GUÍA DE PRIVACIDAD DESDE DISEÑO

Un DroneRules.eu PRO recurso para los fabricantes de drones.

Tabla de Contenidos

¿Qué es esta guía de privacidad desde diseño?

Esta guía de privacidad desde el diseño está dirigida a los fabricantes de drones y su objetivo es ayudarles a incorporar la privacidad en el proceso de diseño y construcción de los drones. La guía:

- le introducirá en los principios fundamentales de la privacidad desde el diseño,
- le guiará a través de su aplicación en la práctica, proporcionándole un cuestionario que le ayudará a evaluar los riesgos para la privacidad y a identificar las medidas de protección adecuadas, y
- le proporcionará una visión general de los riesgos para la privacidad que pueden derivarse de las diferentes características de los drones, y le propondrá fácilmente posibles soluciones.

La privacidad por diseño es importante porque el Reglamento General de Protección de Datos (RGPD) exige que las organizaciones que traten datos personales apliquen los principios de protección de datos desde el diseño y por defecto (por ejemplo, pilotos y operadores de drones). Estos principios tienen por objeto garantizar que las consideraciones relativas a la protección de datos y a la privacidad desempeñen un papel en el diseño y el desarrollo de nuevas tecnologías, en los procesos y planes de vuelo desde el principio y que garanticen que, por defecto, se procesen tan pocos datos personales como sea posible.

Seguir esta guía y sus recomendaciones puede ayudarle a incorporar la privacidad en los productos que crea desde la etapa de diseño y desarrollo. Los riesgos para la privacidad pueden surgir en relación con varios aspectos del diseño y funcionamiento de un dron, desde sus actividades de recogida y tratamiento de datos,[1] hasta su funcionamiento[2] e incluso su apariencia.[3] Por estas razones, la privacidad desde el diseño tiene que estar un paso adelante en el diseño y la fabricación de los drones.[4] Esto es particularmente importante en el caso de los drones. Gracias a su tamaño, agilidad y diversidad de capacidades, los drones podrían recoger grandes cantidades de datos personales de forma muy poco transparente.

En el RGPD, los requisitos de protección de datos desde el diseño y por defecto se aplican a los responsables del tratamiento, es decir, a las personas o entidades que determinan los fines y medios del tratamiento de datos personales. En el contexto de las operaciones con drones, lo más probable es que se trate de los operadores (o, dependiendo de sus acuerdos contractuales, de sus clientes) y de los pilotos, pero esto se deberá analizar caso por caso. Aunque estas obligaciones no se aplican directamente al fabricante de un dron, se aplican a los operadores a la hora de elegir su equipo antes de la recogida de datos personales. Por lo tanto, es necesario

[1] Anne Gerdes, y Privacy Issues, Information, Technology and Innovation Research Group at University of Southern Denmark, Drones, 2017, diapositivas de presentación. http://infotechinno.sdu.dk/pdfs/Drones%20and%20privacy%20SDU_042418.pdf

[2] Altawy Riham y Amr. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey", *ACM Transactions on Cyber-Physical Systems,* Vol. 1, Issue 2, Article 7, November 2016, 25 pages. https://users.encs.concordia.ca/~youssef/Publications/Papers/Drone-Survey.pdf.

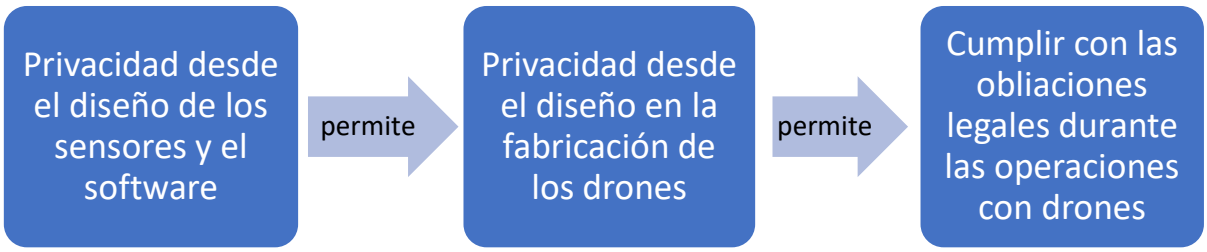
[3] Chang, Victoria, Pramod Chundury, Marshini Chetty, ""Arañas en el cielo": User Perceptions of Drones, Privacy, and Security", *CHI '17* Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, May 06-11, 2017, Denver, CO., USA, pp. 6765 - 6776. https://hci.princeton.edu/wp-content/uploads/sites/459/2017/01/CHI2017_CameraReady.pdf

[4] Cavoukian, Ann, "Privacy and Drones: Unmanned Aerial Vehicles", Information and Privacy Commissioner, Ontario, Canadá, agosto de 2012, pág. 4. https://www.pc.on.ca/wp-content/uploads/Resources/pbd-drones.pdf

implementar los principios de protección de datos y los requisitos de privacidad desde el diseño y por defecto como fabricante para que sus clientes puedan operar legalmente su dron. Por lo tanto, podría darle una ventaja competitiva significativa y ayudarlo a distinguir sus productos de los de sus competidores al apoyar el cumplimiento de la protección de datos de sus clientes.

Además de mejorar la calidad y la capacidad comercial de su dron, ciertas características que mejoran la privacidad pueden convertirse pronto en obligatorias para los drones en el mercado europeo. Los legisladores europeos están debatiendo actualmente ciertos requisitos técnicos para los drones, algunos de los cuales tienen una relación directa con el impacto de los drones en la privacidad. Una vez que estos requisitos se conviertan en ley, usted estará legalmente obligado a cumplirlos si desea vender sus drones en Europa.

Por último, algunas partes de esta guía también son relevantes para los fabricantes de sensores (cargas útiles fijas o modulares) y software, utilizados en la fabricación de drones. Las partes y piezas de los drones a menudo provienen de diferentes fuentes y son ensambladas por un solo fabricante o, en el caso de cargas útiles modulares, son fijadas a un dron incluso por el operador del dron. Es igualmente importante garantizar que el software y los sensores utilizados en la fabricación de un dron incorporen la privacidad desde el diseño siempre que sea posible.



Le sugerimos que consulte esta guía junto con otros recursos de DroneRules PRO disponibles en el sitio web, así como cualquier actualización relevante de la legislación que pueda ser aplicable a sus actividades de fabricación de drones, especialmente cuando sus drones puedan ser utilizados para tratar datos personales.

7 principios de privacidad desde el diseño en el contexto de la fabricación de drones

Existen siete principios fundamentales de la privacidad desde el diseño que ayudan a explicar lo que este concepto significa en la práctica.[5] Esta guía le presentará algunos riesgos y salvaguardas específicos que se deben considerar como una forma de aplicar la privacidad desde el diseño a su trabajo. Sin embargo, estos principios constituyen una guía general sobre sus obligaciones que puede ser utilizada para desarrollar medidas específicas de privacidad mediante el diseño para el uso y las operaciones de su dron. Hemos incluido a continuación una breve descripción de los principios generales de privacidad desde el diseño y cómo podrían aplicarse a la fabricación de drones.[6]

1. Proactivo, no reactivo

La privacidad desde el diseño requiere un enfoque proactivo. En lugar de esperar a que el riesgo se materialice, como fabricante de drones, debe actuar de forma preventiva y considerar la mejor forma de proteger la privacidad mediante la implementación de características y medidas de seguridad adicionales en el diseño y la construcción de su dron. Al considerar la implementación de tecnologías que pueden mejorar la privacidad y que pueden ser usadas en los drones que usted fabrica, no sólo está haciendo que sus productos sean más competitivos, sino que también puede estar impidiendo eficazmente que se produzcan infracciones sobre la privacidad.

Entre los ejemplos clave de características de los drones que podrían ayudar a lograr este principio se incluyen:

- Proporcionar al dron con capacidades de geo-cercado ("*geo-fencing*") y otras tecnologías de detección de limitaciones geográficas;
- Equipar el dron con controles de software que permitan a los usuarios adaptar fácilmente los sensores utilizados y la calidad de los datos capturados en una operación particular;
- Incorporar software o funcionalidades en el software de control del dron que permita a los usuarios activar o desactivar los sensores y/o las cargas útiles que se van a activar para un vuelo en particular, logrando así la modularidad en la práctica;
- Proporcionar controles de software para que los usuarios puedan activar o impedir la grabación de datos cuando lo deseen durante un vuelo;
- Incorporar controles de acceso y encriptación en el dron y en los datos almacenados en él, así como en el sistema de control en tierra a través del cual es operado;
- La implementación de características adicionales de software que permitan minimizar los datos por medio de:
    - la limitación en la recogida de datos, por ejemplo, desactivando la recogida de datos cuando un dron se desvía de su ruta de vuelo predeterminada o permitiendo su fácil encendido y apagado para que sólo funcione cuando sea necesario,
    - la limitación en la retención de datos, por ejemplo, borrando automáticamente todos los datos en el dron después de haber sido descargado después de un vuelo,

[5] Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles", Information and Privacy Commissioner, Ontario, Canadá, enero de 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
[6] Ver Cavoukian *supra* n 4, p. 19.

- la detección automática de formas humanas y eliminación de las mismas mediante blanqueo, ocultación o difuminado, anonimizando así los datos personales capturados.

- Garantizar un alto nivel general de seguridad de la información y de las tecnologías de la información en los sistemas del dron, protegiendo así el dron y el acceso a sus datos.

2. La privacidad configurada por defecto

El diseño y la configuración de los drones, su carga útil y el software que utilizan deben estar orientados a garantizar la privacidad de forma predeterminada. Tan pronto como un dron sea desembalado, debe ser programado para que proteja lo máximo posible la privacidad. Esto es similar al principio de protección de datos por defecto, que exige que el principio de protección de datos desde el diseño sea respetado tanto por los fabricantes como por los operadores y debe aplicarse a todo el ciclo de vida de una tecnología, incluidos su diseño y fabricación[7]. Esto no sólo le permitirá mostrar las características más avanzadas del dron, sino que también ayudará a los usuarios a cumplir con sus obligaciones con mayor facilidad.

Al considerar la privacidad y la protección de datos desde el diseño y la fabricación de sus drones, el equipo, la interfaz, los programas y los controles implementados deben ser tan privados como sea posible por defecto. Sin necesidad de que los usuarios finales alteren las características o ajustes del dron, por ejemplo:

- cumplir con las limitaciones de geo-cercado u otras limitaciones que puedan ser detectadas,
- exigir controles de acceso, como contraseñas, para limitar el acceso a los datos recogidos y a los controles del dron,
- encriptar datos en el dron,
- recoger la menor cantidad de datos mediante, entre otros, estar equipados con capacidades de software que puedan activar los sensores de datos y las capacidades de recogida de datos sólo cuando se cumplen una serie de condiciones (tales como la ubicación, la sincronización, el vuelo dentro de un área predeterminada),
- almacenar los datos durante el menor tiempo posible.

Si los usuarios desean cambiar estos ajustes, deberían poder hacerlo, pero tendrían que decidirlo específicamente y tomar una decisión consciente a tal efecto.

3. La privacidad integrada en el diseño

El diseño y la arquitectura de los sistemas y productos de los drones deben tener en cuenta consideraciones de privacidad. Las consideraciones de privacidad deben formar parte del producto y de su funcionalidad, en lugar de añadirse una vez finalizado el diseño. Al considerar sistemáticamente el potencial impacto sobre la privacidad de su dron y su equipo, así como la forma en que probablemente sea utilizado, usted podrá decidir qué medidas de seguridad son apropiadas para incorporar en el diseño de su dron, sus cargas útiles, su software y su interfaz.

[7] Grupo de trabajo sobre protección de datos del artículo 29, Dictamen 01/2015 sobre cuestiones de privacidad y protección de datos relativas a la utilización de zánganos, 01673/15/ES WP 231, 16 de junio de 201, p. 14. (Llamado'A29WP Opinion on Drones' abajo)

4. Plena funcionalidad

La privacidad desde diseño no debe venir a expensas de la calidad y la funcionalidad de su producto. La privacidad desde el diseño puede ser incorporada de una manera que mejore su producto y no interfiera desproporcionadamente con sus características clave. No debe haber una elección entre la privacidad y la buena funcionalidad de su producto. Ambas pueden lograrse juntas, especialmente si se considera que la protección de la intimidad es una mejora adicional de de los drones.

5. Seguridad de extremo a extremo

La privacidad debe protegerse mediante consideraciones de seguridad incorporadas a lo largo de todo el proceso de funcionalidad de los drones. Esto significa que las medidas de seguridad deben cubrir la seguridad de los drones mientras estén en el aire o en tierra. La seguridad debe proteger los datos a lo largo de todo su ciclo de vida en el dron, desde la recogida de datos hasta su almacenamiento local en el don o tras su transmisión a otros programas o dispositivos y, por último, hasta el borrado seguro de los datos. En la sección "Ciberseguridad en todos los sistemas del dron" se incluye una sección especial relativa a la seguridad de la información y de las tecnologías de la información en el contexto de la fabricación de drones.

6. Visibilidad / transparencia

El principio de visibilidad y transparencia busca asegurar que todas las partes interesadas tengan manera de verificar que la privacidad sea respetada por la tecnología o el proceso que se está desarrollando. En el contexto de las operaciones con drones, las personas en tierra deben tener suficiente transparencia y visibilidad de las actividades del dron y del operador o piloto. En el contexto de la fabricación, este principio requiere que se desarrollen drones que sean claramente visibles, pero también que proporcionen información detallada a los pilotos u operadores sobre su producto y sobre cómo puede utilizarse para proteger la privacidad de las personas sobre el terreno.

En este contexto, estos principios podrían aplicarse de varias maneras:

- hacer que los drones se noten e implementar elementos en el diseño que puedan indicar a las personas en el suelo que los sensores del dron están activos y capturando datos,
- poner a disposición información sobre los componentes, las piezas de construcción y las características del software del dron, que mejoran la privacidad y la forma en que funcionan,
- cumplir con las normas de seguridad/privacidad auditadas o códigos de conducta y presentar los documentos que lo respalden,
- implementar características en el software del dron que permitan registrar y rastrear los comandos dados al dron durante las operaciones, el acceso a los datos o la eliminación de datos,
- incluir un manual de usuario detallado y un folleto en el embalaje del dron con:
    - información sobre las características de privacidad, e
    - información detallada sobre las diferentes cargas útiles y sus ventajas y desventajas para ayudar a los pilotos y operadores a elegir las mejores características que necesitan;
- dotar al dron de capacidades y características que le permitan comunicarse e integrarse con aplicaciones o plataformas destinadas a proporcionar información al público sobre

las operaciones en curso o futuras que tengan lugar con un modelo específico de dron o una selección de modelos diferentes.

7. Respeto por las personas / Enfoque centrado en el usuario

El respeto por la privacidad de las personas debe guiar todas sus acciones al implementar el la privacidad desde el diseño. Poniendo a los usuarios y a los individuos en el centro de sus actividades y considerando cómo (1) respetar su privacidad y (2) permitir que otros, usando su producto, respeten su privacidad. Esto se puede hacer incorporando características que respeten la privacidad, así como haciendo que estas características sean fáciles de usar e informando a sus clientes sobre cómo implementarlas.

Por un lado, este principio requiere que usted considere cómo diseñar y construir su dron con características que hagan que el respeto de los deseos de la gente sea fácil de lograr. Por ejemplo, las capacidades de geo-cercado podrían permitir detectar fácilmente cuando se entra en áreas donde el dron podría no ser bienvenido e informar rápidamente al piloto, lo que permitiría a este último, tomar medidas correctoras.

Por otro lado, también debe considerar a los usuarios cuando construya su dron. Como fabricante, debe hacer que las funciones para preservar la privacidad sean fáciles de entender y de usar. Esto hará que sea mucho más probable que se utilicen en la práctica y ayudará a mejorar el atractivo de su producto y la conformidad de los usuarios con su dron.

Regulación de la UE sobre los drones y diseño de drones que mejoran la privacidad

Las autoridades europeas están trabajando actualmente en la regulación de los drones y se está considerando la obligatoriedad de algunas características que mejoren la privacidad. Las regulaciones que se publicaron el 11 de junio de 2019 separan a los drones en diferentes clases, determinadas por su tamaño, capacidad de elevación y capacidad de vuelo, y asignarán a cada clase determinados requisitos. Estas regulaciones son:

- el Reglamento de ejecución (UE) 2019/947 de la Comisión de 24 de mayo de 2019 relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas [8] y su ANEXO[9] (denominado en lo sucesivo "Reglamento de ejecución sobre drones"), y
- el Reglamento delegado (UE) 2019/945 de 12 de marzo de 2019 de la Comisión sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas[10] (denominado en lo sucesivo "Reglamento delegado sobre drones").

El Reglamento delegado sobre drones proporciona información, en particular sobre los drones que se utilizan en las operaciones de "categoría abierta". Eso significa vuelos realizados:

- en la línea visual de un piloto o de un miembro de su equipo,
- la masa máxima de despegue de la aeronave no tripulada es inferior a 25 kg
- en alturas que no superen los 120 m por encima de la superficie, salvo cuando sobrevuele un obstáculo (tal como se define en el Reglamento de ejecución sobre drones),
- que el piloto a distancia garantiza que la aeronave no tripulada se mantiene a una distancia segura de las personas y que no vuela sobre concentraciones de personas, y
- teniendo en cuenta los riesgos implicados, no requiere ni una autorización previa de la autoridad competente, ni una declaración del operador del SANT antes de que se lleve a cabo la operación.

Este reglamento podría tener un impacto en la forma en que usted incorpora la privacidad en su trabajo al imponer requisitos o limitaciones a los drones y al proceso de fabricación de los mismos. Además, algunos aspectos de la regulación pueden contribuir a la protección de la vida privada desde el diseño, al exigir que tecnologías que mejoran la privacidad se incorporen a los drones.

---

[8] Reglamento de ejecución (UE) 2019/947 de la Comisión de 24 de mayo de 2019 relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0947&from=EN).

[9] Anexo del Reglamento delegado (UE) 2019/945 de 12 de marzo de 2019 de la Comisión sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0945&from=EN).

[10] Reglamento delegado (UE) 2019/945 de 12 de marzo de 2019 de la Comisión sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0945&from=EN). Para más información sobre las últimas novedades legislativas de la AESA en relación con la categoría "abierta" de operaciones, véase https://www.easa.europa.eu/document-library/opinions/opinion-012018.

El Reglamento de ejecución divide los drones en diferentes clases, en función de su tamaño y de su masa máxima de despegue. Cada clase (C0, C1, C2, C3, C4) debe cumplir una serie de requisitos técnicos diferentes. El cumplimiento de estos requisitos no sólo determinará si su dron puede venderse en el mercado de la Unión Europea, sino que también puede influir en la forma en que los operadores y pilotos utilizan los drones en la práctica, por ejemplo, si pueden o no utilizarlos en subcategorías particulares de operaciones de drones "abiertos".

Además, las diferentes clases de drones están sujetas a diferentes requisitos técnicos y obligaciones en cuanto a características o equipos. Los requisitos generales incluyen obligaciones específicas sobre la seguridad en el diseño y la fabricación, así como el suministro de información a los usuarios sobre el uso seguro y responsable de los drones. Sin embargo, existen requisitos específicos con respecto a las capacidades de los drones, a la seguridad y a la tecnología que difieren en función de las distintas clases. A medida que vayamos introduciendo diferentes formas de incorporar la privacidad desde el diseño en los drones, iremos destacando los requisitos que se convertirán en obligaciones legales en el futuro.

Se recomienda que se utilicen las obligaciones legales establecidas en el Reglamento delegado sobre los drones como guía para otros drones que se fabriquen. Aunque el Reglamento delegado sobre los drones sólo se aplica a los drones destinados a ser utilizados en vuelos de categoría "abierta", debería considerar la posibilidad de ampliar muchas de estas recomendaciones más allá de lo que exige la ley por las razones que se exponen a continuación:

- Independientemente de la categoría de operación del dron, los operadores y pilotos de tendrán ciertas responsabilidades en cuanto a la privacidad y a la protección de datos de acuerdo con el RGPD que se deberán cumplir. Éstas pueden incluir la responsabilidad de informar a las personas sobre el terreno de sus actividades, cómo puede minimizar la cantidad de datos recopilados y conservados, así como garantizar la seguridad de los datos tratados. Las características de los drones son extremadamente importantes para lograr esto.
- La mayoría de las operaciones cerca o sobre concentraciones de personas no involucradas en el vuelo serán operaciones de categoría "específica". Es más probable que las operaciones de categoría "específica" planteen problemas significativos de privacidad y protección de datos. El Reglamento de ejecución sobre drones reitera la responsabilidad de los operadores en operaciones "específicas", de disponer de procedimientos (y equipos) para garantizar el cumplimiento de la legislación sobre protección de datos.[11]
- El Reglamento de ejecución sobre drones faculta a los Estados miembros de la UE a restringir las operaciones con drones en determinadas zonas geográficas, incluyendo por razones de privacidad y protección de datos. Como parte de ello, los Estados miembros podrán exigir que los drones estén equipados con dispositivos especiales de protección de la intimidad para poder operar en determinadas zonas designadas, por ejemplo, las[12] ciudades. Todavía está por ver cómo los países decidirán regular esto.

[11] UAS.SPEC.050 (1)(a)(iv) Anexo del Reglamento de ejecución (UE) 2019/947 de la Comisión de 24 de mayo de 2019 relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0947&from=EN).

[12] Artículo 15 Reglamento de ejecución (UE) 2019/947 de la Comisión de 24 de mayo de 2019 relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0947&from=EN).

Por estas razones, se recomienda que considere las recomendaciones sobre la incorporación de la privacidad desde el diseño en todos los drones que cree, incluso en aquellos que no están destinados a ser utilizados en operaciones de categoría "abierta" y que todavía no están sujetos a una regulación concreta de mejora de la privacidad o a un proyecto de regulación.

Riesgos y salvaguardas para la privacidad en la fabricación de drones

Con el fin de comprender la interacción entre los drones y la privacidad, destacaremos cómo los diferentes aspectos de un dron pueden interferir con la privacidad y los datos personales de las personas sobre el terreno. Específicamente, hemos dividido esta sección en cuatro temas:

(1) Diseño de los drones
(2) Hardware del dron
(3) Software del dron
(4) Embalaje del dron

En cada sección, destacaremos los principios y requisitos en los que los drones podrían interferir y propondremos salvaguardas y características específicas que podrían utilizarse para incorporar consideraciones de privacidad en el dron. En los casos en que determinadas características relevantes para la privacidad se discutan también como requisitos legales en el Reglamento de ejecución sobre los drones, se pondrá de relieve este aspecto.

El objetivo final es proporcionarle las herramientas necesarias para crear drones que ayuden a los usuarios de drones a cumplir con sus propias obligaciones legales de privacidad y protección de datos y a operar de forma responsable.

Diseño de drones y privacidad

La forma en que se diseña un dron puede afectar la forma en que es percibido por los individuos sobre el terreno y las preocupaciones sobre la privacidad y la seguridad que experimentan. Los aspectos clave que pueden hacer que su dron sea menos amenazador incluyen:

- vigilancia,
- forma,
- sonidos (viento),
- los movimientos de los drones y las capacidades de grabación. [13]

Si los individuos en el suelo sienten que su dron supone una amenaza a nivel psicológico, es más probable que se sientan vigilados e incómodos. Esto podría llevarlos a autocensurar sus actividades (en lo que se conoce como efecto de "paralizador")[14], a buscar activamente a los pilotos y operadores y a impedir su operación, o a aplicar medidas propias para evitar que los drones vuelen cerca de ellos o de sus hogares, por ejemplo, mediante el uso de tecnología contra drones.

Sin embargo, hay pasos, que usted podría tomar para evitar que los individuos se sientan incómodos alrededor de los drones y evitar que los perciban como máquinas hostiles.

Color y logotipos

Los diseños tradicionales de color oscuro monocromático pueden ser percibidos como poco amigables y menos fiables por la gente. Además, la falta de logotipos u otros signos en el dron

[13] Véase Chang *supra* n 3, págs. 7-9.
[14] Finn, Rachel L., David Wright, Laura Jacques, Paul De Hert, "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations: Summary for Industry", Comisión Europea, Ref. Area(2015)322948- 27/01/2015, Noviembre 2017, p. 7.

podría incomodar a las personas, ya que no permiten atribuir el comportamiento del dron a una persona o empresa ni identificar a sus controladores[15]. Esto menoscaba la transparencia y la responsabilidad de quienes controlan el dron. Además, los colores opacos y camuflados, especialmente en los drones pequeños, podrían aumentar el riesgo de que las personas que se encuentran en el suelo no sean conscientes de que los drones operan sobre ellos.

Usted puede remediar fácilmente estas preocupaciones usando colores más brillantes en su diseño, lo que haría que los drones parezcan menos amenazadores y que su dron sea más visible desde el suelo. Los colores más brillantes también se han asociado con la evocación de emociones más positivas en las personas.[16] Además, en el futuro, los drones de las clases C1, C2 y C3 deberán estar equipados con luces para mejorar la capacidad de control, ampliando en algunos casos el requisito a condiciones de luz diurna y nocturna.[17] Estas luces también podrían mejorar significativamente la visibilidad y la notoriedad de los drones.

Además, puede colocar pegatinas con su logotipo y el número de serie del dron u otra información de identificación, en un lugar claramente visible pero protegido. Esto no sólo ayudará a informar a los usuarios de los drones de las capacidades particulares de su dron, sino que también puede hacer que la gente se sienta más segura al hacerles saber quiénes son los responsables de la operación.

Número de palas del rotor

El número de rotores que tiene un dron también puede afectar la forma en que es percibido por los individuos. El diseño de los drones se ha vinculado siempre a la apariencia intimidante, violenta, militar o como "arañas"[18]. Esto podría sugerir que los drones con más de 4 rotores - pentacópteros, sextacópteros, etc. - podrían ser percibidos como más amenazadores. Por otro lado, los drones circulares pueden ser considerados más amigables por la gente[19]. Además, disponer de protecciones alrededor de las palas del rotor también puede utilizarse para "suavizar" el aspecto de los drones y hacer que los usuarios se sientan más seguros.[20]

Tamaño de los drones

El Reglamento delegado sobre drones impone requisitos a las diferentes clases de drones, al ser utilizados en operaciones de categoría "abierta" en lo que respecta a su masa máxima de despegue (MTOM) o a la potencia ejercida durante una colisión. A continuación, se presenta un resumen de dichos requisitos, tal y como figuran en el Reglamento:

	Clase C0	Clase C1	Clase C2	Clase C3	Clase C4
MTOM, incluida la carga útil	< 250 g	<900 g, durante un impacto entre el dron y una cabeza	< Menos de 4 kg	< Menos de 25 kg	< Menos de 25 kg

[15] Véase Chang, *supra nota* 3, pág. 7.
[16] Hemphill, Michael, "A Note on Adults' Color-Emotion Associations", *The Journal of Genetic Psychology,* Vol. 157, Issue 3, 1996, pp. 275-280.
[17] Parte 2.16, parte 3.18, parte 4.14 del anexo del Reglamento delegado de la Comisión sobre drones.
[18] Ver Chang *supra* n 3, p. 7.
[19] *Ibídem,* pág. 11. Sung, Ja-Young, Lan Guo, Rebecca E. Grinter, Henrik I. Christensen,"My Roomba is Rambo": íntimos electrodomésticos" UbiComp '07 Proceedings of the 9th International Conference on Uniquitous Computing, Innsbruck, Austria, 16-19 de septiembre de 2007, pp. 145-162.
[20] Ver Chang *supra* n 3, p. 8.

		humana a velocidad terminal, transmite energía < 80J			

Sin embargo, además de su clasificación, los diferentes tamaños de los drones también pueden evocar diferentes respuestas y preocupaciones de las personas que se encuentran en el suelo. Si los drones son demasiado grandes, las personas pueden sentirse incómodas porque sienten que no saben qué carga útil lleva u oculta un dron grande. Por otro lado, si los drones son demasiado pequeños, pueden volverse menos notorios y sigilosos. Además, los drones pequeños pueden tener acceso a áreas restringidas debido a su tamaño.[21]

Parece que no hay una solución fácil para este problema, ya que ambos extremos en el tamaño dan lugar a preocupaciones diferentes. Sin embargo, hay algunos pasos que usted puede tomar para mitigar ambas situaciones. Por ejemplo, si fabrica drones de gran tamaño, proporcione orientación e información, dando instrucciones a los usuarios para que no los utilicen en los casos en que un dron más pequeño pueda ser suficiente. Si desea construir drones más pequeños debido a su peso ligero y a la menor probabilidad de herir a las personas, utilice otros medios para que los drones se noten, tales como diseños de colores, señales de luz o sonido. Combine esto con proporcionar información sobre su uso e instruya a los usuarios para que no operen los drones de manera oculta. El tema de la información a los usuarios se detallará más adelante cuando se hable del embalaje de los drones.

Sonido de los drones

Algunas personas reportan sentirse amenazadas por el sonido y el viento producido por los drones. Aunque un dron más ruidoso podría ser más fácil de notar para las personas en el suelo, no se recomienda el uso de drones ruidosos. Podrían causar molestias a las personas no involucradas y dar lugar a sentimientos de malestar. Estas consideraciones se han reconocido en el Reglamento delegado sobre drones y el nivel máximo de potencia acústica ejercido por los drones, en el momento de su comercialización, se ha fijado en 85 dB(A) para los drones de las clases C1 y C2.[22]

Ubicación de la cámara

Las personas también pueden sentirse incómodas cerca de los drones debido a que no saben dónde se encuentra la cámara o incluso si el mismo está equipado con una cámara. Debido a que las cámaras de los drones son pequeñas, es posible que no se noten fácilmente. Esto podría dificultar que las personas en el suelo sepan si la cámara está apuntando en su dirección o no.[23] Puede remediar esto haciendo que las cámaras sean claramente visibles, por ejemplo, llamando la atención sobre ellas a través de los colores brillantes que rodean al objetivo de la cámara.

Falta de información sobre la carga útil

La falta de una indicación externa en el propio dron sobre si los sensores de la carga útil están funcionando y capturando información o la falta de comprensión por parte del público en general de cómo interpretar tales señales puede hacer que las personas se sientan observadas aunque no

[21] Ver Chang *supra* n 3, p. 7.
[22] Parte 15 del anexo del proyecto de Reglamento delegado de la Comisión sobre drones.
[23] Véase Chang *supra* n 3, págs. 8-9.

lo estén.[24] Las personas en tierra pueden sentirse vulnerables cuando hay un dron en sus inmediaciones si no tienen forma de saber si la carga útil está activada, por ejemplo, si una cámara está grabando o si ni siquiera está encendida. Aquí nos referimos a los sensores de carga útil que tienen por objeto recoger datos para cumplir el propósito del vuelo, y no simplemente a los sensores que se necesitan para operar y garantizar un vuelo seguro y estable, como los estabilizadores de giroscopios.

Usted podría mitigar esta situación incorporando una señal visual para permitir conocer a la gente alrededor del dron que sus sensores están activados y capturando datos. Esto podría incluir una luz parpadeante de un solo color o un cambio de color. Incluir en el folleto informativo una guía sobre cómo los pilotos y operadores pueden utilizar estos sensores de retroalimentación y aconsejarles que difundan información a las personas que se encuentren en las proximidades sobre esta función y su significado.

Hardware Dron (cargas útiles y capacidades) y privacidad

Las cargas útiles de los drones, que incluyen sensores y permiten capturar datos, podrían dar lugar a problemas de privacidad entre las personas que se encuentran en tierra. Al capturar datos, como imágenes, sonido, geolocalización y otros, un dron podría interferir con la privacidad de las personas sobre el terreno, especialmente si los datos capturados permiten la identificación de las personas (lo que en tal caso es calificado como tratamiento de datos personales en términos del RGPD)[25]. La difuminación de los rostros de las personas no siempre garantiza evitar tal identificación en contextos que contienen otros detalles, como los números de las casas o de las matrículas de los coches. Por lo tanto, se recomienda que usted, como fabricante, considere con qué tipo de características y capacidades de hardware debe estar equipado un dron.

Proporcionalidad en el diseño de los drones

Las diferentes capacidades y cargas útiles pueden dar lugar a diferentes problemas de privacidad, dependiendo del tipo de información que capturen. Una combinación de estas cargas útiles o capacidades podría llevar especialmente a la materialización de riesgos potenciales para la privacidad, por ejemplo, una combinación de imágenes o vídeos capturados con la ubicación y la hora precisas podrían menoscabar más fácilmente la privacidad de las personas capturadas, ya que podría permitir el seguimiento del paradero y las actividades de las personas. Encuentre un breve análisis en la tabla siguiente:

Carga útil / Capacidad	Impactos potenciales sobre la privacidad
Cámara con zoom	Privacidad del cuerpo Privacidad de datos e imagen Privacidad del comportamiento y de la acción Privacidad de asociación Privacidad de los pensamientos y sentimientos *(dependiendo del contexto)*
Cámara térmica / infrarroja	
Cámara NDVI multiespectral	
Cámara de alta resolución	
Sensores LIDAR (láser)	
Capacidad de reconocimiento facial	
Otras herramientas de captura de imágenes	
Capacidad de ver en primera persona	

[24] Ver Chang *supra* n 3, p. 9.
[25] Véase Finn *supra* n 14, pág. 6.

Alcance y resistencia ampliados	Deshumanización de los vigilados y falta de responsabilidad proactiva del operador/piloto
Micrófono direccional	Privacidad de la comunicación personal Privacidad de los pensamientos y sentimientos Privacidad del comportamiento y de la acción Privacidad de la asociación
Galileo, GPS u otros sensores de geolocalización	Privacidad de la ubicación y el espacio
Capacidades de reconocimiento automático de matrículas (ANPR)	Privacidad de la ubicación y el espacio (*cuando se aplica a las matrículas de los automóviles, por ejemplo)*
Antenas de telecomunicación, conexión satelital o capacidades de router WiFi	Privacidad de la comunicación personal
Pulverizadores utilizados para la distribución de sustancias en la agricultura	Ninguno
Detectores de gas	Ninguno

Cuando diseñe y construya un dron, considere qué tipo de sensores son apropiados para él y para qué tipo de operaciones será utilizado, dependiendo del tipo de clientes que vayan a utilizar el dron. Considerar, además, la calidad de los datos que deberían ser capaces de capturar y consevar. La calidad de las imágenes capturadas no siempre permite la identificación de las personas registradas. No sería proporcionado instalar una cámara muy potente con gran capacidad de zoom en un dron destinado a ser un juguete para niños, por ejemplo. Si es posible, trate de ejercer su mejor juicio a la hora de decidir qué capacidades se adaptan al dron, por supuesto, teniendo en cuenta sus propios intereses legítimos como fabricante y como empresario privado.

Como fabricante, sus productos tendrán que competir en el mercado sobre la base de las características de los drones que usted ofrece, incluyendo la calidad de sus sensores. Por lo tanto, el uso de sensores de menor calidad puede no ser siempre su elección. Es importante que cuando los drones estén equipados con sensores más potentes, también estén equipados con mejores medidas de mitigación. Estas podrían ser características de software que permiten limitar qué datos se recopilan y cuándo, o que permiten que los datos innecesarios se borren automáticamente. Las salvaguardas del software se discutirán con más detalle más adelante en este documento.

Además de la relación entre los diferentes sensores y los tipos de privacidad afectados, cabe señalar que se considera que los diferentes tipos de información recopilada interfieren con la privacidad en distinta medida. Por ejemplo, las grabaciones visuales de las actividades de las personas y las grabaciones sonoras de sus conversaciones tienen un mayor impacto en su privacidad que los simples registros de la ubicación de una persona. Del mismo modo, una secuencia de vídeo continua tiene un mayor impacto que un conjunto de imágenes individuales. Por último, la grabación de secuencias de vídeo o imágenes tiene un mayor impacto que el streaming en directo.

La mayoría de los drones probablemente requerirán algún tipo de carga útil y esto es especialmente cierto para los drones usados para aplicaciones comerciales. Además de elegir las

cargas útiles más apropiadas, usted puede mejorar la conciencia de privacidad de los drones al permitir que los usuarios de drones controlen fácilmente (1) qué sensores de drones utilizan, (2) cuándo están activados los sensores de drones y (3) qué calidad de sensores de drones utilizan / qué calidad de datos de drones recopilan.

Control de la carga útil y del sensor

Durante las fases de planificación y ejecución de la operación con drones, los pilotos y operadores tendrán que considerar y planificar cómo minimizar su interferencia con la privacidad de las personas y recopilar la menor cantidad posible de datos personales. Como recomendación general, los drones equipados con software que permite un control preciso de los sensores de carga útil pueden mejorar la capacidad de los usuarios de drones para cumplir con este requisito.

Se recomienda que los drones estén equipados con capacidades de software que permitan a los usuarios controlar qué sensores de carga útil deben activarse y desactivarse durante un vuelo, adaptando eficazmente las capacidades de los drones a lo que sea necesario para su funcionamiento. Además, debe incorporar controles fáciles de usar para encender y apagar los sensores durante el vuelo. Este software podría adaptarse para permitir el acoplamiento de los sensores dentro de una zona de vuelo concreta o durante diferentes partes de un vuelo. Además, el software podría permitir a los usuarios predefinir y documentar el uso de los sensores / capacidades en un vuelo planeado previamente. Esto ayudaría a los pilotos y operadores a recoger fácilmente sólo los datos que necesitan, haciendo así que sus actividades sean más respetuosas con la normativa europea sobre privacidad y protección de datos. Esto puede ayudar a los operadores y a los pilotos a recopilar la menor cantidad posible de datos personales sobre las personas en tierra.

Además de adaptar los sensores utilizados, sería beneficioso para los usuarios poder controlar la calidad de los datos recogidos por dichos sensores. Si está desarrollando un dron comercial de alta calidad, es posible que desee equiparlo con sensores de la más alta calidad disponible. Naturalmente, estas capacidades serían la mejor opción para una entidad comercial, ya que permitirían llevar a cabo una amplia gama de operaciones. Sin embargo, unos pocos controles de software podrían permitir fácilmente a los usuarios elegir manualmente la calidad de los datos que desean capturar para cada vuelo individual, ya sea antes o durante el vuelo.

Capacidades de comunicación

Además de otras capacidades, los drones están equipados con hardware que les permite comunicarse con diferentes dispositivos utilizando diferentes canales debido a una gran variedad de razones, incluyendo garantizar la seguridad del vuelo y habilitar otras características de los drones. Las capacidades de comunicación son especialmente necesarias para:

- el control de los drones mediante equipos de pilotaje,
- los datos capturados por el dron,
- coordinar las trayectorias de vuelo con drones en el mismo espacio aéreo, por ejemplo, en el contexto de los sistemas de gestión del tráfico de los vehículos aéreos no tripulados (UTM),
- garantizar la actualización de las bases de datos de los espacios geo-cercados,
- comunicar datos de identificación electrónica por dron.

Es probable que se desarrollen normas pertinentes a nivel internacional o europeo para garantizar la interoperabilidad de los drones con los diferentes sistemas de información; sin embargo, esto

todavía está en fase de desarrollo. Con respecto a la UTM, actualmente hay muchos proyectos en curso para probar diferentes formas de comunicación entre drones.[26] No obstante, se anima a los fabricantes a seguir de cerca la evolución de los requisitos de comunicación y a seguir las normas pertinentes cuando estén disponibles para permitir la interoperabilidad, así como para garantizar la seguridad de los enlaces de datos que transmiten información, como se explica más adelante.

Características del software de mejora de la privacidad del dron

Ciertas capacidades de software pueden ayudar a incorporar consideraciones de privacidad en el diseño y la construcción de los drones y aumentar el control que ejercen los usuarios sobre la interfierencias con la privacidad de los que se encuentran en tierra. Esta sección examinará tales características y capacidades que mejoran la privacidad del software.

Capacidades de geoconsciencia

Una forma de mejorar el respeto de la privacidad es impedir que los drones entren en zonas restringidas. Los Estados miembros podrán definir zonas de exclusión aérea para los drones y tendrán que mantener bases de datos con la ubicación de dichas zonas.[27] Una forma de señalar estas zonas es mediante el establecimiento de geo-cercado - fronteras virtuales que identifican zonas libres de drones.[28] Para responder a esta situación, los drones de las categorías C1, C2 y C3 deberán estar dotados de capacidades de geoconsciencia, que alerten a los pilotos u operadores cuando vuelen en zonas restringidas de exclusión aérea.[29] Los requisitos para el sistema de geoconsciencia, que se proponen actualmente, son los siguientes

- Una interfaz para cargar y actualizar datos sobre las limitaciones del espacio aéreo de forma segura,
- una alerta de advertencia cuando se detecte una posible violación de las limitaciones del espacio aéreo, y
- Información sobre el estado del dron y una alerta cuando la posición o navegación del dron no pueda funcionar correctamente.

Si equipa el dron con capacidades de geo-cercado / sistema de control de vuelo, asegúrese de que funciona sin problemas, sin poner en peligro la seguridad del vuelo, y proporciona información al piloto cuando las capacidades de geoconsciencia no puedan funcionar correctamente[30]. Además, la eficacia de las capacidades de geo-consciencia depende de que drones tengan acceso a las bases de datos más recientes y precisas sobre espacios aéreos restringidos. Es importante garantizar que los drones reciban las actualizaciones oportunas y seguras sobre el geo-cercado y las zonas de no vuelo.[31] Debe establecerse una interfaz para cargar y actualizar dichos datos que

[26] Eurocontrol, UTM Current State-of-the-Art. https://www.urocontrol.int/articles/utm-current-state-art
[27] Artículo 15 del Reglamento de ejecución (UE) 2019/947 de la Comisión de 24 de mayo de 2019 relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0947&from=EN).
[28] Gettinger, Dan y Arthur Holland Michel, "Drone Sightings and Close Encounters: An Analysis", Center for the Study of the Drone, Bard, College, diciembre de 2015, p. 17 http://dronecenter.bard.edu/files/2015/12/12-11-Drone-Sightings-and-Close-Encounters.pdf
[29] Parte 2.13, parte 3.15, parte 4.10 del anexo del proyecto de Reglamento delegado de la Comisión sobre drones.
[30] Parte 2.13, letra c), parte 3.15, letra c), y parte 4.10, letra c), del anexo del proyecto de Reglamento delegado de la Comisión sobre drones.
[31] Kruse, Brandao, Jacques y Eva Schulz-Kamm, "Security and Privacy by Design: Securing the Future of UAVs", 2016, p. 4. https://rpas-civops.om/wp-content/uploads/2016/11/NXP-Semiconductors_DE_WP.pdf

garantice la calidad, integridad y validez de los datos utilizados.[32] Para reforzar esta función, considere la implementación de controles de software que eviten que el dron despegue si su base de datos de zonas geocercadas o sin vuelo no está actualizada.

Además de limitar el acceso de los drones a las zonas de exclusión de aérea restringida a nivel nacional, la gente puede desear mantenerlos alejados de sus lugares de trabajo o domicilios privados. Del mismo modo, las instituciones pueden considerar inapropiado el vuelo de drones en sus inmediaciones, en particular si los edificios son de naturaleza delicada, como edificios religiosos, escuelas y guarderías, instalaciones militares, comisarías de policía, cárceles o juzgados, hospitales y clínicas, etc. - todos los lugares que puedan merecer o merezcan un nivel especial de protección debido a la sensibilidad de la información que un dron pueda captar. Anteriormente existían iniciativas privadas que permitían a los particulares designar zonas como restringidas a los drones. De hecho, ha habido intentos de utilizar el posicionamiento Wi-Fi para implementar barreras de drones virtuales.[33]

Estas iniciativas son bien recibidas y se fomenta la participación de los fabricantes en ellas. Los fabricantes pueden actuar como intermediarios entre dichas plataformas y los usuarios permitiendo la interoperabilidad entre los drones y dichas iniciativas, o incluso poner en marcha un sistema propio que permita a los particulares designar su propia zona de exclusión aérea. Estas iniciativas pueden ayudar a los operadores y pilotos a operar drones cumpliendo en mayor medida los requisitos de privacidad y protección de datos, y podrían servir de marca de calidad para los drones dotados de dichas capacidades.

Esas capacidades podrían ampliarse para aumentar la capacidad de respetar los deseos y, por extensión, la intimidad de las personas sobre el terreno. Una parte fundamental del respeto a la privacidad puede ser el respeto a la voluntad de las personas de no ser grabadas. De este modo, la base de datos de ubicaciones geocercadas podría ampliarse o complementarse con bases de datos adicionales, que permitirían a los particulares determinar sus hogares y jardines como zonas de exclusión aérea para los drones.

Por último, las capacidades de geoconsciencia podrían ampliarse a capacidades de geo-cercado, que no sólo alerten a los pilotos cuando un dron entra en un espacio restringido, sino que también impiden que un dron entre en ese espacio en primer lugar, al tiempo que garanticen la estabilidad y la seguridad del vuelo.

Identificación directa a distancia

El funcionamiento de los drones puede plantear algunas cuestiones de responsabilidad y transparencia, ya que es posible que la gente no siempre sepa quién está operando un dron o con qué propósito, ni a quién dirigirse con más preguntas. Un nuevo requisito propuesto mencionado en el Reglamento delegado sobre drones es que las aeronaves no tripuladas de las clases C1, C2 y C3 estén equipadas con un sistema de identificación a distancia, destinado a contrarrestar esta situación y a aumentar la transparencia de las operaciones. Este sistema debería:[34]

[32] Parte 2.13, letra a), parte 3.15, letra a), y parte 4.10, letra a), del anexo del Reglamento delegado de la Comisión sobre drones.
[33] May, Patrick,'Virtual Barriers, Manipulation Tools Enlisted to Keep Drones at Bay', Government Technology, 17 de agosto de 2016. http://www.govtech.com/public-safety/Virtual-Barriers-Manipulation-Tools-Enlisted-to-Keep-Drones-at-Bay.html
[34] Parte 2.12, parte 3.14 y parte 4.9, parte 6 del anexo del Reglamento delegado de la Comisión sobre drones.

- Permita cargar el número de registro del operador del SANT de conformidad con el articulo 14 del Reglamento de Ejecución (UE) 2019/947 y únicamente aplicando el proceso proporcionado por el sistema de registro;
- Garantice, en tiempo real durante toda la duración del vuelo, la difusión periódica directa desde la ANT utilizando un protocolo de transmisión abierto y documentado de los datos siguientes, de manera que puedan ser directamente recibidos por dispositivos móviles existentes dentro de la gama de difusión:
    - El número de registro del dron,
    - El número de serie físico único del dron que cumpla la norma ANSI/CTA-2063,
    - La posición geográfica del dron y su altura por encima de la superficie o el punto de despegue;
    - la trayectoria medida en el sentido de las agujas del reloj a partir del norte geográfico y la velocidad de la ANT respecto al suelo; y
    - La posición geográfica del piloto a distancia o, si no se dispone de ella, el punto de despegue.
- garantice que el usuario no pueda modificar los datos mencionados en el apartado b), incisos ii, iii, iv y v.

Además de ser una parte fundamental de un futuro sistema UTM, la transmisión de identificación electrónica podría ayudar a informar a los responsables del dron al emitir el número de registro del operador y, al informarles del punto de despegue del dron, podrían informarles sobre dónde podrían (potencialmente) encontrar al personal de pilotaje que pudiera responder a sus preguntas y escuchar sus preocupaciones.

Las transmisiones de identificación a distancia deben realizarse en la banda de frecuencias de 2,4 ó 5 GHz, utilizando un protocolo de transmisión abierto y documentado.[35] Deben ser recibidas por los dispositivos móviles dentro del rango de transmisión, permitiendo a las autoridades y a las personas en tierra el acceso a la información sobre quién está operando el dron (el operador) y dónde pueden obtener más información (el punto de despegue). Esto aumentaría la transparencia y la responsabilidad de las operaciones.

Por último, los fabricantes que adopten la transmisión de identificación a distancia también podrían considerar cómo proteger y mejorar la información que pueda emitirse a través de esta capacidad. Para proteger dicha información, utilice medidas de seguridad que impidan su modificación no autorizada. Para mejorarlo, los fabricantes podrían incluir un campo en el que los operadores o pilotos pudieran incluir un mensaje a la gente de su entorno, como una breve introducción de la operación del dron, su propósito general o una referencia a un sitio web con información más detallada. Como fabricante, se le anima a pensar en las formas en que los drones podrían mejorar las capacidades del operador y del piloto para informar a las personas que los rodean de sus actividades.

Registros de vuelos y actividades

Para ayudar a asegurar la responsabilidad de los usuarios de drones y la transparencia de sus operaciones, puede configurar los drones para que almacenen (al menos temporalmente) cierta información operativa, como la fecha y hora de las últimas descargas de geo-cercado o de las

[35] *Ibídem.*

trayectorias de vuelo, así como las trayectorias usadas y cuando se activaron los sensores de carga útil. Esto podría servir como prueba de la diligencia (o negligencia) de los pilotos y operadores de drones.

También puede ayudar a asegurar la responsabilidad de los pilotos y operadores de drones implementando una interfaz que registre y rastree la secuencia de comandos realizados, así como las acciones y cambios en el sistema.[36] Por ejemplo, cuando se pueden personalizar y alterar ciertas funciones de los drones, se puede guardar información sobre cuándo se ha hecho y, si es posible, determinar por quien a través de controles de acceso.

Minimización automatizada de datos

Una vez recogidos los datos personales, considere los medios para minimizarlos dentro del sistema del dron. Esto puede ser posible, por ejemplo, si utiliza un software que detecte automáticamente los rasgos faciales y/o los números y los borre, siguiendo instrucciones específicas. Esto podría ayudar a los pilotos y operadores a cumplir la legislación sobre protección de datos en la Unión Europea.[37]

Otra salvaguarda que puede aplicar en este contexto podría ser la utilización de un software que borre automáticamente todos los datos recogidos y almacenados después del final de un vuelo y después de que los datos se hayan descargado con éxito a otro dispositivo. Considere cómo desarrollar mejor esta característica, por ejemplo, cómo permitir que los usuarios se puedan apartar de ella. Preste especial atención a qué tipo de datos pueden ser razonables para mantenerlos durante períodos de tiempo más largos, tal vez con fines de responsabilidad y prueba del cumplimiento de la ley por parte de los usuarios de los drones. Usted podría permitir a los operadores y a los pilotos determinar qué datos se eliminan, cuales se retienen y en qué momento a través de la interfaz del dron.

Por último, a veces los drones pueden capturar y recoger datos potencialmente personales a través de sensores, destinados a la seguridad de su vuelo. Por ejemplo, la seguridad del dron puede mejorarse mediante la incorporación de sistemas de"detectar y evitar" en el avión no tripulado que le permitan prevenir accidentes y colisiones en tiempo real mediante el uso de sensores para detectar, rastrear y evitar obstáculos alrededor del avión no tripulado, de forma muy similar a como lo haría un piloto humano[38]. Podría considerar cómo desarrollar o elegir un sistema apropiado para "sentir y evitar", que minimice automáticamente los datos capturados a lo que es estrictamente necesario para evitar colisiones y accidentes - a los contornos de objetos y personas.[39] Esto contribuiría a la capacidad de un dron para descartar datos innecesarios y minimizar la posible interferencia con la privacidad de las personas.

Seguridad digital y protección de datos del dron

La seguridad puede desempeñar un papel clave en la protección de los drones, sus controles y los datos que almacenan y transmiten. La seguridad de la información y de las tecnologías de la información es un requisito previo fundamental para la protección de los datos capturados por un

[36] Ver Altawy *supra* n 2, p. 15.
[37] El artículo 5, apartado 1, letra c), del Reglamento 2016/679 (Reglamento general de protección de datos) exige específicamente que sólo se recojan y traten los datos personales que sean "adecuados, pertinentes y limitados a lo necesario en relación con los fines" del tratamiento.
[38] Véase Gettinger, *supra nota* 27, pág. 18.
[39] Vivet, Laura y Lauren Smith, "Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft", Future of Privacy Forum, 2 de agosto de 2016, p. 4. https://fpf.rg/wp-content/uploads/2016/08/Drones_and_Privacy_by_Design_FPF_Intel_PrecisionHawk.pdf

dron y la privacidad de las personas. Un sistema de seguridad poco efectivo podría permitir que los controles de los drones fueran manipulados por personas no autorizadas y que se utilizara un dron para vigilar a las personas sin que los responsables fueran detectados. Además, el acceso a los datos almacenados o transmitidos por el dron, podría afectar a la intimidad de las personas capturadas y podría dar lugar a una brecha de seguridad, lo que daría lugar a una serie de procesos que los usuarios deberían seguir en virtud del RGPD. Por lo tanto, la seguridad desde el diseño debe intentar implantarse junto con la privacidad desde diseño, garantizando la seguridad de la información y de las tecnologías de la información durante todo el ciclo de actividades de los drones.

Algunos elementos concretos de seguridad pronto se convertirían en requisitos legales. Por ejemplo, en el Reglamento delegado sobre drones, los drones de clases C1, C2 y C3 deben estar equipados con salvaguardas para protegerlos en caso de pérdida de enlace de datos. En tales casos, es necesario que existan medios fiables y predecibles para recuperar el enlace de datos o finalizar el vuelo de forma que se reduzca al mínimo cualquier impacto a terceros en el aire o en tierra[40]. Este impacto podría incluir impactos en la privacidad. Por lo tanto, los fabricantes deben considerar qué salvaguardas pueden ser apropiadas. Por ejemplo:

- El aterrizaje en lugares no planificados podría evitarse equipando un dron con una función para volver automáticamente a su punto de despegue en caso de emergencia y errores, o para volver y volar en un lugar anterior mientras se restablece la conexión de enlace de datos,
- El acceso no autorizado a los datos almacenados localmente en el dron, cuando aterriza en ubicaciones no planificadas, puede evitarse mediante controles de acceso (que podrían configurarse temporalmente para la operación concreta) o mediante el cifrado de los datos.

Además, el proyecto de Reglamento propuesto sobre drones prevé que los drones de la clase C2 deben estar equipados con un enlace de datos protegido contra el acceso no autorizado a las funciones de mando y control.[41] Este requisito se orienta principalmente a garantizar la seguridad del vuelo, aunque también podría proteger la privacidad al impedir el uso irresponsable de los drones para la recogida de datos por parte de personas no autorizadas. Este requisito podría ampliarse para proteger un enlace de datos del acceso no autorizado y de las imágenes transmitidas entre el dron y el equipo de mando y control, ya que esto podría interferir con la privacidad de los que se encuentran en tierra.

La seguridad es una consideración fundamental en la construcción de los drones. Se requiere un enfoque global, que la considere como parte de cada función y del equipo del dron. Se anima a los fabricantes a que presten la debida atención a esta cuestión. Por supuesto, también se debe tener en cuenta que puede haber normas legales sobre una determinada tecnología de almacenamiento y/o transmisión con la que un dron debe estar equipado. Esto puede ser más claro a medida que se avanza en la regulación de un sistema de UTM, por ejemplo, y debe cumplirse a medida que se aclara. Sin embargo, hay otros pasos que los fabricantes ya pueden dar ahora.

Por ejemplo, la utilización de componentes que cumplan las normas de seguridad o los sistemas de certificación podría ser un paso para garantizar la seguridad de los datos y la comunicación y podría servir como indicador de la calidad de la construcción final del dron y como elemento que

[40] Parte 2.7, parte 3.7, parte 4.5 del anexo del proyecto de Reglamento delegado de la Comisión sobre drones.
[41] Parte 3.8 del anexo del Reglamento delegado de la Comisión sobre drones.

contribuya a su seguridad y, por extensión, a su capacidad para proteger los datos personales tratados a través de él. El uso de componentes certificados también puede ser considerado como una característica distintiva de calidad y como información adicional para los operadores y los pilotos a considerar cuando planifican o ejecutan vuelos. Aquí hablamos de esquemas generales de certificación de seguridad de la información, sin embargo, como algunos drones están conectados a Internet, pueden ser vistos como dispositivos del Internet de los objetos ("*internet of things*") y también pueden beneficiarse de dicha certificación.

Ofreciendo una visión más general, en la siguiente tabla puede encontrar un análisis de los riesgos relevantes para la seguridad de la información que pueden surgir en las diferentes etapas de la funcionalidad del dron y ejemplos de salvaguardas que se pueden implementar para eliminar o mitigar estos riesgos.[42]

	Riesgo potencial	Posibles salvaguardas
Garantía general de la seguridad de la información y de las tecnologías de la información	Se puede utilizar hardware o software malicioso para atacar tanto el dron como los sistemas de control en tierra.[43] Esas vulnerabilidades podrían dar lugar a la pérdida de datos confidenciales o a la pérdida de control sobre los drones mientras están en funcionamiento, lo que podría plantear problemas de privacidad y seguridad.	Debe garantizarse la seguridad de toda la cadena de suministro de software y componentes que se utilizan para fabricar un dron. Asegúrese de que la actualización o parcheo del software no interfiera con el funcionamiento del dron, especialmente durante el vuelo. El uso de cortafuegos, sistemas antivirus y sistemas de detección de intrusos puede ser un paso fundamental hacia la seguridad del dron.
Vuelo del dron, tanto cuando se opera de forma autónoma como manual	Las vulnerabilidades de seguridad de la información y de las tecnologías de la información en el sistema de control en tierra del dron o en la transmisión de información y órdenes entre el dron y su punto de control podrían permitir a personas no autorizadas tomar el control del dron o perturbar su funcionamiento normal. Esto podría suscitar preocupación sobre la privacidad de las personas sobre el terreno, ya que este sujeto no autorizado sería desconocido para ellos, pero también podría plantear problemas de seguridad debido a los daños físicos y a los daños que podrían causar a los drones.	La instalación de controles de autorización en el sistema de control en tierra podría ayudar a limitar el acceso y control no autorizados o la interferencia no autorizada con las características y ajustes del dron.

[42] Ver Altawy *supra* n 2.
[43] Un ejemplo de malware específico de un avión no tripulado es Maldrone, que permite a un atacante tomar el control de un avión no tripulado e inyectar información en las comunicaciones de control de vuelo al avión no tripulado y en las lecturas de los sensores enviadas por el avión no tripulado.

	Dado que los sistemas mundiales de navegación por satélite (GNSS), como Galileo, GPS o GLONASS son señales de libre acceso, no codificadas y no autorizadas, un dron podría recibir señales GNSS engañosas para alterar sus cálculos de coordenadas geográficas.[44] Esto podría llevar a que un dron cambie su ruta de vuelo y podría plantear problemas de privacidad y seguridad, en particular cuando el dron está funcionando de forma autónoma.	Las características de los programas informáticos capaces de detectar señales GNSS falsas deben incorporarse al producto. Se recomienda una función de interfaz mediante la cual se pueda restaurar fácilmente el control manual y anular el funcionamiento autónomo.
	Las señales GNSS también podrían interferir. Esto interrumpiría la conexión entre el dron y la navegación externa, lo que llevaría a que el dron se desorientara y se estrellara potencialmente.[45]	Podrían considerarse medios alternativos de navegación, como las preguntas visuales y de inercia y la necesidad de que los pilotos y operadores presten atención a la puesta en marcha manual. El uso de receptores GNSS para más de un sistema también puede mitigar el riesgo de ataques GNSS.
Recogida y tratamiento de datos	La operación y el funcionamiento de drones podrían ser atacados inyectando datos de sensores falsos en el controlador de vuelo. Este tipo de ataque puede afectar a todos los tipos de sensores de drones, incluyendo los de radar, infrarrojos y electro-ópticos.	Un dron podría utilizar procedimientos operativos alternativos para comparar los datos recibidos a través de diferentes sensores y lecturas de comprobación cruzada. Esto podría permitir que el dron tolere el mal funcionamiento de los componentes o la información infectada.
Transmisión de datos entre el dron y otros dispositivos (por ejemplo, el sistema de control)	Los flujos de datos en tiempo real pueden ser pirateados e interceptados, especialmente si no están encriptados o protegidos. Esto puede poner en peligro la privacidad de las personas capturadas, así como la seguridad de la propia operación al no controlar el acceso a los datos clave.	La incorporación de la autenticación mutua continua entre el operador y el dron puede ayudar a autenticar la comunicación. El cifrado podría ayudar a proteger estos datos. El uso de claves de seguridad para autenticar la conexión y las transmisiones puede garantizar su seguridad.
Datos almacenados en el dron	Al explotar la información y las vulnerabilidades de seguridad, el personal no autorizado puede acceder a los datos almacenados en un dron.	Use encriptación para asegurar que los datos almacenados estén protegidos.

[44] Ver Altawy *supra* n 2, p. 9.
[45] *Ibídem.*

	Esto podría ocurrir en caso de accidente del dron, así como explotar las vulnerabilidades del hardware y software del dron. Esto podría plantear problemas de privacidad para las personas cuyos datos se capturan.	Implementar controles de acceso al propio dron que requieran autorización para acceder a los datos. Incorpore capacidades para detectar brechas de seguridad y alarmar a los usuarios.

Embalaje del dron y privacidad

Proporcionar información a los pilotos y operadores de drones

Como parte de su papel como fabricante de drones, se le pedirá que proporcione cierta información a sus consumidores, incluyendo, dependiendo de la clase de su dron, cómo operarlo, sus características específicas, limitaciones y controles, así como los riesgos de operar drones. Existe un amplio consenso entre los expertos en que la sensibilización de los usuarios de drones sobre las normas y directrices del espacio aéreo para un funcionamiento responsable de los drones es un paso clave para lograr vuelos seguros y protegidos.[46] Además, informar a los usuarios de las capacidades y características precisas del dron y de cómo utilizarlo puede permitirles ponerlo en práctica de manera que contribuya a su funcionamiento de acuerdo con los requisitos de minimización de datos y el respeto a la privacidad.

A nivel básico, todas las clases de drones deben incluir instrucciones suficientes en el embalaje para permitir que los pilotos remotos controlen el dron de forma segura[47]. Además, también hay que incluir más información para algunas clases de drones. Los drones C0 (menos de 250 g MTOM) y los C4 (modelos de aeronaves) deben ir acompañados de material informativo que incluya un conjunto de instrucciones claras de funcionamiento, las características técnicas del dron y sus limitaciones, y que destaque los riesgos relacionados con su operación.[48] Drones más grandes para uso general - Los drones C1, C2, C3 también deben venir con un manual de usuario que agregue más detalles de información, incluyendo la funcionalidad de las características de geo-consciencia, mantenimiento e instrucciones para la resolución de problemas.[49] Los riesgos señalados en dichos documentos deben adaptarse a los drones concretos y a los usuarios previstos para los mismos. Estos riesgos pueden incluir riesgos para la privacidad.

Al proporcionar orientación detallada a los usuarios sobre cómo volar el dron, preste atención a la introducción de todas las características, especialmente aquellas relevantes para la privacidad: controles y compromiso de los sensores, seguridad de los datos y encriptación, controles de acceso relevantes. Además, para garantizar la claridad, toda la información facilitada a los usuarios debe ofrecerse en un lenguaje accesible y apropiado, teniendo en cuenta a los posibles usuarios.

Por último, también se exigirá a los fabricantes que incluyan una nota informativa aprobada por la EASA en el embalaje de su dron. Esta nota informativa introducirá a los usuarios a las limitaciones y obligaciones aplicables al funcionamiento del dron[50]. A este respecto, en el sitio

[46] Véase Gettinger, *supra nota* 27, pág. 19.
[47] Parte 1.4, parte 2.4, parte 3.3, parte 4.3 del anexo del Reglamento delegado de la Comisión sobre drones.
[48] Parte 1.8, parte 5.3 del anexo del Reglamento delegado de la Comisión sobre drones.
[49] Parte 2.18, parte 3.19, parte 4.15 del anexo del Reglamento delegado de la Comisión sobre drones
[50] Parte 1.9, parte 2.19, parte 3.20, parte 4.16, parte 5.7 del anexo del Reglamento delegado de la Comisión sobre drones.

web de la AESA ya se puede encontrar una serie de propuestas de carteles de información al consumidor, aunque no son definitivos.[51]

Además, cuando considere que la información adicional al folleto aprobado por la EASA puede ser pertinente o apropiada, le recomendamos que considere la posibilidad de proporcionar folletos informativos adicionales con información clave sobre los riesgos para la privacidad, la seguridad y el seguro, así como recomendaciones sobre cómo operar los drones de manera responsable. Para una mejor medición, sería beneficioso que incluyera también un enlace al sitio web de DroneRules PRO. En el anexo de este documento encontrará folletos que podrá utilizar fácilmente. Estos folletos están destinados a complementar y no a sustituir a los folletos aprobados por la AESA.

Etiquetado de los drones

Del mismo modo, los operadores y los pilotos deben estar al tanto de los detalles del dron que están operando para planificar mejor sus operaciones y comprobar sus capacidades. Es evidente que marcar un dron a tal efecto podría ayudarles en este sentido. Cuando un dron cumpla los requisitos técnicos y de seguridad pertinentes establecidos en el proyecto de Reglamento propuesto para una clase determinada, deberá etiquetarse claramente a tal efecto. Este es un requisito para todas las clases de drones, destinados a ser utilizados en operaciones de categoría "abierta", e incluye una etiqueta del tipo de clase (es decir, C0, C1, C2, C3 o C4), así como una marca de certificación CE.[52]

Además, se debe proporcionar un número de serie único, que cumpla con la norma ANSI/CTA-2063 y debe colocarse en el dron y en el manual del usuario (o en el embalaje) de manera legible para los C1, C2 y C3[53]. Esta información puede ayudar a los operadores a registrar sus drones, cuando sea necesario, y formará parte de la información transmitida por el sistema de identificación electrónica del dron, mejorando la transparencia y la responsabilidad de los vuelos.

Por último, como ya se ha mencionado anteriormente, también pueden tomarse medidas y se puede observar el uso de componentes que cumplen con los esquemas de estandarización o certificación de seguridad para que sus usuarios potenciales puedan distinguir la calidad del dron y se proporcione así una forma fácil de comprobar y de hacer referencia a las características de seguridad relevantes del dron.

[51] EASA, "Flying a Drone - do's and don'ts", Proposed Consumer Information, 2018. https://www.easa.europa.eu/sites/default/files/dfu/217307_EASA_DRONE_POSTER_2018%20final.pdf

[52] Artículo 16, proyecto de Reglamento delegado de la Comisión sobre drones. Parte 1, Parte 2, Parte 3, Parte 4, Parte 5 del anexo.

[53] Parte 2.11, parte 3.13, parte 4.8, parte 5.5 del anexo del proyecto de Reglamento delegado de la Comisión sobre drones.

Cómo aplicar estos principios en la práctica

La aplicación de los principios y características anteriores en la práctica puede parecer abrumadora y confusa al principio. Por esta razón, sugerimos un enfoque paso a paso utilizando una metodología de Evaluación del Impacto sobre la Privacidad: comprender las operaciones previstas o previsibles, identificar los riesgos y, a continuación, considerar las salvaguardas adecuadas y la forma de aplicarlas (hay que tener en cuenta que una Evaluación de Impacto de la Privacidad no es una Evaluación del Impacto sobre la Protección de Datos (PIA), siendo esta última exhaustiva y con el objetivo de dar cumplimiento a lo dispuesto en el artículo 35 del RGPD). Puede utilizar las siguientes preguntas para ayudar a estructurar sus actividades de planificación. Adapte estas preguntas al dron específico que está fabricando y considere cómo se puede utilizar. Puede realizar preguntas adicionales que considere relevantes para sus actividades.

	Características del dron	Recogida de datos	Conservación de datos	Tratamiento de datos	Borrado de datos
Mapas de datos	**Entender el contexto en el que se mueve su dron** ¿Qué es tu dron? ¿Para qué está diseñado? ¿Cuáles son los escenarios probables en los que operará? ¿En qué categoría / clase se encuentra? ¿Cómo navega su dron? ¿Tiene su dron características adicionales, tales como vuelo autónomo o funciones de seguimiento?	**¿Cómo captura (recopila) su dron los datos?** ¿Qué sensores tiene? ¿Qué tipo de sensores son? ¿Cómo son de potentes? ¿Cómo pueden ser controlados, cuando su seguridad/control se encuentra comprometido? ¿Qué tipo de datos recoge el dron? Incluya aquí todo el tipo de información con la que opera el dron, incluyendo coordenadas GNSS, señales WiFi, etc.	**¿Cómo almacena los datos su dron?** ¿Se registran los datos? ¿Se graba en el dron o se transmite? Si se transmiten datos, ¿cómo se transmiten? ¿Qué canales de comunicación se utilizan y cuál es el dispositivo receptor? Si los datos se almacenan en el dron, ¿qué medios se utilizan para el almacenamiento?	**¿Cómo se tratan los datos en su dron?** ¿Los datos se someten a algún tipo de tratamiento adicional en el interior del dron? Por ejemplo, ¿el dron está equipado con capacidades de software para llevar a cabo la difuminación automática de las caras? ¿El tratamiento de datos se realiza de forma automática?	**¿Cómo borra el dron los datos?** ¿Cuánto tiempo se guardan los datos en el dron/equipo? ¿En qué momento se borran? ¿Se programa automáticamente el borrado? ¿Se puede sobrescribir manualmente?

	Características del dron	Recogida de datos	Conservación de datos	Tratamiento de datos	Borrado de datos
Identificación de riesgos	**¿Existe algún riesgo con respecto a su dron en general?** ¿Está cumpliendo con todos los requisitos legales relacionados con su clase de dron (según lo regulado por la EASA), incluidos los requisitos de privacidad y seguridad? ¿Existen riesgos o vulnerabilidades en la navegación de su dron? ¿El dron es lo suficientemente ágil como para navegar fácilmente según sea necesario para sus probables usos? ¿Existen riesgos o vulnerabilidades en las funciones autónomas y semiautónomas de su dron?	**¿Qué riesgos para la privacidad y la protección de datos se derivan de la recogida de datos por el dron?** ¿Es probable que se capturen datos personales? ¿Se ve afectado uno de los siete tipos de privacidad (privacidad corporal, privacidad de datos e imagen, privacidad de ubicación y espacio, de comportamiento y acción, de asociación, de comunicación personal o de pensamientos y sentimientos)? ¿Se puede minimizar la captura de datos, por ejemplo, los usuarios podrían operar fácilmente los sensores encendiéndolos y apagándolos cuando lo deseen, podrían especificar qué calidad de datos desean que capturen los sensores? ¿Se verifican los datos y se asegura la precisión del sensor durante la recogida?	**¿Qué riesgos para la privacidad y la protección de datos se derivan del almacenamiento de datos en el dron?** ¿Están protegidos los datos almacenados en el dron contra el acceso de personas no autorizadas? ¿Están encriptados los datos almacenados en el dron? ¿Están protegidos los datos transmitidos desde y hacia el dron de capturas o interferencias no autorizadas?	**¿Qué riesgos para la privacidad y la protección de datos se derivan del tratamiento de los datos?** ¿Pueden los usuarios activar y desactivar fácilmente las funciones de tratamiento de datos? ¿Pueden los usuarios personalizar fácilmente las funciones que permiten el tratamiento de datos?	**¿Qué riesgos para la privacidad y la protección de datos se derivan del borrado de datos?** ¿Es adecuado el período establecido para el borrado automático de los datos almacenados? ¿Pueden los usuarios personalizar fácilmente las funciones de borrado de datos? ¿Es seguro e irreversible el borrado?

	Características del dron	Recogida de datos	Conservación de datos	Tratamiento de datos	Borrado de datos
Identificación y aplicación de salvaguardas	**¿Cómo puede eliminar o mitigar los riesgos relacionados con el dron en general?** ¿Qué pasos debe seguir para asegurarse de que cumple con los requisitos legales como fabricante para esta clase particular de drones? ¿Qué medidas de seguridad podría aplicar para garantizar la navegación segura y fiable de su dron? ¿Podría incluir características de navegación adicionales, incluyendo diferentes velocidades de crucero o facilidad de navegación? ¿Qué medidas de seguridad podría implementar para asegurar el funcionamiento seguro y fiable de las características autónomas y semiautónomas de su dron? ¿Podrían los pilotos humanos anular fácil y rápidamente esas funciones?	**¿Cómo puede eliminar o mitigar los riesgos relacionados con la recogida de datos por parte del dron?** ¿Puede utilizar hardware o software que permita a los operadores y pilotos personalizar fácilmente las capacidades del dron, por ejemplo, mediante la implementación de un diseño modular que permita cambios sencillos en las cargas útiles, mediante el uso de interfaces que permitan a los usuarios controlar la calidad de los datos capturados por los sensores o que permitan a los usuarios encender y apagar los sensores con facilidad? ¿Puede equipar su dron con funciones para preservar la privacidad, como la anonimización automática de las grabaciones visuales? ¿Podría implementar medidas de seguridad para asegurar la exactitud de los datos capturados? ¿Sería posible cotejar los datos captados por	**¿Cómo puede eliminar o mitigar los riesgos relacionados con el almacenamiento de datos?** ¿Qué tipo de información y medidas de seguridad informáticas puede emplear para limitar el acceso a los datos almacenados en el dron y a los datos transmitidos por y hacia el dron desde los dispositivos de control? Estas salvaguardas podrían incluir controles de acceso, cifrado, verificación continua de la identidad de los dispositivos de envío y recepción, etc.	**¿Cómo puede eliminar o mitigar los riesgos relacionados con el tratamiento de datos por el dron?** ¿Puede colocar controles fáciles de usar en el software del dron para cada una de las funciones del software? ¿Puede implementar funcionalidades que minimicen la captura de datos personales, eliminando o difuminando, por ejemplo, el número de casas, matrículas de automóviles o las caras?	**¿Cómo puede eliminar o mitigar los riesgos relacionados con el borrado de datos?** ¿Puede implementar funcionalidades automáticas para borrar los datos del dron después de que éste haya completado su operación y se hayan descargado los datos pertinentes? ¿Puede este procedimiento (y cuando ocurra) ser fácil de operar y personalizar para los usuarios de drones? ¿Hay alguna medida que pueda tomar para asegurar que el borrado de datos sea irreversible?

	Características del dron	Recogida de datos	Conservación de datos	Tratamiento de datos	Borrado de datos
		diferentes sensores? ¿Sería necesario o apropiado, considerando el uso probable del dron?			

Conclusión

Dado que los drones se utilizan en diversos campos, su impacto en la privacidad y la protección de datos está más claro y mejor estudiado. Los operadores y los pilotos se enfrentan a una multitud de regulaciones y requisitos que deben cumplir cuando planifican o llevan a cabo vuelos teledirigidos, incluyendo estos requisitos. Los fabricantes y productores pueden desempeñar un papel clave en el apoyo a los operadores y a los pilotos, para que éstos cumplan con estos requisitos, y es posible que ellos mismos tengan pronto la obligación legal de equipar a algunos drones con características que mejoren la privacidad. Además, los drones que permiten y apoyan el uso responsable constituyen la base de la aceptación de los drones y del cumplimiento de la legislación en Europa.

La presente guía tiene por objeto ayudar a los fabricantes a comprender las medidas concretas que pueden adoptar para mejorar sus drones durante las fases de diseño, desarrollo y producción, así como presentarles algunos de los requisitos del Reglamento delegado de la Comisión sobre drones. No obstante, se anima a los fabricantes a considerar cómo ampliar o mejorar dichas características y equipar a todos los drones que producen con las características adecuadas y proporcionadas de forma que mejoren la privacidad con la ayuda de esta Guía.

Anexo I Folleto sobre protección de datos y privacidad

Manejo responsable de su dron: privacidad y protección de datos

Si usted opera su dron cerca de personas, puede estar corriendo riesgos relativos a la privacidad y la protección de datos. La privacidad y la protección de los datos personales están reconocidos como derechos fundamentales en la Unión Europea y son legalmente exigibles. Con el Reglamento General de Protección de Datos (RGPD), usted está obligado a tomar ciertas medidas para asegurar que los datos personales que captura con su dron sean tratados de manera responsable y segura. Deberá, por lo tanto, informarse acerca de los riesgos y salvaguardas que se deben implementar por ley y por respeto a los demás.

DroneRules.eu ha identificado 8 principios rectores que los operadores profesionales deben tener en cuenta para apoyar el cumplimiento del RGPD cuando recogen información personal.

1. **Informar:** Siempre que capture o registre cualquier información sobre una persona, especialmente imágenes claras de su rostro, infórmele sobre ello. Redacte y publique una declaración/política de privacidad para aumentar la transparencia.
2. **Escuchar:** Pregunte a las personas qué puede y qué no puede hacer con su información y cumpla con sus deseos en todo momento. Conozca los derechos de protección de datos de las personas.
3. **Minimizar:** Piense siempre en qué tipo de dron utiliza y cómo se puede capturar la menor cantidad posible de datos sobre las personas en el área de su operación. Anonimice los datos personales siempre que sea posible. Borrar las caras, los números de las casas y de los coches puede ayudar a aliviar sus obligaciones bajo el RGPD.
4. **Respetar:** Garantizar que las personas puedan ejercer su derecho a oponerse al tratamiento de datos, cambiar de opinión al respecto o hacer que se eliminen sus datos. Recuerde, las personas también tienen derecho a acceder a sus datos, recibir una copia de los mismos y corregirlos.
5. **Limitar:** Limite la finalidad para la que usted utiliza los datos estrictamente a la finalidad que usted ha indicado en un principio y limite la conservación de los datos personales al período mínimo requerido.
6. **Proteger:** Proporcione la seguridad adecuada a los datos personales y no los comparta con terceros sin informar a las personas y asegurar que los datos estén protegidos con sus destinatarios. Si es posible, comparta sólo datos anónimos.
7. **Evaluar:** Actúe responsablemente y planifique sus actividades teniendo en cuenta la privacidad. Si sus actividades pueden presentar un alto riesgo para los derechos de las personas sobre el terreno, lleve a cabo una evaluación del impacto de la protección de datos (PIA). Vea los recursos de DroneRules.eu para más orientación y las plantillas.
8. **Demostrar:** Documente su vuelo y los pasos que ha tomado para que sea proporcionado y respetuoso con la privacidad. Asegúrese de que puede demostrar que tiene una base jurídica para sus actividades, por ejemplo, el consentimiento de los interesados.

Seguir estos principios reducirá considerablemente sus riesgos al recoger y tratar información personal a través de un dron.

Anexo II Folleto sobre protección y seguridad

Seguridad y protección de los drones durante el vuelo

Como operador y piloto, es su responsabilidad asegurarse de que los drones sean operados de una manera segura. Aunque no es una lista completa, más abajo puede encontrar algunas sugerencias para operar de una manera segura.

Seguridad: estar informado y preparado
Compruebe los requisitos legales de su operación. Los nuevos Reglamentos guiarán la forma en que deben operarse los drones en los vuelos de las categorías "abierta" y "específica". Asegúrese de comprobar qué requisitos y limitaciones legales deben ser aplicados a su vuelo y llévelos acabo.

Compruebe su ubicación: Infórmese sobre la ubicación y las áreas donde planea volar el dron. En particular, tome nota de cualquier zona de exclusión aérea o zona restringida designada y asegúrese de que dispone de la información más reciente sobre las ubicaciones geo-cercadas. Planifique su vuelo de manera que cumpla con dichas limitaciones.

Habilite las capacidades de geo-consciencia siempre que su dron esté equipado con ellas. Asegúrese de actualizar regularmente su base de datos de ubicaciones geo-cercadas y, en el mejor de los casos, trate de hacerlo antes de cada misión con drones.

Compruebe el tiempo meteorológico: Como último paso antes del vuelo, asegúrese de comprobar el tiempo en tierra. Tenga cuidado y use los drones sólo en un entorno en el que estén diseñados para resistir.

Seguridad: proteger los drones y los datos
Proteja los drones y los datos durante las transmisiones: Proteger a los drones de ser secuestrados y de que personas no autorizadas obtengan el control sobre ellos. Además, proteja los datos transmitidos por un dron y comunicados a otros equipos de ser interceptados, corrompidos o vistos por otros. Puede hacerlo, por ejemplo, mediante:

- colocación de controles de acceso en las funciones de mando y control
- garantizar el enlace de datos entre el dron y el equipo de pilotaje, por ejemplo, mediante el cifrado.

Proteja los datos en los drones: Proteja los datos almacenados localmente en los drones para que no puedan ser accedidos por personas no autorizadas, garantizando que las medidas de seguridad estén habilitadas y activadas, por ejemplo:

- eliminar regularmente los datos más antiguos,
- colocar controles de acceso para ver los datos almacenados en los drones,
- encriptar los datos almacenados en los drones.

Anexo III Folleto de seguro

Protéjase y esté asegurado

Cuando utilice drones por razones comerciales profesionales como operador, está obligado a contratar un seguro de responsabilidad profesional para proteger sus activos y cubrir cualquier daño que su equipo o sus empleados o contratistas causen durante la operación de un dron. Los siguientes pasos pueden ayudarle a elegir el seguro adecuado:[54]

Paso 1: Declare todas sus actividades en la póliza del seguro
Asegúrese de que las actividades que realiza con los drones estén debidamente declaradas a la compañía de seguros. Usted puede hacer esto mencionando parte de su negocio en el programa de la póliza. Asegúrese de que las operaciones con drones figuren específicamente en su contrato de seguro.

Paso 2: Compruebe el alcance de la cobertura de su contrato
Asegúrese de que su seguro de responsabilidad profesional cubra la responsabilidad por lesiones corporales accidentales, así como los daños accidentales a la propiedad que resulten de la operación de los drones. También tome nota de cualquier límite territorial a su cobertura de seguro.

Paso 3: Compruebe las exclusiones enumeradas en su contrato
Observe cuidadosamente qué exclusiones hay en su seguro, es decir, en qué casos la aseguradora no tiene que pagarle. Estas exclusiones le informarán de los riesgos no cubiertos por su póliza.

Paso 4: Asegurarse de que el límite de responsabilidad propuesto por el seguro sea suficiente
Consulte el Reglamento (CE) 785/2004, es un reglamento que garantiza que las víctimas de accidentes tienen acceso a una indemnización adecuada, para identificar el nivel mínimo de cobertura de seguro por accidente requerido, dependiendo de la masa máxima de despegue (MTOM) del dron. Identifique el nivel apropiado de seguro para usted.

Paso 5: Obtenga un certificado de seguro
Para estar seguro de que está asegurado, pida a su compañía de seguros un certificado de seguro que indique claramente que está protegido cuando opera drones con fines comerciales.

Paso 6: Mantenga la información actualizada
Manténgase en contacto con su aseguradora e infórmele si comienza a realizar nuevas actividades o si las actividades que ha declarado evolucionan significativamente.

Asegúrese de que su póliza de seguro y su certificado de seguro aclaran que usted está cubierto en relación con sus actividades específicas.

[54] DroneRules.eu, Insurance Checklist. http://dronerules.eu/en/professional/resources/pdf/1349.