SECCIÓN DISERTACIONES

EL USO DE TECNOLOGÍA DE *COOKIES*: IMPLICANCIAS JURÍDICAS Y CONSIDERACIONES ÉTICAS

Pablo Rafael Banchio[24]

"Conferencia mundial: Entornos digitales, nuevas tendencias en redes sociales y el fin de las contraseñas"
Escola de Direito das Faculdades Londrina (Brasil), 31 de agosto 2023

1. Introducción

Distinguidos participantes, colegas y expertos en el ámbito jurídico, es un privilegio presentarles esta exposición centrada en el trascendental tema del fin de las contraseñas en los entornos digitales en el marco de esta conferencia mundial sobre "Entornos digitales, nuevas tendencias en redes sociales y el fin de las contraseñas", organizado por la Escola de Direito das Faculdades Londrina (Brasil).

En un mundo donde la ciberseguridad es esencial, la evolución hacia métodos más avanzados plantea desafíos legales y cuestiones de seguridad jurídica que debemos abordar de manera cautelosa, cosa que intentaremos hacer en este marco.

2. El fin de las contraseñas

2.1. El paradigma actual de las contraseñas

El "fin de las contraseñas" en los entornos digitales se refiere a la transición hacia métodos de autenticación y seguridad en línea que no dependan exclusivamente de contraseñas tradicionales para verificar la identidad de un usuario.

[24] Posdoctor cum laude en Nuevas Tecnologías y Derecho, Università degli Studi di Reggio Calabria (Italia). Posdoctor en Principios Fundamentales y Derechos Humanos y Doctor en Derecho Privado (UCES). Posdoctorando en Globalisation and Human rigths (Institute for Research and European Studies (IRES). Magíster en Derecho Empresario (UA). Especialista en Asesoría Jurídica de Empresas (UBA). Coordinador académico del Doctorado en Ciencias Jurídicas, Facultad Interamericana de Ciencias Sociales (FICS). Miembro Titular del Centro de Estudios de Derecho Privado (CEDEP) de la Academia Nacional de Ciencias de Buenos Aires. Miembro de la Rede de Pesquisa Direitos Humanos e Transnacionalidade (REDHT).

Las contraseñas han sido durante mucho tiempo el estándar para la autenticación y acceso a plataformas digitales y la forma mas común de proteger cuentas en línea y sistemas informáticos. Sin embargo, esta práctica presenta limitaciones significativas en términos de seguridad y han demostrado ser susceptibles a problemas de seguridad, como robos, filtraciones y ciberataques.

Tanto crecieron las aplicaciones digitales y tan necesarias se hicieron las contraseñas para acceder a ellas que comenzaron a proliferar las llamadas "contraseñas débiles", la reutilización de contraseñas y los riesgos de filtración de datos, que convirtieron a esta forma de autenticación en un objetivo para los ciberdelincuentes.

La idea detrás del "fin de las contraseñas" es buscar alternativas más seguras y convenientes para autenticar a los usuarios.

2.2. Nuevas tecnologías de autenticación

Algunas de estas opciones incluyen nuevas formas que fueron desarrolladas en los últimos tiempos, entre las cuales podemos señalar las siguientes:

a) Autenticación de "dos factores" (2FA) o "multifactor" (MFA): Este método requiere que el usuario proporcione dos o más elementos de autenticación para acceder a una cuenta. Puede ser una combinación de algo que el usuario sabe (contraseña), algo que el usuario tiene (un dispositivo móvil) y algo que el usuario es (huella digital, reconocimiento facial).
b) Autenticación biométrica: Utiliza características físicas o de comportamiento únicas del usuario, como huellas dactilares, reconocimiento facial, escaneo de iris o voz, para verificar la identidad.
c) Tokens de seguridad: Dispositivos físicos o aplicaciones móviles que generan códigos temporales únicos para autenticar al usuario.
d) Autenticación basada en contexto: Analiza el contexto en el que el usuario intenta acceder, como la ubicación, la red o el dispositivo que utiliza, para determinar la legitimidad de la solicitud de acceso.
e) Contraseñas de un solo uso (OTP): Son contraseñas que solo se pueden usar una vez y se generan para cada inicio de sesión.

La adopción de estas nuevas tecnologías recién enunciadas está transformando el panorama de la seguridad digital ya que todos estos métodos se consideran más confiables y convenientes para los usuarios, sobre todo porque reducen la dependencia de las contraseñas.

La idea detrás de estas soluciones es mejorar la seguridad al reducir las vulnerabilidades asociadas con las contraseñas tradicionales, especialmente

como dijimos, las contraseñas débiles o reutilizadas que pueden ser fácilmente copiadas por repetición.

Estas alternativas buscan ofrecer una experiencia de usuario más fluida y conveniente, porque eliminan la necesidad de recordar y gestionar múltiples contraseñas, generalmente anotándolas en papel ya que la cantidad de sitios y sus diversas formas de solicitarlas hace imposible memorizarlas. Otras tantas veces nos vemos obligados a guardarlas en un llavero digital en las computadoras y teléfonos o en la memoria virtual de los aparatos, con el consiguiente riesgo de robo de estos y pérdida de dichos datos.

Sin embargo, es importante señalar que, aunque estas soluciones pueden mejorar la seguridad en línea, también pueden tener sus propias limitaciones y desafíos. Por ejemplo, los sistemas biométricos pueden enfrentar problemas de privacidad y falsificación, mientras que los métodos de autenticación basados en dispositivos pueden presentar los mismos riesgos de las contraseñas tradiciones si no se cuenta con el aparato, o también si se pierde o es robado.

Por lo tanto, la transición hacia el "fin de las contraseñas" debe abordarse de manera cuidadosa y considerada, teniendo en cuenta tanto la seguridad como la comodidad del usuario por los desafíos legales que enfrenta.

2.3. Acceso equitativo y discapacidad

Si bien la eliminación de las contraseñas puede aumentar la seguridad, también puede presentar desafíos para las personas con discapacidades (especialmente no videntes, motrices o auditivos) ya que -hasta ahora- no están pensados para ellos. Es importante que las nuevas soluciones sean accesibles para todos, cumpliendo con los principios de igualdad y no discriminación. Las regulaciones deben garantizar que ningún grupo se vea excluido o desfavorecido por los nuevos métodos de autenticación.

3. El uso de *cookies*

3.1 Robo de datos biométricos o información de contexto

Otro aspecto importante por considerar en esta disertación es el que se produce a través del uso de *cookies* distinguiéndolo del robo de datos mediante *"phishing"* (simulando ser una entidad de confianza mediante una comunicación electrónica), *"vishing"* (aparentando representar bancos o compañías en las que se contrató un servicio) o *"smishing"* (vía *SMS* -siglas en ingles de Servicio de mensajes cortos-).

En este sentido, las *cookies* son pequeños archivos de texto almacenados en los dispositivos de los usuarios cuando acceden a sitios *web*. Estas herramientas tecnológicas permiten a los sitios recopilar y almacenar información sobre la actividad en línea de los usuarios, como preferencias, historiales de navegación y detalles de inicio de sesión. Las *cookies* pueden ser de diferentes tipos, como *cookies* de sesión y *cookies* persistentes, cada una con diferentes duraciones y propósitos.

3.2 Marco legal y regulatorio

El uso de *cookies* en línea está sujeto en muchas jurisdicciones a un marco legal y regulatorio que busca proteger la privacidad y los datos de los usuarios. El Reglamento General de Protección de Datos *(GDPR)* en la Unión Europea y leyes similares en otras regiones imponen requisitos estrictos para obtener el consentimiento informado y claro de los usuarios antes de recopilar y utilizar sus datos personales a través de *cookies*. Además, exigen que las organizaciones proporcionen a los usuarios opciones claras para administrar y eliminar *cookies*.

Pero tanto la selección rápida del tipo de *cookies* que vamos a permitir como el. consentimiento informado y la transparencia no están garantizados por si solos con el "acepto" mediante la tecla "*enter*" o el "*double-click*", que ya han demostrado ser insuficientes.

3.3. Consentimiento Informado y transparencia

Uno de los aspectos más cruciales en el uso de *cookies* es obtener un consentimiento informado de los usuarios. Las organizaciones deben ser transparentes sobre qué datos se recopilan, cómo se utilizarán y con quién se compartirán.

El consentimiento debe ser específico y basarse en una comprensión clara por parte de los usuarios. Cualquier cambio en la política de *cookies* debe ser comunicado de manera efectiva, brindando a los usuarios la opción de aceptar o rechazar las nuevas condiciones.

Por eso, como expondremos a continuación, se plantean nuevos desafíos legales cruciales, en la transición hacia el fin de las contraseñas.

3.4 Derechos del usuario

Una de las principales cuestiones de la regulación es que debe garantizar que las nuevas tecnologías de autenticación respeten los derechos de privacidad

y protección de datos de los usuarios.

El uso indebido de *cookies* puede infringir los derechos de privacidad de los usuarios. La información recopilada puede ser utilizada para perfiles detallados de usuarios, lo que plantea preocupaciones sobre el seguimiento excesivo y la toma de decisiones automatizadas.

Los usuarios tienen el derecho de acceder a los datos recopilados a través de *cookies* y de solicitar su eliminación si así lo desean.

3.5 Consideraciones éticas

Si bien el cumplimiento legal es esencial, también es fundamental abordar las consideraciones éticas relacionadas con las *cookies*.

Las organizaciones deben garantizar que el uso de *cookies* no comprometa la privacidad de los usuarios ni perpetúe la discriminación o la exclusión. La recopilación de datos debe tener un propósito legítimo y beneficiar tanto a las organizaciones como a los usuarios.

4. Privacidad

4.1 Privacidad y protección de datos

La adopción de tecnologías de autenticación avanzadas también debe considerar las implicancias para la privacidad y la protección de datos.

La biometría y otros métodos planteados para el fin de las contraseñas recopilan información altamente sensible, lo que requiere una gestión cuidadosa y transparente de los datos personales por eso que la recopilación y el almacenamiento de los datos biométricos, por ejemplo, deben estar sujetos a regulaciones estrictas para evitar abusos y asegurar el consentimiento informado eficaz.

4.2 Contexto y fundamentos legales

Las leyes de protección de datos deben aplicarse de manera rigurosa para garantizar la seguridad jurídica. Son un derecho fundamental consagrado en numerosas legislaciones y tratados internacionales.

La ya mencionada Declaración Universal de Derechos Humanos y el Reglamento General de Protección de Datos (*GDPR*) de la Unión Europea y las próximas leyes a entrar en vigor de Servicios digitales y de Mercados digitales del mismo organismo geopolítico, son ejemplos de instrumentos legales que

subrayan la importancia de garantizar la privacidad de los individuos en el procesamiento de sus datos personales.

4.3. Principios fundamentales de la protección de datos

Los principios rectores de la protección de datos, como el consentimiento informado, la finalidad específica y la minimización de datos, son la base para el tratamiento adecuado de la información personal para evitar el uso indebido.

La proliferación de las redes sociales, el internet de las cosas y la analítica de datos plantean desafíos únicos en términos de protección de la privacidad. La recopilación masiva de datos y el perfilado de usuarios presentan riesgos significativos si no se gestionan de manera adecuada.

En un mundo globalizado, la transferencia de datos a través de fronteras presenta desafíos adicionales. Por eso la extraterritorialidad de regulaciones como el *GDPR* y las cláusulas contractuales de protección de datos son instrumentos esenciales para proteger los datos personales contra amenazas cibernéticas. La respuesta legal ante tales incidentes debe ser ágil y eficaz y especialmente rápida para evitar que sigan produciéndose los robos y filtraciones.

5. Conclusión

En esta exposición, hemos explorado el desafiante tema del fin de las contraseñas en los entornos digitales. A medida que adoptamos tecnologías de autenticación más seguras y convenientes, es esencial que las consideraciones legales y de seguridad jurídica guíen nuestra transición.

La colaboración entre juristas y profesionales de la tecnología será fundamental para abordar estos desafíos en constante evolución y será crucial para garantizar un equilibrio adecuado entre la innovación y la protección de los derechos de los usuarios. Es imperativo que las organizaciones comprendan y cumplan con los requisitos legales para proteger la privacidad de los usuarios y garantizar un uso responsable de los datos en un marco de consideraciones éticas que guíen el uso de *cookies* para garantizar que la tecnología beneficie a la sociedad en su conjunto.

Por eso celebramos esta convocatoria de la universidad organizadora con la presencia de grandes juristas de todo el mundo.

Muchas gracias por su atención.