

Lineamientos constitucionales sobre la responsabilidad de las empresas de servicios en internet y las medidas de restricción de acceso a contenidos

Víctor Abramovich, * María Luz Silveira **
y Facundo Capurro Robles ***

Resumen

Este artículo aborda discusiones vinculadas a la recepción jurisprudencial de los lineamientos constitucionales en materia de responsabilidad de las empresas de servicios en internet, con especial énfasis en las medidas de restricción de contenidos.

La Corte Suprema y los tribunales argentinos han resuelto en la última década importantes casos que revelan las tensiones derivadas de la difusión de expresiones en la esfera digital, recurriendo a los clásicos estándares de libertad de expresión delineados para los medios gráficos. Ello resulta

* Víctor Abramovich es Abogado (UBA) y Magister en Derecho Internacional (Washington College of Law - American University); Profesor titular de la asignatura Derechos Humanos y Garantías (Facultad de Derecho, UBA). Procurador Fiscal ante la Corte Suprema de Justicia de la Nación.

** María Luz Silveira es Abogada (UBA) y Magister en Derecho Internacional Humanitario y Derechos Humanos (Geneva Academy of international Humanitarian Law and Human Rights - Geneva Graduate Institute); Docente de la asignatura Fuentes del Derecho Internacional Público (Facultad de Derecho, UBA). Actualmente se desempeña en la Procuración General de la Nación.

*** Facundo Capurro Robles es Abogado (UBA) y Magister en Estudios Legales Internacionales (Washington College of Law - American University); Docente de la asignatura Derechos Humanos y Garantías (Facultad de Derecho, UBA); actualmente es funcionario de la Procuración General de la Nación.

insuficiente. Además, la relevancia y el escaso apego de las empresas transnacionales de redes, plataformas y servicios a los estándares de derechos humanos complejiza el panorama. En el primer apartado abordaremos el debate conceptual sobre la caracterización de las empresas de servicios en internet efectuada por nuestra Corte Suprema, y cómo esa conceptualización ha comenzado a virar en el derecho comparado hasta el punto de imponerle a estas empresas deberes de diligencia y cuidado en la identificación de riesgos y gestión de contenidos. En el segundo apartado analizaremos los criterios de ponderación que permiten abordar los conflictos entre la libertad de expresión en internet y otros derechos, con especial atención a las pautas relativas a las medidas de bloqueo o filtrado de contenidos. En tercer término, haremos hincapié en el diseño de las medidas restrictivas de contenidos en la esfera digital y el deber de explorar medidas alternativas menos lesivas a la censura digital. En cuarto lugar, abordaremos las discusiones referidas a la preservación del anonimato del emisor de información cuestionada y las obligaciones de las empresas gestoras en relación con la preservación de los datos de los usuarios. Por último, haremos mención a las discusiones procesales y jurisdiccionales que conlleva en nuestro país la irrupción de estas empresas transnacionales. Al final, realizaremos unas breves conclusiones sobre la necesidad de incorporar las nuevas tendencias en la materia y los desafíos que enfrenta nuestra Corte Suprema de Justicia, dada la propia dinámica y especificidad de la esfera digital.

Palabras claves: Libertad de expresión, Corte Suprema de Justicia, responsabilidad, intermediarios, plataformas, redes sociales, esfera digital, moderación de contenidos, debida diligencia, filtrado, restricción de contenidos, empresas transnacionales.

Constitutional Guidelines in Argentina on both the Liability of Internet Service Companies and the Digital Content Restrictive Measures

Abstract

This article addresses discussions concerning how courts have interpreted constitutional guidelines on the liability of Internet service providers, with a particular emphasis on content restriction measures.

The Argentine Supreme Court and lower courts have ruled on significant cases over the past decade that reveal the tensions arising from the dissemination of expressions in the digital sphere, relying on traditional free speech standards originally designed for print media. This approach has proven insufficient. Moreover, the influence and weak adherence of transnational social media companies, platforms, and service providers to human rights standards further complicate the landscape.

In the first section, we will examine the conceptual debate surrounding the characterization of Internet service companies by our Supreme Court and how this conceptualization has begun to shift in comparative law—to the point of imposing due diligence obligations on these companies, requiring them to identify risks and manage content proactively.

The second section will analyze the balancing tests used to resolve conflicts between freedom of expression online and other rights, with particular attention to the standards governing content blocking or filtering measures.

Third, we will emphasize the design of content-restrictive measures in the digital sphere and the duty to explore less intrusive alternatives to mitigate the risks of digital censorship.

Fourth, we will address debates concerning the preservation of anonymity for speakers of contested information and the obligations of service providers regarding user data retention.

Finally, we will discuss procedural and jurisdictional challenges arising from the emergence of these transnational companies in Argentina.

In closing, we will offer brief conclusions on the need to incorporate emerging trends in this field and the challenges facing our Supreme Court of Justice, given the unique dynamics and specificities of the digital realm.

Keywords: Freedom of Expression, Supreme Court of Justice, Responsibility, Intermediaries, Platforms, Social Networks, Digital Sphere, Content Moderation, Due Diligence, Filtering, Content restriction, Transnational corporations.

I. Introducción

En la última década los tribunales argentinos, y en particular la Corte Suprema, han sido convocados a dirimir diferentes cuestiones constitucionales

relativas a la protección de derechos fundamentales en la esfera digital. En distintos precedentes han ratificado la idea básica de que los derechos constitucionales a la libertad de expresión e información, a la privacidad y a la igualdad y no discriminación tienen aplicación plena en el ámbito de internet, aunque han buscado adaptar los estándares jurídicos que rigen su protección y garantía a las características específicas y diferenciadas del entorno virtual y de las nuevas tecnologías de la información. Al respecto cabe recordar que los estándares constitucionales que resuelven, por ejemplo, las tensiones entre la libertad de expresión y la privacidad o la reputación fueron desarrollados principalmente para regir las expresiones difundidas por la prensa y por los medios de comunicación tradicionales. El tipo de conflictos analizados al elaborar esos criterios constitucionales no da cuenta de la naturaleza de los procesos expresivos en la esfera digital, definidos por flujos masivos de información, que circulan a una velocidad desconocida, originados en una multiplicidad de emisores y propagadores en gran medida anónimos, y cuya gestión corresponde centralmente a megaempresas transnacionales que administran redes, plataformas y servicios y cuentan con una variedad de recursos técnicos para ordenar, priorizar, filtrar o bloquear el acceso a información, pero cuyas políticas de moderación de contenidos o de tratamiento de información resultan opacas o directamente confidenciales.

Así, ante la ausencia de reglas definidas por el legislador, algunos criterios jurisprudenciales elaborados gradualmente por los tribunales nacionales y por la Corte, caso tras caso, contribuyen a dirimir conflictos normativos y sentar las bases para imponer deberes y responsabilidades a los diferentes actores del ecosistema digital.

En este artículo vamos a analizar algunas de estas discusiones centrales.

En primer lugar, abordaremos el debate conceptual acerca de la caracterización de las empresas de servicios en internet, aspecto que incide sobre los factores de atribución de responsabilidad jurídica. Una postura inicial de los tribunales argentinos, reflejada en el precedente *Rodríguez*¹ resuelto por la Corte Suprema en el 2014, consideró a los “motores de búsqueda” como bibliotecas estáticas o meros transmisores neutrales de información producida por terceros, de modo que no podían ser responsabilizados por esa

1. CSJN, sentencia del 28 de octubre de 2014, *Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios*, Fallos: 337:1174.

información, hasta tanto no tomaran conocimiento efectivo de la difusión de contenidos ilícitos. Esta tesis ha comenzado a variar en el derecho comparado y en el derecho internacional en los últimos años, y en varios casos se plantea la necesidad de revisar esta caracterización inicial, atribuyendo a las empresas gestoras de plataformas, redes y servicios –como los motores de búsqueda– la calidad de “editores de contenidos” y responsables del “tratamiento de datos personales”, e imponiéndoles deberes de diligencia y cuidado en la identificación de riesgos sistémicos de circulación de contenidos ilícitos y la adopción de políticas de moderación y de reparación.

En segundo lugar, analizaremos los criterios de ponderación que permiten abordar los conflictos entre la libertad de expresión en internet y otros derechos, como el acceso a información, la privacidad, la reputación y la protección antidiscriminatoria. Al respecto la Corte Suprema ha considerado que las medidas de desvinculación, bloqueo o filtrado de contenidos digitales interrumpen o dificultan el proceso comunicativo y por ello constituyen mecanismos de censura que solo proceden en supuestos excepcionales y bajo parámetros muy estrictos. Ello se agudiza cuando se trata de restringir el acceso a expresiones sobre asuntos de interés público que son especialmente protegidos por la libertad de expresión. En ese marco, en esta sección describiremos las pautas fijadas por los tribunales para autorizar medidas de bloqueo o filtrado en función de los diferentes derechos en juego y las características de la expresión cuestionada.

En tercer lugar, en el examen de la procedencia de las medidas de bloqueo o filtrado de información, se han establecido algunos criterios para asegurar la reparación adecuada de los daños causados por contenidos ilícitos con una mínima afectación de la libertad de expresión. En particular vamos a analizar los requisitos de estricta determinación del contenido que debe ser restringido y el deber de explorar medidas alternativas menos lesivas a la censura digital.

En cuarto lugar, abordaremos las discusiones referidas a la preservación del anonimato del emisor de información cuestionada y las obligaciones de las empresas gestoras de plataformas y redes en relación con la preservación de los datos de los usuarios.

Finalmente, vamos a examinar el alcance de la jurisdicción de los tribunales argentinos para juzgar a empresas transnacionales de servicios de internet y la posibilidad de notificar las acciones e imponer condenas a sus filiales.

II. La discusión sobre el papel de los servicios en internet ¿simples canales neutrales o editores de información y responsables del tratamiento de datos personales?

En el caso *Rodríguez* la Corte examina, por primera vez, la responsabilidad de los buscadores de internet por los contenidos generados por terceros y define a los motores de búsqueda como “intermediarios” de internet. El caso tuvo su origen en una demanda promovida contra Google Inc. y Yahoo de Argentina SRL por la difusión no autorizada de la imagen de la demandante y la vinculación de su nombre e imagen con sitios de contenidos sexual y pornográfico.

El tribunal sostiene que la responsabilidad civil de los motores de búsqueda se basa en criterios subjetivos basados en la intención de dañar, o bien en la culpa o negligencia al no evitar diligentemente la producción de un daño –según los factores de atribución previstos en los artículos 1721 y 1724 del Código Civil y Comercial de la Nación– y rechaza la aplicación de un sistema de responsabilidad “objetiva”, que hubiera permitido responsabilizarlos por cualquier contenido ilícito que alojen, con la sola comprobación de la producción de un daño derivado de ese contenido.²

La Corte justifica la adopción del modelo de responsabilidad subjetivo en el principio de que las empresas que gestionan buscadores de internet no tienen una obligación general de monitoreo activo sobre los contenidos que sus usuarios suben a la red, regla que ha sido ampliamente reconocida tanto a nivel internacional como regional, en instrumentos internacionales de *soft law*,³ como así también en distintas normativas aprobadas por

2. La responsabilidad “objetiva” es aquella que se atribuye al dueño o guardián de una “cosa” o al responsable de una actividad que produce un daño, basado en el carácter intrínsecamente riesgoso o peligroso de la actividad, prescindiendo de la noción de culpa o dolo (por ej. mediante la introducción de una determinada maquinaria “riesgosa” o por los daños generados por automóviles). En estos casos, el factor de atribución de responsabilidad civil es objetivo, ya que el dueño o titular es responsable por la mera introducción de ese elemento riesgoso, y solo puede eximirse de responsabilidad demostrando que el daño se originó por una circunstancia ajena a ello.

3. Ver *Principios de Manila sobre Responsabilidad de los Intermediarios*, del 24 de marzo de 2015, principio I.d) y *Declaración conjunta sobre libertad de expresión e internet del año 2011*, suscripta por el Relator Especial de las Naciones Unidas (ONU) sobre la

los Estados.⁴ En tal sentido, refiere que al no existir una obligación general de supervisar se desprende lógicamente la imposibilidad de atribuirles responsabilidad directa por la información que es producida por terceros. Asimismo, reconoce que éste ha sido el enfoque adoptado en otros países, como en los Estados Unidos, donde –sobre la base de la Sección 230 de la Communications Decency Act (CDA) de 1996–, se interpreta que las empresas de servicios en internet no pueden ser tratadas como editores por el contenido publicado por terceros en sitios web. Mediante esa ley, junto con la Digital Millenium Copyright Act (DMCA) de 1998, se estableció un mecanismo que obliga al proveedor que ha sido anoticiado sobre la existencia de contenido considerado ilegal, dañoso o violatorio del derecho de autor, a adoptar medidas para removerlo (mecanismo de “notice ante take down”).⁵

En definitiva, la Corte sostiene que responsabilizar a los buscadores con base en un criterio objetivo de responsabilidad equivaldría a sancionar a una biblioteca por facilitar, a través de sus ficheros y catálogos, el acceso a contenidos lesivos obrantes en un libro.⁶ Por ese motivo, sienta como doctrina que para atribuir responsabilidad al motor de búsqueda, aquel debe haber tomado conocimiento efectivo de la existencia de un contenido ilícito, tras lo cual deberá actuar de modo diligente, a fin de inhabilitar el acceso a

Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (OEA), y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), punto 2, disponible en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2>

4. En el ámbito de la normativa europea, por ejemplo, este principio ha sido recogido en la *Directiva sobre el comercio electrónico* (artículo 15), del 17 de julio de 2000, en la *Directiva sobre derechos de autor y derechos afines en el mercado único digital* (artículo 17), del 17 de abril de 2019 y, recientemente, en el *Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales*, del 19 de octubre de 2022 (artículo 8).

5. La Sección 230 de la *Communications Decency Act (CDA)* de 1996 establece que “ningún proveedor o usuario de un servicio interactivo de computación será tratado como un editor o emisor de cualquier información que provenga de otro proveedor de contenido informativo” (traducción propia).

6. CSJN, *Rodríguez*, cit., considerando 16°.

esos contenidos dañosos en los resultados de búsqueda.⁷ Según ese esquema, solo tienen responsabilidad civil si se demuestra que el buscador actuó con culpa o dolo.

Esta posición asume que los buscadores son meros canales o transmisores de información, que actúan como nexo entre un emisor y los receptores del acto comunicativo. Se considera que son ajenos al contenido creado y diseminado por los usuarios, y por ello su responsabilidad jurídica emerge recién cuando toman “efectivo conocimiento” de la existencia de un contenido ilícito.

Es importante señalar que la postura de la Corte se alinea con la perspectiva dominante en aquel momento. En tal sentido, la idea de que el papel de las empresas de servicios en internet se reduce a una mera transmisión de datos ya estaba presente en la Declaración Conjunta sobre Libertad de Expresión e Internet, suscripta en 2011, que estableció como principio la no responsabilidad de aquellas empresas que ofrezcan únicamente servicios digitales de acceso, búsqueda o de almacenamiento de información en la memoria *caché* y no intervengan en la generación de los contenidos o se nieguen a cumplir con una orden judicial que exija su supresión.⁸ Por otro lado, en un informe del año 2017, la Comisión Interamericana de Derechos Humanos (CIDH) reconoce la importancia que reviste el régimen de responsabilidad aplicable a la actuación de las empresas que gestionan plataformas, redes y servicios de búsqueda en internet para la tutela de la libertad de expresión en el entorno digital, al señalar que un régimen de responsabilidad estricta u objetiva es incompatible con la libertad de expresión, pues incentiva la censura privada e incrementa el riesgo de injerencia estatal sobre la circulación de ideas e información en internet.⁹ En sentido coincidente, si bien existen distintos modelos de responsabilidad aplicables a estos servicios, las legislaciones y directrices internacionales han aceptado la prohibición general de monitoreo de los contenidos generados por los usuarios y el rechazo al modelo de responsabilidad objetiva.

Ahora bien, la “autorregulación” de estas empresas también pone en

7. CSJN, *Rodríguez*, cit., considerando 17°.

8. *Declaración conjunta sobre libertad de expresión e internet del año 2011*, cit., punto 2.

9. CIDH, RELE, *Estándares para una Internet libre, abierta e incluyente*, 2017, OEA/Ser.L/V/II/CIDH/RELE/INF.17/17, 15 de marzo de 2017, párrs. 101, 104-105, 107, 115 y 124.

riesgo el ejercicio de derechos fundamentales, en tanto la actividad de los motores de búsqueda y las plataformas digitales incide en el flujo informativo, la generación del discurso público, el acceso a la información y la autodeterminación informativa. De tal modo, la regulación del espacio digital genera una tensión que, si bien al momento de resolverse el caso “*Rodríguez*” ya había sido advertida por el Relator de las Naciones Unidas para la Libertad de Expresión,¹⁰ ha cobrado especial relevancia en los últimos años, al punto de que las plataformas digitales fueron calificadas por ese mismo organismo de “reguladores enigmáticos”.¹¹

Así, se ha abandonado gradualmente la visión de que las empresas de servicios en internet actúan como meras “bibliotecas” o “canales neutrales”, dando paso a nuevos modelos regulatorios del espacio digital que, si bien mantienen el sistema de responsabilidad subjetiva, les imponen una serie de obligaciones de debida diligencia y cuidado, orientadas a dotar de mayor transparencia y previsibilidad al entorno en línea, como también fomentar la aplicación de los estándares internacionales de derechos humanos a su actividad.

A diferencia del modelo adoptado en los Estados Unidos, en el ámbito europeo, en el año 2014 el Tribunal de Justicia de la Unión Europea (TJUE) emitió su decisión en el caso *Costeja*, en el cual reconoció que los motores de búsqueda (en ese caso, Google) son entidades de alojamiento y tratamiento de datos personales y realizan una actividad diferente a la de un editor de un sitio de internet, por cuanto buscan información allí emplazada por terceros, la indexan, la almacenan y la ponen a disposición de otros internautas en un orden específico. Por lo tanto, pesa sobre estas empresas un cúmulo de obligaciones derivadas de esta actividad, diferente a las que puede imponerse a un periódico.¹² Posteriormente, con el dictado del Regla-

10. Informe del Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, A/HRC/17/27, del 16 de mayo de 2011, párrs. 40 y 42.

11. Informe del Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, relativo a la regulación del contenido en línea generado por los usuarios, David Kaye, del 6 de abril de 2018, A/HRC/38/35, párr. 1.

12. TJUE, sentencia del 13 de mayo de 2014, caso *Google Spain S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Asunto C-131/12. Ver en este sentido R. Post, “Data Privacy and Dignitary Privacy: Google Spain, the right to be

mento General de Protección de Datos de 2016¹³ y, más recientemente, del Reglamento de Servicios Digitales¹⁴ que ha comenzado a surtir efectos este año –ambos del Parlamento Europeo y del Consejo Europeo–, se delineó el marco legal que rige a estas empresas en el ámbito de la Unión Europea.¹⁵

En particular, el Reglamento de Servicios Digitales reafirma el principio de responsabilidad subjetiva y establece que no se impondrá a los prestadores de servicios intermediarios una obligación general de monitoreo de información¹⁶ pero, a la vez, les impone obligaciones de debida diligencia en la moderación de contenidos y el respeto de los derechos humanos. Entre los deberes mencionados se encuentran la exigencia de contar con mecanismos de “notificación y acción” ante las denuncias de los usuarios sobre la presencia de contenidos ilícitos,¹⁷ de proveer salvaguardas que garanticen el consentimiento informado, de adoptar medidas de transparencia en las decisiones de moderación o curación de contenidos, de establecer procedimientos de reclamo respecto de dichas decisiones, presentar informes periódicos sobre

forgotten, and the construction of public sphere”, *Duke Law Journal*, Vol. 67, 981, 2018. Allí el autor considera que el fallo “Costeja” se asienta sobre una comprensión del derecho a la privacidad que tiene en miras regular el manejo de información personal en un contexto donde ésta es administrada por grandes organizaciones con fines específicos (*data privacy*); mientras que existe otra concepción del derecho a la privacidad (*dignitary privacy*), que tiene en miras proteger la dignidad humana, en un marco de interacción provocada por individuos que entablan un diálogo intersubjetivo sin fines específicos, lo cual, en definitiva, representa el proceso comunicativo.

13. Parlamento Europeo y Consejo de la Unión Europea, *Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (“Reglamento General de Protección de Datos”), 27 de abril de 2016.

14. Parlamento Europeo y Consejo de la Unión Europea, *Reglamento 2022/2065 relativo a un mercado único de servicios digitales*, por el que se modifica la Directiva 2000/31/CE (“Reglamento de Servicios Digitales”), 19 de octubre de 2022.

15. Reglamento 2022/2065, considerando 5 y artículo 3.g; Reglamento 2016/679, artículo 2, inc. 4.

16. Reglamento 2022/2065, cit., artículos 4, 5, 6 y 8.

17. El artículo 3 define “contenido ilícito” como “Toda información que, por sí sola o en relación con una actividad, incluida la venta de productos o la prestación de servicios, incumpla el Derecho de la Unión o el Derecho de cualquier Estado miembro que cumpla el Derecho de la Unión”.

la actividad de moderación de contenidos realizada, de incluir en sus condiciones generales información sobre cualquier restricción que impongan, y el deber de actuar de manera diligente, objetiva y proporcionada al aplicar y hacer cumplir esas restricciones. Este Reglamento prevé también obligaciones adicionales para las plataformas y motores de búsqueda de gran tamaño,¹⁸ tales como la obligación de realizar evaluaciones de riesgos sistémicos o la de someterse a auditorías independientes.¹⁹ Por su parte, el Reglamento General de Protección de Datos consagra el derecho de los usuarios a solicitar la rectificación y supresión de información personal obrante en internet, al tiempo que obliga a las empresas a contar con procedimientos que permitan a los usuarios solicitar el acceso, rectificación, supresión o limitación de los datos personales que les conciernan obrantes en esas bases.²⁰

Por otro lado, el cambio de concepción sobre el carácter de la actividad que realizan las empresas de servicios en internet y los modelos regulatorios también puede verse reflejado en algunos pronunciamientos recientes y en informes temáticos.

En efecto, en Estados Unidos, donde el modelo de responsabilidad subjetiva posee sólidos fundamentos y la protección constitucional del discurso en línea se basa en la Primera Enmienda, algunos Estados locales, con el declamado objetivo de alcanzar “mayor neutralidad” de las redes, sancionaron leyes que limitan las facultades de las plataformas para participar en la moderación de contenidos. Ello motivó la reciente decisión de la Suprema Corte en el caso *Moody v. Netchoice*.²¹ A pesar de que el alcance de tal decisión puede circunscribirse a determinadas acciones de la plataforma —el contenido generado por el “News Feed” de Facebook (en otras palabras, la pestaña de publicaciones destacadas y más recientes) y la página de inicio de YouTube—, el tribunal consideró que el modo en que son exhibidos a los usuarios los contenidos que se comparten en las grandes plataformas

18. El Reglamento las define como aquellas que cuentan con al menos 45 millones de destinatarios activos mensuales en la Unión Europea, ver artículo 33(1).

19. Reglamento 2022/2065, cit., Capítulo III, artículos 3, 5, 8, 9, 12, 14-16, 20, 23, 24, 34 y 37, entre otros.

20. Arts. 15 a 19 del Reglamento 2016/679.

21. Suprema Corte de los Estados Unidos, sentencia del 1 de julio de 2024, caso *Moody, Attorney General of Florida, et al. v. Netchoice, LLC, DBA Netchoice, et al.*

de redes sociales depende de una actividad desplegada por estos servicios que comprende incluir, remover, organizar, priorizar y etiquetar contenidos millones de veces por día, de conformidad con sus reglas internas. Para el tribunal, la actividad realizada por las plataformas Facebook y YouTube involucra una decisión sobre los contenidos que se exhiben y el orden de su publicación, de modo que estas plataformas desarrollan una “actividad expresiva”, similar a la que realiza un editor en una revista, que se encuentra protegida por la Primera Enmienda.²² En nuestro país, este tema se planteó en las audiencias públicas convocadas en los casos *Rodríguez y Denegri*,²³ donde los integrantes de la Corte Suprema formularon a los representantes de Google numerosas preguntas vinculadas al modo en que las empresas gestoras de los motores de búsqueda elaboran los resultados de búsqueda exhibidos a los usuarios.²⁴ En la más reciente, los representantes de Google reconocieron que la actividad del buscador no era meramente pasiva ni exclusivamente automatizada. Pese a ello, la Corte al fallar se limitó a mencionar el problema de la falta de transparencia del funcionamiento de los algoritmos que emplean los motores de búsqueda y a alertar sobre los riesgos de la actividad de “perfilamiento” que llevan adelante las empresas que los gestionan y la necesidad de afrontar en el futuro esa problemática.²⁵

Por su parte, la Relatoría para la Libertad de Expresión (RELE) de la CIDH afirmó recientemente que, con la evolución tecnológica y la aparición de nuevas modalidades de servicios y negocios, las plataformas digitales ya no actúan como meras transmisoras de la información compartida por personas usuarias, sino que realizan también otras acciones como la selección, clasificación y organización de la información disponible para las personas usuarias, “modificando su visibilidad en función de sus hábitos

22. Suprema Corte de los Estados Unidos, caso *Moody*..., cit., voto de la jueza Kogan, punto I, A. p. 5.

23. CSJN, caso *Rodríguez*, cit.; y CSJN, sentencia del 28 de junio de 2022, *Denegri, Natalia Ruth c/Google Inc s/derechos personalísimos: acciones relacionadas*, Fallos: 345:482.

24. La primera audiencia se llevó a cabo en el año 2014 y la segunda en el año 2022. Ambas pueden visualizarse en el canal de YouTube del Centro de Información Judicial: <https://www.youtube.com/watch?v=Bxlikawvc-I> y <https://www.youtube.com/watch?v=crCdoJpkzoo>

25. CSJN, *Denegri*, cit., considerando 23°.

y determinados criterios comerciales”.²⁶ Asimismo, el Relator alertó, entre otros temas, sobre los riesgos asociados a la concentración del control en unas pocas plataformas y sobre un deterioro de la calidad del debate público generado, por un lado, por los negocios, políticas y prácticas de algunas plataformas digitales, y por el otro, por las respuestas estatales para atender a parte de estos problemas.²⁷

En términos de propuestas de regulación, la UNESCO propicia un enfoque multidimensional y basado en los derechos humanos que comprende una serie de principios básicos aplicables a los sistemas de gobernanza del entorno digital. En primer lugar, se reconoce la necesidad de que las empresas adopten el principio de debida diligencia en materia de derechos humanos. Sin embargo, las directrices también proponen que los buscadores y plataformas de redes sociales acudan al derecho internacional de los derechos humanos para determinar si están frente a contenidos ilícitos que deben ser restringidos, como para evaluar si una restricción a la libertad de expresión sería legítima a la luz de ese cuerpo normativo. Por otro lado, estipulan que cualquier decisión sobre la legalidad de un contenido debe ser sometida a un control judicial posterior. A diferencia del modelo europeo, aquí se reconoce cierto margen a las empresas para definir sus procesos de identificación, moderación de contenidos y evaluaciones de riesgo, reservando al sistema público la fiscalización del cumplimiento de las obligaciones de debida diligencia en materia de derechos humanos. Las directrices también contienen sugerencias para fomentar un mayor acceso a la información y al proceso de toma de decisiones de las empresas en favor de los usuarios, a través de una mayor transparencia y rendición de cuentas, el establecimiento de mecanismos internos eficaces y la concreción de auditorías.²⁸

En la misma línea, el *Pacto Digital Global* incluyó entre sus objetivos fomentar un espacio digital inclusivo, abierto y seguro, que reconozca como

26. CIDH, RELE, *Inclusión digital y gobernanza de contenidos en Internet*, OEA/Ser.L/V/II/CIDH/RELE/INF.28/24, junio 2024, párrs. 182-183.

27. Cit., párrs. 45, 47-48 y 50.

28. UNESCO, *Directrices para la gobernanza de las plataformas digitales: salvaguardar la libertad de expresión y el acceso a la información con un enfoque de múltiples partes interesadas*, ISBN 978-92-3-300215-9, 2023, disponible en <https://unesdoc.unesco.org/ark:/48223/pf0000387360>.

marco el derecho internacional de los derechos humanos, tanto en lo que respecta a la libre circulación de información e ideas como a la protección de los usuarios frente a las violaciones, abusos y todas formas de discriminación a las que pueden estar expuestos en el entorno digital. A su vez, en el documento se exhorta al sector privado a aplicar los *Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas*²⁹ del año 2011, instando a ejercer la diligencia debida en materia de derechos humanos y a crear mecanismos eficaces de supervisión y reclamos por parte de los usuarios. En particular, propone la regulación de marcos de rendición de cuentas que aumenten la transparencia en relación a los sistemas y procesos utilizados, en cuanto a las condiciones del servicio, las políticas de moderación de contenidos, los algoritmos de recomendación y el tratamiento de los datos personales de los usuarios. En línea con la propuesta de UNESCO, se incluye la necesidad de desarrollar soluciones para mitigar o contrarrestar los posibles efectos dañosos derivados de su actividad.³⁰

Como puede advertirse, en la actualidad existe un consenso en las principales regulaciones y directrices del entorno digital –y en particular de la gestión de las redes sociales– en cuanto a que se requiere un marco normativo para su adecuado funcionamiento y que las empresas deben desplegar ciertos deberes básicos de debida diligencia y cuidado a fin de identificar patrones o riesgos sistémicos de circulación de contenidos ilícitos, implementar políticas de moderación de contenidos y transparentar los criterios y procesos de moderación. También que deben contar con procedimientos estipulados claramente para que se realicen denuncias de contenidos ilícitos

29. ONU, Informe del Representante Especial del Secretario General sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas, John Ruggie, *Principios Rectores sobre las empresas y los derechos humanos*, 21 de marzo de 2011, A/HRC/17/31. En estos principios se resalta el papel de las empresas como órganos de la sociedad que desempeñan funciones especializadas y que deben cumplir todas las leyes aplicables y respetar los derechos humanos, así como también que los derechos y obligaciones vayan acompañados de recursos adecuados y efectivos en caso de incumplimiento. Se subraya, entre otros aspectos, que las obligaciones de debida diligencia en materia de derechos humanos abarcan los deberes de identificar, prevenir, mitigar y responder a las consecuencias negativas de sus actividades sobre los derechos humanos (principio 17).

30. ONU, Asamblea General, *El Pacto para el Futuro*, 20 de septiembre de 2024, A/79/L.2, en especial Anexo I (*Pacto Digital Global*), objetivo nro. 3, párrs. 22 a 29 y 36.

y se adopten medidas de reparación.

Este nuevo enfoque de la cuestión no se ha visto todavía reflejado en la jurisprudencia de la Corte Suprema. En decisiones posteriores al caso *Rodríguez*, reiteró que los buscadores son meros intermediarios y que no crean la información disponible en la red, sino que la recorren e indexan de manera automatizada.³¹ En buena medida, ello puede deberse a que el tribunal no ha tenido que analizar hasta ahora la responsabilidad de las plataformas en la moderación de contenidos ilícitos.

Sin embargo, la Procuración General de la Nación (PGN), en el marco de una acción de habeas data, sostuvo que los servicios de motores de búsqueda y las plataformas de redes no resultan meros canales neutrales de transmisión de información, sino que su actividad puede encuadrarse como de alojamiento y tratamiento de datos, y resulta por lo tanto alcanzada por las disposiciones de la Ley 25.326 de Protección de Datos Personales.³² Destacó que la red social Facebook “permite a los usuarios, de manera automatizada, constante y sistemática, almacenar, conservar y registrar datos y, entre ellos, datos personales propios y de terceros; la red social además organiza esos datos según criterios y finalidades predeterminadas; y finalmente, permite a los usuarios relacionar, acceder y difundir los datos personales de terceros”, actividades que se realizan con propósitos que exceden el uso exclusivamente personal (cfr. arts. 1 y 2, Ley 25.326 y decreto reglamentario). En consecuencia, tales acciones ponen en juego el derecho a la autodeterminación informativa comprendido en el artículo 43 de la Constitución Nacional. También señaló que estas disposiciones deben ser adaptadas a las características del entorno digital. Esta posición fue ratificada por la PGN en un caso posterior contra la misma plataforma.³³ Estos casos se encuentran pendientes de una decisión de la Corte, de modo que tendrá la oportunidad de analizar con mayor profundidad esta cuestión.

31. CSJN, *Denegri*, cit., consid. 11º y CSJN, sentencia del 12 de septiembre de 2017, *Gimbutas, Carolina Valeria c/ Google Inc. s/ daños y perjuicios*, Fallos: 340:1236, consid. 5º.

32. Dictamen de la PGN del 27 de mayo de 2022 en *Quinteros, Héctor Andrés c/ Facebook Argentina SRL s/ amparo ley 16986*, causa FLP 25923/2017/CS1. La Procuración sostuvo que tal actividad se encuentra encuadrada en los arts. 1 y 2 de la Ley 25.326 y en el art. 1 del Decreto 1558/2001.

33. Dictamen de la PGN del 9 de noviembre de 2023 en *C, F. c/ Facebook Argentina SRL s/hábeas data*, causa FLP 7640/2019/CS1.

III. La censura en internet. Criterios aplicables a las medidas de bloqueo y filtrado de contenidos

a. Estándares constitucionales aplicables a la materia

Otra cuestión compleja es la definición del marco constitucional que rige las medidas de bloqueo y filtrado de contenidos digitales.

El término “bloqueo” refiere a diversas acciones que pueden llevar a cabo las empresas que gestionan motores de búsqueda, las plataformas de redes sociales, los proveedores de servicios de internet y los operadores de red, a través de las cuales se impide que sus usuarios reciban, publiquen o accedan a determinada información en una ubicación específica. Estas medidas pueden ser variadas y consistir en el bloqueo del acceso a sitios web completos o sitios específicos, la suspensión de la cuenta de un usuario, la eliminación del contenido publicado en una plataforma digital o el bloqueo de un determinado contenido para todos los usuarios de una plataforma o para determinados grupos de usuarios sobre la base de diferentes criterios (por ejemplo, geográficos), entre muchas otras. Es importante señalar que algunas medidas de bloqueo tienen por efecto impedir el acceso a un determinado contenido, pero no implican su supresión. Ello sucede, por ejemplo, en el caso del filtrado que es aplicado por los proveedores de servicios de internet, donde el contenido todavía existe en otros lugares de internet pero se bloquea el acceso a aquellos usuarios de la red a los que se aplica el filtro,³⁴ como también en las llamadas medidas de desindexación, aplicables por los motores de búsqueda, las cuales se dirigen a desvincular enlaces (direcciones URL) de determinadas palabras clave, como el nombre de una persona, a fin de que tales sitios no aparezcan en los resultados de búsqueda.

De tal modo, los motores de búsqueda y plataformas digitales cuentan con diferentes herramientas para limitar la circulación de contenidos y este tipo de medidas puede afectar la libertad de expresión y otros derechos fundamentales. En consecuencia, para evaluar la procedencia de ese tipo

34. R. Mackinnon; E. Hickok; A. Bar; H. Lim, *Fostering Freedom Online. The role of Internet Intermediaries*, editado por UNESCO, 2014, pp. 23-26, disponible en <https://unesdoc.unesco.org/ark:/48223/pf0000231162>.

de medidas resulta indispensable identificar los estándares constitucionales aplicables.

La RELE examinó la cuestión³⁵ y señaló, en línea con los principios establecidos en la Declaración conjunta sobre libertad de expresión e Internet de 2011,³⁶ que las medidas obligatorias de bloqueo y filtrado constituyen restricciones a la libertad de expresión que deben ser adoptadas de manera absolutamente excepcional y que solo son admisibles en la medida en que cumplan con los estrictos parámetros establecidos en el artículo 13(2) de la Convención Americana sobre Derechos Humanos (CADH) para restringir la libertad de expresión.³⁷ Resalta que cualquier medida de bloqueo debe superar el examen basado en el cumplimiento de tres condiciones (“test tripartito”) que desarrollaron los órganos del sistema interamericano de derechos humanos para determinar si una medida restrictiva resulta compatible con la libertad de expresión. Puntualmente, este test exige que la restricción esté previamente prevista en una ley formal, que sea necesaria para el logro de un objetivo imperioso y que sea estrictamente proporcionada. La primera condición es que los supuestos objetivos en los que se podrá restringir la expresión deben estar establecidos en una ley de manera clara y precisa. Respecto de la segunda condición los tratados generales de derechos humanos prevén como propósitos legítimos la protección de bienes jurídicos colectivos, como la seguridad nacional, el orden público, la salud o la moral pública, pero también el respeto de la reputación o de los derechos de terceros.³⁸ Por último, la proporcionalidad implica que la medida sea idónea y adecuada, lo que requiere demostrar que su alcance sea estrictamente necesario para alcanzar el propósito que persigue y que no existen medidas

35. CIDH, RELE, *Libertad de Expresión e Internet*, cit., 2013; *Estándares para una Internet Libre, Abierta e Incluyente*, cit., 2017 y, recientemente, *Inclusión digital y gobernanza de contenidos de internet*, cit., 2024.

36. *Declaración conjunta sobre la libertad de expresión e Internet de 2011*, cit., punto 3(a).

37. CIDH, RELE, *Libertad de Expresión e Internet*, cit., párr. 84 y *Estándares para una Internet Libre, Abierta e Incluyente*, cit., párrs. 85 y 87.

38. Artículos 13.2 de la Convención Americana sobre Derechos Humanos, 19.3 del Pacto Internacional de Derechos Civiles y Políticos y 10.2 del Convenio Europeo de Derechos Humanos.

alternativas disponibles para alcanzar esa finalidad.³⁹

En ese marco, la RELE reconoce que podrían adoptarse medidas de bloqueo y filtrado ante la existencia de contenidos abiertamente ilícitos o que constituyan expresiones no protegidas por la libertad de expresión. Para esta oficina, los discursos de odio que inciten a la violencia, la propaganda en favor de la guerra, la incitación directa y pública al genocidio y la pornografía infantil se encuentran excluidas del ámbito de protección del derecho a la libertad de expresión con sustento en expresas prohibiciones contenidas en el derecho internacional de los derechos humanos.⁴⁰

En virtud de las características de internet y de las formas de comunicación en las redes sociales, estas expresiones tienen un enorme potencial para amplificarse rápidamente en la red y generar una agudización de la violencia contra ciertos grupos o sectores sociales. Por ese motivo, el bloqueo o filtrado de información en línea puede llegar a constituir una medida eficaz para restringir la circulación de cualquiera de esos contenidos ilícitos y evitar un daño concreto e inminente contra determinados individuos o grupos de personas.

Desde el punto de vista de las obligaciones estatales, es posible afirmar que los Estados tienen el deber de adoptar medidas para evitar la propagación de ese tipo de discursos. Ello surge de la obligación de protección

39. V. Abramovich, “Dilemas jurídicos en la restricción de los discursos de odio”, en *El límite democrático de los discursos de odio* de V. Abramovich, M. J. Guembe y M. Capurro Robles (coord.), Editorial Teseo, 2021, pp. 46-48.

40. CIDH, RELE, *Marco Jurídico Interamericano del Derecho a la Libertad de Expresión*, cit., párr. 261 y *Estándares para una Internet Libre, Abierta e Incluyente*, cit., párrs. 78 y 229. La exclusión de estas categorías se realiza sobre la base de la prohibición contenida en el artículo 13, quinto párrafo, de la Convención Americana y de lo dispuesto en preceptos contenidos en otros tratados internacionales, como la Convención para la Prevención y la Sanción del Delito de Genocidio (artículo 3, inciso c), la Convención sobre los Derechos del Niño (artículo 34, inciso c) y su Protocolo Facultativo relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, algunos de los cuales pertenecen al derecho internacional consuetudinario. Una postura similar mantiene el Tribunal Europeo de Derechos Humanos, quien en varios precedentes ha sostenido que los discursos de odio están excluidos de la protección del artículo 10 del Convenio Europeo y en ocasiones ha resuelto aplicar la figura del abuso del derecho prevista en el artículo 17 de ese instrumento (ver Casos no. 35071/97, sentencia del 4 de diciembre de 2003, “Gündüz v. Turkey”, párr. 41; y no. 34367/14, sentencia del 27 de junio de 2017, “Belkacem v. Belgium”, párrs. 30 y 32).

frente a actos de particulares, que el derecho internacional de los derechos humanos les impone. Por otro lado, desde una concepción sustantiva de la igualdad, es exigible al Estado que asuma un rol activo para adoptar acciones y políticas dirigidas a proteger a grupos que son con frecuencia víctimas de violencia en el entorno digital,⁴¹ como las mujeres, las personas travestis trans o las minorías étnicas y raciales.⁴²

En las mencionadas *Directrices de UNESCO*, este mandato de intervención se extiende a las empresas privadas. En tal sentido, estipulan que, en caso de identificar contenidos que podrían ser restringidos en virtud de la normativa internacional de los derechos humanos, las plataformas digitales deben adoptar medidas tendientes a eliminar o limitar la amplificación de aquellos contenidos.⁴³ En sentido similar, la CIDH ha admitido que frente a un peligro claro y actual de daño significativo, los contenidos “manifiestamente ilegales o violatorios de los derechos humanos” podrían ser removidos u objeto de un bloqueo sin mediar orden judicial, con el propósito de prevenir situaciones de violencia. Este órgano incluso ha señalado que imponer en cabeza de las empresas deberes para que moderen y remuevan ese tipo de contenidos podría contribuir al cumplimiento de la obligación estatal de garantía de los derechos protegidos por la CADH.⁴⁴

En nuestro país, la Ley 27.736,⁴⁵ que introdujo modificaciones a la Ley 26.485 de Protección Integral para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres –entre las cuales se encuentra la inclusión de la violencia digital como forma específica de violencia de género–, configura un ejemplo de legislación que contempla la remoción o el bloqueo de contenidos como medida de protección de un colectivo determinado. Tanto el Mecanismo de Seguimiento de la Convención Belém do Pará (MESECVI)

41. V. Abramovich, cit. pp. 27 y 28.

42. M. Marques, “Violencia y abuso online contra las mujeres: lo real de una pandemia virtual” en *El límite democrático de los discursos de odio* de V. Abramovich, M. J. Guembe y M. Capurro Robles (coord.), Editorial Teseo, 2021, p. 350.

43. UNESCO, *Directrices para la gobernanza de las plataformas digitales*, cit., párr. 100.

44. CIDH, RELE, *Inclusión digital y gobernanza de contenidos en Internet*, cit., párrs. 26, 212 y 224.

45. Denominada “Ley Olimpia”, B.O. 23/10/2023.

de la Comisión Interamericana de Mujeres de la OEA⁴⁶ como el Comité de CEDAW en el ámbito de la ONU han alertado recientemente sobre el rol que poseen las plataformas digitales en la naturalización de esta forma de violencia y la necesidad de que las empresas asuman un papel activo en su prevención, a través de políticas de moderación de contenidos que brinden una respuesta inmediata y efectiva a la violencia contra las mujeres.⁴⁷

Por su parte, la Ley Olimpia prevé expresamente que los jueces pueden ordenar a las plataformas digitales o sitios webs la supresión de contenidos que constituyan violencia digital o telemática contra las mujeres.⁴⁸ La norma exige que la medida sea dispuesta por auto fundado y contenga una identificación clara de las direcciones URL específicas que serían afectadas por la medida, elementos que constituyen garantías para asegurar las condiciones de necesidad y proporcionalidad.⁴⁹

b. El examen de ponderación de las medidas de bloqueo

La Corte Suprema argentina, en consonancia con los estándares interamericanos y con su propia doctrina de tutela de la libertad de expresión,⁵⁰ considera que las medidas de filtrado o bloqueo constituyen formas de censura que se presumen inconstitucionales y solo proceden en casos absolutamente excepcionales.⁵¹

46. MESECVI, Informe *Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de Convención Belem do Pará*, 2022, p. 99, disponible en <https://lac.unwomen.org/>.

47. Comité CEDAW, *Recomendación general núm. 40, relativa a la representación igualitaria e inclusiva de las mujeres en los sistemas de toma de decisiones*, 25 de octubre de 2024, CEDAW/C/GC/40, punto V.F., párrs. 36, 37 y 39, punto h.

48. Ley 27.736, artículo 12, primer párrafo, modificatorio del artículo 26 de la Ley 26.485, que establece un catálogo de medidas preventivas urgentes que pueden emplear los jueces ante alguna de las modalidades de violencia contempladas por la ley.

49. CIDH, RELE, *Inclusión digital y gobernanza de contenidos de internet*, cit., párr. 211.

50. Ver doctrinas “Campillay” y de la “real malicia” adoptadas por la Corte Suprema en Fallos: 308:789, *Campillay* y 310:508, *Costa*, respectivamente; así como también el criterio de ponderación estricto elaborado por la Corte en materia de responsabilidad por la difusión de opiniones que emana de los Fallos: 321:2558, *Amarilla* y 335:2150, *Quantín*.

51. CSJN, sentencia del 3 de diciembre de 2019, *Paquez, José c/ Google Inc. s/ medidas precautorias*, Fallos: 342:2187, consid. 9; *Denegri*, cit., consid. 11° y 12°; y dictámenes

En tal sentido, si bien la Corte reconoce que las medidas que ordenan la desindexación de contenidos, la supresión del almacenamiento *caché* de un buscador o el cese de la difusión de enlaces de internet difieren conceptualmente de las medidas de retiro o supresión de contenidos digitales, estima que todas estas medidas, con distinta intensidad, impiden o dificultan el acceso a información y el proceso comunicacional.

Además, las expresiones sobre asuntos de interés público, lo que comprende los asuntos referidos a funcionarios o a personalidades públicas o asuntos que atañen al Estado y a sus instituciones o concitan gran interés social, gozan de mayor protección constitucional.⁵² Estas expresiones son consideradas discursos “especialmente protegidos” por la libertad de expresión, lo que implica que el margen de intervención estatal en estos casos es reducido. La RELE entiende que, como regla, los Estados deben abstenerse de imponer medidas de filtrado o bloqueo para limitar la difusión de este tipo de discursos.⁵³ En esa línea, cuando la restricción puede afectar un discurso de interés público, debe ser sometida a un examen más estricto y exigente y solo procederá en casos absolutamente excepcionales. En sentido contrario, cuando el discurso que se pretende bloquear no reviste interés público, los tribunales tienen mayor margen para dar prevalencia a la protección de derechos de terceros, como el derecho a la reputación, a la propia imagen o a la intimidad, por sobre el derecho a la libertad de expresión. Consecuentemente, para determinar la procedencia de una medida de bloqueo resulta indispensable analizar inicialmente la naturaleza del discurso involucrado.⁵⁴

La Corte examinó esta cuestión en el caso *Paquez* de 2019, donde resolvió dejar sin efecto una medida cautelar que disponía el bloqueo de una serie de publicaciones que contenían críticas a un funcionario público por una serie de hechos relacionados con el ejercicio de su cargo. En particular, observó que la información que se pretendía restringir versaba sobre asuntos de interés público y, por lo tanto, que pesaba sobre la medida restrictiva una

de la PGN del 22 de mayo de 2017 y el 1 de diciembre de 2021, emitidos respectivamente en tales casos.

52. CIDH, *Marco Jurídico Interamericano sobre el Derecho a la Libertad de Expresión*, cit., párrs. 32 a 56.

53. CIDH, RELE, *Estándares para una Internet Libre, Abierta e Incluyente*, cit., párr. 92.

54. CSJN, *Denegri*, cit., considerando 13°.

fuerte presunción de invalidez que no había sido revertida por la cámara. En esa línea, señaló que la cámara había tenido por acreditada la afectación ilegítima del derecho al honor del actor, sin haber analizado mínimamente el contenido de las publicaciones. La sentencia concluyó que la decisión era arbitraria, porque la cámara había omitido evaluar si se estaba en presencia de un supuesto excepcionalísimo que justificara el dictado de la medida preventiva de bloqueo.⁵⁵

También analizó los efectos que pueden acarrear las medidas de filtro o bloqueo que pueden aplicar los motores de búsqueda, pues si bien no conllevan la eliminación de la información objetada, interrumpen los procesos comunicativos, afectando la dimensión social de la libertad de expresión. En concreto, luego de destacar el rol fundamental que desempeñan los motores de búsqueda para el acceso de los usuarios a la información disponible en internet, señaló que las medidas de bloqueo son remedios extremos que afectan severamente la circulación de información. Asimismo, indicó que las medidas que disponen la eliminación de determinadas sugerencias de búsqueda, la desvinculación del nombre de una persona con ciertos enlaces (direcciones URL) o la eliminación de contenidos almacenados por el buscador constituyen también una forma de censura, pues al impedir el acceso a la información que se pretende restringir, impiden o dificultan la concreción del acto de comunicación.⁵⁶ Las medidas de desvinculación (usualmente referida como “desindexación”) como la ordenada en el caso *Paquez* implican en la práctica que la información se vuelve prácticamente inaccesible por los usuarios, quienes deberían acudir a vías alternativas para encontrarla

55. CSJN, *Paquez*, cit., consids. 12° a 13°. En sentido similar, en una decisión reciente la Corte Suprema resolvió, por remisión parcial a los fundamentos expuestos por la PGN, que era arbitraria una sentencia de la Sala III de la Cámara Civil y Comercial Federal que, con sustento en la doctrina emanada del precedente *Rodríguez*, cit., obligaba al buscador de Google a indemnizar a una persona por los daños provocados por contenidos publicados en dos blogs de internet, y a aplicar una medida de bloqueo y supresión de contenidos digitales. La Corte consideró que la alzada ponderó únicamente la potencialidad de la información de dañar la reputación del actor, sin haber analizado los planteos introducidos por la demandada vinculados con la afectación de la libertad de expresión (ver CSJN, sentencia del 5 de noviembre de 2024, *Vecchi, Amado Alejandro c/ Google Inc. s/ daños y perjuicios*, CIV 60439/2013/2/RH1).

56. CSJN, *Denegri*, cit., consids. 9° y 11°.

(como el uso de buscadores de internet menos populares) o conocer el enlace exacto que dirija al contenido en cuestión.

La cuestión volvió a examinarse en el caso *Denegri* del año 2022, en el que se requería el dictado de una medida de desindexación con sustento en el llamado “derecho al olvido”. Las actuaciones tuvieron su origen en la demanda interpuesta por la actora, actriz y productora de medios, con el objetivo de que se ordenara a Google Inc. la desvinculación de su nombre, en los buscadores de Google y de YouTube, con determinados sitios webs con contenidos referidos al resonante caso judicial conocido como “caso Coppola”, en particular, de aquellas páginas que exhibían intervenciones suyas en programas televisivos referidos a hechos del pasado, ocurridos hace más de 20 años. Se aducía que tales contenidos afectaban el honor y la intimidad y carecían de interés actual en razón del transcurso del tiempo. La Corte, compartiendo la opinión expresada por la PGN, consideró que se pretendía limitar la difusión de información veraz vinculada con un asunto de interés público y referida a una persona pública que había consentido la difusión inicial de esa información. En primer término, consideró que todos los aspectos vinculados con la cobertura mediática del caso Coppola eran de interés público, incluidas las entrevistas a sus protagonistas, los escándalos y las peleas que lo caracterizaron. Para la Corte esos programas revestían interés social más allá del valor cultural, periodístico o estético de la información, y además ese interés subsistía pese al transcurso del tiempo. En relación con ello, el tribunal señaló que si se posibilitara a los usuarios restringir recuerdos del acervo público, se “abriría un peligroso resquicio, hábil para deformar el debate que la libertad de expresión pretende tutelar”.⁵⁷ En segundo término, ponderó que la actora era una figura pública, que había cobrado notoriedad a raíz de su participación en diversos programas televisivos que se emitieron durante la cobertura del caso. A partir de ello, entendió que se estaba ante un discurso especialmente protegido por la libertad de expresión y que la actora no había brindado razones válidas para revertir la presunción de inconstitucionalidad de la medida de restricción peticionada.

En la ponderación que debe ser llevada a cabo para determinar si se está ante un discurso protegido, es importante tener en cuenta que algunos de los criterios jurídicos tradicionalmente empleados por la Corte para

57. CSJN, *Denegri*, cit., consid. 14°.

resolver las tensiones entre la libertad de expresión y derechos personalísimos de una persona requieren de una redefinición para poder aplicarlos a la comunicación en internet.

En tal sentido, al analizar la naturaleza del discurso, tanto en *Denegri* como en *Paquez*, la Corte Suprema mantiene la tradicional distinción entre sujetos públicos y privados, según el cual se aplica a las figuras públicas y los funcionarios públicos un estándar de protección atenuada del derecho a la reputación y la privacidad. Ello implica que aquellos deben mostrar, en relación con los particulares, una mayor tolerancia a las expresiones críticas, irritantes o intrusivas, y encuentra sustento en la necesidad de garantizar un debate libre y desinhibido sobre asuntos de interés público, pero también, en la posibilidad que tienen de replicar tales expresiones por contar con un mayor acceso a los medios de comunicación.⁵⁸ Sin embargo, en el entorno digital esta clasificación puede verse desdibujada con la intervención de nuevos actores, como los “influencers”, esto es, particulares usuarios que cuentan con grandes audiencias en plataformas, que en ocasiones llegan a superar el millón de seguidores. En efecto, los “influencers” tienen la capacidad de emitir y replicar expresiones lesivas y al mismo tiempo generan discusión pública sobre sus expresiones y estilos de vida en las redes o en ciertas comunidades específicas, de modo que pueden ser agraviados o afectados en su reputación o privacidad. Existe un debate abierto sobre si corresponde darles el tratamiento de las personalidades públicas o de los simples particulares.⁵⁹

Por otro lado, si bien la noción de interés público sigue siendo un concepto clave para determinar la procedencia de una medida de bloqueo, también requiere de una reinterpretación en el espacio digital. Ello, por cuanto

58. Ver en ese sentido, entre otros, las sentencias de la Corte Suprema de Justicia en Fallos: 310:508, *Costa*; 330:4615, *Franco*; 331:1530, *Patitó*; 335:2283, *E., R. G.*; 342:1665, *De Sanctis*; 345:482, *Denegri* y, más recientemente, sentencias del 29 de octubre de 2024 en los casos *B., M. y otros c/ Editorial La Página S.A. y otros s/ daños y perjuicios*, CIV 075332/2008/CS001 y *B., L. B. y otros c/ Grondona, Mariano y otros s/ daños y perjuicios*, CIV 84116/2005/2/RH2.

59. F. Lomonte; S. Leibert, “Internet Famous: Are Online Influencers and Micro-Celebrities Public Figures Under Defamation Law?”, *Missouri Law Review*, Vol. 88, Issue 3, 2023, pp. 731-732, disponible en <https://scholarship.law.missouri.edu/mlr/vol88/iss3/7>.

existen temas que, aunque no califiquen estrictamente como “áreas que preocupan, importan o interesan a toda la sociedad”, pueden tener relevancia e impacto en sectores determinados de la población, ámbitos delimitados o en pequeñas comunidades. Así, por ejemplo, la información subida en una plataforma digital referida a un caso de corrupción en una pequeña localidad o a una situación de abuso sexual que afecta a una determinada institución educativa, pueden llegar a ser considerados “discursos especialmente protegidos”, lo que determinaría la aplicación del estándar de proporcionalidad estricto fijado por la Corte. Esta cuestión fue analizada por la PGN en el caso *C., F.*, donde se valoró que los hechos de violencia de género denunciados –que involucraban a dos estudiantes universitarios– revestían de notorio interés para la comunidad educativa involucrada y por lo tanto, correspondía otorgar la mayor amplitud posible a la circulación de los contenidos objeto, en virtud del deber estatal de debida diligencia en la prevención de violencia de género que surge de la Convención de Belem Do Pará.⁶⁰

c. La obligación de explorar la disponibilidad de medidas alternativas y de requerir la identificación del contenido o expresión que se pretende restringir

Un aspecto relevante de la decisión de la Corte en *Denegri* es que establece que las medidas de filtro o bloqueo deben limitarse estrictamente a aquella información indispensable para satisfacer la finalidad pública que se persigue,⁶¹ con mínima interferencia en la libre expresión. De modo que el tribunal incorpora aquí un análisis riguroso sobre la proporcionalidad de la medida.

Como ha sido mencionado, el examen de proporcionalidad comprende el deber de los jueces y tribunales de verificar que la finalidad perseguida no pueda ser alcanzada mediante medidas menos restrictivas de la libertad de expresión. En otras palabras, la medida de bloqueo solo puede ser adoptada “cuando sea la única medida disponible para alcanzar una finalidad imperativa”.⁶²

60. Dictamen de la PGN del 9 de noviembre de 2023 en *C., F. c/ Facebook Argentina SRL s/habeas data*, causa FLP 7640/2019/CS1.

61. *Denegri*, consid. 11º.

62. CIDH, RELE, *Estándares para una Internet Libre, Abierta e Incluyente*, OEA/

Ello implica que previo a resolver un pedido de bloqueo de contenidos online, los jueces deben evaluar las distintas posibilidades que ofrece internet para reparar de manera adecuada los daños ocasionados al derecho presuntamente vulnerado. Este ha sido el enfoque recomendado por la CIDH como por el ex Relator Especial para la libertad de expresión de la Organización de las Naciones Unidas, Frank La Rue. Ambos han destacado en sus informes la importancia de explorar la existencia de alternativas que pueden brindar los avances tecnológicos, en especial, la posibilidad de ejercer de manera efectiva y rápida el derecho de rectificación o respuesta,⁶³ lo que tiene especial relevancia cuando se alega la afectación al derecho al honor.

La PGN siguió esta pauta en un caso reciente⁶⁴ donde examinó la procedencia de una medida de bloqueo solicitada para que Google restringiera el acceso a información que había devenido desactualizada, referida a una condena penal anulada varios años después. La medida afectaba información de interés público, ya que los sitios web se referían al vínculo profesional del actor con un ex presidente, quien lo había indultado en ese mismo caso.

En el dictamen se señaló que la medida no era estrictamente necesaria para el logro de la finalidad imperiosa que perseguía, porque estaban disponibles otras medidas idóneas para tutelar el derecho al honor del actor, que eran menos lesivas de la libertad de expresión. En esa línea, se remarcó que el espacio digital brinda oportunidades tecnológicas que permiten adoptar medidas adecuadas para reparar el derecho a la reputación del actor, sin afectar el acceso a los archivos digitales con información de interés público. Puntualmente, se indicó que, en lugar de disponer la desvinculación definitiva del nombre del actor con la información referida a sus antecedentes penales, se podía ordenar al motor de búsqueda que establezca en los sitios web cuestionados un vínculo directo a un sitio digital que albergue la información relativa a la anulación de la sentencia. De esa manera, se sugirió una

Ser.L/V/II CIDH/RELE/INF.17/17, 15 de marzo 2017, párr. 139.

63. CIDH, RELE, *Libertad de expresión e Internet*, cit., párr. 64; ONU, *Informe del Relator de la Organización de las Naciones Unidas sobre la libertad de expresión*, Frank La Rue, A/HRC/17/27, cit., párr. 27.

64. Dictamen de la PGN del 6 de julio de 2023 en *Vecchi, Amado Alejandro c/ Google Inc. s/ daños y perjuicios*, causa CIV 68640/2013/4/RH1.

alternativa que implica incrementar el caudal de información al que tienen acceso los internautas, en vez de restringirlo.⁶⁵

Para el caso de que se concluya que no existe una medida alternativa menos lesiva, quien evalúa la procedencia de la medida de bloqueo debe observar que sea cuidadosamente diseñada, a fin de que impacte exclusivamente sobre los contenidos reputados ilegítimos.

En tal sentido, la RELE⁶⁶ ha remarcado que el bloqueo debe estar dirigido contra contenidos específicos. Ello implica que no puede ser ordenado en términos excesivamente amplios, ni basarse en criterios ambiguos y poco claros, pues en tales casos los efectos de la medida se extenderían sobre contenidos legítimos ajenos a la acción deducida. El Tribunal Europeo de Derechos Humanos (TEDH) abordó esta cuestión en una serie de casos de afectación de la libertad de expresión por medidas judiciales que impedían el acceso a sitios web enteros o que disponían bloqueos generalizados.⁶⁷ En esas decisiones el tribunal señaló que las restricciones que tienen como consecuencia automática el bloqueo del acceso a contenidos legítimos producen efectos desproporcionados sobre el ejercicio de la libertad de expresión y, en consecuencia, constituyen una interferencia estatal arbitraria incompatible con el artículo 10 del convenio europeo.

Las órdenes de bloqueo mal diseñadas o inadecuadamente calibradas que omiten individualizar los contenidos específicos a restringir, o bien los describen de forma imprecisa o ambigua, conllevan el riesgo de producir un daño excesivo y desproporcionado en la libre expresión. En consecuencia, la autoridad judicial que recibe una solicitud de bloqueo debería requerir al peticionante la identificación clara de los contenidos que se pretende bloquear. En esa línea, los jueces Lorenzetti y Maqueda se refirieron a este tema en su disidencia parcial en el caso *Rodríguez*, donde postularon que la previa y precisa identificación de los enlaces que se quiere bloquear resulta

65. La Corte Suprema omitió expedirse sobre la cuestión, al declarar inadmisibile el recurso extraordinario invocando el artículo 28o del Código Procesal Civil y Comercial de la Nación (ver sentencia del 5 de noviembre del 2024).

66. CIDH, RELE, *Estándares para una Internet Libre, Abierta e Incluyente*, cit., párr. 88.

67. TEDH, sentencia del 18 de diciembre de 2012, caso *Ahmet Yildirim v. Turkey*, párr. 68 y, más recientemente, sentencias del 23 de junio de 2020 en casos *OOO Flavus and others v. Russia*, párr. 38 y *Vladimir Kharitonov v. Russia*, párr. 43, respectivamente.

una condición de admisibilidad de los pedidos de eliminación de vinculaciones formulados en acciones de tutela preventiva.⁶⁸ Asimismo, este estándar fue receptado en forma reciente por la “Ley Olimpia”, en donde se incluyó la individualización de las direcciones web involucradas como uno de los requisitos para que pueda ordenarse la remoción de contenidos online que constituyan violencia digital.⁶⁹

IV. La expresión anónima en redes

Otro de los temas vinculados al ejercicio de la libertad de expresión en el entorno digital, en los cuales los tribunales se verán interpelados en forma creciente, está vinculado al derecho de los usuarios a comunicarse en forma anónima en las redes sociales. Esta forma de expresión, si bien no es novedosa, ha cobrado mayor relevancia en los últimos tiempos por las características propias del entorno digital, que presenta una mayor fluidez y dispersión en cuanto a sus foros y emisores. Es necesario por lo tanto hacer una breve mención a algunos estándares globales en la materia y a las obligaciones de las empresas gestoras ante un pedido de develar información acerca de un usuario anónimo.⁷⁰

68. CSJN, *Rodríguez*, cit., disidencia parcial de los jueces Lorenzetti y Maqueda, considerando 30°. En igual sentido, ver dictamen de la Procuración General de la Nación del 1 de abril del 2025 en *Recurso de queja n° 1 – Incidente n° 2 – C. Z., M. c/ Google Argentina SRL y otros s/art. 250 C.P.C – Incidente civil*, causa CIV 89459/2015/2/1/RH3.

69. Ley 27.736, artículo 12, primer párrafo.

70. Si bien en este apartado hablamos de los estándares relativos a los pedidos de “revelación” en el marco de acciones vinculadas a pedidos de bloqueo o de una reparación pecuniaria, debemos mencionar que, en forma reciente, en una causa donde se investiga la posible comisión del delito de amenazas coactivas agravadas a raíz de los mensajes intimidatorios y amenazantes enviados por usuarios de redes sociales –en un contexto electoral– a miembros de la familia de uno de los principales candidatos en las elecciones presidenciales del año 2023 en Argentina, la Cámara Nacional Electoral confirmó el procesamiento dictado contra los titulares de algunas de las cuentas de Instagram denunciadas. Entre sus fundamentos, el tribunal destacó que el anonimato que ofrecen las redes sociales puede conducir al maltrato y a la proliferación de discursos de odio, como también a actos de violencia política en los procesos electorales. Ver Cámara Nacional Electoral (CNE), decisión del 29 de octubre de 2024, causa CNE 9500/2023/6/CA2.

De modo general, debe tenerse presente que la protección a la expresión anónima o al anonimato se vincula con la necesidad de desvincular el discurso del emisor, con el fin de resguardar a la persona frente a las posibles represalias derivadas de dicha expresión, evitar el “efecto inhibitor” y asegurar de este modo un mayor flujo de información que se vuelca en el debate público.

Por lo tanto, desde diversos organismos internacionales se remarcó que las decisiones de develar datos de usuarios anónimos deben cumplir en forma estricta con los principios en materia de restricciones a los derechos humanos, en especial la necesidad y la proporcionalidad, y deben ser llevadas a cabo mediante una orden judicial basada en una ley clara, evitando las prohibiciones abiertas, y con estricto apego al debido proceso legal.⁷¹

A su vez, existe en la mayoría de los sistemas una fuerte protección a esta forma de expresión. En el ámbito europeo, el TEDH analizó la adopción de medidas tendientes a revelar la identidad del autor en un caso del 2021⁷² y advirtió que, si bien el derecho de los usuarios a comunicarse en forma anónima no es absoluto, las medidas que obligan a revelar la identidad pueden tener un efecto inhibitorio sobre los participantes de un foro de discusión.

La CIDH, por su parte, destacó en un informe de 2013 que el anonimato tiene un papel relevante en el ejercicio de la libertad de expresión, en tanto promueve la participación en el discurso público al evitar el riesgo de represalias asociadas con la opinión.⁷³ Luego, en 2017,⁷⁴ volvió a referirse a la importancia de proteger la expresión anónima y señaló que los Estados solo pueden adoptar medidas para identificar fehacientemente a una persona en el marco de una investigación judicial y siempre y cuando se respete el principio de proporcionalidad. Allí también se reconoció que la

71. Ver informes del Relator Especial de la ONU sobre Libertad de Expresión, A/HRC/29/32, del 22 de mayo de 2015, párr. 60 y A/HRC/38/35, del 6 de abril del 2018, cit., párr. 30.

72. TEDH, sentencia del 7 de diciembre del 2021, caso *Standard Verlagsgesellschaft MBH v. Austria*, párr. 74.

73. CIDH, *Libertad de Expresión e Internet*, cit., párr. 134.

74. CIDH, RELE, *Estándares para una Internet Libre, Abierta e Incluyente*, cit., párrs. 227-229.

obligación de proteger el anonimato se extiende a las empresas privadas, quienes deben evitar incluir en sus condiciones de uso la exigencia de consignar la identidad real.⁷⁵

Hasta el momento, la Corte Suprema no se ha expedido sobre reclamos que involucren revelar el anonimato en redes. Sin embargo, la PGN ha analizado este punto en los ya referidos casos *Quinteros y C., F.*, en los cuales, a través de acciones de habeas data, los actores perseguían la eliminación de contenidos digitales y la divulgación de información relativa a los titulares de las cuentas donde se habían efectuado las publicaciones.

En *Quinteros*, en línea con los estándares internacionales examinados, la PGN sostuvo que la expresión o a divulgación de ideas, opiniones e información en forma anónima, como modo de participación en debates de asuntos de interés público, es una manera usual de expresión en internet y en las redes sociales, por lo que la revelación del autor es una forma indirecta de

75. En cuanto al derecho comparado, puede relevarse la situación de los Estados Unidos, donde la Suprema Corte sostuvo que el derecho a hablar anónimamente está protegido por la Primera Enmienda, ya que el anonimato es “un escudo frente a la tiranía de la mayoría [...] para proteger a los individuos impopulares de represalias [...] a manos de una sociedad intolerante”. Consecuentemente, esa Corte otorgó mayor protección constitucional al discurso político anónimo que al discurso comercial anónimo difamatorio, que infringe los derechos de autor o viola la ley penal. A su vez, entendió que un Estado puede criminalizar la incitación a una acción ilícita inminente, o la realización de ciertas amenazas, sin entrar en conflicto con la Primera Enmienda (ver decisión del 19 de abril de 1995 en *McIntyre v. Ohio Elections Comm’n*). La Corte de ese país también sostuvo que la identificación [forzada] y el miedo a las represalias podría disuadir discusiones perfectamente pacíficas sobre asuntos públicos importantes (v. decisión del 7 de marzo de 1960 en *Talley v. California*). Por otro lado, los tribunales inferiores han generado una copiosa jurisprudencia en materia de revelación de la identidad frente a discursos anónimos (“unmasking”), tanto en casos civiles como penales. Así, los tribunales adoptaron diferentes criterios para decidir sobre cada uno de estos pedidos. Estos hacen foco en la viabilidad de la demanda, en la finalidad perseguida y en la debida diligencia demostradas por el solicitante. Presumiblemente, se busca separar las acciones que poseen un objetivo legítimo de aquellas que tienen como finalidad amedrentar o disuadir al emisor. Alguna de las pautas delineadas suelen ser: demostrar la “buena fe” en la solicitud, que el planteo pueda sobrevivir a una moción de desestimación, que la información no pueda conseguirse por otros medios, entre otras. Ver en este sentido, L. Arbatman; J. Villaseños, “Anonymous Expression and ‘Unmasking’ in Civil and Criminal Proceedings”, *Minnesota Journal of Law, Science & Technology*, Vol. 23, Issue 1, 2022, disponible en <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1509&context=mjlst>.

limitar esa modalidad de expresión, ya que puede inhibir expresiones futuras. Por lo tanto, configura una restricción de la libre expresión en esa esfera comunicativa, que debe satisfacer estrictos recaudos de razonabilidad. Allí el pedido de revelación de identidad del emisor se efectuó en el marco de la publicación de información sobre un funcionario público, relativa a asuntos de interés público, es decir, un discurso especialmente protegido por la libertad de expresión, lo que exige aún mayor prudencia. La cámara había hecho lugar a la medida. Sin embargo, la PGN analizó que esa decisión se había impuesto violentando las reglas del debido proceso, por lo que la restricción a la libertad de expresión resultaba infundada.

Por su parte, en el caso *C., F.* el actor había solicitado que se ordenara a Facebook Argentina SRL la divulgación de información tendiente a identificar a los administradores de las cuentas de Facebook e Instagram a través de las cuales se había publicado la información considerada difamatoria. La PGN nuevamente rechazó esta pretensión del actor, esta vez fundado en que el pedido de divulgación excedía el ámbito de protección del derecho a la autodeterminación informativa, que consagra el artículo 43, tercer párrafo de la Constitución. Se explicó que la Ley 25.326, reglamentaria del instituto de habeas data, contempla el derecho a la rectificación, actualización, supresión o confidencialidad de los datos personales. Ahora bien, en el caso el actor solicitaba que se revele la identidad de terceras personas con la finalidad de iniciar una acción resarcitoria en su contra, con lo cual dicho objetivo no se compadecía con el objeto de la regulación, que es permitir el ejercicio del derecho de los ciudadanos a controlar y disponer de sus datos personales en registros o bancos de datos. Se advirtió, asimismo, que la Ley 25.326 (art. 15, inc. 2) prohíbe expresamente el suministro de datos pertenecientes a terceros, aun si estos guardan vinculación con el interesado. Por último, la PGN subrayó que si bien el decreto reglamentario 1558/2001 contempla el supuesto de requerir información “sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos” (art. 14, párrafo tercero, inciso c), ello solo resulta procedente si el conocimiento de la fuente o medio por donde se obtuvieron los datos resulte indispensable para la consecución de alguno de los objetivos enunciados en la Ley 25.326, lo que no se configuraba en el caso.⁷⁶

76. PGN, *C., F. c/ Facebook Argentina SRL s/habeas data*, cit.

V. Debates en torno a la jurisdicción y la representación en juicio

La posibilidad real de los usuarios de ejercer sus derechos se encuentra directamente vinculada con el sometimiento efectivo de las empresas intermediarias a la jurisdicción de los tribunales nacionales y a la participación que adopten estas empresas en los procesos judiciales. El asunto adquirió mayor notoriedad a nivel regional con la decisión de la justicia de Brasil de suspender temporalmente el acceso a la plataforma X a los usuarios allí localizados, en parte, por no haber designado representantes en el país, en el marco de una investigación judicial.⁷⁷

Una cuestión a considerar en esta disputa es que el carácter transnacional de los flujos de información facilita una cierta deslocalización de las empresas de servicios, pues si bien tienen una casa matriz, no suelen estar registradas como sociedades legales en todos los países en los que comercializan sus servicios. En su caso, existe una discusión abierta sobre la posibilidad que tiene la justicia argentina de juzgar, o de someter a su jurisdicción, a las sociedades controlantes no constituidas legalmente en el país, y también sobre el carácter de las sociedades que funcionan como filiales locales de la casa matriz, en el sentido de que puedan ser consideradas representantes o sociedades vinculadas a la empresa controlante o a un grupo económico.

En el referido caso *Costeja* el TJUE estableció la naturaleza del vínculo entre Google Inc. –empresa matriz del grupo Google que gestiona el buscador “Google Search”, con domicilio en Estados Unidos– y Google Spain, empresa con personalidad jurídica propia y domicilio en Madrid, España, que actúa como filial y agente comercial del grupo Google en ese país. En ese caso, Google Inc. había designado a Google Spain como responsable del tratamiento ante la Agencia Española de Protección de Datos (AEPD). Sin embargo, la actividad de tratamiento de datos personales a través de la búsqueda e indexación, en sí misma, es una actividad que realiza Google Inc. y no la filial española. Sin desconocer ese contexto, el tribunal tuvo en cuenta,

77. Para profundizar el análisis sobre la legalidad de esta medida, ver Conversatorio de *OBSERVACOM* titulado “Bloqueo a X en Brasil: ¿medida legítima o desproporcionada?” del 9 de septiembre de 2024, disponible en <https://www.observacom.org/bloqueo-a-x-en-brasil-medida-legitima-o-desproporcionada/>.

por un lado, que la filial realiza actividades dentro del territorio de España, entre ellas, la promoción y venta de los espacios publicitarios del motor de búsqueda, lo cual sirve para rentabilizar el servicio propuesto por el motor, que sí incluye el tratamiento de datos personales. A la vez, a los fines de calificar su actividad como tratamiento de datos, la norma europea no exigía que éste fuera efectuado por el propio establecimiento en cuestión, sino que se realizara “en el marco de sus actividades”. Según el tribunal, entonces, las actividades de ambas empresas se encontraban “indisociablemente ligadas”.

En nuestro país, este tema se discutió en distintos pronunciamientos, como en *Quinteros y C., F.*, donde la PGN adoptó en gran medida criterios similares a los delineados por el tribunal de justicia europeo. En ambos casos las acciones de habeas data fueron dirigidas contra Facebook Argentina SRL y la empresa había argumentado carecer de legitimación para ser demandada, pues la gestión de la red social –y, por lo tanto, la potestad sobre la gestión de contenidos– es realizada por la casa matriz, Facebook Inc. (antes Facebook Ireland Ltd). Esta última no se encuentra inscripta ante la Inspección General de Justicia de nuestro país, lo que sí ocurre con Facebook Argentina SRL.

La PGN tuvo en cuenta, por un lado, la “interdependencia económica” de las actividades realizadas por ambas empresas, por cuanto Facebook Argentina SRL tiene por objeto “brindar servicios relacionados con soportes de ventas para publicidad, marketing y relaciones públicas” de la red social que gestiona Facebook Inc., mediante una actividad que conlleva el tratamiento de datos personales de habitantes de nuestro país, y que, por lo tanto, encuadra en la Ley 25.326 y su decreto reglamentario. Así, se consideró que la filial argentina “se aprovecha del tratamiento de datos a los efectos de desarrollar su actividad comercial y, además, ese tratamiento de datos se sostiene y alcanza beneficios económicos para el grupo a partir de las actividades de publicidad, marketing y relaciones públicas realizadas por la sede argentina”.

Por otro lado, consideró la apariencia de representación que exhibe la filial local respecto de la casa matriz y del grupo económico. En tal sentido, la filial local no solo desarrolla una actividad económica ligada a la del grupo, sino que se encarga de las relaciones públicas de la red social en nuestro país. Estos elementos resultan idóneos para generar confianza en los usuarios y potenciales víctimas residentes en Argentina sobre la vinculación jurídica de ambas sociedades y la posibilidad de la filial local de representar y responder por la gestión de la red social.

VI. Reflexiones finales

El enfoque que concebía a las empresas de servicios en internet como meros “canales neutrales” de contenidos generados por terceros y que inspiró en gran medida las primeras sentencias de la Corte Suprema desde *Rodríguez*, se encuentra sujeto a replanteos y fuertes cuestionamientos. Aquella tesis inicial rechazó la adopción de un sistema de responsabilidad objetiva basada en el riesgo de la actividad económica de estas empresas, y se inclinó por un esquema de índole subjetiva, basado en la respuesta negligente ante el conocimiento efectivo de un contenido ilícito. La postura que predomina en la actualidad en los organismos internacionales especializados, como la CIDH, la RELE y UNESCO, así como en ámbitos multilaterales como la UE, consiste en proponer modelos regulatorios que contemplan la diversidad de actores que interactúan en el entorno digital, y que imponen a las empresas de servicios en línea deberes básicos de diligencia para identificar riesgos sistémicos de contenidos ilícitos, transparencia activa sobre sus criterios de gestión de la información y sus políticas de moderación, así como la disponibilidad de recursos adecuados para los usuarios y terceros afectados por contenidos nocivos.

En esta nueva perspectiva entonces, si bien no se impone una responsabilidad objetiva basada en el riesgo de la actividad y se preserva para la mayoría de los casos el presupuesto del conocimiento efectivo del contenido ilícito, se reconoce que las empresas de servicios en internet realizan tareas de “edición de contenidos” y de “tratamiento de datos personales” que trascienden la mera difusión de contenidos producidos por terceros. Por ende, están obligadas a desplegar un esfuerzo básico de supervisión, con el propósito de identificar riesgos sistémicos de circulación de contenidos nocivos, como las expresiones de odio y la violencia digital. El caudal de información y la velocidad de circulación coloca a estas empresas en un lugar insustituible para adoptar criterios y políticas de moderación de contenido. A su vez, estas políticas suelen implementarse a través de mecanismos automatizados y en resguardo de un determinado modelo de negocios sin mayor consideración del interés social. De allí que la tensión que se presenta es evidente, pues un exceso de celo en la moderación puede cercenar expresiones legítimas y excluir a determinadas voces de la discusión pública, mientras que una actitud displicente puede habilitar la reproducción de contenidos ilícitos a gran escala. Ambas situaciones afectan la calidad e integridad de los procesos comunicativos.

En este enfoque además se reconoce el papel clave de los Estados como garantes de la libertad de expresión en internet, lo que en ocasiones se traduce en deberes específicos de protección frente a la acción de los particulares, y de regulación de los servicios de redes y plataformas digitales. Las pautas básicas para la regulación de empresas de servicios en línea constituyen una valiosa guía para los decisores de política pública y, a su vez, pueden orientar futuras regulaciones en nuestro país y en la región.

Al mismo tiempo, estas pautas deben integrarse a la discusión constitucional relativa a la responsabilización jurídica de las empresas de servicios digitales, los criterios generales para imponer deberes de moderación, así como responsabilidad civil por la falta de debida diligencia y la opacidad de sus políticas y marcos de actuación.

La elaboración de estándares jurisprudenciales consistentes resulta imprescindible para garantizar la libre expresión en el entorno digital al mismo tiempo que se alcanza una ecuación de cierto equilibrio en el resguardo de la privacidad, la reputación y la vida sin violencia. Como ocurre con las políticas empresariales de moderación de contenidos en línea, también los sistemas judiciales enfrentan el desafío de calibrar ajustadamente el alcance de su intervención para resguardar los derechos fundamentales afectados por la circulación de contenidos nocivos, sin obturar la comunicación y el debate público.

Como vimos, en el ámbito de la Corte Suprema se han identificado algunos principios constitucionales que aportan un marco de racionalidad a la discusión jurídica y acotan el margen de la arbitrariedad judicial. En particular: la protección especial de las expresiones de interés público; la conceptualización de las medidas de bloqueo, filtrado y desindexación como formas de interrupción del proceso comunicativo y, por lo tanto, como mecanismos de censura que requieren, para su procedencia, de una justificación constitucional muy estricta; la necesidad de diseñar esos remedios sobre la base de una pauta de rigurosa proporcionalidad que obliga a explorar la disponibilidad de otras medidas disponibles y menos lesivas tales como las medidas de vinculación de contenidos –links–, que amplían y no suprimen información; la identificación precisa de los remedios de bloqueo o filtrado, para evitar formulaciones generales o ambiguas, entre otros principios.

Sin embargo, como expusimos a partir del relevamiento de casos judiciales, resta abordar en esta materia varios temas espinosos que carecen de pautas jurisprudenciales claras, como el tratamiento del anonimato, las

expresiones de interés en comunidades específicas, la condición pública o privada de los “influencers” y, en especial, los criterios para resolver conflictos de jurisdicción y representación procesal que plantea el carácter transnacional y el ropaje jurídico de las grandes empresas de plataformas, redes y buscadores.

En suma, en la medida en que el espacio digital se erige como el principal ámbito donde se desarrolla la discusión pública, su funcionamiento supone graves desafíos para la Corte Suprema y el sistema de justicia, pues obliga a revisar y adaptar las categorías tradicionales de su jurisprudencia sobre libertad de expresión e incluso sus enfoques iniciales sobre el papel de las empresas de servicios en internet. A su vez, el desarrollo de nuevas herramientas tecnológicas genera posibilidades que deben ser aprovechadas por los tribunales para formular medidas de reparación de los daños generados por la propalación de contenidos violentos, difamatorios o intrusivos sin interferir excesivamente en la libertad de expresión. Se trata de incorporar reglas de civilidad que favorezcan y no obstaculicen la discusión pública.

Bibliografía

- V. Abramovich, “Dilemas jurídicos en la restricción de los discursos de odio”, en *El límite democrático de los discursos de odio* de V. Abramovich, M. J. Guembe y M. Capurro Robles (coord.), Editorial Teseo, 2021, pp. 46-48.
- L. Arbatman; J. Villasenor, “Anonymous Expression and ‘Unmasking’ in Civil and Criminal Proceedings”, *Minnesota Journal of Law, Science & Technology*, Vol. 23, Issue 1, 2022, disponible en <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1509&context=mjlst>.
- F. Lomonte; S. Leibert, “Internet Famous: Are Online Influencers and Micro-Celebrities Public Figures Under Defamation Law?”, *Missouri Law Review*, Vol. 88, Issue 3, 2023, pp. 731-732, disponible en <https://scholarship.law.missouri.edu/mlr/vol88/iss3/7>.
- R. Mackinnon; E. Hickok; A. Bar; H. Lim, *Fostering Freedom Online. The role of Internet Intermediaries*, editado por UNESCO, 2014, pp. 23-26, disponible en <https://unesdoc.unesco.org/ark:/48223/pf0000231162>.
- M. Marques, “Violencia y abuso online contra las mujeres: lo real de una pandemia virtual”, en *El límite democrático de los discursos de odio* de

- V. Abramovich, M. J. Guembe y M. Capurro Robles (coord.), Editorial Teseo, 2021, p. 350.
- R. Post, “Data Privacy and Dignitary Privacy: Google Spain, the right to be forgotten, and the construction of public sphere”, *Duke Law Journal*, Vol. 67, 981, 2018.