DURÁNSINDREU

Newsletter Derecho Digital, IT y protección de datos

Novedades primer trimestre 2026

Las recientes actuaciones de las autoridades de protección de datos confirman un refuerzo significativo del control regulatorio en materia de privacidad y entorno digital. La AEPD ha sancionado prácticas que evidencian deficiencias en la seguridad de los datos, el uso desproporcionado de sistemas de videovigilancia y el incumplimiento de resoluciones firmes, subrayando que los errores humanos o la adopción posterior de medidas no eximen de responsabilidad. A nivel europeo, destaca la primera gran sanción impuesta bajo la Ley de Servicios Digitales, que marca un punto de inflexión en la supervisión de las grandes plataformas. Asimismo, las autoridades alertan sobre los riesgos de la IA agéntica y analizan reformas normativas clave, insistiendo en la necesidad de integrar la protección de datos desde el diseño.

Índice de contenidos

La Agencia Española de Protección de Datos (en adelante "AEPD") actúa frente a prácticas que comprometen la seguridad y el adecuado tratamiento de los datos personales.

En las últimas resoluciones publicadas, se han analizado distintos supuestos en los que, empresas de sectores muy diversos, han tratado datos personales especialmente sensibles sin la correcta aplicación de la normativa de protección de datos, recordando la obligación de aplicar medidas técnicas y organizativas que garanticen un nivel de protección adecuado al riesgo. Estas decisiones ponen de manifiesto la importancia creciente del cumplimiento normativo en materia de privacidad, así como las consecuencias derivadas de no adoptar medidas suficientes.

1. Resoluciones y sanciones

Resoluciones de la AEPD

Sanción de 10.000 € a una operadora de telecomunicaciones, por enviar a un cliente sus credenciales completas de acceso a través de correo electrónico

La AEPD inició el correspondiente expediente sancionador tras tener conocimiento de los hechos expuestos a continuación. Un cliente de una operadora de telecomunicaciones recibió un mensaje informativo, a través del correo electrónico, sobre la actualización del área privada de clientes, por lo que interpuso una reclamación ante la AEPD.

En dicho correo figuraban sus credenciales completas de acceso, incluyendo una nueva contraseña que había sido modificada por la empresa sin previo aviso. El afectado denunció que en el portal se almacenaban numerosos datos personales, como nombre y apellidos, dirección, DNI, teléfono, correo electrónico, contrato, facturas, detalle de llamadas y consumo de datos e información bancaria. Además, el acceso no contaba con autenticación multifactor, por lo que el reclamante lo consideró una brecha de seguridad.

La empresa sostuvo durante el procedimiento que el incidente fue consecuencia de un error humano puntual, que no se produjeron accesos no autorizados ni exfiltración de datos y que actuó con diligencia una vez detectado el problema, ya que reinició la contraseña del cliente, modificó el procedimiento interno de gestión de credenciales y reforzó sus protocolos de seguridad.

La AEPD, sin embargo, subraya en su resolución que el artículo 32 del RGPD exige aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y que dicha obligación no depende de que se materialice un daño efectivo. Para la Agencia, la mera remisión de credenciales en claro por correo electrónico supone una exposición indebida de un elemento crítico de autenticación y evidencia una insuficiencia de las medidas organizativas implantadas. El hecho de que se tratara de un "error humano puntual" no exime de responsabilidad si revela que no existían controles adecuados para evitar este tipo de situaciones. Tampoco desvirtúa la infracción la adopción posterior de medidas correctoras, ya que la adecuación de la seguridad debe valorarse en el momento en que se produce el incidente.

Al graduar la sanción, la Agencia tuvo en cuenta lo siguiente:

- Como factores agravantes: la vinculación de la actividad de la empresa con el tratamiento masivo de datos personales y la negligencia apreciada en la gestión de credenciales, consideradas un elemento especialmente sensible desde el punto de vista de la seguridad.

- Como circunstancias atenuantes: valoró que el incidente afectara a un único interesado y que la entidad adoptara medidas correctoras tras tener conocimiento de los hechos.

En consecuencia, la AEPD **impuso una multa de 10.000 € por infracción grave del artículo 32 del RGPD, reiterando que la gestión y comunicación de contraseñas exige medidas reforzadas y que el envío de credenciales en texto plano por correo electrónico no garantiza un nivel de seguridad adecuado al riesgo.**

La AEPD refuerza su vigilancia sobre el uso de sistemas de videovigilancia en centros de trabajo

La AEPD ha impuesto una sanción de 1.200€ al responsable de una clínica dental por vulnerar la normativa de protección de datos personales a través del uso de sistemas de videovigilancia.

El procedimiento sancionador se inició el 3 de diciembre de 2025, tras la denuncia presentada por una extrabajadora que alegó haber sido grabada sin su consentimiento durante su relación laboral, entre abril de 2024 y enero de 2025. La reclamación señalaba que las cámaras estaban instaladas tanto en la recepción como en el gabinete de tratamiento, sin carteles informativos para clientes ni empleados, y que las imágenes podían ser grabadas con audio.

Tras la denuncia, la AEPD solicitó al responsable que explicara el funcionamiento del sistema y las medidas adoptadas para cumplir con la normativa, pero en sus escritos indicó que las cámaras tenían fines de seguridad, con acceso restringido mediante aplicación móvil, y que las grabaciones se conservaban durante un máximo de siete días. También afirmó que la captación de audio se limitaba al gabinete clínico y que la supervisión del cumplimiento de la normativa estaba delegada en empresas externas especializadas.

A pesar de estas alegaciones, la AEPD consideró que se había producido una infracción del artículo 5.1.c) del RGPD, **relativo al principio de minimización de datos atendiendo a la configuración y localización de las cámaras y al área de grabación de las mismas**. Así, la AEPD argumenta la infracción del citado principio en base al hecho que 1) una de las cámaras incluiría la grabación de imágenes durante el tratamiento de los pacientes; y 2) **una de las cámaras grababa no solamente la imagen, sino también el sonido, pudiendo grabar conversaciones privadas entre pacientes y los trabajadores**.

En consecuencia, la AEPD estableció inicialmente una multa de 2.000 €. Tras reconocer su responsabilidad y efectuar el pago voluntario aplicando las reducciones previstas por la normativa, el responsable de la clínica abonó 1.200 €.

Además de la sanción económica, la AEPD recordó que debían adoptarse medidas correctivas para garantizar el cumplimiento de la normativa de protección de datos en la clínica. Entre estas medidas

se incluyen la correcta señalización de las zonas videovigiladas, la limitación estricta del acceso a las grabaciones y la eliminación de los datos en los plazos legales establecidos.

Primeras sanciones de la Ley de Servicios Digitales

La UE impone a X la primera gran sanción del DSA: un antes y un después en la regulación digital

La Comisión Europea ha impuesto una multa de 120 millones de euros a X (antes "Twitter"), convirtiéndose en la primera gran sanción dictada bajo la Ley de Servicios Digitales (en adelante "LSD" o "DSA" por sus siglas en ingles). Esto representa un precedente significativo para la regulación europea, ya que demuestra su disposición a hacer cumplir de forma estricta las nuevas obligaciones de transparencia y responsabilidad de las grandes plataformas.

La LSD es una normativa europea que establece un conjunto de reglas para los servicios en línea que usan los ciudadanos, destinadas a reforzar la transparencia, limitar los riesgos sistémicos y garantizar la protección de los usuarios, con el fin de crear un espacio digital más seguro y respetuoso con los derechos fundamentales. Su objetivo es proteger a usuarios y consumidores, garantizar obligaciones claras para las plataformas y facilitar que pymes y empresas emergentes puedan crecer en Europa. Su aplicación directa en todos los Estados miembros convierte la presente sanción en un precedente relevante para plataformas de gran tamaño.

Según la Comisión, X vulneró varias obligaciones esenciales:

- **Uso engañoso de la verificación de cuentas**: la plataforma permitía conseguir el "check azul", como símbolo de cuenta verificada, simplemente pagando, sin comprobar la identidad real del usuario. Esto generaba confusión entre la gente y se considera un diseño engañoso, algo que el DSA prohíbe.

- **Falta de transparencia publicitaria**: la plataforma no ofreció información suficiente sobre sus anuncios, sus responsables ni los criterios de segmentación, incumpliendo la obligación de mantener un repositorio claro y accesible.

- **Restricciones al acceso para investigación**: X obstaculizó el trabajo de investigadores y auditores, puso trabas y bloqueó ese acceso, impidiendo que los especialistas pudieran analizar la plataforma y evaluar sus riesgos, pese a que la DSA exige facilitar datos relevantes para analizar fenómenos.

Importe de la sanción

La sanción, equivalente al 5 % de los ingresos globales de X en 2024, se aproxima al límite máximo previsto para este tipo de infracciones. Con ello, la Comisión envía un "mensaje"; las obligaciones del DSA son vinculantes y su incumplimiento tendrá consecuencias inmediatas y cuantiosas.

Además de la multa, la decisión obliga a la plataforma a corregir sus prácticas en plazos concretos, marcando la línea sobre cómo deberán actuar otras plataformas sometidas al nuevo régimen, ya que este caso supone un aviso para toda la industria tecnológica.

Sanción por incumplimiento de resoluciones de la Autoridad de Control

Del mismo modo que la AEPD sanciona las deficiencias en seguridad o en el uso de sistemas de videovigilancia, también actúa con firmeza cuando una entidad incumple las "obligaciones de hacer" que la propia Agencia le ha ordenado corregir. No aplicar estas obligaciones correctivas de la autoridad de control mantiene vigente la infracción inicial y puede derivar en nuevas sanciones, ya que no sólo perpetúa la infracción inicial, sino que puede generar nuevas sanciones adicionales, como demuestra el siguiente caso.

La AEPD sancionó a una empresa de instalaciones deportivas por incumplir una resolución previa

El origen del caso se sitúa en un procedimiento sancionador anterior en el que la AEPD, además de imponer una sanción económica, ordenó a la empresa adaptar su formulario de "Acuerdo de usuario. Consentimiento informado y asunción de riesgo" a las exigencias del Reglamento General de Protección de Datos. En concreto, se le exigía acreditar que el consentimiento recabado de los usuarios cumplía con los requisitos legales, otorgándole para ello el plazo de un mes.

La resolución fue notificada por medios electrónicos, pero la empresa no accedió inicialmente a la notificación dentro del plazo establecido, por lo que esta se tuvo por rechazada. Posteriormente, la Agencia reiteró el requerimiento en dos ocasiones adicionales, concediendo nuevos plazos para que acreditara la adopción de las medidas correctoras. Aunque estas notificaciones sí fueron recibidas, la entidad no presentó documentación alguna que demostrara haber adaptado el formulario ni formuló alegaciones.

La resolución inicial adquirió firmeza y carácter ejecutivo, aunque pese a ello, la empresa no dio cumplimiento a la orden dictada por la autoridad de control.

Ante esta inactividad, la AEPD inició un nuevo procedimiento sancionador por incumplimiento de las resoluciones dictadas en ejercicio de sus poderes correctivos, en virtud del artículo 58.2 del RGPD. Esta conducta está tipificada en el artículo 83.6 del mismo reglamento y calificada como infracción muy grave por la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, al tratarse del incumplimiento de una resolución firme de la autoridad de protección de datos.

La empresa no presentó alegaciones en el plazo concedido, por lo que el acuerdo de inicio del expediente se convirtió directamente en propuesta de resolución.

En atención a las circunstancias del caso y al carácter de microempresa de la entidad, la AEPD acordó imponer una multa de 900 €. Además, reiteró la obligación de acreditar en el plazo de un mes el cumplimiento de las medidas correctoras ordenadas en el expediente anterior.

La resolución advierte expresamente que, en caso de persistir el incumplimiento, la conducta podría dar lugar a la apertura de un nuevo procedimiento sancionador por la misma causa. Por ello, la Agencia consideró acreditado el incumplimiento y recordó que **desatender los requerimientos de adaptación a la normativa constituye una infracción autónoma, independiente de la sanción inicialmente impuesta.**

Finalmente, se le impuso a la empresa una **multa de 900 €,** reiterando aún y así la obligación de cumplir las medidas correctivas ya impuestas en la primera resolución dentro del plazo de un mes, bajo apercibimiento de nuevas sanciones en el caso en el que la empresa sancionara volviera a desatender esta nueva resolución.

2. Criterios de las Autoridades de Protección de Datos en Materia de IA

La AEPD alerta a empresas y administraciones sobre la IA agéntica

La inteligencia artificial agéntica es un sistema avanzado, ya que no se dedica únicamente a responder comandos, sino que actúa de forma autónoma. No solo ejecuta lo que se le pide, sino que identifica, planifica y coordina por su cuenta tareas complejas, con una mínima intervención humana. Esta capacidad para percibir el entorno digital, razonar y actuar coloca a estos sistemas en un nivel muy superior al de los chatbots tradicionales, y supone un cambio significativo para empresas y administraciones públicas.

Esta es precisamente la advertencia del nuevo documento **"Inteligencia Artificial Agéntica desde la perspectiva de protección de datos"**, publicado por la AEPD. En él se detallan oportunidades, riesgos y obligaciones para cualquier organización que integre este tipo de tecnologías en su día a día.

Algunos de los riesgos más relevantes respecto a la protección de datos son los siguientes:

- Acceso a información interna del usuario o de la organización.
- Consultas a servicios externos de forma autónoma.
- Almacenamiento de memoria a corto y largo plazo. Memorias extensas que combinan información de varios tratamientos.
- Toma de decisiones y ejecución de acciones, incluso en nombre del usuario.
- Coordinación de múltiples herramientas para cumplir sus objetivos.

Estas nuevas aptitudes hacen que, cuando se integran en un tratamiento de datos personales, el impacto no sea simplemente técnico, sino que cambie la naturaleza, el contexto, los riesgos y hasta las finalidades del tratamiento. Por ello, **las organizaciones deben revisar completamente sus procesos y garantías antes de automatizar operaciones con IA agéntica**.

Con su llegada también se han identificado vulnerabilidades específicas que no existían en la IA generativa tradicional, como la interacción "opaca" con servicios externos, que puede exponer datos personales sin que el usuario lo perciba o su autonomía elevada, que puede dar lugar a acciones erróneas, irreversibles o no autorizadas, ya que se llevan a cabo procesos de razonamiento complejos, susceptibles a desviaciones y con comportamientos impredecibles.

Lo que la AEPD quiere resaltar es que las obligaciones legales existentes se intensifican con la llegada de esta IA avanzada, y entre las acciones recomendadas a las empresas se encuentran las siguientes:

- Identificar nuevos encargados o destinatarios, como proveedores de modelos de lenguaje.
- Realizar o actualizar los registros de actividades de tratamiento.
- Revisar la base jurídica y la minimización de datos.
- Garantizar un ejercicio de derechos efectivo, incluso dentro de las memorias internas de los agentes.
- Evaluar si surgen decisiones automatizadas del artículo 22 del RGPD.
- Reconsiderar el riesgo del tratamiento.
- En muchos casos, realizar una nueva Evaluación de Impacto en Protección de Datos (EIPD).

Si bien es cierto **que la IA agéntica abre grandes oportunidades para automatizar procesos empresariales**, mejorar eficiencia y reducir tareas manuales, también exige un nivel de responsabilidad organizativa mucho mayor, por lo que adoptar estos sistemas sin control, sería un riesgo inasumible. **Será crucial integrarla con protección de datos desde el diseño, aplicando medidas preventivas y un profundo conocimiento técnico y normativo.**

Para más información puede consultar el documento "INTELIGENCIA ARTIFICIAL AGÉNTICA DESDE LA PERSPECTIVA DE PROTECCIÓN DE DATOS" elaborado por la AEPD.

Protección de datos y captación de imágenes

La APDCAT avala la grabación de trabajadores sociales durante desahucios siempre que exista interés legítimo

La Autoridad Catalana de Protección de Datos (en adelante "APDCAT") ha concluido en un Dictamen, que la captación y difusión de imágenes del personal municipal que participa en desahucios ordenados judicialmente puede ser lícita cuando se basa en el interés legítimo de la ciudadanía o de los medios de comunicación. El dictamen responde a la consulta de un ayuntamiento cuyos trabajadores han expresado preocupación por la posibilidad de ser identificados y sufrir represalias.

Según el organismo, la grabación de estos empleados en espacios públicos y como parte accesoria de un acontecimiento de interés general es compatible con la normativa de protección de datos. La APDCAT señala que no existe una exigencia general de anonimato para estos profesionales, aunque el Ayuntamiento puede adoptar medidas preventivas, como por ejemplo la indumentaria homogénea, que reduzcan su identificación directa.

También indica que las administraciones pueden dirigirse a los medios para solicitar que eviten identificar al personal cuando ello no sea necesario para informar. Asimismo, establece que un mal uso o una difusión innecesaria o desproporcionada de las imágenes puede vulnerar derechos fundamentales y generar responsabilidades legales, incluso si la grabación original era lícita.

Además, el dictamen recuerda **que la normativa europea de protección de datos no se aplica cuando una persona graba imágenes únicamente para un uso privado o doméstico**. Sin embargo, en el contexto de un desahucio, al ser un acto público en la vía pública, es habitual que las grabaciones puedan difundirse más allá del ámbito estrictamente personal, lo que activa plenamente las obligaciones del Reglamento General de Protección de Datos y de la Ley Orgánica 3/2018. En este sentido, la APDCAT destaca que la licitud de la grabación depende de la finalidad y del respeto a los principios de proporcionalidad y minimización.

Asimismo, la **Autoridad subraya que, aunque la captación de imágenes pueda estar amparada por el interés legítimo, la difusión posterior debe evaluarse de forma independiente**, ya que podría vulnerar derechos fundamentales si expone innecesariamente al personal público a riesgos, represalias o estigmatización. En caso de una difusión indebida, los trabajadores afectados disponen de varias vías de protección, como reclamaciones ante la autoridad de control, acciones civiles por vulneración del derecho a la propia imagen u otros mecanismos legales, dependiendo de la gravedad de los hechos.

Armonización de Ensayos Clínicos: EDPB y EDPS Piden Garantías en Protección de Datos

Integración del principio de privacidad desde el diseño y por defecto

En una declaración conjunta del pasado 12 de marzo, el Comité Europeo de Protección de Datos (EDPB) y el Supervisor Europeo de Protección de Datos (EDPS) han manifestado su apoyo a la iniciativa de crear un marco normativo unificado para los ensayos clínicos bajo la futura Ley Europea de Biotecnología. Reconocen que esta armonización es clave para impulsar la investigación, acelerar la innovación en el sector de la salud y mejorar la competitividad de la UE.

No obstante, ambas autoridades han subrayado que este avance no puede producirse a expensas de los derechos fundamentales. Advierten que la nueva legislación debe integrar, desde su concepción,

salvaguardias efectivas para proteger la privacidad y los datos personales de los participantes en los ensayos, considerando la especial sensibilidad de la información sanitaria.

Para lograr este equilibrio, sus recomendaciones se centran en los siguientes pilares:

- **Establecimiento de bases jurídicas claras y específicas** para el tratamiento de datos sanitarios en el contexto de los ensayos, evitando ambigüedades y garantizando la licitud del tratamiento desde el origen.
- **Refuerzo de los derechos de los interesados**, asegurando que los participantes puedan ejercer un control efectivo sobre su información personal, incluyendo el derecho de acceso, rectificación y, crucialmente, las condiciones para la retirada del consentimiento.
- **Garantía de una supervisión coherente y efectiva** por parte de las autoridades de protección de datos nacionales, que deben tener las competencias y recursos necesarios para auditar y hacer cumplir la normativa en un entorno transfronterizo.

En definitiva, el mensaje del EDPB y el EDPS refuerza que el progreso científico y la protección de datos no son objetivos contrapuestos, sino complementarios. La futura Ley Europea de Biotecnología debe diseñarse para que sea plenamente compatible con los principios y exigencias del Reglamento General de Protección de Datos (RGPD), asegurando así un ecosistema de investigación innovador, ético y fiable que respete la privacidad de los interesados.

Opinión sobre el reciente Digital Omnibus

La UE examina el "Digital Omnibus": autoridades de privacidad alertan de riesgos en la propuesta de simplificación normativa

El **Comité Europeo de Protección de Datos** (en adelante "EDPB") y el **Supervisor Europeo de Protección de Datos** (en adelante "EDPS"**) publicaron el pasado 10 de febrero una opinión conjunta sobre la propuesta de Reglamento Digital Omnibus con el que la Comisión Europea pretende simplificar el ecosistema normativo digital**, reducir cargas administrativas y reforzar la competitividad de las organizaciones europeas.

Aunque ambas autoridades valoran positivamente el objetivo general de armonización, advierten de que algunos de los cambios propuestos podrían debilitar la protección de datos y generar incertidumbre jurídica si no se revisan en profundidad.

Respaldan el objetivo de simplificación normativa del Digital Omnibus, pero insisten en que la competitividad europea no debe comprometer los derechos fundamentales ni debilitar el marco de protección de datos que caracteriza a la Unión Europea.

Impacto del Digital Omnibus sobre la normativa de reutilización de datos

El EDPB y el EDPS quieren entender cómo afectará el Digital Omnibus a varias normas importantes, como el RGPD, la Directiva E Privacy y las distintas Leyes que regulan la reutilización de datos públicos. Los aspectos que generan más preocupación son los siguientes:

- Si esta reforma realmente hace las cosas más fáciles para quienes deben cumplir la normativa.
- Si aporta más claridad legal, es decir, si deja menos dudas sobre qué se puede hacer y qué no.
- Si mantiene intacta la protección de los derechos fundamentales, especialmente la protección de datos personales.

Es decir, quieren asegurarse de que esa simplificación que nos presenta el Digital Omnibus, no implique perder garantías ni abrir la puerta a un uso inadecuado de los datos, incluidos los datos públicos que pueden volver a utilizarse en nuevos proyectos o servicios.

Dudas sobre la modificación de la definición de dato personal

Uno de los puntos más controvertidos es la propuesta de modificar la definición de “datos personales” en el Reglamento General de Protección de Datos (RGPD) y en el Reglamento de Protección de Datos de la UE (EUDPR).

Ambos organismos muestran su rechazo al considerar que la reforma reduciría de forma sustancial el alcance de los datos protegidos, se alejaría de la jurisprudencia consolidada del Tribunal de Justicia de la UE, y con ello podría restringir significativamente el concepto de dato personal. Además, critican que a la Comisión Europea se le otorgue un poder excesivo para decidir, mediante un acto de ejecución, qué datos pseudonimizados dejan de considerarse personales tras un proceso de seudonimización, ya que esto afectaría directamente al ámbito de aplicación de la legislación europea de protección de datos, y precisamente el Supervisor Europeo de Protección de Datos, Wojciech Wiewiórowski, insistió en que cualquier reforma debe mantener un alto nivel de protección y confianza ciudadana.

Por lo tanto, para las autoridades, esta modificación podría suponer un debilitamiento estructural del sistema europeo de protección de datos, aunque también se reconocen elementos beneficiosos del Digital Omnibus.

Avances reconocidos por las autoridades.

- Propuesta de ajustar cuándo y cómo una empresa tiene que notificar una brecha de seguridad, de forma que solo sea obligatorio informar cuando el incidente sea realmente grave y afecte de verdad a las personas.
- Plazos más amplios para informar.
- Introducción de plantillas y formularios comunes para brechas y EIPD.
- Nueva posibilidad de usar biometría bajo control del usuario, con garantías.
- Claridad y coherencia al definir “investigación científica”.

También valoran muy positivamente las mejoras previstas en la **Directiva E Privacy** dentro del Digital Omnibus, especialmente **aquellas orientadas a reducir la fatiga del consentimiento y la saturación de banners de cookies**. Respaldan la introducción de señales automáticas y legibles por máquinas que permitan expresar de forma sencilla las preferencias de los usuarios, ya que esto facilitará el cumplimiento de las empresas y hará que las elecciones de los ciudadanos sean más efectivas. También apoyan la incorporación de excepciones limitadas para el acceso a datos del dispositivo, así como medidas que incentiven la publicidad contextual frente a la publicidad basada en el rastreo, siempre con garantías. Además, están de acuerdo con que la supervisión de estas cuestiones quede en manos de las autoridades de protección de datos, lo que refuerza la coherencia regulatoria y la protección del usuario.

Contacto

Carme Setó

Socia | Derecho Digital, IT y protección de datos
cseto@duransindreu.com
93 602 52 22

Núria Galera

Abogada | Derecho Digital, IT y protección de datos
ngalera@duransindreu.com
93 602 52 22

Iván Roda

Abogado | Derecho Digital, IT y protección de datos
iroda@duransindreu.com
93 602 52 22

Bàrbara Boguñá

Abogada | Derecho Digital, IT y protección de datos
bboguna@duransindreu.com
93 602 52 22