

## **Contribución de la Agencia Española de Protección de Datos a la Consulta de la Comisión sobre un enfoque global de la protección de datos personales en el la Unión Europea**

En respuesta a la invitación de la Comisión, la Agencia Española de Protección de Datos (en adelante, AEPD), autoridad de supervisión para la protección de datos en España conforme a lo previsto en el artículo 28 de la Directiva 95/46/CE, considerando su deber de proteger los derechos y libertades de las personas en relación al tratamiento de datos de carácter personal, desea contribuir a la Consulta planteada con las siguientes propuestas.

### **INTRODUCCIÓN**

La Agencia Española de Protección de Datos no puede sino mostrar su satisfacción por la adopción de esta iniciativa, así como por el empeño de la Comisión en modernizar el marco jurídico de la Unión en el ámbito de la protección de los datos de carácter personal y la disposición a hacer de este derecho una prioridad en el desarrollo de las políticas comunitarias. La AEPD considera de particular relevancia la referencia al artículo 8 de la Carta de los Derechos Fundamentales de la UE, que confiere carácter autónomo al derecho fundamental a la protección de los datos personales, como elemento primordial en la creación de una normativa global y coherente en material de protección de datos en el ámbito de la Unión y como base jurídica para la nueva regulación.

### **GARANTIZAR UNA PROTECCIÓN ADECUADA EN CUALESQUIERA CIRCUNSTANCIAS**

La piedra angular sobre la que gira el despliegue de garantías que ofrece la normativa de protección de datos es el concepto de datos personales. Se ha considerado que una persona es identificada cuando, dentro de un grupo de personas, se la “distingue” de todos los demás. Por otro lado, una persona es identificable, directa o indirectamente cuando, aunque no se la haya identificado todavía, sea posible hacerlo. Si bien la definición de datos personales aportada por la Directiva refleja la intención del legislador europeo de mantener un concepto amplio de datos personales, los elementos que conforman este concepto pueden verse condicionados por la aparición de nuevas tecnologías. Hoy son la Web colaborativa (2.0) y la Web semántica (3.0), pero en el futuro otros desarrollos pueden provocar una ampliación de este concepto y ruptura con lo que a día de hoy podemos interpretar como dato personal. En este sentido, podemos afirmar que la información es uno de los motores que mueven Internet tal y como lo conocemos hoy en día. El usuario aporta información conscientemente pero también de manera inconsciente mientras navega. Mediante el análisis de esta navegación, puede extraerse información en cuanto a su perfil, pudiendo ser singularizado a través de indentificadores aunque su nombre real no se conozca. Esta circunstancia plantea retos a los actuales planteamientos en torno a este concepto.

Sería deseable, y en ese sentido la AEPD coincide con la Comisión, que la definición de “datos personales” sea lo suficientemente amplia para anticiparse a las posibles evoluciones y cubrir todas las “zonas grises” existentes en su ámbito de aplicación, haciendo al mismo tiempo uso legítimo de la flexibilidad.

Por tanto, el concepto de dato personal debería cubrir aquellas situaciones en las que desconoce el nombre del sujeto, pero se tiene un perfil completo sobre él. El Grupo de Trabajo del Artículo 29 lo expresaba en su Dictamen 4/2007 sobre el concepto de datos personales estableciendo que si bien “la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien”.

De este modo, la AEPD propone:

- Que la identificabilidad no sea el único elemento a la hora de considerar el concepto de dato personal.
- Configurar una definición lo suficientemente amplia para anticiparse a las posibles evoluciones de la tecnología que incluya los procedimientos y técnicas para el tratamiento de la información que permitan singularizar a una persona o usuario.

## **AUMENTAR LA TRANSPARENCIA PARA LOS INTERESADOS**

La AEPD acoge con satisfacción la específica mención de la Comunicación sobre la información a los niños y la especial protección que ha de conferírseles. Es una realidad que, al menos en el entorno de Internet, cada vez existe una mayor y más activa participación de los nativos digitales, siendo todavía es necesario trabajar con las empresas en una mayor concienciación sobre este colectivo.

En cuanto a la necesidad de mejorar los mecanismos de transparencia, las posibilidades actuales y los medios hacen que técnicamente existan distintos modos de proporcionar esta información. Los entornos en línea plantean una especificidad y sobre todo una difusión hasta ahora sin precedentes. La AEPD tiene la convicción de que una forma efectiva de llegar a los usuarios sería la creación de iconos informativos que, al igual que se han hecho en otros sectores (por ejemplo el tráfico o la seguridad), permitan a los usuarios de Internet conocer las características de los tratamientos que se están llevando a cabo en un contexto concreto. De este modo se ayudaría a un mayor conocimiento y arraigo de una cultura de protección de datos.

La Agenda Española de Protección de Datos propone por tanto:

- Acuñar símbolos o iconos informativos sobre el tratamiento de protección de datos.
- Promover acciones informativas que garanticen su difusión a los ciudadanos
- Reforzar la consideración jurídica del deber de información como pilar fundamental del consentimiento válidamente otorgado.

## NOTIFICACIÓN DE VIOLACIONES DE DATOS PERSONALES

El documento señala de forma acertada la importancia de que los ciudadanos sean oportunamente informados cuando sus datos sean objeto de destrucción o alteración, o cuando se produzcan accesos por parte de personas no autorizadas a dichos datos. La reciente reforma de la Directiva sobre la privacidad y las comunicaciones electrónicas, que incluye la obligación de notificación en el sector de las telecomunicaciones, ha sido un primer paso sobre el que la Comisión se compromete a estudiar la extensión de dicha obligación a otros sectores siempre, según se detalla, garantizando un enfoque sistemático y coherente a ese respecto.

La Agencia Española de Protección de Datos considera esta iniciativa de particular importancia al entender que la extensión de dicha obligación a otros sectores de actividad – como pudieran ser el financiero, el sanitario o la Administración Pública – redundaría en beneficio de los individuos cuyos datos son tratados, favorece la transparencia en la información que se proporciona a los ciudadanos y garantiza un mejor cumplimiento de las obligaciones existentes en materia de seguridad de la información.

No obstante lo anterior, esta Agencia entiende que la adopción de esta medida ha de hacerse buscando el necesario equilibrio con el resto de las obligaciones que afectan al responsable del tratamiento y teniendo en cuenta su impacto sobre las actividades de control de cumplimiento normativo. En ese sentido, se considera de capital interés que el marco normativo resultante de la reforma armonice los procedimientos y modalidades de notificación a las autoridades de control y a los afectados, la definición de los umbrales de notificación y el reflejo que dichos procedimientos tengan en relación con las actividades de cumplimiento normativo. Un marco común de referencia para las notificaciones permitiría igualmente la obtención de información e indicadores a nivel de la Unión, lo que redundaría de forma directa en un mejor conocimiento y evaluación de la evolución en este ámbito.

La obligación de notificación de las violaciones de datos personales ha de ser un instrumento ágil que beneficie principalmente al ciudadano y que, sobre esa base, garantice de forma equilibrada el cumplimiento de las obligaciones atinentes a los responsables del tratamiento y las autoridades de control.

Por tanto, la Agencia Española de Protección de Datos considera necesario:

- La ampliación de la obligación de notificación de violaciones de datos personales a otros sectores de actividad
- Que se creen mecanismos que aseguren la armonización de los procedimientos y modalidades de notificación de violaciones de datos personales.
- Que dichos procedimientos, garantizando los derechos de los titulares de los datos, hagan posible, de forma equilibrada, el cumplimiento de las obligaciones que afecten a los responsables de ficheros y tratamientos y a las autoridades de control.

## REFORZAR EL CONTROL SOBRE LOS PROPIOS DATOS

La AEPD acoge con satisfacción la preocupación manifestada por la Comisión sobre la necesidad de clarificar el llamado “derecho al olvido”, en especial en Internet. En su papel de

autoridad nacional de supervisión, esta Agencia aprecia que aparecer en buscadores o redes sociales plantea, para muchos usuarios, problemas personales, sociales y laborales; y que muchos de ellos desearían que dicha información personal dejase de estar disponible en la Red, borrándose el rastro creado durante el tiempo que utilizaron Internet.

El actual marco normativo europeo en materia de protección de datos ofrece, en nuestra opinión, mecanismos suficientes para concretar este derecho:

- Por un lado, una de las características fundamentales de todo consentimiento es que puede ser revocado.
- Por otro, el artículo 6.1.c) de la Directiva establece expresamente que los datos objeto de tratamiento no podrán ser excesivos. Del mismo modo, el artículo 6.1.d) recoge que “deben tomarse todas las medidas razonables para que aquellos datos inexactos e incompletos (...) sean suprimidos o rectificadas”.
- Asimismo, el artículo 12.b) garantiza el derecho del interesado a obtener del responsable del tratamiento, “en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos”.
- E igualmente, el artículo 14 sanciona el denominado derecho de oposición.

Todos estos mecanismos, adecuadamente combinados, deberían permitir un ejercicio efectivo del llamado “derecho al olvido”. No obstante, el marco comunitario debe clarificar las posibilidades del ejercicio de dicho derecho a través de medidas de obligado cumplimiento para los responsables del tratamiento, que garanticen mecanismos sencillos para su ejercicio, la adopción de tecnologías que impidan la indexación de datos de carácter personal por motores de búsqueda y su aplicación efectiva en plazos perentorios.

Por todo lo anterior, esta Agencia propone:

- Establecer condiciones que permitan la utilización eficiente de los mecanismos que, en la actualidad, permiten el ejercicio del llamado “derecho al olvido”.
- Articular estos mecanismos para que permitan tanto suprimir la información, como evitar su indexación por motores de búsqueda y prohibir su conservación y uso por parte de terceros.

## **CATEGORÍAS ESPECIALES DE DATOS**

La AEPD coincide con la Comisión en que es necesario revisar las disposiciones relativas a las categorías especiales de datos. En la actualidad, como bien recoge la Comunicación, el tratamiento de datos relativos a dichas categorías está prohibido con carácter general, con excepciones limitadas bajo algunas condiciones y garantías. En opinión de esta Agencia, en las actuales circunstancias tecnológicas y sociales se hace necesario ofrecer un régimen de protección que, siendo profunda y escrupulosamente garantista, arroje cierta flexibilidad sobre este tipo de tratamientos.

Documentos de amplia aceptación internacional, como el Convenio 108 del Consejo de Europa<sup>1</sup> o la denominada Resolución de Madrid<sup>2</sup>, abordan esta problemática permitiendo con carácter general el tratamiento de este tipo de datos, a condición de que se establezcan garantías apropiadas para preservar los derechos de los interesados, fijándose para ello las condiciones adicionales que resulten necesarias. Esta aproximación resulta, desde nuestro punto de vista, más equilibrada que la basada en una mera prohibición, permitiendo además adecuar las garantías a establecer a cada caso concreto, en función de criterios como riesgo derivado de su posible utilización indebida, o las naturaleza más o menos íntima de los datos de carácter personal en cuestión. De esto modo, aclarar la posibilidad de discriminar distintos niveles de protección para las actuales categorías especiales de datos permitiría diferenciar las garantías exigibles, por ejemplo, a la información sanitaria básica y a otras más sensibles como puede ser la información relativa al VIH o a la psiquiatría.

Ello no es óbice para que nuevas categorías de datos sean incluidas expresamente en los listados actualmente en vigor, en especial los relativos a la información genética de las personas.

Por todo ello, esta Agencia sugiere:

- Sustituir, con carácter general, la prohibición para tratar datos relativos a categorías especiales por la obligación de establecer garantías apropiadas para garantizar que su tratamiento preserva los derechos de los interesados.
- Analizar las ventajas que implicaría añadir nuevas categorías de datos a los listados actuales, y la mención expresa de otras, como los datos genéticos.

## RÉGIMEN SANCIONADOR

Señala la Comisión respecto al régimen sancionador en materia de protección de datos que va a evaluar la necesidad de reforzar las disposiciones vigentes en materia de sanciones, utilizando como ejemplo el uso de sanciones penales para las violaciones de las normas de protección de datos, con el fin de reforzar su eficacia.

En el marco de su experiencia como autoridad de control, la Agencia Española de Protección de Datos entiende que las sanciones en el marco de normas administrativas especializadas son en general más eficaces que el régimen penal, a la vez que garantizan la protección de los derechos de las partes y la posibilidad de control judicial posterior.

Por otro lado, sería deseable que la reforma contemplara una mínima armonización en el régimen sancionador aplicable a nivel de la Unión, que garantizara un cierto grado de equivalencia en las sanciones a imponer por hechos similares en los diferentes Estados miembros. La graduación de las sanciones, particularmente cuando se trate de sanciones pecuniarias, debería tener en consideración criterios objetivos de evaluación de la gravedad de los hechos, pudiendo servir como ejemplo aquellos basados en los beneficios obtenidos

<sup>1</sup> Convenio del Consejo de Europa para la protección de las personas en relación con el tratamiento automatizado de sus datos personales, de 28 de enero de 1981 (ETS nº 108).

<sup>2</sup> Resolución de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, de 5 de noviembre de 2009, sobre Estándares Internacionales de Privacidad.

por la comisión del ilícito, el tamaño de la empresa o entidad así como la evaluación del daño causado a los individuos afectados.

No obstante lo anterior, la Agencia Española de Protección de Datos ve con satisfacción la posibilidad de ampliar la capacidad de recurso a órganos jurisdiccionales a las autoridades de control.

De este modo, la Agencia Española de Protección de Datos considera:

- Que la adopción de un régimen sancionador basado en normas administrativas especializadas redundaría en una mejor protección y en un sistema más eficiente.
- Que se debe armonizar el régimen sancionador a nivel de la Unión con el fin de garantizar que hechos similares se evalúan y sancionan, en su caso, con los mismos criterios y efectos.
- Que el régimen sancionador ha de basarse, siempre que sea posible, en el uso de criterios objetivos de evaluación de la gravedad de los hechos que permitan la modulación de las sanciones.

### **CLARIFICAR LAS NORMAS RELATIVAS A LA LEGISLACIÓN APLICABLE**

En un mundo globalizado y tecnificado, revisar y clarificar las normas relativas a la legislación aplicable en el ámbito de protección datos cobra una importancia capital. Es por ello que no podemos sino acoger favorablemente esta iniciativa, y proponemos un criterio doble para su implementación:

- Para aquellos tratamientos realizados en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio de un Estado miembro, proponemos conservar el actual modelo de determinación de la ley aplicable. En tal sentido, resulta de vital importancia consolidar el criterio asentado por el Grupo del Artículo 29 en su Dictamen 8/2010, según el cual “el elemento decisivo para calificar que un establecimiento está sometido a la Directiva es el ejercicio real y efectivo de actividades, en el contexto de las cuales se traten datos de carácter personal”,<sup>3</sup> con independencia de la forma jurídica bajo la que se desarrollen dichas actividades o de los acuerdos privados a los que se pretendan someter.
- En cuanto a aquellos responsables del tratamiento no establecidos en el territorio de la Unión Europea, y como criterio complementario (o incluso sustitutivo) al tradicional de recurrir a medios situados en dicho territorio, se propone que les sea de aplicación la legislación de aquellos Estados miembros a los que dirijan específicamente sus servicios. Es este un criterio ampliamente consolidado en España, introducido por el artículo 4 la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico; y compatible a su vez con los criterios de competencia establecidos por el Reglamento (CE) 44/2001, del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el

<sup>3</sup> Dictamen 8/2010 del Grupo del Artículo 29, de 16 de diciembre, sobre Ley Aplicable.

reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Del mismo modo, sería aconsejable aclarar la expresión “recurrir a medios”, tanto en lo relativo a su alcance como a su diferente redacción en las distintas versiones lingüísticas de la Directiva. En tal sentido, nos remitimos al citado dictamen 8/2010 del Grupo del Artículo 29, y en especial a sus páginas 23 in fine y siguientes.

De este modo, la AEPD entiende necesario:

- Consolidar el concepto de “establecimiento” conforme a la interpretación dada por el Grupo del Artículo 29.
- Aplicar, a aquellos responsables del tratamiento no establecidos en territorio de la Unión Europea, la legislación de aquellos Estados miembros a los que dirijan específicamente sus servicios.

### **FOMENTAR LAS INICIATIVAS EN MATERIA DE AUTORREGULACIÓN**

La Agencia Española de Protección de Datos celebra la decisión de la Comisión de fomentar las iniciativas de autorregulación y la promoción de códigos de conducta. Estos códigos de conducta suponen un paso adelante para que los diferentes sectores se adapten a las particularidades de la protección de datos, teniendo en cuenta además el dinamismo de algunos de ellos.

Los códigos de conducta pueden suponer una mayor facilidad para adaptarse a los cambios, y un instrumento de valor añadido tanto para los sectores como para los ciudadanos. Estos sistemas de autorregulación deben garantizar la representación del sector, gozar de credibilidad y garantizar la actualidad de sus disposiciones. Sería importante que existiera un mecanismo claro de acreditación de la adhesión a estos instrumentos, de forma que exista una transparencia y sean identificadas las entidades comprometidas.

Además sería preciso que el nuevo texto de la directiva recogiera elementos que aseguren el cumplimiento del mismo mediante la posibilidad de realizar auditorias eficientes, creando sistemas de control de cumplimiento y respeto por la normativa y pudiendo actuar ante eventuales incumplimientos de las normas del código y de la legislación vigente. Estos sistemas habrán de recoger mecanismos internos de control que impliquen consecuencias para aquellas empresas que incumplan lo en ellos estipulado, no sustituyendo en ningún caso las competencias de las autoridades de protección de datos ni la sanción que eventualmente se pueda imponer por incumpliendo.

Por otro lado, la AEPD apoya la posibilidad de instaurar regímenes europeos de certificación siempre que estos sean objetivos y de calidad suficiente.

Visto lo anterior, la AEPD opina que:

- Estos sistemas de autorregulación deben garantizar la representación del sector, gozar de credibilidad y garantizar la actualidad de sus disposiciones.
- Deberán contar con sistemas internos de control de cumplimiento, que no sustituyan

una eventual inspección por parte de la autoridad de protección de datos ni su régimen sancionador.

## **TRANSFERENCIAS INTERNACIONALES DE DATOS**

El movimiento internacional de datos constituye uno de los mayores riesgos que el tratamiento de datos personales puede generar en la protección de la privacidad de las personas. Sin embargo, resulta impensable el desarrollo y mantenimiento de un sistema como el actual, caracterizado por un importante componente de globalización, sin que dichos movimientos se lleven a cabo en la práctica.

La creación, por parte del Grupo del Artículo 29, de las denominadas “Normas Empresariales Vinculantes”, supuso la introducción de un elemento de flexibilización en lo que a la autorización de transferencias internacionales de datos en el seno de multinacionales se refiere. La AEPD acoge con satisfacción la iniciativa de la Comisión de mejorar y facilitar su aplicación, instándola respetuosamente a prever expresamente su existencia, de cara a posibilitar su aplicación (y su aprobación mediante un procedimiento de reconocimiento mutuo) en todos los países de la Unión Europea.

En relación con lo anterior, avances tecnológicos como la “informática en la nube” demuestran que, en la práctica, aquellas multinacionales dedicadas a la prestación de servicios globales a terceros precisan de un instrumento análogo a dichas Normas Empresariales Vinculantes, de aplicación a los denominados “encargados de tratamiento”, que garantice un nivel adecuado de protección en lo que al tratamiento de datos personales dentro de su estructura empresarial se refiere. En este sentido, la creación de tal instrumento debería ser igualmente prioritaria, pudiendo tomarse como referencia los principios establecidos en la Decisión de la Comisión 2010/87/UE, que deberían ser aplicables a su vez a la situación descrita en el considerando vigésimo tercero de dicha Decisión.

La AEPD entiende, asimismo, que la propuesta introducida por la citada Resolución de Madrid en lo que a transferencias internacionales de datos se refiere (en concreto, su apartado 15) resultaría de gran utilidad de cara a la mejora y racionalización de los procedimientos actualmente en vigor. En tal sentido, es de destacar que países como México han adoptado como modelo este documento, tendencia que se sucede en toda Latinoamérica, y que no debe obviarse. De decidirse la inclusión en el futuro marco legislativo del denominado “principio de rendición de cuentas”, o “accountability”, el control previo de la adecuación podría recaer en el propio exportador de datos, reservándose el trámite burocrático de la autorización previa para aquellos supuestos en los que el riesgo para los interesados fuese especialmente elevado (movimientos internacionales de datos considerados especiales, por poner un ejemplo). De este modo, quien pretenda realizar la transferencia debería cerciorarse de que la misma se realiza con pleno respeto a las exigencias contenidas en la normativa europea, debiendo rendir cuentas frente a la autoridad de supervisión y frente a los propios interesados de que ha recabado todas las garantías necesarias para que la transferencia cumpla con el marco jurídico vigente y no perjudique los derechos e intereses de los interesados.

Del mismo modo, y en relación con la evaluación del carácter adecuado del nivel de protección garantizado por un tercer país, los criterios y condiciones aplicables han de tener en cuenta las particularidades jurídico-constitucionales de los Estados sometidos a evaluación. Ello permitiría crear un procedimiento que, sin dejar de ser riguroso, contase con la suficiente flexibilidad como para poder abarcar a estados que no ofrezcan un nivel de protección “equivalente” al europeo, pero sí un nivel que pueda ser considerado “adecuado”.

Finalmente, resulta fundamental introducir un mecanismo que aclare las garantías exigibles para la realización de transferencias internacionales de datos entre administraciones públicas ubicadas en diferentes países.

Por todo lo anterior, la AEPD recomienda:

- Incorporar expresamente las “Normas Empresariales Vinculantes” al nuevo marco jurídico europeo de protección de datos.
- Explorar la posibilidad de crear un instrumento análogo para aquellas multinacionales que se dediquen a prestar servicios de tratamiento de datos a terceros, con especial atención a la llamada “informática en la nube”, en la línea de los principios establecidos por la Decisión de la Comisión 2010/87/UE.
- Analizar la posibilidad de que el control previo sobre determinadas transferencias internacionales de datos sea realizado por el exportador, conservando en todo caso las autoridades de supervisión la facultad de realizar controles “a posteriori”.
- Adaptar los criterios y condiciones de adecuación a la realidad jurídica de los Estados evaluados.
- Introducir un mecanismo de transferencia internacional de datos entre organismos públicos.

## REFUERZO DEL MARCO INSTITUCIONAL

La Agencia Española de Protección de Datos agradece el reconocimiento expreso del papel de las autoridades nacionales de control en el control de la aplicación de las normas de protección de datos, como guardianes independientes del derecho fundamental a la protección de los datos personales. Igualmente, coincide en la necesidad de reforzar la cooperación entre dichas autoridades y de coordinar mejor las actividades que impliquen a varias de ellas, sobre todo en el marco de problemas de dimensión transfronteriza.

En este sentido, y reconociendo los beneficios que aportará el refuerzo de las tareas y competencias del Grupo de Trabajo del Artículo 29, la Agencia entiende que se debe hacer especial hincapié en las mejoras en los procedimientos de cooperación e intercambio de información entre las autoridades de control nacionales, así como en el diseño de un marco que permita el desarrollo de actividades conjuntas con plena seguridad jurídica, incluyendo los aspectos de cumplimiento normativo, con autoridades de control fuera del ámbito de la Unión Europea.

De particular interés sería permitir la posibilidad de que una autoridad de control pudiera participar con pleno amparo legal en actividades de investigación y auditoría realizadas en

otro Estado miembro cuando los hechos objeto de análisis afecten a individuos bajo su tutela, y que el resultado de dichas investigaciones pueda ser utilizado con plena eficacia, en su caso, en el marco del régimen sancionador aplicable en su jurisdicción.

Por tanto, a tenor de lo anterior, la Agencia Española de Protección de Datos propone:

- La mejora en los procedimientos de cooperación e intercambio de información entre las autoridades de control nacionales
- El diseño de un marco legal que permita el desarrollo conjunto de actividades de cooperación y cumplimiento normativo, incluyendo, con las debidas garantías, a aquellas que se realicen con autoridades fuera del ámbito de la Unión.
- Extender el ámbito de actuación de las autoridades de control a otros Estados miembros cuando los hechos objeto de investigación así lo justifiquen.