Facultad de Derecho

Informe legislativo 7/2022

Proyecto de ley de "seguridad en línea" de Reino Unido

Lucía Camacho G.
CELE

Agosto de 2022

"Esta legislación histórica acabará con la era de la autorregulación".[1] Esas es una de las expresiones que justifican y condensan el objetivo del proyecto de ley de seguridad en línea que está siendo tramitado en Reino Unido.

El proyecto busca hacer de ese país el más seguro en internet. Su articulado se dirige al contenido generado por los usuarios *user-generated content* y los servicios de búsqueda para luchar contra el contenido dañino e ilegal en contra de los menores de edad y de los adultos.

En el logro de ambas tareas prevé un nuevo "deber de cuidado" a cargo de las plataformas en línea, endurece el deber de transparencia que tienen a cargo, crea un nuevo estándar de valoración del contenido dañino según el riesgo que representa para cada uno de estos dos tipos de audiencia e incentiva a las plataformas para identificar y actuar contra el contenido ilegal y dañino en internet.

Antecedentes y trámite

Los antecedentes de la iniciativa datan de 2019 cuando se publicó la primera consulta escrita de un cuestionario con 18 preguntas y a la que respondieron más de 2,400 personas y organizaciones de la sociedad civil, academia, sector privado, entre otros.

La consulta se extendió desde el mes de abril y concluyó en el mes de julio. En ese mismo tiempo el gobierno sostuvo encuentros con múltiples partes interesadas para discutir su

[1] "This landmark legislation will end the era of self-regulation", ver pg. 1 del "Memorandum from the Department for Digital, Culture, Media and Sport and the Home Office to the Delegated Powers and Regulatory Reform Committee", publicado el 12 de mayo de 2021.

contenido. Los resultados de la consulta, de dichos encuentros y las respuestas del gobierno a cada uno fueron recogidos en febrero y diciembre de 2020.

En dichos documentos se resumieron las respuestas de participantes y del gobierno así:

- En materia de libertad de expresión: ante la preocupación sobre el impacto que el enfoque regulatorio tendría en la libertad de expresión fruto de las medidas a favor de la remoción de contenidos, el gobierno se comprometió a requerir a las plataformas de internet, en lugar de la remoción de contenidos, la puesta en práctica de sistemas y procesos para luchar contra el contenido dañino en línea de manera proporcionada y basada en un enfoque de evaluación de riesgos, así como la oferta de mecanismos de queja para sus usuarios para cuestionar la remoción de ciertos contenidos.
- Sobre las empresas de internet que estarían obligadas: Las empresas de internet más pequeñas manifestaron confusión en torno a si estarían cobijadas por la propuesta de ley. El gobierno aclaró que cobijaría solo a las más grandes empresas que hospedaran contenidos de usuarios de internet.
- Sobre el regulador encargado: Los respondientes se mostraron favorables a que fuese OfCom -la autoridad que regula las comunicaciones en Reino Unido- la autoridad encargada de la aplicación de la propuesta regulatoria final que fuese confeccionada por el gobierno. El gobierno dijo estar de acuerdo con delegar su aplicación a una autoridad ya existente con experiencia en la materia.
- Obligaciones en materia de transparencia: algunos participantes expresaron preocupación por los efectos del enfoque *one size fits all* (o de talla única) en materia de transparencia. El gobierno dijo introducir en el proyecto de ley un enfoque en el que los deberes de transparencia se ajustaran al tipo de servicio de internet ofertado y a los tipos de riesgos enfrentados por el intermediario.
- Protección de la niñez: si bien no recoge los comentarios recibidos en este sentido, el gobierno dijo introducir en el proyecto mecanismos de verificación de la identidad para prevenir a menores de edad de acceder a contenido inapropiado, entre otros.

Pese a que el proyecto de ley ha recibido un segundo debate en la Cámara de los Comunes, sigue siendo objeto de crítica y controversia. Algunas van desde su redacción extensa, imposible de analizar y propensa a la contradicción interna, hasta las que acusan la merma de garantías a favor de la privacidad de las personas, del anonimato en línea y del cifrado; el debilitamiento de la libertad de expresión en línea a través de las facultades amplias que se conceden a las plataformas que podrán fijar reglas sobre qué contenido es considerado dañino y de decidir en torno a su retiro; entre otros.

Entre las organizaciones que han formulado críticas al proyecto de ley en trámite y que abogan por su retiro o su modificación total se encuentran Artículo 19; Index of Censorship y Open Rights Group,. Por su parte, diversas organizaciones de mujeres han rechazado en un comunicado conjunto las demoras asociadas al trámite de la iniciativa que esperan que se convierta en ley.

Entre el listado de documentos producidos a raíz de este proyecto de ley se encuentran:

- El memorando de delegación de poderes del Ministerio de Medios de Comunicación, Cultura y Deporte (DCMS por sus siglas) y el Ministerio del Interior para el Comité de Poderes Delegados y de Reforma Regulatoria.
- Evaluación de impacto preparada por el DCMS
- Opinión del Comité de Política Regulatoria sobre el proyecto de ley.
- Análisis de compatibilidad entre el proyecto de ley de seguridad en línea y la Convención Europea de Derechos Humanos, preparada por el DCMS.
- Comentarios del Comité Conjunto designado por la Cámara de los Comunes y la Cámara de los Lores encargado de efectuar un análisis pre-legislativo del proyecto de ley.
- Respuesta del gobierno a las recomendaciones del Comité Conjunto sobre el proyecto de ley.

Qué prevé este proyecto de ley

Es un proyecto de ley extenso y que ha mutado considerablemente desde la publicación de su primera versión el día 12 de mayo de 2021. Al cierre del segundo debate en la Cámara de los Comunes el texto tenía un total de 12 partes[2], 197 artículos en total y un apéndice con 15 secciones[3], casi tan profuso como el resto del articulado.

---

[2] **Parte 1** "introducción"; **parte 2** "definiciones clave"; **parte 3** "proveedores de servicios regulados de usuario-a-usuario y servicios regulados de búsqueda: deberes de cuidado"; **parte 4** "otros deberes de los proveedores de servicios regulados usuario-a-usuario y servicios regulados de búsqueda"; **parte 5** "deberes de los proveedores de servicios regulados: cierto contenido pornográfico"; **parte 6** "deberes de los proveedores de servicios regulados: tasas"; **parte 7** "poderes y deberes de OfCom en relación con los servicios regulados"; **parte 8** "apelaciones y super-quejas"; **parte 9 "**funciones de la Secretaría de Estado en relación con los servicios regulados"; **parte 10** "delitos de comunicación"; **parte 11** "suplementos y general"; **parte 12** "interpretación y provisiones finales.

[3] Las secciones del apéndice se denominan "Schedule".

Schedule 1 "excepciones en servicios usuario-a-usuario y servicios de búsqueda"; **Schedule 2** "usuario-a-usuario y servicios de búsqueda que incluyen proveedores de contenido pornográfico"; **Schedule 3** "tiempo para las evaluaciones de los proveedores"; **Schedule 4** "códigos de práctica según la sección 37: principios, objetivos, contenido"; **Schedule 5** "delitos de terrorismo"; **Schedule 6** "explotación sexual infantil y delitos de abuso"; **Schedule 7** "delitos prioritarios"; **Schedule 8** "reportes de transparencia de proveedores de servicios de las categorías 1, 2Ay 2B"; **Schedule 9** "ciertos servicios de internet no sujetos a los deberes relacionados a los proveedores de contenido pornográfico"; **Schedule 10** "recuperación de los costos iniciales de OfCom"; **Schedule 11** "categorías de servicios regulados de usuario-a-usuario y servicios regulados de búsqueda: regulación"; **Schedule 12** "poderes de entrada, inspección y auditoría"; **Schedule 13** "penalidades impuestas por OfCom bajo el capítulo 6 de la parte 7"; **Schedule 14** "enmiendas consiguientes a los delitos de la parte 10 de esta ley"; **Schedule 15** "responsabilidad de las empresas matrices".

El análisis que sigue se enfoca en las previsiones relevantes en materia de libertad de expresión, y se orienta en la última versión publicada del proyecto de ley del día 28 de junio de 2022.

Sujetos obligados

Aplica respecto a los servicios de usuario-a-usuario y los servicios de búsqueda que tengan relación con Reino Unido.

Dicha relación puede estar dada bien porque el servicio tiene un número significativo de usuarios en ese país, o porque los usuarios de ese país son un mercado objetivo o son el único mercado objetivo del servicio, o porque son servicios que son capaces de ser usados por personas en el Reino Unido, incluso entrarán en dicha categoría los servicios sobre los que hay motivos razonables para creer que el contenido generado por los usuarios y el contenido en servicios de búsqueda representa un riesgo material de un daño significativo para las personas en ese país.

Los *servicios usuario-a-usuario* son los servicios de internet que ofrecen a los usuarios la posibilidad de crear, cargar y compartir contenido directamente en el servicio, sin importar si dicho contenido ha sido descargado o compartido o no con otro usuario.

Los *servicios de búsqueda* son los que permiten a una persona realizar búsquedas en sitios web o bases de datos, así como el servicio que permiten buscar en todos los sitios web y bases de datos.

Algunas de las excepciones previstas respecto a cada servicio son las siguientes:

- Los servicios de usuario-a-usuario que permiten únicamente la generación de contenido que no es identificatorio, es decir, todos los relacionados a mensajes SMS, MMS y algunos servicios de correo.
  También se exceptúa a los servicios de generación de contenido con funcionalidades limitadas como postear únicamente comentarios o evaluaciones al proveedor del contenido, compartir dichos comentarios en otro servicio de internet, expresar una opinión sobre dichos comentarios o evaluaciones (a través de botones de “me gusta” o “no me gusta”; a través de su valoración con emojis, de votaciones tipo sí/no, o de rating o puntuación del contenido).
- Si los servicios de usuario-a-usuario y servicios de búsqueda son un recurso o herramienta interna de una o más de una empresa o negocio o sin son responsabilidad de personas que persiguen fines de educación y cuidado de la niñez.

El proyecto crea tres categorías de sujetos obligados: la categoría 1, categoría 2A y la categoría 2B. La categoría impacta en el tipo y la cantidad de deberes a cargo.

La categoría 1 comprende a los servicios de usuario-a-usuario. *La categoría 2A* abarca los servicios de búsqueda y los servicios combinados -que son al tiempo de búsqueda y de usuario-a-usuario-. *La categoría 2B* incluye a los servicios de usuario-a-usuario. Ofcom tiene a su cargo la inclusión de cada servicio en la categoría que corresponda, siempre que el servicio determinado cumpla con un umbral y condiciones específicas.

Dichos umbrales serán definidos a futuro por el Departamento de Estado (sin que se explique muy bien por qué Ofcom no tiene a cargo dicha tarea) teniendo en cuenta, entre otros, el número de usuarios registrados en el servicio, sus funcionalidades y otros criterios que sean relevantes.

Ver: secc 2; shedule 1 (part 1, secc. 1- 4); secc. 82; schedule 11.

Obligaciones de los servicios de usuario-a-usuario

- Deber de emplear evaluaciones de análisis de riesgo del contenido ilegal (secc. 8)

Busca la evaluación suficiente y apropiada del riesgo de contenido ilegal en el servicio. El análisis de riesgo debe incluir una evaluación de la base de usuarios; el nivel de riesgo de que un usuario encuentre cierto contenido ilegal (el calificado como prioritario y el contenido ilegal de otro tipo); los algoritmos empleados que impactan en qué tan fácil, rápido y masivo se vuelve un contenido una vez diseminado; el nivel de riesgo que representan ciertas funcionalidades del servicio que facilitan la diseminación de contenido ilegal; la naturaleza y severidad del daño que puede sufrir el usuario; qué medios y tecnologías empleadas por el servicio están destinadas a reducir el riesgo, entre otros.

- Deber de seguridad sobre el contenido ilegal (secc. 9)

Apunta a la toma de medidas efectivas de mitigación y manejo del riesgo de daño a las personas. Para su ejecución se debe implementar sistemas y procesos diseñados, entre otros, a prevenir y minimizar que las personas encuentren “contenido ilegal prioritario” y “contenido ilegal”; recibir alertas de contenido ilegal prioritario y proceder a su retiro inmediato.

Para el logro de dicho final habilita al empleo de algoritmos, políticas de moderación y retiro de contenido, medidas de apoyo al usuario, bloquear a ciertos usuarios de acceder a cierto contenido, entre otros.

- Deber en torno al reporte de contenidos (secc. 17)

Tienen que contar con sistemas y procesos que permitan a las personas reportar fácilmente contenido que consideren dañino de ser accedido por niños, o que sea dañino para los adultos.

- Deberes en torno a los procedimientos de queja (secc. 18)

Las quejas en torno a los contenidos reportados deben ser fáciles de usar por los niños, así como accesibles y transparentes; las políticas accesibles sobre el procedimiento de atención a las quejas; mecanismos de reclamo para las quejas de los usuarios cuyo contenido ha sido retirado y que debe incluir el recibo de quejas asociadas al uso de 'tecnologías proactivas' que han intervenido en el retiro del contenido.

En los servicios es los que es probable que accedan niños se pueden elevar así mismo quejas si se considera que el proveedor de servicio no está cumpliendo con los deberes de proteger a la niñez (de la secc. 11); quejas asociadas a la toma de medidas de protección a la niñez basadas en consideraciones sobre la edad de la persona que resultan ser incorrectas, etc.

- Deberes en torno a la libertad de expresión y la privacidad (secc. 19)

En el cumplimiento de otros deberes deben respetar la libertad de expresión de conformidad con la ley; proteger a los usuarios en casos de que se configure un incumplimiento de los términos de servicio que afecten su privacidad; contar con términos y condiciones, así como mecanismos claros y accesibles para elevar quejas sobre contenido removido.

Los servicios de categoría 1 también deberán incluir en el proceso de toma de decisiones sobre las medidas y políticas de seguridad, implementar evaluaciones de impacto en materia de privacidad y libertad de expresión; mantener dicho análisis actualizado; publicarlo e informar sobre las acciones positivas que han sido desplegadas para proteger el derecho a la libertad de expresión y privacidad de las personas.

- Deber de mantener registros y reportes de revisión (secc. 20)

Los servicios de usuario-a-usuario deben mantener registro escrito de todos los análisis de evaluación de riesgos, de las medidas implementadas dirigidas a su reducción, de las medidas que no han sido aplicadas o que no se encuentran en uso, entre otros.

- Deberes de seguridad de la niñez en línea (secc. 10 y secc. 11)

Tanto la sección 10 y 11 conforman el gran "deber de cuidado" de la niñez, insignia de este proyecto.

En la sección 10 se prevén todas las acciones asociadas a las evaluaciones de riesgo de servicios de usuario-a-usuario que es probable que sean accedidos por niños. Dichas evaluaciones deben ser apropiadas, suficientes, estar actualizadas e incluir una evaluación de impacto de las acciones que serán implementadas a futuro.

Así mismo la evaluación de riesgo debe describir la base de usuarios, el nivel de riesgo según grupos de edad, y el tipo de contenido al que podrían estar expuestos: "contenido de prioridad principal", "contenido prioritario" y "contenido no designado". También, se debe integrar una evaluación de riesgo según las funcionalidades del servicio, según el contenido que afecta a ciertos grupos o características de grupos de niños, una estimación de la severidad del riesgo en caso de concretarse, entre otros. Este deber también incluye el deber de notificar a Ofcom sobre la presencia de "contenido de prioridad principal".

En la sección 11 se deben implementar dos tipos de acciones. Las medidas que efectivamente permitan mitigar y manejar los riesgos de niños según grupos de edad y mitigar el impacto que representa el contenido dañino a los niños según grupos de edad. Y las medidas de integrar en el serio sistemas y procesos proporcionados dirigidos a prevenir que niños de cualquier edad encuentren "contenido de prioridad principal" así como dirigidas a prevenir, según grupos de edad más en riesgo de exposición al contenido dañino, de encontrarlo en el servicio. El proyecto sugiere por ejemplo el uso de tecnologías de verificación de la edad o cualquier otro medio que cumpla ese fin.

Estas medidas deben estar implicadas no solo en los procesos de moderación de contenido, sino en el funcionamiento de todo el servicio de usuario-a-usuario.

Se debe informar en los términos del servicio cómo se previene que los niños de cualquier edad encuentren "contenido de prioridad principal", y cómo se previene que los niños que pertenecen a los grupos de edad de mayor riesgo están siendo protegidos para no encontrar "contenido de prioridad principal" ni "contenido no designado" que es dañino para éstos.

El servicio debe determinar si es o no del todo o en parte apropiado para ser accedido por niños, y de ser posible dicho acceso parcial, tiene a su cargo la implementación de sistemas y procesos para asegurar que el acceso solo sea posible para el grupo de edad que corresponda, o si no está diseñado para su acceso, para restringirlo del todo.

Deben informar sobre el tipo de "tecnologías proactivas" que están usando, cómo y para satisfacer qué fines asociados al deber de protección de la niñez.

- Deber de seguridad de los adultos en línea (secc. 12 - 14)

Solo los servicios de categoría 1 tienen a su cargo los deberes de protección de los adultos a través de (i) los análisis de riesgo, (ii) un deber de presentar en los términos del servicio términos el resultado del análisis de riesgo, (iii) de especificar en los términos del servicio cada

tipo de contenido considerado dañino y que será tratado bajo dicha consideración a través de su retiro, la restricción en su acceso, la limitación de la recomendación del mismo y de que éste sirva para recomendar terceros contenidos, (iv) de ajustar el contenido de los términos del servicio de manera clara y accesible.

Los servicios de categoría 1 tienen, a su vez, el deber de notificar a Ofcom de los contenidos no designados que sean considerados dañinos. Y tienen los mismos deberes en materia de libertad de expresión y privacidad descritos en la sección 19. También se les asigna el deber de empoderar a sus usuarios a través de la inclusión de características a sus servicios que le permitan a éstos un mayor control sobre los contenidos dañinos, para filtrar usuarios no verificados y prevenir la interacción con estos, entre otros.

- Deber de proteger contenido de importancia democrática y contenido periodístico (secc. 15 y 16)

Los servicios de categoría 1 deben usar sistemas y procesos proporcionados que permitan asegurar la protección del contenido de importancia democrática para lo cual deben advertir cómo harán dicho tratamiento, y qué acciones desplegarán en contra del usuario que lo crea, carga o comparte en el servicio.

Según la sección 15, el contenido de importancia o relevancia democrática se define como (i) el contenido de editores de noticias con presencia en dicho servicio, (ii) el contenido generado por un usuario regulado, (ii) el contenido que es o aparenta estar específicamente dirigido a contribuir con el debate democrático en el Reino Unido, o con una parte o área de este territorio.

En la sección 16 se prevén disposiciones de contenido similar y se añade que estos servicios deberán contar con un procedimiento de queja expedito para los eventos en que un contenido que haya sido retirado, o que su acceso haya sido restringido, pueda ser considerado por el servicio como un contenido periodístico, objeto de ser protegido.

Esa solicitud o queja la puede elevar el usuario que generó, cargó o compartió el contenido (una persona o entidad en Reino Unido), o el creador del contenido.

En la calidad de creador de contenido periodístico se incluye a todos los medios y editores de noticias reconocidos en dicha condición. Según el proyecto entre los medios reconocidos se incluye a la Corporación de Medios Británica; Sianel Pedwar Cymru o el Canal 4 Galés; los tenedores de licencias de transmisión o cualquier entidad que cumpla con alguno de los siguientes requisitos: (i) tener como objetivo principal la publicación de contenidos de noticias, (ii) publicar dicho material en relación con una empresa con o sin ánimo de lucro, (iii) esté sujeto a un código de prácticas, (iv) tener procedimientos para el manejo y trámite de quejas, (v) tener un negocio registrado en el Reino Unido, (vi) ser una persona sujeta a ser responsable por el contenido publicado, entre otros) (ver. Secc. 50, parte 1).

Obligaciones de los servicios búsqueda

- Deberes de cuidado (secc. 21)

La ley remite a distintos deberes que ya fueron descritos para los servicios de usuario-a-usuario y que, en esencia, consisten en casi las mismas acciones aunque con algunas previsiones adicionales que hacen sentido al tratarse de motores de búsqueda, como los deberes de explicabilidad sobre los procesos de priorización de contenidos, por ejemplo, o el trámite de peticiones de personas interesadas en no aparecer más en resultados de búsqueda o para que se les conceda una menor prioridad en los resultados que arroja dicho servicio (ver secc. 28).

Este deber de cuidado agrupa al de (i) evaluación del riesgo del contenido ilegal (secc. 23), de actuar ante el contenido ilegal (secc.24), (iii) de reportar el contenido ilegal (secc. 27), (iv) los deberes de protección de la libertad de expresión y privacidad (secc. 29), y de (v) conservación de registros y revisiones.

- Deberes de seguridad de la niñez en línea (secc. 25 y 26)

Estos deberes tienen una redacción similar a los que describimos que son aplicables a los servicios de usuario-a-usuario.

Los servicios de búsqueda, sin embargo, parecen estar sujetos a un nivel menos intenso de exigencia en la seguridad menor, pues a diferencia de los servicios de usuario-a-usuario (ver secc. 26, parte 3, literal a y b) que deben prevenir y proteger a los niños de encontrar contenidos de prioridad principal. Estos, en cambio, deben encargarse de mitigar dicho riesgo.

En la implementación de este deber también deben informar sobre el uso de tecnologías proactivas dirigidas a la realización de las acciones a su cargo.

Complejidades: la taxonomía porosa de los contenidos regulados

Contenido ilegal, contenido ilegal prioritario, contenido de prioridad principal, contenido prioritario, contenido no designado (secc. 9, 10 y 11). Cada uno, según el proyecto, presenta diferentes niveles de riesgo según la secc. 11 (punto 6, c).

Las definiciones del proyecto de ley sobre los límites de cada contenido no son fáciles de aprehender en su primera lectura. Dificultad que se profundiza en tanto que hay taxonomías de contenido diferenciadas según puedan impactar a los niños o los adultos.

- Contenido (secc. 52, parte 3)

Como contenido se define a todo uso de ciertas palabras, imágenes, discurso o sonidos presentes en el servicio.

- El “contenido ilegal” (secc. 52 y Schedule 7)

Es el contenido que equivale a un delito relevante (secc. 52). A su turno, no provee una definición de delito relevante, sino que provee un listado extenso de delitos que entran en esa categoría. Incluye los de terrorismo y los asociados al abuso y la explotación sexual infantil.

En ese listado hay, a su vez, una remisión a más de media docena de legislaciones diferentes: las que regulan la asistencia al suicidio, las amenazas de muerte, el acoso público, la venta de drogas prohibidas o controladas, la venta de armas de fuego, la asistencia a la migración ilegal, la de explotación sexual y prostitución, la de posición de imágenes con contenido sexual, la de regulación del fraude, de actividades financieras no permitidas.

Y remata por incluir cualquier delito donde la víctima sea un individuo o conjunto de individuos, un elemento tan vago y abierto que disuelve la vocación del listado taxativo que le antecede.

Aclara, en todo caso, que no se consideran como delitos relevantes los asociados a la infracción de la propiedad intelectual, a la seguridad y calidad de ciertos productos, y la calidad de un servicio provisto por una persona no calificada para ejecutarlo.

- El “contenido de prioridad principal” (secc. 52; schedule 6 y 7)

Incluye los contenidos sobre terrorismo, abuso sexual y explotación infantil y todo el que esté incluido en el Schedule 7, que es básicamente el mismo listado de leyes a la que referimos en la sección anterior.

Entonces, ¿cuál es la naturaleza de este contenido, y qué lo diferencia del contenido ilegal del que los servicios de usuario-a-usuario deben hacer análisis diferenciados de riesgo?, no resulta del todo claro pues el único elemento diferenciador de esta tipología de contenido y el “contenido ilegal” es que esta incluye los de abuso y explotación sexual infantil.

- Contenido dañino para los niños (secc. 53)

En esta categoría el proyecto desglosa distintos tipos de contenido. El “contenido de prioridad principal dañino para los niños”, el “contenido prioritario dañino para los niños”, y el “contenido dañino para los niños”.

El “contenido de prioridad principal dañino para los ninos” y el “contenido prioritario dañino los niños” serán los que califique así el Departamento de Estado.

El “contenido dañino” parece ser una categoría sombrilla pues puede ser tanto el “contenido de prioridad principal”, “contenido prioritario que es dañino” o el “contenido no designado”.

El “contenido no designado” es el que no es “contenido de prioridad principal” ni “contenido prioritario” y que puede significar un riesgo significativo para un número apreciable de niños en el Reino Unido.

Y el contenido ilegal está definido en sus propios términos, según la sección 52.

- Contenido dañino para los adultos (secc. 54)

El contenido dañino para los adultos agrupa al “contenido prioritario dañino para adultos” y “el contenido dañino para adultos”. El “contenido prioritario dañino para adultos” es el que reciba dicha calificación que será reconocida vía regulación por el Departamento de Estado.

El “contenido dañino para adultos” parece ser otra categoría sombrilla que integra al “contenido de prioridad principal” o el contenido que no sea de ese tipo pero que pueda significar un riesgo significativo de daño para un número apreciable de adultos en el Reino Unido.

El contenido ilegal está definido en sus propios términos, según la sección 52.

Las tecnologías proactivas, más categorías complejas.

La expresión “tecnologías proactivas” (secc. 187) reúne a todas las tecnologías digitales dirigidas a la (i) moderación de contenidos, (ii) el perfilamiento de los usuarios de esa tecnología, y (iii) de tecnologías de identificación del comportamiento en el servicio.

Las tecnologías proactivas de *moderación de contenidos* son las que están dedicadas a analizar el contenido relevante para determinar si es ilegal o dañino para la niñez, y que analiza si el contenido es o no publicidad fraudulenta.

Las tecnologías proactivas de *perfilamiento de usuarios* son las que analizan contenido relevante, datos de los usuarios o metadatos relevantes de un contenido o usuario en aras de construir un perfil que permita evaluar características tales como su edad.

Las tecnologías de *identificación del comportamiento del usuario* son las de análisis del contenido relevante, de los datos del usuario o metadatos del contenido para evaluar si el comportamiento en línea de un usuario permite evaluar su condición de víctima potencial de actividades ilegales.

El proyecto aclara que las tecnologías dirigidas a determinar la edad de una persona a través del análisis de datos que proveyó para dicho fin, que no analizan otros datos o contenido alguno, no serán consideradas como “tecnologías proactivas”.

Estas definiciones se apoyan en la expectativa de diferenciación de las tecnologías a partir de sus funciones desagregadas que, según el proyecto, es tajante para cada uno de estos tres casos. Una misma tecnología digital que cumpla al tiempo con las funciones de identificación del comportamiento y de perfilamiento del usuario ¿es una que estará amparada por el contenido de la ley?, ¿qué hay de los impactos en materia de privacidad que significa su puesta en marcha, concretamente en aspectos tan sensibles como el anonimato en línea o el cifrado?

Además, se deposita por el legislador la confianza en que las tecnologías de moderación de contenido harán la diferenciación clara entre un contenido ilegal y uno dañino, siendo que la taxonomía del contenido al que hace referencia este proyecto es, por decir lo menos, difusa.

No hay previsiones asociadas, por ejemplo, a la necesidad de que la identificación del contenido en uno u otro sentido o las acciones que se tomen al respecto deban estar supervisadas por un humano, mucho menos consideraciones en torno a la explicabilidad de su funcionamiento o la apertura, publicación y auditoría de los algoritmos en juego. Acciones que no están expresas en el deber de llevar a cabo análisis de evaluación de riesgo y que tienen a su cargo los servicios regulados.

Futuro del proyecto de ley

El futuro de este proyecto de ley es, por ahora, incierto. Su contenido podría estar en manos de Liz Truss, candidata a ser primera ministra de Reino Unido y que de ser electa, ha prometido revisarlo en su integridad para asegurarse de que “no dañará la libertad de expresión”, al tiempo que ha afirmado de que se debe avanzar en la regulación de las redes sociales en aras de proteger a la niñez en línea.

Tal y como lo expresó el periodista Alex Hern, en The Guardian, el debate que queda no será más fácil para nadie. Se trata de un proyecto ampliamente debatido, que todavía no deja a ninguna parte satisfecha con su contenido.

Es interesante que, pese a la discusión de borradores y propuestas por más de tres años, y al despliegue de las mejores prácticas imaginables en materia de diseño regulatorio, y de haber contado con la participación de cientos de voces e intereses, el proyecto haya sido confeccionado de manera tan compleja y confusa que ni siquiera ahora sea fácil estimar cuáles serán los efectos positivos que pueda generar para la economía de internet fuera dentro y fuera ese país.

Por ahora, la discusión legislativa fue relegada a otoño, junto con otros proyectos de ley en curso y algunos nuevos, como el de regulación de las apuestas en línea que pronto será

publicado y cuyo contenido podría aumentar los deberes de bloqueo de contenido ilegal a cargo de los servicios de internet.

El riesgo que se corre con este proyecto es que pueda, al menos en parte -aunque sea mínima- aumentar la seguridad en línea de la niñez, sin importar el riesgo que pueda significar para otros derechos de valor democrático. Sea esta iniciativa o cualquier otra en su lugar en caso de ser abandonada, lo cierto es que en Reino Unido parece haber un consenso de las mayorías parlamentarias para avanzar en la regulación de las empresas de internet.

La pregunta es ¿cómo lograr el balance pese a las preocupaciones fundadas de todas las partes? Las leyes de servicio digital y mercado digital de la Unión Europea son, por lo menos, un buen gran avance que imitar.