u otras,[104] otros crímenes cometidos a través de formas de expresión,[105] delitos de propiedad intelectual,[106] delitos de juego y apuestas,[107] difamación,[108] coerción,[109] incitación pública a un delito,[110] ataque a la santidad de la religión,[111] incitación a la guerra,[112] fraude de tarjetas de crédito,[113] delitos de todo tipo relacionados con ordenadores,[114] delitos contra la integridad de los sistemas TIC,[115] delitos contra la intimidad,[116] fraude de identidad,[117] delitos relativos a contenidos ilegales,[118] delitos de protección de los derechos de la propiedad intelectual,[119] obtención no autorizada de datos,[120] acceso no autorizado a sistemas de procesamiento de datos,[121] daños a los datos[122] y fraude por ordenador.[123] En el

[87] Argentina 3, Bélgica 3, Suiza 8, España 3, con la excepción del "tráfico de pornografía infantil". Japón menciona la excepción del Art. 21 (4) de la Ley de Prevención de la Competencia Desleal que recoge elementos de competencia jurisdiccional.
[88] Suecia 2.
[89] Japón 3.
[90] China 4.
[91] Se alude a numerosas infracciones penales de los Países Bajos, ver Países Bajos 10-12, citando a Evert Stamhuis, Relator nacional de los Países Bajos para la Sección 1. Se subraya que en muchos casos la dimensión transnacional de los ciberdelitos no resulta de la naturaleza misma de las infracciones, sino más bien de los métodos típicos de perpetración Países Bajos 17).
[92] Argentina 3, Turquía 8, Brasil 5.
[93] Argentina 3, Turquía 8, Italia 4.
[94] Argentina 3, Turquía 8, Polonia 4, Italia 4.
[95] Argentina 3.
[96] Argentina 3.
[97] Argentina 3.
[98] Argentina 3.
[99] Argentina 3.
[100] Argentina 3, Italia 4, Brasil 5.
[101] Argentina 3.
[102] Turquía 4, Italia 4.
[103] Turquía 4.
[104] Turquía 4.
[105] Turquía 4.
[106] Turquía 8.
[107] Turquía 9.
[108] Finlandia 5.
[109] Finlandia 5.
[110] Finlandia 5.
[111] Finlandia 5.
[112] Finlandia 5.
[113] Polonia 4.
[114] Dinamarca 3, España 3.
[115] Alemania 7.
[116] Alemania 7.
[117] Alemania 7.
[118] Alemania 7.
[119] Alemania 7.
[120] Suiza 6.
[121] Suiza 6.
[122] Suiza 6.

derecho penal sustantivo se puede observar que la mayoría de los Estados han construido los elementos de los ciberdelitos relacionados como una variación de los delitos basados en un acto físico. Como resultado de ello, las definiciones de los delitos relacionados con la informática están todavía bastante cerca de los delitos de carácter físico: el robo del ordenador tiene mucho en común con el robo; la destrucción de datos informáticos es similar a la demolición del inmueble y el hacking se parece al allanamiento.

Los relatores nacionales italianos se refieren al hecho de que, como consecuencia de la aplicación del art. 3 de la Convención contra la Delincuencia Organizada Transnacional, se ha abierto paso en el sistema jurídico italiano una definición de delito transnacional: "Por tanto, un delito se considera transnacional si está castigado al menos con pena de cuatro años de prisión y (a) se comete en más de un Estado, o (b) se comete dentro de un solo Estado, pero una parte sustancial de su preparación, planificación, dirección o control se realiza en otro Estado; o (c) se comete en un solo Estado, pero implica a un grupo delictivo organizado que realiza actividades delictivas en más de un Estado; o (d) se comete en un solo Estado, pero tiene efectos importantes en otro Estado".[124] Es considerado muy probable que esta definición se aplique a los ciberdelitos. El Informe alemán afirma que: "Como regla general, el alcance jurisdiccional de los delitos tipificados en el derecho alemán se produce sólo si las definiciones de los delitos se interpretan junto con las normas generales relativas a la competencia jurisdiccional".[125] La regla establecida de esta manera puede ser considerada como la norma aplicable a todos los Estados. Al final, la competencia jurisdiccional sobre un delito está determinada por la parte general junto con el correspondiente delito de la parte especial.

Cuestiones de parte general

Tampoco las reglas de la parte general distintas de la competencia jurisdiccional han sido modificadas como consecuencia de la introducción de los ciberdelitos.[126] Se puede suponer que esta es también la regla para los Estados que no informaron específicamente sobre esta cuestión. Esto significa que hay Estados para los que los partícipes tienen su propio *locus* y Estados en los que los partícipes siguen el *locus* del autor principal. En Turquía parece que los partícipes tienen su propio *locus*.[127] En otras palabras, si el autor cometió el delito en Turquía y el cómplice prestó su ayuda desde el extranjero, este último no está dentro de la jurisdicción de Turquía. Finlandia utiliza un sistema diferente: se considera que el inductor o cómplice han cometido el delito tanto en el lugar en el que se cometió el acto de complicidad como en el que se considere que se ha cometido el delito.[128] En Italia, se considera que un delito se ha cometido en Italia también cuando sólo una parte de la conducta de uno de los partícipes ha tenido lugar en Italia.[129]

Según la ley suiza los actos preparatorios realizados en Suiza no son suficientes para considerar que ese país es el *locus*, al menos debe haberse llegado al estadio de tentativa.[130] La teoría de la ubicuidad se aplica también a las tentativas en Derecho suizo.[131] En cuanto a la participación, la actuación de un coautor en Suiza supone que el lugar de comisión es Suiza para todos los coautores.[132] Los inductores y los cómplices de delitos de resultado tienen como *locus* Suiza. La misma conducta en Suiza con un resultado en el extranjero está fuera de su jurisdicción.[133] También se aplican estas normas de participación pues han fracasado los intentos de regular la responsabilidad penal de los proveedores.[134] Como resultado, un proveedor de contenidos puede considerarse fácilmente como autor, mientras que el proveedor de acceso y alojamiento pueden ser calificados como cómplices, siempre que tengan algún conocimiento de lo que está sucediendo.[135]

Para Alemania es relevante que el Derecho penal alemán se aplica también al representante de un proveedor que tiene su sede en Alemania y sube datos ilegales[136]. Si bien el Derecho alemán sí crea responsabilidades para las personas jurídicas en su *Telemedia Act*, esta no puede ser equiparada a la responsabilidad penal. La legislación distingue entre el "proveedor de contenidos", que es responsable de los contenidos que ofrece, y el "proveedor de acceso", que en general no es responsable[137]. La legislación alemana incorpora la Directiva de la

[123] Suiza 6.
[124] Italia 5 y 6.
[125] Alemania 7.
[126] Brasil 5, Dinamarca 3.
[127] Turquía 9.
[128] Finlandia 2.
[129] Italia 6.
[130] Suiza 10.
[131] Suiza 13.
[132] Suiza 14.
[133] Suiza 14 y 15.
[134] Suiza 26-28.
[135] Suiza 30.
[136] Alemania 4, en referencia al art. 14 del Código penal (actuar en lugar de otro).
[137] Alemania 7 y 8.

UE 2000/31 sobre el comercio electrónico. La amplia aplicación de las normas a los representantes puede compensar la ausencia de responsabilidad penal de las personas jurídicas en Derecho alemán.

La responsabilidad penal de las personas jurídicas

Sobre esta cuestión hay que señalar la gran división entre los Estados que aceptan la responsabilidad penal de las personas jurídicas y de los Estados que no la aceptan. Algunos Estados categóricamente descartan la responsabilidad penal de las personas jurídicas: Argentina, Turquía, Alemania y Japón.[138] Polonia parece estar en una categoría intermedia, ya que prevé la responsabilidad de las personas jurídicas, pero considera que esta es *quasi-penal.*[139] Otros Estados aceptan la responsabilidad penal de las corporaciones: Suecia (con la condición de que la empresa esté activa en el país), los Estados Unidos (cuando se cometen contra un *ordenador protegido*), Finlandia (cuando está prevista para el delito específico), Italia y España (cuando se prevé para el delito específico, estando prevista para varios ciberdelitos),[140] Brasil (para delitos ambientales solamente).[141] China (para actos que atenten contra la sociedad),[142] Bélgica, los Países Bajos, Suiza y Dinamarca aceptan la responsabilidad de las personas jurídicas respecto de todos los delitos.[143]

En Suiza, la "responsabilidad de las personas jurídicas juega un papel importante si se puede atribuir la responsabilidad a un proveedor de alojamiento a través de las normas de participación. Si un proveedor de alojamiento no es una persona natural, sino una persona jurídica, sólo se prevé la responsabilidad penal en los casos en que sea aplicable el art. 102 (1) del Código Penal suizo. Este requiere, en primer lugar, que la responsabilidad por el acto criminal no pueda ser imputada a una persona física, por ejemplo, un empleado, debido a los defectos de organización. En segundo lugar, la disposición exige que el delito se cometa "en el ejercicio de actividades comerciales de acuerdo con los objetivos de la empresa". Este requisito garantiza que existe un vínculo entre el delito subyacente por el cual es responsable la persona jurídica y la actividad de la misma. Sólo si se cumplen estos requisitos puede un proveedor de alojamiento que sea una persona jurídica ser considerado penalmente responsable de acuerdo con la legislación suiza".[144] Como consecuencia de ello, las normas de atribución de la responsabilidad a los proveedores pueden tener implicaciones jurisdiccionales y crear un *locus* en Suiza. Más en general, parece ser que en los Estados que aplican la responsabilidad penal de las empresas los factores que imputan la conducta de los individuos a la persona jurídica son exactamente los mismos que establecen el nexo de unión relevante que justifica la jurisdicción sobre la conducta de la corporación.

Los regímenes divergentes sobre la responsabilidad penal de las personas jurídicas pueden causar problemas para las empresas internacionales con sucursales en más de un Estado. Puede ocurrir que el mismo comportamiento en un Estado llevado a cabo por una sucursal no pueda dar lugar a responsabilidad penal de la empresa, por el contrario, en otro Estado puede ser que sí dé lugar a responsabilidad penal para otra sucursal. Sin embargo, uno podría preguntarse si se trata de una situación en la que la posición de las personas jurídicas es muy diferente de la de las personas físicas. En el contexto de las dificultades que más tarde veremos en lo que respecta a las investigaciones y la ejecución, es recomendable crear la responsabilidad penal de las personas jurídicas que operan en un entorno transnacional.[145]

Cuestiones de legalidad y de la doble incriminación

Con respecto a la cuestión de si un Estado puede regular las cuestiones jurisdiccionales de manera aislada, las respuestas difieren enormemente. Algunos Estados se refieren a las amenazas de la ciberdelincuencia y la necesidad de actuar sobre ella, y, posteriormente, aceptan que un Estado puede determinar unilateralmente sus normas de competencia jurisdiccional.[146] Algunos sugieren que esto puede hacerse sobre la base de un tratado.[147] Zagaris, al informar sobre los EE.UU., describe las opiniones de su gobierno con el siguiente título: "El

[138] Aunque la responsabilidad del proveedor se debate en Japón, ver Japón 4.
[139] Polonia 5.
[140] Italia 7, España 3.
[141] Brasil 6.
[142] China 5.
[143] Sin embargo, en los Países Bajos también se prevé la exoneración de intermediarios en la parte general del Código Penal. El art. 54a puede traducirse como sigue: "El intermediario que suministra la transmisión o almacenamiento de datos provenientes de un tercero como un servicio de telecomunicación, no será perseguido como tal si obedece una orden del fiscal, adoptada con autorización del juez instructor a propuesta del fiscal, dirigida a la adopción de todas las medidas que le sean razonablemente exigibles para hacer esos datos inaccesibles". Dinamarca 4, Bélgica 4, Suiza 35.
[144] Suiza 35.
[145] A este respecto, la Propuesta de resolución 11: "Los Estados podrían considerar el establecimiento de la responsabilidad penal de las personas jurídicas en relación con los ciberdelitos."
[146] España 3, Japón 4.
[147] Suecia 2, Turquía 8, Italia 6, Suiza 24, 25 y 50. Rusia propuso un Convenio sobre la Seguridad Internacional de la Información, el 21 de septiembre de 2011, con disposiciones dirigidas a limitar la competencia sustantiva y procesal al territorio del Estado parte.

Gobierno de los EE.UU. cree que puede regular el ciberdelito por sí mismo"[148]. Los EE.UU. creen que, en determinadas circunstancias, un delito puede haber sido cometido en el territorio de un Estado y, por tanto, enjuiciado por sus tribunales penales, a pesar de que el autor se encuentre físicamente fuera del territorio. La respuesta de Finlandia a esta pregunta es totalmente diferente: se trata de una cuestión que un Estado no puede regular por sí solo. Debido a que los ciberdelitos no respetan las fronteras de los países, la armonización de la legislación juega un papel esencial en la lucha contra los mismos.[149] En el Informe francés se afirma desde el principio: "La ciberdelincuencia y la cibercriminalidad suscitan en el plano jurídico cuestiones tanto más difíciles de resolver cuanto que afectan a una sociedad globalizada. Esta situación convierte *a priori* en ilusoria la regulación a un nivel exclusivamente nacional, territorial. Impone, pues, la necesidad de poner en marcha un cibercontrol a escala regional, o bien mundial."[150] Está claro que la conclusión del Informe francés es que un Estado no puede regular y combatir eficazmente una forma tan fluida de criminalidad como los ciberdelitos.[151]

El Informe danés intenta encontrar el equilibrio entre las medidas unilaterales y las multilaterales: "los ciberdelitos son transnacionales por naturaleza. Podrían ser regulados a nivel nacional por iniciativas legislativas nacionales aisladas, pero sólo con el riesgo de un innecesario trabajo legislativo duplicado, la falta de importantes vínculos internacionales y complicados procedimientos de asistencia judicial recíproca. Las TIC hacen que sea especialmente importante mejorar la cooperación internacional en materia penal. La naturaleza de Internet hace posible que los responsables encuentren refugios libres bajo la jurisdicción de los países que no penalizan los ciberdelitos sistemáticamente, no mantienen actualizadas las normas de competencia jurisdiccional, o no tienen acuerdos de extradición o entrega suficientes. La ciberdelincuencia y la volatilidad de los datos electrónicos crean la necesidad de procedimientos rápidos y, en ocasiones, secretos. Las normas de asistencia mutua mejoradas, que a menudo dependen del requisito de la doble incriminación, también motivan la necesidad de disposiciones sustantivas equivalentes y armonizadas".[152] Una posición intermedia adopta Alemania, que reconoce la competencia de los Estados para determinar su propia jurisdicción. Sin embargo, los ciberdelitos no son de una gravedad tal, comparable al genocidio y los crímenes contra la humanidad, que les califique para el Derecho internacional. Un tratado sería una opción.[153]

El informe italiano señala un tema importante que complica la aplicación unilateral de la competencia jurisdiccional: "En relación con los ciberdelitos menos graves puede haber algunos obstáculos para un sistema de este tipo, la doble incriminación seguirá siendo la más controvertida. ¿Qué pasa si una conducta criminal en un Estado constituye el ejercicio de un derecho legítimo en otro Estado? El equilibrio entre los intereses en conflicto sólo se puede hacer a nivel nacional y no se puede imponer a través de un Estado extranjero y sus autoridades".[154] Esta observación, en esencia, se refiere a la aplicación del principio de legalidad. También el informe de Suiza expresa una preocupación en relación con la libertad de expresión y los derechos políticos.[155]

Conclusión

Sorprendentemente, la imagen que surge es que los Estados no tienen dificultades para extender y aplicar sus principios jurisdiccionales a los fenómenos modernos de la actividad criminal. El problema/frustración parece encontrarse en la imposibilidad de llevar a los culpables ante la justicia. Como se afirma en el Informe suizo: "Además de las normas armonizadas a nivel de la legislación penal sustantiva, que luego son incorporadas al Derecho interno, es necesario disponer de herramientas adecuadas de cooperación internacional para la prevención, detección, investigación y enjuiciamiento de los ciberdelitos".[156]

Hay varias cuestiones en juego aquí. La primera es si los Estados tienen la competencia para determinar su propia jurisdicción sobre los delitos. Los puntos de vista que prevalecen son que efectivamente disponen de ella. No hay ninguna norma en Derecho internacional que lo prohíba. Como la mayoría de los Estados en la actualidad aplican el principio de territorialidad para ubicar a los ciberdelitos dentro de sus fronteras, el potencial de conflictos en teoría es más bien limitado. En la aplicación de principios distintos del de territorialidad la mayoría de los Estados exigen el requisito de la doble incriminación. La mayoría de los principios jurisdiccionales, con excepción del principio de jurisdicción universal, requieren que la conducta esté penalizada por la ley del lugar donde se ha cometido. La justificación de esto radica en los requisitos de legalidad.[157] Para Turquía sólo si no puede establecerse el *locus* en el país, la determinación del *locus* es relevante en vista del requisito de la doble

[148] EE.UU. 7. Esta posición se comparte en el Derecho polaco, en particular porque se relaciona con la soberanía, Polonia 4.
[149] Finlandia 9. También el Informe chino llama a la resistencia, China 5.
[150] Francia 3.
[151] Francia 4.
[152] Dinamarca 3.
[153] Alemania 6.
[154] Italia 15. La misma cuestión se suscita de manera explícita en otros Informes, ver Dinamarca 2, Bélgica 2, Japón 3.
[155] Suiza 50.
[156] Suiza 25.
[157] Por tanto no debería abolirse, España 3.

incriminación.[158] La consecuencia es una vez más que el delito debe ser ubicado y ya vimos que esto puede ser difícil. Cuando los Estados aplican otros principios jurisdiccionales distintos del de territorialidad y exigen la doble incriminación, los intereses protegidos por el principio de legalidad no están en peligro. Cabe esperar del agresor que conozca el Derecho del *locus*.[159]

Es interesante ver que, en el contexto del ciberdelito, es el principio de territorialidad el que motiva la preocupación[160]. Dependiendo del tipo de delito, la cuestión que debe plantearse es si el autor ha sido capaz de conocer la norma prohibitiva. En otras palabras, tenemos que analizar lo que el principio de legalidad exige en este contexto. Al aplicar el principio de territorialidad, los Estados pueden argumentar que los que cometen un delito en su territorio deben conocer la legislación aplicable. Sin embargo, con la amplia interpretación del principio de territorialidad los autores pueden cometer delitos en otros lugares sin estar presentes en el territorio. Esto debe dar lugar a la exigencia adicional de que un autor debe ser capaz de saber que su conducta puede causar efectos en otros lugares. Los Estados se inclinan a aceptar que hay competencia jurisdiccional cuando el autor desea alcanzar a dicho Estado. No está claro si existe jurisdicción sobre los autores que dieron acceso al contenido al que se puede acceder desde otros Estados también. Por tanto, debemos hacer frente a este problema ahora.

La situación que nos preocupa a nosotros tiene que ver con la conducta de un agresor que realiza la conducta en el extranjero, causando efectos en la jurisdicción del Estado que reclama su competencia jurisdiccional. Es pertinente hacer una distinción en función de si el autor tiene como objetivo la producción de efectos en el Estado territorial. A primera vista, parece lógico considerar previsible para el autor que una determinada norma prohibitiva es aplicable si su propósito o la intención es dañar el ordenador de un individuo concreto, atacar un sistema bancario específico etc. Un enfoque similar se puede adoptar para delitos relativos al contenido enviado a un individuo específico. Con insultos y expresiones de odio enviados a un individuo específico existe la expectativa de que cause efectos allí. La cuestión a plantear es si lo que se ha dicho hasta ahora con respecto a las víctimas individuales también se aplicaría en situaciones en las que el autor puede ser consciente de su identidad o domicilio. La competencia territorial se podría justificar sobre la base de su autor siendo indiferente lo relativo a quién y dónde ocurrirán los efectos.

Así, la situación en la que el autor no envía nada, pero proporciona contenido que entra dentro de la legislación penal de un Estado desde el que los individuos pueden tener acceso. Esto podría relacionarse con el lenguaje o la opinión empleados, lo que podría violar las disposiciones sobre injurias, incitación al odio, libertades políticas. También podría referirse a las normas nacionales sobre la moral y la religión. El contenido puede ser considerado como la pornografía o violar la moral sexual. El contenido puede equivaler a la blasfemia. En estos casos, la reivindicación de la jurisdicción territorial sobre la base de los efectos en el Estado no parece estar justificada pues el autor cumple con las leyes penales del Estado donde se produce o tiene el contenido. Permitir que el Estado que criminaliza este contenido aplique sus leyes penales conduciría al mínimo denominador del que hace las reglas e infringiría gravemente las libertades políticas y los derechos humanos de los individuos[161].

¿Debería ser esto diferente si el sitio web es accesible sólo en el idioma del Estado del territorio? No lo creo. Siempre y cuando se trate de una elección libre de las personas que se encuentran en el Estado territorial la de acceder a la página web y, siempre y cuando no se enfrenten con contenido no solicitado, los intereses del Estado territorial no resultan realmente perjudicados.[162] Sostener lo contrario significaría que un Estado podría imponer su legislación en todo el globo.[163] Por tanto, al criterio distintivo de los efectos producidos en un Estado hay que añadir la cuestión de si eran o no solicitados. Las personas que descargan contenido en el Estado del territorio pueden estar sujetas a su legislación ya que poseen el contenido ilegal en el mismo.[164]

---

[158] Ver Turquía 3.

[159] Una anotación crítica al respect podría ser que include para el autor puede ser difícil saber dónde está actuando.

[160] Pese a esto debería seguir siendo el primer principio. Ver Propuesta de Resolución 3: "El principio de territorial debe seguir siendo el primer principio de competencia jurisdiccional en el ciberespacio."

[161] La Propuesta de Resolución 5 indica: "Con la excepción de aquellos crímenes para los que se acepta la jurisdicción universal por parte del Derecho internacional, los Estados no deberían aplicar la jurisdicción universal de hecho o de derecho a los casos de contenido prohibido en el ciberespacio."

[162] La Propuesta de resolución 8 se refiere a la necesidad de requerir un nexo particular: "En determinados efectos, los Estados tomarán en consideración la existencia de un nexo particular con la infracción, como la intención del autor."

[163] Así se expresa en la Propuesta de resolución 9: "Cuando un Estado localiza entre sus fronteras los efectos de una infracción, el principio de legalidad exige que el autor pueda haber tenido una expectativa razonable de que su conducta causaría efecto en aquel país."

[164] Ver Propuesta de resolución 10: "Un Estado puede ejercer su competencia jurisdiccional sobre un individuo que se encuentra en su territorio y "atrae" contenido prohibido por su propio sistema legal, incluso si es lícito conforme al sistema jurídico del productor."

3. Investigaciones en el ciberespacio

En este apartado analizaremos en qué medida los Estados pueden investigar en el mundo cibernético sin la necesidad de aplicar mecanismos de asistencia mutua por parte de otro Estado. En otras palabras, ¿qué pueden hacer por sí mismos? ¿Dónde hay que poner los límites y con qué bases? Nos referiremos a todas las medidas de investigación, con independencia de si tienen relación o no con la inteligencia, obtención de una posición de información o pruebas a emplear en un proceso penal. Como sucedía en cuanto a la jurisdicción/competencia, también respecto de la investigación en el ciberespacio la localización de la información o pruebas tiene un papel crucial. Una primera observación es que mientras que se acepta comúnmente que los Estados pueden aplicar su Derecho penal a conductas realizadas en otros Estados, el Derecho internacional no permite otorgar a un Estado la competencia para recoger pruebas por su cuenta en otro Estado, lo que no parece lógico.

Preliminar: conocimiento experto y límites de la tecnología

Allí donde la tecnología juega un papel decisivo, las posibilidades técnicas pueden ser determinantes para los desarrollos y posibilidades legales. Este fenómeno puede llevar a cuestiones altamente interesantes acerca de dónde debe estar la primacía a la hora del desarrollo del Derecho. ¿Determina Microsoft si pueden llevarse a cabo investigaciones, así como cuándo y cómo?

Algunos Estados y organizaciones internacionales disponen de satélites y otros artilugios para tener una foto clara y detallada de cualquier lugar del mundo. ¿Debería el Derecho regular su uso con fines de investigación o persecución de carácter penal? En caso afirmativo, ¿a qué nivel, nacional o internacional, debería regularse y cuáles son los temas en cuestión?[165]

Al margen del hardware y software que integran el mundo virtual, quien investiga debe tener el conocimiento necesario para hacerlo. Se insiste en que hay una gran necesidad de conocimiento experto específico para la investigación de los ciberdelitos.[166] Los Países Bajos han adoptado un cierto número de iniciativas para generar conocimiento experto entre sus agencias policiales y judiciales sobre la sociedad de la información y el ciberdelito.[167] Francia ha especializado y centralizado sus puntos de contacto relativos al intercambio de información en materia de ciberdelitos.[168]

Aunque el Derecho turco prevé la interceptación de las telecomunicaciones, limita esta posibilidad a ciertos delitos. Y los ciberdelitos no se encuentran, como tales, en la lista.[169] Para el Derecho turco es relevante si el usuario de las telecomunicaciones se encuentra en su territorio. El Derecho turco no autoriza registros por acceso remoto.[170] La interceptación de datos es sólo posible si los proveedores se encuentran en Turquía. Los Países Bajos disponen de una panoplia de disposiciones para la interceptación de telecomunicaciones y la transferencia de datos en muchas circunstancias.[171] Muchos Estados limitan estos métodos de investigación a las formas más graves de delitos,[172] pues infringen gravemente el derecho a la intimidad y sus expectativas. Si la dirección IP del ordenador se encuentra en el extranjero, debe solicitarse la asistencia internacional. Si el proveedor se encuentra en el extranjero, y no tiene ninguna extensión en el país, los Países Bajos no pueden aplicar directamente su competencia.[173] En Derecho alemán, las autoridades no pueden acceder a datos localizados fuera del país, salvo con base en una demanda de asistencia.[174] Se admite como excepción los datos informáticos almacenamos de modo públicamente disponible (*open source*). La obligación de los proveedores de cooperar con las medidas de investigación de forma que deban disponer de los medios técnicos para ello e interceptar en la práctica ha sido regulada por la *Telecommunication Surveillance Regulation*.[175] Con base en esta legislación la interceptación puede no continuar si se identifica que el ordenador o teléfono celular se encuentra en el extranjero, salvo que la comunicación a interceptar pueda estar conectada a un ordenador o almacenador de datos en Alemania. El Derecho alemán no autoriza búsquedas online discretas.[176]

Revisión de la localización

La mayoría de los Estados aplican la regla de que la localización en la que se encuentra la información determina si resulta aplicable la legislación nacional o no. Para esos Estados determinar el lugar de la información es muy relevante. En el Informe suizo se indica que la policía puede hacer en internet todo lo que pueda equipararse a un

[165] Nos recuerda las "telepantallas" que predijo George Orwell en su famosa novela 1984.
[166] Turquía 11.
[167] Países Bajos 52-53.
[168] Francia 30.
[169] Turquía 18.
[170] Turquía 18.
[171] Países Bajos 23, de manera similar Italia 8, Dinamarca 4, Francia 18-22 y Alemania 10-12.
[172] E.g. Japón 5.
[173] Países Bajos 29, de manera similar Dinamarca 5.
[174] Alemania 10.
[175] Alemania 12.
[176] Alemania 12.

patrullaje policial en el mundo real.[177] Muchos informan de que no hay legislación alguna sobre registro de sitios web u ordenadores localizados fuera del país,[178] si bien aplicando el principio de libertad de la prueba es posible hacer uso de fuentes públicamente accesibles.[179] Esta es una regla que aparentemente muchos Estados aplican y deriva del art. 32 del Convenio sobre Ciberdelincuencia.

En el contexto de la sociedad de la información y en cuanto a la obtención de información y pruebas con fines de investigación penal diversas situaciones merecen atención, presumido que es todavía posible localizar la información y la pruebas: 1. Información y pruebas libres (*open*). Esta es la información públicamente accesible simplemente navegando por la red. 2. Información protegida. Información a la que no se tiene acceso público, pero a la que puede accederse hackeando. 3. Información y pruebas que exigen hacerse con el control de un ordenador o red localizada en otro país. Respecto de la primera categoría, la información públicamente accesible, la localización del contenido es irrelevante en tanto en cuanto sea públicamente accesible sin mayor problema. Para los Países Bajos, parece que el art. 32 del Convenio sobre Ciberdelincuencia pone los límites. Y este se interpreta en el sentido de que la información públicamente accesible puede ser buscada y objeto de registro con independencia de dónde se encuentren almacenados los datos. Además, puede obtenerse el consentimiento de la persona u organización legitimada para revelarlos.[180] Hay jurisprudencia que acepta el uso de fotografías tomadas de Google earth. Se informa de que el Ministerio de Seguridad y Justicia está redactando una legislación que autorizaría a la policía a registrar sistemas sin el consentimiento del propietario. Se informa de que, en casos de transferencia de datos decodificados, podría ser posible una orden de descodificación. Los Países Bajos están considerando el establecimiento de una obligación legal a tal efecto. El Relator nacional de los Países Bajos apoya esos registros.[181] Esta es ya la práctica en Francia, donde la infiltración electrónica es posible.[182] El Informe turco propone tres estándares diferentes dependiendo del tipo de información: información abierta, información protegida y control remoto de un ordenador. La primera no requiere autorización, mientras que las otras dos sí.[183] La distancia espacial entre el autor y la víctima es un elemento inherente al ciberdelito.[184]

Bélgica tiene una legislación especial "en el contexto específico de los sistemas de información, hay que hacer referencia al art. 88ter CPP, que autoriza –en ciertas condiciones– a la extensión de un registro ordenado por un juez instructor desde un sistema de información (o parte del mismo) a un sistema de información (o parte del mismo) localizado en un lugar diferente de donde el registro tiene físicamente lugar, en la medida en que la persona mandatada para el uso del sistema de información original al que el registro se refieran, tiene acceso al sistema de información (o parte de él) localizado en otro lugar. De manera diferente a lo que sucede cuando los datos a los que se tiene acceso por esta vía se encuentran localizados en el territorio belga (en cuyo caso los datos afectados no pueden ser objeto de registro, copia, bloqueo, hacerlos inaccesibles o incluso eliminarlos con base en el art. 39bis CCP), los datos localizados en el extranjero pueden ser sólo copiados, en cuyo caso las autoridades competentes del país extranjero (siempre que puedan ser razonablemente identificadas) serán informadas por el Ministerio belga de justicia. Finalmente, se considera no problemático el acceso a información públicamente disponible."[185] El art. 706-102-1 del Código procesal penal francés autoriza a investigar datos, con independencia de dónde se encuentren sin permiso del propietario o proveedor.[186]

La imagen que emerge es que no es decisivo dónde se encuentran localizados realmente los datos, si se trata de información públicamente accesible para su uso en la investigación. Algunos Estados trazan la línea con base en la necesidad de hacer uso de medidas coercitivas y otros hacen la distinción de si la información obtenida o a la que se ha tenido acceso será usada como prueba. Las investigaciones que no requieren de medidas coercitivas pueden llevarse a cabo sin necesidad de procedimiento alguno de asistencia legal mutual.[187] Respecto de la recogida de pruebas, la determinación del lugar donde se almacenan las pruebas es relevante para algunos Estados,[188] pero no para otro.[189] En algunos Estados es necesario saber dónde se almacena la prueba para que sea admisible.[190]

[177] Suiza 42.
[178] Suecia 3, Polonia 7.
[179] Brasil 9, España 10.
[180] Países Bajos 34.
[181] Países Bajos 36.
[182] Francia 22 y 23.
[183] Turquía 21 y 22.
[184] Turquía 11.
[185] Bélgica 6 y 7.
[186] Francia 21 y 22.
[187] Suecia 2, Dinamarca 6.
[188] Países Bajos 9, Italia 3.
[189] Dinamarca 2.
[190] Argentina 2.

En los dos casos significa que la información debe ser localizada y aquí es cuando esto se convierte en difícil. Nuevamente, también en lo relativo a la localización en la que realmente se encuentran los datos, se suscitan problemas cuando los datos se encuentran en la nube y pueden ser movidos de un servidor a otro, dependiente de la disponibilidad de espacio de los servidores interconectados. Los archivos pueden almacenarse en copias y partes en diferentes servidores. El sistema mismo será, entonces, dependiendo de la cantidad de datos, el que determine dónde es más eficiente el almacenamiento y moverá los datos al servidor correspondiente.[191] Incluso los proveedores del servicio de nube pueden no conocer en todo momento dónde se encuentran los (sus) datos. Claramente esto complica mucho la investigación en y la captura del material. Abordada la cuestión de manera clásica podría significar que mientras que la policía obtiene el permiso de registrar un servidor, los datos en cuestión pueden haber sido movidos automáticamente a otra localización desconocida.

En el Informe Nacional alemán la determinación de la localización de los datos se describe como algo crucial, pero también muy difícil: "Un importante problema práctico tiene que ver con el hecho de que es frecuentemente difícil determinar dónde se encuentra localizada una información específica. Así por ejemplo, el registro o la búsqueda de datos relativos a información localizada en un servidor fuera de Alemania sería ilegal en la medida en que violaría la soberanía del Estado donde se encuentra el servidor."[192] Un ejemplo de ello es el de la interceptación de telecomunicaciones inalámbricas. Si dos personas conversan hacienda uso de teléfonos móviles, ello puede estar involucrando a seis Estados.[193] ¿Deberían todos estos Estados tener algo que decir en si las conversaciones pueden ser interceptadas? Si tantos Estados pueden tener soberanía sobre una investigación de este tipo, debe afirmarse que la reclamación individual de un Estado por su soberanía se convierte en más bien débil.

Las reglas generalmente aplicables sobre registro y captura de grabaciones contenidas en el Código Penal suizo son aplicables a las comunicaciones por email. Esto significa que el registro y captura en un servidor localizado fuera del país puede realizarse por las autoridades locales.[194] El Derecho suizo prevé la vigilancia de las conversaciones telefónicas por internet.[195] Sin embargo, la legalidad de las diversas posibilidades es incierta.[196] Para los agentes de policía es casi imposible responder a las demandas. De una parte, no pueden usar sus medios coercitivos cuando los datos se encuentran localizados fuera del país. De otra parte, es a menudo imposible localizar los datos. Esto llevó a Geist a suscitar la pregunta del millón de dólares: *¿Hay ahí un ahí?*[197]

Otros retos recogidos por los relatores nacionales belgas: ˝Cuestiones adicionales, generadas por el avance técnológico, tienen que ver mayormente con la posibilidad de que delincuentes (potenciales) resulten indetectados. Las tarjetas SIM de prepago, que no requieren registro alguno, permiten a los autores hacer llamadas telefónicas no trazables, un fenómeno que mina completamente cualquier regulación relativa a la interceptación de telecomunicaciones. Igualmente no susceptible de trazabilidad es el uso de internet a través de *hot spots* que utilizan direcciones IP alternativamente, por ejemplo, en aeropuertos. El VoIP, también conocido como voz por IP, permite llamadas telefónicas por internet. Cuando se usa VoIP desde *un hot spot*, la conversación puede ser imposible de trazar. Además, la detección en internet puede ser fácilmente eludida usando el *Tor Browser*, o simplemente instalando un *IP-shielder*. Incluso el uso del "modo privado" suministrado disponible ya desde Google Chrome va haciendo más difícil la tarea de aplicación de la ley. Otros desafíos, por estar ampliamente sin regulación, son la observación transfronteriza mediante el uso de cámaras, drones espías y grabadoras de ambiente (a distancia, por ej., mediante medición laser de la vibración de las ventanas y deduciendo de ello la voz).˝[198]

Los Estados han desarrollado prácticas para compensar los problemas que pueden derivar de la dificultad de localizar dónde se almacenan los datos. El Relator nacional de los EE.UU. se expresaba de este modo: "Los EE.UU. como otros países, adoptan la posición de que pueden utilizar sus propios mecanismos legales para solicitar datos de cualquier servidor de nube, localizado en cualquier lugar del mundo, en la medida en que el proveedor de servicio de nube esté sujeto a la jurisdicción USA —esto es, cuando la entidad tenga su base en los

[191] Koops y otros, p. 7.
[192] Alemania 4.
[193] Gert Vermeulen, Wederzijdse rechtshulp in strafzaken in de Europese Unie, dissertation Gent 1999, p. 224-293.
[194] Suiza 39.
[195] Suiza 41: "El Gobierno suizo presentó un proyecto de ley al Parlamento en febrero de 2013, dirigido a la introducción de una base jurídica que regule de manera específica el uso de *spyware* con fines policiales. Conforme a este proyecto, el uso de *GovWare*, sujeto a ciertos criterios, se permitirá para la interceptación del contenido de una conversación y tráfico de datos con fines de investigación y persecución de determinados delitos particularmente graves recogidos en una lista por la ley, pero no con fines meramente preventivos. Al mismo tiempo, el proyecto de ley prohíbe los registros online y la vigilancia de espacios cerrados con micrófonos o cámaras."
[196] Suiza 40 y 41.
[197] Michael A. Geist, Is there a there there? Toward Greater Certainty for Internet Jurisdiction, Berkely Tecnología Law Journal 2001.
[198] Bélgica 10.

EE.UU., tenga una oficina auxiliar en los EE.UU o de alguna otra manera desarrolle su actividad de manera continua y sistemática en los EE.UU."[199]

Otros Estados imponen obligaciones a los proveedores. En la práctica se informa al proveedor de que la captura de datos va a tener lugar para prevenir el que la información no sea trazable (*cloud computing*).[200] El Derecho italiano autoriza la interceptación de conversaciones por teléfono móvil si el proveedor es italiano, si el propietario (el que llama o recibe la llamada) de uno de los celulares involucrados es italiano, con independencia de dónde se encuentre el proveedor o el satélite.[201] En tales casos no se necesita asistencia legal internacional. Debe ser posible someter a un proveedor a la jurisdicción fáctica de un Estado en orden a interceptar la telecomunicación.[202] Los Relatores nacionales de España indican que la legislación española es completamente insuficiente puesto que, debido al entendimiento constitucional del derecho a la intimidad de las comunicaciones, sólo prevé la interceptación telefónica, pero no de otras modalidades de telecomunicación.[203]

Autoservicio

Los Estados continúan teniendo reglas más bien estrictas que prohíben la presencia física de los agentes policiales extranjeros en su territorio.[204] ¿Se aplican estas reglas en el contexto del mundo cibernético que crea una realidad virtual? ¿Se aplican también esas reglas cuando los agentes no entran físicamente en el territorio de otro Estado, sino que practican registros en redes u ordenadores localizados en otro.[205] ¿Son aplicables las mismas reglas y, en caso afirmativo, se aplican en la realidad? Y, si las reglas que prohíben la presencia física no se aplican, ¿por qué es así?

En este contexto es relevante referirse a una disposición única del Código Penal suizo: los funcionarios extranjeros que realizan investigaciones en Suiza deben ser autorizados por las autoridades suizas. En otro caso, esas investigaciones pueden derivar en una conducta delictiva, al violar el art. 271 del Código Penal suizo, que incrimina las actividades ilícitas para un Estado extranjero. La incriminación del Derecho suizo probablemente es única en el mundo. No se encuentra en el mismo caso la regla prohibitiva a la que sirve conforme al Derecho internacional. Un problema de definición puede surgir aquí, al poderse discutir si un funcionario de policía que sentado en su oficina de su Estado doméstico se encuentra descargando datos de un ordenador o servidor localizado en el extranjero está operando extraterritorialmente.[206]

Las investigaciones extraterritoriales requieren del permiso del Estado en cuyo territorio tienen lugar. No se permite el autoservicio.[207] Finlandia informa de que las investigaciones extraterritoriales están reguladas por la Ley de Medidas Coercitivas.[208] Con todo, en Dinamarca se informa que el Tribunal Supremo danés ha establecido que el registro de una cuenta de Facebook y Messenger es legal incluso si la información se encuentra almacenada en un servidor en un país extranjero. La práctica del registro se realizó por las autoridades danesas con objeto de investigación y con base en la información legalmente obtenida (contraseñas obtenidas por interceptación de la telecomunicación) por un crimen sometido a la jurisdicción danesa, y el registro se desarrolló sin la participación de las autoridades extranjeras.[209]

Muchos Estados informan de la posibilidad de establecimiento de equipos conjuntos de investigación.[210] También se refieren a ello los arts. 40 y 41 del Convenio de aplicación del Acuerdo de Schengen, que autorizan la persecución e infiltración transfronterizas.[211] Todos estos ejemplos se refieren a la presencia física de autoridades en el territorio de otro Estado. Alemania alude al art. 89 del Tratado de Funcionamiento de la Unión Europea que dispone: "El Consejo fijará, con arreglo a un procedimiento legislativo especial, las condiciones y límites dentro de los cuales las autoridades competentes de los Estados miembros mencionadas en los artículos 82 y 87 podrán

[199] EE.UU. 10 y 25.
[200] Argentina 2. Ver también Propuesta de resolución 14: "Los Estados deberían considerar el establecer, en Derecho interno, la obligación de los proveedores de servicios de cooperar con las agencias de persecución de los delitos, haciendo que la transferencia de datos en el mundo cibernético sea trazable, dando acceso a las contraseñas, desencriptando contenido o instalando mecanismos de búsqueda con fines de investigación. Esta obligación se someterá al principio de proporcionalidad."
[201] Italia 9.
[202] Argentina 5, Turquía 12.
[203] España 4.
[204] O Los funcionarios de policía solo pueden entrar en otro país para el cumplimiento en cumplimiento de sus funciones si esto puede apoyarse en un acuerdo internacional codificado o con base en una autorización *ad hoc*. El uso de medidas coercitivas queda generalmente excluido. Con excepciones menores, como la detención de un fugitivo en caso de persecución en caliente transfronteriza. Ver, e.g. art. 41 del Convenio de aplicación del Acuerdo de Schengen.
[205] El Informe Japonés señala que la recogida de información pública no infringe la soberanía de otro Estado, ver Japón 8.
[206] Suiza 46 y 47.
[207] Turquía 21, Italia 11, Brasil 8, Alemania 13.
[208] Finlandia 7.
[209] Dinamarca 5.
[210] Polonia 7, Italia 11, España 10, Francia 16.
[211] Francia 16.

actuar en el territorio de otro Estado miembro en contacto y de acuerdo con las autoridades de dicho Estado. El Consejo se pronunciará por unanimidad, previa consulta al Parlamento Europeo."[212] Aun cuando el Tratado de Funcionamiento de la Unión Europea otorga un mandato para legislar sobre esta cuestión, por el momento no se ha adoptado ninguna iniciativa. El art. 32 del Convenio sobre Ciberdelincuencia se considera que otorga tal permiso en Derecho internacional. El Informe belga propone además permitir el autoservicio si el Estado requerido no puede, por razones de capacidad, cumplir con la solicitud de asistencia.[213]

Los Países Bajos tienen legislación generalmente aplicable a las investigaciones extraterritoriales. El art. 539a del Código Procesal Penal otorga a las autoridades de policía de los Países Bajos los mismos poderes y competencia en el extranjero como los que tienen en el interior del país, siempre que ello no sea contrario al Derecho internacional.[214] El Capítulo 13 de las Directrices de investigación criminal del Código Procesal Penal japonés también declara aplicable el Código fuera del Japón, siempre que el otro Estado lo acepte. Una consecuencia lógica es que, como se indica en el Informe nacional de los Países Bajos, haya jurisprudencia que no haya aceptado que el funcionario de policía entrara en una cuenta email sin haber obtenido respuesta positiva a su solicitud de asistencia internacional a los EE.UU. en el caso de Microsoft Hotmail.[215]

Esto es algo que se ve de manera diferente en los EE.UU. El Relator nacional señala que los EE.UU. tienen al menos nuevo métodos diferentes de coerción dirigida a la obtención de pruebas localizada en el extranjero, para obtener testimonio de testigos localizados fuera, y para asegurar la transferencia de bienes privados a los EE.UU.[216] Los métodos usados por las autoridades de EE.UU. son a menudo cuestionados por la persona cuya información es objeto de registro, así como por tribunales extranjeros. Los EE.UU. tienen la práctica de prestarse a sí mismos la asistencia que necesitan. No hay legislación que regule esta cuestión.

Análisis

Lo anterior demuestra que los Estados tratan de hacer uso de los poderes de investigación que tengan conforme a su propio sistema jurídico para las investigaciones en su territorio. Como en el caso de la competencia en el Derecho penal sustantivo, vemos que los Estados se inclinan a localizar las cosas en su territorio. Esto se refleja en actitudes en las que los Estados dónde se encuentran los datos y en situaciones en que se demuestra que no están realmente interesados en saber dónde está la información. Los Estados han expandido también sus investigaciones a la web públicamente accesible y parece que la línea divisoria que marca el límite está en el hecho de que se utilicen métodos coercitivos de investigación o si se necesitan pruebas. ¿Qué pensar de esta evolución?

Una primera observación es que esto no se ha visto seguido paralelamente por un desarrollo similar al de la presencia física de funcionarios de policía en otro país. Esto es algo lógico en la medida en que el ataque a la soberanía es ciertamente menor. Uno puede incluso preguntarse si hay algún ataque a la soberanía de otro Estado si las agencias policiales realizan búsquedas en la www públicamente disponible. ¿Por qué se va a violar la soberanía de un Estado que es incapaz de aplicar su legislación a una cierta situación sólo porque otro Estado desea hacer algo? ¿Qué es la soberanía estatal en el contexto del mundo cibernético?[217]

Las reglas estipuladas a este respecto son racionalizaciones de la soberanía, que siguen los modelos de la presencia física. Sin embargo, debe suscitarse la cuestión de si esto tiene sentido. ¿Qué Estado se ve involucrado cuando se navega por la web? Esto puede cambiar de un momento a otro. Los Estados pueden hasta no saber qu tenían soberanía sobre algo y cuándo. Si los Estados están tan preocupados por su soberanía, deberán hacer mucho más para protegerla. La soberanía tiene que ver con la competencia para determinar las reglas aplicables en tu territorio con la clara finalidad de proteger los intereses de tus residentes y al propio Estado. Los residentes tienen derecho y pueden reclamar determinadas expectativas respecto del Estado en el que viven.[218] Es una forma de contrato social de que sus derechos no se verán infringidos, salvo que así se prevea por la ley del Estado que les protege.

¿Cuáles son las legítimas expectativas de un ciudadano respecto de la www? Ningún Estado posee la www, ningún Estado puede garantizar que su legislación será siempre aplicable; algo posiblemente aún más importante: los Estados no son capaces de dar a los ciudadanos de internet la protección que podrían necesitar. La reclamación de soberanía requiere tener el poder de hacerla exigible y aplicarla, si fuera necesario, por la

[212] Alemania 13.
[213] Bélgica 9.
[214] Países Bajos 33.
[215] Países Bajos 35.
[216] EE.UU. 25 y 26.
[217] Ver sobre esta cuestión Propuesta de resolución 26: ". Las responsabilidades de un determinado Estado por violaciones de derechos humanos deberían decidirse tras el conocimiento de la violación y no como condición para la admisibilidad de una queja ante el mecanismo de supervisión."
[218] Propuesta de resolución 15: "Todas las personas tienen derecho a la protección por parte de un sistema nacional si la expectativa de protección por dicho sistema puede considerarse legítima.."

fuerza. Los Estados son demasiado débiles para hacerlo, la www es una responsabilidad compartida de la comunidad de los Estados.

Mirar al mundo cibernético como un área en la que los Estados comparten soberanía tiene varias consecuencias: los ciudadanos pueden hacer lo que quieran en la medida en que no infrinjan los derechos de los demás, pero lo mismo vale para las agencias policiales.[219] Para formularlo con una terminología concreta, las agencias policiales podrían practicar registros en internet con arreglo a su Derecho nacional si todos los aspectos de su intervención se dieran en el marco delimitado por las fronteras. Si esto incluye la producción de pruebas (un informe de lo que ven o leen / una muestra del contenido) si no hay a aplicación de medios coercitivos,[220] no parece haber impedimento alguno para su uso como pruebas,[221] en la medida en que no hay expectativa de protección. En esta argumentación, la línea decisoria es si existe una expectativa legítima de protección. Esto podría relacionarse con el registro de un servidor, el registro de un ordenador, la toma de control remoto de un ordenador personal, la infiltración por un agente encubierto en un grupo de discusión y similares.

¿Quién o qué Estado debe dar en estos casos la protección? Sólo puede ser el Estado que tiene el poder y la obligación de proteger. Si utilizo mi pc, es mi Estado doméstico del que espero recibir protección frente a las autoridades extranjeras que toman el control de mi ordenador. Este ejemplo muestra una vez más que la localización es importante. Tengo una demanda legítima de protección porque tanto mi ordenador como yo mismo nos encontramos en el país. Si esta perspectiva es correcta, hay que recomendar que en otras situaciones (datos en la nube) se determine el lugar donde se producen. Los ciudadanos que quieren ser protegidos tienen interés en la localización. Si la localización es difícil, es fácil predecir que los Estados (en ausencia de acuerdos internacionales) recurrirán a medios unilaterales. Es necesario por ello un acuerdo internacional sobre investigación para recogida de pruebas y aplicación de la ley, para poner al ciberespacio bajo el imperio de la ley. Esto es tanto más urgente cuanto que puede esperarse que los siguientes adelantos tecnológicos aumentarán las posibilidades de investigación con efectos extraterritoriales. En el futuro los Estados serán *de facto* capaces de hacer más por sí mismos.

4. Asistencia mutua en asuntos penales

En el apartado anterior nos hemos centrado en la medida en que los Estados pueden regular cosas por sí mismos y aplicar las técnicas investigadoras disponibles con base en su propia legislación. Se ha visto cómo los Estados pueden hacer algo para llevar el Estado de derecho al ciberespacio y evitar que la asistencia mutua se vea sobrepasada por el autoservicio. En este apartado nos fijaremos en las consecuencias que los desarrollos técnicos tienen para la asistencia legal mutua en asuntos penales.

La primera observación a realizar es que, según los informes, los Estados no han cambiado su legislación sobre asistencia mutua en asuntos penales. El Informe francés señala que el ciberdelito como tal no ha llevado a cambiar las características generales del Derecho francés en materia de asistencia internacional. Esto significa que las reglas aplicables antes de la llegada de la Sociedad de la información y la ciberdelincuencia no se han visto alteradas, y continúa siendo la base el que el Estado requirente envíe una solicitud al Estado requerido, que la examinará y ejecutará o rechazará, indicando las causas del rechazo. Las causas del rechazo continúan vigentes.[222] Los Estados informan de que se han introducido una amplia variedad de nuevas técnicas investigadoras, que permiten a las agencias policiales investigar en el mundo moderno.[223] Y si bien ciertamente la ciberdelincuencia llevó a algunas disposiciones específicas relativas a nuevas técnicas de investigación, esto no supuso un cambio en las características de la legislación.[224]

Alemania puede asistir a otros Estados con la interceptación de telecomunicaciones con base en su legislación de asistencia internacional en materia penal.[225] Puede hacerlo y sin necesidad de basarse en un tratado. Con todo, este país ha concluido diversos convenios bilaterales y multilaterales que especifican con mayor detalle las condiciones en las que se puede prestar esa asistencia. Además, se refiere a las decisiones marco 2003/577/JAI

---

[219] Propuesta de resolución 13: "Las agencias de persecución de delitos, al Igual que los ciudadanos, tienen el derecho de navegar por las redes TI libres, sin permiso de los proveedores, y con independencia de si el contenido contemplado se encuentra almacenado o no."

[220] Propuesta de resolución 17: "Sea cual sea la nacionalidad de la persona en cuestión Estado debería poder aplicar medidas coercitivas en otro Estado, salvo que lo permita el Estado del territorio."

[221] Propuesta de resolución 16: "Los Estados, con sujeción al Derecho interno, deberían poder usar libremente la pruebas que encuentren en redes TI públicamente accesibles."

[222] Es interesante ver que el Convenio sobre Ciberdelincuencia sigue plenamente los principios clásicos de la cooperación internacional en materia penal: solicitud por un Estado a otro para que le preste asistencia. La naturaleza de la asistencia internacional no ha cambiado por la emergencia de los ciberdelitos, ver Brasil 6.

[223] Propuesta de resolución 18: "Los Estados deberían implementar las técnicas investigadoras necesarias que les capaciten para prestarse asistencia muta respecto de los ciberdelitos, con base en el principio de proporcionalidad."

[224] Francia 17, Suiza 36 y 37.

[225] Alemania 10 y 11.

sobre embargo preventivo de bienes y aseguramiento de pruebas y 2008/978 sobre la orden europea de para obtención de pruebas.

Aun cuando Italia no ha ratificado todavía los convenios sobre asistencia legal mutual que específicamente tratan de la interceptación de telecomunicaciones, sí que proporciona asistencia en este área.[226] También España informa de que, excepto por lo que se refiere al Convenio UE de 2000 sobre asistencia mutua, no ha concluido convenios que específicamente traten de ello. Sin embargo, puede ofrecerse la interceptación a otros Estados con base en las cláusulas generales de los tratados de asistencia legal mutua.[227] Se aplican además las reglas generales de rechazo.[228] La introducción de estas nuevas técnicas no ha cambiado por sí misma las reglas de la cooperación internacional.[229]

Lo que emerge de los informes nacionales es que la sociedad de la información ha confrontado a los Estados con un nuevo desafío causado por la velocidad en que se desarrolla la vida en el mundo virtual.[230] El análisis del Relator alemán es que los cambios en la asistencia mutual provocados por la moderna tecnología son múltiples. Por un lado, los delitos cometidos mediante el uso de la moderna tecnología tienen casi por definición una dimensión transnacional. Como consecuencia de la limitación territorial de sus actividades, las autoridades policiales se ven obligadas a demandar la asistencia del extranjero. La fluidez de los datos unida al tiempo que precisan por su propia naturaleza los procedimientos de asistencia se presenta como un problema. De otra parte, el desarrollo de la moderna tecnología ha contribuido a nuevos métodos de investigación y creado la posibilidad de la transferencia electrónica de documentos entre las autoridades estatales.[231]

La importancia de la rapidez se reconoce también explícitamente por parte de los relatores suizos: "Una considerable cantidad de tiempo puede transcurrir desde la demanda de asistencia mutua y la emisión de una orden final y vinculante de vigilancia en el marco de los procedimientos de asistencia legal mutua. Esta larga duración contrasta fuertemente con la natural rapidez y fluidez de los datos electrónicos, que pueden moverse a través de las fronteras en segundos y no se encuentran frecuentemente almacenados por mayor tiempo. Por ello, estos datos pueden no estar ya disponibles cuando se concluyan los procedimientos de asistencia mutua. Los datos electrónicos difieren mucho, por tanto, de las piezas "tradicionales" de prueba, que persisten generalmente en el tiempo y no son fácilmente movibles de una localización a otra."[232] El Derecho suizo prevé por consiguiente una orden provisional de captura del tráfico de datos, que se ve seguida por un procedimiento formal de asistencia mutua antes de que la información obtenida sea transferida al Estado requirente.[233]

Obtención de una posición informativa[234]

Es la velocidad a la que van las cosas lo que ha forzado a algunos Estados a establecer y mantener su posición informativa. Sin estas medidas la información se hubiera perdido, o el intercambio de información podría no cumplir su función de prevención de los delitos. Esencialmente esto supone una nueva dimensión con fines de investigación criminal y asistencia mutua. Si en el pasado se necesitaban información y pruebas para responder a los delitos ya cometidos, en la actualidad, el intercambio de información tiene muchas veces que ver con la prevención de delitos futuros y la preservación de pruebas de infracciones a cometer más tarde.[235]

Especialmente como parte de un paquete de medidas relacionadas con el combate del terrorismo, los Estados se sienten ávidos de obtener una buena posición informativa con objeto de prevenir ataques terroristas u otros crímenes. Dado el uso del tráfico aéreo en el pasado, como medio de ataques terroristas, los Estados han dado prioridad a tener más conocimiento sobre los pasajeros y la carga. En relación con los pasajeros se han concluido los llamados acuerdos de Registro de Nombres de Pasajeros (PNR).[236] También se intercambian datos en otras áreas, como las transacciones financieras y asuntos de visados. Estos acuerdos no están exentos de crítica,

[226] Italia 9 y 14 y Brasil 7.
[227] España 5-10.
[228] Ver también Alemania 12, Francia 17, Japón 6.
[229] Algunas excepciones a esto serán objeto de comentario *infra*. China daría la bienvenida a una innovación de las reglas de asistencia mutua, China 7.
[230] Japón 4.
[231] Alemania 9, Suiza 37.
[232] Suiza 43.
[233] Suiza 43 y 44.
[234] Se refiere a la definición dada por Hans Nijboer, Relator general de la Sección III: "La existencia y el uso de cantidades enormes de información operativa es denominada a veces como posición informativa (*information position*) de las autoridades de investigación y persecución."
[235] Propuesta de resolución 21: "La información obtenida mediante la asistencia legal mutual con fines de investigación debería poder ser usada como pruebas, con sujeción al Derecho interno."
[236] Los acuerdos concluidos por la UE con los EE.UU. y con Australia en esta materia. Ver Decisión 2010/16/PESC/JAI del Consejo, de 30 de noviembre de 2009, relativa a la firma, en nombre de la Unión Europea, del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos, a efectos del Programa de seguimiento de la financiación del terrorismo, DO 2010, L 8/11.

especialmente por lo que se refiere a su capacidad de infracción de los derechos de intimidad y protección de datos.[237]

Debemos ser conscientes del hecho de que estamos entrando en la esfera del derecho a la intimidad. Si por una parte debería evitarse que el foco del debate se centre en los elementos de la protección de la intimidad, es, por otra parte, inevitable que algunos elementos del derecho a la intimidad sean objeto de debate. ¿En qué medida se van a intercambiar los datos para la investigación criminal y con qué bases jurídicas? ¿En qué medida las personas afectadas tienen la posibilidad de prevenir/corregir/borrar la información? ¿En qué medida puede utilizarse la información intercambiada como prueba?[238]

Los EE.UU. han concluido acuerdos sobre intercambio de datos PNR, SWIFT y Visa. Los EE.UU. tienen una unidad *on-call* disponible 24/7. Este es también el caso de los Estados miembros de la UE, excepto Dinamarca.[239] Francia ha concluido tratados bilaterales de intercambio de información entre las autoridades policiales, con, entre otros, Serbia.[240] Suiza concluyó diversos convenios al respecto con los EE.UU., Canadá y estableció vínculos con Europol y Sirene.[241]

Un desarrollo más reciente es el establecimiento de bases de datos supranacionales y la consulta *online* de las bases de datos de otros. Un ejemplo de esto existe en la UE, donde algunos Estados miembros han establecido un mecanismo para acceder a datos de ADN, licencias de vehículos y huellas digitales directamente desde otro Estado miembro.[242] Varios Estados de la UE informan de que se ha desarrollado ya esta práctica.[243] También otros datos, como los datos de visado, la información de aduanas, los antecedentes judiciales y el sistema de seguimiento de la explotación de niños resultan ya accesibles y usados. Una de las consecuencias es que ya no se le pide que dé la información al Estado cuyos datos son usados, y no tiene que tomar ninguna decisión sobre casos individuales. También significa que las causas de rechazo ya no son consideradas ni aplicadas en el estado inicial del intercambio de información.[244] La información que un Estado Miembro puede ver solo puede utilizarse como prueba con el permiso del Estado Miembro que la introdujo en el sistema. ¿Es éste un buen avance? En el marco de la UE se han desarrollado planes ulteriores para crear un acceso directo a los registros de antecedentes penales de todos los Estados miembros.[245] Los desarrollos aquí recogidos son predominantemente europeos y de los EE.UU. La UE también ha concluido diversos acuerdos sobre intercambio de datos relativos a transacciones financieras: como lo ya mencionado con los EE.UU., y con Suiza y Japón.[246] Además, ha adoptado la Decisión 2008/633 que da a Europol acceso al Sistema de Información de Visados. Parece que en los EE.UU. se distingue entre información a presentar en el proceso e inteligencia. La primera requiere una solicitud formal, la segunda puede ser lograda más fácilmente mediante la consulta directa.[247]

Todos los Estados informantes participan en Interpol. La mayoría de ellos participan en Europol. Los Países Bajos informan de que la UE ha adoptado la iniciativa de establecimiento del Centro Europeo de Ciberdelincuencia EC3, que tiene su sede en las instalaciones centrales de Europol.[248] Japón y otros 14 países de Asia-Pacífico participan en la Red de Tecnología de Información sobre Ciberdelincuencia (*Cybercrime IT Network system)*, que

[237] Francia 31 y 32.
[238] En el contexto de la UE, se ha adoptado un instrumento legal especial para regular reglas de protección de datos en el marco de la cooperación en materia penal. Ver Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO 2008, L 350/60.
[239] Dinamarca 6.
[240] Francia 30.
[241] Suiza 48 y 49.
[242] Decisión 2009/1023 del Consejo de 21 de septiembre de 2009 relativa a la firma, en nombre de la Unión Europea, y a la aplicación provisional de determinadas disposiciones del Acuerdo entre la Unión Europea, Islandia y Noruega para la aplicación de determinadas disposiciones de la Decisión 2008/615/JAI del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, y de la Decisión 2008/616/JAI del Consejo relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, y de su anexo, DO 2009, L 353/1; Decisión 2008/615/JHA del Consejo de 23 de junio de 2008 sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO 2008, L 210/1.
[243] Finlandia 8, Polonia 8, Países Bajos 38, Italia 11.
[244] Con todo, los instrumentos jurídicos relevantes estipulan que si la información va a utilizarse como pruebas, debe seguir una solicitud regular de asistencia internacional.
[245] Decisión Marco 2009/315/JHA del Consejo, de 26 de febrero de 2009 elativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros, DO 2009, L 93/23.
[246] Alemania 15.
[247] EE.UU. 37.
[248] Países Bajos 20. Ver también Bélgica 8.

fue creada en 2001.[249] Casi todos los Estados informan de que tiene una disponibilidad 24/7 para las solicitudes de intercambio de información y asistencia.

No parece que haya problemas en aquellas situaciones en que se solicita la asistencia legal mutua. Un ejemplo se da en el Informe de los EE.UU. Los EE.UU. consideran que sus intereses se encuentran suficientemente protegidos a través de las causas de rechazo existentes. Como el Derecho de EE.UU. prevé una serie de medidas de interceptación de telecomunicaciones, también es posible hacer uso de ellas a partir de la solicitud de una autoridad extranjera. Con todo, los EE.UU. solo pueden satisfacer demandas de asistencia de interceptación de comunicaciones si estaban autorizadas de manera independiente como de una investigación ligada o paralela en los EE.UU. y la revelación de los contenidos de las comunicaciones interceptadas se considera de algún modo apropiada.[250] Esto significa que debe haber una orden judicial en los EE.UU.

En algunos Estados se exige la doble incriminación para algunas demandas relativas a pruebas.[251] En otros, se indica que la doble incriminación podría ser abolida.[252] Los EE.UU. han desarrollado una práctica de no exigencia de la doble incriminación en los Tratados que firman sobre Asistencia Legal Mutua.[253] Los Relatores daneses mencionan que los delitos relacionados con ordenadores son una de las categorías de delitos recogidas en la lista del art. 2 de la Decisión Marco 2002/584 sobre Orden de Detención Europea, lo que significa que en los procedimientos de extradición no se controlará en lo sucesivo la doble incriminación.[254] Esto es también relevante para las demás formas de cooperación con la UE basadas en el principio de reconocimiento mutuo.

Los peligros parecen surgir cuando no se solicita la asistencia mutual en material penal, sino que simplemente se obtiene en autoservicio. Esto puede llevar a una situación en la que no puedan llegar a aplicarse las causas tradicionales de rechazo (doble incriminación, tipo de delito, *ne bis in idem*). ¿Sería entonces posible o necesario reducir la aplicación de las causas de rechazo en esta área? Esta es una cuestión relevante en la medida en que se informa que al margen de la asistencia internacional formal, también se ofrece asistencia contorneando las vías oficiales.[255] El problema o reto clave reside una vez más en la localización de la información o prueba que se necesita. La nube, en particular, pone en cuestión los métodos tradicionales de asistencia legal mutual y sus elementos clave, como la solicitud previa. Las dificultades de localización de los datos requeridos tienen también un impacto en la cooperación internacional, en la medida en que hacen difícil saber a quién dirigir la solicitud de asistencia.[256]

El papel en todo esto de las partes privadas no debe ser subestimado, como lo demuestra la referencia al caso belga Yahoo de 2007.[257] Las autoridades belgas querían obtener información de Yahoo y solicitaron ayuda a la rama belga (*Yahoo Customer Care*). Esta rechazó el suministro de la información remitiendo a sus oficinas centrales en EE.UU. Las autoridades belgas solicitaron entonces asistencia a las autoridades de los E.UU. Este es sólo un ejemplo de situaciones en las que las partes privadas muestran cómo no consideran su función convertirse en ayudantes de los funcionarios de policía. Uno puede entender en cierta medida que dar asistencia a la policía supone tiempo y cuesta, por tanto, dinero. Sin embargo, en todo sistema de justicia penal los ciudadanos pueden ser obligados de cooperar con las investigaciones, incluso si les cuesta tiempo y dinero. En el ciberespacio las partes privadas operan como milicias, piratas u otro tipo de entidades autónomas y eluden lo anterior como resultado de la debilidad de los Estados de exigir el respeto y defender su soberanía.

¿Qué decir sobre las obligaciones de retención de datos sobre la transmisión de información? ¿Tienen los proveedores la obligación de organizar su red de manera que pueda cumplir con las tan diferentes y complicadas solicitudes de asistencia provenientes de las agencias de aplicación de la ley de los demás Estados?[258] ¿Cómo puede esto exigirse respecto de proveedores que no tengan su sede en el Estado relevante? Otro ejemplo problematico surge cuando la policía desea conocer quién aloja un sitio web. Técnicamente la policía puede mirar en el servidor web e identificar así las direcciones IP reales de otro país. En ese momento, existe la posibilidad de obtener prueba y hacer que el sitio web resulte inaccesible a los demás.[259] El Derecho turco contempla al Estado

[249] Japón 10.
[250] EE.UU. 22.
[251] Argentina 5, Turquía 12. El Derecho Japonés mantiene la doble incriminación, salvo en relación con los EE.UU., ver Japón 6.
[252] España 10. Ver además la Propuesta de resolución 20: "situaciones en las que hay un entendimiento común de los ciberdelitos, debería promoverse la eliminación del requisito de la doble incriminación como condición para la asistencia legal mutua."
[253] EE.UU. 25.
[254] Dinamarca 5.
[255] Suiza 37.
[256] Koops y otros, p. 7.
[257] Koops, p. 22.
[258] Los proveedores japoneses están obligados a cooperar con la policía japonesa, Japón 5.
[259] Koops y otros, p. 46.

donde el proveedor tiene su sede legal como el Estado al que deberían remitirse las demandas de asistencia legal mutua.[260]

Las dificultades de localización y ejecución apoyan la propuesta de un acuerdo internacional que regule en qué circunstancias puede obligarse a las partes privadas a establecer sus sistemas de manera que pueda obtenerse la información necesaria. Una opción podría ser obligarles a localizar actividades en el mundo cibernético (incluso aplicando una ficción legal). Esta opción podría también apoyar la faceta protectora de la localización. La existencia de diferentes estándares en las reglas de protección de datos se considera también un obstáculo para la asistencia internacional.[261] En Argentina, Brasil y España existe el concepto de *habeas data*, que autoriza al ciudadano a conocer y solicitar la corrección o borrado de los datos que le conciernen.[262]

Otra opción podría ser que se llegue a un acuerdo internacional sobre las circunstancias en que los Estados pueden llevar a cabo acciones unilaterales y aplicar técnicas específicamente reguladas. Es interesante ver que cada vez surgen más formas de cooperación que pueden ser contempladas como métodos especiales o específicos de investigación. Lo que esos métodos tienen en común es que no resulta claro en el momento de su aplicación si los delitos serán al final perseguidos en un Estado o en otro. Además, se han desdibujado los clásicos roles de Estado requirente y requerido. El progreso tecnológico de la sociedad de la información llevará a una grave disminución de la asistencia mutua en materia penal tanto *de iure*, como *de facto*.

5. Ejecución en la nube

Las casi ilimitadas posibilidades de la tecnología de la información suscitan cuestiones en relación a si los Estados pueden ejecutar directamente sentencias o medidas provisionales haciendo uso de la tecnología de la información, sin pedir permiso a cualquier otro Estado. Parece que sobre este tema el deseo de intervenir y las posibilidades técnicas de hacerlo deben conciliarse con el hecho de que puede violarse la soberanía de otro Estado.[263]

En una situación en la que hay una decisión legal de que un cierto sitio web debe cerrarse porque contiene pornografía infantil, discursos de odio u otro material ilegal, ¿debería autorizarse a las agencias policiales a hackear el sitio con el fin de prevenir la comisión de ulteriores delitos desde el mismo? Es por ello relevante examinar tanto la posibilidad de adopción de medidas provisionales como la de ejecución de las decisiones firmes.

Muchos Estados informan de la inexistencia de medios legales para cerrar un sitio web.[264] Frecuentemente la referencia va hacia las obligaciones del proveedor de borrar el contenido ilegal. En los Países Bajos esto supone que el Fiscal puede ordenar a un proveedor a hacer algo. No hacerlo constituye una infracción penal.[265] Pero, si el proveedor se encuentra fuera de los Países Bajos, no podrá ejecutarse.

Con base en el Derecho turco de internet, los tribunales pueden ordenar la "medida provisional" ("*precautionary measure*") de impedir el acceso al contenido de un sitio específico. Se informa que como consecuencia del hecho de que los legitimados a recurrir la medida ante los tribunales turcos se encuentren en el extranjero, la medida puede alcanzar carácter definitivo.[266] El vínculo necesario mínimo para que Turquía pueda adoptar esa medida es que pueda haber acceso al contenido desde Turquía. El Derecho polaco prevé un procedimiento de notificación y cierre en el art. 14 de la Ley de Servicios Electrónicos de 2002.[267] Dinamarca puede confiscar un dominio si contiene materiales ilegales.[268] Pueden hacer lo mismo España, con base en la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico,[269] y Bélgica con base en el art. 39bis par. 3 del Código Procesal penal.[270] Francia puede aplicar su Ley n° 2011-267 de 14 de marzo de 2011 de orientación y programación para el desarrollo de la seguridad interior (LOPPSI II).[271]

Italia tiene medios jurídicos para denegar el acceso a los usuarios italianos mediante una orden dirigida al proveedor del servicio.[272] La nacionalidad del sitio web es irrelevante. Si la autoridad judicial decide proceder a la

[260] Turquía 3.
[261] Turquía 12, Francia 23, Suiza.
[262] Brasil 9.
[263] Propuesta de resolución 19: "Los Estados deberían ser, en particular, capaces de suministrar rápida asistencia y debería introducirse una orden provisional de preservación de los datos. La obligación de preservación de los datos debería ser sólo por un tiempo razonable."
[264] Suecia 3, Brasil 9, Alemania 15, Japón 10.
[265] Países Bajos 22.
[266] Turquía 3 y 24.
[267] Polonia 8.
[268] Dinamarca 7.
[269] España 11.
[270] Bélgica 8.
[271] Francia 23. Con todo, esto no autoriza a aplicar expediciones *fishing* remotas en ordenadores personales, ver Francia 33.
[272] Italia 14.

captura de un sitio web, emite una orden al proveedor italiano del Servicio, que debe desactivar el acceso en Italia. Los EE.UU. pueden hacer uso de un proceso de notificación y cierre con base en una orden judicial. Existe una amplia práctica en relación con las infracciones de copyright.[273] El Relator nacional es de la opinión de que un sistema de ejecución internacional para implementar decisiones, como las órdenes de supresión o inhabilitaciones en el área del ciberdelito, solo puede tener éxito en el contexto de un tratado que tenga una participación sustancial por parte de los Estados a lo largo y ancho del mundo y sea implementado por una organización de afiliación casi universal.[274] Hay bastante escepticismo en cuanto a la posibilidad de un sistema de estas características.[275] En todo caso, la complejidad de la ejecución en un mundo virtual exige un acuerdo internacional.[276]

Resulta claro de los pocos Estados que informan sobre el punto relativo a la ejecución que, una vez más, la localización del dónde tiene lugar el acto de cierre o borrado de los datos es una cuestión clave. Los Estados que intervinieron localizaron la responsabilidad en el proveedor. Esta es una herramienta que puede incrementar las posibilidades de ejecución de las decisiones. Sería preferible que los Estados pudieran llegar a un acuerdo sobre lo que pueden hacer y no con y sin la asistencia de otros Estados.[277] Esto no solo es relevante de cara a la investigación y persecución, sino también para la defensa. Cuando las responsabilidades están claras, es más fácil para la defensa reclamar sus derechos. Sin claras responsabilidades existe una gran oportunidad de que los recursos jurídicos tampoco puedan localizarse.

6. La sala de vistas virtual

En este apartado nos fijaremos en las consecuencias de las nuevas posibilidades de preparación de la investigación y desarrollo de las vistas. La telecomunicación moderna crea la posibilidad de contacto directo con el acusado, las víctimas y los testigos. ¿Debería autorizarse y, en tal caso, en qué condiciones? En caso negativo, han de aplicarse las reglas clásicas de asistencia mutua (demanda y respuesta) y por qué?

La notificación de sentencias, decisiones, citaciones y otros documentos jurídicos puede tener consecuencias jurídicas. De manera similar a las notificaciones en papel del viejo estilo, el Derecho ligará esas consecuencias también a las notificaciones enviadas por medio de la tecnología de la información.[278] Con base en el Derecho alemán, las autoridades alemanas pueden contactar directamente con las personas que se encuentran en el extranjero cuando no pueda esperarse que el otro Estado lo vaya a considerar una violación de su soberanía.[279] El Informe de los Países Bajos puede imaginar que los sospechosos y testigos sean contactados por email e invitados al proceso de esta manera.[280] El Derecho francés es muy abierto respecto del uso de las nuevas técnicas en el proceso penal: "La utilización de las nuevas tecnologías de la comunicación puede ser útil para llevar a cabo diversos actos procesales. Puede serlo especialmente para facilitar la audición de testigos, peritos, víctimas o acusados durante la investigación o instrucción, o en la fase de enjuiciamiento en la vista. Esta posibilidad existe en Francia en virtud de las disposiciones del Código procesal penal relativas a la utilización de medios de telecomunicación en el proceso (art. 706-71)."[281]

Como los contactos entre las personas se hacen cada vez más por medio de elementos electrónicos, la cuestión que se suscita es si la administración de justicia debería seguir como hace siglos.[282] Los billetes de avión se emiten electrónicamente, las citas con el dentista se hacen por sms, y las invitaciones a todo tipo de reuniones se envían por email. En algunos las nuevas leyes ya no se imprimen en papel, sino que sólo se publican en formato digital en el sitio web del gobierno. Se informa de que es posible que los tribunales de los Países Bajos sólo tengan registros digitales de las actas en un futuro próximo. Para ambos aspectos: la facilitación de la

[273] EE.UU. 34 y 35.
[274] EE.UU. 36, Turquía 25, Países Bajos 41, Brasil 10, Bélgica 4, España 11.
[275] Polonia 9, Italia 15, Dinamarca 7, Japón 10.
[276] Propuesta de resolución 2: "Los Estados deberían considerar el acceso a los instrumentos internacionales existentes sobre cibercriminalidad o desarrollar otros mecanismos jurídicos internacionales con el fin de establecer el estado de derecho en el ciberespacio y evitar potenciales conflictos entre los Estados con ocasión de la aplicación de sus políticas y legislación en el ciberespacio."
[277] Propuesta de resolución 22: "La decisión (provisional) de un tribunal penal de cierre de un servidor, sitio web o elementos similares debería poder ser ejecutada de manera directa si así lo establece un acuerdo internacional o la ley del Estado en el que se localiza el proveedor del servicio."
[278] Se informa de que los Países nórdicos lo están discutiendo (Suecia 3). En 2010, e.g., los servicios postales alemanes introdujeron la distribución electrónica, similar a la notificación formal por un ujier.
[279] Alemania 17.
[280] Países Bajos 51.
[281] Francia 32.
[282] Propuesta de resolución 27: "Las autoridades podrán enviar comunicaciones directamente a los acusados, testigos, víctimas y peritos que se encuentren físicamente en otro Estado, siempre que dicho Estado acepte este método de comunicación."

administración de justicia y de la investigación preliminar, personalmente estaría a favor del uso del contacto directo con testigos, víctimas, peritos, acusado y su abogado.

Testimonio por video

Muchos Estados informan de la práctica del uso de videoconferencias, audiencias con uso de skype, envío por email de documentos escaneados, etc.[283] El Informe italiano señala que: "La tecnología de la información puede facilitar la asistencia mutua, sin cambiar su naturaleza. (…) Las peculiaridades de la tecnología de la información hacen posible llevar a cabo actividades tradicionales como el testimonio, sin que se necesite trasladar a la gente a un Estado extranjero. (…) Sin embargo, es difícil creer que estos nuevos métodos puedan ser aplicados sin la asistencia de la autoridad del Estado involucrado."[284] No obstante, otros Informes nacionales subrayan el cambio producido: "El desarrollo de la tecnología de la información, como, por ejemplo, los satélites terrestres en órbitas medias y bajas y los servidores extranjeros, han impactado de manera profunda en la naturaleza misma de la asistencia legal mutua. Se ha creado la necesidad de cooperación y asistencia legal mutua cuando tal necesidad no existía antes, añadiendo una dimensión internacional a situaciones que anteriormente eran meramente nacionales."[285]

Los Derechos turco, polaco, italiano, danés, español y finlandés prevén videoconferencias con testigos y peritos.[286] Polonia (causa obligatoria de rechazo) y los Países Bajos (causa opcional de rechazo) han excluido explícitamente la videoconferencia con el acusado.[287] El sitio de justicia electrónica de la UE recoge en una lista todas las instalaciones de la UE que tienen capacidad para videoconferencias. Aun cuando los Estados están ampliando las posibilidades, no puede excluirse que la diferente velocidad a la que los Estados pueden suministrar la infraestructura tecnológica pueda llevar a situaciones en las que el Estado requerido no pueda ofrecer la asistencia demandada, por carecer de esa técnica.

Muchos Informes nacionales no ven impedimento legal para el uso de videoconferencia, depende del otro Estado.[288] Skype es una alternativa a las llamadas telefónicas, conforme al Informe belga.[289] El Informe italiano sugiere que durante la investigación puedan autorizarse contactos directos con las víctimas y testigos potenciales.[290] Pero es diferente una vez que se ha llegado al nivel del juicio. Entonces es preciso realizar una solicitud formal de asistencia.[291] La resistencia en Alemania en cuanto al interrogatorio de testigos encuentra su base en el principio de inmediación, que exige que toda la prueba deba presentarse en la vista. Con todo, el Derecho alemán prevé una excepción en el caso de testigos que se encuentran en el extranjero y no son capaces o no están dispuestos a viajar hasta la sala de vistas.[292] La audiencia del acusado por medio de la pantalla no es posible en la mayor parte de los casos porque viola la obligación del acusado de estar presente.[293] Sólo en casos menores es posible no renunciar a esta obligación. El Relator nacional de Alemania alude a las ventajas de las videoconferencias en comparación con la lectura de testimonies escritos en cuanto a la facilitación de los procesos y mayor calidad de la prueba y el uso del derecho de confrontación, que no es posible por medio de los escritos leídos. Sin embargo, en comparación con la comparecencia personal de los testigos sigue habiendo desventajas, pues no es posible la impresión directa respecto del testigo.[294]

El Informe nacional francés apunta otra limitación relativa a los estándares de derechos humanos. El uso del testimonio vía videoconferencia debe respetar el derecho a un juicio justo conforme al art. 6 del Convenio europeo de derechos humanos.[295] Los Estados no están completamente de acuerdo sobre la cuestión de si la presencia física del acusado o testigos es una necesidad absoluta. Cuando se alude a las obligaciones en materia de derechos humanos debe indicarse que ni la presencia física del testigo ni la presencia de acusado constituye una exigencia absoluta con arreglo a los tratados de derechos humanos. Respecto de ambos son posibles las excepciones. Es el sistema de justicia penal nacional el que establece aquí los límites. La cuestión que se suscita es si la búsqueda de la mejor prueba obliga siempre a la presencia física por ser considerada la situación ideal.

---

[283] Argentina 8, Brasil 12, Alemania 17 y 18.
[284] Italia 7 y de manera similar Bélgica 6.
[285] Bélgica 5.
[286] Turquía 28, Finlandia 9, Polonia 10, Países Bajos 49, Italia 18, Dinamarca 8, España 12.
[287] Polonia 10, Países Bajos 50.
[288] Suecia 3, España 13.
[289] Bélgica 10.
[290] Similarmente Bélgica 9.
[291] Italia 17.
[292] Alemania 17 y 18.
[293] Una cuestión es si la presencia puede ser sólo presencia física.
[294] Alemania 17 y 18, Japón 13.
[295] Francia 32 y 33, Italia 17.

Del informe danés: "Deberían respetarse la soberanía de los Estados, los principios del proceso debido y las reglas procesales fundamentales (p.e. traducción a la lengua nativa del sujeto, autoacusación y las reglas relativas al juramento y testigo no apremiable). El contacto directo entre el acusado y el Estado extranjero lo convertirían en una difícil tarea."[296] Es interesante ver que la preocupación tanto por la soberanía como por el juicio justo puede llevar a una resistencia contra los Estados. Personalmente vería la necesidad de salvaguardar los derechos de los individuos contactados por la vía de la moderna tecnología. Cualquier persona que reciba cualquier tipo de notificación debe ser informada de las consecuencias de (no) responder a la misma. Las personas que testifican desde el extranjero deben saber si están obligadas a hacerlo, conocer las reglas de perjuio y los privilegios de los testigos.

La sala de vistas virtual

¿Podemos imaginar una sala de vistas virtual, en la que tenga lugar la vista sin presencia de nadie en la sala de vistas real?[297] Si bien el Informe brasileño puede prever un desarrollo futuro en esta línea, [298] el Informe italiano se opone muy claramente a este escenario.[299] El Informe argentino sugiere que podremos ver una cierta "litigación digital" en un futuro próximo: "La computación en la nube (*cloud computing*), será uno de los temas con los que tendrá que lidiar en los próximos años la introducción e implementación del expediente digital."

El simple hecho de que se haya convertido en algo crecientemente simple el hablar con personas en el extranjero a través de técnicas audiovisuales (skype, videoconferencia) suscita la cuestión de si esto no debería llevar al establecimiento de un nivel más alto de exigencia respecto de la extradición con fines de persecución penal. Si el acusado no está presente en el Estado que le persigue puede tener lugar la extradición. A la vista de la grave violación de la libertad del acusado que ello supone, puede suscitarse la cuestión de si no debería preferirse el desarrollar el juicio mediante una conexión de video.[300] También la presunción de inocencia se opondría a la gravosa extradición. ¿Deberíamos reservar la extradición para los condenados?

Seguridad de la comunicación

Es necesario verificar la identidad del remitente de mensajes vía email y similares.[301] La confidencialidad de las líneas de comunicación debe asegurarse.[302] Se critica al Convenio sobre Ciberdelincuencia por no ofrecer suficientes garantías para la confidencialidad.[303] La seguridad de la información debe igualmente garantizase. Esta es una de las razones para involucrar a otro Estado.[304] La protección de la confianza y la rigurosidad de las líneas de comunicación es de la máxima urgencia.[305]

7. Derechos Humanos reales en un mundo virtual

Gradualmente parece claro que la dificultad de localización de datos, conductas e infracciones tiene un gran impacto en la protección de los derechos humanos. Los mecanismos de supervisión de los derechos humanos otorgan derechos a los individuos frente al Estado en cuya jurisdicción se encuentran.[306] Esto requiere, por tanto, que pueda identificarse que los derechos humanos afectados se encuentran dentro de la jurisdicción. Como con todo lo relativo al ciberespacio, esto puede ser difícil. Anteriormente yo consideraba que el mundo cibernético tiene las características de un área en la que se comparten las responsabilidades. Cuando se comparten las obligaciones, los derechos humanos son especialmente vulnerables, porque hay que identificar qué Estado debe usar sus poderes de protección.[307]

El Informe suizo apunta a la vulnerabilidad de los derechos humanos en el ciberespacio: "Diversos derechos humanos del la Constitución suiza (que encuentran frecuentemente su correspondencia en las constituciones cantonales) son potencialmente puestos en cuestión en el contexto de investigaciones penales con uso de tecnología de la información. Entre ellos, el derecho a la intimidad de la vida familiar y privada de las personas, en

---

[296] Dinamarca 8.
[297] Propuesta de resolución 29: "Debería animarse a los Estados a considerar la posibilidad y condiciones de recogida de prueba mediante tecnología digital, incluso aun cuando el individuo no se encuentre físicamente presente en la vista."
[298] Brasil 12.
[299] Italia 8.
[300] Propuesta de resolución 28: "Siempre que lo consienta el individuo afectado, deberían ampliarse las posibilidades de uso de la tecnología digital, como los viodeolinks, con objeto de disminuir la necesidad de medidas tan intrusivas como la extradición."
[301] Países Bajos 23.
[302] Francia 32.
[303] Francia 36.
[304] Italia 17.
[305] Propuesta de resolución 30: "La seguridad y confianza de las líneas de comunicación en uso por parte de las autoridades debe ser de mayor nivel. Las comunicaciones deberían protegerse frente al pirateo."
[306] Japón 11 y 12.
[307] Propuesta de resolución 23: "Los Estados respetarán los estándares de derechos humanos internacionalmente reconocidos también en el contexto del mundo digital."

su hogar y en relación con su correo y telecomunicaciones, el derecho a protección contra el uso abusivo de sus datos personales y la libertad de expresión e información."[308] El Tribunal Constitucional alemán ha desarrollado el derecho a la integridad y confidencialidad de los sistemas informáticos, que resulta también aplicable en un contexto de cooperación.[309] El Derecho suizo obliga a los funcionarios de policía a obedecer la Constitución sea cual sea el lugar en el que se encuentren.[310] En suma, los derechos potencialmente violados son el derecho a la intimidad y libertad de expresión y posiblemente el derecho a un juicio justo. Otros derechos que exigen la presencia física, como la protección de la vida, la prohibición de la tortura y el derecho a la libertad son menos vulnerables en el mundo virtual.

En sus respuestas a la cuestión relativa a los derechos humanos los Relatores nacionales no informan de aspectos específicos. El cuestionario no estaba probablemente bien redactado pues se dirigía a obtener una imagen de la responsabilidad que los Estados pueden tener por los derechos humanos violados por otros Estados o por violaciones en las que no es posible derivar la responsabilidad estatal.[311] Los Relatores nacionales suecos sugieren que su país puede resultar responsable por abuso de información transmitida a otro Estado.[312] Las autoridades turcas no pueden utilizar material como prueba si se ha recogido por las autoridades extranjeras en violación de las reglas de derechos humanos.[313] Conforme al Derecho japonés, la prueba ilícitamente recogida en cualquier lugar puede ser inadmisible en un proceso penal en Japón. En un caso en el que el acusado fue interrogado en China, la fiscalía japonesa estuvo presente en los interrogatorios en Chica, con el fin de evitar toda cuestión relativa a violaciones de derechos humanos.[314]

El Informe francés describe un interesante caso en el que las autoridades policiales de EE.UU. crearon un sitio en internet destinado a atraer a pederastas.[315] Cuando un francés mostró interés la información fue transmitida a las autoridades francesas que hicieron uso de la misma en el contexto de una investigación criminal. La *Court de Cassation* no tuvo en cuenta la información obtenida por las autoridades americanas, por considerar que se trataba de una trampa en violación del derecho a un juicio justo protegido por el art. 6 CEDH. El Relator nacional cita a un autor criticando a las autoridades policiales que señalaban que el ciberdelito debe ser combatido por sus mismos medios. Sin embargo, el Estado de derecho obliga a las autoridades estatales a respetar el derecho a un juicio justo, incluso frente a personas que no respetan el Derecho.[316]

8. Conclusiones

En suma, parece que el impacto de la sociedad de la información en el Derecho penal internacional es triple. Primero, la sociedad de la información genera una amenaza transnacional para ciertos bienes jurídicos, si bien otros quedan sin resultar afectados por ella. En segundo lugar, la sociedad de la información crea, por otra parte, una herramienta para la justicia penal. El tercer impacto de importancia tiene que ver con la pérdida de soberanía. La sociedad de la información ha hecho disminuir gravemente (o hasta eliminado) el valor e importancia de la territorialidad. Como la localización es difícil, imposible o en desplazamiento permanente, esta es la cuestión clave del ciberespacio. En todos los aspectos el ciberespacio no presenta suficiente permanencia para permitir a los Estados reclamar por su soberanía sobre todo lo que sucede.

El principal reto es por tanto reconocer la responsabilidad compartida de los Estados en relación con el mundo cibernético. Guste o no, el Derecho penal y la ejecución en la práctica deben aprender a vivir con la pérdida de localización. No debe verse como exagerado el decir que es tiempo de repensar la aplicación del Derecho. Osinga lo describió de la manera siguiente: "Todavía utilizamos el léxico del mundo físico para describir el ciberespacio –"entramos", "navegamos", "nos movemos por", hay lugares, surfeamos, almacenamos y a veces nos perdemos en él, pero no hay ahí ahí: es un espacio desterritorializado. Y de forma distinta a otros ámbitos el ciberespacio no tiene obstáculos físicos, ni límites "reales" como una costa. Es más, la distancia y el tiempo no tienen sentido en su significado tradicional, de hecho, en el ciberespacio la distancia desaparece. Los datos pueden aparecer de maneras simultánea o casi en diversos lugares."[317] Todo ello suscita la cuestión de si

[308] Suiza 51.
[309] Alemania 17.
[310] Propuesta de resolución 24: "Si los Estados actúan extraterritorialmente al investigar en el ciberespacio, respetarán los estándares de derechos humanos aplicables en su jurisdicción (*agent control standard*)."
[311] Propuestas de resolución 25 y 26: "25. Los Estados deberían grabar las investigaciones en el ciberespacio con vistas a asegurar la responsabilidad del Estado en caso de violaciones de derechos humanos. 26. Las responsabilidades de un determinado Estado por violaciones de derechos humanos deberían decidirse tras el conocimiento de la violación y no como condición para la admisibilidad de una queja ante el mecanismo de supervisión."
[312] Suecia 3, similarmente, Italia 17, Brasil 11, Bélgica 8, Alemania 17.
[313] Turquía 27.
[314] Japón 12 y 13.
[315] Francia 36 y 37.
[316] Francia 37, nota 95, citando a Chilstein.
[317] Frans Osinga, Introducing Cyber Warfare, in: Paul Ducheine, Frans Osinga, Joseph Soeters (eds.), Cyber Warfare, Asser Press, The Hague 2012, p. 9.

deberíamos tener igualmente en cuenta que la localización puede no ser posible. Este Informe General parte de la presunción que la localización es posible bien directamente o mediante el uso de una ficción jurídica, como lo es la localización de los datos en el proveedor.

El sentimiento general al leer todos los Informes nacionales es que tanto la legislación estatal como los tratados convencionales van muy por detrás de lo técnicamente posible y es hora de dar unos pocos pasos. En el Informe brasileño esto se resume de la manera siguiente: "en tiempos en los que la información trafica de manera excesivamente veloz y sin respetar fronteras, la armonización legislativa entre los países puede generar efectos benéficos al combate de la criminalidad informática."[318] Es necesario evitar que llegue a un estado de anarquía.

Como ningún Estado es completamente capaz de aplicar su legislación en el ciberespacio, los derechos humanos se encuentran desprotegidos en el mundo virtual. Tal vez esto puede remediarse si también se localizan las obligaciones de derechos humanos. Siguiendo las reglas de localización de las conductas y datos, resulta que el proveedor podría ser tomado como punto de referencia para la aplicación de la legislación de un específico Estado. Es lógico que si el Estado aplica su legislación a algo, que ello suponga también la aplicación de los derechos humanos.

La libertad creada por el ciberespacio tiene muchas facetas de las que se han beneficiado los individuos. Sin embargo, se ve que también existen graves peligros para esa libertad.[319] Si los Estados no son capaces de encontrar una vía para diseñar su responsabilidad sobre internet y llevarlo al Estado de derecho, el ciberespacio se asimilará a un Estado de anarquía. Y esto resultaría en un mundo en el que las reglas relativas al crimen organizado y en materia de derechos humanos quedarían sin sentido.

[318] Brasil 5 y 6.