Por:
Álvaro Gastañaduí

# *PATRONES OSCUROS, DATOS PERSONALES Y SOMBRAS LEGALES: ENTENDIENDO A LOS PATRONES OSCUROS DESDE LA NORMATIVA PERUANA SOBRE PROTECCIÓN DE DATOS PERSONALES*

**Autor**

Es Bachiller (2021) y Abogado (2023) en Derecho por la Universidad de Piura. Fue miembro del equipo finalista y mejor orador del "E-Moot de Libre Competencia 2020" y miembro del equipo finalista del "MootComp 2020". Su idioma nativo es el español y habla fluido inglés e italiano. Actualmente labora como asociado en el área regulatoria de "Miranda & Amado Abogados"

**Resumen**

Los "patrones oscuros" pueden definirse como los mecanismos implementados en entornos digitales a efectos de influir, e inclusive manipular, las decisiones de los usuarios de un sitio web o de un aplicativo. Estas decisiones pueden estar orientadas a los datos personales, de modo que los patrones oscuros apuntarían, entre otros objetivos, a que los usuarios entreguen datos personales o autoricen finalidades que, en otro contexto, no hubieran entregado o autorizado. Con base en ello, el presente artículo analiza, en primer lugar, la definición y clasificación de los patrones oscuros en el marco de la protección de los datos personales. En segundo lugar, cómo esta problemática ha sido abordada en otras jurisdicciones; para, posteriormente, determinar cuál es el tratamiento que recibiría en el ordenamiento jurídico peruano.

**Palabras clave**

datos personales, patrones oscuros, consentimiento, privacidad en línea, internet, manipulación, sesgos conductuales, aplicaciones, sitios web, normativa sobre protección de datos personales.

**Abstract**

"Dark patterns" can be defined as the mechanisms implemented in digital environments in order to influence, and even manipulate, the decisions of the users of a website or an application. These decisions may be oriented towards personal data, so that dark patterns would aim, among other objectives, at users to provide personal data or authorize purposes that, in another context, they would not have provided or authorized. Based on this, this article analyzes, first of all, the definition and classification of dark

patterns within the framework of the protection of personal data. Secondly, how this problem has been addressed in other jurisdictions; to subsequently determine what treatment it would receive in the Peruvian legal system.

**Key words**

personal data, dark patterns, consent, online privacy, internet, manipulation, behavioral biases, applications, websites, regulations on the protection of personal data.

**Sumario**



## I. INTRODUCCIÓN

El aumento significativo del uso de internet es indiscutible[151]. Un número creciente de personas interactúa con diversas plataformas digitales como sitios web y aplicativos diariamente. Las razones son diversas: obtener información, adquirir un producto, contratar un servicio, ser parte de una red social, acceder a un juego, entre otros. Esto no ha sido ignorado por las empresas; las cuales, considerando que los datos personales de sus usuarios son un activo estratégico y de sumo valor para su modelo de negocio[152],

[151] De acuerdo con el Servicio Nacional del Consumidor de Chile, ello se debería "*a las facilidades de acceso, la masificación del comercio electrónico, el uso de dispositivos móviles y redes sociales*". Servicio Nacional del Consumidor de Chile, *Consentimiento en el Uso de Cookies: Evidencia Experimental sobre el Impacto de la Privacidad por Defecto y los Patrones Oscuros en las Decisiones de los Consumidores* (Santiago de Chile, marzo de 2022), 5.

[152] ISACA, Eliminating Deceptive Privacy Practices: Building Trust by Addressing Privacy Dark Patterns (2023), 5, https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/eliminating-deceptive-privacy-practices_0823.pdf.

despliegan diversos mecanismos con el propósito de obtener estos de sus titulares (vía *cookies*, *web beacons*, formularios de captación de datos, entre otros).

La información derivada de los datos personales puede, a modo de ejemplo, develar hábitos de compra de los clientes. Con ello, las empresas podrían identificar patrones que les permitan potenciar sus estrategias de marketing, generando así un impulso en sus ventas y sus ingresos[153]. Por ello, se debe ser consciente de que algunos (por no decir muchos) de los servicios "gratuitos" en términos monetarios que se encuentran en internet se pagan con los datos personales que uno termina compartiendo[154]. Dicho de otro modo, los consumidores (en particular, sus datos) terminan siendo el producto antes que los clientes.

Este interés en los datos personales ha causado que, con cada vez más frecuencia, se implementen diseños en los entornos digitales que busquen "optimizar" la obtención de estos. Se han desarrollado mecanismos para la captación de datos personales conocidos como "patrones oscuros". Estos mecanismos se apalancan en el diseño de experiencia de usuario (UX), el cual se centra en la experiencia que se desea lograr que sienta el usuario en la plataforma; así como en el diseño de interfaz de usuario (UI), el cual se ocupa de lo que se despliega e interactúa con el usuario.

Como se explicará en el presente artículo, un patrón oscuro es una estrategia digital desplegada en una plataforma con el objeto de que el usuario realice (o no realice) una acción que, en realidad, no quisiera realizar (o, de ser el caso, que sí quisiera realizar). Con la finalidad de que los usuarios se alejen de la estricta racionalidad al momento de tomar decisiones, los patrones oscuros apuntan principalmente a explotar los sesgos cognitivos de estos; es decir, aquellas desviaciones de la racionalidad basadas en creencias y preferencias (por ejemplo, el que las personas suelen seguir las actitudes de la mayoría, o que prefieran un placer inmediato pese al costo a mediano plazo que este generaría).

Aplicado a los datos personales, los patrones oscuros se implementan con la finalidad de que el usuario entregue más datos de los que en realidad estaría dispuesto a entregar, acepte finalidades que en otras circunstancias no hubiese aceptado, o se le dificulte el ejercicio de sus derechos.

A su vez, es importante comprender la actitud de los usuarios frente a estas campañas de recolección de datos personales; concretamente, qué es la "paradoja de la privacidad". En numerosos estudios los usuarios de plataformas digitales han expresado su preocupación por la privacidad de sus datos; sin embargo, su conducta termina ignorando –y hasta contrariando– dicha preocupación (por ejemplo, a través de la publicación de imágenes

153 Ibíd.

154 Jarovsky, Luiza. "How Cognitive Biases Make You Vulnerable to Dark Patterns". LinkedIn, 19 de mayo de 2022. https://www.linkedin.com/pulse/how-cognitive-biases-make-you-vulnerable-dark-luiza-jarovsky/

o de un recuento de sus actividades en redes sociales)[155]. Esta "paradoja de la privacidad" también se ha confirmado de manera empírica: en diversos entornos de laboratorio las personas que expresan gran preocupación por su privacidad suelen revelar detalles íntimos de sus vidas a cambio de recompensas triviales[156].

En vista de lo anterior, resulta claro que "*los consumidores cada vez están más expuestos a entregar información de manera consciente o inconsciente en el mundo digital, sin necesariamente saber cómo y en qué medida sus datos personales son recopilados, almacenados y tratados*"[157]. Ello, más aún, frente al riesgo de los "patrones oscuros".

Evidenciado el problema que suscitan los patrones oscuros, en el presente artículo se analizará, *de un lado*, la dimensión práctica de estos; se abordará su definición, clasificación y los problemas que acarrean. *Del otro*, y con base en lo anterior, se explorará el tratamiento que han recibido en otros países para, posteriormente, evaluar qué tratamiento recibirían en el marco del ordenamiento jurídico peruano.

## II. ENTENDIENDO A LOS "PATRONES OSCUROS"

Para una comprensión más profunda de los patrones oscuros, especialmente en el marco de la protección de datos personales, es importante explorar su relación con la Experiencia del Usuario (UX) y el Diseño de Interfaz de Usuario (UI) en las plataformas digitales. Además, es esencial examinar cómo estos patrones interactúan con los individuos y sus sesgos cognitivos.

En este complejo entramado de elementos, emerge el fenómeno conocido como patrones oscuros. Estos, de manera resumida y conforme se ahondará más adelante, representan estrategias que son desplegadas en los sitios web o aplicativos para que los usuarios tomen decisiones sub-óptimas en lo referido a la protección de sus datos personales (al entregar más datos de los requeridos, aceptar finalidades no esenciales, entre otros).

### A. SESGOS COGNITIVOS, UX, UI Y PLATAFORMAS DIGITALES

A lo largo del día, las personas se enfrentan a innumerables decisiones. Muchas veces se asume que estas decisiones surgen de un análisis estrictamente objetivo y racional. Sin embargo, junto con dicha racionalidad (así como otras variables) están siempre

---

155 Leslie K. John, "We Say We Want Privacy Online, But Our Actions Say Otherwise", Harvard Business Review, 16 de octubre de 2015, https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise.

156 Ibíd.

157 Servicio Nacional del Consumidor de Chile, *Consentimiento en el Uso de Cookies: Evidencia Experimental sobre el Impacto de la Privacidad por Defecto y los Patrones Oscuros en las Decisiones de los Consumidores*, 5.

presentes, en todos los ámbitos de elección, los **sesgos cognitivos**. Un **sesgo cognitivo** es "*una desviación sistemática, involuntaria e inconsciente de una norma o de un estándar de racionalidad al emitir un juicio perceptual o conceptual, al recordar un evento o al hacer una predicción. No se trata de un simple error, sino de comportamientos que ocurren consistentemente bajo circunstancias similares, y que por lo tanto son predecibles y replicables*"[158]. Es así como, de una manera inconsciente la mayoría de las veces, se terminan tomando decisiones desviadas de la objetividad y racionalidad e inspiradas, en cambio, en factores psicológicos, sociales o emocionales que afectan la percepción, la memoria y el razonamiento.

Estos sesgos, estudiados por el marketing, son aprovechados para diseñar anuncios o campañas publicitarias, acomodar puntos de venta, definir la oferta de un producto y sus presentaciones, entre otros. Sin embargo, la influencia de estos sesgos no se limita solo al ámbito del marketing; se extiende al diseño de experiencias digitales. Al observar más de cerca el diseño de sitios web y aplicativos, se revela, incluso, cómo los sesgos cognitivos impactan directamente en las decisiones de privacidad de los usuarios.

Por ejemplo, y sin perder de vista la vasta cantidad de sesgos cognitivos que podrían mencionarse, se encuentra el **sesgo de escasez y aversión a la pérdida**, conocido como el *fear of missing out* (FOMO). Este sesgo se basa en que "*la frustración de perder algo suele ser más intensa que la felicidad de encontrarlo*"[159]. En el diseño de sitios web de comercio electrónico, este sesgo se emplea para crear estrategias que provoquen decisiones de compra precipitadas.

Otro ejemplo es el **sesgo de arrastre**, también llamado *bandwagon effect*, a partir del cual "*tendemos a apoyar lo que la mayoría de la gente que nos rodea piensa y hace*"[160]. Este sesgo se emplea en el diseño de redes sociales, donde la visibilidad de las actividades de otras personas influye en las decisiones de los usuarios: desde qué contenido consumir hasta qué productos comprar.

Para comprender cómo influyen los sesgos cognitivos en el diseño de un sitio web o un aplicativo es importante centrarnos en la UX y la UI. La UX consiste en cómo se siente y se percibe globalmente la interacción de una persona con un producto o servicio (en este

---

158 Andrés Paz, "Los sesgos cognitivos y la legitimidad racional de las decisiones judiciales (Cognitive Bias and the Rational Legitimacy of Judicial Decisions)", Razonamiento Jurídico y Ciencias Cognitivas, 2021, 3.

159 "Los 7 sesgos cognitivos en marketing que impulsarán tus conversiones", Rebold, 29 de noviembre de 2021, https://letsrebold.com/es/blog/sesgos-cognitivos-en-marketing/#:~:text=Un%20sesgo%20cognitivo%20ocurre%20cuando,vital%20en%20términos%20de%20marketing.

160 Carlos Traseira, "Sesgos cognitivos. Los más usados en marketing digital", LinkedIn, 29 de noviembre de 2022, https://www.linkedin.com/pulse/sesgos-cognitivos-los-más-usados-en-marketing-digital-carlos-traseira/?originalSubdomain=es.

caso, digital), lo cual incluye aspectos emocionales, prácticos y estéticos. Por su parte, la UI se centra en los elementos visuales y de diseño que facilitan la interacción entre el usuario y el producto, como botones, íconos y diseños de pantalla. Así, la UX abarca la experiencia completa del usuario mientras que la UI se concentra en la presentación visual y la disposición de los elementos en esta.

Como se aprecia, tanto la UX y la UI resultan cruciales para el éxito de una plataforma digital, toda vez que su diseño depende de ambos conceptos. Por ello, para un mejor resultado, muchos sitios web y aplicativos son diseñados teniendo en cuenta los sesgos cognitivos antes indicados. Con ello, y dependiendo de los objetivos a los cuales atiendan las referidas plataformas (entre ellos, no solo vender productos sino también **captar datos personales**), se suelen desplegar interfaces que promueven que los usuarios tomen decisiones a partir de sus sesgos. Decisiones que, de otro modo, no tomarían. Muchos usuarios terminan adquiriendo productos que en realidad no necesitan, o terminan entregando sus datos y aceptando finalidades que, en otros contextos, no proporcionarían ni autorizarían. A este tipo de mecanismos se les conoce como patrones oscuros.

Estos patrones tienen en cuenta, además, la ya mencionada paradoja de la privacidad: pese a que los usuarios presentan una importante preocupación por su privacidad y el tratamiento de sus datos personales, tienen una tendencia a entregarlos o difundirlos con una facilidad que no conversa con la preocupación anterior. Es así como "*las personas suelen dar más peso a las consecuencias inmediatas de una decisión y a menospreciar aquellas que se materializarán en el futuro*"[161]; propiciando una entrega de datos personales a cambio de una recompensa muchas veces banal.

## B. DEFINICIÓN Y CLASIFICACIÓN DE LOS PATRONES OSCUROS

Antes de entrar a las complejidades legales de este fenómeno, es crucial entender su esencia e impacto en la toma de decisiones de los usuarios y la protección de datos personales. Definir a los patrones oscuros resulta, además, indispensable para un correcto análisis y evaluación jurídica.

Santos y Rossi[162] explican la importancia de institucionalizar el uso de dicho término (especialmente, en el marco de resoluciones o sentencias). Ello permitiría, entre otras cosas, ***(i)*** promover la adopción de un lenguaje común que es necesario para detectar,

---

161 Servicio Nacional del Consumidor de Chile, *Consentimiento en el Uso de Cookies: Evidencia Experimental sobre el Impacto de la Privacidad por Defecto y los Patrones Oscuros en las Decisiones de los Consumidores*, 6.

162 Cristiana Santos y Arianna Rossi, "The emergence of dark patterns as a legal concept in case law", Internet Policy Review, 31 de julio de 2023, https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept.

prohibir y sancionar este fenómeno generalizado; ***(ii)*** fomentar un enfoque sistémico de los patrones oscuros, ayudando a evitar la fragmentación entre diferentes reguladores, así como conectar a académicos, profesionales y grupos de vigilancia que se enfocan en el análisis de los patrones oscuros; y ***(iii)*** funcionar como un elemento disuasorio para las empresas, de modo que estas puedan evaluar mejor los riesgos y la conformidad de sus diseños, mientras que los responsables de la formulación de políticas se pueden concientizar sobre la magnitud del uso de patrones oscuros e intensificar la aplicación de la normativa.

Siendo ello así, corresponde comprender con mayor detalle qué son los patrones oscuros; o, como ahora son catalogados por el *European Data Protection Board*, "patrones de diseño engañosos"[163].[164] Como punto de partida, y aplicando los conceptos antes explicados, estos mecanismos pueden entenderse como "trucos" de experiencia de usuario (UX) que los sitios web y las aplicaciones utilizan para desalentar ciertas acciones, oscurecer deliberadamente la información o engañar a los usuarios[165]. Partiendo de esta explicación, es posible analizar definiciones más complejas dadas por la experiencia internacional.

En España, la Agencia Española de Protección de Datos (la "AEPD") indica que dicho término (dark patterns) –en lo referido a los datos personales– "hace referencia interfaces e implementaciones de experiencia de usuario **destinadas** a influenciar en el comportamiento y las decisiones de las personas en su interacción con webs, apps y redes sociales, de forma que tomen **decisiones potencialmente perjudiciales** para la protección de sus datos personales" (énfasis añadido).[166] Profundizando en el tipo de decisión a la cual apuntan a generar los patrones oscuros, la Guía de Protección de Datos

---

163 De acuerdo con el *European Data Protection Board* el término en inglés "deceptive design pattern" resulta un término más inclusivo y descriptivo que "dark pattern". European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (2022), 8.

164 Ahondando en estos diferentes términos, Santos y Rossi indican que los "patrones oscuros" presentan diversas nomenclaturas; como, por ejemplo, diseños engañosos ("*deceptive design*"), patrones perjudiciales ("*damaging patterns*"), arquitectura de elección manipuladora en línea ("*manipulative online choice architecture*") o técnicas de influencia engañosa en línea ("*online misleading influencing techniques*"). Santos y Rossi, "The emergence of dark patterns as a legal concept in case law".

165 Traducción y adaptación de la siguiente cita: "*Dark patterns are essentially user experience (UX) tricks that websites and apps use to discourage certain actions, deliberately obscure information, or mislead users.*" Jeffrey Edwards, "What are Dark Patterns? How UI Influences Consent and Compliance", CHEQ, 23 de enero de 2023, https://cheq.ai/blog/what-are-dark-patterns/

166 "Dark patterns: Manipulación en los servicios de Internet", AEPD: Agencia Española de Protección de Datos, 19 de mayo de 2022, https://www.aepd.es/prensa-y-comunicacion/blog/dark-patterns-manipulacion-en-los-servicios-de-internet.

por Defecto emitida por la AEPD indica que este tipo de mecanismos buscan influir "**a través de manipulaciones psicológicas y de forma encubierta, en las elecciones del interesado**"[167] (énfasis añadido).

A nivel europeo, el European Data Protection Board ha definido a los "deceptive design patterns" como interfaces y trayectos de usuario (traducción literal de "users journey", el cual se refiere a la serie de acciones o pasos que los usuarios realizan para alcanzar sus objetivos en plataformas) implementados en plataformas que **buscan influenciar** a los usuarios para tomar decisiones **no deseadas, no consentidas y/o potencialmente perjudiciales**, a menudo a favor de una opción que va en contra de los mejores intereses de los usuarios y en beneficio de los intereses de las plataformas; en este caso, en lo que respecta a sus datos personales. Estos patrones buscan influir en el comportamiento de los usuarios, generalmente aprovechando los sesgos cognitivos. Asimismo, pueden obstaculizar su capacidad para proteger efectivamente sus datos personales y tomar decisiones conscientes, por ejemplo, al evitar que den un consentimiento informado y libre[168].

En el contexto latinoamericano, el Servicio Nacional del Consumidor de Chile (el "SERNAC") ha definido a estos como "opciones de diseño presentes en las interfaces de sitios web o aplicaciones que dificultan la decisión de los consumidores, obligando o guiando a los usuarios para que tomen **decisiones sub-óptimas para sus propios intereses**"[169] (énfasis añadido).

---

167 Agencia Española de Protección de Datos, Guía de Protección de Datos por Defecto (2020), 20.

168 Traducción y adaptación libre de la siguiente cita:

> "*In the context of these Guidelines, "deceptive design patterns" are considered interfaces and user journeys implemented on social media platforms that aim to influence users into making unintended, respectively unwilling, and/or potentially harmful decisions, often toward an option that is against the users' best interests and in favour of the social media platforms interest, with regard to their personal data. Deceptive design patterns aim to influence users' behaviours, generally relying on cognitive biases, and can hinder their ability "to effectively protect their personal data and make conscious choices"(...), for example by making them unable "to give an informed and freely given consent*".

European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 9.

169 Servicio Nacional del Consumidor de Chile, *Consentimiento en el Uso de Cookies: Evidencia Experimental sobre el Impacto de la Privacidad por Defecto y los Patrones Oscuros en las Decisiones de los Consumidores*, 19.

En el caso peruano, uno de los pocos acercamientos que han existido (a la fecha de redacción del presente artículo) es el efectuado por el Indecopi en el marco del Expediente No. 075-2022/CC3. En dicho expediente se emitió la Resolución No. 075-2022/CC3[170], en la cual se analizó si determinada conducta del titular de una plataforma de intermediación calificaba como una infracción a las normas de protección al consumidor. Dentro del referido análisis la Comisión de Protección al Consumidor No. 3 (la "CC3") señaló (a partir de la evaluación de su Secretaría Técnica) lo siguiente sobre los "patrones oscuros":

> "En el IFI la Secretaría Técnica consideró el empleo de "Patrones Oscuros" o "Dark patterns" a través de plataformas digitales que tomaron relevancia con el avance de la tecnología y la implementación de la economía colaborativa (…), creando un mercado abierto para el uso temporal de mercancías o servicios ofrecidos a menudo por los particulares (…). (…). Finalmente, consideró que, con la aparición de este modelo de negocio, ha aparecido también el neologismo "Patrones Oscuros" (Dark Patterns), (…), referido a todas aquellas estrategias o tácticas empleadas deliberadamente por los diseñadores web con el objetivo principal de engañar al usuario para que realice acciones indeseadas o que, de no haber mediado el patrón o haber tenido la información adecuada, no hubieran efectuado (…)"[171].

En línea con ello, añade la CC3, "los diseñadores utilizan su conocimiento sobre el comportamiento humano (por ejemplo, psicología) y los deseos de los usuarios finales para **implementar funciones engañosas que no son lo mejor para el usuario**"[172]. (Énfasis añadido). Complementando el análisis de la CC3, es importante notar que detrás de la aparente apariencia neutral de un servicio (en estos caos, una plataforma) puede haber elecciones y profesionales con conocimientos en la creación de interfaces efectivas para los negocios, pero al mismo tiempo dañinas para los intereses de los usuarios de las plataformas[173].

---

170 A la fecha de redacción del referido artículo, la Resolución No. 075-2022/CC3 fue impugnada; dicho recurso, a la presente fecha, no ha sido resuelto.

171 Expediente No. 075-2022/CC3, Comisión de Protección al Consumidor No. 3, 20 de junio de 2023, 043-2023/CC3 (Perú), 10.

172 Expediente No. 075-2022/CC3, Comisión de Protección al Consumidor No. 3, 20 de junio de 2023, 043-2023/CC3 (Perú), 10.

Dicha cita, además, fue extraída del siguiente documento: Colin M. Gray et al., "The Dark (Patterns) Side of UX Design", en *CHI '18: CHI Conference on Human Factors in Computing Systems* (New York, NY, USA: ACM, 2018), 2, https://doi.org/10.1145/3173574.3174108.

173 Luiza Jarovsky, "Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness", *SSRN Electronic Journal*, 2022, 8, https://doi.org/10.2139/ssrn.4048582.

Como se aprecia, si bien existen diversas definiciones que pueden darse de los patrones oscuros, todas recogen en mayor o menor medida los mismos elementos: **(i)** un diseño web o de aplicativo, **(ii)** deliberadamente destinado, **(iii)** a generar un resultado sub-óptimo para el usuario del sitio web o del aplicativo, **(iv)** que, sin su implementación, no se habría alcanzado.

Ahondando en la intencionalidad sobre el resultado sub-óptimo, Jarovsky[174] precisa que, para ser considerado un patrón oscuro, el diseño debe ser **manipulador y malicioso**. Si el diseño fuese **manipulador pero no malicioso**, ello podría considerarse problemático desde el punto de vista moral, pero no bastaría para calificar al diseño como un patrón oscuro (puesto que el objetivo final y el resultado obtenido podrían ser beneficiosos para el usuario).

Esta autora, además, parte de un criterio objetivo de responsabilidad; de modo que, cualquier diseño que perjudique al individuo debería calificar como malicioso, incluso si esa no fue la intención del diseñador detrás de ello. Ello, por cuanto los diseñadores tienen acceso a una serie de herramientas y técnicas para afectar sistemáticamente el comportamiento del usuario, incluida la explotación de sesgos que podrían actuar en contra de los usuarios de manera inconsciente[175]. Sin embargo, la valoración legal de la intencionalidad del diseñador y el titular de la plataforma dependerá de cada ordenamiento jurídico y del criterio (objetivo o subjetivo) que se emplee.

Ahora bien, entendiendo que un patrón oscuro constituye un diseño web o de aplicativo deliberadamente destinado a generar un resultado sub-óptimo para el usuario del sitio web o del aplicativo (a efectos del presente análisis, en lo referido a la protección de sus datos personales), que sin su implementación no se habría alcanzado, se debe analizar su clasificación.

No existe una propuesta taxonómica definitiva para los patrones oscuros; existen diversas clasificaciones que dependen del criterio que se emplee. A modo de ejemplo, podrían clasificarse de acuerdo con el momento en el cual se le presentan al usuario. Así, siguiendo a la AEPD, los patrones oscuros podrían presentarse en etapas diversas tales como "durante el proceso de registro o alta en una red social, al iniciar sesión o también en otros escenarios como en la configuración de las opciones de privacidad, en los banners de cookies, durante el proceso de ejercicio de derechos, en el contenido de una comunicación informando sobre una brecha de datos personales o incluso al intentar darse de baja de la plataforma"[176].

---

174 Jarovsky, "Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness", 6.

175 Jarovsky, "Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness", 7.

176 "Dark patterns: Manipulación en los servicios de Internet".

En el presente artículo (enfocado en la protección de los datos personales) la clasificación se centrará en aquella propuesta por el European Data Protection Board, empleando como criterio cómo interactúa el usuario con el patrón, así como el impacto en los primeros. No obstante, será importante tener en cuenta que existen diversas (aunque muchas veces similares) formas de clasificarlos.

Siendo ello así, es posible identificar los siguientes patrones[177]:

(i) **Patrones de sobrecarga ("overloading")**: este tipo de patrones consisten en generar que los usuarios se enfrenten a una vasta cantidad de solicitudes, información, opciones o posibilidades con la finalidad de causarles fatiga y cansancio. Con ello, se busca inducirlos a compartir más datos de los que en otras condiciones compartirían o a que permitan el procesamiento de sus datos personales en contra de sus expectativas.

Dentro de este tipo de patrones se encuentran las siguientes modalidades:

- Solicitud continua ("continuous prompting"): se insta a los usuarios a proporcionar más datos personales de los que resultan necesarios o a aceptar otras finalidades al solicitarles repetidamente ello; estas solicitudes repetitivas pueden darse a través de uno o varios dispositivos. El resultado es que el usuario termine cediendo al estar cansado de rechazar en cada oportunidad estas solicitudes (lo cual interrumpiría su experiencia en la plataforma).

- Laberinto de privacidad ("privacy maze"): se hace que los usuarios tengan que navegar por demasiadas páginas para obtener información sobre cómo sus datos son procesados o para ejercer sus derechos. Ello puede terminar generando que el usuario decida ignorar dicha información o renuncie al control sobre sus datos personales.

- Muchas opciones ("too many options"): se le ofrece al usuario una importante cantidad de opciones, lo cual puede generar que no tomen algunas decisiones o decidan ignorar (la existencia o inexistencia de) ciertas configuraciones que se relacionan con el cómo se procesan sus datos personales.

---

177 El detalle de cada tipo de patrón ha sido elaborado a partir de los siguientes documentos:

(i) European Data Protection Board, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, 3-4. (En particular, la explicación de cada modalidad se centra en gran medida en la traducción y adaptación de este documento).

(ii) "Dark patterns: Manipulación en los servicios de Internet".

(ii) **Patrones de omisión ("skipping")**: implican un diseño de interfaz o del trayecto del usuario de manera que pierdan de vista o no puedan ser conscientes de todos o algunos de los aspectos que involucra la protección de sus datos personales.

Dentro de este tipo de patrones se encuentran las siguientes modalidades:

- Comodidad engañosa ("deceptive snugness"): este patrón implica que las características y opciones más invasivas para los datos personales del usuario se encuentren habilitadas por defecto. Ello trae consigo que muchos usuarios no cambien dichas preferencias, incluso teniendo la posibilidad de hacerlo.

- Mirar para otro lado ("look over there"): este patrón consiste en colocar una acción o información no necesariamente relacionada con la protección de datos personales en contraposición con alguna que sí está relacionada con ello. A través de ello, se busca que los usuarios elijan la opción distractora y olviden la otra.

(iii) **Patrones de incitación ("stirring")**: estos patrones afectan la elección que los usuarios hacen al apelar a sus emociones o utilizar indicadores visuales (a través de efectos que se despliegan en la plataforma).

Dentro de este tipo de patrones se encuentran las siguientes modalidades:

- Orientación emocional ("emotional steering"): mediante esta modalidad se utilizan expresiones o elementos visuales (como estilo, colores, imágenes u otros) con la finalidad de que la información se les presente a los usuarios sea de manera muy positiva (haciéndolos sentir bien, seguros o recompensados) o de manera muy negativa (haciéndolos sentir asustados, culpables o castigados). Influenciar el estado emocional de los usuarios de esta manera probablemente los llevará a realizar una acción que va en contra de la protección de sus datos personales.

- Oculto a primera vista ("hidden in plain sight"): mediante esta modalidad se emplea un estilo visual para la información o para los controles de los datos del usuario de forma tal que se le induzca a optar por opciones menos restrictivas y, por lo tanto, más invasivas.

(iv) **Patrones de obstrucción ("obstructing")**: dificultan o bloquean a los usuarios en sus procesos de informarse o de gestionar sus datos al hacer que la acción sea difícil o imposible de conseguir.

Dentro de este tipo de patrones se encuentran las siguientes modalidades:

- Callejón sin salida ("dead end"): este tipo de patrón consiste en no habilitar enlaces o, habiéndolos habilitados, que estos no funcionen, a efectos de no permitirles a los usuarios obtener información o controlar cómo se procesan sus datos personales.
- Más largo de lo necesario ("longer than necessary"): este tipo de patrón consiste en estructurar la experiencia del usuario en la plataforma de manera que la activación de opciones más invasivas requiera de menos pasos que aquellos necesarios para la activación de opciones menos invasivas.
- Acción engañosa ("misleading action"): este tipo de patrón consiste en presentar una discrepancia entre la información y las acciones disponibles para los usuarios, de manera que se vean inducidos a hacer algo que no pretenden. La diferencia entre lo que los usuarios esperan y lo que obtienen probablemente los desanime a continuar.

(v) **Patrones de inconsistencia ("fickle")**: consisten en un diseño de interfaz inconsistente y poco claro, de modo que se le dificulte al usuario navegar entre las diferentes herramientas de control de protección de datos y comprender el propósito del procesamiento de sus datos.

Dentro de este tipo de patrones se encuentran las siguientes modalidades:



- Falta de jerarquía ("lacking hierarchy"): a través de este diseño la información relacionada con la protección de datos carece de jerarquía, presentándose de diversas maneras y en múltiples ubicaciones. Esta redundancia puede desconcertar a los usuarios, dejándolos incapaces de comprender completamente cómo se procesan sus datos y cómo ejercer control sobre ellos.
- Descontextualización ("decontextualising"): a través de este diseño la información o el control de protección de datos se ubican en una página cuyo contexto no responde a esta temática. Los usuarios tienen pocas probabilidades de encontrar la información o el control, ya que no resulta intuitivo buscarlos en esa página específica.
- Interfaz inconsistente ("inconsistent interface"): a través de este diseño la interfaz de la plataforma no mantiene coherencia entre diferentes contextos (por ejemplo, un menú relacionado con la protección de datos que muestra elementos diferentes en dispositivos móviles y de escritorio) o con las expectativas de los usuarios (por ejemplo, una opción cuya ubicación ha sido intercambiada con la de otra). Estas diferencias pueden llevar a los usuarios a no encontrar la información deseada o los controles sobre sus datos; o, inclusive, a interactuar con elementos de la interfaz de manera automática, aunque esto conduzca a tomar decisiones de protección de datos no deseadas.

- Discontinuidad en el lenguaje ("language discontinuity"): a través de este diseño la información relacionada con la protección de datos no se proporciona en el o los idiomas oficiales del país donde residen los usuarios, a pesar de que el servicio sí lo está. Si los usuarios no dominan el idioma en el que se presenta la información sobre cómo se procesan sus datos, es probable que no puedan leerla fácilmente y, por lo tanto, no lleguen a conocer esto.

(vi) **Patrones de oscurecimiento ("left in dark")**: implica que una interfaz esté diseñada de manera que oculte información (a través, por ejemplo, de un lenguaje poco claro) o las herramientas de control de los datos, o deje a los usuarios inseguros sobre cómo se procesan sus datos y qué tipo de control podrían tener sobre ellos en relación con el ejercicio de sus derechos.

Dentro de este tipo de patrones se encuentran las siguientes modalidades:

- Información conflictiva ("conflicting information"): esta modalidad implica proporcionar a los usuarios información que entra en conflicto con otra información ya entregada. Esto puede dejar a los usuarios inseguros sobre lo que deben hacer y las consecuencias de sus acciones, lo que probablemente los lleve a no tomar ninguna acción y mantener la configuración predeterminada.
- Redacción o información ambigua ("ambiguous wording or information"): esta modalidad implica emplear términos ambiguos y difusos al proporcionar información a los usuarios. Esto podría dejar a los usuarios inseguros sobre cómo se procesarán los datos o cómo ejercer control sobre sus datos personales.

Como se aprecia de lo anterior, existen diversos patrones oscuros que pueden menoscabar la protección de los datos personales de los usuarios de plataformas digitales. Es importante señalar que la clasificación anterior sirve para entender mejor a los patrones oscuros, pero no por ello cada patrón deberá encasillarse en una categoría de manera exclusiva. Podría ser el caso que existan patrones que califiquen como más de una de las modalidades presentadas; o que, inclusive, puedan exceder las categorías propuestas.

## C. PROBLEMÁTICA DE LOS PATRONES OSCUROS

Evidentemente, los patrones oscuros en el marco de las plataformas digitales constituyen un problema para los usuarios; ello, más aún, debido a los diversos ámbitos en los cuales estos pueden impactar. Es posible resaltar el riesgo que representan en materia de protección al consumidor y en materia de protección de datos personales.

En materia de protección al consumidor (y únicamente a modo de referencia), el riesgo radica en que estos lleven a un menoscabo de los derechos de los consumidores finales que interactúan con sitios web o aplicativos: En el Perú, la CC3[178] clasificó a los patrones oscuros según sus intenciones, diseño o efectos en las siguientes categorías: ***(i)*** asimetría, ***(ii)*** tendencia al engaño, ***(iii)*** encubrimiento, ***(iv)*** ocultaciones y ***(v)*** restricciones. Por ejemplo, los **patrones oscuros de asimetría** consistirían en "*presentar las opciones al usuario de forma desproporcionada o con un diseño totalmente desigual, siendo que, en estos, se busca conseguir los resultados deseados aplicándolos como la configuración por defecto, sabiendo que en muchos casos los usuarios no lo cambiarán por "comodidad" o en su defecto, se genera puntos llamativos en la página para distraer la atención de otros de igual relevancia*"[179].

Ahora, no solo los derechos de consumo de los usuarios se pueden ver afectados; sino que, además, sus datos personales podrían encontrarse en riesgo. Como se ha indicado, los patrones oscuros se apalancan en los sesgos cognitivos de los usuarios a efectos de que los titulares de los datos personales ***(i)*** entreguen más datos de los que en otros contextos entregarían; ***(ii)*** acepten finalidades que no conversan con sus expectativas; o, en general, ***(iii)*** no tengan (o tengan un menor) control sobre sus derechos relacionados a sus datos personales.

Estos patrones, como bien resalta el *European Data Protection Board*, plantean una problemática incluso mayor respecto de ciertas poblaciones (debido a su especial vulnerabilidad), tales como menores de edad o personas mayores. Por un lado, dentro de los menores de edad se pueden encontrar individuos que le den una importancia menor (incluso menor a la poca importancia que algunos mayores de edad ya le dan) a la protección de sus datos personales; o que sean más susceptibles ante ciertos patrones.

Respecto de los adultos mayores es posible identificar individuos con discapacidad visual o aquellos con una menor alfabetización digital; quienes, en virtud de dichas condiciones, enfrentan un desafío mayor frente a este tipo de patrones. En cualquier caso, los grupos vulnerables mencionados pueden tener dificultades para identificar prácticas de diseño manipuladoras, así como carecer de la plena conciencia de que su comportamiento digital está siendo influenciado por el titular de la plataforma[180].

También se resalta el potencial daño a los individuos de bajos recursos y de niveles educativos inferiores. Estos patrones pueden afectar de manera desproporcionada a aquellos con menor alfabetización tecnológica y a aquellos que, viviendo en determinado

---

178 Expediente No. 075-2022/CC3, Comisión de Protección al Consumidor No. 3, 20 de junio de 2023, 043-2023/CC3 (Perú), 10.

179 Ibíd.

180 European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 10.

país, no hablan el idioma de este como lengua materna. Ello, pese a que la brecha en la educación y habilidades técnicas no debería ser un obstáculo para el ejercicio efectivo de su privacidad[181].

Pese a su creciente prevalencia y el riesgo que estos traen consigo (tanto en materia de protección al consumidor como en materia de protección de datos personales), el ordenamiento jurídico peruano carece de un marco regulatorio específico que los aborde como tales. Esta carencia parece agregar una capa adicional de complejidad a su identificación y, de ser el caso, sanción. No obstante, y si bien la falta de un enfoque legal específico puede dejar a los usuarios en una situación de vulnerabilidad, ello no implica que los patrones oscuros no puedan ser investigados, calificados como un acto infractor y sancionados a partir del régimen general de protección de datos personales que actualmente existe.

Por ende, a continuación, se analizará cuál es el tratamiento que los patrones oscuros podrían recibir desde el marco legal peruano actual. Para ello, y como paso previo, se analizará cómo han sido abordados en otras jurisdicciones.

## III. TRATAMIENTO LEGAL DE LOS "PATRONES OSCURUS" EN EL MARCO DE LA PROTECCIÓN DE LOS DATOS PERSONALES

Los patrones oscuros representan una problemática que, con cada vez más frecuencia, están siendo abordados por los ordenamientos jurídicos. A continuación, se explicará brevemente cuál ha sido la experiencia de otros ordenamiento frente a dicha problemática; y, posteriormente, cuál sería el tratamiento que recibirían en el ordenamiento jurídico peruano.

### A. EXPERIENCIA INTERNACIONAL

La presente sección presenta una explicación general sobre cómo otros ordenamientos jurídicos han venido abordando la problemática descrita. Al respecto, es posible identificar jurisdicciones que han dado un primer paso en analizar la problemática, la experiencia y vulnerabilidad de sus propios ciudadanos frente a estos patrones; sin llegar, necesariamente, a emitir alguna norma al respecto. Junto con estas, se tiene a aquellas que sí han emitido disposiciones específicas que buscan prohibirlos (o, cuando menos regularlos). Finalmente, existen jurisdicciones en las cuales ya se han sancionado patrones oscuros calificando a estos como tales. A continuación, se presentan ejemplos de estos casos.

[181] ISACA, Eliminating Deceptive Privacy Practices: Building Trust by Addressing Privacy Dark Patterns, 6.

Como ejemplo de una jurisdicción en la cual se ha analizado de manera práctica dicho fenómeno se encuentra **Chile**. El SERNAC llevó a cabo un experimento sobre preferencias de configuración de *cookies*; este experimento devino en el Informe Técnico "Consentimiento en el uso de *cookies*: evidencia experimental sobre el impacto de la privacidad por defecto y los patrones oscuros en las decisiones de los consumidores". El experimento puso de manifiesto que el uso de patrones oscuros en el diseño aumenta significativamente el porcentaje de usuarios que aceptan *cookies* adicionales (lo cual implica un procesamiento de datos más invasivo). Una de las lecciones del Informe Técnico resalta, incluso, lo perjudicial de determinados patrones oscuros, toda vez que "*la arquitectura de decisión está diseñada para que los consumidores acepten cookies adicionales (opt-out) en circunstancias en que* ***su consentimiento libre e informado es improbable***"[182] (énfasis añadido).

Dentro de las jurisdicciones que han tomado un rol más activo en contra de estos se encuentra **California**, donde se ha prohibido el uso de los patrones oscuros para la obtención de consentimiento. La *California Privacy Rights Act*[183] ha dispuesto que el acuerdo obtenido a través de patrones oscuros no constituye consentimiento ("*agreement obtained through use of dark patterns does not constitute consent*"). Dicha norma, además, define a los patrones oscuros como una interfaz de usuario diseñada o manipulada con el efecto sustancial de subvertir o menoscabar la autonomía, la toma de decisiones o la capacidad de elección del usuario.

En la **Unión Europea**, por su parte, se encuentra la Digital Services Act. Esta norma "*contiene una obligación que equivale a una prohibición de utilizar los llamados patrones oscuros en las plataformas en línea*"[184]. Específicamente, dicha norma prohíbe que los prestadores de plataformas en línea diseñen, organicen y gestionen sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas[185]. En adición a esta norma, el *European*

---

182 Servicio Nacional del Consumidor de Chile, *Consentimiento en el Uso de Cookies: Evidencia Experimental sobre el Impacto de la Privacidad por Defecto y los Patrones Oscuros en las Decisiones de los Consumidores*, 52.

183 California. The California Privacy Rights Act.

184 Comisión Europea, "Ley de Servicios Digitales: Preguntas y respuestas", Shaping Europe's digital future | European Comission, 17 de enero de 2024, https://digital-strategy.ec.europa.eu/es/faqs/digital-services-act-questions-and-answers.

185 Unión Europea. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), aprobado el 19 de octubre de 2022, artículo 25.

*Data Protection Board* adoptó para consulta pública la siguiente Directriz: *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them* (Directrices sobre patrones oscuros (dark patterns) en interfaces de redes sociales, Cómo reconocerlos y evitarlos). Este documento define, ejemplifica y analiza los patrones oscuros en el marco de la normativa europea sobre protección de datos personales.

Finalmente, existen ordenamientos jurídicos que, a la fecha, ya han sancionado patrones oscuros considerándolos como tales, en tanto representaban una afectación a la normativa aplicable sobre protección de datos personales. Un ejemplo se encuentra en **España**, en donde se identificaron y sancionaron dichos patrones bajo el siguiente análisis:

> "*En el caso que nos ocupa, **el patrón oscuro de sobrecarga (overloading) y de ocultación (skipping)**, se observa cuando se accede al apartado "Lista de proveedores", una vez allí, el interesado se encuentra con una lista de unas 130 empresas (proveedores), de las cuales, más de la mitad tienen marcada por defecto la casilla de "aceptar tratamiento de datos por Interés legítimo", lo que obliga, en el caso de querer mostrar la oposición al tratamiento a marcar una a una a lo largo de toda la lista, sin que exista la opción de poder oponerse indicándolo una sola vez o un número de veces que resulte razonable y no genere fatiga en el afectado.*
>
> (...)
>
> *Los hechos expuestos anteriormente pueden ser constitutivos de una infracción a lo establecido en el artículo 5.1.a) del RGPD* [los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)], *con el alcance expresado en los Fundamentos de Derecho anteriores.*"[186]
>
> *Esta infracción puede ser sancionada con multa de 20.000.000 € como máximo* (...)."

De la misma manera, el *Garante per la Protezione dei Dati Personali* de **Italia** sancionó a una empresa por el uso de patrones oscuros en su plataforma digital (aparición de *banners*, aparición de botones que destacaban la opción del consentimiento, botones para rechazar consentimiento con diseños y apariencias secundarias en el sitio web, entre otros) a través de los cuales buscaba que los usuarios otorguen su consentimiento para finalidades de marketing. De esta decisión se debe resaltar que la autoridad basó su análisis en las Directrices del *European Data Protection Board*. Asimismo, se resaltó que la evaluación acerca de cómo se implementan las interfaces gráficas de usuario es independiente de la calificación formal (es decir, del nombre de "patrones oscuros") y es evaluable en términos concretos (al amparo de la normativa vigente, tal como el Reglamento General de Protección de Datos Personales) incluso antes de que el *European*

[186] Agencia Española de Protección de Datos Personales, Resolución del Procedimiento Sancionador del Expediente No. EXP202211953 (PS/00080/2023) (España), 22-23.

*Data Protection Board* formalizara el principio de patrones oscuros en sus Directrices[187]. Por ende, se consideró la existencia de una infracción contraria a, entre otros, el artículo 5.1(a) del Reglamento General de Protección de Datos Personales [los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»).

La revisión de cómo otras jurisdicciones abordan esta problemática evidencia un panorama de reciente crecimiento. Comprender las estrategias de otros lugares frente a los patrones oscuros brinda un marco esencial para evaluar el tratamiento que los patrones oscuros podrían recibir bajo el ordenamiento jurídico peruano. A continuación, se analizará cómo esta problemática es abordada a partir de las normas relevantes para ello.

## B. TRATAMIENTO DE LOS PATRONES OSCUROS EN EL ORDENAMIENTO JURÍDICO PERUANO

En el Perú, la protección de los datos personales se encuentra regulada, principalmente, por la Ley No. 29733, Ley de protección de datos personales (la "LPDP") y por el Decreto Supremo No. 003-2013-JUS, Reglamento de la LPDP (en adelante, el "RLPDP"). Con base en estas normas, y en el marco del análisis que se efectuará a continuación, es importante apreciar las siguientes definiciones:

(i) En primer lugar, por **datos personales** se debe entender a "(t)*oda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.*"[188] Ejemplos de datos personales son el nombre, la imagen, la voz, la edad, datos de salud, hábitos de consumo, entre otros. Cabe precisar que a la persona natural a quien correspondan determinados datos personales calificará como el **titular de los datos personales**[189].

(ii) Los datos personales pueden ser objeto de **tratamiento**, lo cual consiste en "(c)*ualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o*

187 Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A. - 23 febbraio 2023 [9870014], Garante per la Protezione dei Dati Personali, 23 de febrero de 2023, 9870014 (Italia).

188 Perú. Ley de Protección de Datos Personales, Ley 29733, artículo 2.4.

189 Ley de Protección de Datos Personales, artículo 2.16.

*cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales*"[190].
Por ejemplo, captar datos personales a través de un buzón de "Déjanos tus datos para recibir publicidad" en un sitio web, así como almacenar datos personales en una nube, califica como tratamiento de datos personales.

(iii) Del otro lado, se encuentran los **titulares de bancos de datos personales**. Es decir, cualquier "(p)*ersona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad*"[191]. El titular del banco de datos personales califica como el **responsable del tratamiento**[192] de los datos que se hayan recopilado.
Para entender mejor los conceptos anteriores se presenta el caso de una empresa A. Esta empresa se encarga de vender zapatillas a través de su sitio web. Para poder finalizar la compra y gestionar el despacho de las zapatillas los usuarios deben dejar su nombre completo, su dirección, un número de teléfono y un correo electrónico. El conjunto de datos de los clientes de la empresa A que ha recopilado y que almacena califica como un banco de datos personales de Clientes. Por consiguiente, la empresa A (quien decide cómo se procesan los datos personales de sus clientes) califica como la titular del banco de datos; y, a su vez, como la responsable del tratamiento.

A partir de las definiciones anteriores, es posible analizar el fenómeno de los patrones oscuros:

### *a) ¿Cuándo la LPDP y el RLPDP le es aplicable a las plataformas digitales tales como sitios web y aplicativos?*

La primera cuestión consiste en determinar si es que las plataformas digitales objeto de análisis deberían o no cumplir con la LPDP y el RLPDP. Puesto que, si no fuese así, no cabría considerar un análisis jurídico de estos patrones en el ordenamiento peruano.

Para responder a esta interrogante cabe analizar el artículo 3 de la LPDP. Este artículo dispone que la LPDP será de aplicación "*a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de*

190 Ley de Protección de Datos Personales, artículo 2.19.

191 Ley de Protección de Datos Personales, artículo 2.17.

192 Para un mayor detalle sobre este concepto, revisar la Opinión Consultiva No. 034-2021-JUS/DGTAIPD.

*administración privada, **cuyo tratamiento se realiza en el territorio nacional**"*[193] (énfasis añadido). El alcance territorial del artículo anterior (es decir, aquello que se entenderá como dentro del territorio nacional) es desarrollado por el artículo 5 del RLPDP[194]. Este artículo establece los siguientes supuestos de aplicación territorial:

- Cuando el tratamiento "(s)*ea efectuado en un establecimiento ubicado en territorio peruano correspondiente al titular del banco de datos personales o de quien resulte responsable del tratamiento*.
- (Cuando) (s)*ea efectuado por un encargado del tratamiento, con independencia de su ubicación, a nombre de un titular de banco de datos personales establecido en territorio peruano o de quien sea el responsable del tratamiento*.
- (Cuando) (e)*l titular del banco de datos personales o quien resulte responsable del tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana, por disposición contractual o del derecho internacional*.
- (Cuando) (e)*l titular del banco de datos personales o quien resulte responsable no esté establecido en territorio peruano, pero utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento*."



Como se desprende de lo anterior, será de aplicación la LPDP y al RLPDP al tratamiento de datos personales (incluso cuando se efectúe a través de una plataforma digital) siempre que se lleve a cabo en el territorio nacional por parte de un responsable de tratamiento establecido en el país. Por ejemplo, el caso de una empresa constituida en el Perú (VENTA DE ROPA SAC) que comercializa pantalones a través de un sitio web con despacho a todo Lima. Para poder concretar la venta, el usuario debe dejar sus datos personales. En este caso, VENTA DE ROPA SAC estaría obligada a cumplir con la LPDPD y el RLPDP.

En adición a ello, estas normas podrán aplicarse responsables de tratamiento no establecidos en el país, siempre que concurra alguno de los dos siguientes supuestos: *por un lado*, si es que la legislación peruana le es exigible a dicho responsable de tratamiento por disposición contractual, que sería el caso si es que dicho responsable se obliga en el marco de un contrato a cumplir con esta normativa. O, también, por aplicación del derecho internacional; es decir, cuando por aplicación de un tratado internacional el derecho peruano sea el derecho aplicable a dicho responsable de tratamiento.

193 Ley de Protección de Datos Personales, artículo 3.

194 Perú. Reglamento de la Ley de Protección de Datos Personales, Decreto Supremo 003-2013-JUS, artículo 5.

*Por otro lado*, este régimen también será de aplicación cuando el responsable del tratamiento utilice medios situados en el Perú. Para entender este escenario, resultan ejemplificativas las Resoluciones Directorales No. 975-2020-JUS/DGTAIPD-DPDP y No. 71-2020-JUS/DGTAIPD. De acuerdo con estas se debe entender por "medios situados en el territorio peruano" incluso a los equipos (dispositivos de escritorio o móviles) de los usuarios residentes en el Perú, en tanto sean "utilizados" por el responsable del tratamiento para almacenar información de forma local.

En ese sentido, y a criterio de la Autoridad Nacional de Protección de Datos Personales (la "ANPD"), los responsables de tratamiento no establecidos en el territorio peruano, pero cuyas plataformas se empleen también en el Perú (a través de redes de telecomunicaciones y dispositivos ubicados en este territorio) estarán obligadas a cumplir con la LPDP y el RLPDP.[195] Si bien el criterio de la ANPD puede ser discutible, principalmente en lo referido a sus alcances, no por ello se debe de perder de vista que constituye el criterio actual de la autoridad.

En conclusión, el análisis jurídico sobre los patrones oscuros que se realizará a continuación será de aplicación a los siguientes responsables de tratamiento (por cuanto se encuentran obligados a cumplir con la LPDP y el RLPDP): ***(i)*** responsables de tratamiento domiciliados en el país que llevan a cabo el tratamiento de los datos personales en el territorio nacional, ***(ii)*** responsables de

---

195 En adición a los escenarios expuestos, es importante considerar que el Proyecto del Nuevo Reglamento de Protección de Datos Personales, publicado mediante Resolución Ministerial No. 0270-2023/JUS, incluye dos nuevos supuestos que, de aprobarse, serían de relevancia para los responsables de tratamiento no domiciliados en el país. Estos escenarios son los siguientes:

> "*5.1 Las disposiciones de la Ley y del presente Reglamento son de aplicación al tratamiento de datos personales cuando:*
> (...)
> *4. El titular del banco de datos personales o quien resulte responsable del tratamiento no se encuentra en territorio peruano, pero realiza actividades relacionadas a la oferta de bienes o servicios dirigidos a los titulares de datos personales ubicados en territorio peruano.*
> *5. El titular del banco de datos personales o quien resulte responsable del tratamiento no se encuentra en territorio peruano, pero realiza actividades orientadas al análisis de comportamiento de los titulares de datos personales ubicados en territorio peruano, así como la elaboración de perfiles que busquen predeterminar conductas, preferencias, hábitos o similares.*
> (...)."

Ministerio de Justicia. *Proyecto de Nuevo Reglamento de la Ley No. 29733, Ley de Protección de Datos Personales*, publicado el 25 de agosto de 2023, artículo V.

tratamiento no domiciliados a quienes les es exigible la LPDP y la RLPDP en virtud de una disposición contractual o del derecho internacional, ***(iii)*** responsables de tratamiento no domiciliados cuyas plataformas son empleadas en el territorio nacional.

### *b) ¿Existe alguna regulación específica para los patrones oscuros? ¿Se encuentran expresamente prohibidos?*

No, el ordenamiento jurídico peruano no ha previsto, a la fecha de redacción del presente artículo, alguna regulación específica que aborde a los patrones oscuros como tales. Por ende, no existe ninguna prohibición ni regulación expresa de los patrones oscuros aplicados al tratamiento de datos personales.

Ello no significa, sin embargo, que no puedan ser analizados al amparo del estado actual de la LPDP y el RLPDP. Lo cierto es que, incluso cuando los patrones oscuros no han recibido algún tratamiento específico en el ordenamiento peruano, podrían de todas formas constituir un acto infractor cuando estos contravengan alguna de las disposiciones vigentes y exigibles a los responsables de tratamiento antes indicados.

Es más, si bien los patrones oscuros no han sido denominados como tales, existen disposiciones y lineamientos que prohíben (o, cuando menos, recomiendan evitar) el contenido material específico de algunos de estos:

- El artículo 18 de la LPDP dispone expresamente que las políticas de privacidad en línea deben ser fácilmente accesibles e identificables. Un patrón oscuro que pretenda restringir o impedir el acceso a esta estaría prohibido.

- El artículo 4 del RLPDP señala la obligación de comunicar determinada información al titular de los datos de manera clara y a través de un lenguaje sencillo. Un patrón oscuro que contravenga estas características estaría prohibido.

- La Guía Práctica para el Deber de Informar, emitida por la ANPD en el 2019, indica que, al momento de solicitar el consentimiento del titular de los datos, debe evitarse presentar casillas pre-marcadas[196].

- Este mismo documento recomienda evitar listas demasiados extensas de finalidades (por desalentar su lectura y resultar difícil de comprender), por lo que recomienda ajustar la extensión de estas explicaciones y agrupar las

[196] Autoridad Nacional de Protección de Datos Personales, Guía práctica para la observancia del "deber de informar" (Lima, 2019), 21.

finalidades por categorías. Asimismo, recomienda evitar términos o frases genéricas o inexactas que no expresen claramente las finalidades del tratamiento de los datos[197].

Como se aprecia de lo anterior, incluso cuando el marco normativo vigente no prevé un régimen específico que aborde a los patrones oscuros, sí existen disposiciones que prohíben o buscan evitar el uso de determinados patrones (sin llegar a catalogarlos así). Sin embargo, resulta importante hacer un análisis más comprensivo de los patrones oscuros (y no limitado a determinadas modalidades) al amparo de la LPDP y el RLPDP. Ello, para entender adecuadamente la legalidad de este fenómeno en su conjunto.

Para dicho análisis, se debe revisar, en primer lugar, el contenido de las principales obligaciones de los titulares de bancos de datos en materia de protección de datos personales, las cuales podrían entrar en conflicto con los patrones oscuros:

- Los titulares de bancos de datos personales están obligados a "*efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa*"[198]; salvo en los supuestos de excepción consignados en el artículo 14 de la LPDP[199]. Esta

197 Guía práctica para la observancia del "deber de informar" (Lima, 2019), 19.

198 Ley de Protección de Datos Personales, artículo 28.1.

199 LPDP

"***Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales***

*No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:*

*1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.*

*2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.*

*3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.*

*4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.*

*5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.*

*6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto*

obligación es consistente con el Principio de Consentimiento, de acuerdo con el cual, para el tratamiento de los datos personales, debe mediar el consentimiento libre, previo, expreso, informado e inequívoco de su titular[200].

A modo de ejemplo, en caso una empresa quisiese utilizar (dar tratamiento) el correo de un cliente (un dato personal) con el fin de remitirle publicidad, deberá, con anterioridad al envío del material publicitario, haber obtenido su consentimiento (un consentimiento libre, expreso, e informado).

A continuación, se detalla cada característica del consentimiento de acuerdo con el RLPDP:

- "*Libre: sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales (...). El condicionamiento de la prestación de un servicio, o la advertencia o amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no*

*profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.*

*7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.*

*8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.*

*9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.*

*10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.*

*11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.*

*12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.*

*13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley*".

Ley de Protección de Datos Personales, artículo 14.

200 Este principio está recogido en el artículo 5 de la LPDP y el artículo 7 del RLPDP.

*restringido, sí afecta la libertad de quien otorga consentimiento para el tratamiento de sus datos personales, si los datos solicitados no son indispensables para la prestación de los beneficios o servicios.*

- *Previo: con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.*
- *Expreso e Inequívoco: cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.* (...).
- *Informado: cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente: a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos. b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos. c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso. d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda. e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso. f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo. g. En su caso, la transferencia nacional e internacional de datos que se efectúen."*[201]

A efectos de cumplir con este "deber de informar", el artículo 18 de la LPDP señala que, si los datos son recogidos en línea, este se puede cumplir "*mediante la publicación de políticas de privacidad, **las que deben ser fácilmente accesibles e identificables***"[202] (énfasis añadido).

Como ha sido indicado, existen casos en los que no es necesario captar el consentimiento del titular de los datos personales (estos supuestos han sido previstos en el artículo 14 de la LPDP). Sin embargo, **la ANPD[203] considera que, aun así, se deberá cumplir con el mencionado deber de informar**; es decir, se deberá poner en conocimiento del titular de los datos toda aquella información que describa cómo serán tratados sus datos personales y cómo puede ejercer sus derechos.

---

201 Reglamento de la Ley de Protección de Datos Personales, artículo 12.1.

202 Ley de Protección de Datos Personales, artículo 18.

203 Para un mayor detalle, revisar la Opinión Consultiva No. 32-2020/JUS/DGTAIPD.

- Están obligados a "(n)*o recopilar datos personales por medios fraudulentos, desleales o ilícitos.*"[204] (esta obligación es consistente con el Principio de Legalidad, previsto en el artículo 4 de la LPDP). Sobre estas disposiciones, la ANPD ha considerado que estas "*establecen que la recopilación de datos personales no podrá realizarse por medios que sean contrarios a sus estipulaciones, así como al ordenamiento jurídico en general, ya sean normas legales o reglamentarias escritas, principios generales del derecho, y cualquier otra fuente normativa vigente en el Perú en el que se establezcan disposiciones especiales respecto del tratamiento de datos personales,* (...)"[205].

  Por consiguiente, señala Vásquez Rodríguez, se "*prohíbe particularmente la recopilación mediando la comisión de hechos ilícitos (penales o administrativos), así como aquel en el cual se enajena la voluntad del titular de los datos personales contrariando la buena fe, induciendo a error o engaño, lo cual constituye el tratamiento desleal y fraudulento*"[206].

- Están obligados a "(r)*ecopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades*[207] *determinadas, explícitas y lícitas para las que se hayan obtenido*"[208].
  Esta obligación se desprende de los Principios de Finalidad ("(l)*os datos personales deben ser recopilados para una finalidad determinada, explícita y lícita*"[209], de modo que el tratamiento no se extienda "*a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación*"[210]), de

---

204 Ley de Protección de Datos Personales, artículo 28.2.

205 Dirección de Protección de Datos Personales, 1 de marzo de 2022, Resolución Directoral No. 1022-2022-JUS/DGTAIPD-DPDP (Perú), 18. Esta resolución fue confirmada por la Resolución Directoral No. 82-2022-JUS/DGTAIPD.

206 Raúl Vásquez Rodríguez, "La protección de los datos personales en el sistema de reporte de créditos peruano", *Revista de Derecho YACHAQ*, n.º 10 (2019): 12.

207 De acuerdo con la Guía Práctica del del Deber de Informar, "(l)*a descripción de la o las finalidades responde a la pregunta ¿para qué serán tratados los datos personales recabados?, es decir, cuál o cuáles serán los usos específicos que se les darán a los datos personales obtenidos*". Guía práctica para la observancia del "deber de informar" (Lima, 2019), 19.

208 Ley de Protección de Datos Personales, artículo 28.3.

209 Ley de Protección de Datos Personales, artículo 6.

210 Ibíd.

Proporcionalidad ("(t)*odo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados*"[211]) y de Calidad ("(l)*os datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados*"[212]).

- Están obligados a "(a)*lmacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular*"[213]. Junto con esta obligación, el artículo 53 del RLPDP dispone que "(e)*l titular del banco de datos personales o responsable del tratamiento está obligado a establecer un procedimiento sencillo para el ejercicio de los derechos*"[214]. Esta obligación incluye los derechos de acceso, de rectificación, de cancelación o supresión, de oposición, de revocación del consentimiento, y de información.

Como se aprecia de lo anterior, la LPDP y el RLPDP han establecido un régimen de acuerdo con el cual, incluso cuando los patrones oscuros no se encuentran expresamente prohibidos, bien podrían constituir una contravención a sus disposiciones. Ello, sin embargo, dependerá de cada caso concreto.

### *c) ¿Qué disposiciones de la LPDP y el RLPDP podrían contravenir los patrones oscuros? ¿Son los patrones oscuros sancionables?*

De lo explicado, resulta claro que la implementación de patrones oscuros podría constituir una contravención a la LPDP y el RLPDP. No obstante, cada análisis dependerá del caso concreto; siendo que, si es que se quiere sancionar a algún administrado por el establecimiento de patrones oscuros, se deberá cumplir efectivamente con el Principio de Tipicidad.

El Principio de Tipicidad, aplicable a cualquier procedimiento administrativo sancionador, ha sido recogido en el artículo 248, numeral 4, del Texto Único Ordenado de la Ley del Procedimiento Administrativo General (Decreto Supremo No. 004-2019-JUS). De acuerdo con este, "(s)*olo constituyen conductas sancionables administrativamente las infracciones* ***previstas expresamente*** *en normas con rango de ley*

---

211 Ley de Protección de Datos Personales, artículo 7.

212 Ley de Protección de Datos Personales, artículo 8.

213 Ley de Protección de Datos Personales, artículo 28.5.

214 Reglamento de la Ley de Protección de Datos Personales, artículo 53.

*mediante su tipificación como tales, sin admitir interpretación extensiva o analogía*"[215] (énfasis añadido).

En aplicación de dicho principio, no se podrá sancionar la existencia de un patrón oscuro por su sola existencia (ni mucho menos por la calificación moral que se le pretenda dar). Dicha práctica podrá ser objeto de sanción, únicamente, si es que esta configura un tipo infractor expresamente tipificado por la normativa relevante. Considerando ello, a continuación, se presentará qué tipo de infracción[216] podría materializar, potencialmente, cada uno de los patrones oscuros descritos con anterioridad[217]:

| PATRONES DE SOBRECARGA ("OVERLOADING") | | |
|---|---|---|
| **Modalidad** | **Análisis** | **Posibles infracciones** |
| **Solicitud continua ("continuous prompting")** | De acuerdo con el funcionamiento de esta modalidad, se evidencian dos potenciales contravenciones a la LPDP y el RLPDP. En primer lugar, podría implicar recopilar más datos personales que aquellos necesarios para la finalidad dispuesta, o pretender justificar una extensión del tratamiento a una finalidad que no se encontraría | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción leve). |

215 Perú. Texto Único Ordenado de la Ley del Procedimiento Administrativo General, Decreto Supremo 004-2019-JUS, artículo 248.4.

216 Las infracciones han sido extraídas de la siguiente fuente: Reglamento de la Ley de Protección de Datos Personales, artículo 132.

217 Un análisis similar fue efectuado por el *European Data Protection Board* en el marco del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Dicho análisis puede encontrarse en European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them.

| | | |
|---|---|---|
| | inequívocamente establecida.<br><br>En segundo lugar, y toda vez que se estaría intentando forzar al titular de los datos personales a aceptar la entrega de sus datos o finalidades adicionales, se podría estar ante un supuesto en el que el consentimiento de este no calificaría como libre (al haber mediado, por ejemplo, la mala fe del responsable del tratamiento). | 2. Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción grave).<br><br>3. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave). |
| **Laberinto de privacidad ("privacy maze")** | Este patrón, dependiendo de su modalidad, puede impedir (o, cuando menos, limitar) que el titular de los datos acceda a la información sobre cómo sus datos son procesados. Dicha información, cabe reiterar, se debe entregar incluso cuando se está ante un supuesto de excepción al consentimiento.<br><br>Asimismo, podría evitar (o, cuando menos obstaculizar) que el | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos |

| | | |
|---|---|---|
| | titular de los datos ejerza sus derechos. | personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |

| | | |
|---|---|---|
| **Muchas opciones ("too many options")** | Al ofrecerle al titular de los datos una importante cantidad de opciones, de modo que este no tome en cuenta algunas decisiones o decida ignorar ciertas configuraciones que se relacionan con el cómo se procesan sus datos personales, el consentimiento de este se podría ver afectado.<br><br>Dependiendo de cada caso, se podría terminar obteniendo un consentimiento que, en realidad, no es libre y/o no es informado.<br><br>A su vez, si es que este exceso de opciones se presenta con el objeto de que el titular de los datos ejerza sus derechos, se podría estar ante un caso de obstaculización del ejercicio de estos. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |
| **PATRONES DE OMISIÓN ("SKIPPING")** | | |
| **Modalidad** | **Análisis** | **Posibles infracciones** |

| | | |
|---|---|---|
| **Comodidad engañosa ("deceptive snugness")** | Sobre esta modalidad, la Guía Práctica para el Deber de Informar emitida por la ANPD es clara en indicar que "(e)*n la acción de solicitar el consentimiento debe evitarse presentar casillas pre-marcadas*"[218].<br><br>Si bien lo anterior fue planteado en términos de recomendación, no por ello se podría descartar que, bajo determinadas condiciones, dicha práctica impida que el consentimiento del titular sea libre y/o informado.<br><br>Asimismo, y cuando estas casillas pre-marcadas hacen alusión a finalidades del tratamiento, se podría estar ante un caso en el cual estas no se encuentren establecidas de manera inequívoca.<br><br>Este patrón oscuro podría verse agravado si es que no estamos ante un escenario de casillas pre-marcadas únicamente. Sino que, en cambio, las configuraciones de privacidad más invasivas | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción leve).<br><br>2. Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción grave).<br><br>3. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave). |

[218] Guía práctica para la observancia del "deber de informar" (Lima, 2019), 19.

| | | |
|---|---|---|
| | ya están implementadas por defecto. | |
| **Mirar para otro lado ("look over there")** | Este diseño podría estar orientado, de un lado, a que el titular de los datos no ejerza un adecuado control acerca de los datos que entrega y las finalidades que autoriza. Ello podría afectar el consentimiento que estaría otorgando.<br><br>Del otro, podría buscar que el titular de los datos no ejerza sus derechos o encuentre obstáculos para ello. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave). |

| | | |
|---|---|---|
| | | 2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |
| **PATRONES DE INCITACIÓN ("STIRRING")** | | |
| **Modalidad** | **Análisis** | **Posibles infracciones** |
| **Orientación emocional ("emotional steering")** | Esta modalidad busca influir en la sensibilidad del titular de los datos de modo tal que opte por una acción que sea sub-óptima para la protección de sus datos personales.<br><br>Si bien el tipo infractor dependerá de la acción en la cual se haya buscado influir, se podrá estar ante un consentimiento viciado; o, de ser el caso, ante un obstáculo para el ejercicio de sus derechos. A su vez, y si es que a través de la referida manipulación emocional se estaría buscando recopilar datos no necesarios o que se acepten finalidades no determinadas ni que consten inequívocamente, se podría estar ante una infracción de este tipo. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción leve).<br><br>2. Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción grave). |

| | | |
|---|---|---|
| | | 3. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>4. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |

| | | |
|---|---|---|
| **Oculto a primera vista (“hidden in plain sight”)** | Esta modalidad buscaría ocultar, a través de técnicas de diseño, las opciones menos restrictivas para la gestión de los datos personales del titular.<br><br>Esta situación podría generar un consentimiento viciado (al impedir que el titular conozca efectivamente todas las opciones que tenía, o al limitar la información a la cual accede) o un obstáculo para el ejercicio de sus derechos.<br><br>Asimismo, si es que lo que se estaría intentando ocultar son las finalidades al cual se sometería el tratamiento, se podría estar ante una contravención de la LPDP y el RLPDP. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción leve).<br><br>2. Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. (Infracción grave).<br><br>3. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>4. No atender, impedir u obstaculizar el ejercicio |

| | | |
|---|---|---|
| | | de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |
| PATRONES DE OBSTRUCCIÓN ("OBSTRUCTING") | | |
| Modalidad | Análisis | Posibles infracciones |

| | | |
|---|---|---|
| **Callejón sin salida ("dead end")** | En este caso se estaría ante un caso infractor más claro; toda vez que, o no se habrían habilitado los enlaces necesarios, o estos no funcionarían.<br><br>De esta manera, se estaría impidiendo el acceso a la información sobre cómo se procesan los datos personales. Sobre ello, es importante recordar que el artículo 18 de la LPDP dispone que las políticas de publicidad que se publiquen en plataformas en línea **deben ser fácilmente accesibles e identificables**<br><br>Adicionalmente, y de ser el caso, se podría estar impidiendo el acceso a los mecanismos para que el titular ejerza sus derechos. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |
| **Más largo de lo necesario ("longer than necessary")** | Estas modalidades intentarían desincentivar las acciones del titular de los datos al incorporar pasos innecesarios o al darles información contradictoria, | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, |

| | | |
|---|---|---|
| **Acción engañosa ("misleading action")** | respectivamente, para el acceso a la información o para poder controlar el procesamiento de sus datos.<br><br>Ello podría afectar el consentimiento que el titular otorgaría; y, de ser el caso, obstaculizaría el ejercicio de derechos. | expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |
| **PATRONES DE INCONSISTENCIA ("FICKLE")** | | |
| **Modalidad** | **Análisis** | **Posibles infracciones** |
| **Falta de jerarquía ("lacking hierarchy")** | En el contexto de estos tres patrones se le presentaría una inconsistencia al titular de los datos, principalmente de diseño. Dicha inconsistencia traería consigo que el titular de los datos no pueda acceder a la información sobre cómo se procesan sus datos (evitando un consentimiento informado).<br><br>Asimismo, podría generar que el titular de los datos no identifique los mecanismos para el ejercicio de sus derechos. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el |
| **Descontextualización ("decontextualising")** | | |
| **Interfaz inconsistente ("inconsistent interface")** | | |

| | | |
|---|---|---|
| | | Título III de la LPDP y el RLPDP. (Infracción grave). |
| **Discontinuidad en el lenguaje ("language discontinuity")** | Brindar información o detalles en un idioma que no responde al idioma que razonablemente entendería el titular de los datos contraviene la obligación de que la información se proporcione de forma clara, expresa e indubitablemente y con lenguaje sencillo. Ello, consecuentemente, impediría que el titular de los datos conozca cómo serán procesados su datos personales.<br><br>A su vez, esta discontinuidad en el lenguaje podría impedir el ejercicio de derechos, cuando los accesos a estos se encuentren en un idioma desconocido para el titular de los datos. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |
| **PATRONES DE OSCURECIMIENTO ("LEFT IN DARK")** | | |
| **Modalidad** | **Análisis** | **Posibles infracciones** |

| | | |
|---|---|---|
| **Información conflictiva ("conflicting information")** | De la misma manera como el caso anterior, estos patrones podrían contravenir la obligación de que la información se brinde de manera clara, expresa e indubitablemente y con lenguaje sencillo. Ello, una vez más, impediría que el titular de los datos conozca cómo serán procesados su datos personales.<br><br>Asimismo, se podría generar el problema ya mencionado de acceso a los mecanismos para ejercer derechos. | Dependiendo del caso concreto, se podría estar ante alguna de las siguientes infracciones:<br><br>1. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP y el RLPDP. (Infracción grave).<br><br>2. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo con lo establecido en el Título III de la LPDP y el RLPDP. (Infracción grave). |
| **Redacción o información ambigua ("ambiguous wording or information")** | | |

Sin perjuicio del análisis antes efectuado, y, en cualquier caso, constituirá también un acto infractor muy grave recopilar datos personales mediante medios fraudulentos, desleales o ilícitos. Ello, de acuerdo con lo explicado, podría darse cuando se empleen mecanismos que, de mala fe, busquen engañar a los titulares de los datos personales con el objeto de que estos entreguen sus datos personales. Además, no se deberá de perder de vista que, de manera general, también constituirá una infracción leve "(d)*ar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento.*"[219]

Ahora bien, para analizar la responsabilidad sobre este tipo de conductas, es necesario tener en cuenta el artículo 38 de la LPDP. Este dispone que "(l)*os administrados son responsables objetivamente por el incumplimiento de obligaciones derivadas de*

[219] Reglamento de la Ley de Protección de Datos Personales, artículo 132.

*las normas sobre protección de datos personales*"[220]. Ello implica que, para la determinación de responsabilidad de los responsables de tratamiento, bastará que se haya configurado el acto infractor, resultando irrelevante cualquier análisis de dolo o culpa del agente. En otras palabras, resultará irrelevante la intencionalidad del responsable del patrón oscuro siempre que objetivamente se configure alguno de los actos infractores tipificados como tal. De ser así, el administrado deberá ser hallado responsable y, consecuentemente, sancionado.

A modo de conclusión, queda evidenciado que ningún patrón oscuro podrá ser sancionado por calificar teóricamente como tal. En cambio, y en estricto cumplimiento del Principio de Tipicidad, estos podrán ser sancionados únicamente cuando su diseño e impacto impliquen la contravención de una obligación prevista en la LPDP y el RLPDP. Esto, consecuentemente, configuraría un acto infractor.

### *d) ¿Es necesaria una regulación específica sobre patrones oscuros?*

De lo explicado, resulta claro que, a la fecha, los patrones oscuros sí podrían implicar una contravención a la LPDP y el RLPDP e implicar una sanción (siempre y cuando configuren una infracción tipificada como tal). Sin embargo, ello no significa que el ordenamiento jurídico peruano no pueda modificarse a efectos de establecer un régimen más estricto en contra de dichos patrones. Ello deberá depender, no obstante, de un análisis más profundo que excede el objeto del presente artículo.

Y es que, entendiendo que la mayoría de las veces los patrones oscuros se apalancan en los sesgos cognitivos de las personas, la regulación que se les dé requiere preguntarse hasta qué punto las empresas (las cuales actúan como responsables del tratamiento) deben ser responsables del comportamiento no racional de los usuarios.

La respuesta dependerá del criterio por el cual los reguladores peruanos quieran optar. De un lado, autores como Jarovsky plantean que los sesgos cognitivos son rasgos inherentes al ser humano, por lo que, si la regulación pretende proteger a seres humanos reales (es decir, no a modelos teóricos distorsionados o anticuados de la racionalidad humana), se debe reconocer correctamente los sesgos cognitivos y cómo se puede sucumbir ante prácticas manipuladoras como lo son los patrones oscuros[221]. De manera similar, Waldman señala que el modelo de elección racional

---

220 Ley de Protección de Datos Personales, artículo 38.

221 Traducción y adaptación de la siguiente cita:

> "*Cognitive biases are inherent human traits and can be empirically demonstrated.3 As I argued in my academic article on dark patterns, if data protection law wants to protect real humans (i.e., and*

es ineficaz y no describe la toma de decisiones en materia de privacidad. Los individuos tendrían, más bien, una racionalidad limitada, lo que limita su capacidad para adquirir toda la información relevante y traducirla en una decisión basada en pruebas[222].

Del otro lado, autores como Rodríguez García[223] indican que "*la estrategia sancionadora frente a patrones oscuros es bastante rudimentaria y tosca. Presupone que en verdad las personas no queremos lo que quizás sí queremos (quedarnos con el servicio) o que es posible poner a todos los individuos en un mismo saco de padecimientos cognitivos*". Así, añade, "*podemos hacer mucho más daño con intervenciones crudas que normalmente gustan a quienes creen que solo se puede defender al consumidor con más obligaciones para los proveedores.*"

De cualquier forma, la respuesta que regulatoriamente se dé a los patrones oscuros en el ordenamiento jurídico peruano deberá partir de un análisis práctico acerca de qué tan expuestos están los usuarios peruanos a este tipo de diseños; y, además, cuál es el riesgo efectivo frente a estos. Además, será necesario no caer en posturas reduccionistas sobre los patrones oscuros; puesto que, si bien diversos patrones oscuros se apalancan únicamente en sesgos cognitivos, no es el caso de todos. Y es que, como bien resalta Waldman, aunque no existiera ninguno de estos obstáculos cognitivos en la toma de decisiones, los usuarios se seguirían enfrentando a las limitaciones que les impone el diseño de las plataformas. Por ello, pese a que un usuario se intente preocupar por su privacidad, el diseño de las plataformas podría dificultar (e, inclusive impedir) que este haga realidad sus preferencias[224].

---

> *not distorted or outdated theoretical models of human rationality), it must correctly acknowledge cognitive biases and how they might lead to manipulative practices - such as dark patterns.*"

Jarovsky, "How Cognitive Biases Make You Vulnerable to Dark Patterns".

222 Traducción y adaptación de la siguiente cita:

> "*The rational choice model is ineffective. It also fails to describe privacy decision-making. Individuals have bounded rationality, which limits their ability to acquire all relevant information and translate it into an evidencebased decision (...). Recent research has identified myriad cognitive and behavioral barriers to rational privacy and disclosure decision-making (...).*"

Ari Ezra Waldman, "Cognitive biases, dark patterns, and the 'privacy paradox'", Current Opinion in Psychology 31 (febrero de 2020): 3, https://doi.org/10.1016/j.copsyc.2019.08.025.

223 Gustavo Rodríguez García, "La psicología detrás de los patrones oscuros y lo que la regulación debería tener en cuenta - AGNITIO", AGNITIO, consultado el 30 de diciembre de 2023, https://agnitio.pe/articulo/la-psicologia-detras-de-los-patrones-oscuros-y-lo-que-la-regulacion-deberia-tener-en-cuenta/

224 Traducción y adaptación de la siguiente cita:

Adicionalmente, será necesario considerar que, incluso asumiendo que determinados usuarios sí están en capacidad de ser conscientes y evitar a voluntad sus sesgos cognitivos, no sería posible hacerlo respecto de otras poblaciones; principalmente, aquellas que presentan alguna vulnerabilidad por edad, preparación técnica, entre otros. Sobre ello, si bien la LPDP y la RLPDP establecen reglas especiales para los menores de edad al disponer, entre otros, que queda prohibida la entrega de obsequios o el otorgamiento de beneficios a estos a cambio de sus datos personales, todavía podría resultar necesario mayores mecanismos de protección para esta y otras poblaciones.

Sin embargo, mientras dicho análisis es efectuado por la ANPD y, de ser el caso, se prepara y emite alguna regulación específica sobre patrones oscuros, lo más apropiado será su difusión y puesta a conocimiento. Es cierto que el conocimiento de su existencia no evita que estos se implementen o que los usuarios sean "víctimas" de estos patrones; no obstante, sí podría permitir a estos últimos estar más atentos a la hora de interactuar en plataformas digitales, así como permitirá a los responsables de tratamiento ser conscientes sobre ciertos posibles diseños a evitar.

En última instancia, corresponde a la ANPD analizar el fenómeno de los patrones oscuros para que, con la colaboración efectiva de las empresas y los usuarios, se llegue a una conclusión aplicable a nuestra sociedad y ordenamiento. De ser el caso, y mientras se espera una posible regulación específica de la ANPD sobre patrones oscuros (de concluirse que es necesaria), la estrategia más adecuada en la actualidad es la difusión y concientización. Esta medida puede fomentar, de un lado, usuarios más conscientes y capaces de tomar decisiones informadas sobre los posibles riesgos de los patrones oscuros; y, del otro, empresas más proactivas que implementen buenas prácticas de privacidad en el diseño de sus plataformas.

---

"*Even if none of these cognitive hurdles to rational disclosure decision-making existed, internet users would still face the limitations imposed on them by design. By 'design', I am following Hartzog's (...) broad definition, which embraces the "processes that create consumer technologies and the results of their creative processes instantiated in hardware and software.*

(...)

*Many internet users care about their privacy. And yet, technology companies have made design choices that make it difficult for users to realize those preferences.*"

Waldman, "Cognitive biases, dark patterns, and the 'privacy paradox'", 4-5.

## IV. CONCLUSIONES

(i) Los sesgos cognitivos pueden definirse como la desviación sistemática, involuntaria e inconsciente de la racionalidad y la objetividad al momento de tomar decisiones. Diversas plataformas digitales, apalancándose en estos sesgos, son diseñadas (teniendo en cuenta la experiencia del usuario – UX y la interfaz del usuario – UI) con el propósito de inducir a los usuarios a que tomen decisiones sub-óptimas sobre la protección de sus datos personales.

(ii) Diversos académicos y autoridades han intentado definir a los patrones oscuros. A partir de estas definiciones, es posible concebirlos como un diseño web o de aplicativo deliberadamente destinado a generar un resultado sub-óptimo para el usuario del sitio web o del aplicativo (en lo referido, entre otros aspectos, a la protección de sus datos personales) que sin su implementación no se habría alcanzado.

(iii) Los patrones oscuros presentan diversas clasificaciones. A partir de la interacción del patrón oscuro con el usuario y el impacto en este es posible clasificarlos en patrones de sobrecarga, de omisión, de incitación, de obstrucción, de inconsistencia y de oscurecimiento. Esta clasificación es útil a efectos de entender cada patrón oscuro, pero debe tenerse en cuenta que es posible que existan patrones que se subsuman en más de una de las categorías propuestas; o que, inclusive, puedan exceder estas.

(iv) Los patrones oscuros representan una problemática que no puede ser ignorada. Se resaltan sus impactos en los derecho de consumo de los usuarios y en la protección de sus datos personales. Particularmente, los patrones constituyen un riesgo mayor para determinadas poblaciones tales como menores de edad, adultos mayores, individuos de bajos recursos, e individuos con niveles educativos inferiores.

(v) La creciente preocupación sobre los patrones oscuros ha generado que diversas jurisdicciones empiecen a tomar medidas al respecto. En Chile, el SERNAC ha llevado a cabo análisis y estudios con el objeto de identificar el impacto de estos patrones en su población y la protección de los datos personales de estos. En California y la Unión Europea se han dictado normas que prohíben el uso de este tipo de mecanismos. En países como España e Italia ya han existido sanciones, incluso, por patrones oscuros que fueron considerados como tales.

(vi) Un análisis sobre el tratamiento de los patrones oscuros bajo el ordenamiento jurídico peruano parte por definir si es que la LPDP y el RLPDP es exigible a las plataformas digitales. Frente a dicha interrogante, se aprecia que estas normas serán de aplicación a los siguientes responsables de tratamiento (y sus plataformas digitales): ***(a)*** responsables de tratamiento domiciliados en el país que llevan a cabo el tratamiento de los datos personales en el territorio nacional, ***(b)*** responsables de tratamiento no domiciliados a quienes les es

exigible la LPDP y la RLPDP en virtud de una disposición contractual o del derecho internacional, ***(c)*** responsables de tratamiento no domiciliados cuyas plataformas son empleadas en el territorio nacional.

(vii) A la fecha de redacción del presente artículo, no existe regulación específica que aborde a los patrones oscuros como tales. Sin embargo, pese a que los patrones oscuros no se encuentran expresamente prohibidos, bien podrían constituir, bajo determinadas circunstancias, una contravención a las disposiciones de la LPDP y el RLPDP.

(viii) Los patrones oscuros no pueden ser sancionados por calificar como tales. En aplicación del Principio de Tipicidad, solo aquellos patrones oscuros que configuren una conducta infractora tipificada como tal podrán constituir una infracción. Potencialmente, los patrones oscuros podrían configurar infracciones consistentes en recopilar más datos personales que los necesarios, dar tratamiento a datos personales sin contar con un consentimiento libre y/o informado, y obstaculizar el ejercicio de los derechos del titular.

(ix) La necesidad de contar con marco regulatorio específico para los patrones oscuros depende de un análisis pormenorizado del regulador. Dicho análisis deberá considerar, entre otros factores, ***(a)*** cuál es el grado de responsabilidad que deberían asumir los responsables de tratamiento por las decisiones desviadas de la racionalidad de los usuarios, ***(b)*** cuál es la concepción y el modelo de ser humano sobre el cual buscan erigir la regulación, ***(c)*** cuál es el grado de exposición e impacto al cual el usuario ubicado en el territorio peruano se vería efectivamente expuesto, ***(d)*** si es que resulta necesario reglas específicas para la protección de las poblaciones especialmente vulnerables frente a estos patrones.

En cualquier caso, la emisión o no de dicha regulación no puede pasar por alto la necesidad de difusión y concientización. Solo con ello se puede lograr tener usuarios más conscientes y empresas más proactivas frente al riesgo de los patrones oscuros.

## V. BIBLIOGRAFÍA


- "Cómo mejorar el índice de consentimiento evitando los patrones oscuros". Iubenda. Consultado el 30 de diciembre de 2023. https://www.iubenda.com/es/help/106796-como-mejorar-el-indice-de-consentimiento-evitando-los-patrones-oscuros.
- "Dark patterns: Manipulación en los servicios de Internet". AEPD: Agencia Española de Protección de Datos, 19 de mayo de 2022. https://www.aepd.es/prensa-y-comunicacion/blog/dark-patterns-manipulacion-en-los-servicios-de-internet.
- "Los 7 sesgos cognitivos en marketing que impulsarán tus conversiones". Rebold, 29 de noviembre de 2021. https://letsrebold.com/es/blog/sesgos-

cognitivos-en-marketing/#:~:text=Un%20sesgo%20cognitivo%20ocurre%20cuando,vital%20en%20términos%20de%20marketing.

- "Sesgos cognitivos en las ventas: teoría, práctica, aplicación". Pipedrive. Consultado el 28 de diciembre de 2023. https://www.pipedrive.com/es/blog/persuadir-sesgos-cognitivos-venta.
- "UI y UX: ¿qué son y cómo se distinguen en el diseño web?" Rock Content, 3 de noviembre de 2019. https://rockcontent.com/es/blog/ui-ux/#:~:text=El%20término%20UX%20viene%20de,después%20de%20usar%20tu%20producto.
- Agencia Española de Protección de Datos Personales. Resolución del Procedimiento Sancionador del Expediente No. EXP202211953 (PS/00080/2023) (España).
- Agencia Española de Protección de Datos. Guía de Protección de Datos por Defecto. 2020.
- Autoridad Nacional de Protección de Datos Personales, Guía práctica para la observancia del "deber de informar" (Lima, 2019).
- Autoridad Nacional de Protección de Datos Personales. Guía práctica para la observancia del "deber de informar". Lima, 2019.
- Blesch, William. "Dark Patterns, the FTC and the GDPR". TermsFeed, 22 de septiembre de 2023. https://www.termsfeed.com/blog/dark-patterns/.
- California. The California Privacy Rights Act. 2020.
- Ch, Carlos. "Patrones oscuros en privacidad: las bases". Medium, 1 de agosto de 2023. https://medium.com/privacimiento/patrones-oscuros-en-privacidad-las-bases-9199435d003a.
- Comisión Europea. "Ley de Servicios Digitales: Preguntas y respuestas". Shaping Europe's digital future | European Comission, 17 de enero de 2024. https://digital-strategy.ec.europa.eu/es/faqs/digital-services-act-questions-and-answers.
- Commission Nationale de l'Informatique et des Libertés. Shaping Choices in the Digital World. 2019. https://www.cnil.fr/sites/cnil/files/2023-06/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.
- Dirección de Protección de Datos Personales. 1 de marzo de 2022. Resolución Directoral No. 1022-2022-JUS/DGTAIPD-DPDP (Perú).
- Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. 14 de diciembre de 2022. Resolución Directoral No. 82-2022-JUS/DGTAIPD (Perú).
- Edwards, Jeffrey. "What are Dark Patterns? How UI Influences Consent and Compliance". CHEQ, 23 de enero de 2023. https://cheq.ai/blog/what-are-dark-patterns/.

- European Data Protection Board. Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them. 2022.
- Expediente No. 075-2022/CC3. Comisión de Protección al Consumidor No. 3. 20 de junio de 2023. Resolución No. 043-2023/CC3 (Perú).
- Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt y Austin L. Toombs. "The Dark (Patterns) Side of UX Design". En CHI '18: CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM, 2018. https://doi.org/10.1145/3173574.3174108.
- Indecopi. "Cyber Days: Indecopi advierte que proveedores podrían usar 'patrones oscuros' en sus páginas web para influir en decisiones de compra". 28 de marzo de 2023. https://repositorio.indecopi.gob.pe/bitstream/handle/11724/8829/NP%20220328%20Patrones%20Oscuros.pdf?sequence=2&isAllowed=y.
- ISACA. Eliminating Deceptive Privacy Practices: Building Trust by Addressing Privacy Dark Patterns. 2023. https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/eliminating-deceptive-privacy-practices_0823.pdf.
- Jarovsky, Luiza. "Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness". SSRN Electronic Journal, 2022. https://doi.org/10.2139/ssrn.4048582.
- Jarovsky, Luiza. "Dark Patterns in Privacy: An Autonomy Problem". LinkedIn, 1 de marzo de 2023. https://www.linkedin.com/pulse/dark-patterns-privacy-autonomy-problem-luiza-jarovsky/.
- Jarovsky, Luiza. "Examples of Dark Patterns in Privacy". LinkedIn, 13 de abril de 2023. https://www.linkedin.com/pulse/examples-dark-patterns-privacy-luiza-jarovsky/?trackingId=v9b6fShbSLOeK9cULl1q1Q==.
- Jarovsky, Luiza. "How Cognitive Biases Make You Vulnerable to Dark Patterns". LinkedIn, 19 de mayo de 2022. https://www.linkedin.com/pulse/how-cognitive-biases-make-you-vulnerable-dark-luiza-jarovsky/.
- Jarovsky, Luiza. "You Are Probably Doing Privacy UX Wrong". Luiza's Newsletter, 19 de enero de 2023. https://www.luizasnewsletter.com/p/you-are-probably-doing-privacy-ux.
- Jha, Deepak. "How Does Dark Pattern Affect Your Data Privacy?" LightBeam.ai, 23 de febrero de 2023. https://www.lightbeam.ai/post/how-does-dark-pattern-affect-your-data-privacy.
- John, Leslie K. "We Say We Want Privacy Online, But Our Actions Say Otherwise". Harvard Business Review, 16 de octubre de 2015. https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise.

- Ministerio de Justicia. Proyecto de Nuevo Reglamento de la Ley No. 29733, Ley de Protección de Datos Personales. Publicado el 25 de agosto de 2023.
- Ordoñez, Oscar. "¿Qué son los patrones oscuros y cómo afecta a la protección de datos?" LogTec Consulting Group, 29 de noviembre de 2022. https://dataprotected.com.co/blog-proteccion-de-datos/seguridad/que-son-los-patrones-oscuros-y-como-afecta-a-la-proteccion-de-datos/.
- Paz, Andrés. "Los sesgos cognitivos y la legitimidad racional de las decisiones judiciales (Cognitive Bias and the Rational Legitimacy of Judicial Decisions)". Razonamiento Juridico y Ciencias Cognitivas, 2021, 187–222.
- Perú. Ley de Protección de Datos Personales. Ley 29733. Aprobada el 2 de julio de 2011.
- Perú. Reglamento de la Ley de Protección de Datos Personales. Decreto Supremo 003-2013-JUS.
- Perú. Texto Único Ordenado de la Ley del Procedimiento Administrativo General. Decreto Supremo 004-2019-JUS.
- Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A. - 23 febbraio 2023 [9870014]. Garante per la Protezione dei Dati Personali. 23 de febrero de 2023. 9870014 (Italia).
- Rodríguez García, Gustavo. "La psicología detrás de los patrones oscuros y lo que la regulación debería tener en cuenta - AGNITIO". AGNITIO. Consultado el 30 de diciembre de 2023. https://agnitio.pe/articulo/la-psicologia-detras-de-los-patrones-oscuros-y-lo-que-la-regulacion-deberia-tener-en-cuenta/.
- Santos, Cristiana y Arianna Rossi. "The emergence of dark patterns as a legal concept in case law". Internet Policy Review, 31 de julio de 2023. https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept.
- Servicio Nacional del Consumidor de Chile. Consentimiento en el Uso de Cookies: Evidencia Experimental sobre el Impacto de la Privacidad por Defecto y los Patrones Oscuros en las Decisiones de los Consumidores. Santiago de Chile, marzo de 2022.
- Traseira, Carlos. "Sesgos cognitivos. Los más usados en marketing digital". LinkedIn, 29 de noviembre de 2022. https://www.linkedin.com/pulse/sesgos-cognitivos-los-más-usados-en-marketing-digital-carlos-traseira/?originalSubdomain=es.
- Unión Europea. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). Aprobado el 19 de octubre de 2022.
- Vásquez Rodríguez, Raúl. "La protección de los datos personales en el sistema de reporte de créditos peruano". Revista de Derecho YACHAQ, n. º 10 (2019): 73–94.

- Waldman, Ari Ezra. "Cognitive biases, dark patterns, and the 'privacy paradox'". Current Opinion in Psychology 31 (febrero de 2020): 105–9. https://doi.org/10.1016/j.copsyc.2019.08.025