Training of Lawyers on the European Data Protection Reform

#TRADATA

THE ROLE OF THE DATA PROTECTION OFFICERS AND OF THE EDPS

"IN GOD WE TRUST - EVERYONE ELSE WE AUDIT"

Diana Alonso Blas, DPO and Head of the DP service at Eurojust

Topics

- The role of the DPO so far
- EU DPOs professional standards
- The role of the DPO in the GDPR
- Own experience: DPO of Eurojust.
- The role of the EDPS

Data Protection Officers in the EU now: Family picture

The DPO in Directive 95/46/EC

Article 18

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
  - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
  - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

  thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

Regulation 45/2001

Regulation (EC) No 45/2001 provides that every Community institution and body must appoint a **Data Protection Officer (DPO)**. He or she is fundamental in ensuring that these administrations respect their data protection obligations. Some institutions have also provided for an assistant or deputy DPO. The European Commission has appointed a **Data Protection Coordinator (DPC)** in each directorate-general (DG). This has been justified by the size of the institution and the necessity to have relays in the different DGs. It has also appointed a specific DPO for OLAF.

Some DPOs were appointed even before the EDPS started his activities, some after. They have proved to be of high importance, not only because of their internal work within the institution or body, but also in the establishment of a DPO network. This network, which meets at regular intervals, has been a useful forum for exchanging views on common issues and to provide advice. Apart from bilateral meetings and contacts with the DPOs, the EDPS also takes part in the regular meetings of the DPO network. These meetings serve as useful means for exchange of information and discussions on current issues.

The Data Protection Officers have various functions:

•ensuring that controllers and data subjects are informed of their rights and obligations;

•ensuring in an independent manner the internal application of the Regulation;

•carrying out inquiries where necessary;

•keeping a register of the processing operations carried out by the controller;

•notifying the EDPS of processing operations which may present specific risks;

•responding to requests from the EDPS and cooperating with the EDPS.

* * *

“DPO shall ensure…

… that rights and freedoms of data subjects are unlikely to be adversely affected by the processing operations.” Reg. 45/2001 Art 24.1

Data Protection officers check and monitor compliance with data protection rules.

Professional Standards for EU DPOs

- Paper drafted together with Laraine L. Laudati (DPO OLAF) on professional standards for DPOs of the EU institutions and bodies and adopted at DPOs meeting in London on 14th October 2010.
- EDPS has "very much welcomed and endorsed this excellent paper which underlines the importance of the work and role of the DPO in the achievement of compliance with DP rules".
- Purpose of this tool is 1) to assist DPOs in performing their duties, and 2) to assist institutions/bodies to select a qualified DPO and to understand the role of the DPO
- Available on EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/10-10-14_DPO_Standards_EN.pdf

DPO profile

- Art. 24.2 of Reg. 45/2001: "The DPO shall be selected on the basis of his or her personal and professional qualities and, in particular, his or her expert knowledge of data protection"
- Best Practices:
  - More knowledge and experience if DP related to core business (7 yrs as compared to 3 yrs, if not related to core business)
  - Knowledge of legal framework, institution
- Opportunity for regular training and certification (EIPA course)
- Independence: DPO position weakened if part-time, limited contract, reporting to a HoU or director .

DPO Status

- **Best practices**

1. DPO post as Advisor, HoU or Director
2. Five year appointment
3. Permanent contract, sufficient experience
4. Full time for large institutions/bodies, and in initial period for small ones
5. Additional DP Staff, where DP is core business
6. Cooperation from all staff assured in rules
7. DPO should report directly to head of institution/body
8. EDPS given opportunity to provide input on performance review
9. DPO's own budget line
10. DPO signing power for DP correspondence

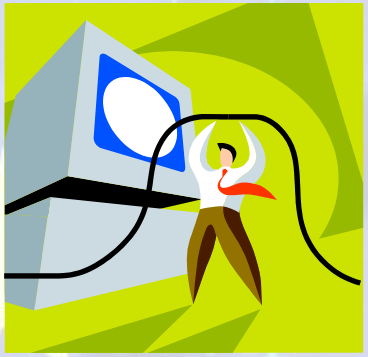
DP

DATA PROTECTION OFFICER

DPO duties

- Duty to inform
  - Controllers
  - Data Subjects
- Duty to cooperate with EDPS
- Duty to maintain a register of processing operations
- Duty to notify EDPS of risky processing operations
- Duty to provide appointing institution/body with recommendations and advice
- Duty to ensure compliance
- Duty and power to investigate

Best practices

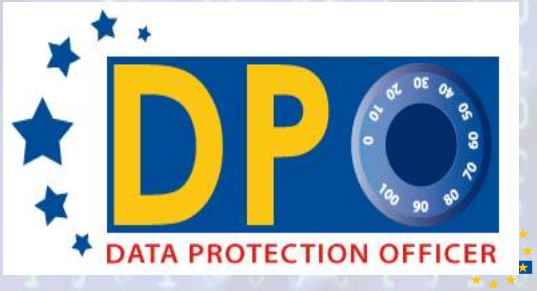


- Periodic DPO report
- Work Programme
- Involvement in relevant discussion groups
- Network of DP coordinators
- (DP website)

DP
DATA PROTECTION OFFICER

Ethical Standards

- Duty of loyalty
- Need to know
- Duty of confidentiality
- Conflict of interest



Relations between the DPO and the EDPS

- Exchange of views and information
- Inspections
- Complaints

DP
DATA PROTECTION OFFICER

The DPO after the DP reform

- Article 37 of the GDPR introduces:

  - a mandatory DPO for the public sector/private sector if regular and systematic monitoring of data subjects in a large scale or large scale processing of special categories of data or data related to criminal convictions and offences

  - Possibility for a single DPO for groups of undertakings or for several authorities or bodies taking into account their organisational structure and size

  - requirements for the DPO professional profile: expert knowledge of DP law and practices and ability to fulfil the tasks referred to in art 30

  - obligation to communicate to the DPA and the public the name and contact details of the DPO

The DPO after the DP reform II

Article 38 - the position of the DPO

Obligations to the controller/processor:

- to involve properly and timely the DPO in all issues related to the protection of personal data
- to support the DPO in performing the tasks and provide resources necessary to carry out tasks and access to data and processing operations and maintain the expert knowledge.
- to ensure that the DPO does not receive any instructions. The DPO directly reports to the highest level of management of the controller/processor.
- Data subjects may contact DPO with regard to all issues and exercises of rights
- Confidentiality obligations
- No conflict of interests

The DPO after the DP reform III

Article 39 - tasks of the DPO

- to inform and advise the controller/processor
- to monitor compliance with this Regulation, other applicable rules and with policies of the controller/processor, including the assignment of responsibilities, awareness and training of staff and audits
- to provide advice as regards the data protection impact assessment and monitor its performance
- to cooperate with DPA
- to act as the contact point for the DPA and consult with the DPA, including the prior consultation

DPOs in the future

- The role of the DPOs has been acknowledged within EU institutions, bodies and agencies as a key instrument to build compliance
- Big international companies have built on this idea by appointing “Chief Privacy Officers”
- The EU reform will undoubtedly increase its role

Eurojust

© Corné Bastiaansen, Rijksvastgoedbedrijf 2017

- **What Is Eurojust?**
  Eurojust is a (new) European Union body established in 2002 to enhance the effectiveness of the competent authorities within Member States when they are dealing with the investigation and prosecution of serious cross-border and organised crime.

  What Is Eurojust Doing?
  Eurojust stimulates and improves the co-ordination of investigations and prosecutions between competent authorities in the Member States. Eurojust improves co-operation between the competent authorities of the Member States, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests. Eurojust supports the competent authorities of the Member States in order to render their investigations and prosecutions more effective when dealing with cross border crime.
- Increasing caseload: from 192 cases in 2002 to 2550 in 2017 .

My own experience

DPO at Eurojust

- **Internal control: DPO (article 17 EJ Decision).**
- **Independence.**
  - Tasks: ensuring compliance and lawfulness in independent manner
  - Access to all data and all premises
  - Issues annual survey on compliance for College and JSB
  - Procedure in case of non-compliance
  - Eurojust postholders can address enquiries, information requests, claims and complaints to DPO. No one shall suffer prejudice!

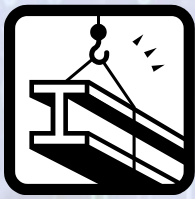
  ➢ DP service is there to advise controllers regarding processing of personal data issues

- **External control: Joint Supervisory Body (Art. 23): Members are judges or equal level of independence. JSB monitors the correct application of the rules on DP and carries out frequent inspections.**

How to get started?

- Learn to know your organisation: core tasks, procedures, management lines and organisation…
- First task should be to inventarise the data processing operations in place, identify the controllers and start building your inventory/notifications and so forth
- Look for allies within the organisation. How can help to build awareness, influence culture and so forth. Build contacts!
- Ensure you become part of the processes and discussions within the organisation, also regarding technical developments.
- Analyse the existing legal framework and see if it is necessary to add, modify, create procedures….Think about complaint handling, access requests, security incidents management and so forth. Obligations of staff members to cooperate with DPO is also key.
- Awareness, awareness, awareness… Use every possible occasion!
- Be proactive and do not wait for people to come to you.

4 main areas of work for DPO EJ



1. **Development of "legislative" framework**: drafting of DP and security rules, security incidents procedure, involvement in third country-agreements, input given in discussion review EJ Decision, new EJ Regulation…
2. **Privacy-compliant/enhancing technological solutions**: close involvement in technological issues such as development/redesign of fully DP compliant CMS, involved in secure network developments, part of security committee advising on most technical matters;
3. **Awareness**: Intranet, induction session for newcomers, additional sessions for certain groups, sessions with administration and College, involvement in College teams, advice on specific issues (on request or proactively)…
4. **Enforcement/ compliance monitoring**: weekly CMS checks+reports, full annual surveys since 2006 on, regular reviews and meetings with persons responsible for main processing operations within administration, several data subject rights requests, complaints and enquiries dealt with. Procedures fully in place now.

Some best practices to "sell" DP within organisation:

1. DPO annual work programme but also try to get DP in other relevant work programmes of the organisation
2. Involvement in relevant discussion groups (such as College teams, meeting of HoU/S with Director)
3. Ensure sufficient bilateral meetings with highest hierarchal level of organisation (president of College)

Very importance to build stable professional relationship with high level players and invest in showing benefits of compliance ("selling the product").

4. Frequent info session, using interesting occasions (DP day, pre inspections, presentation of survey, new issues…). The more focused the presentation, the more interesting for individuals.

Case example: audit and compliance work at Eurojust

- **Based on complementary steps:**
  - weekly CMS checks+reports,
  - monthly time limits reviews
  - full annual surveys reports

- **Information is shared with College and with Joint Supervisory Body who uses it as input for their own inspections**

Weekly checks

- Methodology: every Friday based on a standard checklist going through all main DP issues in the system
- Report produced for own accountability purposes (documentation) but also as basis to raise issues bilaterally or, if more structural, with president/College
- Problems are solved bilaterally but escalation procedure exists in case of need

Monthly time limits reviews

- Carried out around the 20th of every month
- Tolerance limit of 5% applied
- Information sent to every NM as to compliance (white/black list). Non compliance is exceptional and always followed up.
- Compliance is almost 100% since this system is in place

DPO annual survey report

- Article 27.1 of Eurojust DP rules: *the DPO shall run **annual surveys** on the compliance with the DP rules within Eurojust. The DPO shall report to the College and the JSB on the results of these surveys.*
- Excellent opportunity to build close cooperation with controllers and discuss open issues
- Complementary to regular inspections of the JSB and useful tool to keep track of progress made

Methodology of annual survey DPO Eurojust

- Involvement every year of 5 national desks (all covered once at least in meantime): new NMs
- On the basis of an extensive questionnaire covering DP and security issues provided in advance
- Including checks on the spot (office, manual files, etc)
- Checks on the CMS regarding all countries
- Some checks concerning security practices by security unit
- Effort to keep the report rather short and to provide extensive statistical information per national desk
- One administrative unit checked every year. HoU is given chance to comment on findings and follow-up
- Presentation to College including conclusions and best+worst 5 results per topic (wake up call)
- Follow-up is great opportunity to address things

EDPS

- EDPS created as new concept: supervising the institutions regarding processing of personal data and based on Article 286 EC and Regulation 45/2001
- EDPS = Giovanni Buttarelli + Wojciech Wiewiórowski (Assistant Supervisor)
- First EDPS was Peter Hustinx and assistant Joaquin Bayo Delgado
- Needed to harmonise level of protection within institutions with level in Member States (public and private sector).
- Wide responsibility ensuring respect of fundamental rights by EU-institutions.
- Not only supervision (prior checking for instance) but also “consultation” and “cooperation”.
- Very important opinions regarding upcoming EU legislation (website). Influential role
- Role of the EDPS further defined/reconsidered during recast of Regulation 45/2001 (ongoing)

EDPS interaction with DPOs and DPAs

- Role of Data Protection Officers supported by EDPS through network of DPO's to which DPO's of Europol and Eurojust also participate
- EDPS will provide secretariat to EDPB which will start operating on 25/5:
  "EDPB will not be a successor of EU Article 29 Working Party, we will turn a new page. The DPA group is no longer just a consultative body."
- A quarter of EDPS staff will form the secretariat of the EDPB, but they will work separately as already defined in the Memorandum of Understanding between the two bodies.

Any questions?

Contact Information

Diana Alonso Blas

Data Protection Officer

dalonsoblas@eurojust.europa.eu

+31 70 412 5510

www.eurojust.europa.eu

Seguridad de los datos, códigos de conducta, certificación y auditorias.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Seguridad de los datos

La seguridad se configura, en el RGPD, como un <u>principio</u>, según establece su artículo 5; y como una <u>obligación</u> que se desarrolla en el Capítulo IV (Artículos 32 a 34).

(...) teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Seguridad de los datos

- **La seudonimización:** El Reglamento Europeo, en su artículo 4.5, señala que seudonimización es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional.
- **El cifrado de datos personales: A** fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el RGPD, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado.
- La capacidad de garantizar la **confidencialidad, integridad, disponibilidad y resiliencia** permanentes de los sistemas y servicios de tratamiento.

Códigos de conducta

Se puede acreditar el cumplimiento de las medidas de seguridad (artículo 32.3 RGPD) si el responsable o el encargado se han adherido a un Código de conducta.

- **Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del Reglamento.**

- **Aquellos responsables o encargados a los que no es de aplicación el Reglamento pueden (de forma potestativa) adherirse a códigos de conducta aprobados a fin de ofrecer garantías adecuadas en el marco de las transferencias internacionales de datos.**

Training of Lawyers on the European Data Protection Reform

#TRADATA

Códigos de conducta

- El código de conducta debe contener mecanismos que permitan al organismo de control verificar el cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control competentes.

- Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control competente lo presentará por el procedimiento del artículo 63 (**mecanismo de coherencia**), antes de su aprobación o de la modificación o ampliación.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Códigos de conducta

La Disposición transitoria segunda del anteproyecto de LOPD advierte que los promotores de los códigos tipo registrados en la AEPD deben adaptarse al RGPD en el plazo de **un año** desde la entrada en vigor de la reformada LOPD.

En todo caso, **los Códigos Tipo existentes deben adaptarse al Reglamento Europeo de Protección de Datos** para producir los efectos previstos en éste siendo recomendable que incorporen procedimientos extrajudiciales u otros como la mediación para resolver las controversias entre responsables y afectados.

Certificación

El RGPD concede una atención especial a la implantación de esquemas de certificación y ofrece diversas posibilidades para su gestión.

La acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del RGPD será llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones (art. 40 ALOPD).

Certificación

Competencia para expedir certificaciones:

- Los organismos de certificación (artículo 43 RGPD)

- La AEPD, como autoridad de control competente en España, sobre la base de los criterios aprobados por dicha autoridad (de conformidad con el artículo 58.3 RGPD)

- El Comité (de conformidad con el artículo 63 RGPD). En este caso podrá dar lugar a una certificación común: el **Sello Europeo de Protección de Datos.**

Certificación

- La certificación es **voluntaria** y debe estar disponible a través de un proceso transparente (artículo 42.3 RGPD), además, el que una entidad está certificada no limitará su responsabilidad en lo que se refiere al cumplimiento del Reglamento.

- La certificación se expedirá a un responsable o encargado por un **período máximo de tres años** y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos establecidos.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Muchas gracias

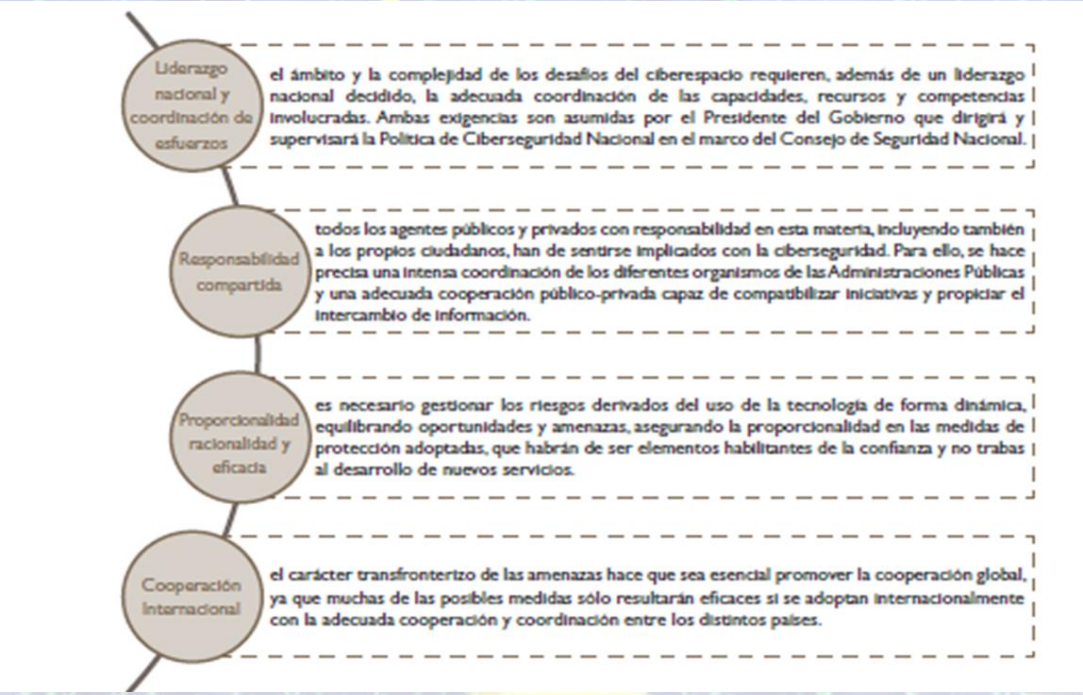
Diego Pérez
finreg360

dperez@finreg360.com

Training of Lawyers on the EU Data Protection Reform (TRADATA)

The project is co-financed with the support of the European Union's Rights, Equality and Citizenship programme

La Estrategia de Ciberseguridad Nacional de 2013 es el **documento estratégico** que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de **implantar** de forma coherente y estructurada acciones de **prevención, defensa, detección, respuesta y recuperación** frente a las ciberamenazas.



Los **principios rectores** de la ECSN consisten en una serie de líneas sobre las que debe construirse la regulación en ciberseguridad.

Estos principios también resultan aplicables a la protección de la información y los datos personales.

Training of Lawyers on the European Data Protection Reform

#TRADATA

LÍNEA DE ACCIÓN 4

Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia

Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.

Esta línea de acción se concentra en combatir el terrorismo y la delincuencia que actúan en el ciberespacio, en su doble vertiente de instrumento facilitador de sus actividades y de objeto directo de su acción. En este concepto se incluyen también las organizaciones que hacen uso de la tecnología para financiarse o lucrarse, posibilitando la comisión de delitos y el blanqueo de capitales.

En esta línea de acción, el Gobierno de España abordará las medidas correspondientes, entre ellas:

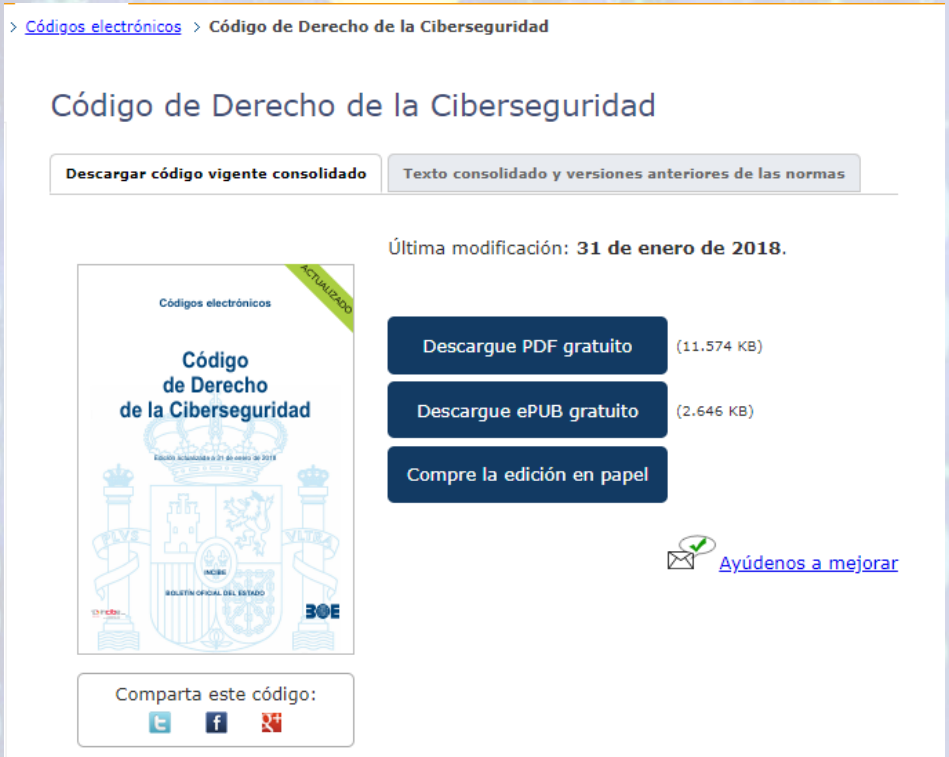
- Integrar en el marco legal español las soluciones a los problemas que surjan relacionados con la ciberseguridad para la determinación de los tipos penales y el trabajo de los departamentos competentes.
- Ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad, a través del intercambio de información e inteligencia por los canales de comunicación adecuados.
- Fortalecer la cooperación policial internacional y fomentar la colaboración ciudadana, articulando los instrumentos de intercambio y transmisión de información de interés policial.
- Asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, es especialmente importante la cooperación con el Consejo General del Poder Judicial, la Abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la Criminalidad Informática y el Consejo General de la Abogacía Española.

La capacitación de los juristas es uno de los objetivos recogidos en la ECSN 2013.

En particular, la línea de acción 4 tiene por objeto potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, **sobre la base de un marco jurídico y operativo eficaz**.

Training of Lawyers on the European Data Protection Reform

#TRADATA



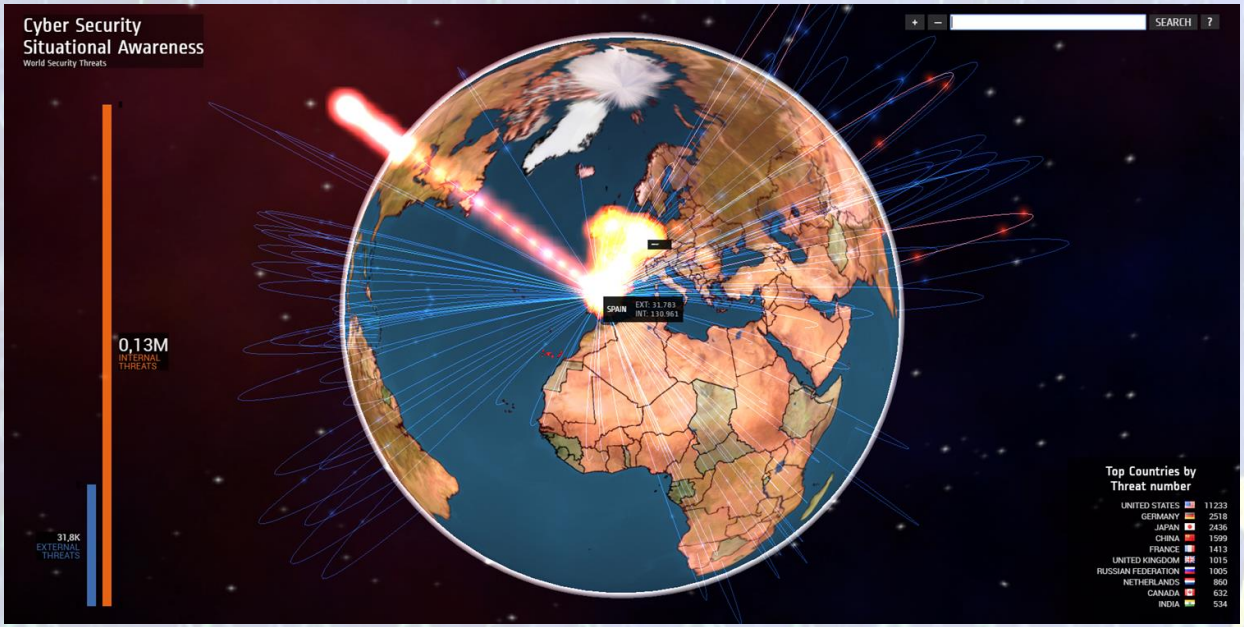
En España, desde el año 2015 existe un código electrónico en el que se compila la normativa que afecta a aspectos relacionados con la ciberseguridad.

Esta regulación nacional se va a incrementar en breve con la publicación de la nueva LOPD, la Ley NIS, y próximamente con la previsible aprobación del Reglamento de e-privacy o la Cybersecurity Act, por citar algunas.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Ciberseguridad y la protección de datos: herramientas para contribuir al mercado digital.



Tanto el RGPD como la Directiva NIS obligan a las organizaciones a implementar **medidas de protección técnicas y organizativas adecuadas y efectivas**:

- El **RGPD** para todas las empresas y administraciones públicas que traten **datos de carácter personal** (*data breach*).
- La **Directiva NIS** sólo para las empresas incluidas en el ámbito de aplicación de la norma, pero para **cualquier tipo de información** que manejen (*security breach*).

Training of Lawyers on the European Data Protection Reform

#TRADATA

El riesgo en el RGPD: la privacidad desde el diseño y el SGSI

Artículo 25. Protección de datos desde el diseño y por defecto (Considerando 83).

1. *Teniendo en cuenta el **estado de la técnica**, el **coste de la aplicación** y la **naturaleza**, ámbito, contexto y fines del tratamiento, así como los **riesgos** de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, **medidas técnicas y organizativas apropiadas**, como la **seudonimización**, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*

Se refiere a la obligación de crear un sistema de gestión de seguridad de la información (SGSI) basado en riesgos, que sea eficaz (ya lo hecho. Pero ¿lo he hecho bien?).

¿El debate DPO/CISO/ Compliance Officer?

O

Un SGSI con RGI

Training of Lawyers on the European Data Protection Reform

#TRADATA

Las iniciativas públicas para la protección de la ciberseguridad

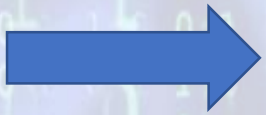
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Medidas preventivas

- Guías, protocolos, políticas
- Alertas
- Formación (MOOC)
- Serious games (Itinerarios)
- Herramientas gratuitas (Test autodiagnóstico, servicio antibotnet, CONAN)
- Kit de concienciación
- Ciberejercicios
- Cibercooperantes
- Teléfono de ayuda

cyberex_

Medidas reactivas

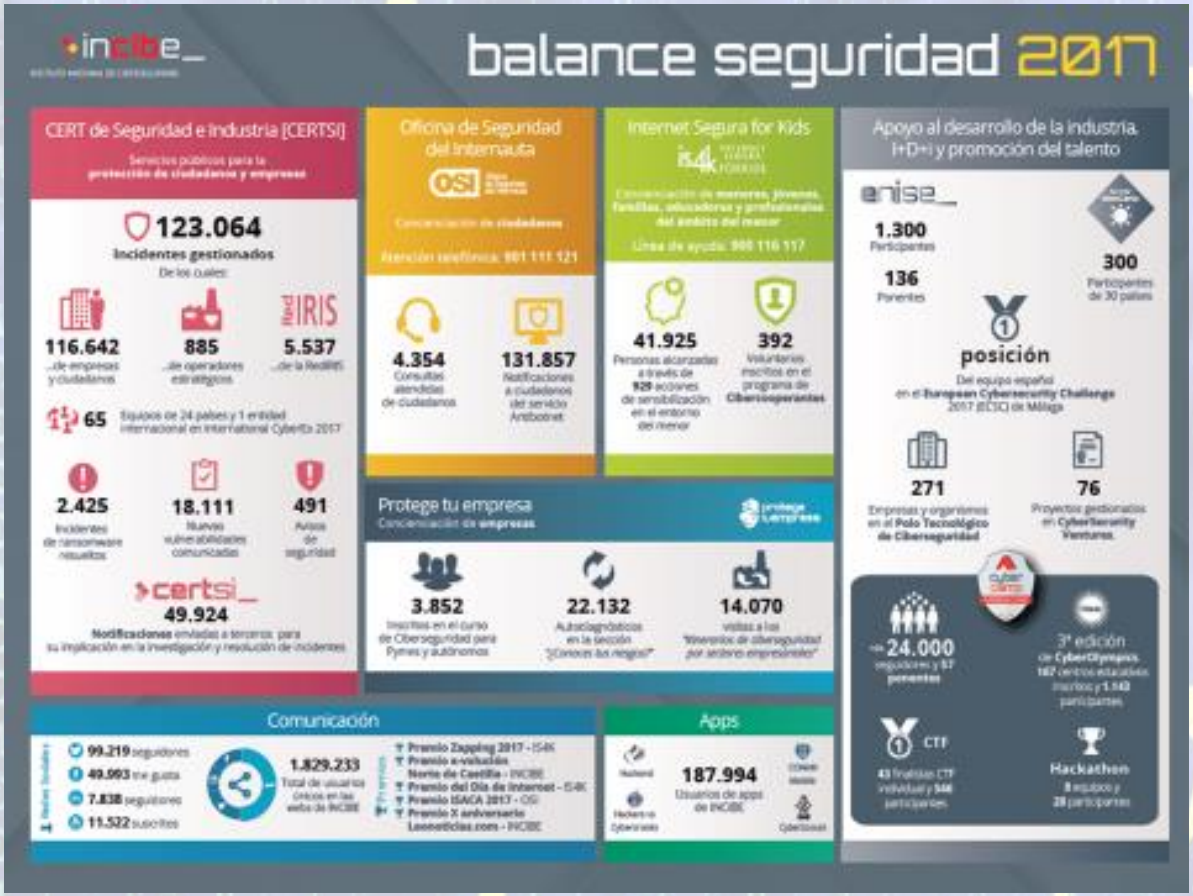


certsi_

Regulado en la DA 9ª de la LSSI y en la Directiva NIS como entidad competente para la gestión de incidentes de ciberseguridad

Training of Lawyers on the European Data Protection Reform

#TRADATA



Confidencialidad: la información sólo debe estar accesible para aquellos que estén autorizados (arquitectura, permisos, auditorías…)

Integridad: la información debe permanecer inalterada y como el emisor la originó, sin manipulaciones externas. (cifrados, IRM…)

Disponibilidad: La información debe estar accesible cuando se requiera (redundancia, monitorización, back ups, centros de contingencia…)

El Considerando 76 del RGPD dice:

> *El riesgo debe ponderarse sobre la base de una **evaluación objetiva** mediante la cual se determine si las operaciones de tratamiento de datos **suponen un riesgo o si el riesgo es alto**.*

Obligación de **análisis de riesgos** (por nivel y por cantidad) **y de implementar medidas** técnicas y organizativas eficaces que eviten daños.

R (riesgo) = P (probabilidad) x I (impacto posible)

La **Probabilidad** es un elemento subjetivo. Si no es = 0, te ocurrirá.

El **Impacto** (como daño interno o externo) y la **responsabilidad** son lo importante.

Por eso es imprescindible hacer **análisis de impacto** (PIA) para evitar o minimizar los posibles daños (físicos, reputacionales, de continuidad de negocio…) y disminuir (buena fe, diligencia…) la responsabilidad legal del responsable (CISO, CEO…).

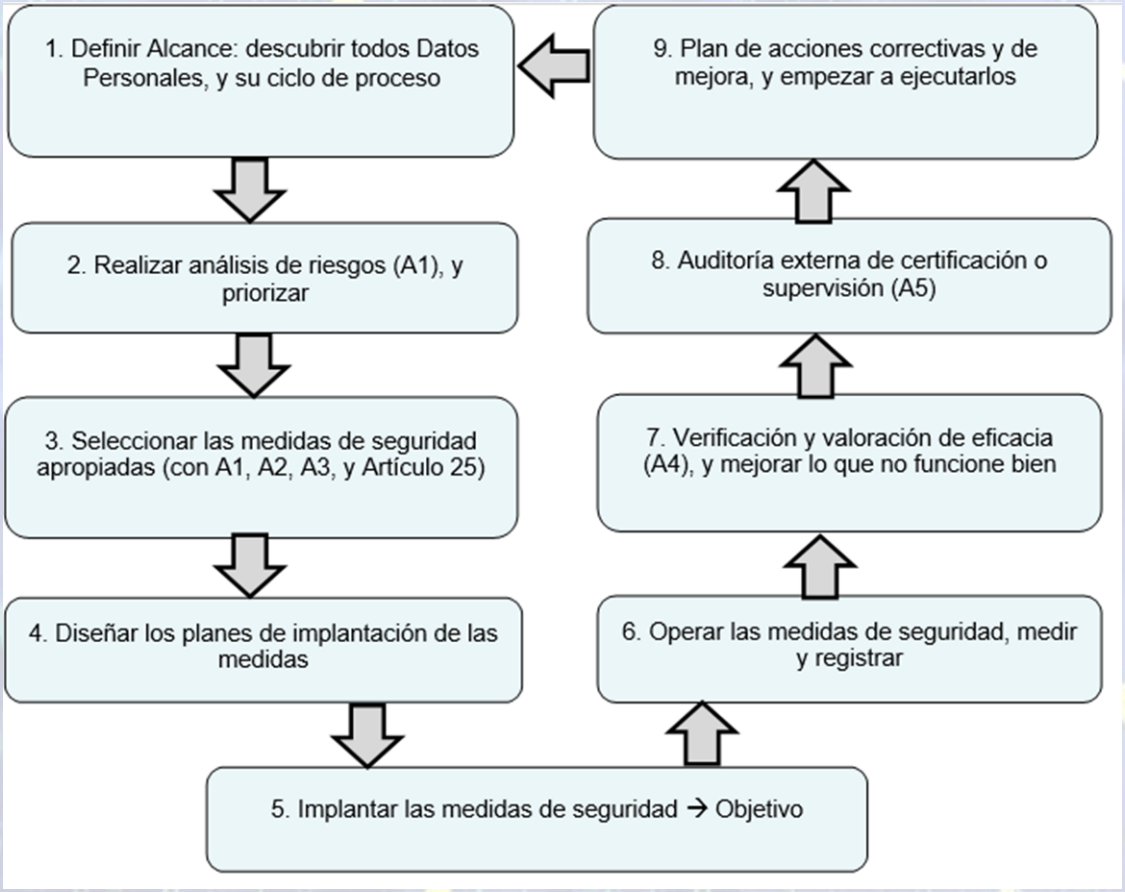
Training of Lawyers on the European Data Protection Reform

#TRADATA

El ciclo de gestión de seguridad de la información

Training of Lawyers on the European Data Protection Reform

#TRADATA



Medidas técnicas: Identificar las medidas adecuadas: disponibles, eficaces y actualizadas. Seguridad por capas

- Herramientas contra la suplantación de identidad
- VPN
- Cifrado
- Antivirus
- Anti-Ddos
- Copias de seguridad
- Prestador cloud
- Antibotnet
- Anti-phishing

Medidas organizativas: procedimientos incluidos en registro de actividades (art. 30 RGPD). Cultura de ciberseguridad

- Formación al empleado y a los directivos
- Concienciación (*awareness*)
- Sensibilización

La seguridad de la información en los despachos de abogados

Training of Lawyers on the European Data Protection Reform

#TRADATA

DLA Piper
Calculating the Cost of NotPetya - June 2018
Direct Costs of IT Staff; Excludes Lost Productivity of Partners and Lawyers

IT Staff:					
Normal Working Day		8	hours	5	days per week
Post-Attack Work Day		21	hours	7	days per week
Average Hourly Rate	$	100.00			
Overtime Rate	$	150.00			
Additional Hours of Overtime		15,000	across "all IT staff"		
Calculations:					
Additional hours of overtime		15,000	hours		
Overtime hours per IT staff		40	normal work week		
		147	post-attack work week		
		107	additional hours per week post-attack		
Number of IT staff		140	(15,000 hours divided by additional hours per staff)		
Cost of Recovery	**$**	**2,250,000**			
For the first two weeks	$	1,507,500			
For the third week	$	742,500			

Note: these are Michael's estimates based on what the article says, not DLA Piper's official numbers

Training of Lawyers on the European Data Protection Reform

#TRADATA

La seguridad de la información en los despachos de abogados

La suplantación de identidad: riesgo de *phishing* y crisis de reputación
Ataques Ddos y *botnets*
Fugas de información y de datos: *insider threats*, fraude del CEO, ingeniería social.
La responsabilidad de administradores y directivos ante fugas de datos
Las pólizas de seguro
El cifrado de comunicaciones en las comunicaciones con el cliente y con los compañeros. Ej: Have I been pwnd?
La seguridad de proveedores y clientes del despacho
Las crisis de comunicación
La responsabilidad deontológica y la obligación de proteger el secreto profesional en el código deontológico: la independencia del abogado (art.2). La confianza en el abogado (art. 4), el secreto profesional (art. 5).

Training of Lawyers on the European Data Protection Reform

#TRADATA

Muchas gracias por su atención

Francisco Pérez Bes
Secretario General
Instituto Nacional de Ciberseguridad de España (INCIBE)

francisco.perez@incibe.es
@pacoperezbes

finReg360

Principios, roles y actores en el nuevo RGPD. Derechos de los interesados.

Javier Aparicio - Abogado
finReg360

ARTICULO 4: DEFINICIONES

7) **«responsable del tratamiento» o «responsable»**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros **determina los fines y medios del tratamiento**, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;
8) **«encargado del tratamiento» o «encargado»**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales **por cuenta del responsable del tratamiento**;
9) **«destinatario»**: la persona física o jurídica, autoridad pública, servicio u otro organismo al que **se comuniquen datos personales**, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;
10) **«tercero»**: persona física o jurídica, autoridad pública, servicio u organismo **distinto** del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un **tercero**, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Artículo 13 Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, **el responsable del tratamiento**, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación

Artículo 14 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, **el responsable del tratamiento** le facilitará la siguiente información

Artículo 15 Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener **del responsable del tratamiento** confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información

Artículo 16 Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida **del responsable del tratamiento** la rectificación de los datos personales inexactos que le conciernan.

Artículo 17 Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida **del responsable del tratamiento** la supresión de los datos personales que le conciernan

Artículo 18 Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener **del responsable del tratamiento** la limitación del tratamiento de los datos

Artículo 19 Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los **destinatarios** a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20 Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un **responsable del tratamiento**

Alcalá 85 · 28009 Madrid · Spain
finreg360.com

Training of Lawyers on the EU Data Protection Reform (TRADATA)

Jurisprudencia del TEDH y del TJUE: casos claves y recientes

JUAN JOSÉ TALENS LLINÁS
ABOGADO
TUTOR NACIONAL DEL PROGRAMA HELP DEL CONSEJO DE EUROPA

The project is co-financed with the support of the European Union's Rights, Equality and Citizenship programme

Training of Lawyers on the European Data Protection Reform

#TRADATA

Reglamento (UE) 2016/679 del Parlamento y del Consejo

“El tratamiento de datos personales debe estar concebido para servir a la humanidad.”

Considerando (4)

Training of Lawyers on the European Data Protection Reform

#TRADATA

- El derecho a la privacidad y el derecho a la protección de datos están garantizados por instrumentos jurídicos desarrollados tanto por el Consejo de Europa como por la Unión Europea.

- Estos dos ordenamientos europeos convergen a menudo, pero también difieren en ciertos aspectos, y ambos tienen que ser tomados en consideración por los profesionales del Derecho cuando se trata de los derechos a la privacidad y a la protección de datos.

Training of Lawyers on the European Data Protection Reform

#TRADATA

En el Derecho de la UE, el derecho al respeto de la vida y el derecho a la protección de datos han sido reconocidos como derechos fundamentales separados, protegidos respectivamente por el Artículo 7 y el Artículo 8 de la Carta de los Derechos Fundamentales (la Carta de la UE).

En el Derecho primario de la UE, se establece la competencia general de la UE para legislar sobre cuestiones de protección de datos de acuerdo con el Artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE).

El principal instrumento del Derecho derivado de la UE sobre protección de datos es actualmente la Directiva sobre Protección de Datos (DPD), sustituida por el Reglamento General de Protección de Datos (RGPD), aprobado en abril de 2016 y que entrará en vigor en mayo de 2018.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Los derechos a la privacidad y a la protección de datos personales están protegidos en virtud del Artículo 8 del Convenio Europeo de Derechos Humanos, que garantiza el derecho al respeto de la vida privada y familiar, de domicilio y de correspondencia.

Existe también un instrumento vinculante fundamental elaborado por el Consejo de Europa que regula específicamente la protección de datos: el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (también conocido como el Convenio nº 108).

Artículo 8 Convenio Europeo de Derechos Humanos (CEDH)

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Training of Lawyers on the European Data Protection Reform

#TRADATA

El Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos personales (Convenio nº108) se abrió a la firma en 1981 y entró en vigor en 1985. Es el primer instrumento internacional jurídicamente vinculante que regula explícitamente la protección de datos. En 2001, se adoptó un Protocolo Adicional al Convenio nº108, que establece disposiciones sobre las transferencias transfronterizas de datos a terceros países y sobre el establecimiento obligatorio de las autoridades nacionales de protección de datos. Todos los Estados miembros de la UE son partes del Convenio nº108.

Actualmente el Convenio está en proceso de modernización:
https://www.coe.int/en/web/data-protection/convention108/modernised

Training of Lawyers on the European Data Protection Reform

#TRADATA

En 2000, la UE proclamó la Carta de los Derechos Fundamentales de la Unión Europea (la Carta).

La Carta incorpora todo el abanico de derechos civiles, políticos, económicos y sociales de los ciudadanos europeos, sintetizando las tradiciones constitucionales y las obligaciones internacionales comunes a los Estados miembros.

La Carta adquirió fuerza jurídica vinculante como Derecho primario de la UE en 2009. Las instituciones de la UE, así como los Estados miembros, al aplicar el Derecho de la UE, deben respetar y garantizar los derechos incluidos en la Carta (artículo 51 de la Carta).

Training of Lawyers on the European Data Protection Reform

#TRADATA

Los derechos a la vida privada y familiar y a la protección de datos están protegidos por las siguientes disposiciones de la Carta:

Artículo 7.-
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Artículo 8.- Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Training of Lawyers on the European Data Protection Reform

#TRADATA

La tarea principal del TJUE en Luxemburgo es garantizar que la legislación de la UE se interprete y se aplique de la misma manera en todos los países de la UE, así como garantizar que los Estados miembros y las instituciones se rijan por la legislación de la UE. En el ámbito de la privacidad y de la protección de datos, el TJUE es competente para determinar si un Estado miembro ha cumplido con sus obligaciones en virtud de los artículos 7 y 8 de la Carta de los Derechos Fundamentales, con el objetivo de asegurar su aplicación efectiva y uniforme en toda la UE.

Training of Lawyers on the European Data Protection Reform

#TRADATA

ALGUNOS PRONUNCIAMIENTOS SOBRE CUESTIONES DE CONCEPTO

En Rotaru vs Rumania, en relación con un fichero conservado por los servicios de seguridad con información sobre la vida del demandante, de más de cincuenta años de antigüedad, el TEDH consideró que el tratamiento de la información recogida durante cincuenta años sobre la vida privada entra en el ámbito de "vida privada" a los efectos del artículo 8.1 del Convenio.

El TEDH estimó una violación del artículo 8 del CEDH, porque la ley rumana permitía la recogida, el registro y el archivo de información secreta que afectaba a la seguridad nacional, sin establecer límites en el ejercicio de estas actividades, manteniéndose a la discreción de las autoridades. Por ejemplo, la legislación nacional no definía el tipo de información que podía ser tratada, las categorías de personas contra las que se podrían tomar medidas de vigilancia, las circunstancias en las que podrían adoptarse tales medidas o el procedimiento a seguir. Debido a estas deficiencias, el TEDH concluyó que la legislación nacional no se ajustaba a la exigencia de previsibilidad en virtud del artículo 8 del Convenio Europeo y, en consecuencia, entendió que dicho artículo había sido vulnerado.

Training of Lawyers on the European Data Protection Reform

#TRADATA

En el asunto Volker y Markus Schecke, el TJUE tuvo que juzgar la proporcionalidad de la publicación, requerida por la legislación de la UE, de los nombre de los beneficiarios de los subsidios agrícolas de la UE y de las cantidades que recibieron. El TJUE, estimando que el derecho a la protección de datos no es absoluto, argumentó que la publicación en una página web de los datos de los nombres de los beneficiarios de los dos fondos de ayuda agrícola de la UE, y de las cantidades exactas recibidas, constituye una intromisión en la vida privada de éstos, en general, y en la protección de sus datos personales, en particular.

El TJUE consideró que dicha injerencia en los artículos 7 y 8 de la Carta estaba establecida por ley y respondía a un objetivo de interés general reconocido por la Unión Europea, a saber, la mejora de la transparencia del uso de los fondos comunitarios. Sin embargo, el TJUE consideró que la publicación de los nombres de las personas físicas beneficiarias de las ayudas agrícolas de la UE, a partir de estos dos fondos, y las cantidades exactas recibidas, constituía una medida desproporcionada y no justificada en virtud del artículo 52.1 de la Carta. Así, el Tribunal declaró la nulidad parcial de la normativa de la UE sobre la publicación de la información relativa a los beneficiarios de los fondos agrícolas europeos.

Training of Lawyers on the European Data Protection Reform

#TRADATA

En cuanto al ámbito sustantivo, el derecho a la protección de datos cubre todo el tratamiento de la información personal relacionada con una persona identificada o identificable independientemente de que su tratamiento carezca de efecto alguno sobre su privacidad. El derecho a la protección de los datos personales puede ser visto como un derecho fundamental que protege todos los datos personales de los interesados (Lindqvist, incluso fuera del contexto de la "vida privada" - y tiene por objeto facilitar el tratamiento de los datos (siempre y cuando se observen las reglas establecidas en las disposiciones legales correspondientes), y no su prohibición.

En cuanto al ámbito de aplicación personal, las personas jurídicas son, en principio, excluidas del derecho a la protección de datos (véase, por ejemplo, VolkerundMarkusScheckeGbR y HartmutEifertc. LandHessen, § 53), mientras que, por su parte, el TEDH sí ha reconocido que las personas jurídicas disfrutan del derecho a la privacidad (véase, por ejemplo, la sentencia del TEDH BernhLarsen Holding As y otros c. Noruega).

Training of Lawyers on the European Data Protection Reform

#TRADATA

Como ya se ha mencionado anteriormente, la "vida privada" y el "derecho a la privacidad" son conceptos amplios (véanse los asuntos del TEDH Amann c. Suiza, §65 y Niemietz c. Alemania, § 29 y el asunto del TJUE VolkerundMarkusScheckeGbR y HartmutEifert c. LandHessen, § 52). Por otra parte, como ya se ha subrayado, estos conceptos siguen en constante evolución. El derecho a la privacidad, por lo tanto, es más amplio que el derecho a la protección de los datos personales ya que abarca muchas otras dimensiones, además de la protección de los datos personales.

El TEDH reconoce que la "vida privada" incluye la protección de los datos personales definidos como cualquier información relativa a una persona física identificada o identificable. Sin embargo, el TEDH no aplica el derecho de privacidad a todo tratamiento de los datos personales. A partir de un análisis más detallado de la jurisprudencia, parece que el TEDH exige un elemento adicional de privacidad a fin de que la información personal sea incluida en el ámbito de la vida privada. Bien porque el tratamiento realizado sea intrusivo en la vida privada de la persona (por ejemplo, cuando el tratamiento se refiera a los datos médicos o a los datos sobre el estado de salud de grupos vulnerables, como los niños) o bien porque el tratamiento sea permanente o de larga duración de manera que constituya una infracción del derecho a la privacidad.

El artículo 8.1 establece aquellos derechos que deben serle garantizados a un individuo por parte del Estado - el derecho al respeto de la vida privada y familiar, de domicilio y de correspondencia. El TEDH aún no ha establecido una definición clara y precisa de lo que se entiende por "vida privada". Según el TEDH, el concepto de vida privada es claramente más amplio que el derecho a la privacidad y se refiere a aquella esfera dentro de la cual todo el mundo puede lograr la realización y el libre desarrollo de su personalidad.

El ámbito de aplicación del artículo 8 sigue evolucionando en la jurisprudencia del TEDH de acuerdo con su propia naturaleza como instrumento vivo que requiere ser interpretado a la luz de las cambiantes condiciones sociales, legales o tecnológicas con el fin de ser práctico y efectivo (Tyrer c. Reino Unido). El TEDH ha aportado en su jurisprudencia una interpretación muy amplia del artículo 8.

Training of Lawyers on the European Data Protection Reform

#TRADATA

En M. M. vs Reino Unido, en relación con una amonestación emitida por la policía trece años antes de que fuera comunicada a un posible empleador en un proceso de selección de personal, el TEDH consideró que la información sobre una condena penal, o sobre la comisión de una infracción, se entiende dentro del ámbito de la vida privada de la persona, en cuanto el hecho se aleja en el pasado, entendiéndose incluida dentro del ámbito de aplicación del artículo 8 del Convenio.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Hasta ahora, el TEDH ha estimado que el artículo 8 cubre, por ejemplo: el mero almacenamiento de información sobre la vida privada de un individuo (Leander c. Suecia.), la vigilancia y la interceptación de comunicaciones telefónicas y de correo (Klass c. Alemania.), la vigilancia en el lugar de trabajo (Copland c. Reino Unido), el uso de circuito cerrado de televisión (CCTV) (Pack c. Reino Unido), la protección de la imagen personal (Von Hannover c. Alemania 2) y la reputación (Pfeifer c. Austria). Por otra parte, no sólo el artículo 8 abarca dicha esfera dentro de la cual cada individuo puede realizarse y desarrollar libremente su personalidad, sino que también se extiende a la posibilidad de desarrollar relaciones con los demás y con el mundo exterior (Niemietz c. Alemania).

En cuanto a si la limitación es necesaria en una sociedad democrática, el TEDH sostiene que cualquier limitación debe estar motivada en razones relevantes y suficientes y debe ser proporcional a los objetivos legítimos que se persiguen.

Training of Lawyers on the European Data Protection Reform

#TRADATA

En el asunto Leander c. Suecia, el TEDH dictaminó que el escrutinio secreto de las personas que solicitan empleo en puestos de importancia para la seguridad nacional no era, en sí mismo, contrario a la exigencia de ser necesaria dicha injerencia en una sociedad democrática. Las garantías especiales previstas por la legislación nacional para la protección de los intereses del titular de los datos - por ejemplo, los controles ejercidos por el Parlamento y por el Ministerio de Justicia - dieron lugar a que el TEDH estimara que el control de las autoridades suecas sobre su personal cumplía con los requisitos del artículo 8.2 del CEDH. Visto el amplio margen de apreciación de que dispone, el Estado demandado tenía derecho a considerar que en el caso del demandante los intereses de la seguridad nacional prevalecían sobre los individuales. El TEDH concluyó que no había habido violación alguna del artículo 8 del CEDH.

En el artículo 8.2, el CEDH establece una lista limitada de objetivos legítimos que pueden justificar la injerencia en la vida privada, es decir, los intereses de la seguridad nacional, la seguridad pública, el bienestar económico del país, la prevención de las infracciones penales, la protección de la salud o la moral y la protección de los derechos y libertades de los demás.

En Peck c. El Reino Unido, el demandante intentó suicidarse en la calle cortándose las muñecas, sin saber que una cámara de circuito cerrado de televisión (CCTV) le había estado grabando durante el intento. Después de que la policía, que estaba viendo las cámaras de circuito cerrado, lo rescatara, la autoridad policial correspondiente pasó la grabación a los medios de comunicación, que la publicaron sin cubrir la cara del demandante. El TEDH consideró que no había razones relevantes o suficientes para justificar la revelación directa de las imágenes por las autoridades al público sin haber obtenido el consentimiento del demandante o sin cubrir u ocultar su identidad. El TEDH concluyó que se había producido una violación del artículo 8 del CEDH.

Las limitaciones de los derechos deben estar previstas por ley. Un requisito fundamental para que concurra un fundamento jurídico suficiente es que la limitación sea comprensible por las personas afectadas y previsible en cuanto a sus efectos. Esto significa que tiene que estar formulada de una forma suficientemente precisa y debe permitir a cualquier persona poder adaptar su conducta (si es necesario con el asesoramiento apropiado). Las normas de carácter muy general no cumplen con este criterio (Amann c. Suiza).

En Rotaru c. Rumania, el TEDH estimó una violación del artículo 8 del CEDH, porque la ley rumana permitía la recogida, el registro y el archivo de información secreta que afectaba a la seguridad nacional, sin establecer límites en el ejercicio de estas actividades, manteniéndose a la discreción de las autoridades. Por ejemplo, la legislación nacional no definía el tipo de información que podía ser tratada, las categorías de personas contra las que se podrían tomar medidas de vigilancia, las circunstancias en las que podrían adoptarse tales medidas o el procedimiento a seguir. Debido a estas deficiencias, el TEDH concluyó que la legislación nacional no se ajustaba a la exigencia de previsibilidad en virtud del artículo 8 del Convenio Europeo y, en consecuencia, entendió que dicho artículo había sido vulnerado.

Training of Lawyers on the European Data Protection Reform

#TRADATA

OTROS PRONUNCIAMIENTOS

En K.U. c. Finlandia, el TEDH estimó que el Estado tiene la obligación, conforme el artículo 8, de disponer de un sistema destinado a proteger a los menores de ser víctimas potenciales de pedófilos a través de Internet. El Estado, además, tiene la obligación de (*OBLIGACIONES POSITIVAS*) establecer un marco legal que sirva para rastrear la identidad de este tipo de criminales en línea.

La ausencia de un marco de este tipo supuso que el Estado había fallado en su obligación de proteger la vida privada del demandante.

Training of Lawyers on the European Data Protection Reform

#TRADATA

En Gardel c. Francia, el TEDH estimó que el objetivo de prevención para la creación de una base de datos con información relativa a los delincuentes sexuales, en la que se introdujeron los datos del demandante después de haber cumplido una pena de 15 años de prisión por la violación de un menor de edad, podría representar una medida para que el Estado pudiera cumplir con su obligación de proteger a los grupos vulnerables de aquellas actividades criminales particularmente reprobables. El TEDH consideró que el Estado tenía discreción (*MARGEN DE APRECIACIÓN*) para aplicar este tipo de medidas y que el equilibrio en cuestión establecido entre los intereses privados y públicos era justo, estimando, por tanto, que no constituían, dichas medidas, una violación del artículo 8 del CEDH.

Training of Lawyers on the European Data Protection Reform

#TRADATA

En el asunto CemalettinCanli c. Turquía, el TEDH estimó una violación del artículo 8 del CEDH por la elaboración de informes policiales incorrectos en los procesos penales. El demandante había estado implicado en dos ocasiones en dos procesos penales debido a su pertenencia a organizaciones ilegales, pero nunca fue condenado. Cuando el demandante fue nuevamente arrestado y acusado de otro delito, la policía presentó ante el juzgado de lo penal un informe titulado "Informe sobre delitos adicionales", en el que se presentó al demandante como miembro de dos organizaciones ilegales. La petición del demandante para la modificación de los registros del informe policial no tuvo éxito. El TEDH estimó que la información contenida en el informe de la policía estaba dentro del alcance del artículo 8 del CEDH, la información pública podría también ser objeto del alcance de la "vida privada" cuando se recoge y se almacena en ficheros de las autoridades de manera sistemática. Por otra parte, el informe de la policía era incorrecto y su elaboración y presentación al juzgado de lo penal era contrario a Derecho. El TEDH concluyó que se había vulnerado el artículo 8.

En Ciubotaru c. Moldavia, el demandante no pudo cambiar el registro de su origen étnico en los ficheros oficiales del de moldavo al de rumano, supuestamente debido a la falta de justificación sustantiva de dicha solicitud. El TEDH consideró admisible que los Estados requieran pruebas objetivas para el registro de la identidad étnica de un individuo. Cuando tal afirmación se basa en razones puramente subjetivas y sin fundamento, las autoridades podrían denegar la solicitud. Sin embargo, la pretensión del demandante se había basado en algo más que en la mera percepción subjetiva de su propia etnia; habiendo proporcionado vínculos objetivamente verificables con la etnia rumana como el idioma, el nombre, el arraigo y otros. Sin embargo, en virtud de la legislación nacional, era necesario que el solicitante justificase la pertenencia de sus padres a la etnia rumana. Teniendo en cuenta la realidad histórica de Moldavia, este requisito había creado una barrera infranqueable en el registro de una identidad étnica distinta de la registrada por sus padres ante las autoridades soviéticas. Al no permitir que se examinaran de forma objetiva las pruebas aportadas por el demandante respecto a su pretensión, el Estado había incumplido con su obligación positiva de asegurar el respeto efectivo a la vida privada del demandante. El TEDH estimó que se había producido una violación del artículo 8 del CEDH.

Training of Lawyers on the European Data Protection Reform

#TRADATA

El TJUE ha estimado que las imágenes de los circuitos cerrados de televisión (CCTV) pueden vulnerar la normativa de protección de datos.

El Sr. Rynes instaló un sistema de vídeovigilancia en su casa después de que su familia fuese objeto de varios ataques en los últimos años, causando daños en su propiedad, sin ser capaz de identificar al autor de tales delitos. Gracias al sistema de videovigilancia los presuntos atacantes fueron identificados y, posteriormente, enjuiciados. Uno de los sospechosos denunció la ilegalidad del propio sistema de videovigilancia, dado que fue grabada parte de la acera pública. La Agencia de Protección de Datos competente falló a favor del sospechoso y multó al Sr. Rynes. Éste último argumentó que la Directiva de Protección de Datos no era aplicable en virtud de la exención de las actividades domésticas del artículo 3.2. El TJUE sostuvo que Rynes no podía ser responsable de una multa por haber actuado con el objeto de ayudar a enjuiciar a un criminal. Sin embargo, la sentencia estimó que, de no ser el caso de una comisión previa de un delito, el demandante sí habría vulnerado la normativa de protección de datos. La Directiva dispone como excepción de su aplicación el tratamiento de datos efectuado "por una persona física en el ejercicio de actividades exclusivamente personales o domésticas", pero el Tribunal consideró que la excepción no siempre debe aplicarse cuando una cámara está grabando imágenes del espacio público como una acera. Los jueces sostuvieron que: "la instalación de un sistema de cámaras, que tiene como resultado la grabación en vídeo de las personas, almacenada en un dispositivo de grabación continua, como una unidad de disco duro, instalada por una persona en su domicilio familiar para los fines de proteger la propiedad, la salud y la vida de los propietarios de las viviendas, pero que también controla un espacio público, no equivale al tratamiento de los datos en el curso de las actividades exclusivamente personales o domésticas, a los efectos de esta disposición".

Al concepto del **"contexto de las actividades"** se le da una interpretación amplia:
Asunto C-131/12 Google España SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014]

Hechos:
Con anterioridad: el Sr. Costeja González había planteado con éxito un caso ante la Agencia Española de Protección de Datos en contra de Google España y Google Inc. Estas últimas interpusieron las correspondientes demandas contra la decisión de la Audiencia Nacional española, que remitió una cuestión prejudicial al TJUE.
Las conclusiones del TJUE:
Google España constituye una filial de Google Inc. en el territorio español y es un "establecimiento" en el sentido del artículo 4.1 (a) de la DPD.
El TJUE consideró que Google Inc. trata los datos personales conforme al artículo 2 (b) de la DPD y constituye un responsable de conformidad con lo dispuesto en el artículo 2 (d) de la DPD. Google Inc. trata exclusivamente aquellos datos personales tratados mediante el procedimiento principal y opera exclusivamente con el buscador de Google. La actividad de Google España se limita a proporcionar apoyo a la actividad publicitaria del grupo Google que está separado de su servicio de buscador.
Fallo: "El tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento del responsable del tratamiento en el territorio de un Estado miembro, en el sentido de dicha disposición, cuando el operador de un motor de búsqueda se configura en un Estado miembro, a través de una sucursal o filial, que tiene por objeto promocionar y vender espacios publicitarios ofrecidos por dicho motor de búsqueda y que orienta su actividad hacia los residentes de dicho Estado miembro ".

Training of Lawyers on the European Data Protection Reform

#TRADATA

Tratamiento de Datos Personales: Datos GPS
Uzun v. Alemania
2 septiembre 2010

El solicitante, sospechoso de haber participado en atentados con bombas de un movimiento extremista, plantea que su vigilancia vía GPS y la utilización de los datos obtenidos de tal modo en el proceso penal contra él habían violado su derecho al respeto de vida privada.

La Sala sostuvo que no había habido violación del artículo 8 de la Convención. Es cierto que la vigilancia del GPS y el tratamiento y la utilización de los datos obtenidos de tal modo habían interferido con el derecho del solicitante al respeto de su vida privada. Sin embargo, la Corte observó que había perseguido los objetivos legítimos de proteger la seguridad nacional, la seguridad pública y los derechos de las víctimas y de prevenir la delincuencia. También había sido proporcionada: la vigilancia por GPS se había ordenado sólo después de que los métodos de investigación menos intrusivos habían demostrado ser insuficientes, se habían llevado a cabo durante un período relativamente corto (unos tres meses), y habían afectado al solicitante sólo cuando estaba viajando en el coche de su cómplice. Por lo tanto, no se puede decir que el solicitante ha sido objeto de una vigilancia total y exhaustiva. Dado que la investigación se refería a delitos muy graves, la vigilancia del solicitante por el GPS había sido así necesaria en una sociedad democrática.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Tratamiento de Datos Personales: Datos de Salud
Izquierdo v. Letonia (núm. 52019/07)
29 abril 2014

El solicitante alegó, en particular, que la recopilación de sus datos médicos personales por una agencia estatal – en este caso, la inspección de control de calidad para la atención médica y la aptitud para el trabajo ("MADEKKI") – sin su consentimiento había violado su derecho al respeto por su vida privada.
En esta sentencia, el Tribunal recordó la importancia de la protección de los datos médicos para el disfrute del derecho al respeto de la vida privada. Sostuvo que había habido una violación del artículo 8 de la Convención en el caso del solicitante, al constatar que la ley aplicable no había indicado con suficiente claridad el alcance de la discreción conferido a las autoridades competentes y la forma de su ejercicio. El Tribunal observó, en particular, que la legislación letona no limitaba en modo alguno el alcance de los datos privados que podrían recabar los MADEKKI, lo que dio lugar a la recopilación de datos médicos sobre el solicitante en relación con un período de siete años de forma indiscriminada y sin previa evaluación de si tales datos podrían ser potencialmente decisivos, pertinentes o de importancia para lograr cualquier objetivo que pudiera haber sido perseguido por la investigación en cuestión.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Interceptación de comunicaciones, escucha telefónica y vigilancia secreta
Wisse v. France
22 de diciembre de 2005

Los dos demandantes fueron arrestados bajo sospecha de haber cometido robos a mano armada y puestos en detención preventiva. Bajo una orden emitida por el juez de instrucción, se registraron las conversaciones telefónicas entre ellos y sus familiares en las salas de visita de la prisión. Los solicitantes hicieron una solicitud sin éxito para declarar inválidos los pasos en los procedimientos relacionados con la grabación de sus conversaciones. Argumentaron que la grabación de sus conversaciones en las salas de visita de la prisión había constituido una interferencia con su derecho al respeto por su vida privada y familiar.

El Tribunal sostuvo que se había violado el artículo 8 de la Convención y consideró que la legislación francesa no indicaba con suficiente claridad cómo y en qué medida las autoridades podían interferir con la vida privada de los detenidos, o el alcance y la forma de ejercicio de sus poderes de discreción en esa esfera. En consecuencia, los solicitantes no habían disfrutado del grado mínimo de protección requerido por el estado de derecho en una sociedad democrática. El Tribunal observó en particular que la grabación sistemática de conversaciones en una sala de visitas para fines distintos de la seguridad privaba a las salas de visita de su única razón de ser, a saber, permitir que los detenidos mantuvieran cierto grado de vida privada, incluida la privacidad de las conversaciones con sus familias

Training of Lawyers on the European Data Protection Reform

#TRADATA

Monitorización de los empleados
Bărbulescu v. Rumania
5 de septiembre de 2017 (gran sala)

Este caso se refería a la decisión de una empresa privada de despedir a un empleado – el solicitante – después de supervisar sus comunicaciones electrónicas y acceder a sus contenidos. El solicitante se quejó de que la decisión de su empleador se basaba en una violación de su privacidad y que los tribunales nacionales no habían protegido su derecho al respeto de su vida privada y su correspondencia.

La gran sala decidió, por once votos a seis, que había habido una violación del artículo 8 de la Convención, al constatar que las autoridades rumanas no habían protegido adecuadamente el derecho del solicitante a respetar su vida privada y su correspondencia. En consecuencia, no lograron un equilibrio justo entre los intereses en juego. En particular, los tribunales nacionales no habían podido determinar si el solicitante había recibido notificación previa de su empleador de la posibilidad de que sus comunicaciones pudieran ser
ser monitorizados; tampoco habían tenido en cuenta el hecho de que no había sido informado de la naturaleza o la amplitud de la vigilancia, o el grado de intrusión en su vida privada y correspondencia. Además, los tribunales nacionales no han podido determinar, en primer lugar, las razones concretas que justifican la introducción de las medidas de vigilancia; en segundo lugar, si el empleador podría haber utilizado medidas que entrañaran menos intrusión en la vida privada y la correspondencia del solicitante; y en tercer lugar, si las comunicaciones podrían haber sido accedidas sin su conocimiento.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Monitorización de los empleados
Libert v. Francia
22 febrero 2018

Este caso se refirió al despido de un empleado de SNCF (compañía ferroviaria nacional francesa) después de que la intervención del ordenador propio de su puesto de trabajo hubiera revelado el almacenaje de expedientes pornográficos y de certificados falsificados elaborados para terceras personas. El solicitante se quejó en particular de que su empleador había abierto, en su ausencia, archivos personales almacenados en el disco duro de su ordenador de trabajo.

La Corte sostuvo que no había habido violación del artículo 8 de la Convención, y que en el presente caso las autoridades francesas no habían sobrepasado el margen de apreciación disponible para ellos. El Tribunal observó, en particular, que la consulta de los expedientes por el empleador había ido encaminado a un objetivo legítimo de proteger sus derechos, que podrían legítimamente desear garantizar que sus empleados utilizaran las instalaciones informáticas que habían puesto a su disposición en consonancia con sus obligaciones contractuales y las reglamentaciones aplicables. El Tribunal observó también que la legislación francesa incluía un mecanismo de protección de la privacidad que permitía a los empleadores abrir archivos profesionales, aunque no podían abrir de forma encubierta archivos identificados como personales. Sólo podían abrir este último tipo de archivos en presencia del empleado. Los tribunales nacionales habían dictaminado que los expedientes en cuestión no habían sido debidamente identificados como privados. Por último, el Tribunal consideró que los tribunales nacionales habían evaluado debidamente la alegación del demandante de una violación de su derecho al respeto de su vida privada, y que las decisiones de esos tribunales se habían basado en motivos pertinentes y suficientes.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Videovigilancia
Antović y Mirković v. Montenegro
28 noviembre 2017

Este caso se refirió a una reclamación de dos profesores en la facultad de Matemáticas de la Universidad de Montenegro tras la instalación de cámaras de videovigilancia en las aulas. Afirmaron que no habían tenido control efectivo sobre la información recabada y que la vigilancia había sido ilícita. Sin embargo, los tribunales nacionales rechazaron una reclamación de indemnización, al constatar que la referencia a la vida privada no puede predicarse de entornos como las aulas de una Universidad.

La Corte sostuvo que había habido una violación del artículo 8 de la Convención, al constatar que la vigilancia del aula no había sido conforme a la ley. En primer lugar, rechazó el argumento del gobierno de que el caso era inadmisible porque no había ninguna cuestión de privacidad en juego, ya que el área bajo vigilancia había sido una zona de trabajo pública. En este sentido, la Corte indicó que ya con anterioridad se había pronunciado en el sentido de que la vida privada podría incluir actividades profesionales y consideraba que también era el caso de los demandantes. Por consiguiente, el artículo 8 es aplicable. En cuanto al fondo del caso, el Tribunal determinó que la vigilancia del aula había sido una injerencia en el derecho a la intimidad de los demandantes y que la prueba practicada mostraba que esa vigilancia había violado las disposiciones del derecho interno. De hecho, los tribunales nacionales ni siquiera habían valorado si existía alguna justificación legal para la vigilancia porque habían decidido desde el principio que no había habido invasión de la intimidad.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Videovigilancia
López Ribalda y otros v. España
9 enero 2018

Este caso se refería a la videovigilancia encubierta de los empleados de una cadena de supermercados españolas después de haber surgido sospechas de robo. Los solicitantes fueron despedidos principalmente sobre la base del material de vídeo, que alegaban que habían sido obtenidos violando su derecho a la intimidad. Los tribunales españoles aceptaron las grabaciones como prueba y confirmaron la procedencia del despido.
El tribunal sostuvo que había habido una violación del artículo 8 de la Convención, al constatar que los tribunales españoles no habían logrado un equilibrio justo entre los derechos involucrados, el derecho a la intimidad de los solicitantes y los derechos de propiedad del empleador. Observó, en particular, que, en virtud de la legislación española sobre protección de datos, se debería haber informado a los solicitantes de que estaban bajo vigilancia, pero no lo habían hecho. Los derechos de la empresa podrían haber sido salvaguardados por otros medios y podría haber proporcionado a los demandantes, al menos, información general sobre la vigilancia. Sin embargo, el tribunal sostuvo que no había habido violación del artículo 6.1 (derecho a un juicio imparcial) de la Convención. Constató que el procedimiento en su conjunto había sido justo y el despido procedente porque el material de vídeo no era la única prueba que los tribunales nacionales habían invocado al declarar la procedencia de las decisiones de despido y los demandantes habían podido impugnar las grabaciones en el Tribunal.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Revelación de Datos Personales
Satakunnan Markkinapörssi Oy y Satamedia Oy v. Finlandia
27 de junio de 2017 (gran sala)

Después de que dos compañías publicaran información relativa al IRPF de 1,2 millones personas, las autoridades nacionales dictaminaron que dicha publicación al por mayor de datos personales había sido ilícita bajo las leyes de protección de datos, y prohibió esas publicaciones masivas en el futuro. Las empresas argumentaron que la prohibición había violado su derecho a la libertad de expresión.

La gran sala decidió, por quince votos a dos, que no había habido violación del artículo 10 (libertad de expresión) de la Convención. Observó, en particular, que la prohibición había interferido con la libertad de expresión de las empresas. Sin embargo, no había violado el Artículo 10 debido a que se había procedido conforme a ley, ha perseguido el objetivo legítimo de proteger la intimidad de las personas, y ha alcanzado un justo equilibrio entre el derecho a la intimidad y el derecho a la libertad de expresión. En este caso, la gran sala estuvo de acuerdo con la conclusión de los tribunales nacionales, que la recolección masiva y la difusión al por mayor de los datos tributarios no habían contribuido a un debate de interés público y no habían obedecido a un propósito periodístico.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Muchas Gracias