ISSN 2704-8012

European Journal of Privacy Law & Technologies

2020/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2020/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in June 2020
www.ejplt.tatodpr.eu

European Journal of Privacy Law and Technologies

Summary

pag.

Section I: Articles

Section II: Comments on decisions

Section III: Use Cases

CYBERSECURITY, CONCORRENZA, CONTRATTI E CYBER-RISK

CYBERSECURITY, COMPETITION, CONTRACTS AND CYBER-RISK

Domenico Fauceglia

Avv. Ph.D. at Università di Roma Tor Vergata

Abstract:

Insieme con il cambiamento climatico, la sicurezza delle reti e dei sistemi informativi costituisce un'emergenza mondiale. Dxiverse sono le sfide che, nei prossimi anni, l'Italia dovrà affrontare al fine di promuovere la cultura sulla sicurezza cibernetica. In questo delicato contesto, l'articolo contribuisce a descrivere la disciplina europea e interna in tema di cybersecurity, nonché le problematiche relative all'attività di impresa e alla gestione dei rischi presenti nel cyberspace.

Together with climate change, the security of networks and information systems constitutes a global emergency. There are several challenges that Italy will have to face in the coming years in order to promote the culture of cybersecurity. In this delicate context, the article helps to describe the European and national discipline on the topic of cybersecurity, as well as the issues relating to business activities and the management of risks present in cyberspace.

Parole chiave: sicurezza informativa; concorrenza; Direttiva NIS.

Key-words: *cybersecurity; competition; NIS Directive.*

1. La *Cybersecurity,* Industria 4.0 e *Smart city*

Il fenomeno della *cybersecurity* ha fatto ingresso nel nostro ordinamento con la Direttiva europea NIS 2016/1148/UE (*Network and Information Security*) volta a stabilire le misure per la realizzazione in Europa di un ambiente digitale sicuro e affidabile [1].

Per evidenziare l'importanza della disciplina della cybersecurity, occorre osservare il continuo procedimento di trasformazione digitale dei più importanti settori della nostra economia. L' evoluzione digitale sta conducendo ad una duplice realtà: reale e virtuale. Diverse imprese, negli ultimi anni, hanno preferito investire sul digitale e sulle nuove tecnologie che permettono un maggiore incremento di efficienza, affidabilità e sicurezza nella produzione di beni, erogazione dei servizi e nella gestione dell'attività d'impresa.

A ciò si aggiunge che l'internet delle cose (Iot) permette una migliore connessione di oggetti del mondo fisico nonché un miglior collegamento e migliore comunicazione (intesa come scambio di dati) tra il mondo virtuale e il mondo reale.

In questo contesto, rilevano le nuove Industrie 4.0 e le *Smart cities c*he operano su due livelli: il livello fisico (la fabbrica o la città) con le sue diverse infrastrutture (i macchinari nel caso della fabbrica, le strade, le reti, i mezzi di trasporto, ecc., nel caso della città) e il livello *cyber c*he, contenendo una rappresentazione "virtuale" delle cose materiali, ne permette il controllo e la gestione attraverso le nuove tecnologie.

Obiettivo del livello cyber è quello di monitorare, in modo continuo, lo stato delle infrastrutture fisiche, adattandole alle esigenze della produzione o dei cittadini al fine di coniugare efficienza e qualità dei prodotti e dei servizi.

In questi termini, si percepisce maggiormente il pericolo o il danno che potrebbe derivare da un possibile attacco *cyber.*

2. La Direttiva NIS e cyber – sicurezza nell'attività di impresa

La Direttiva europea NIS – recepita in Italia con il Decreto Legislativo 18 maggio 2018, n. 65 – affronta, per la prima volta a livello europeo, il tema della *cyber security* e definisce le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei

[1] Cfr. A. CONTALDO, F. PELUSO, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa 2018; A. CONTALDO, D. MULA, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche,* Pisa 2020; B. PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Milano 2020.

sistemi informativi; tra l'altro, la notifica degli incidenti di sicurezza informatica subiti [2]. L'incremento della digitalizzazione e della connettività – anche grazie all'avvento dell'Internet degli oggetti ("*Internet of things*" o *IoT*) – espone le reti e i sistemi informativi a maggiori rischi connessi alla *cyber*-sicurezza, ne deriva che la società è sempre più vulnerabile alle minacce informatiche. Considerati i maggiori pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori, si è rilevata necessaria l'emanazione del Regolamento 2019/881/UE, conosciuto come *Cybersecurity act* [3].

Prima di procedere all'analisi della disciplina relativa alla cybersecurity, si rende doverosa una precisazione sul concetto di cybersicurezza, oggi intesa come «*insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*» (art. 2, Reg. 2019/881/UE).

Anche se la disciplina della *cybersecurity* sia attuale, il termine *Cyber Security* non è nuovo. Esso era già diffuso negli anni Novanta del secolo scorso, ma solo negli ultimi anni sta assumendo contorni maggiormente precisi.

Una delle prime definizioni di *cybersecurity* è riportata all'interno della norma ISO/IEC 27000:2014 che la descrive come: «*quella pratica che consente ad un'entità (un'organizzazione, un cittadino, una nazione, ecc.) di proteggere i propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni, dalle minacce che arrivano dal cyberspace*» (ISO/IEC, 2014).

In quest'ottica, le finalità della Direttiva NIS e del più recente *Cybersecurity act* sono dirette a garantire un livello minimo di "igiene informatica" e a ridurre al minimo possibile l'esposizione delle reti, dei servizi e dei sistemi di comunicazione elettronica, a rischi derivanti da minacce informatiche.

Invero, la direttiva NIS del 6 luglio 2016, al fine di prevenire rischi e incidenti informatici, offre una disciplina diretta a regolare il controllo e le condotte nei casi di incidente (cioè ogni evento pregiudizievole per la sicurezza, art. 4 n.

---

[2] Con il Decreto Legislativo 18 maggio 2018, n.65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cd. Direttiva NIS, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Come si avrà modo di notare nel prosieguo, il decreto si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

[3] L'opportunità di regolare la disciplina con regolamento era già stata manifestata da G. BRUNO (*La* cybersecurity *nel sistema del diritto europeo*, in *Diritto delle Comunicazioni*, a cura di G. Bruno, Torino 2019, p. 470), il quale si era già posto in senso critico alla scelta del legislatore euro-unionale di adottare una direttiva, in particolare l'A. ritiene che «proprio per l'importanza della materia ed in considerazione del carattere sovranazionale di fenomeni che si svolgono su contesti di carattere globale, sarebbe stato opportuno per il legislatore comunitario operare con lo strumento tecnico del Regolamento anziché con quello della Direttiva al fine di evitare spazi di discrezionalità applicativa in grado di alterare nell'effetto pratico le normali dinamiche di un mercato fondato sulla concorrenza».

7 Dir. NIS) e di rischio (cioè ogni evento potenzialmente pregiudizievole, art. 4 n. 9 Dir. NIS) delle reti e dei sistemi informativi.

Per rete e sistema informativo si intende, ai sensi dell'art. 4 n. 1, una rete di comunicazione elettronica e, dunque, i sistemi di trasmissione e le apparecchiature che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse [4].

Ancora, per rete e sistema informativo, si intendono anche qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico dei dati digitali; nonché i dati digitali, trattati estratti o trasmessi per mezzo di reti o dispositivi.

In particolare, la cybersecurity è «*l'insieme delle misure che riducono il rischio che la confidenzialità, l'integrità e la disponibilità dei dati, siano essi in transito o statici, vengano impattate negativamente dalle minacce provenienti dal cybercrime che incombono su di essi e che sono amplificate dalla pervasività e complessità delle interconnessioni di rete attuali e future*» [5].

L'esigenza di rendere maggiormente sicure le reti e i servizi informativi, nonché l'esigenza di una disciplina in caso di rischi e incidenti informatici, sono volte anche ad assicurare il normale esercizio delle attività economiche.

Diversamente le imprese, esponendosi eccessivamente a rischi e danni, inevitabilmente verrebbero colpite da gravi perdite finanziarie conseguenti ad una impossibilità di gestione aziendale nonché ad una diffusa sfiducia dei consumatori e degli utenti. Tali pericoli, insomma, creerebbero particolari danni all'economia europea.

Non solo, la sicurezza delle reti e dei sistemi informativi – svolgendo un ruolo di primaria importanza nell'agevolare i movimenti transfrontalieri di beni, servizi e persone – si rileva essenziale per l'armonioso funzionamento del mercato interno.

Come si è anticipato, la disciplina è diretta a tutelare le reti e i sistemi informativi – ossia le reti di comunicazione elettronica, qualsiasi dispositivo o insieme di dispositivi interconnessi, nonché i dati digitali ivi trattati (cfr. art. 4, n. 1) Direttiva 2016/1148/UE) – è sostanzialmente diretta a tutelare i dati, anche personali, ivi contenuti.

Per tali ragioni, le tre caratteristiche del dato che devono esser salvaguardate sono rappresentate dalla c.d. "***CIA Triad***" (da *Confidentiality, Integrity, Availability*), in particolare:

---

[4] Sul punto si rimanda a D. FAUCEGLIA, *Il contratto di utenza telefonica*, Milano 2020, p. 13 ss.

[5] Y. I. AGOSTINI, *Le basi di Cybersecurity per il giurista*, in Ziccardi, *Tecnologia e diritto*, vol. I, Milano 2019, p. 158

a) la **disponibilità** (*Availability*) che misura l'attitudine di un'entità o sistema ad essere in grado di svolgere una funzione richiesta in determinate condizioni ad un dato istante;

b) la **confidenzialità** (*Confidentiality*), ossia la protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti;

c) l'**integrità** (*Integrity*), ossia la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali (involontarie) oppure effettuate volontariamente da una terza parte, essendo compreso nell'alterazione anche il caso limite della generazione *ex novo* di dati ed informazioni.

In questi termini, dal momento che l'informazione costituisce una utilità (dunque un bene in senso giuridico *ex* art. 810 cod. civ.) e dal momento che, oggigiorno, la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati.

Invero, occorrerebbe chiarire la natura di dato digitale. In questo contesto, l'art. 810 cod. civ. non fornisce una definizione universale di bene giuridico, limitandosi a descrivere il procedimento di oggettivazione attraverso cui una certa entità acquista rilievo per l'ordinamento giuridico come bene giuridico [6].

Una determinata entità (come i dati digitali conservati, estratti e trattati per mezzo di reti e dispositivi *ex* art. 4 lett. 1 Direttiva NIS) suscita determinati interessi (anche non tipizzati) che possono essere soddisfatti solo con l'attribuzione di un certo diritto soggettivo e delle relative tutele [7].

In quest'ottica, si potrà sempre fare ricorso all'analogia ed estendere il procedimento appropriativo della proprietà, come era già stato fatto tempo fa per il *software* ed il *know-how* ed ora anche per le criptovalute e il *cloud computing.*

In ragione degli interessi tutelati, si giustificano precisi obblighi a carico delle imprese in materia di sicurezza delle reti e sistemi informativi.

Si badi, però, non bisogna confondere la disciplina della tutela dei dati personali con la disciplina della sicurezza delle informazioni *tout court* le quali, seppure siano riservate e confidenziali, nulla hanno che vedere con dati personali [8]. Ebbene,

---

[6] Sul punto O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, Milano 1982, p. 39 e ss.; D. MESSINETTI, *Oggettività giuridica delle cose incorporali*, Milano 1970, p. 105, secondo cui «quella dei beni è una vera e propria qualificazione e non una semplice classificazione secondo un ordine determinato e caratteri comuni».

[7] R. NICOLÒ, *Istituzioni di diritto privato*, Milano 1962, p. 3 s.

[8] Per tali ragioni, esiste a livello internazionale la norma ISO 27001 finalizzata alla standardizzazione delle modalità adatte a proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. Lo standard indica i requisiti di un adeguato sistema di gestione della sicurezza delle informazioni (SGSI; in inglese: *Information*

il trattamento dei dati personali, pur essendo richiamato tra i primi articoli della Direttiva NIS (in particolare art. 2), riguarda solo ed esclusivamente la disciplina dei dati personali. Infatti, l'art. 2 della Direttiva Nis, nel distinguere i due *corpora* normativi, precisa che «il trattamento di dati personali ai sensi della presente direttiva è effettuato ai sensi della direttiva 95/46/CE». D'altro canto, la legge sulla privacy infatti non impone alcuna protezione per informazioni prive di dati personali.

La *cybersecurity* si occupa esclusivamente della protezione delle reti e i dei sistemi informativi al fine di tutelare la *CIA triad* dei dati ivi trattati.

In relazione alla protezione degli *asset* informatici, quest'ultima è costituita da un complesso di misure di prevenzione e di protezione, tese ad assicurare: *a*) l'accesso protetto e controllato ai dati, a garanzia della confidenzialità delle informazioni trattate (proprietà di *riservatezza*); *b*) la consistenza dei dati, intesa come completezza e correttezza degli stessi (proprietà di *integrità*); *c*) l'accesso ai dati nei tempi e nei luoghi previsti (proprietà di *disponibilità*).

Le proprietà di riservatezza, integrità e disponibilità dei dati costituiscono l'assunto base sul quale vengono svolte tutte le successive valutazioni di sicurezza. Tali proprietà sono in genere affiancate anche dalla proprietà di *non ripudio*, ovvero dalla possibilità di attribuire un dato a un mittente o proprietario ben identificato.

Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, quali: robustezza del *software* di base e applicativo, affidabilità delle apparecchiature e degli ambienti in cui essi sono collocati.

Con la sicurezza informatica, si enfatizzano qualità di *resilienza (*resistenza a un attacco informatico)*, robustezza* e *reattività* che una tecnologia deve possedere per fronteggiare attacchi mirati a comprometterne il suo corretto funzionamento e le sue performance (attacchi *cyber*).

Al fine di valutare la sicurezza informatica (quindi, il pericolo di attacchi interni o esterni dannosi per gli *asset* informatici) è necessario individuare le eventuali:

---

security management system o ISMS) finalizzato a una corretta gestione dei dati dell'azienda. Una fase indispensabile di ogni pianificazione della sicurezza è la valutazione del rischio e la gestione del rischio. Le organizzazioni possono far certificare ISO 27001 il proprio SGSI. In particolare, lo standard ISO/IEC 27001 (Tecnologia delle informazioni – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti) è una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa. La versione più recente della norma è la ISO/IEC 27001:2017 (pubblicata il 30 marzo 2017), che non è altro che la versione 2013 con due modifiche (emesse dall'ISO nel 2014 e 2015): 1) requisito A.8.1.1: l'inventario, la classificazione e trattamento degli "asset" riguarda ora anche le "informazioni" cui gli asset sono associati; 2) requisito 6.1.3: la Dichiarazione di Applicabilità deve specificare se sono implementati o meno i "controlli necessari", e non solo i controlli riferiti all'Annex A.

a) minacce;

b) vulnerabilità, ossia i punti deboli del sistema riguardo ai quali le misure di sicurezza sono ridotte o, addirittura, assenti;

c) e rischi, ossia la probabilità che un'azione (o una inerzia) possa comportare la perdita di fatti o, comunque, un evento indesiderabile.

In termini pratici, le misure di *cybersecurity* si focalizzano su come comportarsi per prevenire un incidente di sicurezza (ai fini della prevenzione risulta essenziale una dettagliata analisi del rischio [9]) e come comportarsi nel caso un tale incidente si verifichi.

Il procedimento di analisi del rischio inizia con la preventiva identificazione dei beni da proteggere per poi valutare le possibili minacce in termini di potenziali danni e perdite (gravità). Una volta stimato il rischio delle reti e dei servizi informativi, si decidono quali misure di sicurezza adottare (c.d. piano di rischio). L'analisi del rischio tipicamente precede la fase di messa in esercizio del sistema informatico.

Giova ripetere che spesso l'obiettivo dell'attaccante non è rappresentato dai sistemi informatici in sé, ma piuttosto dai dati in essi contenuti: la sicurezza informatica deve quindi preoccuparsi di impedire l'accesso non solo agli utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a specifiche operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati.

Le violazioni possono essere molteplici, vi possono essere: a) tentativi non autorizzati di accesso a zone riservate; b) furto di identità digitale o di file riservati; c) utilizzo di risorse che l'utente non dovrebbe potere utilizzare.

La protezione dagli attacchi informatici viene ottenuta agendo a due livelli principali:

1) ***sicurezza fisica***. Per *sicurezza passiva* (fisica) normalmente si intendono le tecniche e gli strumenti di tipo difensivo, ossia il complesso di misure volte ad impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, dispositivi, apparati, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso fisico a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

2) ***sicurezza logica***. Per *sicurezza attiva* (logica) si intendono le tecniche e

[9] Ciò è anche confermato nelle linee guida (cybersecurity framework) emanate dal National Institute of Standards and Technology (NIST, agenzia del Governo degli Stati Uniti d'America) che prevedono i seguenti macro-processi: identifica (*identify*); proteggi (*protect*); rileva (*detect*); rispondi (*respond*); ripristina (*recover*).

gli strumenti mediante i quali le informazioni e i dati (nonché le applicazioni) di natura riservata sono resi sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autenticato o non autorizzato possa modificarli (integrità) [10].

Le misure di sicurezza passiva e attiva sono tra loro complementari. Entrambe sono indispensabili per raggiungere un livello di sicurezza adeguato degli asset informatici (in termini di prevenzione e di protezione) e sono tese ad assicurare la "*CIA Triad"* dei dati ivi contenuti.

3. La disciplina giuridica della cybersecurity

Come si è anticipato, il D. Lgs. 18 maggio 2018 n. 65 – attuativa della direttiva NIS 2016/1148/UE che lascia spazi di libertà agli «Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi», art. 2, lett. *a*) – individua, invece, i soggetti competenti a dare una prima attuazione alla *cyber* difesa europea.

Al fine di conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, l'art. 2, co. II, D.Lgs. 2018 n. 65, prevede:

a) l'inclusione nella strategia nazionale di sicurezza cibernetica di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del presente decreto;

b) la designazione delle autorità nazionali competenti e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale per lo svolgimento dei compiti di monitoraggio e intervento in caso di incidenti, emissione di preallarmi e analisi dinamica dei rischi;

---

[10] Per intendere cosa sia un sistema di sicurezza logico, occorre fare riferimento all'esperienza media di qualsiasi utente. È noto che gli sviluppatori di *software*, sin dalla progettazione dei programmi, devono attuare misure in grado di assicurare l'efficienza d'uso del programma e le sue capacità di "sopravvivenza" in caso di attacchi esterni e di errori più o meno critici. La sicurezza dei programmi è da due caratteristiche fondamentali: a) *Safety* (sicurezza): una serie di accorgimenti atti ad eliminare la produzione di danni irreparabili all'interno del sistema; b) *Reliability* (affidabilità): prevenzione da eventi che possono produrre danni di qualsiasi gravità al sistema. In quest'ottica, un software (o programma) è tanto più sicuro quanto minori sono le probabilità che si verifichi un malfunzionamento dello stesso. Gli errori di programma non nocivi, come ad esempio gli *spyware* e il *buffer overflow*, hanno la caratteristica di non modificare i file di sistema e non recare danno alle caratteristiche del sistema stesso. Quelli nocivi – come i virus informatici, i Trojan o il Cracking – possono essere contrastati solo con determinate misure di sicurezza logica: 1) *Update* e *Upgrade* di sistemi operativi con *patch* di sicurezza; 2) *Antivirus* che consente di proteggere il proprio *personal computer* da *software* dannosi conosciuti come *virus*. Ma, un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale.

c) il rispetto di obblighi da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante;

d) la partecipazione nazionale al gruppo di cooperazione europeo, nell'ottica della collaborazione e dello scambio di informazioni tra Stati membri dell'Unione europea, nonché dell'incremento della fiducia tra di essi;

e) la partecipazione nazionale alla rete CSIRT nell'ottica di assicurare una cooperazione tecnico-operativa rapida ed efficace.

Ebbene, come rileva dall'art. 2, la normativa si applica anzitutto agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

Gli OSE sono organizzazioni pubbliche o private che forniscono servizi essenziali per la società e l'economia nei settori dell'energia, dei trasporti, bancario, infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile, delle infrastrutture digitali e del campo sanitario [11].

Ai sensi dell'art. 4 co. 2 D.Lgs. 18 maggio 2018, n. 65, i criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti: a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Affinché un incidente possa considerarsi produttivo di effetti negativi rilevanti sulla fornitura del servizio, le autorità competenti NIS (ossia i Ministeri a capo di ogni settore [12]) considerano i seguenti fattori intersettoriali:

---

[11] Ciò in conformità con la direttiva (UE) 2016/1148 ha stabilito obblighi concernenti le capacità nazionali nel campo della cybersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, fornitura e distribuzione di acqua potabile, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di *cloud computing* e mercati online).

[12] Le Autorità competenti NIS sono responsabili dell'attuazione del D.Lgs. 18 maggio 2018 n.65 con riguardo ai settori e ai servizi ivi riportati e vigilano sull'applicazione del decreto a livello nazionale esercitando altresì poteri ispettivi e sanzionatori. Ai sensi dell'art. 7 D.Lgs. n. 65 del 2018, sono designate quali Autorità competenti NIS per i settori e sottosettori di e per i servizi: a) il Ministero dello sviluppo economico per il settore energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali; b) il Ministero delle infrastrutture e dei trasporti per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada; c) il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca D'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze; d) il Ministero della salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il trami-

a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;

b) la dipendenza di altri settori dal servizio fornito da tale soggetto;

c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;

d) la quota di mercato di detto soggetto;

e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;

f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

I FSD, invece, sono le persone giuridiche che forniscono servizi di *e-commerce, cloud computing o motori di ricerca.* È importante notare che non rientrano nella direttiva gli FSD con meno di 50 dipendenti e un fatturato o bilancio annuo inferiore ai 10 milioni di euro (il legislatore richiama nuovamente il concetto di "microimpresa").

Tali soggetti (tanto gli OSE quanto gli FSD):

– devono adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi;

– devono prevenire e minimizzare l'impatto degli incidenti di sicurezza delle reti e dei sistemi informativi;

– sono tenuti a notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, sulla continuità e sulla fornitura del servizio, informandone anche l'Autorità nazionale competente (c.d. NIS).

L'Italia, mediante il Dipartimento delle informazioni per la sicurezza (Dis) della Presidenza del Consiglio, ha identificato gli operatori di servizi essenziali operanti sul nostro territorio. Si tratta in totale di 465 realtà, tra pubbliche e private, delle quali per motivi di sicurezza non sono stati forniti i nomi; verranno resi noti quando il livello di *cyber* difesa di ognuno sarà giudicato all'altezza.

La **notifica degli incidenti** dovrà essere effettuata dagli OSE e FSD al CSIRT (*Computer Security Incident Response Team* italiano), che andrà a sostituire, fondendoli, gli attuali CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e CERT-PA (operante presso l'Agenzia per l'Italia Digitale).

I soggetti giuridici non identificati come OSE e che non sono FSD possono

---

te delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza; e) il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

inoltrare su base volontaria al CSIRT (quest'ultimo istituito presso la Presidenza del Consiglio dei Ministri) notifiche degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati.

Infatti, l'intento della Direttiva NIS è quello di favorire la più ampia diffusione di una cultura nel campo della cyber security e di un conseguente accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni tra gli apparati di *cyber* difesa che gli stati potranno introdurre per far fronte ai crescenti rischi in campo *cyber security*. Solo una puntuale condivisione delle minacce ha permesso e permetterà agli organi di contrasto ed alle autorità nazionali ed europee di accrescere il livello di consapevolezza ed istradare azioni di contrasto efficaci.

In relazione a tali esigenze si spiega la istituzione della rete CSIRT. In questi termini, occorre chiarire che – siccome la sicurezza delle reti e dei sistemi informativi è oggetto di interesse di ogni Stato membro – risulta necessaria una cooperazione internazionale più stretta per migliorare le norme di sicurezza e gli scambi di informazioni e promuovere un approccio globale comune agli aspetti di sicurezza.

Ebbene, la responsabilità di garantire la sicurezza della rete e dei sistemi informativi incombe in larga misura agli operatori di servizi essenziali e ai fornitori di servizi digitali degli Stati membri. In quest'ottica, come previsto dall'art. 12 Direttiva NIS, al fine di contribuire allo sviluppo della fiducia fra stati membri e di promuovere una cooperazione operativa rapida ed efficace, è istituita la rete CSIRT che svolge i compiti di scambio di informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione dei CSIRT.

IL CSIRT italiano, a cui sono attribuite le medesime funzioni del *Computer Emergency Response Team* (CERT), svolge diversi compiti in ambito *cyber security* che se attuati possono realmente contribuire ad incrementare il livello di sicurezza europeo:

– la definizione di procedure per la prevenzione e la gestione degli incidenti informatici;

– la ricezione delle notifiche di incidente con obbligo di informare il Dis, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al Nucleo per la Sicurezza Cibernetica;

– la fornitura, al soggetto che ha effettuato la notifica, di informazioni che possono facilitare la gestione efficace dell'evento;

– l'informazione degli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'OSE o del FSD nonché la riservatezza delle informazioni fornite.

In ultimo, l'aspetto incoraggiante sotto il profilo collaborativo è il fatto che il

CSIRT deve identificare forme di collaborazione, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di *best practice.*

Il modulo per la notifica è unico sia qualora la notifica avvenga su base obbligatoria che facoltativa [13]. Le informazioni richieste sono tante ma non tutte necessarie.

Qualora obbligatoria, la mancata comunicazione espone inevitabilmente le società al rischio sanzione per omessa comunicazione. In attuazione della Direttiva, infatti, l'Italia ha previsto un regime sanzionatorio secondo cui potranno essere irrogate sanzioni amministrative fino a 150.000 euro per gli OSE e fino a 125.000 euro per i FSD.

L'aspetto che tuttavia preoccupa è il numero di comunicazioni, obbligatorie o facoltative, che potrebbe essere necessario effettuare in caso di incidente di sicurezza: all'interessato e al Garante privacy (in caso di *data breach*), al CSIRT, all'Organismo di vigilanza, al management aziendale e in alcuni contesti alla Banca d'Italia e alla BCE.

4. *Cyber-risk* e nuovi prodotti assicurativi

Posto che assume sempre più rilievo la *Cyber Risk,* intesa come ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e per i sistemi informatici, nel mercato assicurativo si stanno sempre più diffondendo prodotti assicurativi relativi al rischio informatico che coprono i soli rischi e non anche le sanzioni.

Nei contratti di assicurazione, volti a coprire il *cyber-risk,* accanto alle prestazioni dell'assicurato e dell'assicuratore, è necessaria l'esistenza del rischio che se non è mai esistito o ha cessato di esistere prima della conclusione del contratto determinerebbe la nullità del contratto (art. 1895 cod. civ.).

Invero, sotto il profilo funzionale, l'assicurazione intesa quale operazione economica attua sempre un trasferimento di un rischio dalla sfera dell'assicurato (che in tal caso è un OSE o FSD) a quella dell'assicuratore, il quale provvederà alla neutralizzazione dello stesso mediante il suo inserimento in una massa di rischi omogenei secondo i principi della tecnica assicurativa.

Come si è già notato, il rischio cibernetico è un rischio di tipo operativo che è associato alle perdite economiche inflitte ad una organizzazione dalla mancata

[13] In attesa che il complesso meccanismo prenda forma basterà collegarsi al sito www.csirt-ita.it. Ad oggi per una eventuale notifica di incidenti potrà essere utilizzato il modulo disponibile nella sezione Modulistica del sito. Che dovrà essere firmato digitalmente e inviato in forma cifrata all'indirizzo e-mail: notifica.nis[at]csirt-ita.it.

confidenzialità, disponibilità di integrità di informazioni e sistemi informativi, propri o di terzi.

Il rischio cybernetico può essere accidentale o deliberato a seconda che l'incidente si verifichi per cause non imputabili ai soggetti coinvolti, ad esempio nel caso dello spegnimento di un *server;* sarebbe, invece, un rischio deliberato nell'ipotesi di eventi che derivano da condotte volontarie di soggetti che hanno lo scopo di raggiungere degli obiettivi personali di varia natura, come nel caso di un attacco cibernetico da parte di un *hacker* che intende sottrarre i dati sensibili.

Invero, l'assicurazione che copre la *Cyber Risk* ha una certa importanza in termini: 1) controllo del rischio in caso di sospetti di incidenti informatici e *data breach;* 2) la polizza assicurativa si pone come ausilio ad una più agevole gestione dell'impresa nella crisi cibernetica (essa accompagna l'impresa a ridurre i danni derivanti da sanzioni, interruzione di esercizio, fermo dell'attività).

La *Cyber Insurance* si pone come strumento volto a minimizzare i rischi e i danni informatici, ma non copre eventuali sanzioni amministrative (si veda Reg. IVASS n. 38/2018 che prevede l'implementazione di un sistema di monitoraggio sistematico per identificare tempestivamente incidenti e valutare la resilienza al *cyber risk*) [14].

5. *Cybersecurity Act*

Il 7 giugno 2019 la Gazzetta Ufficiale della UE ha pubblicato il regolamento comunemente denominato *Cybersecurity Act* o "Regolamento sulla *cybersicurezza"* (Regolamento (UE) 2019/881 del 17 aprile 2019), entrato in vigore il 27 giugno 2019.

Questo intervento, a livello di quadro generale sulla sicurezza del *Web* in ambito unionale, completa precedenti azioni della UE in questo ambito, come la direttiva NIS (direttiva (UE) 2016/1148) ed il *General Data Protection Regulation* (Regolamento 2016/679/UE).

L'Unione europea ha approvato il cosiddetto *Cybersecurity Act* che introduce un complesso quadro normativo al fine di armonizzare maggiormente la politica di *resilienza* da attacchi cibernetici in tutto il territorio europeo. A questo fine, il regolamento interviene su due versanti principali:

[14] A tal riguardo giova richiamare l'art. 32 del citato Reg. IVASS che dispone che deve essere notificato all'Ivass ogni evento che possa ragionevolmente comportare, o abbia già comportato cambiamenti sostanziali dell'attività e dei risultati del sistema di "governance", del profilo di rischio o della condizione finanziaria e di solvibilità dell'impresa.

• il primo, rinnovando il ruolo ed il mandato conferito all'agenzia europea ENISA che, d'ora in poi, sarà un centro di competenza permanente sul tema e fornirà supporto agli Stati membri nell'implementazione delle relative politiche di sicurezza;

• il secondo, mediante la istituzione di un processo di certificazione europeo sulla sicurezza cibernetica, riconosciuto da tutti gli Stati membri.

Invero, come rileva dal *Considerando* n. 65 del Regolamento 2019/881/UE, la certificazione della cibersicurezza riveste un ruolo importante nel rafforzare la sicurezza di prodotti TIC (ossia elementi di reti e sistemi informativi), servizi TIC (ossia la trasmissione, conservazione e recupero di informazioni attraverso la rete o i sistemi informativi) e processi TIC (ossia le attività volte a programmare o sviluppare un prodotto o un servizio TIC) e nell'accrescere la fiducia da parte degli utenti negli stessi.

Il mercato unico digitale, in particolare l'economia dei dati e l'*Internet d*egli oggetti, possono prosperare solo se i cittadini sono convinti che tali prodotti, servizi e processi offrono un determinato livello di cibersicurezza. Invero il sistema di certificazione è già ampiamente utilizzato nei settori delle automobili connesse e automatizzate, dei dispositivi medici elettronici, dei sistemi di controllo per l'automazione industriale e delle reti elettriche intelligenti.

Orbene, il recente regolamento costituisce un ulteriore passaggio verso una maggiore sicurezza del mondo digitale europeo che aveva già registrato precedenti importanti sia col GDPR sia con la direttiva NIS.

L'ambiente informatico è divenuto strategico per la gestione e lo sviluppo delle nostre società; reti, sistemi informativi e servizi di comunicazione elettronica (tecnologie dell'informazione e comunicazione, cosiddette "TIC") «svolgono un ruolo essenziale nella società e sono diventati i pilastri della crescita economica (...) in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e, in particolare, contribuiscono al funzionamento del mercato interno».

L'incremento della digitalizzazione e della connettività – anche grazie all'avvento dell'Internet degli oggetti ("*Internet of things"* o IoT) – «comporta maggiori rischi connessi alla cibersicurezza» mentre di converso, «la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione». "Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di comunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, organizzazioni e imprese, a partire dalle piccole e medie imprese (PMI), fino ai gestori delle infrastrutture critiche.» [Considerando (1-3)].

La politica di supporto alla sicurezza cibernetica in ambito UE è stata perseguita con una pluralità di interventi tra cui i principali sono il GDPR e la direttiva NIS, pur con le dovute differenze connesse ai diversi contesti di riferimento.

Sebbene l'ambito applicativo del GDPR sia confinato al dominio dei dati personali, il tema della sicurezza è affrontato dal regolamento in modo strategico sotto il profilo quantitativo e qualitativo.

Dal punto di vista quantitativo, la definizione molto ampia di "dato personale" fa rientrare nel dominio applicativo del GDPR la quasi totalità del patrimonio informativo di cui necessita un'organizzazione, qualsiasi sia il settore di appartenenza.

Sotto il profilo qualitativo, la sicurezza delle informazioni è un principio di liceità del trattamento dei dati personali, nel senso che l'uso degli stessi non può ritenersi lecito se sprovvisto di un adeguato sistema di misure tecnico-organizzative di salvaguardia.

Per il GDPR, pertanto, un utilizzo non sicuro di dati personali è illecito e suscettibile di sanzioni e di provvedimenti inibitori, con gravi ripercussioni sul business aziendale. La declinazione di dettaglio di questo principio si ritrova nella prescrizione dell'articolo 32 che impone al titolare del trattamento di adottare misure tecnico-organizzative adeguate al rischio nonché nella regolamentazione del processo di violazione dei dati personali ("*data breach"*), la più completa disciplina sul tema in ambito unionale (artt. 33 e 34).

6. L' armonizzazione delle diverse leggi sulla *Cybersecurity* e il GDPR

La Direttiva NIS (UE 2016/1148) costituisce il primo atto giuridico della UE sulla sicurezza cibernetica – oggetto dell'*Alert d*el 5 luglio 2018, cui si rinvia. Essa affronta il tema della sicurezza nelle infrastrutture critiche e della disciplina di eventuali *data breach* in tali ambiti, istituendo «i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri».

La direttiva NIS, come indica il termine, è basata sullo strumento giuridico della "direttiva" unionale anziché su quello del "regolamento" per cui, diversamente da quest'ultimo, si indirizza agli Stati membri e deve essere recepita da questi tramite atti normativi nazionali.

Per l'Italia, la direttiva NIS – lasciando impregiudicata la possibilità di ciascun stato membro di adottare misure necessarie per assicurare la tutela degli interessi essenziali della sua sicurezza (*Considerando* n. 8 Direttiva NIS) – è stata recepita tramite il decreto legislativo n. 65/2018.

In questi termini, differentemente dal GDPR, la direttiva NIS:

• non si riferisce a qualsiasi tipologia di organizzazione ma unicamente ai gestori di infrastrutture critiche (cioè quelli dell'energia e dei trasporti, quello bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) ed ai fornitori di servizi di-

gitali (precisamente, mercato online, motori di ricerca online, servizi di cloud computing).

• impone agli operatori dei servizi essenziali e ai fornitori dei servizi digitali di notificare solo gli incidenti che abbiano un impatto rilevante sui servizi forniti (in tal caso, si tiene conto del numero degli utenti interessati, della durata dello stesso e della diffusione geografica, relativamente all'area interessata dall'incidente), sebbene anche nel contesto NIS, vi sia l'obbligo di adottare le misure per prevenire e minimizzare gli impatti degli incidenti nonché di individuare le misure tecniche e organizzative relative alla gestione dei rischi.

A ciò si aggiunge il *Cybersecurity act* del 17 aprile 2019. Lo strumento giuridico del regolamento europeo è stato prescelto sulla base della considerazione che «*le competenze in materia di cibersicurezza e autorità incaricate dell'applicazione della legge e le relative risposte politiche sono prevalentemente nazionali*» mentre gli attacchi informatici avvengono spesso attraverso le frontiere tanto da richiedere un intervento normativo uniforme.

Gli obiettivi del *Cybersecurity Act s*ono quelli di:

• creare un quadro normativo di riferimento – omogeneo a livello UE – a supporto della resilienza agli attacchi informatici

• creare un mercato unico della sicurezza cibernetica per prodotti, servizi e processi

• accrescere la fiducia dei consumatori nelle tecnologie digitali.

7. Le certificazioni sulla sicurezza

Il *Cybersecurity Act* sostituisce il precedente regolamento (UE) 526/2013 con il quale si era dato l'ultimo rinnovo al mandato dell'ENISA, sino al 2020.

Il regolamento sulla cybersicurezza si compone essenzialmente di due parti:

1. quella in cui vengono specificati il ruolo ed il mandato della rinnovata agenzia europea sulla sicurezza cibernetica ("ENISA") (artt. 1-45)
2. quella in cui si istituisce un sistema europeo per la certificazione della sicurezza informatica di dispositivi, prodotti e servizi digitali (artt. 46-65).

L'Agenzia europea per la sicurezza delle reti e dell'informazione ("ENISA") era già stata istituita nel 2004, con mandato limitato sia sotto il profilo della competenza (prevalentemente consultiva, per contribuire all'obiettivo generale di garantire un livello elevato di sicurezza delle reti e dei sistemi informativi nella UE) sia sotto quello temporale (in quanto, nonostante i ripetuti rinnovi, il mandato all'agenzia sarebbe infine scaduto nel 2020).

Il *Cybersecurity Act* trasforma l'ENISA in un'agenzia permanente – un vero centro di competenza europeo sulla cybersecurity – ampliandone le competenze che includono:

• l'attività di supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri nonché nello sviluppo e nell'attuazione delle politiche comunitarie

• un ruolo di primo piano nella gestione del sistema di certificazione introdotto dal regolamento, mediante la predisposizione di schemi europei per la certificazione sulla sicurezza cibernetica che saranno poi adottati dalla Commissione mediante atti di esecuzione.

L'ulteriore principale intervento del *Cybersecurity Act* consiste nell'aver introdotto un quadro normativo per la **certificazione sulla sicurezza** in internet di valenza unionale per assicurare un approccio comune sul mercato interno dell'Unione e, da ultimo, per migliorare la sicurezza cibernetica dei prodotti digitali incrementando la fiducia riposta dai consumatori nel mercato digitale [15].

Anche in questo caso, la certificazione introdotta dal Cybersecurity Act lascia impregiudicata «l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità» al GDPR «dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento» anche nel caso che le operazioni di trattamento siano integrate nelle TIC [v. Considerando (74)].

La certificazione sulla sicurezza cibernetica disciplinata dal Cybersecurity Act parte da schemi di certificazione che – come detto – sulla base di un quadro complessivo di regole comunitarie, vengono realizzati dall'ENISA, sono approvati dalla Commissione con atti di esecuzione, e conseguentemente vengono riconosciuti in tutti gli Stati membri; in questo modo si viene a modificare la situazione precedente che annoverava schemi di certificazione specifici per prodotti e sistemi TIC, esistenti presso singoli paesi ma non riconosciuti a livello transnazionale: si veda, ad esempio, il caso dei contatori intelligenti (o "*smart meters"*) i cui produttori sono sottoposti a distinti processi di certificazione in Francia, Gran Bretagna e Germania. Quindi, il Cybersecurity Act non istituisce schemi di certificazione direttamente operativi ma definisce un quadro regolatorio per la loro creazione. Una volta adottato uno schema di certificazione europeo, le aziende volontariamente potranno presentare domanda di certificazione dei propri prodotti, servizi o processi agli organismi di certificazione nazionali (in Italia, l'OCSI, Organismo di Certificazione della Sicurezza Informatica);

[15] Per una interessante lettura in tema di certificazioni di qualità, si cfr. E. BELLISARIO, *Certificazioni di qualità e responsabilità civile*, Milano 2011.

salvo che la certificazione di sicurezza non venga espressamente richiesta come obbligatoria per specifici prodotti o servizi da eventuali norme di settore.

Gli obiettivi di maggiore interesse per la certificazione della sicurezza sono:

• appurare che i sistemi, servizi o processi siano in grado di proteggere i dati dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita;

• verificare che siano in grado di proteggere i dati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità;

• che l'accesso di persone, programmi o macchine sia limitato esclusivamente ai dati, ai servizi o alle funzioni per i quali questi dispongono dei diritti di accesso;

• che siano state individuate e documentate le dipendenze e vulnerabilità note, che sia possibile registrare a quali dati, servizi o funzioni è stato effettuato l'accesso, in quale momento e da chi;

• che sia possibile ripristinare tempestivamente la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in caso di incidente fisico o tecnico;

• che siano utilizzati criteri di "security by design" per la progettazione di prodotti e servizi, e "by default", in modo che tali prodotti implementino le impostazioni più sicure, ed infine che il software e l'hardware dei prodotti TIC siano costantemente aggiornati per mezzo di meccanismi protetti.

Tenendo conto che non tutti i sistemi, processi e servizi hanno lo stesso profilo di rischio, il Cybersecurity Act prevede tre livelli di certificazione differenti (art. 52 commi 5, 6 e 7):

• Un livello di affidabilità "di base" per il quale il produttore/fornitore può ricorrere all'autocertificazione, ove prevista; in questa ipotesi può bastare un riesame della documentazione tecnica, o attività di valutazione sostitutive di effetto equivalente intese a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici.

• Un livello di affidabilità "sostanziale" per il quale la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo i rischi noti alla cybersicurezza ed i rischi di incidenti ed attacchi informatici commessi da soggetti che dispongono di abilità e risorse limitate. Le attività di valutazione comprendono almeno un riesame per verificare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti o servizi attuino correttamente le necessarie funzionalità di sicurezza.

• Un livello di affidabilità "elevato", per il quale la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati, commessi da attori che dispongono di abilità e risorse significative.

Le attività di valutazione comprendono: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC attuano correttamente le necessarie funzionalità di sicurezza allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione.

I certificati europei sulla sicurezza informatica non attestano o garantiscono che un prodotto o servizio certificato in base ad un determinato schema accreditato sia sicuro bensì che lo stesso risponda agli specifici requisiti definiti nello schema. I certificati così rilasciati saranno riconosciuti in tutti gli Stati membri dell'Unione, facilitando sia gli affari degli operatori che agiscono a livello transnazionale sia la fiducia e consapevolezza degli acquirenti circa il livello di sicurezza certificato.

Obiettivo del legislatore tramite la certificazione europea sulla sicurezza è quello di promuovere la sicurezza informatica sin dalla fase iniziale di progettazione e sviluppo dei prodotti TIC e di quelli di consumo che costituiscono gli *IoT* ("***security by design***"). Questo consentirà agli utenti di conoscere il livello di sicurezza dei prodotti/servizi scelti assicurando che le misure di sicurezza siano verificate in modo indipendente. Le organizzazioni dovrebbero configurare i TIC da loro progettati «in modo da garantire un livello di sicurezza superiore che dovrebbe consentire al primo utente di ricevere una configurazione predefinita con le impostazioni più sicure possibili («sicurezza predefinita»), riducendo al contempo l'onere in capo agli utenti di» doverlo essi stessi configurare in modo adeguato. La sicurezza predefinita dovrebbe essere possibile senza necessità di «conoscenze tecniche specifiche o di un comportamento non intuitivo da parte dell'utente, e dovrebbe funzionare in modo semplice e affidabile quando attuata».

DATA PRIVACY CHALLENGES OF CONTRACTUAL CONSENT TO PROCESS PERSONAL DATA: THE EXAMPLE OF NETFLIX

Mai-Brit Campos Nielsen
LL.M. at the University of Edinburgh

Abstract:

This article explores the data privacy challenges of the use of contractual consent as a precondition to use the internet-connected streaming services offered by Netflix. In this context, the article explores the regulatory limits of applying contractual consent from the consumer's perspective. The article examines whether the contractual consent in Netflix leads to loss of control for the user, and if so, whether other safeguards in the General Data Protection Regulation are appropriate to protect the data privacy of the user. The article ends by concluding that other regulatory constraint should be considered to protect the data privacy of the users of Netflix's streaming services.

Key-words: consent, privacy policy, control, safeguard, consumer, transparency, purpose limitation.

Introduction

The aim of the General Data Protection Regulation [1] (hereafter GDPR) was to be a response to new technological developments which require a strong and

[1] Council Regulation (EC) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

more coherent data protection framework in the European Union. Natural persons should have control of their own personal data. [2] Still, many Europeans feel that they have insufficient control over their personal data. [3]

Undoubtedly, the scale of collection and sharing of personal data has increased significantly over the years. Similarly, the use of contractual consent to the processing of personal data as a pre-condition to use internet-connected devices is common. This is for example the case for consumers using internet-connected devices such as Fitbits, smart watches, Netflix's services or particular apps on their mobile phone. Consumers are confronted with privacy policies that envisage the processing of a significant amount of their data to which they must agree in order to use the device for its purpose. The data in question can for instance be location data, information of their personal preferences or viewing habits.

This article will explore the data privacy challenges of such contractual consents in relation to relevant principles in the GDPR taking its starting point in the example of the internet-connected service Netflix. First, the article will explore the concept of consent and apply it to the consent required by Netflix to its Privacy Policy. Secondly, the article will assess the data protection implications deriving from contractual consent given to access Netflix's services, including whether contractual consent lead to insufficient control over your own personal data, and whether there are other safeguards to protect the data subject. Finally, the use of contractual consent will be assessed in the view of consumer law, including if any further regulatory constraint is needed. The article will apply the consumer's perspective. When referring to the data subject in this article, this is understood to be the consumer.

1. The example of Netflix

Netflix is chosen as example as it has a growing popularity with its on demand streaming services. Netflix's content can be accessed by different internet-connected devices. Netflix's streaming services allows subscribers to stream television series and films via the Netflix website on personal computers, or the Netflix software on a variety of supported platforms, including smartphones and tablets, digital media players, video game consoles and smart TVs. If a consumer uses his or her internet-connected TV to access Netflix's services, the consumer will be met by a Privacy Policy to agree or disagree in order to continue

[2] See Recital 7 of the General Data Protection Regulation.

[3] PTJ Wolters, 'The control by and rights of the data subject under the GDPR' (2018) 22(1) Journal of Internet Law, 7.

to access Netflix's content. The Privacy Policy states:

'When this TV is connected to the Internet, information about the TV device status and setting, such as network service content and bitrate, Device ID, model name, software version, language, region and country, codec support and settings related to picture, sound and system, may be sent to Sony's Corporation's global servers. This information is necessary to access Internet content. Accepting this privacy policy will mean that a unique number is sent to Sony Corporation's global servers.'

2. General conditions for valid consent

The elements to construe valid consent according to GDPR will be explored in the following.

1. The concept of consent

The role of consent in relation to the processing of personal data is recognised in the EU Charter of Fundamental Rights [4] by the wording in Article 8(2) 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law.'

The processing of personal data is lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes by virtue of Article 6(1)(a) of the GDPR. The possibility of using consent for contractual purposes is covered by Article 7(4).

An indication

Under the Data Protection Directive, the definition of consent was based on an indication of the data subject's wishes. The form of the indication was flexible, and a requirement of 'written' consent has been kept out [5], similarly in the GDPR.

Article 4(11) of the GDPR clarifies that valid consent requires an 'unambiguous indication' by means of 'a statement or by clear affirmative action'. 'A clear affirmative act' means that the data subject must have taken a deliberate

[4] Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 303 14 December 2017 (hereafter 'the EU Charter').

[5] Article 29 Data Protection Working Party. Opinion 15/2011 *on the definition of consent*, 13 July 2011 (hereafter 'WP 29 Opinion on consent'), 11.

action to consent to the particular processing.[6] This can be fulfilled by 'ticking a box' when visiting a website, by choosing technical browser settings, by a statement or by conduct that clearly indicates the data subject's acceptance. In the case of Netflix, the data subject will fulfill the requirement 'a clear affirmative act' by clicking 'agree' to the Privay Policy on the TV.

To signify the agreement

The data subject must signify his or her consent which seems to indicate that simple inaction is insufficient[7] and some sort of action is required to establish consent. Therefore, absence of behaviour or passive behaviour seems to fall out of the scope of indication, and it will neither be considered unambiguous.

Similarly, silence, pre-ticked boxes or inactivity should not constitute a consent.[8] The sole activation of the Bluetooth function for example does not constitute valid consent to receive advertising messages on the mobile phone.[9]

In conclusion, when a data subject clicks 'agree' to the Privacy Policy before accessing Netflix's services, this is considered to be an indication of wishes containing a clear affirmative action signifying an agreement. By clicking 'agree', the data subject gives explicit consent.[10]

2. A specified and informed consent

In order to achieve valid consent, the consent shall be specified and informed.

Specified consent

According to Article 6(1)(a), the consent must be given in relation to 'one or more specific purposes'. A specified consent is closely linked to the basic principle of purpose limitation in Article (5)(1)(b), which is designed to establish the boundaries within which personal data collected for a given purpose may be processed for further use.[11] The requirement of the specified consent should prevent the gradual widening or blurring of purposes for which data is pro-

[6] Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259rev.01 (hereafter 'WP 29 Guidelines on consent'), 16.

[7] WP 29 Opinion on consent (n 6) 12.

[8] See Recital 32 of the General Data Protection Regulation.

[9] WP 29 Opinion on consent (n 6) 12.

[10] WP 29 Guidelines on consent (n 7) 19.

[11] Article 29 Data Protection Working Party. Opinion 03/2003 *on purpose limitation*, 2 April 2013. 00569/13/EN WP 203.

cessed after the first consent is given, also called 'function creep'. [12]

When a data subject clicks 'agree' to the Privacy Policy of Netflix it may cover different operations. However, according to the purpose limitation principle, the operations should serve the same purpose, otherwise it is unlawful processing, which will need new consent from the data subject.

Informed consent

Informed consent is linked to the principle of transparency reflected in Article 5(1)(a). The principle of transparency covers providing accessible information to the data subject, so the data subject is capable of understanding what they agree to by consenting. Article 7(2) requires the information given to be in a clear and understandable manner. [13] The Article 29 WP has described the minimum information requirements that should be given to the data subject. [14]

When a data subject is confronted with a privacy policy to agree on before access to the device's services, not all required information may be available on the screen. More comprehensive information not suitable for the screen may only appear in the privacy policy itself whereto access through a link. This method is deemed acceptable regarding consent provided in apps for example. [15]

In conclusion, it is possible to give some of the minimum information to the data subject by access through a link. It would still be considered informed consent. This is the case with the wording of the Privacy Policy of Netflix, where there is only a minimum of information available on the screen, provided a link to the full text of the Privacy Policy contains the rest of the required information.

3. Limits to contractual consent

1. The scope of Article 7(4) and necessity

[12] WP 29 Opinion on consent (n 6) 12.

[13] ibid 19.

[14] WP 29 Guidelines on consent, 19: '1) the controller's identity, 2) the purpose of each of the processing operations for which consent is sought, 3) the type of data that will be collected, 4) the existence of the right to withdraw consent, 5) information about the use of data for automated decision-making, cf. Article 22, 6) possible data risks of data transfers due to absence of adequacy decision and appropriate safeguards.'

[15] Article 29 Data Protection Working Party. Opinion 02/2013 on apps on smart devices, 27 February 2013. 00461/13/EN WP 202 (hereafter 'WP Opinion on apps on smart devices'), 24.

Article 7(4) permits the tying of consent to process the user's personal data with the performance of a contract.

In the original Commission proposal for the GDPR, [16] consent was not a legal basis if 'there is a significant imbalance between the position of the data subject and the controller'. In the final version of the GDPR, the wording regarding the imbalance was omitted and was instead inserted in Recital 43, which decreases its strength.

To determine the general scope of Article 7(4), it is important to look at the scope of the contract and which data would be necessary for the performance of the contract. [17]

If processing of personal data is necessary to perform the contract (including to provide a service), then Article 7(4) does not apply. The appropriate lawful basis in that case would be Article 6(1)(b) instead.

For instance, it is necessary for the purchase of goods to have the data subject's address information to process credit card information in order to facilitate a payment or to require bank account information to process the salary to an employee. [18] For it to be necessary, following a strict interpretation, there needs to be a direct and objective link between the processing of data and the purpose of the execution of the contract. [19]

In the case of access to Netflix's streaming services on TVs, the user has to agree to a privacy policy, if the user wants access to the Internet content provided. The processing of data includes information about the TV device status and setting, language, region and country, picture, sound etc. The processing is combined with disclosure of data to the company's global servers.

The policy states that the information is necessary to access Internet content, but there is no direct link between the compilation and disclosure of data regarding the TV's status and setting, and the purpose of the performance of the contract (access to the Internet content). Therefore, the situation concerning access to Netflix's streaming services fall within the scope of Article 7(4).

2. The 'freely given' aspect

To assess whether the consent in the context of Article 7(4) is freely given 'utmost account shall be taken of whether, inter alia, the performance of a con-

[16] European Commission, 2012/001. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement on such data (General Data Protection Regulation).

[17] WP 29 Guidelines on consent (n 7) 9.

[18] ibid.

[19] WP 29 Guidelines on consent (n 7) 8.

tract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'

In this respect, it is crucial that the data subject has a real choice. It is presumed not to be freely given, if the consent is bundled up as a non-negotiable part of terms and conditions. [20]

Article 7(4) has been drafted in a non-exhaustive way with the words "inter alia" to be considered. That means, any element of 'inappropriate pressure or influence upon the data subject (...) which prevents a data subject from exercising his or her free will, shall render the consent invalid.' [21]

The concept of freely given also amounts to whether it is possible to refuse or withdraw the consent without detriment, see Recital 42 of the GDPR. In this respect, a refusal to consent having as a consequence that the contract cannot be performed, leaving the data subject without any other option, will not be considered as freely given.

This is in accordance with the example of a mobile app for photo editing. [22] The app required GPS localisation to be activated and collected behavioural data, although neither of these were necessary for the photo editing service. Without consenting to these purposes, the app did not work, thus having a negative consequence on the performance. This consent was not considered as freely given.

The implication is that the more a party seeks to condition the performance of a contract on requiring a data subject to consent to the processing of personal data unrelated to the underlying agreement, the less likely it is that the consent is considered as freely given. [23]

Additionally, according to the 'imbalance between the data subject and the controller' in Recital 43 of the GDPR, if a data subject's relationship with the data controller creates pressure on the data subject to provide consent, or the data subject might not feel at liberty to refuse consent, it was not freely given. [24]

In the case of access to Netflix's streaming services on TV, if the data subject does not give his or her consent to data processing, he or she would be deprived from getting access to the Internet content provided by the contract. Consequently, the data subject is in a situation where he or she does not have a real

---

[20] WP 29 Guidelines on consent (n 7) 5.

[21] ibid 6.

[22] ibid 6.

[23] B Thompson, 'GDPR, Part IV: The Data Subject Consent Provisions' (2017) Mondaq Business Briefing 23 November 2017.

[24] Thompson (n 24) 6.

choice. Therefore, not consenting would have a negative impact on the performance of the contract and the consent would not be freely given.

Netflix's real purpose for the collection of the data can be argued to be 'the profiling approach' in Article 4(4). Hereby is meant processing of data to analyse or predict aspects concerning a person's personal preferences, interests, behaviour, location etc.

4. Does consent gives you control over your data?

In many situations, the data subject gives consent - freely given or not - to the processing of data in order to get access and use internet-connected devices to access services as Netflix's streaming content.

If a consent given is incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing. [25] On the opposite, if a consumer has agreed voluntarily to contract terms allowing collection and use of data, the controller is permitted to grant this power to third parties.

Consent to data allocation through a device implies collection of several data, for instance location data. Similarly, in the example of Location-sharing-based services (LSBS) users allow their location to be disclosed to the service provider in order to share it with their friends, [26] as for example on Facebook. The service provider and third parties can infer private user information, such as their movement patterns, home address, lifestyle and interests, [27] all of which is useful information to target advertisements.

While this may be useful in some aspects, the disclosure of data raises significant privacy concerns as explored below.

In the case of Netflix, its streaming services collect a huge amount of data covering IP address, watch history, search queries, but if the user logs into Netflix on a Web browser, it also collects information on the user's browsing history such as cookies. [28]

Netflix might supplement the collected information with information from other sources, including both online and offline data providers. What is worse is

[25] WP 29 Opinion on consent (n 6) 2.

[26] M Herrmann and others, 'Practical Privacy-Preserving Location-Sharing Based Services with Aggregate Statistics. Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks' (2014), 87-98.

[27] ibid 87.

[28] M Saltzman, 'Netflix has a lot of your personal data, too.' (2018) USA Today, 18 April 2018, Business News p03B.

Netflix's sharing of information with third parties. Hereto, Netflix says it shares information 'for limited purposes, as explained in our Privacy Statement'. [29] This includes sharing information with Internet Service Providers and third-party companies tied to promotional offers with Netflix.

By Netflix's collection and analysis of data based on the user's conduct and browsing history, Netflix is able to draw precise contours of who you are, and additionally share that information with others.

For the data subject, this resembles a long-distance surveillance pattern when collecting data from the user and disclosing it to third parties. As a consequence, the data subject will experience loss of control over his or her data. In addition, there is no way in which Netflix's users can download their own watch history and keep it at themselves.

The increasing power of data controllers may put the consumers in a situation where their party autonomy becomes futile. Furthermore, an increase of power exposes the data subject to more targeted advertising based on profiling; an example of a subtle form of control over the consumer's data.

In contrast to these privacy concerns, the essential service in Netflix's streaming business model is to offer 'personalized recommendations' and to help find 'shows and movies of interest'. More importantly, the user has given consent to this by the Privacy Statement. This is in contrast to the US case of *Vizio,* where Vizio was found to be tracking everything their smart TV users had been watching, reporting it and then tailoring advertising and programme suggestions, all without knowledge or consent of the users. [30] The conduct of Vizio led to a fine by the US government. [31]

Furthermore, it can be argued that users can opt-out of interest-based ads based on cookies by choosing the appropriate setting on the device. In such a case, the user may still see Netflix ads, but they will not be tailored to likely interests. [32] In this way, the user can restrict the use of cookies, but Netflix may still collect and share other information based on the user's use of Netflix.

Notwithstanding, the trend is moving towards Netflix's business model. Broadcasters and content owners, as BBC iPlayer, are learning from the likes of Amazon and Netflix by creating new platforms [33] to offer personalized choices for its users based on data and algorithms.

---

[29] Saltzman (n 29) 87.

[30] G Eastwood, 'How to stop your smart TV from spying on you' (2017) CXO Media, 24 February 2017.

[31] J Curran, 'Vizio to Pay $2.2M settlement for data collection practices' (2017) Cybersecurity Policy Report, 13-02-2017, New York: Aspen Publishers.

[32] ibid.

[33] A Pennington, 'This time, it's personal' (2017) Media Business Insight, 23 February 2017.

To condemn the privacy concerns on location sharing devices, Herrmann [34] suggests different methods, inter alia, to work with obfuscation strategies, such as adding dummy locations or reducing precision, or more preferably identity-based broadcast encryption where the identities are hidden towards the service provider. This is in line with Recital 28 of the GDPR whereby the application of pseudonymisation to personal data can reduce the risks to the data subjects.

In conclusion, a key data protection risk of contractual consent is the lack of transparency which is closely linked to the requirement of informed consent. [35] Another risk is to disregard the principle of purpose limitation. Data collected in relation to the use of apps may be widely distributed to a number of third parties for undefined or elastic purposes such as 'market research'. [36]

Demonstratively, when using services such as Netflix's streaming services on internet-connected devices, the data subject experiences loss of control over his or her data. In this respect, it is a paradox that giving informed and specified consent results in loss of control over your data and increase of power to data controllers and third parties.

5. Other safeguards in the GDPR to protect the data subject

To reduce the key risks to the data subjects described above, there are several obligations and rights in the GDPR to be applied.

The data subject has a right to data portability in Article 20. According to Recital 63, a data subject should have the right of access to personal data which have been collected concerning them. In the case of Netflix, there is no way in which users can exercise their right to data portability as they cannot download their 'watch history'.

Giving consent does not overrule the right to data portability. Under all circumstances, the data subject can insist on this right to get access to the information that Netflix has collected concerning them. However, with reference to Wolters [37], the right to data portability will not improve the protection of data subjects. This is mainly because it does not cover data that has been created by the controller.

Worth mentioning in this context is that the data subject still has his or her right to withdraw the consent at any time according to Article 7(3), followed by

[34] Herrmann (n 27) 88.

[35] WP Opinion on apps on smart devices (n 15) 6.

[36] ibid.

[37] Wolters (n 3) 10.

the right to erasure of data and the rights to restriction, rectification and access as well in Articles 16-20.

Furthermore, controllers shall observe certain obligations when processing data based on consent. For instance, the controller should 'evaluate the risks' inherent in the processing and 'implement measures to mitigate those risks, such as encryption'.[38] The controller shall consider *inter alia* to include 'the pseudonymisation and encryption of personal data' as measures by virtue of Article 32(1), but it is not a guarantee the data subject can impose.

According to Article 24(1), the controller shall also implement appropriate technical and organisational measures to ensure compliance with the GDPR taking into account 'the nature, scope, context and purposes of processing as well as the varying likelihood and severity of the rights and freedoms of natural persons'.

The wording of Article 24(1) leaves room for an assessment by the controller. This may be problematic as the assessment includes a balancing of different rights and purposes which are obviously in contradiction with each other; that is the data subject's transparency right opposed to the business purpose of collecting of as much data as possible in order to provide personalized services. From a consumer's perspective, there is a clear risk that this assessment will fall out in favour of the controller's needs and not the consumer.

Despite the fact that 'necessary' is not mentioned with respect to processing on the basis of consent in Article 6(1)(a), it does not negate the controller's obligations regarding the principles of fairness, necessity and proportionality[39] enshrined in Article 5.

However, the principle of necessity is difficult to apply by the data subject as a safeguard. This is confirmed by Bakos,[40] who claims that the drafter (data controller) can unilaterally define the purpose and the necessity of the contractual clause. To discover what this principle means in a specific situation, the data subject needs to carefully examine the contract, which is not realistic to do. In practice, this means that the performance of the necessity test lies with the data controller.

The applicability of the principle of purpose limitation as a safeguard is also challenging in practice. As Mantelero[41] held, many consumers are not able

[38] Recital 83 of the General Data Protection Regulation.

[39] WP 29 Opinion on consent (n 2) 2.

[40] Y Bakos, F Marotta-Wurgler & D R Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts' (2014) 43(1) Journal of Legal Studies, 31.

[41] A Mantelero, 'The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics' (2014) 30 Computer Law & Security Review, 653.

to understand the purposes and methods of data processing. He argues that consumers do not have the technological knowledge to evaluate the risks associated to data processing. This is supported by other authors, for instance Wolters [42] who stated that a data subject is not practically able to maintain an overview of the controllers and the processing operations.

A data subject giving consent has an expectation about the purpose for which the data will be used, mainly this being restricted to reasons that the data subject can understand and imagine. This might lead to situations where the data subject gives consent to a purpose they think is the principal, but in practice the purpose is more complex and covers more widely.

6. Consumer law's perspective on contractual consent

Demonstratively, there are key data protection risks for the consumer in the contractual consent to process data when using internet-connected devices to access Netflix's content. The level of consumer protection in the context of contractual consents will be examined in the light of general EU consumer law.

1. Imbalance of information

Rhoen [43] has considered the imbalance between the consumer and the data controller as the 'asymmetric information'. In other words, the cost of information per contract is higher for consumers than for controllers, mainly because the controllers unilaterally draft the privacy contracts. Individual consumers usually lack expertise and have little to gain by their resources to negotiate a better deal on privacy in a contract, consequently creating an imbalance. This is supported by Wolters [44] who led us to conclude that the position of the data subject relative to the controller is weak.

Shifting the view to EU consumer protection law by referring to the Unfair Terms Directive, [45] fairness applies to the terms of a contract. Hence, a non-negotiated term in a consent statement is regarded as unfair if 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'. [46]

[42] Wolters (n 3) 7.

[43] M Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) 5(1) Internet Policy Review, Journal on internet regulation, 3.

[44] Wolters (n 3) 7.

[45] Council Directive 93/13/ECC of 5 April 1993 on unfair terms in consumer contracts (Unfair Terms Directive) [1993] OJ L95/29.

[46] See Article 3 of the Unfair Terms Directive.

In the context of Article 7(4), the freely given consent in an app whereby the consumer agrees to collection of location and usage data, would suffice to be fair in relation to the GDPR. Whereas under EU consumer law, the clause would be assessed by the fairness concept, expanding the assessment to factors such as how the app was advertised, whether the conditions it was offered under were misleading, etc. [47]

Applying the consumer law's fairness criterion to contractual consents in data privacy would expand the accountability of data controllers considerably, as the scope of fairness is wider.

2. Enforcement concerns

In addition, as regards enforcement of the fundamental right of data protection in court, consumers may experience difficulties. Data protection law does not clearly describe a minimum level of privacy to maintain. Instead, it provides criteria for the balancing of individual privacy against other interests. Claiming damages for privacy breaches is hampered by the fact that the consumer 'give it away in exchange for so little'. [48]

In a court case, other essential fundamental rights from the EU Charter will compete with the data protection right, for example, the freedom of contract and party autonomy. Thus the court will have to assess the right balance among these rights.

In addition, EU consumer law offers better participation options than the GDPR, as the member states shall ensure consumers to pool resources, reducing the cost in proceedings, [49] whereas the GDPR does not require member states to allow complaints by advocacy groups, it merely allows them to do so in accordance with Article 80(2).

In conclusion, applying principles from EU consumer protection law in the context of contractual consents could increase the power on the users, as the scope of the fairness criteria is wider, and the enforcement options are more consumer friendly.

---

[47] Rhoen (n 44) 7.

[48] B Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data an*d Control Your World* (1st edn, Norton & Company 2015) Chapter 14.

[49] See Article 7(2) of the Unfair Terms Directive and Article 11(1) of the Unfair Commercial Practices Directive, Council *Directive* 2005/29/EC of 11 May 2005 concerning *unfair* business-to-consumer commercial practices in the internal market and amending Council *Directive* 84/450/EEC, *Directives* 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22.

Conclusion

In the case of Netflix, the contractual consent is assessed to fulfill the requirements of being specified and informed. However, the consent given as a precondition to access services by clicking 'agree' to the Privacy Policy will not be considered being freely given as the data subject in practice does not have a real choice. A lack of consent would have a negative impact on the performance of the contract and would deprive the user from access to the Internet content provided by Netflix.

Key risks in the wording and use of contractual consent are *inter alia* observance of the transparency principle and the purpose limitation principle. The data subject does not fully understand the scope of the consent and the purpose, and additionally the collected data may be widely distributed to third parties for undefined or elastic purposes which is in contradiction with the purpose limitation principle.

Demonstratively, when using Netflix's services, the data subject experiences loss of control over his or her own data. It is a paradox that giving an informed and specified consent to Netflix results in loss of control over data. In the case of Netflix, there is no way in which users can exercise their right to data portability as they cannot download their own 'watch history'.

In the light of EU consumer law, the GDPR does not protect consumers sufficiently in situations with contractual consent similar to the case of Netflix. The imbalance of information is in favour of the data controller and the data subject's enforcement remedies are weak.

Some regulatory constraints could be suggested inspired by the consumer protection law, such as widening the fairness criteria to contractual clauses in favour of the data subject. Other options of technological nature may be to encourage the application of pseudonymisation or encryption methods, in order to protect the consumer's personal data.

DATA PROTECTION LAW: A COMPARISON OF THE LATEST LEGAL DEVELOPMENTS IN CHINA AND EUROPEAN UNION

Riccardo Berti
Lawyer at Zumerle Law Firm (Verona, Italy)

Abstract:

The evolution of Data Protection Law in recent years has registered pivotal steps ahead both in China and in the EU.
While the European Union issued the GDPR (Regulation 679/2016), which came into force on 25 May 2018, in China the Cybersecurity Law received major updates and upgrades, among which, on 29 December 2017, the Standardization Administration of China issued the 国标 (guobiao) GB/t 35273-2017 (now GB/t 35273-2020), called 'Personal Information Security Specification' that came into effect on 1 May 2018, recently revised.
Other than the similar date of applicability, the two set of rules share many overlapping dispositions, that witness the growing concerns in this field that both E.U. and China share.
Despite being similar in the form, these rules then vary in the substance.
Therefore, comparing these laws, declined in their respective context, can be useful in order to determine how the right to privacy and data protection is intended in these two legal systems and why some of the European rules have been adopted more leniently in China.

Key-words: Chinese Law, EU Law, Data Protection Law.

sent" in China and in the E.U. – 4.6. The Person in Charge of Network Security and the Data Protection Officer: similarities and differences. – 4.7. Personal data protection Law and Big Data. – 5. Conclusions. – 5.1. Personal Data Protection Law as a tool to rule a global phenomenon. – 5.2. The challenges on the horizon.

1. Introduction

The legal concept of privacy evolves from the so-called "right to be let alone", and was first theorized in 1890 the United States, when jurists Samuel D. Warren and Louis Brandeis wrote 'The Right to Privacy' [1], an article where the phrase "right to be let alone" was used as a definition of privacy.

The article was a response to the worrisome technological developments of the time, such as photography and sensationalist journalism, that posed new types of threats to one person's intimacy.

Since then, the concept of privacy evolved and take broader shape, developing along concepts such as personal information control, the right to be forgotten, big data, etc.

Nowadays, privacy has become a complex concept, difficult to define and with uncertain boundaries [2], that defines the 'claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others'. [3]

The development of this complex concept revolves around concurrent ideas, that see privacy as an evolution of these entitlements: '(1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy'. [4]

While the privacy concept encompasses mostly a series of prohibitions on interference, from this same concept opened out the idea of a pro-active and dynamic way of safeguarding personal data flows, something more than a simple prohibition. [5]

From privacy therefore grew the concept of personal data protection (spawn

[1] SD Warren, L Brandeis, 'Right to Privacy' (1890-1891) IV, Harv. L. Rev.

[2] D Mulligan, C Koopman, N Doty, 'Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy' (2016) 374.118 Phil. Trans. R. Soc. A.

[3] A Westin, 'Privacy and Freedom' (1967) 166 Wash. & Lee L. Rev.

[4] D Solove, 'Conceptualizing privacy' (2002) 90.4 Cal. L. Rev. 1132-1140, D Solove, *Understanding privacy* (Harvard University Press, 2008).

[5] S Rodotà 'Data Protection as a Fundamental Right' in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt (eds) *Reinventing Data Protection?* (Springer, 2009), 77 - 82.

from the privacy "facet" of the 'control of personal information'), this is a notion at the same time broader and more specific than the one of privacy, that involves securing data against unauthorized access, sets limits to the power of others on one's personal data and grants right to data subjects in order to limit or call off the processing of their personal data.

Interestingly enough, exactly as it happened in 1890, other worrisome and uncharted innovations set the start for the latest innovations on the privacy/data protection field. For example, in the European Union the spread of Internet marks the basis for the Directive 95/46/EC of 24 October 1995, that sets common principles for European countries in the field of data protection.

More recent developments are motivated by unforeseen threats to individual privacy, compromised by the development of a real "personal data market", where the bidders are social networks and other web giants. In the light of these developments, both E.U. and China issued new legislation in the field.

The European Union issued the GDPR (Council Regulation (EU) 679/2016 of 27 April 2016), which came into force on 25 May 2018, a Regulation that repeals Directive 95/46/EC and deepens the involvement of E.U. in the privacy field.

In China, the Cybersecurity Law received major updates and upgrades, among which, on 29 December 2017, the Standardization Administration of China issued the 国标 (guobiao) GB/t 35273-2017 (now GB/t 35273/2020), called 'Personal Information Security Specification' that came into effect on 1 May 2018 and was recently revised (thus proving the high interest of Chinese government for the subject).

The truth is that, as technology advances, the ways to threaten one person's data changes. Our increasing ability to share information entails that a personal data violation is no more a local problem but can affect the life of one individual everywhere he or she goes, for the rest of his or her life.

These new laws try to address this phenomenon, let's see if their different approaches can cope with the complex technological issues they are facing.

Regarding the Chinese personal data protection law, it is, then, important to stress that the latest intervention on the subject is a 国标 (*guobiao)*. The *guobiao* (literally "national standard") is a peculiar kind of technical legislation that rules many important fields in China. *Guobiao* can be distinguished by the letters accompanying the number and year identifying them. While the acronym "GB" (*Guobiao)* stands for a mandatory provision, a "GB/t" identifies a recommended provision, where the "t" stands for *tuījiàn* ("recommended" in Chinese).

The 'Personal Information Security Specification' (GB/t 35273-2017) is therefore a recommended standard, but its significance in China is greater than

in other nations, because of the rather unique framework of legal formants in the country.

1.1. Method Note

The examination of the declination of an institution belonging to a legal culture that is autonomous, independent and original as the Chinese one is surely suitable for a comparative methodology.

Furthermore, the Chinese example is rather unique. Suffice it to say that China is one of the few countries in the world that did not suffer a direct colonization by a western country [6], thus offering a research environment not affected by the superstructure of a legal system imposed from above by a western power. The colonial period has in fact, willing or unwilling, tamed many other countries to a western legal framework, watering down their original traits. Therefore, we can still find preserved peculiar institutes in China, a country with a rich and millennial legal tradition.

The basis for comparison is without any doubt the European Union, since Chinese legislation in the field has many common traits with the European one, and since both countries decided (around the same period) that they need a revised and comprehensive legislation on privacy and personal data protection.

In order to study the Chinese legal system, which is so unique and so different from western models, we should first set up a method.

In particular this study takes into consideration the theories of Rodolfo Sacco about "legal formants" [7].

The theory of "legal formants" argues considering the role and hierarchy of the law sources in the country subject to study. Sacco evaluates the legislative, legal, and doctrinal "formants".

The different influences of these "formants" in China, as compared to the Western reality, are essential to understand the present and the future of privacy in the country. Dealing with the People's Republic of China, we must acknowledge the importance of the political formant, despite that it very often acts through the three traditional formants indicated by Sacco, it has a specific

[6] Along with Japan, North Korea, South Korea, Nepal, Bhutan, Thailand, Turkey, Saudi Arabia, Iran, Afghanistan, Ethiopia and Liberia.

[7] R Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II)' (1991) 39 The American Journal of Comparative Law 1, 34; Rodolfo Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law (Installment II of II)' (1991) 39 The American Journal of Comparative Law 343, 401; Rodolfo Sacco, 'Mute Law' (1995) 43 The American Journal of Comparative Law.

weight in Chinese law regardless of its integration into the legal system as it is understood in the West.

Secondly, the tradition, particularly the Confucian one, is considerable according to the classification proposed by Sacco as a "cryptotype" [8], since it certainly contributes to form the mentality of the Chinese jurist, although being unspoken. Another invasive "cryptotype" is surely the one represented by the economic drive, that is behind numerous rules also in the privacy field both in E.U. and in China.

Keeping in mind the role of the political formant and of these "cryptotypes" we can contextualize the noteworthiness of the comparison between China and the European Union in the privacy field. Even if the latest Chinese rules about privacy and data protection, as we have seen, were included in a mere recommended standard, their significance is greater than it would have been in any other country and they have, in fact, already bore an impact in the field, that provides food for thought in this comparison.

Chinese Law in fact often relies on vague core principles, detailed in non-binding rules. This method is really useful for the government since it let to adjust the rule in its practical implementation and to keep it up-to-date without rewrite the law.

The obvious counterpoint of this method is the uncertainty of the law, and the need of some sort of a canister for the population to understand the real weight of a rule.

1.2. Terminology

When dealing with privacy it is important to set straight what do we mean, in both the countries examined, when we talk of privacy, data protection and personal data protection.

As we have seen, privacy evolved from the so called "right to be let alone", to become a complex concept, with uncertain boundaries.

The core meaning of privacy in the legal field is, still today, the exclusion of

[8] A "cryptotype", as defined by Sacco in his *Introduzione al Diritto Comparato* (5th edn, UTET 1992), is: 'a model not verbalized, that was regarded into unexpressed'. The relationship between "formants" and "cryptotypes" is described in the same work: 'of all the formants previously considered here, some are born already verbalized (e.g., the doctrinal formant is closely connected with verbalization), but others are not verbalized at all. We will call 'cryptotypes' these implicit models, the importance of which is immense. The man constantly practices rules that he is not fully aware of, or which, however, he would not be able to express well' [Italian in original text].

unwanted intromission in a subject's life, so it can be defined as a "negative right". On the other side, data protection is the legal control over access to and use of data (regardless the fact that those data qualify as personal data or not). Finally, personal data protection (generally referred to as "personal information protection" in China) is the fraction of data protection that regards personal data (and includes, for example, data security processes, the rules regarding data breaches and how to deal with them, and so on).

By simplifying we can imagine, therefore, a Venn Diagram where the two sets "Privacy" and "Data Protection" overlaps in the "Personal Data Protection" set.

These three concepts are often intertwined and intersecting, and sometimes are used as synonyms, especially when dealing with privacy laws and regulations where, according to the case, the concept of privacy or the concept of data protection is stretched in order to include the other. It is therefore important to understand what privacy, data protection, and personal information protection are in the vocabulary of E.U. and Chinese lawmakers.

In the E.U. we can clearly define two distinct set of "rights" pertaining respectively to privacy and personal data protection [9] that differ in formulation and scope.

While privacy can be identified with the right to respect for private life, the protection of personal data is viewed as 'a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed' [10].

Despite this, in the E.U. the term "data-protection" is a term that identifies personal data protection related laws and, sometimes, privacy related laws.

So, we have the 1995 Data Protection Directive and the General Data Protection Regulation in 2016, despite the fact that these legislations involve only personal data protection and privacy (interestingly enough, the term privacy is never mentioned in GDPR).

In China, we have a clearer distinction between the concepts referred, and in fact the General Rules of the Civil Law [11] discipline in two different articles the right of privacy (Article 110) and the protection of personal information (Article 111) [12]. Data protection is instead mentioned by Chinese lawmakers in the Cy-

[9] Source: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition Last accessed on September 2020.

[10] ibid.

[11] 中华人民共和国民法总则 (General Rules of the Civil Law of the People's Republic of China), adopted at the 5th Session of the 12th National People's Congress of the People's Republic of China on March 15, 2017 and effective since 1 October 2017.

[12] The Chinese Civil Code, which will come into force in January 2021, maintains the same distinction, defining privacy in Article 1032 and Personal Information in Article 1034.

bersecurity Law, a discipline aimed in fact to protect data regardless of their connection to a natural person.

Here we will examine both privacy and data protection concepts, as long as they are comprised in the recent legal developments examined. In particular, we will examine data privacy and data protection, on one side as developed in GDPR and on the other side as developed in the Guobiao GB/t 35273-2017.

2. Privacy and Personal Data Protection in E.U. Law.

The European Union issued in 2016 the General Data Protection Regulation (Reg. 679/2016), a comprehensive legislation on the personal data protection subject, one of a kind, seeking 'effective protection of personal data throughout the Union', via 'the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data'. [13]

This result has grown out a long and articulated journey that originates in initiatives of individual EU Member States [14] and in supranational actions, some of which dates back to the 1950s. We shall examine this evolution.

2.1. Evolution and Arrangement.

The first step that led to the current E.U. privacy legislation was the European Convention on Human Rights (ECHR) [15], signed in Rome on 4 November 1950, that states, in Article 8, as follows:

'(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

This formula bears, *in nuce,* the fundamental concepts of European privacy

[13] Recital 11 Reg. (EU) 679/2016.

[14] For example, the French Act No. 78-17 on Information Technology, Data Files and Civil Liberties adopted on 6 January 1978.

[15] All the Member States of the E.U. are also signatories of the ECHR.

law, where everyone should be granted the right to respect for his privacy, but this is not 'an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality' as is stated, today, by the Recital 4 of Reg. (EU) 679/2016.

After this principle was set, the European Court of Human Rights has given it a broad interpretation in its jurisprudence [16], thus laying the foundations for its codification.

Later on, in 1980, further efforts were made by the Organisation for Economic Co-operation and Development (OECD) [17] in order to create a comprehensive data protection system throughout Europe and the U.S., with the adoption of the 'Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data'.

The OECD Guidelines, however, were non-binding, and data protection laws still varied widely across Europe, with the U.S. and other OECD Member States that, while endorsing the principles within the recommendations, did not implement them in their laws.

In 1981 another institution parallel to the European Community intervened in the matter.

The Council of Europe [18] negotiated within its members the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention 108) [19]. This convention (still in force) obliges the signatories to enact legislation concerning the automatic processing of personal data, which many of the ratifying countries did.

The Convention 108 is really important also because it sets the boundaries between the privacy right and the personal data protection right(s). Later on, in fact, Advocate General Sharpston claimed, in a privacy related case before the Court of Justice of the European Union, that 'two separate rights are here invoked: "a classic right (protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No 108)." [20]

---

[16] See, e.g., *Klass and others v. Germany*, 6 September 1978, Series A no. 28; *Kruslin v. France*, 24 April 1990, Series A no. 176-A; *Huvig v. France*, 24 April 1990, Series A no. 176-B; *Niemietz v. Germany*, 16 December 1992, Series A no. 251-B.

[17] The OECD reunites 36 countries, among them there are most of the European countries, the U.S., Canada, Chile, Australia, and others.

[18] The Council of Europe is an international organization founded in 1949 that has 49 Member States (all the members of the European Union and several others, including Russia), it operates several international treaties, among which there is the European Convention on Human Rights.

[19] European Treaty Series (ETS) No. 108 – 1981.

[20] CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, par. 71.

Meanwhile some problems began to emerge, since many European countries had issued legislation in the privacy sector [21], but these laws differed in approach and procedures. This state of things could impede the free flow of data within the European Community. The European Commission decides, therefore, to step in to harmonize the various rules.

The outcome of these efforts was the Data Protection Directive (Council Directive 95/46/EC of 24 October 1995), that was the pivotal European law in the field until 2018. At the time, the European Commission deemed appropriate to issue a Directive [22] since the field was still unripe for a more active participation of the European Community and it was reasonable to let each E.U. Member State to deal with the privacy matter according to its own criteria.

Despite that, the Data Protection Directive contains many of the rules that still govern privacy and personal information protection in the E.U., the directive set the principles of consent, transparency, proportionality, and legitimate purpose for personal data processing. The same law stated the fundamental difference between a data transfer inside the European Union and outside that (transfer of personal data to third countries) and identified the role of supervisory authorities, that are now the cornerstone of data protection implementation and control.

Almost twenty years later, in 2012, the European Commission announced that it would try to unify data protection law across European Union via a proposed legislation called "General Data Protection Regulation" (GDPR).

After an articulated procedure, Regulation (EU) 679/2016 was adopted in 2016 and is applicable from 25 May 2018. This new law supersedes the 1995 Directive and is a significant step forward in the harmonization of privacy law across Europe. While the data protection law set by the European Parliament and Council in 1995, was a Directive, the 2016 law takes on the form of a Regulation, and the choice is all but casual.

In the E.U. hierarchy of laws [23], a Regulation is in fact a far more impactful

---

[21] The first law on data protection was adopted in the German state of Hesse in 1970. Later on, in 1973, Sweden become the world's first nation to enact a data protection law (Datalagen, 1973:289).

[22] A directive has not binding legal force throughout every EU Member State, these instruments lay down certain results that must be achieved by Member States, but each one is free to decide how to transpose directives into national laws. Regulations, on the contrary, have binding legal force throughout every Member State and enter into force on a set date in all the EU.

[23] Article 288 of the Treaty on the Functioning of the European Union states: 'To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions. A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods'.

set of rules, being directly applicable -as is- in every Member States of the European Union, while a Directive has not binding legal force throughout every EU Member State, merely requiring Member States to reach certain goals, leaving to each state the choice on how to do it and leaving, therefore, potential broad differences in the law from one state to another.

2.2. The Framework of Regulation (EU) 679/2016

On 25 January 2012, the European Commission announced its intention to revise the 1995 data protection directive, in order to update it in the light of technological progress and globalization. [24]

In view of the growing importance of data protection, and in order to guarantee the free movement of data inside the E.U., the aim of this new legislation was also the harmonization of 27 national data protection regulations into one unified Regulation.

Since its original proposal, the European Commission also made clear that the Regulation would apply for all non-E.U. companies active in the E.U. market and offer their services to E.U. citizens.

Later on, after four years of refinement, the General Data Protection Regulation (GDPR) was finally adopted. The GDPR entered into force on 27 April 2016, but has set a compliance date of 25 May 2018, giving E.U. Member States and businesses time to prepare for compliance.

The law is composed by 173 recitals and 99 articles. Recitals, mere interpretative tools of E.U. law, set many relevant principles in European privacy law, useful in order to comprehend how to actually apply its rules.

This preponderance of recitals over articles tells us a lot about the issues encountered by the European legislator in disciplining the complex phenomenon of data protection. Governing privacy with a single law for billion dollars corporations as well for micro-sized businesses, for hospitals and for little sports clubs, for small local authorities and for national ministers, is surely a hard task.

Therefore, European lawmakers resorted to a wide spectrum of quasi-binding principles to guide the application of the fewer rules that reached consensus, for example, an inspiring principle of the new law can be found in its Recital 4, which states that: 'The processing of personal data should be designed to serve mankind'.

Recital 6, instead, explain why it has proved necessary to draft an E.U. Reg-

[24] Source: https://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en Last accessed on September 2020.

ulation on privacy, saying that: 'Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities'.

Other relevant principles can be found in Recital 39, which is like a manifesto for data processing under the GDPR and begin by saying that 'any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed'.

As for the actual rules, the Regulation has its fulcrum in the discipline of the information and access to personal data (Articles 13 and 14 of the Regulation). The law provides a set of mandatory information that the data controller must provide to the data subject when the data are obtained. This information need to be simple and clear (especially when the subject is a minor) and has to explain thoroughly why the data are collected, by whom, how they will be used, how long they will be stored, which are the rights of the data subject and other information in accordance with the specific situation.

It is interesting to note that GDPR contains a broad definition of 'processing', that includes, according to Article 4(2) of the law:

'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

GDPR then makes a fundamental distinction between "common" personal data and "special categories" of personal data. The latter, disciplined in Article 9 of the Regulation, are data that can reveal 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership' and 'genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation'. These data can only be processed with particular cautions and with the consent of the data subject (or in some other limited circumstances).

As for "common" personal data, Article 6 of GDPR lists the legal basis for personal data processing as follow:

a) consent from the data subject;
a) performance of a contract;
b) compliance with a legal obligation to which the controller is subject;
d) protection of vital interests of the data subject or of another natural person;

e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) legitimate interests pursued by the controller or by a third party.

Among these, the last one mentioned is particularly interesting. Legitimate interest is described by the interpreters as a sort of "wild card" that justifies data processing (though in some limited cases) even if the data subject did not consent to the processing nor to a contract (the Article 29 Working Party [25] states, in its Opinion 06/2014 adopted on 09.04.2014 [26], that the legitimate interest could justify, for example, a re-offer from a producer with whom a data subject has already concluded a sale, or even a limited profiling activity on customers in order to perfect the search for what they have requested). This basis for processing is built on the interest pursued either by the controller or by a third party, therefore, the interest of the data subject does not come into play when dealing with legitimate interest.

The regulation then provides key figures of data controller (the one who processes the data), data processor (the one that, as in Article 28 of GDPR, carries out processing on behalf of a controller), and the brand-new figure of the Data Protection Officer.

This role has to be appointed only if the data controller is a public authority (except in the case of a court), if it performs regular and systematic monitoring of data subjects on a large scale, or if it processes special categories of data on a large scale.

When appointed, the Data Protection Officer (DPO) acts as a *trait d'union* between the business and the supervision authority, it has to be salaried by the business but is "designed for betrayal", as one of its role is to monitor compliance with GDPR by the data controller and to cooperate with the supervisory authority.

Other significant innovations brought by Reg. (EU) 679/2016 in the E.U. privacy and personal data protection framework, are a discipline for codes of conducts and certifications, a new set of rules for data transfers outside the E.U., a new advisory body composed by representatives of the supervisory authorities of each Member State and of the European Data Protection Supervisor, which is called the European Data Protection Board (EDPB) [27], and, eventually, incisive sanctions.

---

[25] Article 29 Working Party was an advisory body, constituted semi-spontaneously under the umbrella of Article 29 of the Data Protection Directive, and reunited a representative from each data protection authority across E.U.

[26] Source: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf Last accessed on September 2020.

[27] Disciplined in Article 68 of Reg. (EU) 679/2016, the EDPB supersedes Article 29 Working Party.

In this regard, Article 83 of Reg. E.U. 2016/679 provides two set of fines. The first one, for lesser violations, features administrative fines up to 10.000.000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The second one features administrative fines up to 20.000.000 EUR or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, again, whichever is higher.

One of the most frequent criticism made of the former Data Protection Directive was in fact the leniency of its sanctions, when dealing with giant multinational corporations; with the new set of sanctions provided by GDPR, anchored to the total worldwide turnover, this risk is fully averted.

2.3. The Dualism Between E.U. Law and Member State Law

With the GDPR, the European Union sought to overcome the limits of the Data Protection Directive, pushing further ahead the harmonization of E.U. states on personal data protection. Despite these efforts, there are many aspects of personal data protection law that are still preserve of individual Member States.

The first example is relative to criminal sanctions. Criminal Law is usually a sensitive area, where Member States sore tolerate meddling by E.U. authorities. Also, in the field of privacy the GDPR is content with its incisive administrative sanctions and does not provides for criminal penalties (as explicitly stated in Recital 149 and in Recital 152 of the Regulation).

A second example regards posthumous data protection. As stated in recital 27 of Reg. (EU) 679/2016, E.U. personal data protection law does not apply to the personal data of deceased persons. However, Member States may provide for rules regarding the processing of personal data of the departed.

Some Member States (for example Italy [28] and Estonia [29]) chose to grant protection to personal data even after the death of the data subject, thus reshaping privacy law and posing new complex questions (who can exercise the right of

[28] Italian *Codice in materia di protezione dei dati personali* (Code regarding the protection of personal data) D.Lgs. n. 196/2003, amended in 2018, states in Article 2 *terdecies* that privacy rights must be granted also to deceased persons, and may be exercised by family members for reasons deserving protection.

[29] Estonian Personal Data Protection Act (RT I, 04.01.2019, 11, available here: https://www.riigiteataja.ee/en/eli/523012019001/consolide last accessed on September 2020) was adopted in 2018 and states, in §9, that the successors of the deceased can object to the processing of his or her personal data for 10 years after the death (20 years if the deceased was a minor).

the dead and whether he or she gain access to all the information possessed by the deceased, even if he or she did not express prior consent to their exposition?).

Moreover, each Member State has adopted a more or less thorough legislation covering privacy, and these laws must cohabit with GDPR and respect its principles.

When dealing with E.U. privacy and personal data protection law, therefore, we should bear in mind that we are talking of a complex and ramified system, unified in its (vague) principles, harmonized in its (few) rules, and diverse detailed rules across the Union.

3. Privacy and Personal Data Protection in Chinese Law

The modern concept of privacy originated in the West [30]; China, exposed to it only in recent times, developed a new word to express the concept: *Yinsi* (隱私). [31]

Despite this, China has had a concept comparable with the one of western privacy through its history. Although Confucian philosophy highlights common and shared values, personal privacy has always been important in China and was guaranteed and even 'valuable in valuable in particular contexts'. [32]

In fact, the same Confucius, in his Analects, stigmatize 'improper' gossip or hearsay [33], and this lead some scholars to argue that the protection of privacy was firstly stated in China by the philosopher of the 6th century BC. [34]

---

[30] 'The conditions for the existence of modem privacy began to form after the Chinese "reform and open" movement in late 1979, with the reform of the economic system. The market changed the face of China.' in J. Cao, 'Protecting the Right to Privacy in China' (2005) 36 Victoria University of Wellington Law Review 647.

[31] 'It appears that the word yinsi is a recent neologism whose use has been heavily influenced by exposure to both Western legal scholarship and popular culture in the mid- to late- '80s (Zhu, 1997; McDougall, 2004)' in Kenneth Neil Farrall, 'Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.' (2008) 2 International Journal of Communication 993, 1030. 'The author believes that privacy was protected, to some extent, in ancient China and an awareness of privacy may be found in the Warring States Period, though neither the word "privacy" (yinsi) nor the modem concept of privacy existed.' in J Cao, 'Protecting the Right to Privacy in China' (2005) 36 Victoria University of Wellington Law Review 647.

[32] Kenneth Neil Farrall, 'Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.' (2008) 2 International Journal of Communication 993, 1030.

[33] Hao Wang, 'The Conceptual Basis of Privacy Standards in China and Its Implications for China's Privacy Law' (2012) 7:1 Frontiers of L in China 137.

[34] ibid.

Chinese contemporary law mentions privacy since in its first Constitution, adopted in 1940, that refers to privacy when affirming protection for correspondence (Article 90, then Article 40 of the new Constitution, adopted in 1982).

But for the development of a real data protection framework in China we have to wait until recent times, when some specific rules where adopted.

3.1. Evolution and Arrangement

The first appearance of a "right of privacy" in China dates to 2002, when a draft of the Chinese Civil Code was reviewed. In the draft, the right of privacy was bordered as follow:

(1) the subject of the right to privacy can only be a natural person;
(2) the objects of the right are private activities and personal information;
(3) the scope of the protection of the right is limited by public interest. [35]

While developing the Civil Code (a process that took eighteen years to be completed), China adopted also some jagged administrative standards, dealing with limited aspects of data protection (e.g.: 'Provisions on Protecting the Personal Information of Telecommunication and Internet Users', adopted by the Ministry of Industry and Information Technology on July, 16, 2013, 'Administrative Measures for Online Trading', adopted by the State Administration for Industry and Commerce on January, 6, 2014, and 'Administrative Rules for Short Messaging Services', adopted by the Ministry of Industry and Information Technology on May, 6, 2015, which regulates marketing activities via SMS).

Perhaps the most relevant administrative standards in the field is the 'Decision on Internet Information Protection' [36] by the Standing Committee of its National People's Congress, which was aimed at protecting "electronic information" and is composed by 12 Articles that contain rules relevant to personal data protection and privacy and that were later on transposed in the Cybersecurity Law.

In the meanwhile, the Supreme People's Court issued some significant judicial interpretations in the privacy field. The first dates back to 1988, when the SPC issued the 'Opinions of the Supreme People's Court on Several Issues con-

[35] Farrall (n. 32).

[36] 全国人民代表大会常务委员会关于加强网络信息保护的决定 (National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection), adopted on 28 December 2012 at the 30th Committee Meeting of the 11th National People's Congress Standing Committee.

cerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation)', where the Supreme Court tentatively extended the right to reputation to privacy matters. Then in 1993 the Supreme People's Court issued the 'Reply to Several Questions on Adjudicating the Cases of the Rights of Reputation' and in 2001 the 'Interpretation of the Supreme People's Court Regarding issues of Ascertaining the Liability of Compensation for Spiritual Damage for Tort'.

In 2014, the SPC then issued another significant judicial interpretation, regarding privacy on the web: 'Rules concerning Several Issues in the Adjudication of Civil Disputes over Infringement upon Personal Rights through Information Networks" where the Court deals with the definition of privacy in IT environment, including in its scope genetic information, medical records, criminal records, home addresses and personal activities.

Another relevant Judicial interpretation is the one issued in 2017 by the Supreme People's Court and Supreme People's Procuratorate, called: "Interpretation of Various Issues Concerning Application of Law in Handling Crimes of Infringing upon Citizen's Personal Information". Despite being issued in the criminal law field, the Interpretation clarifies the concept of personal information in China, stating that personal information means any kind of information that, individually or combined with other information, can identify a specific individual. This mean that even a single piece of information (e.g. an IP address, a mobile number, or a license plate) falls within the scope of personal information protection.

After that, the first comprehensive legislation that considered the data protection issue was the China Cybersecurity Law [37], issued on November 7, 2016 and went into effect on June 1, 2017, this law is the outcome of a broader approach to data protection than that adopted by E.U.

While in Europe there is a dedicated law to personal data protection, China favored a discipline aimed at data protection, whether those data are referred to individuals, businesses, etc.

Chapter IV of the Cybersecurity Law (Articles 40-50) deals with 'Network Information Security' and contains many provisions for data protection of citizens online.

The law establishes a right to confidentiality, that shall be respected by network operators (Art. 40) and by departments that deal with cybersecurity supervision (Art. 45), a right to erasure (when network operators have processed data in violation of law, set in Art. 43). Moreover, network operations shall not gath-

[37] GB/t 35273-2017 中华人民共和国网络安全法 (Cyber Security Law of the People's Republic of China) adopted at the 24th meeting of the Standing Committee of the 12th National People's Congress on November 7, 2016.

er user personal information, except when those are processed according to the principles of legality, propriety, and necessity.

Under the scope of the Cybersecurity Law, on April 19, 2019, China's Ministry of Public Security released a 'Guideline for Internet Personal Information Security Protection' (互联网个人信息安全保护指南).

Another pivotal step forward was made with the adoption of the General Rules of the Civil Law, at the 5th Session of the 12th National People's Congress of the People's Republic of China on March 15, 2017 (the law is effective since 1 October 2017).

Article 110 of the General Rules states that natural persons enjoy a list of rights, among which the right to privacy is included.

Then Article 111 of the General Rules stipulates that the personal information of natural persons is protected by law. Any organization or individual who needs to obtain personal information of others shall obtain and ensure the security of the information according to law, and shall not illegally collect, use, process, or transmit the personal information of others, and may not illegally buy, sell, or disclose the personal information of others. This rule constitutes a firm basis in law for the evolution that will take place in this field in China in a near future.

The General Rules will be abolished as soon as the Civil Code of the People's Republic of China (adopted during the 13th National People's Congress on May 28, 2020) will enter into force on January 1, 2021 [38].

The Civil Code includes an entire chapter dedicated to privacy and personal information protection (Chapter 6 of Part IV "Personality Rights", Articles 1032-1039), that further develops the principles contained in the General Rules.

This Civil Code takes up the borders of the 2002 draft and develops the concept in its consequences.

Chapter 6 of the Civil Code opens up with Articles 1032 and 1033, dedicated to the right of privacy. In these articles the law states that 'no organization or individual may infringe upon the privacy rights of others' and lists a series of activities prohibited (except when permitted by law or with the consent of the subject) that includes unwanted calls, text messages, instant messages, e-mails, photographs or films of private life and places, etc.

Article 1034 then defines personal information and states that it is protected by law.

The definition of personal information provided in the same article comprises electronically or otherwise recorded information that can identify a specific

[38] Civil Code of the People's Republic of China (中华人民共和国民法典), Enacting Organs: The 13th National People's Congress on May 28, 2020 in the Diaoyu Islands (at the third plenary session of the Third Session of the 13th National People's Congress), issued on May 28, 2020, effective from January 1, 2021.

natural person individually or in combination with other information (a broad definition that echoes the one contained in Article 4 n. 1) of Reg. EU 679/2016) and include the person's name, date of birth, identity card number, biometric information, address, telephone number, e-mail address, health information, whereabouts information, etc.

When processing personal information, Article 1035 states that the data controller shall follow the principles of lawfulness and necessity and shall be based on the consent of the natural person, unless otherwise provided. Article 1036 then enlists two examples of these provisions that let the processing to happen without consent, the first one is the case of the reasonable processing of information disclosed by the natural person or lawfully obtained, the second one is the case of the reasonable processing of information implemented in order to safeguard the public interest or the lawful rights and interests of the natural person.

It is interesting to note that Article 1037 of the Chinese Civil Code lays down in law the right of access of the data subject, the right to rectification and the right to erasure (that find their counterpart in Articles 15, 16 and 17 of Reg. (EU) 679/2016).

Article 1038 states that data controller shall not disclose or tamper with the personal information they collect or store and that they shall take technical and other necessary measures to ensure the security of the personal information they collect and store. Lastly, Article 1039 declares that even administrative bodies shall keep confidential the personal information of natural persons known in the course of performing their duties, and shall not disclose or illegally provide them to others.

The Civil Code, when it will enter into force in 2021, will surely push forward Chinese personal data protection framework, providing a set of definitions and binding rules that will guide the mandatory standard that will eventually follow the one (GB/t 35273-2017, merely recommended) examined in this article.

In pair with this development, we should expect a personal data protection law to be drafted within 2020 according to the update of the legislative agenda made by the Standing Committee of the National People's Congress of China in September 2018, promising a comprehensive data protection law the end of its term. [39]

[39] Yang Feng, 'The future of China's personal data protection law: challenges and prospects' (2019) 27:1 Asia Pacific Law Review 62-82.

3.2. The Impact of the 'Personal Information Security Specifications'

Another step forward for privacy and personal data protection in China is surely the GB/t 35273-2017 'Information Security Technology Personal Information Security Specification' [40].

This Standard is a Guobiao (literally: "National Standard"). Guobiao are provisions usually issued by the Standardization Administration of China (SAC), that can be distinguished by the letters accompanying the number and year identifying them, specifically, while the acronym "GB" (Guobiao) stands for a mandatory provision, the acronym "GB/t" identifies a recommended provision, where the "t" stands for tuījiàn,

The 'Information Security Technology Personal Information Security Specification' is therefore a recommended standard. Despite its being non-binding, it is particularly interesting for two reasons.

First of all, this Standard has many traits in common with the European GDPR, starting from the date of implementation, set on May 1, 2018, close to the date of applicability of the GDPR (May 25, 2018). [41]

Secondly, the particular layout of the legal framework in China, as seen in the method note, ensures more relevance to this standard, even if it lacks coercive force.

In China the political level, or political "formant" as Sacco would describe it [42], runs parallel to the legislative and administrative levels; the Party still has a significant impact on the decisions taken by other administrative bodies, even if its vision is not yet transposed into law [43]. This entails a situation where the rule of law is not the same as the one known in Western countries but is rather a means for clarity and predictability of the rules of the political leadership, preferable but not necessary. This is the reason why some scholars call the present situation in China 'rule by law' [44].

---

[40] 信息安全技术 个人信息安全规范 (Information security technology - Personal Information security specification) issued by the General Administration of Quality Supervision, Inspection and Quarantine of PRC and Standardization Administration of PRC on 29 December 2017 and implemented on 01 May 2018.

[41] These common traits should not be surprising if we consider that both these rules take their cue from the principles set by a supranational authority, the Organisation for Economic Co-operation and Development (OECD), in 1980.

[42] Sacco (n. 7).

[43] Yuanyuan Shen, ' Conceptions and receptions of Legality: Understanding the Complexity of Law Reform in Modern China' in K. Turner, J. Feinerman, R. Guy, (eds.), *The Limits of the Rule of Law in China* (University of Washington Press, 2000), 20-44; I Castellucci, *Rule of Law and Legal Complexity in the People's Republic of China* (Università degli Studi di Trento, 2012).

[44] I Castellucci, 'Rule of Law with Chinese Characteristics' (2007) 13 Annual Survey of International and Comparative Law 1, 35.

The political relevance of the Standard under consideration is recognized by many scholars [45] and evidenced by the fact that, on February 1, 2019, China's National Information Security Standardization Technical Committee has proposed a set of revisions to the national standard Personal Information Security Specification (ref. GB/t 35273–2017), released for public consultation.

The day after, the China Cyber Security Review Technology and Certification Center announced that some major companies, including Alipay and Tencent, obtained a privacy related certification based on the National Standard. [46]

The Standard sets the principle of explicit consent for the processing (Art. 3.6) referring to the need of "Affirmative Actions" (*kěndìng xìng dòngzuò,* 肯定性动作) in order to process data, as happens in GDPR (Recital 32).

Then the Chinese Standard provides a subdivision of personal data in 'common' data and 'sensitive' data. Sensitive data are defined, in Article 3.2, as data that, once leaked, can threaten personal and property security or easily cause personal reputational damage, physical and mental health damage, or discrimination. [47]

It is interesting to note that, contrary to what does the E.U. law, sensitive data are defined not by category, but by the negative effects of a potential data leak.

The Specification defines also anonymization and de-identification, saying that the anonymization is an irreversible process that does not consent to recover personal data, while de-identification is a process that allows to identify the data subject with the use of additional information (this concept is comparable with pseudonymization, as defined in GDPR).

The rule stipulates that information produced by anonymizing personal data does not qualify as personal data. As the Civil Code, also this Standard discipline the right of access, to rectification and to erasure (Art. 7.4, 7.5, 7.6 respectively). The right to erasure does not seem as developed as its European counterpart, since in the E.U. right of erasure is a genuine right to be forgotten, not pegged to any violation of law (requested for the deletion according to GB/t 35273-2017 Art. 7.6).

---

[45] Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?' (2020) 49:8 Penn St J L & Int Aff 74 (The role of non-binding rules).

[46] Source: https://equalocean.com/fintech/20190203-fintech-giants-acquire-crcc-certifications-on-private-information-security Last accessed on September 2020.

[47] The Standard also provides a list of examples of what could constitute a "sensitive" data: identity card numbers, biometric information, bank account numbers, communication records and contents, property information, credit information, location data, accommodation information, health and physiological information, transaction data, and any data regarding people of 14 years of age or under.

Another interesting definition, contained in the Standard, is the one regarding automatic decision making; when making decisions that significantly affect the subject matter of a personal data subject based solely on the automatic decision-making of the information system (e.g., determining personal credit and loan quota based on the user profiling, or using the user profiling for interview screening), the personal data controller shall provide a method of appeal to the personal data subject.

This rule is quite like the one adopted by E.U. lawmakers, but both the definitions face numerous criticalities, since it is quite uncommon that a decision on relevant matters could be solely machine-based. In most cases the software aims to facilitate the decision of a human being (who could be heavily influenced by the faith in the algorithm capacities), and therefore both Chinese and E.U. law cannot assist the citizen subject to an algorithm-assisted decision.

Further on, the Standard defines, in Article 8.2, the data processor, and requests the controller to supervise the processing of its delegate.

Another institution comparable with its European counterpart is the Security Incident Notification (disciplined in Article 9.2 of the Standard). As it happens under GDPR, the data controller shall promptly notify data subjects of the data breach (through email, letter, telephone, or push notification). If it is difficult to individually inform the data subjects, the controller should deliver a public warning (in an effective and appropriate manner).

In this case we can notice that the Chinese Standard lacks a supervision authority dedicated to privacy violations, that under Reg. (EU) 679/2016 shall be involved in case of data breach.

GB/t 35273–2017 requires also the appointment of an in-house responsible for data protection for businesses which meet certain requirements (at Article 10.1 b). Specifically, the organizations which main business involve the processing of personal data and have more than 200 employees, and the organizations that process data of more than 500.000 people (the revision raise this threshold to 1.000.000 people) or expect to do so within 12 months shall appoint a responsible for data protection. The responsible for data protection, though, is quite different from the data protection officer covered by GDPR.

The Chinese "responsible for data protection" has the task of coordinate and carry out data protection, to formulate, implement and update a privacy policy, to conduct privacy impact assessments, to enlist the data processing conducted by the business, to organize privacy training, to examine data protection related to new services or products, and to conduct security training. These tasks are the one that, in E.U. law, are assigned to the data controller, that surely can and should be helped by its privacy team in case of complex corporate structures. The data protection officer introduced in GDPR, instead, does not carry out these tasks, but solely oversees data protection in the organization that has ap-

pointed him/her and is a contact point between the business and the supervision authority.

The Standard then contains some surprisingly detailed dispositions, as the one that regulates the display of personal data on message boards, stating that data controllers should take measures in order to obtain the de-identification of data subjects (Article 7.2).

3.3. The recent amendment to the 'Personal Information Security Specifications'

The relevance of the standard examined is evidenced by the fact that soon after its release, on February 1, 2019, China's National Information Security Standardization Technical Committee proposed a set of revisions to the national standard Personal Information Security Specification (ref. GB/t 35273–2017), released for public consultation, eventually adopted on 06 March 2020 under the number GB/t 35273-2020 that will be effective from 01 October 2020[48].

As it often happens in China when a standard is decisively revised, the "amendment" replaces the previous standard, keeping the same number (i.e. 35273) followed by the year of adoption of the amendment (2020).

The modifies include a distinction in the concept of consent, with article 3.6 now split in two; on one side article 3.6 will discipline (from 01 October 2020) the "explicit consent" and on the other side the newly introduced article 3.7 will discipline the concept of "consent" (*recte* "implicit consent") a broader concept that includes negative actions such as not leaving the area (for example a website) after being informed of the data processing.

Also, the definitions of 'personal information' and 'personal sensitive information' are enriched by a note that specify that the definition include personal information "created" by the data controller through processing other information (whether personal or not); the note provides the example of an user profile image (Art. 3.1 and 3.2).

It is then introduced a ban on coercing users to agree to data collection by bundling services (Art. 5.3), and also a much welcomed compulsory "separation" of the consent, requiring different shows of assent for "basic business functions" (*jīběn yèwù gōngnéng* 基本业务功能) and "additional business functions" (*kuòzhǎn yèwù gōngnéng* 扩展业务功能), just like the E.U. law that requires

[48] GB/t 35273-2020 信息安全技术 个人信息安全规范 (Information security technology - Personal information security specification) issued by the General Administration of Quality Supervision, Inspection and Quarantine of PRC and Standardization Administration of PRC on 06 March 2020 and effective from 01 October 2020.

(Recital 32 and 43) 'separate consent to be given to different personal data processing operations' in order to attain a 'freely given' consent.

The revision also adds Appendix C.1, C.2, and C.3, regarding the definition and the distinction between "basic business functions" and "additional business functions".

The same revision adds Article 7.5 to the Standard, this Article sets the requirements for "personalized displays" (e.g. newsfeeds and search results personalized depending on the user identity), and it is stated that a clear mechanism of opt-out has to be made available for users. Moreover, personalized displays shall be clearly identified with the words "targeted push" (*dìng tuī* 定推) marked in a prominent way.

Then the renewed Article 7.6 will require that the convergence of personal information collected on different legal basis shall in any case respect the limits of processing set by the Standard.

Another significant innovation is brought about by the introduction of Article 9.7, that governs data access by third parties. The Article requires a security access mechanism between the controller and the third party (if deemed necessary) and the fact that the third party shall obtain the authorization to collect personal information from the data subject (this authorization to the access of a third party, in accordance with the relevant provisions of the Standard, can also be obtained in advance by the original data controller).

If data acquisition by a third party is embedded to an automation tool (such as codes, scripts, interfaces, algorithm models, software development kits, applets, etc.) the data controller shall carry out technical testing to ensure that the data collection comply with the agreed purpose and immediately disconnect them if the data collection exceeds the same purpose.

The revision then provides detailed provisions regarding biometric information and their processing. The renewed Article 6 includes various precautions to adopt when dealing with biometric information (*gèrén shēngwù shìbié xìnxī* 个人生物识别信息).

For one thing, Article 6.3 lett. c) states that biometric information should not be stored, but rather collected only instantaneously collected for authentication purposes and then discarded (e.g. with a dedicated collection terminal).

If the storage is essential for the processing purpose, Article 6.3 lett. b) requires separate storage for biometric information and personal identity information.

Article 9.2 lett. i) then states that personal biometric information may not be shared or transferred to third parties, unless the sharing or transfer is essential for the processing purpose.

As anticipated, the revision of Article 10.2 of the Standard also raises the threshold for the obligation to appoint a responsible for data protection.

The revision then introduces the so-called "Personal Information Security Project" (*gèrén xìnxī ānquán gōngchéng* 个人信息安全工程) that, much akin to the principle of "privacy by design" present in Reg. (EU) 679/2016 (Art. 25), states that data controllers should consider personal information protection requirements at the stage of system engineering, in order to ensure the protection of personal information during system construction.

Lastly, the revision introduces Article 11.3, where are disciplined the 'Records of personal information processing activities', much akin to the 'Records of processing activities' disciplined by Article 30 of Reg. (EU) 679/2016. The same article 10.2 of the revised Standard says that it is 'advisable' to adopt such records. As in the E.U. privacy framework, these records could be a useful instrument for mapping data processing and identify weak spots that need refining.

The revision is a positive step in the right direction, reinforcing the freedom of consent and advising organizations to keep records for data processing.

The only downsides in the revision that will come into force on 01 October 2020 are the introduction of the so-called "implicit consent" (that weakens the safeguards for the data subject) and the increase in the threshold for the appointment of a responsible for data protection (from the data processing of 500.000 people to 1.000.000 people)[49]; it is in fact difficult to believe that a corporation that processes data of more than 500.000 people is not in need of a subject dedicated to ensure the safety of that processing.

On the contrary it is to be welcomed the introduction of another threshold for the appointment of a responsible for data protection consisting in the processing personal sensitive information of more than 100,000 people (albeit, again, too high). [50]

3.4. Latest regulations

Other recent innovations in China bear witness to the increasing importance of privacy in the country.

Various Chinese authorities have in fact begun to take action in the field, in a script that has already been recited in other fields: when the central political level in China is ready for an innovation, before the finalisation of a law, many governmental agencies and local authorities begin to test its principles and effects. [51]

---

[49] Article 10.2 lett. C) (2) of GB/t 35273/2020.

[50] Article 10.2 lett. C) (3) of GB/t 35273/2020.

[51] A useful example can be found in the environmental field, as seen in: Mariagrazia Sempre-

The first example is a so called "privacy seal", announced on 15 March 2019 by the State Administration for Market Regulation and the Office of the Central Cyberspace Affairs Commission and called 'Mobile Internet Application (App) Security Certification Implementation Rules'. The China Cybersecurity Review Technology and Certification Centre will act as the certification authority. The certification is voluntary, but mobile app developers are encouraged to voluntarily obtain this certification, while search engines and app stores are encouraged to give more visibility to certified apps. [52]

On the same topic, on 8 August 2019, the National Information Security Standardization Technical Committee Secretariat issued a notice on the development of a draft of a Guobiao called: 'Basic specification on personal data collection by Mobile Internet Application (App)'. [53]

The standard recalls terms and definitions of GB/t 35273–2017 and comes with an appendix which lists the most common mobile internet application services (the list contains 21 services, such as map navigation app, instant messaging app, and so on) and the minimum information required to provide the service for each category.

Also, some recent court decisions are significant for present purpose, for example Tianjin Binhai New Area People's Court has issued on 20 March 2019 an injunction towards ByteDance (the owner of the renowned video app TikTok), ordering that it immediately stop providing the WeChat/QQ open platform authorised login to its recently launched app Duoshan (a short video-based messaging app), and that the same app must stop using WeChat/QQ user profile photos and nicknames in order to suggest new contacts. [54] The case is still on trial and the ruling will surely address the problem of balancing the interest of consumers to their data protection and to data portability, along with the interest of the two tech giants to hold back and to obtain personal data of their users.

Despite the injunction stems from a competition problem between two tech giants, it is interesting enough to note that this problem would have been avoided if those companies had adopted the Standard GB/t 35273–2017 that imposes, especially after the proposed revision, a complete control for the data subject of

---

bon, 'The Environmental Issue in China: Norms and Enforcement After Cop-21 Climate Summit in Paris' (2016) 3(1) Geoprogress Journal.

[52] Source: https://www.insideprivacy.com/international/china/china-introduces-mobile-application-security-certification-scheme/ Last accessed September 2020.

[53] Source: http://www.cac.gov.cn/2019-08/08/c_1124853418.htm (CN) Last accessed on September 2020.

[54] Source: https://www.tmtpost.com/nictation/3830482.html, https://www.theepochtimes.com/law-professor-sues-chinese-zoo-for-mandatory-face-scanning_3138101.html Last accessed on September 2020.

the data shared (willingly or not) with third parties.

Another very recent case is the one that involved a the Hangzhou Safari Park that switched from fingerprint authentication to facial identification for its visitors to access the park and was sued by one of its customers that was willing to access via fingerprint scanner but not to grant the park his facial identification data. The case was filed on October 28, 2019 and is still pending. [55]

The case has many interesting contact points with an Illinois litigation that was brought before Court in 2014, when an amusement park begun to use fingerprint authentication in place of tickets, leading to the Court ruling against the park and awarding punitive damages to the aggrieved party on January, 25, 2019 [56], despite the law effective in the State (Biometric Information Privacy Act, BIPA) being quite generic on the matter.

Before the Guobiao GB/t 35273/2017 and the Cybersecurity Law, there was a limited case law related to privacy and personal data protection in china, there were some significant criminal cases (among which the Qi Yuling v. Chen Xiaoqi case and the Wang Fei case [57]).

In the Qi Yuling v. Chen Xiaoqi case, Ms. Qi complained that that Ms. Chen stole her identity in order to obtain admission to University "on her behalf". The Supreme People's Court ruled in favor of Ms. Qi on the basis of infringement of her constitutional rights. About the Wang Fei case, we will further examine it in Chapter 3 (Comparison).

Apparently, criminal prosecution was the preferred way for Chinese citizens to protect their rights to their personal information. The Hangzhou Safari Park case is the sign of a recent turnaround. Another element that lately pushed Chinese plaintiffs to turn to the civil judge is the establishment of the so called "Internet Courts". The first Internet Court was set in Hangzhou [58] in 2017 after a stage of pilot establishment and has jurisdiction over the internet-involved civil and administrative cases. In addition to deal with internet-related cases, Inernet Courts benefits from a high-tech procedure (e.g. hearings through video-chat). After Huangzhou, similar courts were established in Beijing and in Guangzhou in 2018. It is clear that many privacy related cases, that nowadays often involve

---

[55] Source: https://www.bbc.com/news/world-asia-china-50324342, https://www.theepochtimes.com/law-professor-sues-chinese-zoo-for-mandatory-face-scanning_3138101.html Last accessed on September 2020.

[56] *Rosenbach v. Six Flags Entertainment Corp.* 123186 (Ill. 2019).

[57] Mentioned in the In-Depth Analysis "The data protection regime in China" by the European Parliament Directorate General For Internal Policies, that can be accessed at the following link: http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf Last accessed on November 2019.

[58] Hangzhou is home to many Chinese high-tech companies, distinctly Alibaba.

networks and technology, will be examined by these specialized courts.

Finally, perhaps the most significant element that shows the growing interest for privacy in China is the fact that a personal information protection law drafting has been included in this term's legislative plan [59] and the space devoted to privacy and personal information protection in the Civil Code recently approved.

In a note issued on the National People's Congress (NPC) website on 6 June 2019, a spokesman confirmed that drafting of personal information protection law has been included in the legislative plan for this term. Reacting to the worrisome issues of the so called "browser home page hijacking" and "mobile app hijacking" (widespread redirect viruses), the spokesman confirmed the illegal nature of these practices and ensured that the National People's Congress is going to intervene in the fragmented legal framework regarding privacy in China. The Standing Committee of the National People's Congress has, therefore, included the drafting of personal information protection law in the legislative plan of this term. [60]

Given the binding legal basis provided by the Civil Code and the seen mechanisms regulating Chinese legislation, it is to be expected that the Chinese personal data protection law will take extensive guidance from the standard examined in this article.

4. Comparison

When dealing with two legal system so different and rich in tradition as the European and the Chinese one, it is important to calibrate the meaning of the legal concepts that we are dealing with, declined over the two legal systems.

Doing this, we see that privacy, in China and in the West, are different concepts. The modern concept of privacy is born in the U.S. and transposed into law in the E.U., while is alien in Chinese culture. However, it does not mean that in China a concept of privacy "with Chinese characteristics" was present since ancient times. [61]

While European Culture values individualism and, therefore, the right to be left alone, Chinese culture traditionally valued social harmony (a Confucian concept recently recalled even by Xi Jinping in his rhetoric [62]).

In order to obtain social harmony, there is the need of a certain knowledge of

[59] Yang Feng (n. 39).

[60] Source: http://www.npc.gov.cn/npc/c199/201906/86e7ca82949844e29f0136b453781ad6.shtml (CN) Last accessed on September 2020.

[61] See Farrall (n. 32) and Wang (n. 33).

[62] E.g. in his report at the 19th CPC National Congress (10.18.2017).

personal data by the same society. This is not necessarily an intrusion in someone's life, but rather a different approach on privacy, where some fraction of oneself data must be exposed for greater good. The same mechanisms apply in E.U. law, as we have seen, where it relies on a balancing of interests in order to decide whether some personal data can be processed or not.

In China this mechanism is different in the way this balancing is set, but this does not mean that E.U.-like law cannot be applied in China, and this explain the reason behind the adoption of a standard (GB/t 35273–2017) so close to the European one.

Eventually, Chinese society will loose those social ties, pressured by economic growth, progressive urbanization, and rural to urban migrations, that put the Chinese social fabric to a severe stress and make communitarianism become less of a necessity and more of a choice. Therefore, privacy will probably take more and more its place in Chinese law, even if, again, "with Chinese characteristics".

Bearing this in mind, we can examine the differences between China and E.U. when dealing with privacy and data protection.

Also, in China privacy is a concept that is limited to the so-called "right to be left alone", whereas the term "personal information protection" subsume personal data protection related laws.

The lexicon of privacy is indeed complex also in Europe, where "privacy" is a term generally avoided by E.U. lawmakers, with the broader term "data protection" used to subsume personal data protection measures and sometimes privacy rules.

In Europe we have a comprehensive legislation, result of a complex and multiannual evolution, that had led privacy to be part of the everyday life of E.U. citizens, businesses and authorities. Although, this set of rules is difficult to implement in a legal framework as complex as the European one, making almost impossible to obtain the same level of adjustment across the Union.

In China we have a peculiar situation, where the law to this day is still fragmented and composed by few specific laws and standards introduced in sector rules. At the same time, there is already a Standard (although recommended) that sets a comprehensive privacy discipline, comparable to that adopted in the E.U.; moreover, at the political level have been taken numerous clear-cut measures that show the concern over the personal data protection issues.

In any case, it will probably take many years to come in order to instill a culture of privacy (from which personal data protection stems) in Chinese organizations and citizens, especially considering the spread of the so-called "human flesh search"[63] in the country, and some recent initiatives by the government

[63] Human Flesh Search (*Rénròu Sōusuǒ* 人肉搜索) defines the phenomenon of a distributed research of personal data (usually driven by social outrage) through Internet media.

(e.g. the so called "Skynet Project"[64], the so called "Social Credit System"[65] and the comprehensive "Smart City Program"[66]) that seem to encourage a data collection focused on quantity over quality, while, on the other hand, European Union requires that also public authorities minimize their data processing.

4.1. The concept of personal data in China and in the E.U.

We have seen that the concept of privacy, personal data/information and data protection varies in the perception of Chinese and European citizens and traditions. It is really interesting, then, to examine how this concept reverberate in each legislation.

Despite only implying it in its name, E.U. Data Protection legislation is actually aimed only at personal data protection. In fact, Article 2 of Reg. (EU) 679/2016 (headed: 'Material scope') states that: 'This Regulation applies to the processing of personal data'.

Article 4(1) of GDPR then states that "personal data" are 'any information relating to an identified or identifiable natural person'. Then the same Article provides a definition for "identifiable natural person", which is 'one who can be identified, directly or indirectly'.

In the Chinese standard (Article 3.1) there is a similar definition, where personal data include: 'all kinds of information, recorded by electronic or other means, that can be used, alone or combined with other information, to identify a specific natural person or to discover activities of a specific natural person.'

As we can see the definitions (and the material scope of the two rules) are quite superimposable, despite the E.U. one being unnecessarily complex (splitting the definition in two: "personal data" and "identifiable natural person").

Interestingly enough, the Chinese definition seems to extend personal data to data related to "activities" of a natural person. Despite this apparent extension, it is clear that these "activities" are no more than a mean to indirectly identify a

[64] Source: http://paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm (CN) Last accessed on September 2019, http://www.chinadaily.com.cn/a/201712/12/WS5a2fa4f7a3108bc8c6727f5c.html Last accessed on September 2020.

[65] See: C Yongxi, ASY Cheung, 'The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System' (2017) 12(2) The Journal of Comparative Law 356, 378; M Chorzempa, P Triolo, S Sacks, 'China's Social Credit System: A Mark of Progress or a Threat to Privacy?' (2018) Policy briefs.

[66] See: F Yang, J Xu, 'Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law' (2018) 5 Asia Pac Policy Stud. 533, 543; J Wagner Givens, D Lam, 'Smarter Cities or Bigger Brother? How the Race for Smart Cities Could Determine the Future of China, Democracy, and Privacy' (2020) 47 Fordham Urb. L.J. 829-882.

natural person and that only the possibility of a connection between the activity and the natural person qualify the data as personal data.

Given this, we can see that the starting point of both Chinese and E.U. personal data protection rules is quite the same, thus demonstrating that privacy and personal data protection are indeed universal concepts that varies in the details, but maintains a core meaning across the world.

4.2. The scope of application of GDPR and GB/t 35273–2017

According to E.U. Law (Article 2 of GDPR), the regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

This means that data protection is regulated by Reg. (EU) 679/2016 to a greater extent when the processing is automated, while its scope narrows down if the processing happens by "manual" means, involving only data which form part of a filing system (i.e. a categorized database of personal information).

The same Article 2 of GDPR lists some relevant exceptions to the application of its provisions:

a) activities which falls outside the scope of Union law;

b) activities carried out by the Member States regarding foreign and security policy;

c) activities carried out by a natural person in the course of a purely personal or household activity;

d) activities carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

These exclusions are quite relevant and diminish the protection for data subjects in a large series of hypothesis.

Despite the presence of other safeguard measures for the protection of the individuals privacy and confidentiality within E.U. Law, it is clearly compromising that all the comprehensive legislation set in Reg. (EU) 679/2016 cannot be invoked in these cases (e.g. when a person photographs another without his/her consent and spread the image on the web for purely personal reasons, it is difficult to argue that the subject photographed can refer the matter to the supervision authority set in GDPR or call for the application of GDPR fines).

In the Chinese standard the scope of application of the Guobiao is set in Ar-

ticle 1, which states that the standard applies to 'various entities' (*gèlèi zǔzhī* 各类组织), and the processing made when supervising, administering, and assessing the processing activities by supervisory authorities and third-party review organizations.

So, Article 1 clarifies that the scope of the Standard is limited to organizations (companies, firms, associations, and other businesses) and shall be followed also by the public sector and by reviewers when assessing the data processing activities. The rule seems then to self-limit itself to the private sector, stating that the public sector has to follow its rules only when supervising, assessing and administering the processing activities made by the 'various entities' subject to the Standard.

This Standard then is not intended to discipline the data processing made by the Chinese public sector, while the European Regulation is aimed also to Member States and their administrative bodies (except for some particularly sensitive areas, as seen above). It is, obviously enough, a difference that is connatural to the fact that the Chinese Guobiao is a recommended standard, and that the Chinese government will enact and follow its separate specific rules for processing personal data later on. [67] It is interesting to note, though, that this rule would not be capable to curb the phenomenon of human flesh search, [68] since it is not applicable to individuals.

As well, also E.U. law would be inadequate to reach that objective, since it is not applicable to individuals that act for personal means (it is, although, arguable that the collective effort aimed to search for personal data on the web would not fall under the definition of 'purely personal activity').

Other differences arise when examining the types of processing subject to the Standard, with its Article 1 that goes on to state that the Standard applies to the processing of personal data, giving then a non-exhaustive list of types of processing (collection, storage, use, sharing, transfer, and disclosure).

The standard then, seems to be applicable to more kinds of processing when compared to its European counterpart (that excludes manual processing not intended for a filing system).

Here, again, we see that the nature of recommended Standard does not require special care in setting its restrictions, since every voluntary adoption of the Standard is welcomed. The Standard only sets, in Article 1, its intended audience.

Despite the seen differences, it is clear that there are many common traits between the E.U. Regulation 679/2016 and Chinese Standard GB/t 35273-2017.

---

[67] The first rule to usher a liability for administrative bodies that misprocess personal data is contained in Article 1039 of the Civil Code of the PRC, that will come into force in January 2021.

[68] See n. 62.

Both the rules examined, in fact, provide a rather widespread concept of personal data, suitable to include the most relevant processing activities that could undermine personal data of citizens, i.e. the processing made by businesses, that crave for personal data for marketing purposes.

4.3. The information provided to the data subject in China and in the E.U.

Both the E.U. Regulation and the Chinese Standard set a list of information that a data controller shall provide to the data subject when processing his/her personal data. This list is particularly interesting since it details which information is essential, according to each law, in order to allow the data subject to exercise his/her rights.

The European regulation lists the information in Article 13, which states that when the data controller obtains data from a subject, it shall provide all the following information:

– the identity and the contact details of the controller;

– the contact details of the data protection officer, if any;
– the purposes of the processing and the legal basis for the processing;
– the legitimate interests pursued, when the processing is based on it;
– the recipients of the personal data, if any;
– if the controller intends to transfer personal data to a third country or international organization;
– the period for which the personal data will be stored or the criteria used to determine that period;
– the rights of the data subject;
– the rights to withdraw consent, when the processing is based on it;
– the right to lodge a complaint with a supervisory authority;
– if the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
– the existence of automated decision-making, if any, and meaningful information about the logic involved.

For its part, the Chinese standard GB/t 35273–2017 (Article 5.4) requires that controllers shall provide the following information prior to the collection of the personal data (if the collection is subject to the consent of the data subject or when there is an automatic data collection):

– the types of data collected, in relation with the different purposes of the product or service;

– the rules of collecting and using the personal data, among which are:
• purpose of collection and use;
• manner and frequency of collection;
• storage location;
• storage period;
• data security capabilities;
• information related to sharing, transferring, and public disclosure.

It is interesting to note that while the European Law provides that the controller shall give the information when it obtains the data (this rule, in one with the fact that GDPR does not apply to manual processing not intended for its inclusion in a file system, has made possible to argue that the "first contact" between controller and subject does not require immediate information of the latter about the data processing), the Chinese standard is stricter and requires that the controller provides the information prior to the collection of personal data, therefore leaving no room for "first contact" exemption from both consent and information.

Chinese Guobiao also states that, in addition to the seen information (that should be provided when the data are acquired), Chinese data controllers should provide a privacy policy and every data subject should be made aware of its contents (it appears that this policy could be provided to the subject also after the apprehension of personal data).

This privacy policy (Article 5.6 of the Standard [69]) shall include:

1. the basic information of the data controller (name and address, usual business location, contacts of the person in charge, etc.);

2. the purposes of the collection and use of personal data, as well as the different business functions covered by each purpose;

3. the types of personal data collected by each business function, the collection rules (scope, manner and frequency, storage location, storage time limit);

4. the purposes of sharing, transfer, and public disclosure of data, the types of third-party recipients, and the corresponding legal liabilities;

5. the basic principles followed for data security, the security capabilities, and the measures taken;

6. the data subject rights and mechanisms to use them, such as the method of inquiry, the method of correction, the method of deletion, the method of canceling the account, the method of withdrawing the consent, the method of obtaining a copy of the personal information, the method to restrain automated decision-making, etc.;

[69] Article 5.5 of the revised standard, with minor changes.

7. the potential security risks after the provision of the personal data, and the potential impact of not providing the same data;

8. the channels and mechanism for the data subject inquiry and complaints, as well as external dispute resolution agencies and contact methods.

The revision adds up another information to be included in the privacy policy, regarding the distinction between "core" and "additional" business functions, that we will further examine in the next chapter, and the necessity to highlight if the data processed are sensitive data.

As we have seen, the information that shall be provided by a Chinese entity when collecting data on the ground of consent or via automatic means, are quite similar to the one that shall be provided in any case according to Article 5.6 of the Standard.

Therefore, it is possible, for Chinese data controllers, to provide the same privacy policy whether when the processing is based on consent or made by automatic tools, or when the processing is based on other grounds.

The only substantial difference is that, in the case of a processing based the consent of the data subject or when there is an automatic data collection the Standard requests that the information is given prior to the data collection, while in the case of a processing based on other grounds, the Standard does not explicitly requires that the information is provided before the data collection.

Given this, we can note that many of the information listed by both E.U. and Chinese laws are quite superimposable. When collecting personal data of Chinese citizens in China, then, an E.U. company should then modify its privacy policy with a clear statement about the manner and frequency of the data collection (not requested in the same way by E.U. Law) and with an explanation of its data security capabilities, which E.U. Law states that the data controller shall not disclose with the data subject (except in the case of a data transfer outside E.U.) but shall keep available for authority inspection. An E.U. company should also, when collecting data on the ground of the consent of the data subject, consider that it needs to provide him/her the privacy policy before collecting the data.

When collecting personal data of E.U. citizens in Europe, when offering goods or services in E.U., or when monitoring the behavior of E.U. citizens in Europe, instead, a Chinese company should modify its privacy policy including the list of rights granted to the data subject and set out in Article 13 GDPR, including the right to lodge a complaint with a supervisory authority. Finally, it should acknowledge the existence of automated decision-making (e.g. profiling), and provide meaningful information about the logic involved in the automated decision-making, in order to let the subject understand how the automated mechanism works and could affect his/her data and his/her service.

Also, a Chinese company that collects data under the scope of GDPR, should

evaluate if it needs to appoint a data protection officer according to GDPR rules (and, in the case, give its contact details in the information provided to the data subject). Lastly, a Chinese company, when processing data under GDPR, could take advantage of the chance to process data based on its legitimate interest (giving, in the case, information to the data subject about the legitimate interest pursued).

4.4. The rights of the data subject in China and in the E.U.

As we have seen, both GDPR and the Guobiao requires that the privacy policy lists the rights of the data subject.

The rights enlisted in both laws are quite similar but with some meaningful differences.

As for the GDPR, the rights of the data subject are listed in Articles 15-22 as follows:

– the right of access, according to which the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data (Article 15);

– the right of rectification, according to which the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her (Article 16);

– the right to erasure ("right to be forgotten") according to which the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay (Article 17);

– the right to obtain from the controller restriction of processing (Article 18);

– the right to portability, according to which the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (Article 20);

– the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her (Article 21);

– the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (Article 22).

In the Chinese Guobiao, instead, these rights (listed in Article 7 [70]) are as follows:

– the right of access, according to which the data subject shall have the right to obtain from the controller access to personal data concerning him or to the categories of personal data concerning him, as long as to the origin and purpose of use of the data and the identity third parties which have obtained the same data (Article 7.4);

– the right of rectification, according to which when a data subject finds an error or something incomplete about their data held by a data controller, it should provide a way to modify data according to the request of the data subject (Article 7.5);

– the right of erasure, according to which a data controller should promptly delete data if it has violated laws or regulations in the collection or use of data or if it has violated an agreement with the data subject in the collection or use of data (Article 7.6);

– the right to withdraw consent, according to which the data subject should be provided with ways to withdraw authorized consent to collect and use their (Article 7.7);

– the right to cancel an account, according to which data controllers who provide services through registered accounts should provide means for data subjects to cancel their account in a simple and convenient way (Article 7.8);

– the right to obtain copy, according to which data controllers should provide data subjects a way to obtain copies of data regarding "individual basic information" and data regarding health, psychological, education and work information, or if technically feasible, directly transfer them to the third party chosen by the data subject (Article 7.9);

the right to file a complaint in case of automated decision making if it could have a significant impact on the data subject's rights and interests (Article 7.10).

Both the regulations open their lists with the right to access data, but the Chinese Standard does not require that the data controller displays every data it is processing, but only to the "categories" of personal data processed by the data controller.

As for the right to rectification the Chinese and the E.U. definition are quite superimposable, as well as the one regarding the right of appeal in the case of an automatic decision making that could have a significant impact on the data subject's rights and interests, as we have seen in Chapter 3.2.

Moving on to the right to be forgotten, it is quite different in the Chinese

[70] Article 8 in the revised Standard.

Guobiao compared to the one present in GDPR. Article 7.6 [71] of the Guobiao in fact provides that the right of erasure is tied to a violation of law by the data controller.

On the other side, Article 17 of the GDPR states that the right to be forgotten may be exercised also when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. This right has been developed after the E.U. Court of Justice has stated, in 2014, that in order to comply with the rights laid down in E.U. regulations the operator of a search engine is obliged: 'to remove from the list of results displayed following a search made on the basis of a person's name, links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful'. [72]

The right to be forgotten finds meaning precisely in this case, where the data processing is lawful, but data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

As for the right to obtain copy, present in the Chinese Standard, this right could be compared to the right to portability granted in GDPR but, while E.U. law states that the data controller shall provide the data subject with his or her data 'in a structured, commonly used and machine-readable format', Chinese law provides instead, more broadly, that the data controller shall transfer personal data directly to the third party chosen by the data subject 'if technically feasible'.

The data portability rule has been criticized in E.U. for its being generic about the formats and for being too difficult to implement. [73] Chinese rule, being more general, has a lesser impact, but on the other side avoids the risks caused by the strict and tricky to implement European rule.

As for the right to withdraw consent, GDPR includes it in Article 13 (that provides the aforementioned list of information that the data controller must provide to the data subject), while the Chinese standard lists it among the rights to be granted to the data subject, but the essence of the rule does not change. It is possible to withdraw consent at any time and both rules specify that the withdrawn of consent does not affect the lawfulness of processing based on consent before its withdrawal.

---

[71] As well Article 8.3 of the revised Standard.

[72] Judgment of 13 May 2014 *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 88.

[73] See: J Wong, T Henderson, 'How Portable is Portable? : Exercising the GDPR's Right to Data Portability' (2018) Pervasive and Ubiquitous Computing and Wearable Computers, 911–920.

Likewise, the right to cancel an account is similar in the E.U. an in China and is implicit in the E.U. right to erasure and in the right of restriction. This specific right is a definite sign of the Chinese interest to protect its citizens when they disseminate their own data online.

Lastly, the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, is present only in the GDPR and not in its Chinese counterpart. This right to object is directly addressed to processing made in the public interest and/or on the basis of legitimate interest.

The absence of the right to object in the Chinese Standard is therefore related from one side to the fact that the Standard is not directed to public bodies, and from the other side to the absence of a lawful processing based on the legitimate interest of the data controller or of a third party.

It will be, anyway, important to add this right when the Standard will discipline also personal data processing made by administrative authorities.

We have, therefore, a complete set of rights provided both in GDPR and in the Chinese Guobiao, that testify to the Chinese choice to tighten its privacy law according to the reference standard.

Only few differences remain, and some of them call for an implementation when China will sediment its privacy and data protection culture.

4.5. The concept of "consent" in China and in the E.U.

Bearing this in mind, we can examine the differences between China and E.U. when dealing with "consent" for the purposes of the law of personal data protection. In China the law does not require explicit and free consent in order to process personal data, but the recommended standard GB/t 35273–2017 prohibits data processing unless a free consent is given. According to the Standard (Article 3.6) the free consent shall be provided by an "affirmative action", which includes a voluntary statement (in electronic or paper form), also via checking a box, or clicking "agree," "sign up," "send," "dial," etc.

The proposed revision both strengthen and weakens this framework.

From one side the revision offers a much-welcomed distinction between "basic business functions" (*jīběn yèwù gōngnéng* 基本业务功能) and "additional business functions" (*kuòzhǎn yèwù gōngnéng* 扩展业务功能). The former is aimed to meet the desiderata of the consumer, in his perspective (e.g. the use of an email address to answer one's email inquiry), the latter is aimed to expand the data processing beyond the expectations of the data subject.

In the revision, Appendix C2, C3 and C4 help identify "basic business func-

tions" and "additional business functions". For example, the improvement of product or services, the enhancement of user experience or the development of new services shall not be classified as basic functions.

When processing data, a data controller should seek consent for the basic business functions and then obtain consent for each and every processing activity that falls under the scope of the "additional business functions".

Before the additional business function is used for the first time, the data controller should inform the data subjects through the interactive interface or design (e.g. via pop-up windows, filling boxes, etc.).

The revision, in this regard makes the Chinese Standard much closer to E.U. rules, which requests "granular" consent collection for the various purposes pursued by the data controller, giving the data subject the chance to freely select if he/she wants to give consent for each purpose presented.

Recital 32 of GDPR indeed states: 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided'.

Given this, the Chinese choice seems more rational since it breaks down the consent in the two macro-categories basic and advanced business functions, of which the first is what the data subject expects from the service and the second is whatever the data controller wants to "add up", thus consenting a more efficient way to deal with consent, avoiding unnecessary confusion between mandatory and optional consent.

The European choice, for its part, provides a more complex subdivision of consents, that does not keep into account what the consumer expects from the service provided.

From the other side the revision contained in GB/t 35273-2020 weakens the safeguards for Chinese data subjects with the introduction of the so-called "implicit consent" (in Article 3.7).

This "implicit consent" (shòuquán tóngyì 授权同意) as opposed to the "ex-

press consent" (míngshì tóngyì 明示同意) disciplined in Article 3.6 of the Standard, includes negative actions, such as not leaving a website after being informed of the data processing.

This distinction is surely a step back from the original discipline, intended to reserve for selected categories of data and processing an affirmative consent.

The renewed Guobiao calls for an express consent when the data processing concerns "additional business functions" or whenever it involves sensitive data, biometric information or data related to minors under the age of fourteen.

The affirmative consent is needed also when the identity of the data controller changes as a result of an acquisition, merger, bankruptcy, ecc. and the purpose of data processing varies as well (Article 9.3 lett. b) of the renewed Standard) and, lastly, when the data controller intends to publicly disclose the data.

When comparing E.U. law and Chinese Guobiao, then, another significant difference that arise is the one related to the absence, in the latter, of the legitimate interest. The legitimate interest of the data controller or a third party is not, therefore, a valid legal basis for data processing in China. This "jolly" has proved itself very useful in E.U. in order to loosen a bit the strict terms of the Regulation, letting the data controller to make a comparison between the interests at stake and deem worthy or not the intended processing. [74]

Since the Chinese Guobiao is as strict as the E.U. Regulation in terms of consent, and could be even stricter after its revision will enter into force, it would be probably a good idea to introduce such a "wild card" to use in order to legitimate processing in limited, deserving occasions.

Suffice it to say that in the E.U. the activity of Research and Development of a product sold to a customer could involve the same costumer on the ground of the legitimate interest of the producer to ask him/her to provide feedback on what he/she has purchased. In China, since this activity cannot be classified as a "core activity" of the contract, it could be carried out only with the prior consent of the data subject. [75]

However, disciplining an institute like the one of the legitimate interest, based upon a delicate balancing of interests, makes it absolutely necessary to explain in detail how this works and control that it won't be abused. The easiest way to do so is probably to appoint an independent authority, in charge for giving opinions, control and penalties. The lack of a supervisory authority dedicated to data protection is, therefore, probably one of the major issues of the

[74] I Kamara, P de Hert 'Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach' in E. Selinger, J. Polonetsky, O. Tene (eds.), *Cambridge handbook of consumer privacy* (Cambridge Univ Press 2018) 321-352.

[75] Obviously only if the data controller adheres to the GB/t 35273 Standard.

Standard, since the Cyberspace Administration of China (appointed by the Cybersecurity law as a reference authority) is competent only if the data processing is made using IT tools.

4.6. The Person in Charge of Network Security and the Data Protection Officer: similarities and differences

As we have seen, GB/t 35273–2017 requires the appointment of an in-house responsible for data protection for businesses which meet certain requirements. The responsible for data protection is quite different from the data protection officer covered under E.U. GDPR.

Let's start from the requirements that made the appointment compulsory.

According to the Chinese Standard, the organizations which main business involve the processing of personal data and have more than 200 employees have to appoint a responsible for data protection, as well as the organizations that process data of more than 500.000 people (the revision will raise this threshold to 1.000.000 people) or expect to do so within 12 months shall appoint a responsible for data protection.

E.U. Law requires the appointment of a data protection officer when the processing is carried out by a public authority or body, when the core activities of the controller consist of processing data with regular and systematic monitoring of data subjects on a large scale, and when the core activities of the controller consist of processing on a large scale of special categories of data. The threshold for appointment is similar in both the norms, in the E.U. law the concept of "large scale" (exemplified in many occasions by supervisory authorities [76]) plays a key role.

A partial remedy here will be provided when the revision of the Chinese standard will come into force, offering a new threshold for data controllers that process sensitive data (they will need to appoint a responsible for data protection if process sensitive data of more than 100.000 people). [77] Albeit being too high, this threshold is however comforting, since the absence of a distinction in

[76] E.g. some examples for the healthcare sector were provided by the Dutch Supervisory Authority (AP): https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg Last accessed on September 2020. Some useful directions on the "large scale" concept can also be found in the Guidelines on Data Protection Impact Assessment (DPIA) from the Article 29 Working Party (wp248rev.01), last amended on October 13, 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 Last accessed on September 2020.

[77] Article 10.2 lett. C) (3) of GB/t 35273/2020.

the threshold between "common" data processing and "sensitive" data processing was a serious gap in the Chinese discipline.

Moving to the tasks, the responsible for data protection has the task of coordinate and carry out data protection, to formulate, implement and update a privacy policy, to conduct data protection impact assessments, to enlist the data processing conducted by the business, to organize data protection training, to examine data protection related to new services or products, to conduct security training.

Here the differences with E.U. law are considerable. All the tasks of the responsible are tasks assigned to the data controller and its privacy team. The tasks of the data protection officer (listed in Article 39 of Reg. (EU) 679/2016) are the monitoring of the compliance with data protection law by the controller, to provide advice when requested and to cooperate and act as a contact point with the supervisory authority.

Again, the difference between Chinese and E.U. law arise from the lack of an independent authority to safeguard a healthy application of data protection rules. The same difference can be seen in the discipline of data breach, where to have an independent specialized authority as a "first responder" is surely an opportunity.

4.7. Personal data protection Law and Big Data

The abuse of big data [78] is one of the major concerns for data protection nowadays, as we have seen data protection legislation develops along with worrisome technological developments. Well, the current challenge to face is how to deal with these enormous amounts of data, that could be used in order to profile both large numbers of people or single individuals and could be shared with little if no effort at all.

Both E.U. and Chinese rules adopt a principle of data minimization, that if thoroughly applied could stern the risks connected with the abuse of big data.

E.U. Law provides, at Article 5, that the data processing shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')'.

The Guobiao, for its part, sets this principle in Article 5.2, where it is stated that businesses could process only data that have a direct relationship with the

[78] Big Data have been defined as "data that exceeds the processing capacity of conventional database systems." (Source: M Corrales, M Fenwick, N Forgó, 'Introduction' in M Corrales, M Fenwick, N Forgó (eds.) *New Technology, Big Data and the Law* (Springer Nature 2020) 3.

realization of business purposes. The Standard then is sure to specify that "direct relationship" means that without the personal data, the products or services sold could not be used. The Standard also requires the minimum possible frequency for automatic collection of data and in parallel the collection of only the minimum possible quantity of data.

Despite these rules, as we have seen, Chinese society is still prone to a "socialization" of data, since an intrusive breach in someone personal life is tolerated if it allows to obtain a greater good. In this regard, "human flesh search" is a meaningful phenomenon, eagerly developed in China, where collaborative effort by netizens is set to "hunt down" someone that deserves to be found and, maybe, "shamed". Here, Chinese netizens expect from one side large datasets of personal data readily accessible and from one other side impunity.

Until 2009 this perception was substantiated by the case-law. That year, the Wang Fei v. Zhang Leyi case [79] was decided, with the condemnation of the person that spread personal data of the victim, kicking off the human flesh search. The amount awarded to the victim was, however, very low. According to some commentators [80] the low amount awarded (later confirmed by the Court of Appeal) reflects the indulgence of the Court toward human flesh search behaviors.

Also, Chinese government, in order to attain the greater good of social stability and once sampled the great benefits that a widespread video surveillance system could provide to law enforcement authorities, endorsed an expansion and improvement of the same surveillance system.

In doing so, Chinese government inevitably collects a tremendous amount of data. Also, these data are elaborated with the help of artificial intelligences, thereby increasing even more the invasiveness of the surveillance. Pushing the project forward, many issues related to privacy concerns were raised. [81] Chinese government officials answered these objections highlighting the numerous measures adopted to the protection of personal data involved, and justified the widespread control balancing privacy concerns with personal safety concerns, considering the latter more worthy of protection.

---

[79] The case originated when a friend of the wife of Wang Fei (who had an affair) published the diary of the wife, who commit suicide after discovering the affair. Chinese netizens then exposed other personal data of Wang Fei and his lover, subjecting them to public shaming and verbal assaults.

[80] R Ong, 'Online vigilante justice Chinese style and privacy in China' (2012) 21(2) Information & Communications Technology Law 127-145; Dong Han, 'Search boundaries: human flesh search, privacy law, and internet regulation in China' (2018) 28(4) Asian Journal of Communication 434, 447.

[81] B Aho, R Duffield, 'Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China (2020) 49:2 Economy and Society.

The real Chinese policy regarding big data is therefore contained not in the GB/t Standard, but rather in the Social Credit System Project, in the Skynet Project and in the Smart City Project. [82]

While E.U. tries to curb personal data accumulation, China tries to centralize them in the hand of the Government, taking at a level previously unimaginable the so-called "surveillance capitalism" [83]. In this regard the fragile recommended Standard GB/t 5273–2017 pales in the face of the efforts made by the Chinese Government to trace the activities of its citizens.

Not even Article 1039 of China's Civil Code (which will enter into force in 2021) will be able to limit this activities, since when it disciplines data processing by administrative bodies it simply states that those shall keep confidential the personal information of natural persons known in the course of performing their duties, and shall not disclose or illegally provide them to others, but implicitly consent such activities of data gathering to be performed far over the limits set by the principle of data minimization.

What differs in E.U. and China is, as said, the balance of interests between social safety and national interests from one side and privacy and personal data protection from the other side. While China has chosen the former, E.U. has focused on the latter.

A question remains, which is the best balance of interest in the case?

While Europe sacrifice on the altar of data protection a perfect chance to empower its law enforcement, China takes full advantage of the possibilities offered by modern technology, at the price of total surveillance.

5. Conclusions

As we have seen a concept of privacy "with Chinese characteristics" was rooted in China for a long time. [84] This concept of privacy was willing to sacrifice to a certain extent the right to self-isolate in order to guarantee social harmony.

Nowadays, a piece of that concept still lives, shaping what privacy is in China and justifying a path that differs from the Western one on the subject. While the whole world sets toward a concept of privacy shared in its core tenets, it is clear that some secondary (but nevertheless not irrelevant) aspects of personal

[82] ibid.

[83] S Zuboff 'Big Other: Surveillance capitalism and the prospects of an information civilization' (2015) 30(1) Journal of Information Technology 75–89.

[84] See n. 32, 33.

data protection rules take different shapes according to the different jurisdictions examined.

Even with a Regulation and a Standard that look so much alike (and bear witness to this evolution based on a worldwide trend), in actual fact China and E.U. apply personal data protection in different ways.

The core principles of privacy and data protection (that extend throughout the whole world) can be seen in this comparison with the overlap of many dispositions from the E.U. legislation and the Chinese one. The focus on the consent of the data subject [85], the right to be informed, the safeguard measures for personal data security, and the same definition of personal data are appear, in fact, very similar when confronting the latest innovation in privacy law both in China and in the E.U.

This is thanks to the latest effort of the Chinese legislator, that has developed in a short period of time, a comprehensive legislation in the privacy field, in step with the well-established E.U. Law. Suffice to say that, in some respects, Chinese legislation seems stricter [86] (since it requests that privacy policies are provided to the data subject before the data collection) or better drafted (in its distinction between basic and advanced business functions) than its European counterpart.

The analysis highlights that the worries related to the technological sector are a major drive in the Chinese Standard (e.g. in the separate right to cancel an account, and in the various "notes" that exemplifies rules to fit in the informatic environment), while the economic drive plays a major role in the E.U. Regulation (marked by its impressive set of sanctions).

The long and stratified history of privacy and data protection measures in E.U. plays a role in its law, that fits in a society well aware of the values of personal data protection.

China, on the other side, has developed at an increasing pace in the privacy field, therefore its social fabric (and its government) is not fully prepared to adopt a standard as rigid as the E.U. one. For this reason, the Chinese government has put in place the Guobiao GB/t 35273–2017 as a practice run, in order to accustom its businesses to an increasingly strict ruling in the field.

The second step in this direction is the crystallization of the core principles of privacy and personal information protection in the Civil Code and the finalizing move will be the enactment of a personal data protection law by the end of 2022.

---

[85] Although watered-down in the revision that will be applicable from 01 October 2020.

[86] Albeit it is contained in a merely recommended standard. We should in fact remember that this same standard, by virtue of the peculiar temper of Chinese legal system, is less "optional" than it appears to be for many players. Also this same standard will be the basis for future binding legislation in the field.

5.1. Personal Data Protection Law as a tool to rule a global phenomenon

As we said, perhaps the most interesting result of this comparison is the highlight that China and E.U. have developed comparable rules and share a common approach on privacy and personal data protection.

As said, the most prominent endeavour of the Chinese legislator is related to the demands of the technological sector, a drive that is clearly demonstrated by the introduction of specialized courts to deal with tech related cases (i.e. Internet Courts).

Despite the seen differences, in fact, in a globalized world the IT field needs common rules, so then China has tried to implement a state-of-the-art personal data protection for technology users (both Chinese citizens and foreigners that use Chinese technology).

These efforts resulted in the Cybersecurity Law and in the Standard GB/t 35273-2017. This complex work surely paid off as to the form, with a set of rules that provides rigid terms and clear requirements for data processing.

As global phenomena, privacy and data protection need universal rules, because these are supposed to rule data, a volatile asset that can be managed everywhere in the world, regardless of the nationality of the data subject.

So it is a forward-looking choice for China to harmonize its laws to the reference standard (GDPR) in order to ease for its companies to adapt their policies, networks and security measures in order to process data of Chinese citizens as well as of people from the rest of the world.

This also means that privacy in China is no more a second-tier right and that the People's Republic will soon enough require compliance to strict standards from businesses that would like to process data of Chinese citizens.

But we should also consider that privacy and personal data protection will never be the same in China and in the E.U., given the value of the traditional formant in the People's Republic, that values privacy in a way that is quite different that in the West.

A clear demonstration of this difference lies in the phenomenon of the human flesh search [87], that is, still today, carried out with unparalleled extension in China than in other countries, that bears witness to the willingness of Chinese citizens to sacrifice a fraction of each citizen in order to obtain safety and, eventually, harmony.

Also, the fact that Chinese citizens often welcome a widespread dissemination of video surveillance cameras [88] explains much about the different approach toward privacy in China compared with E.U.

---

[87] See n. 62.

[88] See: H Zhang, J Guo, C Deng, Y Fan, F Gu, 'Can Video Surveillance Systems Promote the

The Chinese government seems then to grant privacy to its citizens only when dealing with companies, but not when dealing with the government itself.

So, the question that arise is why Chinese government adopted a Standard so similar to its European counterpart. The answer is probably that both GDPR and GB/t 35273–2017 are tools, that can vary in their effectiveness depending on the values prioritised in the country examined, and on the consequent balancing of interest between privacy and other values.

For example Article 5.4 of the Chinese Standard [89] sets that a data controller does not need to obtain consent from the data subject for the processing of data under a series of situations (e.g. when data are directly related to public safety, public health, or significant public interests, criminal investigation, prosecution, trial, judgment enforcement, or when the data processing is aimed to safeguard major lawful rights and interests).

On the same page the GDPR states (in Article 6), that a data controller does not need to obtain consent from the data subject for the processing of data under a comparable set of situations (e.g. when the data processing is made in compliance with a legal obligation, when processing is necessary in order to protect the vital interests of the data subject or of another natural person, when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and, lastly, when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party).

Therefore, both rules can perfectly fit to various different countries and legal traditions and can vary along with the spirit of the time. The law is the same, the difference is in the interests balancing.

5.2. The challenges on the horizon

This does not mean that China has already overcame every difficulty.

What still lacks in China is, obviously and first of all, a binding rule to take over for the recommended standard GB/t 35273/2017 (the soft power of politics in China that can make substantially binding an optional standard, if endorsed at the political level is surely not enough on the long run) and an independent supervisory authority, that could take the lead in set in the relevant context the rules of the Standard. Chinese laws are still fragmented and focused on various

Perception of Safety? Evidence from Surveys on Residents in Beijing, China' (2019) 11(6) Sustainability MDPI 1,21.

[89] Article 5.6 of the of the revised Standard GB/t 35273/2020.

different aspects of privacy and personal data protection, this led to the creation of various authorities (e.g. the Cyberspace Administration of China, which is the authority supervising the application of the Cybersecurity Law, but cannot be involved when a data breach happens "offline").

It will be important also to revise the right to be forgotten, which is now tied to a violation of law by the data controller according to Article 7.6 of the Chinese Standard, while the E.U. rule states (Article 17) that the right to erasure may be invoked simply when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

Another thing that should be implemented as soon as possible is a set of sanctions to measure for tech giants. In practice, the most significant innovation introduced with the GDPR in Europe is the renewed set of sanctions, more proportional but able to frighten multinational corporations, this still lacks in China.

It will be important also that China will implement privacy with the same pace and rules both for private businesses and for State administrations, because the fact that the Standard 35273–2017 (merely recommended) appears applicable only to private enterprises legitimate us to expect that even when it will be transferred in a binding standard it will set aside public administrations, and this could be very problematic.

Again, we are dealing with a tool, that can be more or less effective according to the balancing of interests adopted, this fact suggests to choose at least a formal implementation of personal data protection for every data controller, thus granting a common framework and guarantees to every data subject, without standing in the way when more important right to safeguard are at stake (but hoping that, over time, it could adapt to a situation where privacy and personal data protection are more relevant in the citizen-government relationship in China).

Even if Chinese government will impose compliance with GB/t 35273-2017 to its public bodies, they would still be able to protect the safety of the country and of Chinese citizens, processing data via one of the seen exceptions provided in Article 5.4 of the Guobiao (e.g. Art. 5.4 letter b), that consent data processing without consent if the data are 'directly related to public safety, public health, and significant public interests', or letter c), that consent data processing without consent if the data are 'directly related to criminal investigation, prosecution, trial, and judgment enforcement, etc.' or even letter d), that consent data processing 'when safeguarding major lawful rights and interests').

The other differences that arose in the comparison refer to mere choice of details, that do not undermine the framework of Chinese personal information protection law.

As said the next step, for China, is therefore to make GB/t 35273–2017

mandatory in order to instil greater awareness of the privacy issue to its companies, its authorities and its citizens. Doing so, China could help to shape a global personal data protection law, since every country can agree on some common principles in this field, leaving to each individual nation the choice of balancing between privacy and other core values of its society.

In this regard, the revision of the Standard, recently adopted (on 06 March 2020) has dampened enthusiasm to some extent with its entry into force set far away in October 2020 and with its step down on consent (caused by the introduction of the so-called "implicit consent") despite bringing up some positive news and trims to the Standard.

Again, the real bone of contention could be the field of big data where, as we have seen, the interest of the Government, as well of the private sector, and as well of the citizens goes in the direction of an increased tolerance in order to process these personal data to pursue other relevant values. Both in China and in the E.U. this push leads to a balancing of interests, that today tends more toward social justice or social harmony in China compared to what happens in Europe.

This does not mean that it is impossible to implement a full-fledged culture of privacy, where citizens and businesses value data protection, in China, despite the fact that the society still tolerates an impairment of privacy in order to attain social justice or social harmony.

If this "impairment" is justified with a reasonable balancing of interests and presided by strong security measures granting a safe and controlled data processing, then it could become a central pillar of a Chinese privacy culture.

As always when it comes to China, there is no wrong or right, only time will tell whether it's better to live without social interference, but feeling less safe, or to feel safer, but with overseeing.

FROM INFORMATION PRIVACY TO EMERGENCY PRIVACY

Valeria Manzo

Lawyer in Naples and Ph.D. (c) at Università della Campania Luigi Vanvitelli

Marco Bergamo

Lawyer in Naples

Abstract:

If before the creation and dissemination of computers made it possible to collect, organise and transmit an indistinct series of personal information, the right to privacy was linked to the concept of private property and the means for its protection and then, in a social dimension, came to coincide with the individual's ability to control the circulation of information relating to him – a power that often is essential to maintaining social relationship and personal freedom, With the development of technologies and the use of personal data processing, as well as the possibility of their exchange and aggregation through the Internet and the creation of databases, the needs have evolved (and are evolving) even more significantly towards a collective dimension of information privacy.

The innate mutability of the concept of privacy as a concept which is strongly affected by social, cultural and technological changes, pushes, in this way, to prepare a cautious legal schematization of the institution also in light of the emergency situation generated by the diffusion of the COVID-19.

It is necessary, therefore, to ask whether the existing legislation can be considered sufficiently malleable to the changed framework of protection of personal data or whether the solutions adopted can be considered legitimate and proportionally oriented to respect the new "emergency privacy".

Key-words: privacy, GDPR, contact tracing, COVID-19, Immuni app, data breach.

Summary: 1. The regulatory framework and compression of rights. – 2. The contact tracing and Immuni app. – 3. The data breach. – 4. Conclusions.

1. The regulatory framework and compression of rights

In our legal system [1], the protection of personal data is, today, entrusted to Legislative Decree no. 101 of 10 August 2018, concerning "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

As can be seen from a simple reading of the first reference standards, the above mentioned regulatory patchwork shows that there have been no formal amendments to Legislative Decree no. 196 of 30 June 2003 [2], which are based on a different and more modern approach to the protection of personal data, which is based on the tightening of penalties (including criminal penalties) that already characterized the beginning of the entire legislative system.

In the face of the epidemiological emergency from COVID-19, a series of regulatory acts have followed one another, the most important of which include personal data protection.

On 9 March 2020, the Government adopted Decree Law no. 14/2020, containing "*Disposizioni urgenti per il potenziamento del Sevizio sanitario nazionale in relazione all'emergenza COVID-19*", which came into force the following 10 March – with which, resuming the provisions of the Ordinance of the Head of the Department of Civil Protection (hereinafter O.C.D.P.C.) no. 630 of 3 February 2020, special provisions were dictated on the processing of personal data in the current pandemic context.

With the above mentioned O.C.D.P.C. it has been possible to carry out the processing of personal, particular and also judicial data necessary for the performance of the Civil Protection function, connected to the onset of pathologies deriving from transmissible viral agents, allowing, where necessary, a flow of data exchange between the subjects identified by the Legislative Decree of 2

[1] In relation to the right to privacy the following authors should be noted, among many: SD Warren-LD Brandeis, 'The Right to Privacy' (1890) IV Harvard Law Review 289-320; V Frosini, *Teoria e tecnica dei diritti umani: i diritti umani nella società tecnologica* (3rd edn, Edizioni Scientifiche Italiane 1998); A Giddens, *Il mondo che cambia: come la globalizzazione ridisegna la nostra vita*, (1st edn, Il Mulino 2000); S Rodotà, '*Diritto, diritti, globalizzazione'* (2000) I, *Riv. Giur. Lav*., 766; N Irti, '*Le categorie giuridiche della globalizzazione'* (2002) XLVIII n. 5 *Riv. di dir. Civile 625-635;* TM Ubertazzi, *Diritto alla privacy, natura e funzioni giuridiche* (1st edn, Cedam 2005); F Galgano, *La globalizzazione nello specchio del diritto* (1nd edn, Il Mulino 2005); A Bevere-A Cerri, *Il diritto di informazione e i diritti della persona. Il conflitto della libertà di pensiero con l'onore, la riservatezza, l'identità personale* (2nd edn, Giuffrè 2006).

[2] Bearing "*Codice in materia di protezione dei dati personali*".

January 2018, n. 1 (better known as the Civil Protection Code) in articles 4 [3] and 13 [4].

[3] **Componenti del Servizio nazionale della protezione civile: "***1. Lo Stato, le Regioni e le Province autonome di Trento e di Bolzano e gli enti locali sono componenti del Servizio nazionale e provvedono all'attuazione delle attività di cui all'articolo 2, secondo i rispettivi ordinamenti e competenze.*

2. Le componenti del Servizio nazionale possono stipulare convenzioni con le strutture operative e i soggetti concorrenti di cui all'articolo 13, comma 2 o con altri soggetti pubblici.

3. Le componenti del Servizio nazionale che detengono o gestiscono informazioni utili per le finalità del presente decreto, sono tenute ad assicurarne la circolazione e diffusione nell'ambito del Servizio stesso, nel rispetto delle vigenti disposizioni in materia di trasparenza e di protezione dei dati personali, ove non coperte di segreto di Stato, ovvero non attinenti all'ordine e alla sicurezza pubblica nonché alla prevenzione e repressione di reati".

[4] **Strutture operative del Servizio nazionale della protezione civile**: "*1. Oltre al Corpo nazionale dei vigili del fuoco, che opera quale componente fondamentale del Servizio nazionale della protezione civile, sono strutture operative nazionali:*

a) le Forze armate;

b) le Forze di polizia;

c) gli enti e istituti di ricerca di rilievo nazionale con finalità di protezione civile, anche organizzati come centri di competenza, l'Istituto nazionale di geofisica e vulcanologia e il Consiglio nazionale delle ricerche;

d) le strutture del Servizio sanitario nazionale;

e) il volontariato organizzato di protezione civile iscritto nell'elenco nazionale del volontariato di protezione civile, l'Associazione della Croce rossa italiana e il Corpo nazionale del soccorso alpino e speleologico;

f) il Sistema nazionale per la protezione dell'ambiente;

g) le strutture preposte alla gestione dei servizi meteorologici a livello nazionale.

2. Concorrono, altresì, alle attività di protezione civile gli ordini e i collegi professionali e i rispettivi Consigli nazionali, anche mediante forme associative o di collaborazione o di cooperazione appositamente definite tra i rispettivi Consigli nazionali nell'ambito di aree omogenee, e gli enti, gli istituti e le agenzie nazionali che svolgono funzioni in materia di protezione civile e aziende, società e altre organizzazioni pubbliche o private che svolgono funzioni utili per le finalità di protezione civile.

3. Le Regioni, relativamente ai rispettivi ambiti territoriali, e nei limiti delle competenze loro attribuite, possono individuare proprie strutture operative regionali del Servizio nazionale, in ambiti operativi diversi da quelli di riferimento delle strutture di cui al comma 1.

4. Le strutture operative nazionali e regionali svolgono, nell'ambito delle rispettive competenze istituzionali, salvo quanto previsto dal comma 5, le attività previste dal presente decreto. Con le direttive di cui all'articolo 15, si provvede a disciplinare specifiche forme di partecipazione, integrazione e collaborazione delle strutture operative nel Servizio nazionale della protezione civile.

5. Le modalità e le procedure relative al concorso delle Forze armate alle attività previste dal presente decreto sono disciplinate, secondo quanto previsto in materia dagli articoli 15, 89, comma 3, 92 e 549-bis del decreto legislativo 15 marzo 2010, n. 66, con decreto del Presidente del Consiglio dei ministri, sulla proposta del Capo del Dipartimento della protezione civile, di concerto con il Ministro della difesa, adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400".

With art. 14 of the D.L. [5], referring to the principles enshrined in art. 5 of EU Regulation/2016/679 on data protection (so-called GDPR) of lawfulness, correctness and transparency, minimization, accuracy, limitation of storage, integrity and confidentiality, the following additional corollaries are crystallized with

[5] Disposizioni sul trattamento dei dati personali nel contesto emergenziale: "*1. Fino al termine dello stato di emergenza, deliberato dal Consiglio dei ministri in data 31 gennaio 2020, per motivi d'interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del COVID-19 mediante adeguate misure di profilassi, nonché per assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale, nel rispetto dell'articolo 9, paragrafo 2, lettere g), h) e i), e dell'articolo 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, nonché dell'articolo 2-sexies, comma 2, lettere t) e u), del Decreto Legislativo 30 giugno 2003, n. 196, i soggetti operanti nel Servizio nazionale di protezione civile dell'articolo 9, paragrafo 2, lettere g), h) e i), e dell'articolo 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, nonché dell'articolo 2-sexies, comma 2, lettere t) e u), del decreto legislativo 30 giugno 2003, n. 196, i soggetti operanti nel Servizio nazionale di protezione civile, e i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile 3 febbraio 2020, n. 630, nonché gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 3 del decreto-legge 23 febbraio 2020, n. 6, convertito, con modificazioni, dalla legge 5 marzo 2020, n. 13, anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19.*

2. La comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli di cui al comma 1, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del regolamento (UE) 2016/679, è effettuata, nei casi in cui risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto.

3. I trattamenti di dati personali di cui ai commi 1 e 2 sono effettuati nel rispetto dei principi di cui all'articolo 5 del citato regolamento (UE) 2016/679, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

4. Avuto riguardo alla necessità di contemperare le esigenze di gestione dell'emergenza sanitaria in atto con quella afferente alla salvaguardia della riservatezza degli interessati, i soggetti di cui al comma 1 possono conferire le autorizzazioni di cui all'articolo

2-quaterdecies del decreto legislativo 30 giugno 2003, n. 196, con modalità semplificate, anche oralmente.

5. Nel contesto emergenziale in atto, ai sensi dell'articolo 23, paragrafo 1, lettera e), del menzionato regolamento (UE) 2016/679, fermo restando quanto disposto dall'articolo 82 del decreto legislativo 30 giugno 2003, n. 196, i soggetti di cui al comma 1 possono omettere l'informativa di cui all'articolo 13 del medesimo regolamento o fornire una informativa semplificata, previa comunicazione orale agli interessati della limitazione.

6. Al termine dello stato di emergenza di cui alla delibera del Consiglio dei ministri del 31 gennaio 2020, i soggetti di cui al comma 1 adottano misure idonee a ricondurre i trattamenti di dati personali effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali".

regard to data interchange flow, limiting the scope of application of these rules having regard to the state of health emergency determined by the deployment of COVID-19:

– indispensability (data may be collected only for the purpose of carrying out activities related to the management of the health emergency in progress);
– reconciliation (understood as a balance between fundamental interests such as the need to manage the current epidemiological emergency with the right to protection and confidentiality of the data of the individuals concerned);
– temporariness (the data may be kept for a limited period of time, to be recognized with the cessation of the state of emergency or in the 60 days following the collection).

In view of the above, it is necessary to analyze to what extent it can be considered possible to compress the rights constitutionally protected by reason of the achievement of a superior good, such as public health.

The balance between the protection of the fundamental rights of the individual and the pursuit of collective needs is inherent to the very nature of human rights, which constantly conflict with each other and with general interests [6].

If it is true that the Government has directed its course of action towards the repression of the spread of the virus, this has been achieved through the enactment of measures that have had a profound impact on the individual sphere of human action by compressing rights such as those enshrined in Articles 13, 16, 17, 19 and 24 of the Constitutional Charter.

Let us analyze them individually.

The main *vulnus* of governmental measures has been constituted by the compression of personal freedom (constitutionally guaranteed by art. 13) as "irrepressible prerogative of the person" [7] with the consequence that, in order to trace the legitimacy or otherwise of the interventions of the Central Government, it is necessary to identify the way to understand the reservation of the law.

If, in fact, it is inclined to the relative character of the reservation of law in question, the same must be considered legitimate; illegitimate, if the reservation is intended as absolute.

The relationship between security and freedom has, thus, revealed how, in a balance between the right to freedom of movement and limits to the exercise of the same, it should be reviewed also in the light of the general criterion of "rea-

[6] M. Cartabia, '*I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana'. Atti del seminario svoltosi in Roma*, Palazzo della Consulta, 13-14 ottobre 1994.

[7] F.M. Stornelli, 'La graduale limitazione dei diritti e delle libertà fondamentali nella stagione del coronavirus' (2020), on https://www.iusinitinere.it/la-graduale-limitazione-dei-diritti-e-delle-liberta-fondamentali-nella-stagione-del-coronavirus-26470.

sonableness" understood as the right relationship of the act to the purpose [8].

The current epidemiological emergency has also led the Government to adopt some measures restricting freedom of movement and residence (protected by Article 16 of the Constitution).

The most important measure, from a general and abstract point of view, is Decree Law no. 6 of 2020, which includes a list of the measures that can be adopted in order to contain the spread of contagion, including Article 1, paragraph 2, letter. a) which provides for the "prohibition of removal from the municipality or area concerned", the following letter b) which provides for the "prohibition of access to the municipality or area concerned" and, lastly, letter m) which provides for the possible "limitation of access or suspension of the services of transport of goods and people on land, air, rail, sea and inland waters, on national network, as well as local public transport, even non-scheduled, unless specific exceptions provided by the measures referred to in Article 3", has given rise to many repercussions on the full enjoyment of freedom of movement.

Indirectly, the freedom of assembly (constitutionally guaranteed by article 17) has also been compressed by article 1, paragraph 2, letter c) of the D.L. in question with the introduction of the prohibition to create assemblies, suspending demonstrations or initiatives of any kind.

The same is true with regard to the limitation of freedom of worship (recognized by art. 19 of the Constitutional Charter) compressed by the same D.L. since the competent Authorities have been authorized to adopt measures aimed at suspending any manifestation or event of a religious nature.

Finally, the generalized postponement of hearings and the suspension of deadlines until April 15, 2020 and the provision of specific rules relating to the different types of trial with all the repercussions that have resulted, has produced direct effects on the right to take legal action for the protection of their rights and interests, as well as the right of defense (protected by Article 24 of the Constitution).

Well, from the analysis of what has been highlighted so far, it must be asked: where is the legal basis for the power of the State to limit the rights of individuals in order to pursue an aim of general interest?

If it is true that our Constitution does not contain any provision on the "state of emergency" [9], it is also true that, in our country, this state of emergency connected with natural calamitous events of natural origin that, due to their intensi-

[8] A. Candido, 'Poteri normativi del Governo e libertà di circolazione al tempo del COVID-19' *(2020) 1/2020, Forum di Quaderni Costituzionali,* 419 e ss.

[9] C. Blengino, 'Emergenze e diritti costituzionali' (2020) on *https://www.ilpost.it/carlo blengino/2020/03/19/emergenze-e-diritti-fondamentali/.*

ty/extent, must be faced with extraordinary means and powers, was declared on 31 January 2020 by a resolution of the Council of Ministers pursuant to the first paragraph of Article 24 of the Civil Protection Code.

In the absence of indications both in national legislation and in the Constitutional Charter, reference must be made to the relevant norms of international law and, in particular, to the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (ratified in Italy by Law no. 848 of 4 August 1955) [10].

Many provisions of the Convention in question provide for so-called "limitation clauses" with the possibility of limiting the rights guaranteed in them when this is necessary for the pursuit of objectives of general interest including, in particular, national security and the protection of health and rights.

These clauses are based on a reasoning of the concrete case and it is up to the national authorities to achieve a proportional balance between the limiting measure imposed and the general interest objectives pursued.

The measures adopted by the Government, although particularly restrictive, are proportional, given that the only rules that cannot be derogated from are the right to life and the prohibition of torture and that the prohibitions imposed seem to be the only possible and most effective responses to contain the pandemic.

2. The contact tracing and Immuni app

When and how can it be considered right to sacrifice the right to privacy of the individual for the health of the community?

Although many individuals are willing to give up their data on a daily basis (sometimes completely unconsciously) for purely recreational applications, can the same be said in the face of such a health emergency?

In order to manage unpredictability, is it necessary to develop a culture and education that recognises the value of data as a resource for dealing with critical situations?

Does EU legislation on GDPR contain rules that can be applied in the processing of personal data in particular contexts such as the COVID-19 pandemic?

These are some of the main questions that we will try to answer.

The Data Protection Regulations provide for this:

[10] G. Zagrebelsky, 'La prevista adesione dell'Unione Europea alla Convenzione europea dei diritti dell'uomo' (2007) on *www.europeanrights.eu/public/commenti/Adesione_Zagrebelsky.doc*.

– in recital 46 [11] the possibility that certain objectives, such as monitoring the development of epidemics and their spread, may find the right legal framework;

– in recital 54 [12] the possibility that the consent of the person concerned may be disregarded for public health reasons;

– in point (d) of the first paragraph of Article 6 and point (c) of the second paragraph of Article 9, the lawfulness of treatment only to the extent necessary to safeguard the vital interests of the data subject or of another natural person.

The term "necessary" in the European rules just mentioned is a clear reference to the regulatory principles governing all processing of personal data and, in particular, to the principle of minimisation according to which only personal data that are adequate, relevant and limited to what is necessary to fulfil the purposes for which they are processed may be processed.

On the basis of an analysis of the necessary balance between equally important rights such as personal freedom and the right to the protection of personal data on the one hand and the protection of individual and public health on the other, the question arises as to when a compression of the right to privacy can be considered a necessary, appropriate and proportionate measure within a democratic society, both on the usefulness of adopting ways of informing the public in order to avoid the unconditional dissemination of sensitive data concerning the state of health and, lastly, on the measures that will have to be taken, once the emergency has ceased and the purpose of the processing has been reached, in order not to convert the information collected to the satisfaction of further purposes.

---

[11] "*The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters*".

[12] Which reads: "*The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (1), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies*".

The contact tracing, or the tracking of the people encountered and the places frequented by infected persons, pursues the main purpose of monitoring the spread of the virus on the territory and, at the current state of the art, will be implemented via Bluetooth device, with applications, approved by the authorities, installed on citizens' devices, involving, on a voluntary basis, the analysis of transactions with credit cards or other means of payment, geolocation data available to mobile phone operators, or through the use of Big Data (data from, for example, companies producing "smart" devices, market loyalty cards, license plate detection or cameras with facial recognition).

Such a system of automated analysis and processing of information and personal data is clearly more efficient than the self-declaration of individuals, as it allows to intervene with targeted actions of prevention and containment.

If by order no. 10 of April 16, 2020 of the Extraordinary Commissioner for Emergency, Dr. Domenico Arcuri, the contact tracing app that will be used to counter the COVID-19, called "Immuni", on April 29, 2020 was approved the Justice Decree that introduces, ex multis, urgent provisions on the protection of personal data in the tracking of contacts and contagions from COVID-19 through the new "Immuni app".

The Decree provides, for the sole purpose of alerting people who have come into contact with individuals who have tested positive to COVID-19 and protect their health through prophylaxis measures related to the health emergency, that an IT platform be established at the Ministry of Health for the tracking of close contacts between individuals who install, on a voluntary basis, the Immuni app for mobile phone devices.

The Ministry will therefore have to identify the appropriate technical and organisational measures to ensure a level of security appropriate to the high risks to the rights and freedoms of the persons concerned by ensuring, in particular, the following:

– that users receive, before the application is activated, clear and transparent information in order to achieve full awareness of the purposes and processing operations, the pseudonymisation techniques used and the data retention times;

– that the personal data collected by the application are only those necessary to inform users of the application that they are in close contact with other users identified as positive to COVID-19 and to facilitate the possible adoption of health care measures in favour of the same persons;

– that the processing carried out is based on the proximity data of the devices, rendered anonymous or, where this is not possible, pseudonymised;

– that the confidentiality, integrity, availability and resilience of processing systems and services are guaranteed on a permanent basis, as well as appropri-

ate measures to avoid the risk of reidentification of data subjects to whom pseudonymised data undergoing processing relate;

– lastly, that data relating to close contacts are stored, including in users' mobile devices, for the period strictly necessary for the processing (the duration of which is determined by the Ministry of Health) and that they are subsequently deleted automatically upon expiry of the period.

It is also expressly provided for:

– that the data collected may not be processed for purposes other than those specified;

– that, in case of non-use of the application, there will be no limitation/consequence with regard to the exercise of the fundamental rights of the subjects concerned;

– that the platform must be realized exclusively with infrastructures located on the national territory and managed by administrations or public bodies or companies with total public participation and that the computer programs developed for the realization of the platform are of public ownership;

– finally, that the use of the application and of the platform, as well as any processing of personal data must be interrupted at the date of the end of the state of emergency, and in any case no later than 31 December 2020. By that date, in fact, all personal data processed must be deleted or made permanently anonymous.

Let's analyze, therefore, what are the characteristics, the data tracking mode and what seem to be the limits of the Immuni app.

It can be downloaded on a voluntary basis and free of charge; it will be initially tested, starting from the end of May, in some pilot regions and then adopted at national level.

With regard to the features, the app in question consists of two parts: the first is dedicated to contact tracing through Bluetooth technology [13], the second, however, is intended to host a sort of clinical diary where the individual user can write down all the most relevant information [14].

As far as the tracking mode is concerned, it should be noted that mobile phones will keep in memory (in the form of encrypted anonymous codes) the data of other mobile phones with which they have come into contact; associated

[13] Through the Bluetooth device it is possible to detect the proximity between two smart phones within one meter and retrace back all the meetings of a person who tested positive for COVID-19, so you can track and isolate the potential infected.

[14] Such as gender, age, previous illnesses, medication intake, health conditions and the presence of symptoms compatible with the virus.

with these codes there will be metadata that will come into play in the assessment of the risk of contagion.

In the event that one of the subjects who downloaded the app is positive for the virus, the health care workers will provide an authorization code with which he can download his anonymous code on a ministerial server.

If the app recognizes an infected person's code in its memory, it will display an appropriate notification to the user.

In relation to the limits, the first of an operational nature concerns the voluntary nature of the membership; in fact, as specified by the European Committee on the Protection of Personal Data (EDPB) and by our Guarantor Authority itself in principle, location data can be used by the operator only if made anonymous or with the consent of individuals.

This aspect alone raises perplexity because there is a risk of using an app that involves the processing of particular categories of personal data without having sufficient guarantees about its functionality with the risk of being faced with the "technological drift" mentioned by Rodotà.

Referring to the principles enshrined in the GDPR analyzed above, it is recalled that it is (already) allowed to the competent public health authorities to process personal data in the context of an epidemic, in accordance with national law and under the conditions laid down therein.

Consequently, where treatment is deemed necessary for reasons of overriding public interest in the field of public health, where there is a presumption of lawfulness, the consent of individuals may well be disregarded.

It goes without saying, therefore, that the question arises as to whether the tracking system is based on a different assumption from that of lawfulness; otherwise it would not explain the recourse to the expression of consent (which, however, significantly affects the actual functioning of the system).

Other limits are represented by the necessary adoption of adequate security measures on the entire processing chain in order to ensure compliance with data protection principles, such as the proportionality of the measure in terms of duration and scope, the reduced conservation of the same and the respect of the purpose limitation, as well as the replacement of geolocation at satellite level with Bluetooth connectivity, which has the criticality of not having a generic communication band (such as Wi-Fi).

On this point, the Secretary General of the Authority for the protection of the personal data, Dr. Giuseppe Busia, had underlined how it is necessary that the treatment of the personal data takes place on the basis of a transparent regulation (containing adequate guarantees), under the supervision of the competent public authorities, in respect of the principle of reasonableness at the base of the GDPR, and that the use of the same does not become an instrument aimed at in-

creasing the informative power of the platforms or of the large operators [15].

One wonders, therefore, whether what is contained in the Justice Decree can be considered sufficient to meet the above mentioned protection requirements.

3. The data breach

If and how can contact tracing lead to risks arising from the data breach?

In order to answer this question it is necessary to start from the definition of data breach.

This term refers to a security incident that may result, accidentally or illegally, in the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or processed in the financial, health or industrial property spheres.

The phenomenon under consideration may occur as a result of:

– accidental loss (think of the data breach caused by the loss of a USB stick);
– theft (think of the data breach caused by the theft of a notebook);
– corporate infidelity (think of the data breach caused by an internal person who, having the authorization to access the data, produces a copy for public distribution);
– misuse of data (think of the data breach caused by unauthorized access to computer systems with subsequent disclosure of the information acquired).

With the Provision of the Guarantor for the Protection of Personal Data concerning the implementation of the discipline on the communication of personal data breaches of April 4, 2013, was implemented the European Directive 2009/136/EC which amended, in part, the Directive 2002/58/EC on privacy in the electronic communications sector.

In this way, the Guarantor has introduced the obligation to notify the Authority (see art. 33 GDPR [16]) and users (see art. 34 GDPR [17]) in case of serious vio-

[15] The full interview with the Secretary General of the Garante per la protezione dei dati personali can be found at *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9303684.*

[16] Notification of a personal data breach to the supervisory authority: "*1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

lations following cyber attacks or adverse events that may lead to loss, destruction or undue disclosure of data.

In the regulatory silence, what are the measures to be put in place in order to prevent, manage and resolve episodes of loss and/or destruction of personal data?

Among the organizational measures to be provided for in the procedure, particular importance is given to the preventive classification of risks, distinguishing between an absent (which does not justify any notification to the Guarantor), present (which requires notification) and high (which also requires communication to the parties concerned) risk situation.

In fact, it is evident that, in the event of a violation, it is essential to be able to resort to a prior classification of the risk in order to take the necessary decisions within the prescribed time limits.

It is understood that this prior analysis will also have to take into account the specific elements of context (not a priori preventable).

---

3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article".

[17] Communication of a personal data breach to the data subject: "*1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met".

The risks thus identified can be mitigated through appropriate countermeasures such as:

– legal obligations (the protection of privacy and data security are addressed both in laws having a general scope, such as, for example, the GDPR, and in laws and regulations having a specific character for a specific field [think of the matter of health data or judicial data]);
– the data security policy (as a document concerning the storage of data, both physical and digital, their transport, access modalities, responsibilities, and so on);
– the policy for the use of company equipment (as a document in which all issues relating to the use of the tools that an entity makes available to its employees and consultants are addressed);
– user authorisations (which must be strictly necessary for the operations to be carried out);
– the automation of processes (it was, in fact, found that human error is the first responsible for data breaches and is, normally, the product of a low culture of security, inaccurate, negligent and uncontrolled management of data);
– the promotion of security awareness;
– the use of encryption (where possible);
– tracking and monitoring (access to data and all functions performed on it must be tracked in real time and the logs produced must be kept accurately for the time required by law and internal regulations);
– backup of data (which allows recovery in case of destructive events);
– lastly, patch management (or the adaptation of software and operating systems when new vulnerabilities are detected).

This explains in detail what is the link between phenomena such as the data breach of the INPS [18] website and the Dutch app Covid19 Alert! [19]?

And what is the legal significance of such events?

Both events are symptoms of a strong criticality in the system, where obvious technical and cultural shortcomings make the fundamental rights of individuals even more vulnerable.

[18] On April 1, 2020, on the occasion of the possibility to access the INPS port in order to request and obtain the bonus of 600 euros, the Social Security Institute reported the dispersion of thousands of personal data of users, thus foreshadowing the first data breach during the health emergency by COVID-19.

[19] The application proposed by the Dutch government for the management of contact tracing, Covid19 Alert!, suffered a serious data leak of individuals who tested positive for the virus with the consequence that what were (or should have been) encrypted personal data were irreparably made public.

The absence of a right to guarantee the integrity and confidentiality of computer systems (as a corollary of the more general right to dignity), together with a clear disproportion between the aims pursued and the means used, how can the expectation of full protection of the right to technological and telematic confidentiality of one's own data be generated in individual users?

The violation of personal data represents, once again, a manifestation of the legislator's anxiety to keep up with such a changing reality as the contemporary one characterized by incessant technological progress.

4. Conclusions

Although there is no doubt that the attempt to protect, at least formally, the correct processing and custody of personal data is being made, a detailed and constantly updated regulatory framework is not, and probably will not be, sufficient to incorporate the new values of the economic and social context.

We conclude, therefore, by adopting the thought of Prof. Mantelero according to which: "*occorre che si radichi una cultura della "privacy", fondata sulla consapevolezza dell'importanza dei dati personali e, più in generale, su un maggior rispetto per l'individuo. È questo un processo lungo, in quanto incidente su aspetti valoriali, che può tuttavia essere agevolato da una chiara e coerente applicazione della legge da parte degli organi deputati a vigilare sull'attuazione della stessa e, soprattutto, da una divulgazione più lata possibile dei principi che ne sono a fondamento* [20]".

[20] A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa* (1nd edn, Giuffrè 2007) 84-85.

A FACEBOOK COURT IS BORN: TOWARDS THE 'JURISDICTION' OF THE FUTURE?

Aldo Iannotti della Valle

Ph.D. candidate in 'Humanities and Technologies' at
Università degli Studi Suor Orsola Benincasa di Napoli

Abstract:

The paper, starting from the news of the appointment of the first 20 Members of Facebook's Oversight Board, offers first brief reflections about the entry into force of a Facebook Court, enlightening true or presumed independence from the company, as well as similarities or differences with Google Advisory Council. Last but not least, the paper poses a question that already seems crucial: a model of justice with an own Court for each 'Big Tech' is going to be the 'jurisdiction' of the future?

Key-words: Social networks, Private jurisdiction, Right to erasure and right be forgotten, Data Protection Law, Technology, Internet.

Summary: 1. Facebook's Oversight Board after the appointment of the first 20 Members. – 2. How independent the Oversight Board really is from Facebook? A deeper look through the Charter of the Board. – 3. A comparison between Facebook's Oversight Board and Google Advisory Council. – 4. An own Court for each "Big Tech": towards the "jurisdiction" of the future?

1. Facebook's Oversight Board after the appointment of the first 20 Members

On May 6th 2020 Facebook appointed the first 20 Members of its Oversight Board [1], an own 'Court' which is supposed to review content and issue reasoned

[1] *See* the official website of the Oversight Board for the complete and continuously updated list of members and other relevant information on the newborn 'Facebook Court': https://www.oversightboard.com.

and binding decisions, strongly desired by Facebook itself to clean up its image partially compromised by the controversies occurred to the company in the past years [2]. The Court is scheduled to become operational this year.

The recent news of the appointment of the first 20 Members allows us to carry out the first reflections on the 'Facebook Court' now about to start operating.

First of all, a brief analysis of the profiles identified and the selection procedure allows to understand what kind of 'Court' this Board is going to be. Once this is done, it is crucial to analyze the functions in more detail, trying to understand the real impact the Oversight Board is going to have.

It seems not secondary to start with the recently appointed 20 Members of the Board: all of them are high profile professionals, coming from all over the world, to ensure a global perspective. We could easily call them 'a dream team'. A brief analysis of their *curricula* suggests the leading role that the Board will take in Facebook's intentions.

Each member will serve for a three-year term, for a maximum of three terms, pursuant to the Charter of the Board [3], Article 1, para. 3.

Among the 20 Members, 4 Co-Chairs were appointed: Catalina Botero-Marino, from Colombia, Dean of the Universidad de los Andes, Faculty of Law, Special Rapporteur for freedom of expression at the Organization of American States, alternate Judge of the Colombian Constitutional Court; Jamal Greene, from the United States, Professor at Columbia Law School; Michael McConnel, from the United States, Professor and Director of the Constitutional Law Center at Stanford Law School, former Judge of U.S. Court of Appeals and U.S. Supreme Court advocate; Helle Thorning-Schmidt, from Denmark, former Prime Minister of Denmark, former CEO of Save the Children.

The Co-Chairs, according to the Charter, Article 1, para. 7, who will serve as liaisons to the board administration, lead committees and carry out management responsibilities, such as membership selection and case selection.

Members also include several other Professors from primary Universities from all over the world and Tawakkol Karman, a Nobel Peace Prize laureate.

In fact, in order to be selected, the Members must have specific characteristics, defined in the Board's Charter, Article 1, para. 2: 'For the board to serve its purpose effectively, members must possess and exhibit a broad range

[2] *See* JC Wong, 'Will Facebook's new oversight board be a radical shift or a reputational shield?' (2020) *The Guardian*, 7 May 2020, which poses the following question: 'will Facebook's oversight board live up to its lofty promises and reshape how Facebook shapes the world? Or will it just be a reputational shield for a company whose pathologies run deeper than the question of whether individual pieces of content should be allowed or taken down?'.

[3] For the Charter *see* https://www.oversightboard.com/governance/.

of knowledge, competencies, diversity and expertise. Members must not have actual or perceived conflicts of interest that could compromise their independent judgement and decision-making. Members must have demonstrated experience at deliberating thoughtfully and as an open-minded contributor on a team; be skilled at making and explaining decisions based on a set of policies or standards; and have familiarity with matters relating to digital content and governance, including free expression, civic discourse, safety, privacy and technology'.

Furthermore, according to Article 1, para. 4, of the Charter, the Board will have the following expressly defined powers. First of all, the Board may request that Facebook provide information reasonably required for board deliberations in a timely and transparent manner. The Board will take the decision interpreting Facebook's Community Standards and other relevant policies (collectively referred to as "content policies") in light of Facebook's articulated values. In order to execute the decision, the Board may instruct Facebook to allow or remove content and also instruct Facebook to uphold or reverse a designation that led to an enforcement outcome. Each decision should be motivated by written explanations and, under Article 6 of the Charter, will be made publicly available and archived in a database of case decisions on the Board's website, subject to data and privacy restrictions.

People using Facebook's services and Facebook itself may bring forward content for board review. Furthermore, pursuant to Article 2, para. 1, 'in instances where people disagree with the outcome of Facebook's decision and have exhausted appeals, a request for review can be submitted to the board by either the original poster of the content or a person who previously submitted the content to Facebook for review': in this sense, the Oversight Board seems to be a Facebook's Court of Appeal.

The Board will have no authority or powers beyond those expressly defined by the Charter.

2. How independent the Oversight Board really is from Facebook? A deeper look through the Charter of the Board

Facebook claims that the Oversight Board should be independent from the company. Mark Zuckerberg, Founder and CEO of Facebook, stated: 'We are responsible for enforcing our policies every day and we make millions of content decisions every week. But ultimately I don't believe private companies like ours should be making so many important decisions about speech on our own. That's why I've called for governments to set clearer standards

around harmful content. It's also why we're now giving people a way to appeal our content decisions by establishing the independent Oversight Board'. [4]

In essence, in Zuckerberg's words, the birth of the Board would have followed the call to governments to intervene on the matter, which failed, but Zuckerberg himself seems to be aware of the necessity that the Board should be independent from the company he rules.

The same recently appointed 20 Members of the Board, in the aforementioned intervention on The New York Times, made it clear: 'We are all independent of Facebook. And we are all committed to freedom of expression within the framework of international norms of human rights. We will make decisions based on those principles and on the effects on Facebook users and society, without regard to the economic, political or reputational interests of the company'. [5]

To verify how true this assumption is and how much aspirations correspond to reality it seems necessary to examine in detail the Charter of the Board, as well as By-laws and Code of Conduct.

According to the aforementioned Article 1, para. 2, of the Charter, in order to guarantee the independence of the judgement, the specification, among the requirements, of the absence of any actual or perceived conflict of interest seems to be very important.

It is legitimate to doubt, however, that the conflict of interest may derive from the same selection procedure, envisaged by Facebook, and from the regulation of the remuneration provided for the assignment.

As for the selection procedure, provided by the Charter, Article 1, para. 8, all roads seem to lead to Facebook, since it is Facebook to select the group of Co-Chairs.

Once Facebook has selected the Co-Chairs, Facebook and the Co-Chairs will then jointly select candidates for the remainder of the Board seats, formally appointed by trustees. Facebook and the public may always propose candidates to the Board.

As regards remuneration, the speech is perhaps more complex, since Facebook has taken precautions to prevent criticism from this point of view.

In the aforementioned intervention on The New York Times, the four Co-Chairs ensure that 'independent judgment is guaranteed by our structure. The

[4] M Zuckerberg (2019) at https://www.facebook.com/zuck/posts/one-of-the-most-important-projects-ive-worked-on-over-the-past-couple-of-years-i/.

[5] C Botero-Marino, J Greene, MW McConnel, H Thorning-Schmidt, 'We Are a New Board Overseeing Facebook. Here's What We'll Decide' (2020) *The New York Times*, 6 May 2020.

oversight board's operations are funded by a $130 million trust fund that is completely independent of Facebook and cannot be revoked'.

This is confirmed by reading the Charter: according to Article 5, para. 1, 'the board will be funded by the trust to support its operations and expenses' and, under the para. 2, 'the trustees will maintain and approve the board's operating budget, including member compensation, administration and other needs. The trustees will formally appoint and, if necessary, remove members for violations of the board's code of conduct'.

However, as for the relationship between the trust and Facebook, according to Article 5, para. 2, 'the trust will receive funding from Facebook, and the trustees will act in line with their fiduciary duties. Facebook will appoint independent trustees'.

Therefore, it is still legitimate to doubt that the mechanism devised, also in this respect (and not only for the selection procedure), can guarantee effective independence.

3. A comparison between Facebook's Oversight Board and Google Advisory Council

Before the birth of the Board, a comparable experience was perhaps that of the Google Advisory Council whose establishment indicates, however, a totally different approach from Google. The Council, indeed, seems to have some similitudes with the Oversight Board but also big differences

After the groundbreaking 2014 decision of the Court of Justice of the European Union in the Google Spain case (C-131/12) [6], Google was supposed to take a binding decision in the matter of right to be forgotten. [7]

A first difference with the Facebook Board is here: if the Oversight Board is a Facebook initiative, in the case of Google it was the same pronunciation of the Court of Justice that assigned to Google a function that should not be proper to it and that the same Google has unwillingly accepted: that of 'judge' on requests regarding the right to be forgotten, in the sense of de-referencing made by the Court.

---

[6] CJEU, Grand Chamber, May 13th 2014, C-131/12 (Google Spain).

[7] *See* G Cintra Guimarães, *Global technology and legal theory. Transnational constitutionalism, Google and the European Union* (2019) New York, 156, which observes: 'private companies such as Google will act as a sort of "court of first instance" in the implementation of the right, filtering the requests that will eventually end up being analyzed by data protection authorities and official tribunals'. About the right to be forgotten *see* above all TE Frosini, *Liberté Egalité Internet* (2015) Napoli, 117 ff.

About this new and perhaps undesired function, Google itself stated 'these are difficult judgements and as a private organization, we may not be in a good position to decide on your case'. [8]

At this purpose, Google enforced Google Advisory Council: the Council wasn't really a 'Google Court', like Facebook's one, since Google intended to take 'directly' decisions in the field of right to be forgotten, without worrying about providing a semblance of independence, being expressly allowed by the Court of Justice.

If Google was supposed to take binding decision in matter of right to be forgotten [9], the Council was supposed to help Google to make the right balance between right to be forgotten and other rights and the public's right to information above all. [10]

That's why, in order to make this balance right, Google established a Council of experts from all around the world to require them to weigh, on a case-by-case basis, an individual's right to be forgotten with the public's right to information. The Council of experts, composed of subjects with proven experience and well-known Professors such as in the case of the Oversight Board, but directly nominated by Google, was supposed to review input from dozens of other experts in meetings across Europe, as well as from thousands of submissions through the web. [11]

Another difference is in the scope. Google Advisory Council's scope, at evidence, was limited to advice Google for requests related to right to be forgotten, while the Oversight Board's judgment potentially extends to the removal and maintenance of all content published on Facebook, also for different reasons.

What the Oversight Board and the Google Advisory Council really have in common is that the occasion of their birth is due to the substantial abdication by Nations and the European Union by a web regulation and the consequent jurisdiction.

---

[8] Google's FAQ about right to be forgotten, available at: https://policies.google.com/faq?hl=en.

[9] *See* G Cintra Guimarães, *Global technology,* 158, according to which 'Google increasingly assumes the role of a "court of first instance" for the whole of Europe'.

[10] *See* also G Cintra Guimarães, *Global technology,* 157, which observes that the Advisory Council was a way for Google to make its decision-making more transparent and predictable, since Google would have followed the 'specific advice on the implantation of the judgement' given by the Council.

[11] Google (2015) *The Advisory Council to Google on the Right to be Forgotten*, 7, available at https://static.googleusercontent.com/media/archive.google.com/it//advisorycouncil/advisement/advisory-report.pdf, identified four primary criteria on which the Council advised Google to evaluate delisting requests from individual data subjects: 1. data subject's role in public life; 2. nature of the information; 3. the specific source; 4. time elapsed.

The new model represented by the 'Facebook Court', also because of the spaces left by lawmakers, will be the 'jurisdiction' of the future?

4. An own Court for each 'Big Tech': towards the 'jurisdiction' of the future?

The digital revolution is giving one of the greatest transformations to the world since the era of the industrial revolution. In this framework, the birth of a Facebook Court suggests a first reflection about the evolution of the jurisdiction in the digital era [12], also considering the risks carried out by this evolution. Although Facebook announces the Board as independent of its organization, it is still Facebook to dictate the rules.

Is the justice slowly (or not so slowly) moving towards a 'Big Tech justice'? With virtual life becoming more and more important, do these para-jurisdictional Boards, as Facebook's Oversight Board, not risk becoming more and more central in the global legal experience in the future? If so, will this para-jurisdictional 'drift' be able to equally guarantee effective protection of rights?

In the aforementioned intervention, Mark Zuckerberg, Founder and CEO of Facebook, stated that the birth of the Board followed a call to Governments to intervene in the matter, which failed.

Undoubtedly the spaces for regulatory intervention first and jurisdictional then are those left by national legislators, as well as by the European Union, which have not yet provided for a precise discipline of the matter.

Just think of the case of the right to be forgotten. Despite the huge impact of the Google Spain ruling, which prompted Google to set up the Advisory Council, the GDPR seems to have failed in its task of regulating the right to be forgotten. In fact, GDPR, Article 17, para. 1, only establish the principle according to which the interested party, under certain conditions, has the right to request the cancellation of personal data concerning him (therefore not de-referencing personal data from the search engine as the Court of Justice claimed in the Google Spain decision). [13] Referring only to the cancellation it is not clear if the

[12] *See* B De La Chappelle, P Fehlinger, 'Jurisdiction on the Internet: from legal arms race to transitional cooperation', available at: https://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet.pdf. The paper underlines that 'the theme of "digital sovereignty" gains traction in many jurisdictions in a context of rising tensions and a sense of powerlessness by public authorities to impose respect for their national laws on foreign-based Internet platforms and technical operators'.

[13] *See* S Zanini, 'Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?' (2018) 15 Federalismi.it; D Barbierato, 'Osservazioni sul diritto all'oblio e la (mancata) novità del Regolamento UE 2016/679 sulla protezione dei dati personali' (2017) 6 Resp. civ. e previd., 2100 ff.

GDPR intends to refer this duty to proceed with the cancellation also to the search engines or not. Furthermore, as said, the same Court of Justice of the European Union forced Google to become a judge in the matter of right to be forgotten and the result is the abovementioned Google Advisory Council.

More generally, the gaps regarding several aspects of the web, not only in European legislation, leave huge spaces for the intervention of private subjects and especially of 'Big Tech', as stated by Mark Zuckerberg himself.

If the regulation of the web is theoretically possible, the task seems to be difficult indeed, even for the European Union, given the universalistic and tendentially free nature of the web. [14]

Perhaps, the easier way to regulate the web is by more flexible soft law sources, instead of the traditional hard law. [15] The regulation of the Internet, therefore, risks being mostly entrusted to the "owners" of the house: the law of the future should be Google Law or Facebook Law?

In fact, the giants of the web appear, at present, the only subjects capable of dictating truly large-scale rules on the most varied aspects of the web and also capable of enforcing them, despite their soft law nature.

The rules that germinate within the giants of the web, therefore, still constitute 'law', despite the undoubtedly undemocratic origin and the submission to business logic rather than fundamental rights.

To the crisis of hard law and, more generally, of the state monopoly on the sources of law corresponds the crisis of the state monopoly on jurisdiction. As has been observed, these are two aspects of the same phenomenon: the erosion of state sovereignty in the global space. [16]

---

[14] About the challenge of regulating the web protecting fundamental rights *see* A Iannotti della Valle, 'L'età digitale come "età dei diritti": un'utopia ancora possibile?' (2019) 16 Federalismi.it.; also *see* S. Sassi, *Diritto transnazionale e legittimazione democratica* (2018) Milano, 56 ff., about the need for a transnational law for the regulation of sectoral areas which, by their transnational nature, neither the State nor the international legal system are able to regulate.

[15] *See* MC Gaeta, 'Hard law and soft law on data protection: what a DPO should know to better perform his or her tasks in compliance with the GDPR' (2019) 1 EJPLT. Also *see* E Mostacci, *La soft law nel sistema delle fonti: uno studio comparato* (2008) Milano, 2008; A Somma, 'Soft law sed law: diritto morbido e neocorporativismo nella costruzione dell'Europa dei mercati e nella distruzione dell'Europa dei diritti' (2008) 3 Rivista critica del diritto privato, 437 ff.

[16] About the growing role of the private justice in the globalized world, with particular regard to arbitration, *see* F Marone, *Giustizia arbitrale e Costituzione* (2018) Napoli, 241, according to which: 'Una giustizia "privata", dei privati e per i privati, infatti, meglio si presta ad un contesto costituito da sempre più regole private e meno regole statuali. L'arbitrato, per certi versi, costituisce – sul piano processuale – l'altra faccia della stessa medaglia: da un lato la regolamentazione giuridica dei privati (soft law) erode lo spazio della normazione statale (hard law), dall'altro l'arbitrato (giurisdizione dei privati) erode lo spazio della giurisdizione statale. La riduzione dello spazio della sovranità dello Stato, in definitiva, passa per entrambi i momenti: alla crisi del mono-

In the specific case of the Oversight Board, the institution seems to have been conceived by Facebook to effectively protect fundamental rights and freedom of expression, while not referring to any of the constitutional experiences resulting from centuries of legal civilization in Europe and America.

The Oversight Board's Charter itself, Article 2, para. 2, states that 'the board will review content enforcement decisions and determine whether they were consistent with Facebook's content policies and values': that said, it is clear that Facebook's content policies and values are going to act as a Constitution for the Board's judgements. In fact, the statement, at the bottom of the same Article, according to which 'the board will pay particular attention to the impact of removing content in light of human rights norms protecting free expression', without other specifications, seems to be a style clause, while Facebook's content policies and values are clearly at the first place.

It is also important to outline that, according to the Charter, Article 2, para. 1, 'the board has the discretion to choose which requests it will review and decide upon. In its selection, the board will seek to consider cases that have the greatest potential to guide future decisions and policies'. Therefore, not all requests will enjoy effective protection, which leaves us perplexed. How can the protection of fundamental rights be *à la carte?*

But the real question is the following: can we allow the protection of fundamental rights to be left to the good intentions of the CEOs of Facebook and Google?

It would then perhaps be better if the legislators around the world take back what is up to them and that is recognized by the 'Big Tech' themselves, taking the courage to regulate the most controversial aspects of the web. In fact, a progressive evolution of jurisdiction towards a jurisdiction managed by 'Big Tech', capable of issuing binding decisions in delicate matters, without fully ensuring the rights of defense and the contradictory, would not be acceptable.

The prospect of an increasingly central role of the private justice in the field of rights on the web, however, may be acceptable or even desirable if the legislators, at the highest possible level [17], will be able to impose minimum guarantees that allow defining a judgment actually 'justice': just think of the possibility of technical defense and the effectiveness of the contradictory as well as guarantees on the appointment of truly independent and impartial 'judges'.

Indeed, it was appropriately stated that 'even in the most informal of pro-

polio statale sulle fonti del diritto, quindi, corrisponde la crisi del monopolio statale della giurisdizione'.

[17] It is worth remembering the definition of contemporary constitutionalism as 'multilevel constitutionalism' provided by I Pernice, 'Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitution-Making Revisited?' (1999) 36 Common Market Law Review, 703 ff.

ceedings certain minimum requirements of 'due process' must be met if the award is to be legally binding'. [18]

In presence of such guarantees, forms of private justice can offer undoubted advantages: first of all, as already happens in many countries with administered arbitrations [19] in matters such as banking and financial law [20], public procurement [21] and sport [22], technical bodies appear more suitable to resolve disputes in subjects requiring specific knowledge. In the present case, a knowledge of the technology behind the law [23] as well as a knowledge of the fundamental rights involved, obviously.

[18] E Brunet, 'Arbitration and Constitutional Rights' (1992) 71, 1 NC Law Review, 1992, 81 ff.

[19] About the advantages of the private justice and the arbitration, with particular regard to administrated arbitrations, *see* F Marone, *Giustizia arbitrale*, 188 ff.

[20] *See* L Albanese, 'Banking and financial litigation: between alternative dispute resolution systems and so-called "vessatorietà" of the arbitration clauses' (2017) 6 Resp. civ. e previd., 1873 ff.

[21] *See* I Lombardini, 'Il nuovo arbitrato nei contratti pubblici, obbligatoriamente amministrato dalla Camera arbitrale: rivoluzione copernicana o restaurazione?' (2016) 4 Riv. Arb., 715 ff.

[22] *See* TE Frosini, 'La giustizia sportiva italiana e comparata' (2017) 15 Federalismi.it.

[23] *See* L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Pol. Dir., 339, where the Authors opportunely suggest to look at the law from a technological point of view.

EMPIRICAL METHODOLOGIES FOR THE DESIGN OF INNOVATIVE AUTONOMOUS DRIVING SOLUTIONS

Anna Irene Cesarano
Ph.D. (c) at Università degli Studi Suor Orsola Benincasa di Napoli

Abstract:

This article aims to present itself as an overview of the world of self-driving cars, giving a glimpse albeit fleeting to my research project and clarifying some basic concepts to understand the future developments of this discipline. Concepts like automation levels, self-driving cars, artificial intelligence are essentials and most important to understand all the innovative flow of autonomous driving. Autonomous driving represents the challenge of the future, although many critical aspects must be overcome and addressed.

Key-words: Self-driving cars, Artificial intelligence, Automation levels, Driverless cars, Research project, Autonomous cars.

1. Self-driving cars

The automotive sector is constantly evolving, self-driving cars are the result of a complex design that adopts a good variety of devices and sensors [1] that capture information from the external environment which is then transmitted to an internal computer, in order to guarantee the vehicle efficiency, safety, stability for both passengers and for people who are near the car itself.

Self-driving cars [2] can be defined as those vehicles with systems of autono-

[1] Sensors and devices are: lidar, radar, videocameras, artificial vision, ultrasound.

[2] P. Koopman, M. Wagner, 'Autonomous Vehicle: An Interdisciplinary Challenge' [2017] IEEE Intelligent Transportation Systems Magazine, 90-96.

mously taking control of the car and coping with all aspects of driving such as accelerating and braking, steering control, gear shifting. Self-driving cars, also called "autonomous cars" or "driverless cars" are the product of the continuous evolution of the automotive sector and of a new concept of transport and mobility, which through the application of artificial intelligence become "smart". The modern concept of autonomous driving with cars controlled by artificial intelligence and equipped with the most varied and modern sensors and technological devices, is able to disrupt the classic concept of the car, paving the way for new lines of research and more and more design techniques based on user centered design (UCD), for safer and smarter mobility. [3]

Figura 1. – Self-driving car

2. Automation levels: SAE's classification

SAE [4] society of Automotive Engineers, a body responsible for regulation in

[3] P. Koopman, M. Wagner, 'Challenges in Autonomous Vehicle Testing and Validation' (2016) 4(1) SAE International Journal of Transportation. Safety, 15-24, https://doi.org/10.4271/2016-01-0128, SAE World Congress Exhibition.

[4] SAE J3018, Mar. 20015 Guidelines for Safe On-Road Testing of SAE Level 3, 4, and 5 Prototype Automated Driving.

Systems (ADS); SAE J3061, Jan 2016 Surface Vehicle Recommended Practice: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.

Cfr. A. Cioffi, *Digital Strategy. Strategie per un efficace posizionamento sui canali digitali* (Hoepli, 2018). https://smartrider.ch/it/attualita/5-livelli-di-automazione-sae.

the aerospace, automotive and vehicle sector [5], made up of scientists, engineers and scholars, has classified six levels of autonomous driving, which start from level 0, the lowest, to the highest, level 5, although the rapid development of the automotive market suggests a future increase in levels.

Specifically, the classification of the levels is as follows:

Level 0, No automation: this is therefore the traditional car, in which the driver controls the car without any type of support from a driver assistance system.

Level 1, Driving assistance: where, thanks to on-board electronics, the driver is helped by information but still has full control of the car in terms of driving (and therefore in acceleration, braking, steering and so on). On a "legal" level, if we can say so, the driver is still fully responsible for everything that happens. The car simply gives support to the driver by capturing information from the outside worlds such as obstacles, dangerous situations and so on. Systems such as ABS, Cruise Control or or airbags, parking sensors are Level 1.

Level 2, Partial automation: in Level 2 of assisted driving the electronics start to integrate into the guide allowing it to intervene in certain situations. There is therefore no full control of the vehicle by the driver, who must however continue to deal with driving in almost all its aspects. This type of automation intervenes only in some cases such as, for example, assisted braking (Brake Assist) following the detection of an object that is on a collision course with our car, or emergency collision braking. Another example may be Lane Assist once again, where instead of receiving only an acoustic signal, the car will correct the steering angle to return to the lane.

Level 3 [6], Limited autonomous driving: With this assistance level, in fact, the electronics are able to automate driving in the fundamental aspects: acceleration, braking, steering. Obviously, in addition to “basic” driving, the car also has all the safety and automation levels described above, but the driver must still keep his eyes open, ready to intervene in adverse circumstances such as unfavorable environmental conditions, unpaved road surface or particularly disconnected and so on. Many cars have this level of automation and, for example, the Park Assist with which the car parks itself, is part of this level.

Level 4, High automation: In Level 4 of assisted driving, on the other hand, you can relax and let the car take you to your destination without intervening because the electronics are able to manage any situation that happens in front of them. However, although the car can manage driving completely, the driver cannot use it in adverse conditions. In these cases, the car will ask the driver to start driving again.

---

[5] A. Cioffi, *Digital Strategy* ibid.

[6] Currently level 3 is what is the highest level of automation on the market.

Level 5 [7], Complete automation: one can speak explicitly of autonomous driving in all its aspects. In this case, therefore, human intervention is not required in any situation and the car can also arrive at its destination without someone in the passenger compartment, making decisions and choosing the best route based on traffic. Autonomous vehicles scan the environment with techniques such as radar, lidar, GPS, and artificial vision. Advanced control systems interpret the information received to identify appropriate routes, obstacles and relevant signs. [8]

3. My research project

My research project [9] involves the development of innovative systems to support autonomous driving (partially autonomous driving), combining one of the transversal sectors (Information & Communication Technologies) with a vertical sector (Transport and Logistics) of particular relevance for the Campania. In particular, the research theme involves the development of a new safer and smarter mobility paradigm, with increasing automation shares that must be harmonized with human characteristics to allow it to maintain an active role in the new socio-technical system. The research theme intends to investigate the methodologies necessary for the conceptualization, prototyping and verification of more suitable user interfaces to ensure effective interaction with the driver (in the context of partially or totally autonomous driving), taking into account technological aspects such as those relating to the individual and his cognitive, behavioral, etc. The application of innovative design methodologies (based on UCD and UX) will guide the design in the conceptualization phase, to allow a preliminary prototyping of the technological construct and its interface before it becomes a definitive product and allow to verify in advance how the people interact with the technological system. If this cooperation [10], studied through empirical methodologies, gives promising signals or highlights some critical ele-

[7] A. Semoli, *AI marketing. Capire l'intelligenza artificiale per cogliere le opportunità* (Hoepli, 2019).

[8] For more in-depth legal analysis see M. C. Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies* (Editoriale scientifica, 2019).

[9] My tutor is Roberto Montanari, professor PHD HMI and manager RE:Lab the Interaction Engineering Company.

[10] The concept of cooperation between car and driver is defined in an innovative way by TeamMate car in TeamMate.

HMI design, implementation and V&V results from 1st cycle, 30-06-2017, authors R. Montanari et al., project number: 690705, www.automate-project.eu.

ments, the user interface may be modified accordingly. Therefore, in addition to the conceptualization and prototyping methodologies, the development of technology verification methods is also an essential part of the innovative research system.

Simulation environments are available within the Scienza Nuova [11] research center, both aimed at the automotive domain, and reconfigurable thanks to the presence of a driving simulator and a virtual environment in which different interaction experiences can be reproduced. Several technologically advanced tools can be used such as eye-tracking, biometric sensors, systems for detecting the emotional state through videocameras etc.

4. The ethical and legal perception of autonomous driving

However, the line of studies attributable to autonomous driving remains a niche sector confined to a limited audience and for the most specialist who really knows its functions and applications. For such reason, I have devised and implemented research on perception and representation of autonomous driving in all its aspects, described in detail in my article [12] which will be published later on EJPLT European Journal of Privacy Law & Technologies. It is therefore appropriate to dwell here only on legal aspect of autonomous driving, and analyze research data, infact the ethical-legal issue seems to be one of the most critical, if not the most critical thorny, for the introduction of self-driving cars. The principle of responsibility civil and criminal in road accidents turns out to be a theme of heated debates and able to channel the attention of several scholars [13]. Within the research, this thorny problem is addressed in two questions, asking users directly for their *opinion in case of r*oad accident both with a fully autonomous car and with a partially autonomous car. From the two pie charts in fig. 1-2 a tangible difference immediately emerges in the responses of users to vary (albeit slightly in drafting and reading, but which however has a great meaning) of the question asked. In a car a fully autonomous driving, according to the sample subjects the responsibility civil and criminal would be in 27.8% of the cases of the company that manufactures the car (manufacturer), while in 24.8%

[11] Scienza nuova is the research center of University Suor Orsola Benincasa.

[12] *Autonomous driving: an exploratory investigation on public perception*, which will be published later on EJPLT European Journal of Privacy Law & Technologies http://www.ejplt.tatodpr.eu/.

[13] For a complete and somewhat exhaustive discussion on the subject, see M.C. Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies*, Editoriale Scientifica, Napoli, 2019.

of cases it would fall on the company that produces the car components [14] (manufacturer of the product components), and in 22.6% of the cases is the company that produces the self-driving car components that the owner of the car; the remaining percentages are divided between the owner of the car (17.4%) and very low shares that stand at around 0.4% (equal to 1 person), for different answers given freely through the option "Other" contemplated at the end. In a partially self-driving car it stands out instead a rather high percentage, equal to 39.1% of the answers, which he attributes responsibility to the owner of the car, while a 34.8% is to the owner of the car that to the company that produces the product components; the remaining percentages are divided into 11.7% for the company that produces the components of the car, 7.8% for the company that produces the car and shares equal to 0.4% for every person who has given free answer to this question.

Figure 2. – Answers to the question "In a hypothetical accident committed by a fully driven car autonomous, whose civil and criminal liability would it be?"

Figure 3. – Answers to the question: "In a hypothetical accident committed by a partially driven car autonomous, whose civil and criminal liability would it be?

[14] Sensors, videocameras, etc.

From a comparison between the answers to these last two questions one could affirm that in the case of totally autonomous driving, people attribute the responsibility of the road accident to subjects who do not identify themselves in car owner, but who seem rather divided between various subjectivities external, e.g. the company that manufactures the car, or the components of the car, or in concomitance with the owner. Otherwise it happens when the car is driving partially autonomous: in this case the responsibility is recognized both in the subjectivity of the car owner (39,1%) both when the latter is in concomitance with the company which produces the autonomous driving components(34,8%). As already stated above, for further information on the research conducted on the perception of autonomous driving, see the article below *Autonomous driving: an exploratory investigation on public perception o*n EJPLT (European Journal of Privacy Law & Technologies. As this was not the right place for such a study.

5. Conclusions

The automotive sector shows an innovative and technological character in its continuous evolution. The classic concepts of driving, car, driver are supplanted in favor of a new concept of safer and smarter mobility. Autonomous driving represents the challenge of the future, although many critical aspects [15] must be overcome and addressed. Autonomous driving or robotaxis could be able to revolutionize many sectors of community life, from the purely social one such as allowing certain types of people to increase their productivity or even disabled or elderly people to move in comfort. While on the purely economic side, autonomous driving would be able to save on the costs of resources and staff employed, but the real turning point was that it would be able to drastically reduce road accidents, which according to some statistical data would be caused in the 95% [16] of cases from human distractions, saving many lives.

[15] Many aspects must be considered as people's distrust and fear of autonomous driving.

[16] https://www.europarl.europa.eu/news/it/headlines/society/20190410STO36615/le-statistiche-sugli-incidenti-stradali-mortali-nell-ue-infografica.

Section II: Comments on decisions

IL *TRIBUNALE DE GRANDE INSTANCE DE PARIS* IN MATERIA DI TUTELA DEL CONSUMATORE, DIRITTO D'AUTORE E *PRIVACY:* CLAUSOLE E INFORMATIVA CHIARE NEI CONTRATTI AD OGGETTO DIGITALE

(Commento a Tribunale de Grande Instance de Paris, 1/4 social, Sent., 17 settembre 2019)

Simona Latte

Legal Counsel e Web Marketing Manager

Abstract:

La sentenza del Tribunale de Grande Instance de Paris garantisce l'applicazione di clausole chiare volte a mantenere l'equilibrio tra le parti contrattuali e a tutelare i diritti dei consumatori, in particolare quando il contratto ad oggetto digitale coinvolga il professionista stabilito fuori dall'Unione Europea e il consumatore/utente risieda sul territorio francese.

Key-words: Tutela del consumatore, diritto d'autore, Privacy.

1. Introduzione

Con sentenza del 17 settembre 2019 resa dal *Tribunale de Grande Instance de Paris,* il giudice francese si è pronunciato sulla controversia tra l'associazione "Union Fédérale des consommateurs – Que Choisir" (da ora in poi "UFC – Que Choisir") e la società americana Valve Corporation (da ora in poi "Valve") con sede a Washingotn – società titolare di una piattaforma (piattaforma "Steam") che fornisce un servizio di distribuzione *online* di contenuti digitali,

come video giochi e servizi collegati – in senso favorevole alla prima.

La controversia, nello specifico, concerneva la liceità, sotto diversi profili, di molteplici clausole contrattuali contenute nelle Condizioni Generali di Utilizzo, contratto cui gli utenti della piattaforma avrebbero dovuto aderire per abbonarsi ai servizi offerti.

2. Le questioni

La società Valve forniva l'accesso ai *videogame* ed ai servizi della piattaforma previa sottoscrizione dell'*Accordo di Sottoscrizione Steam* costituente le condizioni generali di utilizzo della piattaforma stessa, cui anche gli utenti francesi avrebbero dovuto vincolarsi per fruirne i contenuti.

L'UFC – Que Choisir rilevava che tale Accordo, comprensivo della "*Privacy Policy*", avesse subìto negli anni diverse modifiche e aggiornamenti, di fatto rendendo difficoltosa la ricostruzione di una disciplina del rapporto contrattuale uniforme e nitida da parte degli abbonati. Inoltre, l'associazione evidenziava, nello specifico, che diverse clausole presenti nel contratto fossero in grado di determinare uno squilibrio tra i diritti e i doveri delle parti contrattuali e che vi fossero profili di illiceità anche in materia di *privacy* e diritto d'autore.

3. Osservazioni del *Tribunale e decisioni*

3.1. Sulla violazione delle norme a tutela del consumatore

In prima analisi il giudice francese si pronuncia sul carattere abusivo o illecito di alcune clausole delle Condizioni Generali d'Utilizzo**,** ricordando che sono o si presumono abusive – ai sensi degli articoli L.212-1, R.212-1, R.212-2 del Codice del Consumo – tutte quelle clausole che creano un disequilibrio tra i diritti e i doveri delle parti contrattuali.

In particolare, il *Tribunale* mette in evidenza come la clausola n.10. (nelle versioni del 2015 e del 2017) avente ad oggetto le modalità di risoluzione delle controversie, determinasse, per gli abbonati residenti nell'Unione europea, l'applicazione alle controversie del diritto Lussemburgese (versione del 2015) ovvero di quello americano (versione del 2017), prevedendo, tra l'altro, un dettagliatissimo e complesso percorso stragiudiziale "obbligatorio" da seguire prima di rivolgersi eventualmente all'autorità giudiziaria competente che, ad ogni modo, non veniva in alcun modo indicata.

Nello specifico, a partire dal 2017 gli utenti residenti nell'Unione europea, nonché quelli francesi, avrebbero dovuto applicare il diritto americano, stando alla lettera della clausola di cui si discorre.

Sottolinea il *Tribunale* che in caso di controversia internazionale, essendo il fornitore domiciliato fuori dall'Unione europea, si sarebbero dovute applicare le norme di *"diritto comune"*. Tuttavia, nulla nella clausola n.10 lasciava intendere all'utente francese di dover far riferimento a tali disposizioni per quanto concerne la giurisdizione competente.

Il giudice *h*a quindi ritenuto la clausola n.10 illecita in rapporto all'articolo R-111-2 8) del Codice del Consumo che obbliga il fornitore del servizio a comunicare l'autorità giurisdizionale competente e la legge applicabile.

In ogni caso, inoltre, il *Tribunale* chiarisce che in base al diritto francese [1] l'attore/consumatore può comunque adire i tribunali francesi se la consegna effettiva della cosa o l'esecuzione della prestazione dei servizi è effettuata in Francia, anche se parte resistente sia stabilita fuori dall'Unione europea.

Parimenti l'art. 18 par. 1 del regolamento 1215/2012 del 12 dicembre 2012 (regolamento Bruxelles 1 bis) afferma che il consumatore può adire la giurisdizione del luogo in cui dimorava al momento della conclusione del contratto o dell'evento dannoso.

Quanto alla legge applicabile, invocando l'art. 6,1 e 2 del Regolamento europeo 593/2008 (c.d. Roma I), il *Tribunale* afferma che: a) si applica la legge dello Stato in cui il consumatore ha residenza abituale se le attività del professionista sono effettuate nel, o dirette verso, tale Stato; b) ovvero, in deroga a tale principio, la legge scelta dalle parti purché ricorrano le condizioni appena menzionate e comunque *tale scelta non vale a privare il consumatore della protezione assicuratagli dalle disposizioni alle quali non è permesso derogare convenzionalmente ai sensi della legge che, in mancanza di scelta, sarebbe stata applicabile a norma del paragrafo 1.*

*I*n base a ciò, il *Tribunale c*hiarisce che il consumatore non può essere privato della tutela posta dallo Stato membro dell'Unione in applicazione della direttiva 93/13/CEE [2] concernente le clausole abusive nei contratti stipulati coi consumatori, essendo in essere quel "legame stretto" tra contratto e luogo di residenza del consumatore.

Sia l'assenza di informazione sulla giurisdizione competente, sia quella concernente la legge applicabile, sia la previsione di una mediazione obbligatoria e preventiva rispetto al ricorso davanti al giudice, configurano così l'ipotesi di illiceità della clausola in relazione alle norme poste a tutela dei consumatori det-

[1] V. art. 46 del code de procédure civile, primo comma.

[2] V. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:31993L0013&from=EN.

tate dal Codice del Consumo francese, poiché creano un disequilibrio significativo tra i diritti e i doveri delle parti contrattuali ed un ostacolo all'esercizio d'azione.

Simili rilievi sono mossi avverso altre clausole dell'Accordo che evidentemente apportano uno squilibrio tra le parti contrattuali, vale a dire: a) le clausole n. 1 e 4 dell'Accordo di Sottoscrizione Steam, sull'esonero da responsabilità in favore della società Valve circa i danni derivanti dall'utilizzo della piattaforma e dell'*account* personale dell'abbonato, clausola che si presume illecita in base al citato articolo R-212-1 6) del Codice del Consumo; b) la clausola 3.C relativa al "Portafoglio Steam", illecita sotto più profili e, in particolare, poiché prevede, contrariamente al disposto dell'articolo R-212-1 1) e 4) del Codice del Consumo, la possibilità di modifica unilaterale da parte del professionista delle condizioni relative alla durata e alle caratteristiche del servizio.

3.2. Sulla violazione delle norme a tutela dei dati personali

Preventivamente, vale segnalare che la società Valve contestava la qualificazione da parte dell'associazione UFC – Que Choisir della *"Privacy Policy" q*uale vero e proprio "accordo" tra la società e gli abbonati alla piattaforma; essa affermava, infatti, che non si trattasse di un contratto, bensì di un "documento informativo". Per tale ragione, in base al Codice del Consumo – che prevede la possibilità per alcune associazioni di poter agire in giudizio a tutela degli interessi dei consumatori sottoscrittori di un contratto con un professionista – secondo Valve, l'associazione UFC – Que Choisir non sarebbe stata legittimata ad agire a tutela degli interessi dei consumatori chiedendo la soppressione delle clausole ritenute abusive e/o illegittime rispetto alla normativa europea e nazionale sulla protezione dei dati personali delle persone fisiche.

Al contrario, però, il *Tribunale* ritiene che l'associazione UFC – Que Choisir non soltanto sia dotata dei requisiti richiesti dal Codice del Consumo [3] per chiedere ed ottenere la cessazione o l'interdizione di comportamenti illeciti nonché la soppressione delle clausole abusive e/o illecite di qualsiasi contratto diretto ai consumatori ma che, stando ad una attenta analisi dell'articolo 1-B dell'Accordo di Sottoscrizione Steam (in tutte le sue versioni), si possa evincere dalla documentazione prodotta che la *Privacy Policy* costituisca parte integrante delle condizioni generali di utilizzo della piattaforma (il giudice osserva che nel documento si legge: "*Le Condizioni di Sottoscrizione, le Regole di utilizzo e la Politica di protezione della vita privata vincolano l'utilizzatore dal momento in cui*

[3] Articoli L. 621-1; L.621-7 *Code de la Consommation*.

questi manifesti il consenso …"), potendosi qualificare tale documento quale avente natura contrattuale, ai sensi dell'art. 1101 del Codice Civile francese.

Pertanto, in ossequio alle norme di cui al Codice del Consumo, è ben possibile per l'associazione UFC – Que Choisir agire per ottenere la soppressione delle clausole abusive e/o illecite quali, appunto, quelle contrarie alle disposizioni di cui al GDPR ed alla Legge Informatica e Libertà. Tuttavia, il giudice chiarisce che l'azione concessa alle associazioni si limita alla soppressione della clausola illecita o abusiva e non comprende la possibilità per queste di richiedere una "messa in conformità" di un contratto concluso tra consumatore e professionista. Per questo motivo rigetta la richiesta di adeguamento delle clausole contrattuali affette da vizio.

L'analisi del *Tribunale s*i concentra, allora, sulla valutazione circa la liceità di alcune clausole e la relativa decisione di ritenerle non apposte: a) in particolare esso dichiara abusiva ai sensi dell'art. 212-1 4) del Codice del Consumo la clausola n. 3.8 che rinvia *"alla legge applicabile sull'e-mail marketing" p*er l'individuazione dei casi in cui i dati possono essere raccolti a scopo di *marketing.* Una previsione, questa, ritenuta inadeguata e poco chiara in quanto non consente all'utente medio di comprendere in quali casi i propri dati personali verranno raccolti a fini di *makreting;* b) In considerazione del fatto che l'art. 46 del GDPR dispone che "*il titolare del trattamento ... può trasferire dati personali verso un paese terzo ... solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi*" e che l'art. 68 della Legge Informatica e Libertà vieti il trasferimento di dati personali verso un paese situato fuori dall'Unione europea in assenza di *"un livello di tutela adeguato", i*l *Tribunale g*iudica abusiva la clausola n. 9 *della Privacy Policy. T*ale clausola è infatti in grado di dissuadere il consumatore dall'agire in giudizio a tutela dei propri diritti concernenti il trattamento dei propri dati personali, poiché prospetta una competenza della *Federal Trade Commission d*egli Stati Uniti d'America in caso di lite, senza specificare che in base all'art. 13,2 d) del GDPR il consumatore avrebbe potuto semplicemente adire l'autorità di controllo competente (nello specifico, la CNIL [4] per i residenti in Francia), di fatto determinando la clausola in oggetto uno squilibrio tra i diritti e i doveri delle parti contrattuali; c) altresì illecite ed abusive sono considerate le clausole nn.8; 3.6 e 3.7 della *Privacy Policy* con riferimento alle disposizioni di cui alla Legge Informatica e Libertà, agli articoli 4 e 5 del GDPR ed al Codice del Consumo. Tali clausole, concernenti l'accesso ai propri dati personali e l'uso di *cookies, pixel* o altri strumenti di raccolta dati e tracciamento anche di terze parti (come *Google Analytics)*, sono state dichiarate illecite dal *Tribunale* in quanto, in pri-

[4] *Commission nationale de l'informatique et des libertés*.

ma analisi, Valve limita ai soli abbonati la possibilità di accedere ai propri dati personali e ottenerne la modifica o la cancellazione, lasciando i semplici visitatori sprovvisti di tali facoltà; in secondo luogo perché, essendo i *cookies* strumenti tecnici utili al buon funzionamento del sito e ad un'ottimale fruizione dei servizi, ma anche molto usati a scopo di analisi e *marketing,* essi possono essere installati sul dispositivo dell'utente solo raccogliendo previamente il consenso dello stesso al trattamento dei propri dati raccolti tramite questi piccoli *file* – consenso che deve essere una manifestazione di volontà chiara, libera, specifica, informata e inequivocabile ai sensi dell'art. 4 11) del GDPR – ed il loro uso e le finalità di tale trattamento – che deve rispondere ai principi di liceità, correttezza e trasparenza ai sensi dell'art. 5.1 GDPR – devono essere indicati in maniera chiara e specifica, non potendo risultare dalle sole condizioni generali di contratto, ciò anche a tutela degli utenti non sottoscrittori.

3.3. Sulla violazione delle regole che disciplinano la proprietà intellettuale

Ultimo profilo affrontato dal *Tribunale* in questa complessa controversia è stato quello concernente l'applicabilità della normativa europea sul diritto d'autore e sui programmi per elaboratore (direttive 2001/29/CE e 2009/24/CE) al *videogame* scaricato dall'utente e poi rivenduto.

Il Tribunale dichiara illecita la clausola 1.C dell'Accordo di Sottoscrizione con riguardo alle disposizioni previste dalle norme sopracitate e, dunque, applicabile il principio di esaurimento del diritto d'autore al programma scaricato con *download.* Il giudice chiarisce che pur usando l'espressione "abbonamento" alla piattaforma, invero, si realizzano due distinte fattispecie: la vendita di un esemplare del *videogame* (essendo il gioco pagato anticipatamente in un'unica soluzione e messo a disposizione dell'abbonato per un tempo illimitato) e, collateralmente, l'abbonamento ai servizi. L'esaurimento del diritto di distribuzione si applica, secondo il ragionamento del giudice, qualsiasi sia il modo di distribuzione del *videogame*, come quello consistente nell'immissione sul mercato per *download.* Di conseguenza, il titolare del diritto interessato non può opporsi alla rivendita di questa copia (o esemplare), nonostante l'esistenza di disposizioni contrattuali che vietino una cessione ulteriore.

4. Conclusioni

Con questa complessa sentenza il giudice di primo grado francese fornisce un nitido contributo alla ricostruzione dell'impalcatura normativa all'interno

della quale è possibile costruire rapporti contrattuali che garantiscano il rispetto della disciplina posta a tutela dei consumatori anche, e soprattutto, con riferimento ai contratti ad oggetto digitale stipulati tra consumatore residente nell'Unione europea e professionista stabilito in un paese *extra*-U.E., offrendo un'ottima risorsa interpretativa anche per il giurista italiano.

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA NOWAK, C-434/16, ECLI:EU:C:2017:994

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Un ciudadano, al amparo de la Ley de protección de datos de Irlanda solicitó el acceso a todos los datos personales que constaban en los distintos exámenes escritos que este último había realizado durante el proceso selectico de oposición al que se había sometido. Ante tal solicitud, tanto la autoridad pública encargada del proceso de oposición, como la Autoridad de Control se niegan a facilitarle tales datos al entender que los datos contenidos en un examen no contienen datos personales a efectos de la Directiva 95/46 (FJ 18 a 21).

Cuestiones claves del asunto:

A) Datos personales. Respuestas de un examen:

El TJUE en este caso valora si las respuestas contenidas en un examen son como tal dato personal a efectos de la Directiva 95/46.

Pues bien, el TJUE parte de la premisa de que el concepto de datos personales establecido en el Art 2.a) evidencia un concepto cuyo significado ha de ser muy amplio, pudiendo abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión (FJ 34 y 35). En elcaso analizado, el TJUE llega a la conclusión de que las respuestas de un examen realizadas por el evaluado son consideradas dato personal a efectos de la Directiva.

Ello es así porque:

- El contenido de tales respuestas revela el nivel de conocimientos y el grado de competencia del aspirante en un área determinada, así como en su caso, el proceso de reflexión, el discernimiento y la capacidad de análisis del propio aspirante. Además, si el examen está escrito a mano, las respuestas contienen también información caligráfica (FJ 37).

- Mediante la obtención de las respuestas se pretende valorar la capacidad profesional del aspirante y su aptitud para ejercer el oficio de que se trate (FJ 38 y 41).
- La utilización de los referidos datos, que se manifiesta, en particular, en el éxito o el fracaso del aspirante en el examen en cuestión, puede tener efectos en sus derechos e intereses, ya que, por ejemplo, puede condicionar sus oportunidades de acceder a la profesión o empleo al que aspira o influir en esas oportunidades (FJ 39).

Por consiguiente, se ha de entender que las respuestas escritas proporcionadas por un aspirante en un examen profesional son datos relacionados con su persona (FJ 36), además, las anotaciones del examinador sobre las respuestas del aspirante, también han de considerarse datos personales del evaluado (FJ 42 y 44), ya que el contenido de esas anotaciones expresa la opinión o valoración del examinador sobre los resultados individuales del aspirante en el examen y, en particular, sobre sus conocimientos y competencias en el área de que se trate (FJ 43) Pudiendo ser esas anotaciones también datos personales del examinador (FJ 44).

B) Derecho de acceso y rectificación:

Se parte de la premisa de que un aspirante que participa en el examen tiene un interés legítimo en poder oponerse a que sus respuestas al examen y las correspondientes anotaciones del examinador sean utilizadas fuera del procedimiento de examen y a que, en particular, se comuniquen a terceros – o incluso sean publicadas – sin su consentimiento (FJ 50).

Pues bien, por lo que se refiere al ***derecho de acceso***, el TJUE viene a indicar que el aspirante que ha realizado dicho examen puede ejercer tal derecho, ya que las respuestas escritas de un aspirante en un examen profesional y en su caso las anotaciones del evaluador pueden someterse una comprobación de la exactitud y en su caso la necesidad de conservación a efectos del Art 6. d) y e). Directiva 95/46 (FJ 26). Sirviendo así al objetivo de garantizar la protección del derecho a la intimidad del aspirante en lo que respecta al tratamiento de sus datos, y ello con independencia de si el aspirante tiene o no ese derecho de acceso también en virtud de la normativa nacional aplicable al procedimiento de examen (FJ 56).

De esta manera, el citado derecho de acceso se muestra indispensable, en particular, para permitir al interesado obtener en su caso del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de esos datos (FJ 57).

Respecto al ***derecho de rectificación***, como es lógico, este derecho no permite obviamente a un aspirante ampararse en él para «rectificar» *a posteriori* las

respuestas «incorrectas» (FJ 52). Ahora bien, es posible que se den situaciones en las que las respuestas de un aspirante en un examen y las correspondientes anotaciones del examinador sean inexactas, en el sentido del artículo 6, apartado 1, letra d), de la Directiva 95/46; por ejemplo, cuando por error, las hojas de los exámenes se hayan entremezclado de tal modo que las respuestas de otro aspirante se hayan atribuido al aspirante afectado, o cuando se haya perdido una parte de los folios que contienen las respuestas de ese referentes aspirante. (FJ 54), permitiendo en estos supuestos ejercer dicho derecho de rectificación.

Por último, por lo que se refiere ***al derecho de supresión***, no se puede descartar que el evaluado tenga derecho a solicitar al responsable del tratamiento de datos dicho derecho de supresión, ya que, transcurrido un determinado período de tiempo, puedan en su caso suprimirse las respuestas del examen y las correspondientes anotaciones del examinador, es decir, que se destruyan (FJ 55).

Decisión Final:

En definitiva, las respuestas por escrito realizadas por un aspirante en un examen profesional y las eventuales anotaciones del examinador a esas respuestas son datos personales (FJ 62). Además, dicho aspirante podrá en su caso ejercer los siguientes derechos.

• Derecho de acceso: Para en su caso comprobar la exactitud de dichos datos personales (respuestas de examen y anotaciones del examinador), así como la necesidad de conservación de tales datos.

• Derecho de rectificación: Partiendo de la premisa de que dicho derecho no pueda comprender una facultad para cambiar las respuestas del examen incorrectas, si puedan en su caso valorarse la rectificación de tales datos en los casos señalados anteriormente.

• Derecho de supresión: En relación a la destrucción de tales datos una vez haya transcurrido un determinado periodo de tiempo.

Artículos implicados del REPD:

Art 4.1, Art 15, Art 16 y Art 17.

Apartado concreto del Temario:

1.2.2, 1.5.2.

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA PUŠKÁR, C-73/16, ECLI:EU:C:2017:725

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Un ciudadano solicita que se elimine su nombre de una lista de personas consideradas testaferros elaborada por la Dirección de Tributos en el contexto de la recaudación y cuya actualización es realizada tanto por la propia Dirección, como por otras dos entidades más. El Tribunal Supremo eslovaco solicita que se estudie el problema a la luz del derecho de la UE en relación a la protección de datos.

Cuestiones claves del asunto:

A) Datos personales y tratamiento. Lista de testaferros.

El TJUE entiende que los datos referidos a una lista de personas considerados testaferros ha de ser considerado un dato personal a la luz de la Directiva y además el tratamiento de dichos datos también ha de considerarse como tal (FJ 33 y 34).

B) Elaboración de listas sin que medie consentimiento. Licitud del tratamiento:

El TJUE considera que, la elaboración de una lista con fines recaudatorios y de lucha contra el fraude es un tratamiento de datos que está legitimado, en la medida que dicho tratamiento es realizado para el cumplimiento de una misión de interés público (FJ 107 y 108), así, el Art 7.a) de la Directiva legitima a las autoridades al tratamiento de datos si dicho tratamiento *es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos* (FJ 106). Como en este caso parece ocurrir.

Decisión Final:

La Directiva 95/46 no se opone a que, sin que medie el consentimiento de los interesados, las autoridades de los Estados miembros traten datos personales a efectos de recaudación y de lucha contra el fraude fiscal, siempre que (FJ 117).

A) Por un lado:

• La normativa nacional confiera a dichas autoridades, a efectos de la disposición mencionada, misiones de interés público.

• La elaboración de la lista y la inclusión en la misma de los interesados sean efectivamente idóneas y necesarias para cumplir los objetivos perseguidos y.

• Existan motivos suficientes para presumir que la inclusión de los interesados en la lista obedece a un motivo.

B) Por otro lado: concurran todas las condiciones y exigencias establecidas en la Directiva 95/46 respecto a la licitud del tratamiento de datos personales.

Artículos implicados del REPD:

Concepto datos personales y tratamiento: Art 4. 1) y 4.2).
Licitud del tratamiento: Art 6.1 e).

Apartado concreto del Temario: 1.2.2, 1.3.2.

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA RĪGAS SATIKSME, C-13/16, ECLI:EU:C:2017:336

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Se produce un accidente en el que se ven involucrados un pasajero que se baja de un taxi y un trolebús que arroya la puerta de dicho taxi una vez que el ciudadano abre la puerta. Del atestado se infiere que el culpable fue el pasajero del taxi. La empresa municipal de trolebús dirige acción de daños y perjuicios contra la aseguradora del taxista, esta última se opone al señalar que la culpa es del cliente del taxi cuando se baja y no del taxista. Ello lleva a la empresa municipal de trolebús a solicitar a la policía municipal los datos identificativos del causante del accidente para en su caso interponer las acciones judiciales correspondiente frente a tal persona. La policía municipal solo entrega parte de los datos solicitados. Por lo que la empresa de Trolebús impugna tal decisión (FJ 2 y 12 a 20).

Cuestiones claves del asunto:

A) Licitud del tratamiento. Plantear una recurso judicial:

El TJUE analiza si la entrega de datos identificativos (Número de identificación y domicilio) sobre una persona por parte de la policía hacia una empresa que pretende ejercer una acción judicial frente a esa persona se encuadra dentro de uno de los supuestos que la ley legitima para un tratamiento de datos. Concretamente, dicho supuesto se refiere al contenido en el Art 7 f) de la Directiva (FJ 24). Este artículo legitima el tratamiento de datos cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezcan el interés o los derechos y libertades fundamentales del interesado (FJ 25).

Para el TJUE, del contenido de esa disposición no se extrae la existencia de una obligación por la cual la policía haya de comunicar dichos datos a los terceros (Empresa de Trolebús), pero tampoco, la Directiva se opone a que en su caso se realice tal comunicación (FJ 26 Y 27).

Por tanto, para valorar en su caso si dicho tratamiento es "necesario", el artículo 7, letra f), de la Directiva 95/46 fija tres requisitos acumulativos para que el tratamiento de datos personales resulte lícito (FJ 28):

- 1. Que el responsable del tratamiento o el tercero o terceros a quienes se comuniquen los datos persigan un interés legítimo. En este sentido, no cabe duda de que el interés de un tercero en obtener información personal de quien haya causado un daño en un bien de su propiedad a fin de demandarlo por daños y perjuicios constituye un interés legítimo (FJ 29)
- 2. Que el tratamiento sea necesario para la satisfacción de ese interés legítimo: Esta claro que resulta necesario para plantear la demanda obtener el domicilio y número de identificación o al menos uno de esos dos datos (FJ 30).
- 3. Que no prevalezcan los derechos y libertades fundamentales del interesado en la protección de los datos. En cuanto al requisito de la ponderación de los derechos e intereses en conflicto, ésta dependerá, en principio, de las circunstancias concretas del caso particular de que se trate (FJ 31). Así, entre las circunstancias que pueden ser valorables destaca el hecho de que dichos datos ya estén disponibles al público (FJ 32) o en su caso el interesado sea un menor (FJ 33). En este caso, esa última circunstancia es irrelevante.

Decision final:

El TJUE considera que no existe obligación de comunicar datos personales a un tercero para que éste último pueda interponer una demanda indemnizatoria en vía civil por los daños que haya causado el interesado en la protección de dichos datos. Aunque tampoco nada impide a que en su caso se produzca tal comunicación (FJ.34). Debiendo en su caso valorarse las exigencias previamente señaladas (FJ 28 a 33).

Artículos implicados del REPD: Art 6.1 f).

Apartado concreto del Temario: 1.3.2.

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

SENTENCIA MANNI, C-398/15, ECLI:EU:C:2017:197

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Un ciudadano (Sr. Manni) es el administrador único de la Sociedad Italiana Costruzioni Srl, dicha sociedad fue adjudicataria de un contrato para la construcción de un complejo turístico. Dicho ciudadano aparece en el Registro de Sociedades como administrador único de una sociedad declarada en concurso de acreedores en 1992. Este ciudadano solicita a la Cámara de Comercio que cancele o en su caso haga anónimos tales datos, ya que entiende que a causa de la publicidad de tales datos, su complejo de viviendas no se vende. Ante esta solicitud, la Cámara de Comercio se niega a cancelar tales datos (FJ 23 a 28).

Cuestiones claves del asunto:

A) Limitación del plazo de conservación:

Lo que trata de dilucidar el TJUE en este asunto es, si la autoridad responsable de la llevanza del registro debe, al expirar un plazo determinado tras el cese de actividades de una sociedad y a petición del interesado, eliminar o hacer anónimos estos datos personales, o limitar en su caso la publicidad de estos, y, si se desprende tal obligación de la Directiva de protección de datos (FJ 44).

Pues bien, para resolver el asunto, en primer lugar, el TJUE indaga en conocer cuál es la finalidad que ha llevado al Registro a tratar dichos datos personales y a la publicación de estos (FJ 48). Así, entre las finalidades que se encuentran latentes a la hora de publicar estos datos en el registro destacan:

- La protección de los intereses de terceros en relación con las sociedades anónimas y las sociedades de responsabilidad limitada. A tal fin, la publicidad debe permitir a los terceros conocer los actos esenciales de la sociedad y ciertas indicaciones relativas a ella, concretamente la identidad de las personas que tienen el poder de obligarla (FJ 49). Sin que dichos terceros interesados deban jus-

tificar la existencia de un derecho o interés legítimo que necesite de protección (FJ 51).

- Garantizar la seguridad jurídica en las relaciones entre las sociedades y los terceros desde la perspectiva de una intensificación del tráfico mercantil entre los Estados miembros (FJ 50).

Señaladas algunas de las finalidades por las que se publican dichos datos y en su caso el tiempo de conversación de estos en el registro, el TJUE llega a la conclusión de que, debido al conjunto de derechos e intereses legítimos que pueden subsistir respecto de terceros una vez que se liquida una sociedad (FJ 53), y a la heterogeneidad de plazos de prescripción del ejercicio de estos derechos previstos en las distintas legislaciones de los países de la UE, resulta imposible establecer un plazo unánime y máximo de publicidad de tales datos por entenderse que ya no son necesarios (FJ 55), debiendo ser los EEMM los que en su caso puedan apreciar o no la existencia de unos plazos mayores o menores (FJ 61), o los propios tribunales nacionales teniendo en cuenta las circunstancias concretas del caso (FJ 62).

B) Derecho de supresión o cancelación:

Por consiguiente, dador que no se puede garantizar un plazo máximo de conservación (publicidad de los datos en el Registro) en relación al principio de conservación de los datos Art 6.1 e), tampoco se puede en su caso garantizar el derecho de supresión o cancelación de los datos establecidos en dicho Registro Público una vez que haya transcurrido un determinado plazo desde la liquidación de dicha sociedad (FJ 56).

Decisión Final:

Debido al estado actual del Derecho de la Unión, deben de ser los Estados miembros los que determinen si las personas físicas cuyos datos aparecen publicados en el Registro analizado, pueden solicitar a la autoridad responsable de dicho registro que comprueben si está excepcionalmente justificado, por razones preponderantes y legítimas relacionadas con su situación particular, limitar, al expirar un plazo suficientemente largo tras la disolución de la empresa de que se trate, el acceso a los datos personales que les conciernen, inscritos en dicho registro, a los terceros que justifiquen un interés específico en la consulta de dichos datos (FJ 64).

Artículos implicados del REPD: Art 5.1 e) (limitación del plazo de conservación) y Art 21 (Derecho de oposición).

Apartado concreto del Temario: 1.3 y 1.5.3.

SENTENCIAS DEL TRIBUNAL SUPREMO (SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO) STS CA.NO RECURSO 3068-2015 FECHA 14-11-2016

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Determinados hechos referidos a un particular son publicados a través de un medio de comunicación, así como en el boletín oficial de la Guardia Civil. En dichos hechos se hace referencia a una serie de datos personales de dicho particular. Es por ello que dicho ciudadano, y en virtud de la normativa sobre protección de datos, solicita a la AEPD que obligue a estos medios a que proceden a la retirada de tales publicaciones. La AEPD deniega tal petición, siendo esta resolución recurrida ante los tribunales.

Cuestiones claves del asunto:

A) Protección de datos vs Libertad de Expresión.

En este caso, el Tribunal Supremo realiza un juicio de proporcionalidad para valorar si la publicación de dichos datos por parte del medio de comunicación y la guardia civil vulneran el derecho a la protección de datos. Así, el TS llega a la conclusión de que no ha existido la alegada vulneración del derecho fundamental a la protección de datos debido a que:

• La publicación periodística se enmarca dentro de lo que constituía la noticia.
• La noticia se refería a una persona con relevancia pública, no por ser como tal político, pero si por realizar actividades vinculada a las propias funciones que se desarrollan por determinadas personas que se incardinan en esa actuación de carácter público.
• No se ha probado que la noticia no sea veraz.
• A ello hay que añadirle además la relevancia constitucional que tienen los derechos de información y de expresión y más concretamente en relación al papel preponderante que juegan los medios de comunicación en una sociedad democrática (FJ 3o).

Decisión Final:

La publicación de una noticia donde aparecen determinados datos de carácter personal de un individuo no supone la vulneración del derecho a la protección de datos, dicha información era de relevancia pública y no se ha demostrado que no fuera veraz.

Artículos implicados del REPD: Art 85. Considerando 153, 65.

Apartado concreto del Temario: 1.5.7.

SENTENCIAS DEL TRIBUNAL SUPREMO-SALA DE LO CIVIL

SENTENCIA TRIBUNAL SUPREMO SALA DE LO CIVIL 609/2015 DE 12 DE NOVIEMBRE

María Bocio Jaramillo

Assistant Researcher at Seville University

Cuestiones de hecho:

En el caso planteado ante nuestro Tribunal Supremo encontramos como el apelante D. Humberto, había interpuesto demanda contra una empresa de construcción conocida como Cotronic por la que solicitó que se declarasen vulnerados sus derechos al honor, a la propia imagen y a la protección de datos. El supuesto es relativo a que Cotronic, que es una subcontrata de Telefónica S.A, había despedido al demandante por haber cobrado supuestamente a un cliente por una operación que era gratuita. Aun sin haber podido demostrar aquello, se procede a su despido. El recurrente comienza la búsqueda de un nuevo trabajo, pero una de las empresas le comunica que sus datos aparecen en un fichero de personal conflictivo al que fue incorporado por Telefónica.

Ante ello, presenta la demanda respectiva que le es desestimada tanto en primera instancia como ante la Audiencia al considerar no probado la existencia de dicho fichero respectivo.

Cuestiones claves y fundamentos de derecho:

Una vez determinado por el tribunal que ha existido un error en la carga de la prueba ya que la demandada debería de haber probado la no existencia del fichero del que existía un principio de prueba sobre su existencia, pasa a determinar si ha existido una vulneración o no del derecho a la protección de datos.

La cesión de datos debe ser trasmitida con el consentimiento del afectado y esto solo se excluye en los casos del artículo 11.2 LOPD. Por otro lado, los datos reflejados en ese fichero no eran veraces debido a que su inclusión se atribuyó a un hecho que no resulto probado.

Continúa el tribunal determinando que se ha producido una infracción al derecho a la protección de datos reconocido constitucionalmente por nuestro TC

en sentencias como la STC 292/2000 de 30 de noviembre. Esto ha conllevado a una infracción del derecho al honor ya que se produjo la afectación de su reputación (FJ 4o).

Valoración final:

Se determina que ha existido una vulneración del artículo 18 CE, en cuanto al honor del demandante, al comunicarse hechos no veraces que afectaban a su reputación y una infracción del derecho a la protección de datos ya que existió una cesión ilícita. En este sentido puede el demandante pedir la cancelación de estos datos en dicho fichero (FJ 4o).

Artículos del REPD: Artículo 6,7 y Considerando 42.

Apartado concreto del temario: 1.4.1. El consentimiento: otorgamiento y revocación.

SENTENCIAS DEL TRIBUNAL SUPREMO (SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO) STS CA. NO RECURSO 2538-2015 DE 02-11-2016

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Un ciudadano ejercita su derecho de cancelación en relación a unos datos personales que constaban en una determinada página web. El responsable de esa página web se niega a cancelar dichos datos, ante esta situación, la AEPD emite resolución obligando a dicho responsable de la página web a que proceda a la cancelación de dichos datos, imponiendo con ello una sanción. Está sanción es recurrida ante los tribunales.

Cuestiones claves del asunto:

A) Libertad de expresión vs Derecho a la protección de datos. Derecho de cancelación:

Para el recurrente en casación, esto es, el responsable de la página web, la sanción que le ha impuesto la AEPD ha vulnerado su derecho a la libertad de expresión.

Ante tal alegación, el TS indica que a la hora de valorar si la libertad de expresión supone una excepción legítima al derecho a la protección de datos en general, y al derecho de cancelación en particular, se requiere de un juicio de proporcionalidad de dicha medida por la que se limita o no se permite al interesado ejercer su derecho de cancelación.

El TS, en este caso, si bien considera que el recurrente ha hecho alusión a la existencia de confrontación de estos dos derechos fundamentales, no ha explicado en que medida se ha vulnerado tal juicio de proporcionalidad realizado por la Agencia y por la sala de instancia una vez revisada tal decisión. Además, el titular de la página web, tampoco ha acreditado en que medida resultaba necesario la cita concreta de los datos personales del interesado una vez que este último ha ejercido su derecho de cancelación. Sin que baste como

se ha dicho antes la mera invocación de sus derechos fundamentales a la libertad de información o de expresión de forma más o menos argumentada, pero en todo caso genérica e inconcreta (FJ 2o).

B) Derecho cancelación de datos. Límites. Publicidad de las resoluciones judiciales

Se valora por parte del TS la argumentación señalada por la parte recurrente al indicar que: los datos obtenidos y que se han tratado en la página web proceden de colecciones legislativas, considerándose dichas fuentes como de acceso al público en el sentido del Art 3 LOPD, lo que permitiría en estos casos que dicho tratamiento no requiriera del consentimiento de los interesados, ni en su caso pudiera ejercer el derecho de cancelación.

Pues bien, dicho esto, el TS derrumba la argumentación señalada por la parte recurrente al señalar que ha quedado acreditado que los datos personales que se utilizaron por parte del recurrente, no constan en ninguna sentencia que haya sido publicada, y además, el propio tribunal indica que a día de hoy, no existe colección jurisprudencial alguna que contenga datos personales de los afectados en las sentencia en ellas publicadas, de manera que dichos datos no se han podido obtener de una determinada colección legislativa o jurisprudencial (FJ 3o).

Decisión Final:

El TS mantiene la sanción establecida por parte de la AEPD, así como la obligación de cancelar los datos del interesado, ya que:

• Por un lado, la parte recurrente no ha probado suficientemente la necesidad de mantener el tratamiento dichos datos una vez el interesado habían solicitado su cancelación, al haber justificado sus alegaciones en una mera alusión a los posibles derechos fundamentales vulnerados.

• Por otro lado, tampoco ha quedado probado que dichos datos fueran públicos por haber sido obtenidos de las colecciones legislativas, así, a día de hoy, dichas colecciones jurisprudenciales no establecen datos personales, ya que dichas sentencias aparecen anonimizadas.

Artículos implicados del REPD: Art 85, Considerando 153, Art 17.

Apartado concreto del Temario: 1.5.7 y 1.5.2

SENTENCIAS DEL TRIBUNAL SUPREMO
(SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO)
STS 4501/2016 - ECLI:ES:TS:2016:4501

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Una ciudadana ejercita su derecho de acceso en relación a los datos personales de ella que obran en de una entidad mercantil de seguros. Concretamente, solicita una copia de la póliza de seguros en virtud de tal derecho de acceso. La entidad mercantil se niega a concederle dicho documento, de manera que la ciudadana denunciar esta actitud de la aseguradora ante la AEPD. La AEPD desestima la petición de la ciudadana considerando que la petición de dichos documentos no forma parte del contenido del derecho de acceso proclamado en la LOPD, por lo que dicha ciudadana recurre tal decisión de la AEPD ante los tribunales.

Cuestiones claves del asunto:

A) Derecho de acceso. Póliza del seguro:

El TS pasa a valorar si la póliza de seguro es un documento que deba de entregarse por parte de una aseguradora fundamentado en el derecho de acceso reconocido en el Art 15 LOPD. Pues bien, para el TS, esta ciudadana, al exigir que la aseguradora le facilite una fotocopia de una póliza de seguro, no esta ejerciendo como tal el derecho de acceso proclamado en la normativa de protección de datos. Ya que, el contenido de dicho derecho no comprende el documento en el que están incluidos en su caso los datos personales (que en este caso están contenidos en la póliza del seguro), sino que comprende el acceso a los datos personales que tenga en su posesión tal aseguradora (FJ 4o). Debiendo en su caso la aseguradora facilitar dichos datos (como en este caso hizo).

Además, existen otros cauces legales para exigir tal entrega de dicha póliza, sin que sea necesario acudir al derecho de acceso proclamado por la normativa en materia de protección de datos (FJ 4o *in fine*).

Decisión Final:

La exigencia de una póliza de seguro a una aseguradora por parte de una ciudadana no se encuadra dentro del contenido del derecho de acceso regulado en el Art 15 LOPD, ya que lo relevante en relación a este derecho no es el documento donde se incluyan tales datos, sino los datos que ostente tal aseguradora. Debiendo en su caso entregar tales datos personales en el documento o por el medio que la aseguradora estime oportuno.

En definitiva, el derecho de acceso proclamado en la normativa sobre protección de datos no puede suponer una vía o instrumento válido para obtener una copia de una póliza de seguros.

Artículos implicados del REPD: Art 15.

Apartado concreto del Temario: 1.5.2.

SENTENCIAS DEL TRIBUNAL SUPREMO
(SALA 3A DE LO CONTENCIOSO ADMINISTRATIVO)
STS 3721/2016 - ECLI:ES:TS:2016:3721

Adrián Palma Ortigosa
Assistant Researcher at Universidad de Sevilla

Hechos:

Ciudadano ejercita su derecho de cancelación frente a Google Spain, solicitando a dicha entidad que tome las medidas necesarias para evitar la indexación de los datos personales contenidos en determinadas páginas web relacionados con unos hechos acaecidos en los años 1993 y 1994 que dieron lugar a la incoación de un proceso penal que se dirigió contra el interesado, se pide por tanto que no aparezcan sus datos en dicho buscador. La AEPD, tras estudiar el asunto, emite resolución obligando Google Spain a la supresión de tales datos, dicha entidad se niega a cancelar dichos datos personales al entender que no es responsable a efectos de la normativa en materia de protección de datos, sino que sería Google Inc, sociedad radicada en EEUU.

Cuestiones claves del asunto:

A) Responsable del tratamiento. Corresponsabilidad en el Tratamiento:

Para situarnos correctamente en el asunto, cabe indicar que, el órgano judicial de instancia, esto es, la Sala de lo Contencioso Administrativo de la Audiencia Nacional de fecha 11 de junio de 2015 (FJ 1o) en el asunto que ahora conoce el TS, consideró que Google Spain era responsable a efectos de la normativa de protección de datos en base a dos razones esenciales (FJ 5o in fine):

• Primera: Google Spain, S.L. es ***corresponsable*** en el tratamiento de datos personales llevado a cabo en el marco del servicio de búsqueda en internet ofrecido por Google Inc. (gestor del motor de búsqueda) en razón de la unidad de negocio que conforman ambas sociedades. Así, la actividad desempeñada por Google Spain, S.L resulta indispensable para el funcionamiento del motor de búsqueda. (Google Search). El concierto de ambas sociedades en la prestación de tal servicio a los internautas lo hace viable económicamente y posibilita su subsistencia.

• Segunda: en aplicación de la doctrina de los actos propios, Google Spain, S.L. ha venido actuando como si fuese responsable del tratamiento de datos, tanto en procedimientos de tutela de derechos seguidos ante la Agencia Española de Protección de Datos como en diversas intervenciones ante tribunales españoles.

El Tribunal Supremo, si bien considera que tanto la Directiva 95/46/CE como LOPD posibilitan la corresponsabilidad en el tratamiento de los datos, a su vez entiende que, para que exista tal corresponsabilidad, se ha de exigir una coparticipación en la determinación de los fines y medios del tratamiento, no existiendo tal corresponsabilidad en el caso analizado. Así, para el TS, las actividades llevadas a cabo por Google Spain vinculadas a la promoción publicitaria del motor de búsqueda de Google Inc no alcanzan la corresponsabilidad mencionada.

En este sentido, el TS indica que es preciso determinar y acreditar en cada caso la existencia y el alcance de la participación de cada uno en la determinación de los fines y medios del tratamiento para que pueda hablarse de corresponsabilidad, lo que en modo alguno se ha producido en este caso respecto de Google Spain. Este planteamiento se confirma y precisa en el nuevo Reglamento (UE) 2016/679, que regula expresamente la corresponsabilidad en el tratamiento de datos, (Art 26). Desprendiéndose de dicho artículo dos elementos básicos que definen al corresponsable (FJ 7o):

• El primero: la efectiva participación en la determinación de los objetivos y los medios del tratamiento.

• El segundo: la delimitación de su concreta responsabilidad en el cumplimiento de las obligaciones impuestas por el Reglamento.

Decisión final:

Google Spain S.L no es un responsable a efectos de la normativa de protección de datos, ya que dicha entidad no es la encargada de establecer los fines y los medios del tratamiento de datos, sin que, como tal, la colaboración o auxilio en otras actividades de Google Spain S.L con Google Inc. impliquen corresponsabilidad en el tratamiento. La resolución de la AEPD debería de haberse dirigido frente a Google Inc. S.L y no frente a Google Spain.

Tener en cuenta la STS Sala 1a (civil) 1280/2016- ECLI: ES:TS: 2016:1280 FJ 3o que considera a Google Spain S.L como corresponsable del tratamiento.

Artículos implicados del REPD: Art 17, Art 24, 26, Considerando 79.

Apartado concreto del Temario: 1.5.2, 1.6.2.

SENTENCIA DEL TRIBUNAL SUPREMO SALA DE LO CIVIL 210/2016 DE 5 DE ABRIL

ECLI:ES:TS:2016:1280

María Bocio Jaramillo

Assistant Researcher at Seville University

Cuestiones de hecho:

Nos encontramos ante un caso donde a través del BOE, el 18 de septiembre de 1999, se publicó un RD de 27 de agosto de 1999 por el que se concedió el indulto de la pena privativa de libertad impuesta al Sr. Alfonso. El 8 de enero de 2009, el demandante, dedicado al sector de las telecomunicaciones, remite un correo electrónico al servicio de gestión del BOE para informarle que, desde hace años, aparece en el motor de búsqueda de Google insertando solo su nombre y apellidos apareciendo su página publicando el indulto en el resultado de búsquedas en primer lugar. El encargado del BOE contestó que la inclusión de los RD de indultos son actuaciones obligatorias en el BOE y lo que realiza la versión electrónica es una reproducción de la versión en papel. Alega que cualquier modificación de la misma supondría una alteración de datos prohibida por el artículo 3.j LOPD. Sin embargo, le comunicó que adoptaría las medidas necesarias para evitar la automatización de sus datos.

Con fecha de 5 de mayo remitió sendos correos a Google y Yahoo! alegando que, incluyendo su nombre y apellidos en los motores de búsqueda, aparecían como resultados informaciones de su vida pasada que afectaban a su derecho al honor, intimidad y propia imagen. Mientras Google contestó con una respuesta estándar, Yahoo! si requirió la ayuda del mismo para indicar que links eran los respectivos.

El 21 de abril de 2009, tiene entrada en la AEPD un escrito contras las 3 instituciones antes referidas. Posteriormente, remite el demandante a Google Madrid un burofax reiterando su problemática, remitiendo otros correos a principios de enero de 2010 a telefónica haciendo referencia a los buscadores Lycos y Terra con la misma cuestión.

El 19 de enero de 2011 el director de la AEPD estimó la reclamación contra Google y Yahoo! (aunque tuvo en cuenta la colaboración con el demandante de esta última) y desestimó la respectiva al BOE.

Posteriormente, incoó otra reclamación contra telefónica ante la AEPD que también fue estimada. Una vez producidas las reclamaciones vistas y estimadas, inició el correspondiente proceso ante los tribunales pertinentes debido a la infracción de sus derechos al honor, intimidad y propia imagen, además del derecho de poder retirar su información personal. Alega igualmente la vulneración de la LOPD en su artículo 19 y el artículo 17 de la Ley de Servicios de la Sociedad de la Información y correo electrónico.

En la fase ante la Audiencia se estiman sus pretensiones por lo que se interpone por Google recurso de casación ante el TS. Entre sus alegaciones se encuentran:

– La no legitimación pasiva de Google Spain ya que no es el responsable del buscador, sino que es Google Inc.

– Prevalencia del derecho de información frente a la protección de datos, en base al artículo 20.1.d CE, doctrina reiterada del TEDH, TJUE y tribunales nacionales.

– Aplicación del derecho al olvido en una situación donde aún no se había reconocido el mismo por el TJUE. Infracción de los artículos 9.3 CE y 19.1 LOPD.

Cuestiones claves y fundamentos de derecho:

1. Legitimación pasiva Google Spain (FJ3o):

Para ello, el tribunal recurre a la doctrina asentada en la STJUE conocida como caso Google. Parte de la definición que se contiene en la Directiva 1995/46/CE, de 24 octubre, del Parlamento Europeo y del Consejo de la Unión Europea, de protección de las personas físicas, de datos personales y a la libre circulación de estos datos en lo que respecta al tratamiento en el artículo 2, letra d) que define al responsable del tratamiento como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales". Por otro parte, acude a los fundamentos 42 a 60 de dicha sentencia.

En la sentencia mencionada, determinada la existencia de Google Search a la que se accede a través del dominio www.google.com, su versión española a través de Google Spain que es filial y tiene el objetivo de gestionar los espacios publicitarios de Google en España que se accede a través de dominio www.google.es y Google Inc, matriz de Google, con domicilio en EEUU, y que gestiona Google Search.

En todo momento considera a Google Spain como establecimiento de Google Inc. En este sentido, y frente a las alegaciones de que era Google Search el responsable del tratamiento de datos, el TJUE afirmó que la Directiva no

exige, para que sea aplicable el derecho nacional aprobado para su transposición, que el tratamiento de datos personales controvertido sea efectuado "por el propio establecimiento en cuestión, sino que se realice "en el marco de las actividades" de éste. "Habida cuenta de este objetivo de la Directiva y del tenor de su artículo 4, apartado 1, letra a), el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero (Google Inc) pero que dispone de un establecimiento en un Estado miembro(Google Spain), se efectúa «en el marco de las actividades» de dicho establecimiento si este está destinado a la promoción y venta". Considera responsable del tratamiento a la filial cuando "el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro" (FJ3o).

2. Derecho al olvido vs derecho a la información (FJo5):

El tribunal entiende que puede existir una confrontación entre el derecho a la protección de datos y el derecho a la información; hace referencia a la STJUE en el caso Brunet donde se establece la necesidad de garantías internas para que los datos recopilados y su tratamiento sean adecuados a la finalidad para la que se recogieron. Además, llama la atención de la necesidad de conservación de estos por un tiempo que no exceda del necesario para la finalidad para los que fueron registrados.

Es necesaria la existencia de una serie de fines para el tratamiento de dichos datos, y que se proteja su tratamiento con respecto a los mismos. Para ello incide en esta idea haciendo hincapié en el caso Google referente al siguiente argumento : "A tenor de este artículo 6 [de la Directiva] y sin perjuicio de las disposiciones específicas que los Estados miembros puedan establecer para el tratamiento con fines históricos, estadísticos o científicos, incumbe al responsable del tratamiento garantizar que los datos personales sean «tratados de manera leal y lícita», que sean «recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines», que sean «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente», que sean «exactos y, cuando sea necesario, actualizados», y, por último, que sean «conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente». En este marco, el mencionado responsable debe adoptar todas las medidas razonables para que los datos que

no responden a los requisitos de esta disposición sean suprimidos o rectificados".

Debido a ello debe de procederse a una ponderación entre el derecho de información y los datos publicados, y dicha ponderación se basará tanto en el carácter ofensivo como en la finalidad pública o interés público en que el indulto aparezca relacionado con sus datos personales en las búsquedas realizadas a través de Google.

Entiende que los datos recogidos deben cumplir con los principios de calidad desde que su recogida y durante todo el tratamiento de los mismos, principios como son proporcionalidad, exactitud, pertinencia y adecuación. Por ello, un tratamiento inicialmente justificado a la finalidad a la que tiende puede devenir posteriormente inadecuado con respecto a dicha finalidad y desproporcionado.

Considera que una vez que han transcurrido estos años, la finalidad con la que se recogieron dichos datos para el indulto ya ha sido cumplida en cuanto a la publicación del RD de indulto como exige la Ley. El hecho de una búsqueda realizada por cualquier finalidad, y no por el hecho de investigar sobre los indultos en España a través de Google, introduciendo solo datos personales como nombre y apellidos, sobrepasa la finalidad por la que fueron recogidos dichos datos y se considera que infringen sus derechos de la personalidad.

El derecho al olvido digital se concibe como: "Una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos. Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, "posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones.

De admitirse esta tesis, se perturbarían gravemente los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país. Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse a un tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su

persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad, inserción que se vería obstaculizada por el rechazo que determinadas informaciones pueden causar en sus conciudadanos" (FJo5).

3. El derecho al olvido digital es una concreción de los derechos que para los afectados se derivan del principio a la calidad de los datos en la normativa sobre protección de datos de carácter personal (FJo7):

Dispone el tribunal que el derecho al olvido digital no es una creación del TJUE, es una concreción de la interpretación que debe de darse a una serie de normas como: la Directiva 95/46 en cuanto a los requisitos de calidad del tratamiento, el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales cuya importancia en el derecho europeo resulta de los artículos 52 y 53 de la Carta de Derechos Fundamentales Europea.

Valoración final:

Debido a los argumentos anteriormente expuestos, el tribunal entiende que hay que reconocer un derecho al olvido digital frente a los motores de búsquedas y, aunque dicho derecho no es absoluto, debe ser proporcional y adecuado a la finalidad por la que se registraron los datos. Debido a las circunstancias presentes donde cualquier búsqueda indiscriminada a través de su nombre y apellidos aportaba la información del indulto, debe de entenderse que no se cumple la finalidad de la recogida y tratamiento de los datos y tampoco la proporcionalidad.

Artículos del repd: Artículos 5, 17, 85, Considerandos 50, 41, 153.

Apartado concreto del temario: 1.5.2 Acceso, rectificación, supresión(olvido), 1.11.3 criterios de órganos jurisdiccionales.

SENTENCIA DEL TRIBUNAL SUPREMO SALA DE LO CIVIL 114/2016 DE 1 DE MARZO

ECLI:ES:TS:2016:796

María Bocio Jaramillo
Assistant Researcher at Seville University

Cuestiones de hecho:

La empresa Abanca S.A concedió un préstamo hipotecario a la entidad Contratas Confer S.L. En dicho préstamo se constituyó como fiadora solidaria a la Sra. Evangelina. La deuda resultó impagada, por lo que Abanca requirió de pago a ambos deudores. Además, procedió a la inclusión de sus datos personales en el fichero de morosos(Badexcug) y a la Central de Información de Riesgos del Banco de España(CIRBE). Abanca llevó a cabo el proceso de ejecución hipotecaria contra ambos deudores, pero en dicho proceso, no se permitió acumular la acción real derivada de la ejecución del préstamo hipotecario contra Contratas Confer y la acción personal debido a su carácter de fiadora solidaria contra la Sra. Evangelina. Por ello, el proceso de ejecución hipotecaria solo se dirigió contra Contratas Confer. Ante dicha situación la Sra. Evangelina presenta demanda por intromisión en su derecho al honor del artículo 18 CE, desarrollado por la L.O 1/1982 de 5 de mayo, debido a la inclusión de sus datos personales en el registro de morosos y en CIRBE. Su argumento se basa en que no existe ninguna sentencia condenándola por la deuda y por ello no existe la veracidad de los datos exigidos en el artículo 4 LOPD para su posterior inclusión en los registros antes mencionados.

Cuestiones claves y fundamentos de derecho

1. Jurisprudencia de la Sala sobre el tratamiento de los datos en los ficheros de solvencia patrimonial

Conforme al artículo 4 LOPD, los datos deben ser exactos, adecuados, pertinentes y proporcionados a los fines para los cuales sean recogidos y tratados. Concretamente establece que: "la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, exige que los datos personales recogidos para su tratamiento sean

adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado, y prohíbe que sean usados para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos" (FJ 5o).

2. Calidad de datos en registros de morosos

El artículo 29 LOPD exige que, para la inclusión de los datos en dichos registros de morosos, estemos ante datos veraces con respecto a la situación que van a reflejar. Dicho artículo fue desarrollado por los artículos 38 y 39 del RPD. En dicho articulado se exige la existencia de deudas ciertas, vencidas y exigibles, la existencia de un previo requerimiento de pago y la información acerca de la posible inclusión de los datos en los registros sobre insolvencia (FJ 5o).

3. El principio de calidad de datos no se limita a exigir la veracidad de la deuda

Hace hincapié el tribunal en la idea de la existencia de datos que pueden ser ciertos y exactos sin ser pertinentes puesto no van a ser determinantes del enjuiciamiento de la solvencia económica de los interesados. Además, dicha solvencia no puede valorarse conforme a deudas de carácter dudoso, por ello, considera que no cabe la inclusión de deudas que sean dudosas o sometidas a litigio, basándose en una prueba documental para apoyar dicha litigiosidad de la deuda (FJ5o).

4. La transcendencia de la anulación parcial del Reglamento

La Sentencia del TS de la Sala Contenciosa-Administrativa de 15 de julio de 2010 anuló el inciso del artículo 38.1 RPD donde se exigía, para la inscripción en los registros aquí tratados, que no existiese reclamación judicial, arbitral o administrativa de la deuda.

Tras ello se consideró que: "ciertamente no es necesario que exista una sentencia que declare la existencia, cuantía y exigibilidad de la deuda para que los datos personales del deudor puedan ser comunicados a un registro de morosos, como tampoco lo era antes de que tal anulación se produjera" (FJ5o).

5. Consideración de CIRBE

Se entiende únicamente como registro administrativo y no como registro a los efectos del artículo 29.2LOPD (FJo5).

Decisión final:

No se requiere la condena judicial de la deuda para proceder a la inclusión de datos en el registro de morosos. En este sentido se cumple lo dispuesto en el artículo 29.4 LOPD sobre datos determinantes para enjuiciar la solvencia patrimonial de un sujeto. Por ello, en este caso la deuda era existente, cierta y exigible y susceptible de enjuiciar la solvencia de Doña Evangelina, por lo que se desestima el recurso (FJ 5o).

Artículos del repd: Artículos 5.b y 6.b.

Apartado concreto del temario: 1.12.3 Solvencia patrimonial.

SENTENCIA DEL TRIBUNAL SUPREMO-SALA DE LO CIVIL

RESEÑA SENTENCIA TRIBUNAL SUPREMO SALA DE LO CIVIL 68/2016 DE 16 DE FEBRERO

ECLI:ES:TS:2016:492

María Bocio Jaramillo

Assistant Researcher at Seville University

Cuestiones de hecho:

Se presenta demanda por seis personas físicas y jurídicas contra la empresa ADT España Servicios de Seguridad S.L(ADT). Dicha empresa se dedica al servicio de seguridad privada de alarmas. En la contratación existía una cláusula de permanencia (considerada como cláusula penal), que al proceder a darse de baja los demandantes, no fue cumplida por los mismos. Los demandantes no pagaron la cantidad correspondiente que le fue exigida por ADT, en concepto de dicha cláusula penal, y ésta habiéndoles informado previamente de la posibilidad de inscribirlos en un registro de morosos, procedió, ante la negativa del pago de dicha cantidad, a la inscripción en el mismo. Los demandantes entendieron que se había infringido el artículo 18.1 y 4 CE, el artículo 7.7 de la LO 1/1982 de 5 de mayo y lo relativo al registro por insolvencias de los artículos 29.4 LOPD y 38.1 RLOPD y de la línea seguida por el TS en sentencias anteriores como la de 24 abril de 2009 y 22 de enero de 2014.

Cuestiones claves y fundamentos jurídicos

1. No aplicación a personas jurídicas

El tribunal niega la protección de los dispuesto en la LOPD a las personas jurídicas. Para ello hace referencia a su artículo 1 donde se dispone que su objetivo es:" garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". Por su parte, el artículo 2.2 del RLOPD excluye de su ámbito de aplicación a las personas jurídicas.

Debido a esto no es de aplicación lo previsto en los artículos 29.4 LOPD y 38.1 RLOPD (FJo3).

2. Registros de morosos y derecho al honor

El concepto de registro de morosos lo concreta en:" ficheros automatizados (informáticos) de datos de carácter personal sobre incumplimiento de obligaciones dinerarias, destinados a informar a los operadores económicos (no solo a las entidades.

financieras, también a otro tipo de empresas que conceden crédito a sus clientes o cuyas prestaciones son objeto de pagos periódicos) sobre qué clientes, efectivos o potenciales, han incumplido obligaciones dinerarias anteriormente, para que puedan adoptar fundadamente sus decisiones sobre las relaciones comerciales con tales clientes" (FJ 4o).

En cuanto al derecho que puede resultar vulnerado con la inclusión de datos en el mismo, señala la lesión a la dignidad, fama y reputación de la persona con la consecuente afectación al derecho al honor (FJo4).

3. Actuación conforme a la Ley para no entender afectado el derecho al honor

Se requiere que la actuación de inscripción se haya realizado conforme los artículos 29.4 LOPD y 38. 1 RLOPD para entender que la actividad no es ilícita y no lesiona el derecho al honor (FJ 4o).

4. El principio de calidad de datos en el tratamiento automatizado de protección de datos con respeto a solvencia económica

De la conjunción de los artículos 29.4 LOPD y 38.1 RLOPD se entiende que debe existir una deuda previa, exigible, vencida, impagada previo requerimiento y que el impago sea determinante para valorar la solvencia económica del inscrito (FJ4o).

5. Proporcionalidad exigible en la inclusión en registro de morosos sobre deudas de escasa cuantía

Siempre que se cumplan los requisitos del apartado anterior, se entiende justificada la inclusión en el registro de morosos debido a que dicha actuación se considera proporcional inclusive en deudas de escasa cuantía. Los registros de morosos tienen dos finalidades: las empresas puedan otorgar créditos con garantías como evitar el sobreendeudamiento de los consumidores (FJ4o).

Decisión final:

La empresa vulneró la normativa de protección de datos ya que no estamos ante una deuda que cumpla las exigencias vistas anteriormente, sino de una reclamación unilateral derivada de la liquidación de una cláusula penal. Además, no se respetaron los principios de prudencia y proporcionalidad ya que dichos datos no son determinantes para enjuiciar la solvencia económica de una persona (FJ 4o).

Artículos del REPD: Artículos 1, 5.b, 6.b y Considerando 14.

Apartado concreto del temario: 1.2.1 y 1.12.3. Solvencia patrimonial.

RESEÑA AUDIENCIA NACIONAL SALA CONTENCIOSO-ADMINISTRATIVO DE 13 DE JULIO DE 2017

ECLI:ES:AN:2017:3257

María Bocio Jaramillo

Assistant Researcher at Seville University

Cuestiones de hecho:

En el caso objeto de análisis, nos encontramos con D. Alberto como parte actora en una reclamación ante la AEPD y Google como contraparte del mismo. Don Alberto había interpuesto reclamación debido a que en los motores de búsqueda de Google aparecían una serie de noticias conectadas a páginas de "ABC" y "El País", referente a su condena por un homicidio por imprudencia profesional cuando realizaba sus laborales de ginecólogo, alegando que con la introducción de sus datos personales en dicho motor de búsqueda no apareciese dicha información. Frente a dicha resolución de la AEPD se interpone recurso de reposición que es desestimado y ante esta resolución de desestimación, se lleva a cabo la interposición del recurso a tratar a continuación.

Google alega que nos encontramos ante una información de interés general debido a la profesión llevada a cabo por este, y que debe respetarse el derecho a la información que se vería infringido en caso contrario. Considera que el nombre y los apellidos de D. Alberto se encuentran subsumidos por su identidad profesional. Sus alegaciones se centran en: la infracción del derecho a la información y la libertad de formación de la propia opinión del artículo 20.1 CE, sendos instrumentos internacionales que recogen este, el artículo 6.2 LOPD junto con el 9.2 del Convenio Europeo para la protección de las personas con respecto a sus datos personales y la doctrina del TJUE derivada de la STJUE de 13 de mayo de 2014.

Cuestiones claves y fundamentos jurídicos:

1. Derecho a la protección de datos (olvido digital) vs derecho a la libertad de expresión

Considera que el derecho a la protección de datos (artículo 18.4 CE) tiene un

ámbito más amplio que otros derechos como la intimidad (artículo 18.1 CE). Entiende que el derecho a la protección de datos extiende: "su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inseparablemente unidos al respeto de la dignidad personal, como el derecho al honor, y al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado".

Por ello, el derecho a la protección de datos abarca tanto datos íntimos, como aquellos que no tengan esta consideración, pero que su conocimiento o empleo por terceras personas puedan suponer la infracción de sus derechos, inclusive constituyendo amenazas para el individuo (FJ 3o).

Por otro lado, la libertad de expresión, entendida en el aspecto de la crítica que se puede realizar a otro sujeto, se puede concebir como aquel mecanismo que hace posible la conformación de la opinión pública facilitando libremente la consolidación de esta. Sin embargo, como todos los derechos, no es absoluta, sino que encuentra sus límites en la protección de los derechos fundamentales. Planteada esta cuestión, es necesario realizar una ponderación de dichos derechos (FJ 3o).

2. Derecho de oposición y acceso

A la hora de realizar la ponderación se toman en cuenta una serie de criterios. Dentro de lo mismos, hay que mencionar la Directiva 95/46 donde se recoge el derecho al olvido. Dicho derecho tiene que venir justificado en una serie de criterios que son mencionados en la STJUE de 13 de mayo de 2014 donde se dispone que: "«A tenor de este artículo 6 (de la Directiva) y sin perjuicio de las disposiciones específicas que los Estados miembros puedan establecer para el tratamiento con fines históricos, estadísticos o científicos, incumbe al responsable del tratamiento garantizar que los datos personales sean «tratados de manera leal y lícita», que sean «recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines», que sean «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente», que sean «exactos y, cuando sea necesario, actualizados», y, por último, que sean «conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente»". Además, menciona la STS

sala de lo civil de 5 abril de 2016 donde en un caso muy similar consideró que el transcurso del paso del tiempo puede hacer inadecuado la finalidad con la que se llevo a cabo el tratamiento. En dicha sentencia se estableció que: "El llamado 'derecho al olvido digital', que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos (...). Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse a un tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador (...)" (FJ 4 y 5 o).

Valoración final:

Como D. Alberto no era un personaje público, y la finalidad para la que se recogieron los datos no abarca que los motores de búsqueda presenten la información referente al respectivo homicidio imprudente entre los resultados principales, se desestima el recurso interpuesto por Google debido a que se ha vulnerado el derecho al honor de D. Alberto (FJ 5 y 6o).

Artículos del REPS: Artículos 5.b y 6.b.

Apartado concreto del Temario: 1.5.2 Acceso, rectificación, supresión (olvido).

Section III: Use cases

Challenge Title: Data protection in the e-commerce field	
Use Case Author	Ph.D. Avv. Maria Cristina Gaeta, Postdoctoral Research Fellow in Law at Suor Orsola Benincasa University of Naples, Ph.D. in Law at Federico II University of Naples, Coordinator of the Editorial Team of EJPLT.
Topic	Data protection in the e-commerce field
Overview	Legal design Ltd is a consulting company that deals with creating websites and managing the related legal aspects, mainly on privacy and e-commerce, adapting the websites created, or to be created, with the existing legislation, as well as drafting updated legal documents, clear and easily understandable, also thanks to the legal design techniques of which they are experts.
1. Engage	
Big idea	Privacy adjustment of an e-commerce website
Essential Question	What processing of personal data is carried out by Fashion Style online shop?
Initial resources	**Useful links** Privacy policy example: https://teoremamoda.shop/privacy-policy-cookie-restriction-mode Cookie policy example: https://teoremamoda.shop/privacy-policy-cookie-restriction-mode https://lavoraconnoi.mediaset.it/cookiespolicy.htm Italian Data Protection Authority, what to do if the website installs cookies (before the GDPR): https://www.garanteprivacy.it/documents/10160/0/Infografica+cookie+e+privacy+-+cosa+devi+fare Provision of the Italian Data Protection Authority of 8 May 2014 «Chiarimenti in merito all'attuazione della normativa in materia di cookie»: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4006878

	Italian Data protection Authority on cookie: https://www.garanteprivacy.it/cookie Italian Data protection Authority on e-commerce: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4840904 European Commission on digital privacy: https://ec.europa.eu/digital-single-market/en/online-privacy Digital Agenda: https://www.agendadigitale.eu/mercati-digitali/ecommerce/e-commerce-e-gdpr-come-essere-in-regola-con-norme-privacy-e-non-solo/ E-commerce Europe: https://www.ecommerce-europe.eu
Guiding Questions	List of the starting questions for the privacy adjustment: – What personal data are collected? – What are the purposes of the processing? – How long are the personal data kept? On which hosting server? – Is the data processing online or offline? In the first case, are there active cookies? – Who are the subjects involved in the processing of personal data? – Are privacy by default and privacy by design tools already in place?
Reflections	Other questions to be discussed: – Is there a need to appoint a Data Protection Officer? – Is there a need to carry out the data protection impact assessment?
Other notes	
2. Investigate	
Activity Description	– Starting from the company's organisational model and personal data processed, what are the next steps? – What documents must be prepared for the privacy adjustment?
Resources	Support material: – Link indicated above
Synthesis	Prepare a word file in which to indicate: – what are the necessary activities or documents to be prepared for the privacy adjustment? – what are the possible but unnecessary activities or documents that should be prepared for greater protection.
Reflections	Reflections on the activities and documents to be prepared.

Other notes	
3. Act	
Solution Prototypes	Possible solutions. Let's read the solutions of some learners.
Solution	Let's definitively establish which activities and documents must be prepared for the privacy adjustment of Wee Ltd.
Implementation plan	– How to proceed to prepare the privacy adjustment? – How long do we need? – What could be a fair and adequate compensation to ask the customer?
Evaluate	Evaluating the simulation carried out, what would you do differently next time in terms of activities and documentation to be provided for the privacy adjustment, timing and fees?
Other notes	
4. Reflection and documentation	
Case notes	Reflections on how this case could best be developed in the future.

Challenge Title: The protection of health data in compliance with the GDPR	
Use Case Author	Ph.D. Avv. Maria Cristina Gaeta, Postdoctoral Research Fellow in Law at Suor Orsola Benincasa University of Naples, Ph.D. in Law at Federico II University of Naples, Coordinator of the Editorial Team of EJPLT.
Topic	The protection of health data.
Overview	Wee Ltd is a company that deals with the provision of services relating to safety and hygiene in the workplace. In particular, the Cis Ltd provides these services for small and medium enterprises (SME). To provide the appropriate services, Wee Ltd. collaborates with medical-health staff, who carry out inspections and medical visits. About the staff employed, instead, the Cis Ltd consists of 10 employees, who perform the role of administrative with secretarial functions, customer service and IT security. Wee Ltd. contacts a law firm to request an advice and the privacy adjustment according to the new European legislation on data protection, in the manner deemed most appropriate.
1. Engage	
Big idea	Privacy adjustment according to the new European legislation on data protection for Wee Ltd.
Essential Question	What processing of personal data is carried out by Wee Ltd.?
Initial resources	Company statute, company registration, minutes of the board of directors. **Useful links** Garante Privacy, Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario, 7 marzo 2019 [doc. 9091942] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9091942 Garante Privacy, Linee guida in materia di Dossier sanitario, 4 giugno 2015 [doc. 4084632] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4084632

	Garante Privacy, Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009 [doc 1634116] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634116 Bonomi M.S., Privacy e dati sanitari: le principali novità introdotte dal GDPR, in Federalismi, osservatorio di diritto sanitario 2018 http://www.astrid-online.it/static/upload/1710/17102018130849-4-.pdf Iaselli M., Dati sanitari, come trattarli alla luce del Gdpr, in Altalex, 2018 https://www.altalex.com/documents/news/2018/04/11/dati-sanitari-come-trattarli-alla-luce-del-gdpr GDPR: le novità apportate in ambito sanitario, in Diritto.it, 2018 https://www.diritto.it/gdpr-le-novita-apportate-ambito-sanitario/
Guiding Questions	List of the starting questions for the privacy adjustment: – What personal data are collected? – What are the purposes of the processing? – How long are the personal data kept? On which hosting server? – Is the data processing online or offline? In the first case, are there active cookies? – Who are the subjects involved in the processing of personal data? – Are privacy by default and privacy by design tools already in place?
Reflections	Other questions to be discussed: – Is it need to appoint a Data Protection Officer? – Is it need to carry out the data protection impact assessment??
Other notes	
2. Investigate	
Activity Description	– Starting from the company's organisational model and personal data processed, what are the next steps? – What documents must be prepared for the privacy adjustment?
Resources	Support material: Provide models to be used for the drafting of the privacy adjustment document.

Synthesis	Prepare a word file in which to indicate: – what are the necessary activities or documents to be prepared for the privacy adjustment? – what are the possible but unnecessary activities or documents that should be prepared for greater protection.
Reflections	Reflections on the activities and documents to be prepared.
Other notes	
3. Act	
Solution Prototypes	Possible solutions. Let's read the solutions of some learners.
Solution	Let's definitively establish which activities and documents must be prepared for the privacy adjustment of Wee Ltd.
Implementation plan	– How to proceed to prepare the privacy adjustment? – How long do we need? – What could be a fair and adequate compensation to ask the customer?
Evaluate	Evaluating the simulation carried out, what would you do differently next time in terms of activities and documentation to be provided for the privacy adjustment, timing and fees?
Other notes	
4. Reflection and documentation	
Case notes	Reflections on how this case could best be developed in the future.

Challenge Title: The prospects of legal design applied to privacy documents in light of the innovations introduced by the GDPR	
Use Case Author	Sergio Guida, Raffaele Serpe, Alsob & 'Legal Design Startup Project' team reps.
Topic	Privacy in Legal Design.
Overview	Everyday people, both as individuals and families and as businesses, are forced to interface with contracts, documents and legal procedures often without having the appropriate skills to "navigate" these systems. In many countries, the difficulty of bureaucracy and legal language often puts citizens in difficulty causing a sense of inadequacy towards the legal system but also the feeling of not having full control of their situation. So, some researchers have begun to discuss how the legal system could be rethought in terms of language and tools through the design approach. The discipline that tries to answer this question has been called "**Legal Design**" and aims to bring the legal world closer to people who have no training or experience in the legal field. In general terms, Legal Design is inspired by the concepts of **Design Thinking** and **User Experience** (UX): the intent is to maintain an approach that puts people at the center of the design and delivery of services also in the legal world to make the more intuitive, usable and inclusive user-experience. Not only does a graphic and visual form made more effective in terms of Visual Law help to understand the content of a privacy document, but it can also help the understanding of the related legal process. In essence, the goal is to make citizens more aware with well-designed rules and procedures in terms of "Legal Design", also towards the production of documents – just even in the Privacy's field - that are simple, clear but above all attractive to the recipients.
1. Engage	
Big idea	Drawing the Privacy of the Future
Essential Question	Will people appreciate the prospects of Legal Design applied to Privacy documents, also in the light of the innovations introduced by the GDPR?
Initial resources	Gatt L., Montanari R., Caggiano I.A., *Consent to the processing of personal data: a legal and behavioural analysis: some Insights into the Effectiveness of Data Protection Law, EJPLT*, 2018, I. Available at https://www.rivisteweb.it/doi/10.1437/87306

	Caggiano I.A., *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *DIMT*, 2017. Available at https://www.dimt.it/wp-content/uploads/2017/06/images_pdf_Caggiano.pdf Passaglia P. e Poletti D. (a cura di), *Nodi virtuali, legami informali: internet alla ricerca di regole: a trent'anni dalla nascita di internet e a venticinque anni dalla nascita del* web, Pisa university press, 2017. Available at: https://www.pisauniversitypress.it/scheda-ebook/paolo-passaglia-dianora-poletti/nodi-virtuali-legami-informali-internet-alla-ricerca-di-regole-9788867418053-455105.html Hagan M., *User-Centered Privacy Communication Design. Proceedings of the Symposium on Usable Privacy and Security* (SOUPS) 2016, Denver, Colorado. Available at SSRN: https://ssrn.com/abstract=2981075 Aulino L., *La conclusione dei contratti online: legal design e clausole vessatorie*, *Diritto dell'Internet*, 2020, https://dirittodiinternet.it/la-conclusione-dei-contratti-online-legal-design-clausole-vessatorie/ Research activities of the *Research Centre of European Private Law* (ReCEPL): https://www.unisob.na.it/ateneo/c008_e.htm?vr=1&lg=en http://www.notaifasanoiaccarino.it/plugins/blocchi_contenuto/public/contents/59/allegati/153929947PDFdellaPubblicazione.pdf http://www.lawbydesign.co/en/legal-design/
Guiding points	– The use of design thinking in the legal field was born at Stanford Law School & d.school in the United States. The intent is to maintain an approach that places people at the center of the design and delivery of services also in the legal world to make the experience more intuitive, usable and inclusive. – The design methodologies offer an opportunity to review the way in which the main tools of privacy's activity are conceived and narrated, namely documents, contracts and procedures. – Citizens perceive the need to simplify the visualization and will appreciate the potential of legal design from the simplification of language, to the redesign of privacy documents, up to the simplification of procedures both for citizens and for professionals and operators.
Reflections	– Users express the need to simplify the display when they interface with long pages of terms and conditions concerning privacy even when they are using digital services.

	– The key point is that, starting from the analysis of the texts of some modules (e.g. 'information on the use of personal data' and 'privacy consent' for various activities, both online and in the physical world), to "translate "the requests - almost always perceived both by the writers and by the users as bureaucratic or slightly more - in simpler questions for the citizen, also adapting to the level of understanding of the user's language. – A dialogical participation with citizens is therefore highly desirable, each of whom has to deal with privacy forms every day, also and above all for web activities.
Other notes	In researching our scenario, we found that, at least in Europe, no particular attention is given to the most vulnerable individuals, including people with disabilities. For them the benefits in terms of accessibility to be reached are: – firstly "passive", such as the effectiveness of the protection relating to the networking of data, but – above all ACTIVE, that is, thanks to which people are put in a real condition to know thoroughly their rights and to be able to exercise them in practice as effectively as required by the regulations.
2. Investigate	
Activity Description	Also in the wake of the GDPR innovations, we experimented practically how the advantages of effectively **involving citizens since by design** could be proved to be the right key so as the legal documents we encounter in everyday life can finally convey to much more substantial transparency and sense of control of the situation but also clearly and immediately perceptible. Questions posed to the interested people during the **field survey** sounded like the following: 1. How much time do you spend reading a privacy policy of the type that has been shown to you? 2. Are you usually inclined to sign this type of information? 3. Have you understood what it entails giving your consent to the processing of your personal data? 4. In light of what has been explained to you, do you think that the content of the privacy information could be written more clearly? 5. In light of what has been explained to you, do you think that the graphics of the privacy policy could have been prepared more clearly and intuitively?

Resources	List any reading, web or video resources here that you think would be good to 'get the readers going'. Our initiative, kindly sponsored by two very important scientific realities such as ReCEPL (Research Centre of European Private Law/Centro di Ricerca in Diritto Privato Europeo) and ALSOB (Associazione Laureati Suor Orsola Benincasa), participated with great success in the XXXIII edition of FUTURO REMOTO 2019, BE 4.0, a well-known Science festival held in Naples at Città della Scienza. Link: http://www.cittadellascienza.it/futuroremoto/legal-design-e-visual-law-applicati-a-documenti-privacy-disegniamo-la-privacy-del-futuro/
Synthesis	The more significant task will be the realization of your video summarizing your point of view. Hopefully, a kind of survey conducted by you would be much appreciated.
Reflections	– The nature and setting of our project lead our project to be particularly close to the world of training but also to impact investing or sustainability themed entities and companies that are among the main stakeholders. – The protection of personal data and privacy is in fact a topical issue for all users, starting from young people, destined to enter early - when they are not already - in the group of " passive subjects", that is "weaker contractors" in any type of contract with entities and companies that produce and use documents written in "legalese". – With legal-designed documents both the issuer and the receiver fully understand each other, and it is minimized any perceived source of concern or possible arbitrators, also and especially online.
Other notes	Particular attention has to be paid to the so-called '**weak subjects**'- e.g. people with disabilities - for whom the fundamental objective is to allow to fully understand the rights expressed in the legal documents, starting just with those Privacy-related. So we imagined a second Startup, specifically dedicated to developments in this direction.
3. Act	
Solution Prototypes	– Recently, in Italy, a team of experts and professionals - all of the **2nd Level University Master in Data Protection Officer & Privacy Law**, after successfully obtaining the title at the University of Suor Orsola Benincasa – illustrated to the interested people

	various examples of legal documents INTERACTIVELY. – During a scientific and popular event of great relevance and affluence, "prototypes" of documents redesigned and re-presented through visual techniques were shown, enriched with illustrations, diagrams and intuitive icons. – Users were happy to report to the (future) Start-up's Team the doubts and difficulties that emerged in their daily experience in the field of privacy and data protection, also providing by feedback comments, ideas and suggestions very useful to 'design the privacy of the future'.
Solution	– Legal design has made possible to highlight how the new design is not only graphic but reduces the information to be communicated to the essential, making it clearer and more understandable – The new design vehicles in an intuitive and immediate way so as not to discourage. Indeed, it promotes the reader to read and understand his or her rights, and how to exercise them in practice.
Implementation plan	In summary, the potential of legal design appears high and substantial, starting from the simplification of the language, to the redesign of the privacy documents, up to the simplification of the procedures for entities and companies and the actual, as well as perceived usability. All details are available at the link: https://www.dataprotectionlaw.it/2020/02/06/legal-design-visual-law-gdpr/
Evaluate	The results of the interviews with interested users as well as your feedback, comments, ideas, suggestions, etc. could be collected in a volume edited by the Startup.
Other notes	This case asks for an innovative path through multidisciplinarity and "contamination" between different disciplines, such as data protection, design thinking, user engagement, management systems and procedures for privacy and security.
4. Reflection and documentation	
Case notes	1. Multidisciplinary skills are very important in the design and implementation of highly innovative products and services based on legal design, aimed at maximizing user experience in fields where "digital transformation" is, in our country, still in its infancy. 2. Pay particular attention to 'weak subjects', for whom, in addition to the fundamental objective of allowing full accessibility and usability of privacy rights, the highest objective would be to bring out and enhance the enormous patrimony in terms of Human Capital which often, even in their case, lies latent and unexpressed.

THE SCIENTIFIC INNOVATIONS OF FETAL SURGERY AND ARTIFICIAL WOMB COULD INNOVATE ALSO THE CONCEPT OF LEGAL PERSONHOOD

Mario Triggiani

Teaching assistant in Private Law at Università degli Studi
Suor Orsola Benincasa di Napoli

Abstract:

In English law, the foetus has no legal personality and it is deemed to have a separate existence from its mother until it is born. This rule may need to be revised, in light of technological advances in foetal surgery and artificial womb technology designed to preserve foetal viability pre-birth. Thus, the technological intervention for the preservation of foetal viability may seem incompatible with traditional legal conception that denies legal personality to the foetus. However, affording the foetus a legal personality may have a huge impact on the fundamental rights of pregnant women over their bodies.

Key-words: Artificial Womb Technology; fetal surgery; legal personhood.

1. Introduction

According to English law, the foetus has no separate legal rights from its mother, and legal personality is assigned at birth [1]. This principle of law was reaffirmed by the European Court of Human Rights' decisions in *Paton v United*

[1] Paton v British Pregnancy Advisory Service Trustees [1979] QB 276 (https://www.bpas.org/media/1182/gjo_uk_patonvbritishpregnancyadvisoryservicetrustees_en.pdf).

Kingdom; [2] and *Vo v France;* [3] in which the European Court of Human Rights ruled that the unborn child had no rights under Article 2 of the Convention of Human Rights. Therefore, there has always been a clear distinction between a foetus, who has no legal personality, and a person born alive, who is afforded all the rights and protection of a child. However, this born/unborn legal dichotomy between the foetus and the child is at risk because of recent medical technological advances in pre-birth treatments of foetuses in the uterus.

In her article, "Challenging the born alive threshold: fetal surgery, artificial wombs, and the English approach to legal personhood ". [4] Elizabeth Chloe Romanis refers to the English legal system, but her reflections are valid for all legal systems in Europe, in light of the European Court of Human Rights judgements in *Paton v United Kingdom* and *Vo v France.* The author points out that the emerging medical advances give cause to question whether the legal concepts of births and born alive in Europe can still be considered a valid approach to assigning personhood in light of new medical technological advances.

These new medical technological advances is exemplified in 2016, when an innovative surgical team succeeded in extracting a pre-viability foetus almost entirely from the uterine environment, removing a life-threatening tumour, and placing the foetus back into the uterus to continue gestating. The baby was then delivered healthy at the end of the normal gestational period, making the headlines as "the baby born twice". [5]

Another technological challenge to the born/unborn dichotomy between the foetus and the child is evidenced by the development of the Artificial Womb Technology (AWT), in which a foetus is outside the mother's body but in a primordial stage of its human development. The complete ectogenesis, in which human beings are created in a laboratory by in vitro fertilization and grown in an AW until 36 weeks from conception, remains a remote possibility. However, the same cannot be said for partial ectongenesis, which involves the pregnant woman, and in which the foetus is either delivered prematurely or extracted by C-section. For example, in 2017, a team of scientists and foetal surgeons announced the development of an artificial womb prototype that had supported lamb foetuses on the viability threshold for four weeks [6]. All test subjects survived the experiment

[2] (1980) 3 EHRR 409.

[3] [2004] ECHR 53924/00.

[4] Elizabeth Chloe Romanis, "Challenging the 'Born Alive' Threshold: Fetal Surgery, Artificial Wombs, and the English Approach to Legal Personhood", *Medical Law Review* (Volume 28, Issue 1, Winter 2020), Pages 93–123, https://doi.org/10.1093/medlaw/fwz014.

[5] "Baby Lynlee 'born twice' after life-saving tumour surgery" BBC 24 October 2016 (https://www.bbc.com/news/world-us-canada-37750038).

[6] "An artificial womb successfully grew baby sheep – and humans could be next" The Verge Apr

without experiencing any of the common complications associated with lamb preterm birth. These results are encouraging because it is hoped that this technology will also have the capacity to overcome the present limitations of neonatal intensive care and improve patterns of morbidity and poor prognoses in human preterm. The artificial wombs could represent an alternative to neonatal intensive care because it treats the foetus as if it had not been removed from the uterus by closely mimicking uterine conditions to effectively prolong gestation.

2. Legal personality and the "born alive" approach

Before we can address the issue of the risks of scientific progress on legal personality, it appears necessary to clarify what is meant by birth. According to English law, the birth corresponds to the separation of gestator and gestational subject [7]. Thus, in order to acquire legal personality, the child must be not only be "born", but also be "born alive", which means it must demonstrate any of the recognisable signs of life (a typical example is autonomous breathing) [8]. Therefore, the vitality of the new-born was fundamental in times when this was the only way to evidence a human being's development and birth. The English law, in fact, has always recognized the existence of "stillbirth", which occurs when a child is born in the twenty-fourth week without having demonstrated any signs of life. [9] The law, however, maintains that a stillbirth child cannot be the victim of a homicide, unlike in the United States, where pregnant women have been criminalised for still-births in some states. [10] Nowadays the "born alive" rule to determining legal personality in English law, and by extrapolation in Europe, may appear an outdated approach, because new technological developments in foetal monitoring, have enabled medical practitioners to determine that developing human beings exist and exhibit signs of supported life pre-birth. This invariably leads to the question: if a foetus is medically ascertained to be alive in uterus, why not ascribe the foetus a legal personality?

25, 2017 (https://www.theverge.com/2017/4/25/15421734/artificial-womb-fetus-biobag-uterus-lamb-sheep-birth-premie-preterm-infant).

[7] Paton (n 1) per Sir George Baker at 279. "The foetus cannot, in English law, in my view, have any rights of its own at least until it is born and has a separate existence from the mother".

[8] Births and Deaths Registration Act 1953 s 41, as amended by Still-Birth Definition Act 1992 s 1 (http://www.legislation.gov.uk/ukpga/Eliz2/1-2/20/section/41).

[9] Section 1(1) Still-Birth (Definition) Act 1992, Chapter 29. (England & Wales).

[10] Ava B. "When Miscarriage is a crime", Plant Parenthood of Arizona, (July 29, 2019), https://www.plannedparenthoodaction.org/planned-parenthood-advocates-arizona/blog/when-miscarriage-is-a-crime.

3. Foetal surgery: problems for women and foetuses

Foetal surgery poses another legal challenge to the concept legal personality. For example, if being born is literally only a matter of not being inside another person anymore, it might be argued that during a surgery the foetus, who is extracted from the pregnant woman's body to be operated upon, remaining attached only by the umbilical cord, is born and has, therefore, a legal personality. However, recognizing the foetus's legal capacity during the operation is not a trivial choice. During the surgery, whatever is done to the foetus physically affects the pregnant woman and the law chooses to consider her the only patient for the purposes of the procedure, therefore, it is only her consent that is significant for the surgery.

In literal terms, in the unlikely event that the foetus is considered born at the time of the surgery conducted outside of the uterus, its rights to personhood should be recognised and protected as such. However, in the circumstances, the legal personhood afforded to the foetus during the surgery must be reversed as soon as the foetus is returned to the uterus. However, there is no legal precedent for reversing the personhood of a human being. The only way to remove legal personality is death, and it is counter-intuitive to imagine that the reinsertion of a foetus into the womb is equivalent to its death.

On the other hand, even the argument that considers a foetus as legally born during an operation outside of the uterus is beset with clear problems. Without personhood during the operation, liability for grossly negligent surgeries causing death in utero and subsequent stillbirth of foetuses might be precluded because gross negligence manslaughter could only be established if a baby was born alive with injuries sustained from negligent surgery that later caused death. Furthermore, the offence of "child destruction" (recognized in England and Wales in the case of killing of "viable foetus", which means a foetus potentially suitable for extra-uterine life [11)] or of procuring miscarriage could not be established because there would be no *mens rea.*

There may be no civil recourse following the stillbirth of a foetus that died in utero as a result of negligent foetal surgery because if the foetus is not born alive, it is not an entity that can bring an action in tort. There could be only a course of action in negligence for the baby born alive but injured by negligent surgery [12].

---

[11] "Any person who by wilful act intentionally destroys such a foetus is guilty of child destruction" Infant Life Preservation Act 1929.

[12] In these circumstances, the baby "born alive" would be able to pursue an action in negligence for damage caused during the surgery because at birth they achieve legal personality and inherit the damaged body for which the foetal surgeon is responsible (Burton v Islington HA (n 59) per Dillon LJ at 219).

4. The risks of affording legal personality to the foetus in the artificial womb

In order to be afforded legal capacity, it is not sufficient to be separated from the uterus, but there must be also proofs that the new-born is alive. The English law states that a child is born alive if it breathes after birth [13]. It has not been specified, however, whether breathing must be demonstrated only immediately after birth or also for some continuing time after. Even in the case of assisted ventilation, the child still uses his lungs to breathe. Instead, a foetus placed inside an artificial womb does not "breathe", acquiring the oxygen not using its lungs but by placental gas exchange through cannulae in the amniotic fluid, just like the foetus in utero [14].

Moreover, the acquisition of oxygen by placental gas exchange rather than ventilation is one of the greatest advantages of the artificial womb, which allows the lungs to continue to develop ensuring they are inactive. It has also been highlighted, however, that breathing is certainly a valid indicator to establish that the subject is "born alive", it cannot be the only vital sign of life taken into consideration [15]. However, it is difficult to identify what the others signs of life may be, since there is no uniformity of views about the sufficiency of primitive circulation or growing movements.

Another possible approach is the one called “forced symmetry”, which states that if a defining characteristic can be isolated that makes a person legally dead, the emergence of that characteristic identifies when a person becomes legally alive. A typical sign of the occurrence of death is the irreversible loss of consciousness [16]. There is no doubt that in the artificial womb the foetus lacks any consciousness and therefore could not be considered alive. It is also evident, however, that this lack of knowledge is not irreversible or permanent because

[13] Births and Deaths Registration Act 1953 s 41, as amended by Still-Birth Definition Act 1992 s 1 (http://www.legislation.gov.uk/ukpga/Eliz2/1-2/20/section/41).

[14] “An extra-uterine system to physiologically support the extreme premature lamb” Nature Communications, 25 April 2017 (https://www.nature.com/articles/ncomms15112).

[15] In R v Brain it was observed that many children are born alive but do not breathe for some time after their birth; in R v Sellis it was suggested breathing is not decisive proof of being born alive because a foetus could breathe and yet have died before birth is complete. The jury were told they must be satisfied that ‘the child was wholly born into the world in a living state’ at the time that it was decapitated, the implication being that a living state encompasses more than breathing.

[16] Academy of Medical Royal Colleges, A Code of Practice for the Diagnosis and Confirmation of Death (2008) http://aomrc.org.uk/wp-content/uploads/2016/04/Code_Practice_Confirmation_Diagnosis_Death_1008-4.pdf.

the foetus will at some point be capable of exercising an independent life and if undisturbed will be removed from the artificial womb. Therefore, it is easy to see that the foetus is not legally alive but also not dead. Considering the foetus in the artificial womb "born alive" could also change the conception of viability because the technology has the potential to change what "capable of being born alive" means.

Viability marks the point from which the foetuses are granted a limited right not to be aborted. Currently, the limit set by the 1967 Abortion Act is 24 weeks [17], after which the foetus is presumed capable of being born alive. Affording legal personality to the foetus in an artificial womb could lead to the contention that a foetus in utero capable of surviving in an artificial womb should be considered "capable of being born alive". The technology of the artificial uterus could therefore considerably reduce the point at which a foetus can survive outside the uterus, since there is no definition of "capable of being born alive only if supported by an artificial uterus". Arguably, Artificial Womb Technology also threatens access to abortion, by empowering the anti-abortion lobby, who could claim AWT in order to advocate for a reduction of the time allowed for abortion.

5. The only possible solution is creating a third status

The current binary structure of personhood, where there is only the possibility of having legal personality or not, appears too restrictive. Therefore, the author suggests the creation of a third status, a "partially born" category, for entities like the foetuses in the artificial womb or the foetuses who undergo a surgery outside the maternal uterus. This third status could be used to identify these subjects accurately, avoiding the creation of a ripple effect in other areas of law and solving relevant discrepancies appropriately.

The English law already affords some protection to foetuses in utero [18], to the embryos created as part of the In Vitro Fertilization process [19] and even to

[17] Abortion Act 1967 s 1, as amended by Human Fertilisation and Embryology Act 1990 (http://www.legislation.gov.uk/ukpga/1967/87/contents).

[18] A foetus is protected by the Infant Life Preservation Act, which criminalises child destruction and the Offences Against the Person Act 1861 criminalising the procurement of miscarriage.
(http://www.legislation.gov.uk/ukpga/Geo5/19-20/34/section/1).
(http://www.legislation.gov.uk/ukpga/Vict/24-25/100/contents).

[19] The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology Act 2008 renders it unlawful to experiment with embryos after 14 days from conception (http://www.legislation.gov.uk/ukpga/2008/22/contents).

the animals [20]. All these entities are not valued to the same degree as a legal person but have their legal existence protected. The creation of different categories of human beings could, however, carry some normative concern and risks of abuse.

[20] The Animal Welfare Act 2006 contains provisions criminalising behaviour that causes excessive suffering to an animal (http://www.legislation.gov.uk/ukpga/2006/45/contents).

LEGAL DESIGN AND ARTIFICIAL INTELLIGENCE IN SUPPORT OF LEGISLATIVE DRAFTING DURING CRISIS

Livia Aulino

Ph.D. candidate at Università degli Studi Suor Orsola Benincasa di Napoli

Abstract:

During the emergency period of the coronavirus, numerous legislative acts have been issued in Italy, the content of which is full of references to other measures, long and complex periods that are incomprehensible to citizens. These measures have revealed a lack of legislative drafting, in which the methodology of legal design can be a remedy.

Key-words: legal design, new technologies law, legislative drafting, covid-19.

Italian citizens, in the emergency Covid-19, have been complying with decree after decree, often announced late at night and entered into force the next day.

These legal texts not only seemed too long and complex, but they were also full of interpretative doubts, so much that amendments and clarification were needed, as well as conferences, explanatory press releases, both at the national and regional level.

For example, the decree of the President of the Council of Ministers announced on the evening of 21 March, which came into force on 23 March [1], contains about 2000 words and ten references to other decrees, laws, ordinances, codes, and protocols.

This is not surprising, considering that the Italian legislation is composed of approximately 110 thousand laws currently in force and there are laws containing even 150 thousand words (such as the budget law of 2018).

But in a similar situation, during a world - wide epidemic, the ambiguity of these normative (or, more correctly, *administrative)* texts has also been noted by

[1] The decree was published by the Italian Council of Ministers on 22 march 2020 and is available at: *http://www.governo.it/sites/new.governo.it/files/dpcm_20200322.pdf.*

eminent legal experts because they were too ambiguous even for them. Indeed, Professor S. Cassese criticized the extension and complexity of the latest Government's decrees on coronavirus [2], instead praising the document (entitled "brevity") in which Churchill, on 9th August 1940, described in four points how government documents should be written.

In fact, the legislator should consider that he is not writing these laws for himself but for an entire and uneven community, to which the principle "*ignorantia legis non excusat"* applies rigidly.

The principle of clarity of legal texts is also enshrined in art. 13 bis, of Law n. 400/1988 (as amended by Law n. 69/2009) according to which: "*a) any rule intended to replace, amend or repeal existing rules or to establish derogations must expressly state the rules replaced, amended, repealed or derogated; b) any reference to other rules contained in legislative provisions, regulations, decrees or circulars shall indicate the text or subject to which they refer or the principle contained in the rules referred to, in full or* ***in clear and brief form***". These premises suggest that a clear and brief form will it remain only a dream in Italy.

This legislative mess, however, had a side effect: the Internet and social networks have become the main source of help, for common citizens, in understanding the rules and lots of national and regional institutions used them to deliver a more clear description of these rules, sometimes in a "particular" manner (we can remember that some regional governors used these channels to communicate more quickly to the citizens who don't wear masks and don't respect social distancing). But that evolution of the information networks came at a cost: considering that the opportunity of technology cannot be exhausted in the speed of the diffusion of information, of whereby social networks are pioneers, we must note that there is an increasing risk of fake news relying, in fact, on the speed of their diffusion and crippling the institutional attempts to control the pandemic.

But there is also a good side of technology. In fact it can help the legislator, through the application of the legal design methodology, to enact clear laws and administrative acts. Legal design is defined by M. Hagan - researcher at Stanford University - as the application of human-centred design to the world of law, in order to create more immediate legal services, usable and fulfilling for the user [3]. This approach is analyzed in the Research Centre of European Private Law (ReCEPL) of Suor Orsola Benincasa University - of which Professor Lucilla Gatt is Director and Professor Ilaria Amelia Caggiano is Deputy Director -

[2] The recent article was published in the newspaper Corriere della Sera on 23rd March 2020) *https://www.corriere.it/editoriali/20_marzo_23/dovere-essere-chiari-b5b36828-6d39-11ea-ba71-0c6303b9bf2d.shtml.*

[3] Hagan M, 'Law by Design' (Retrieved March 2018), in *www.lawbydesign.co/en/home*

where are carried out researches on the subject of legal design, with particular reference to a contract, using various methodologies, including multidisciplinary ones [4].

Returning to the subject of this article, we can say that, first of all, it is necessary to improve the legislative technique through the use of a clearer and unequivocal language, avoiding cryptic references to other normative texts. Indeed, it is crucial to avoid jeopardising values such as legal certainty and the efficiency of justice. Secondly, the legislator could apply the legal design methodology in the drafting of legal texts, providing – also in explanatory annexes – graphical summaries, infographics, maps and interactive tools to ensure a comprehensive and immediate understanding of the rules.

The use of these techniques would make recipients more aware and, as a result, the law would immediately become more effective.

So, following that approach, the first thing a legislator should do is to ask himself if the act/law can be understood by common citizens on a lexical structure and how can improve the text's understanding.

Then he should modify the overall structure of the text by also using images, diagrams, schemes that can show the correct behaviour a citizen should have.

But it is not a simple objective to fulfill during a world crisis. So, what can he do? In a similar context, given the difficulty in ensuring clarity and transparency of rules, with the use of the suggested methodologies combined with the lack of public confidence in the political class and the problems that need to be dealt with during a similar crisis (for example the problem of achieving a solution as quickly as possible), the aid of artificial intelligence can be also considered useful.

In fact, currently, the AI is used within the legislative field only in order to analyze with which probability the laws are approved [5].

It could be a lot more helpful if used during a similar situation, because an AI could not only guarantee the writing of clearer and simpler rules and the understanding of how that rule fits into the legislative landscape in order to predict its efficiency, as we can see during an "ordinary" exercise of legislative power, but it could also help in an emergency situation, analyzing social behavioural patterns, to understand how the rules should be *presented a*nd *explained i*n or-

[4] The Research Centre of European Private Law (ReCEPL) of Suor Orsola Benincasa Univrsity of Naples develops research itineraries on the relationship between law and new technologies. See *https://www.unisob.na.it/ateneo/c008.htm?vr=https://www.unisob.na.it/ateneo/c008.htm?vr=1.*

[5] A study found that out of nearly 70,000 bills submitted to the United States Congress from 2001 to 2015, only 2,513 (4%) were passed and became law. On the point see A. Santosuosso, *Intelligenza artificiale e diritto. Perché le tecnologie di I.A. sono una grande opportunità per il diritto* (Mondadori 2020) 73.

der to gather more support from the population in implementing the efforts needed to control the crisis.

For example, think about social distancing: in a lot of cases it is not clear if it should be maintained or not. And what about the face mask? A lot of people don't understand when it is mandatory to wear it!

We could also think of all those Apps developed in order to help citizens use the public services in the era of social distancing and that a lot of them don't know how to use it correctly.

So it is very clear how the AI can be a *game changer* in every situation of exercise of the legislative power and a real help for the improvement of the citizen's life by clearing away all those doubts and ambiguities that make indecipherable our legal system.

IL DIRITTO "AD ESSERE DIMENTICATI": L'EVOLUZIONE NORMATIVO-GIURISPRUDENZIALE DEL DIRITTO ALL'OBLIO ED I RAPPORTI CON IL DIRITTO DI CRONACA IN UN'OTTICA COSTITUZIONALMENTE ORIENTATA

THE RIGHT TO BE FORGOTTEN: THE REGULATORY-JURISPRUDENTIAL EVOLUTION OF THE RIGHT TO BE FORGOTTEN AND THE RELATIONS WITH THE RIGHT TO INFORM IN A CONSTITUTIONALLY ORIENTED PURPOSE

Federico Sergio

Teaching assistant in Tax Law, Università degli studi Suor Orsola Benincasa di Napoli

Abstract:

Da anni è ormai avvertita, tanto in ambito nazionale quanto a livello europeo, l'esigenza di riconoscere pienamente il diritto all'oblio come diritto fondamentale della persona. Spesso, tuttavia, è necessario operare un contemperamento fra quest'ultimo ed altri diritti altrettanto rilevanti. In tale ottica si colloca l'individuazione dei criteri di bilanciamento fra il "diritto ad essere dimenticati" ed il diritto di cronaca.

For long time, the need to fully recognize the right to be forgotten as a fundamental right of the person has been felt, both at national and European level. However, in many cases it's necessary to make a balance between the over-mentioned right and other equally relevant rights. In this perspective, the identification of the balancing criteria between the "right to be forgotten" and "the right to report" is placed.

Parole-chiave: Diritto all'oblio; diritto alla riservatezza; diritto di cronaca; criteri di bilanciamento costituzionali; protezione dei dati personali.

Key-words: *Right to be forgotten; right to privacy; right to report; criteria of constitutional balancing; data protection.*

la nascita del diritto all'oblio in Italia. – 3.1. Segue: l'espansione del diritto all'oblio – 4. Il riconoscimento del "diritto alla cancellazione" da parte dei giudici eurounitari. – 5. Art. 17 GDPR n. 679/2016: la regolamentazione del diritto all'oblio nella sua natura "composita". – 6. I delicati rapporti fra il "diritto ad essere dimenticati" ed il diritto di cronaca: criteri di bilanciamento in chiave costituzionale. – 7. Riflessioni conclusive.

1. Introduzione

Lo sviluppo dell'odierna "società dell'informazione" ha comportato l'incremento delle istanze di tutela della riservatezza, la cui portata valoriale ha assunto notevole rilevanza in ordine al diritto all'oblio.

Il presente lavoro, infatti, si propone di svolgere un'analisi approfondita sull'evoluzione di tale diritto, principiando dalle più risalenti definizioni storiche giungendo, poi, alla sua espressa regolamentazione nel GDPR n. 679 del 2016 ed ai recentissimi approdi giurisprudenziali interni e sovranazionali.

Crocevia di molteplici riflessioni in diverse branche dell'ordinamento giuridico, il diritto all'oblio ha destato significative valutazioni in merito all'arduo contemperamento dei valori costituzionali con i quali entra in conflitto e dei quali esso stesso è portatore.

In tale ottica, il presente articolo si soffermerà sulla sua specifica accezione di "*interesse di un individuo alla non reiterata pubblicazione di notizie che lo riguardino*", che, così inteso, si connette ineludibilmente al diritto di cronaca quale resoconto di fatti storici riportati tramite l'utilizzo della stampa o della pubblicazione *online* in ragione dell'interesse della collettività nutre nei confronti di tali accadimenti.

Si analizzerà poi il conflitto, sul fronte del bilanciamento dei valori costituzionali venuti in rilievo, derivante dal fatto che mentre il fondamento del diritto all'oblio è rinvenibile nell'art. 2 Cost., essendo concepito come baluardo dei diritti di nuovo conio della persona, il diritto di cronaca, invece, è tutelato dall'art. 21 Cost., nel quale i Padri costituenti hanno esplicitamente accordato tutela al diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto o ogni altro mezzo di diffusione.

Alla luce di una Costituzione che non stabilisce una gerarchia assiologicamente predeterminata dei principi fondamentali, verrà infine scrutinata l'attività ermeneutica della giurisprudenza.

In particolare, si indugerà sullo sforzo effettuato dalla Corte di Cassazione nell'individuare fattualmente le ipotesi in cui il diritto alla riservatezza, nella sua estrinsecazione di "diritto ad essere dimenticati" (o più solennemente "diritto all'oblio"), prevale sul diritto di cronaca.

2. La genesi del concetto di oblio ed i primi arresti giurisprudenziali in materia di riservatezza dei dati personali

L'oblio ha origini antichissime tenuto conto che una sua prima forma embrionale è rinvenibile già nel diritto romano in ordine alla previsione della *damnatio memoriae* [1].

Tale concetto si riferiva alla sanzione inflitta nei confronti dei nemici di Roma e consisteva nella totale cancellazione del ricordo nonché, più in generale, di qualsiasi traccia che potesse permettere ai posteri il riaffiorare nella loro memoria del soggetto tacciato [2].

Da ciò si evince la clamorosa differenza della concezione del diritto ad essere dimenticati in epoca romana da quella che si ha invece nella società odierna [3].

Infatti, mentre in passato la cancellazione della persona dalla memoria collettiva costituiva una pena a tutti gli effetti, attualmente, invece, il fine che si vuole perseguire tramite la valorizzazione del diritto all'oblio risiede proprio nell'opposta possibilità di essere concretamente dimenticati, quale ennesima estrinsecazione dei diritti della personalità costituzionalmente garantiti dall'art. 2 della Costituzione [4].

Per scorgere la prima effettiva disciplina del diritto in esame occorre riferirsi al saggio [5] del 1890 di due avvocati americani ("*The right to privacy"*), nel quale la riservatezza era definita come il diritto di essere lasciati soli (per l'appunto "*the right to be let alone*").

Il diritto all'oblio, così come inteso nella società moderna, deriva dal "*droit*

---

[1] F. NIETZCHE, *Sull'utilità e il danno della storia per la vita* [1874], trad. it. di S. GIAMETTA, Milano, Adelphi, 1974; A. MARGALIT, *The Ethics of Memory*, Cambridge MA, Harvard University Press, 2002; P. RICOEUR, *La memoria, la storia, l'oblio*, a cura di D. IANNOTTA, Milano, Raffaello Cortina, 2003; ID., *Ricordare, dimenticare, perdonare. L'enigma del passato*, trad. it. di N. Salomon, Bologna, Il Mulino, 2012; A. GHEZZI, A. GUIMARAES-PEREIRA, L. VESNIC-ALUJEVIC (eds.), *The Ethics of Memory in a Digital Age. Interrogating the Right to Be Forgotten*, Palgrave Macmillan, 2014; U. PAGALLO, M. DURANTE, *Diritto, memoria ed oblio*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, cit., 65-84; J.L. BORGES, *Funes o della memoria*, in ID., "Finzioni" [1944], trad. it. di A. MELIS, Milano, Adelphi, 2003.

[2] S. RODOTÀ, *Repertorio di fine secolo*, Roma-Bari, Laterza, 1999, 201.

[3] S. MORELLI, *Fondamento costituzionale e tecniche di tutela dei diritti della personalità di nuova emersione (a proposito del "diritto all'oblio")*, in *Giust. civ.*, 1997, 515; D. BARBIERATO, *Osservazioni sul diritto all'oblio e la sua (mancata) novità del regolamento UE 2016/679, sulla protezione dei dati personali*, in *Resp. civ. e prev.*, 2017, 2100 ss.; S. BONAVITA, R. PARDOLESI, *Gdpr e diritto alla cancellazione (oblio)*, in *Danno e resp.*, 2018, 269 ss.; M. TAMPIERI, *Il diritto all'oblio e la tutela dei dati personali*, in *Resp. civ. prev.*, 2017, 1010 ss.; F. MANGANO, *Diritto all'oblio*, in *Giur. merito*, 2012, 2621 ss.

[4] G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. informatica*, 2010, 391 ss.

[5] S. WARREN, L. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, volume 1, 193-220 e ss., disponibile su http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

à l'oubli", il cui contenuto è stato elaborato da alcuni teorici [6] del diritto francese in relazione ad un contenzioso concernente un film avente ad oggetto la biografia di un assassino (*Landru*, 1963). In questo caso, l'amante dell'efferato criminale aveva espresso la propria volontà che la pellicola non fosse prodotta, poiché l'eventuale pubblicazione avrebbe causato la riproposizione di alcuni spiacevoli momenti della sua vita che avrebbe preferito non ricordare. In tal modo, si passa quindi da un generale "diritto a farsi dimenticare" ad un più specifico "diritto a dimenticare determinati episodi della propria vita".

In ambito italiano, stante la mancanza di un'espressa previsione legislativa, il diritto all'oblio viene gradualmente disciplinato dalla dottrina e dalla giurisprudenza [7]. Uno dei primi celebri casi in materia risale al 1958 e concerneva la pubblicazione di un romanzo in cui era descritta la storia d'amore fra Mussolini e la sua amante Clara Petacci. I genitori della donna avevano ritenuto offensivo la riproposizione di tali fatti e la Corte d'Appello di Milano aveva riconosciuto un diritto alle vicende umane connesso ad atti storicamente determinati.

Nella casistica pervenuta al giudizio della Corte di Cassazione verso la fine degli anni '50, il diritto all'oblio è stato vagliato alla luce del noto "caso Caruso" afferente il coinvolgimento del questore di Roma dell'epoca nella famosa strage delle Fosse Ardeatine. In tale circostanza la Cassazione aveva ritenuto che dovesse essere riconosciuta dignità giuridica al "diritto al segreto del disonore", ossia al "*diritto a preservare la propria dignità, anche se fittizia, contro gli attacchi della verità*" [8].

---

[6] LYON-CAEN, nota a *Tribunal de Grande Istance Seine*, in *Juris-classeur pèriodique*, 1966, II, 14482.

[7] A.L. VALVO, *Il diritto all'oblio nell'epoca dell'informazione "digitale"*, in *Studi sull'integrazione europea*, 2015, n. 2, pp. 347-358; E. CRUYSMANS, C. ROMAINVILLE, *Les diverses dimensions du "droit à l'oubli" dans la sphère numérique. Un processus de positivation rentrant en conflit avec la liberté d'expression?*, in C. ALCANTARA *(sous la direction de)*, "E-réputation. Regards croisés sur une notion émergente", Issy-les-Moulineaux, Gualino-Lextenso éditions, 2015, 81-92; P. KORENHOF, J. AUSLOOS, I. SZEKELY, M. AMBROSE, G. SARTOR, R. LEENES, *Timing the Right To Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data*, in S. Gutwirth, R. Leenes, P. de Hert (eds.), "Reforming European Data Protection Law", Springer, 2015, pp. 171-202; C. MARKOU, *The 'Right To Be f*orgotten'. *Ten Reasons Why It Should Be Forgotten*, 203-226; G. ZANFIR, *Tracing the Right To Be Forgotten in the Short History of Data Protection Law. The "New Clothes" of an Old Right*, 227-252; F. DI CIOMMO, *Quello che il diritto non dice. Internet e oblio*, in *Danno e responsabilità*, 2014, n. 12, 1101-1113; F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013; V. MAYER-SCHÖNBERGER, *Delete. Il diritto all'oblio nell'era digitale*, Egea, Milano, 2013; G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio,* in *Il diritto dell'informazione e dell'informatica*, 2010, n. 3, 391-410; M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Edizioni Scientifiche Italiane, Napoli, 2009; D. MESSINA, *Le prospettive del diritto all'oblio nella società dell'informazione e della comunicazione*, in *Riv. trim. dir. pubbl.*, 2009, n. 1, 93-103.

[8] Cass., 13.05.1958, n. 1563, in *Mass. Giur. it.*, 1958.

A seguito di siffatte pronunce di merito e di legittimità, si è provato a chiarire i tratti caratterizzanti di questo nuovo diritto che si affacciava su un panorama giuridico destinato a mutare in seguito all'entrata in vigore della Carta costituzionale del 1948 [9].

A tal riguardo la dottrina aveva elaborato un concetto di oblio (quale estrinsecazione del diritto alla riservatezza) da intendere come "diritto all'anonimato", che si manifestava nell'effettiva possibilità per gli interessati a far dimenticare alla collettività determinati episodi della propria esistenza con l'unico limite consistente nella facoltà di diffondere comunque tali notizie laddove fossero di interesse per la società [10].

3. La Corte di Cassazione sancisce la nascita del diritto all'oblio in Italia

Le pronunce fin qui esaminate hanno analizzato soltanto marginalmente il diritto all'oblio, il quale è stato invece riconosciuto espressamente, poiché meritevole di protezione, solo nell'ultimo lustro del secolo scorso.

Il 1998 segna la data di nascita in Italia del diritto all'oblio, figlio di una storica pronuncia del supremo organo di giustizia ordinaria [11].

In tale statuizione, i giudici di legittimità ne hanno delineato i connotati salienti, definendolo come l'interesse accordato ad ogni persona affinché la propria reputazione non sia lesa in maniera imperitura dalla reiterata pubblicazione di notizie, già divulgate legittimamente in passato.

Tuttavia, siffatto principio deve essere bilanciato con l'interesse all'informazione che sorge ogni qualvolta un accadimento precedente ritorni, in virtù di fatti sopravvenuti, di attualità.

A tal riguardo, in ossequio altresì ad un precedente *dictum* della Cassazione [12] (occupatosi però solo trasversalmente della specifica questione in esame),

---

[9] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014; A. ROUVROY, *"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data*, Council of Europe, Directorate General of Human Rights and Rule of Law, vol. T-PD-BUR(2015)09REV, 2016, reperibile su http://works.bepress.com/antoinette_rouvroy/64/.

[10] Sul punto *ex multis* F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità di fatti criminosi*, in *Archivio giuridico*, 1968, 40 ss.; F. CARNELUTTI, *Diritto alla vita privata,* in *Riv. trim. dir. pubbl*. 1955, I, 3 ss.; A. DE CUPIS, *I diritti della personalità*, Giuffrè, Milano, 1982, 55; A.T. AULETTA, *Riservatezza e droit all'oubli*, in AA.VV., *L'informazione ed i diritti della persona*, Jovene, Napoli, 1983, 129 ss.

[11] Cass., 09.04.1998, n. 3679, in *Mass. Giur. it*., 1998.

[12] Cass., 27.05.1975, n. 2129, in *Mass. Giur. it*., 1975.

la concretizzazione della lesione all'onore ed alla reputazione può avvenire a patto che il diritto di cronaca presenti tre requisiti fondamentali: la verità oggettiva dell'informazione divulgata; la pertinenza, ossia l'effettivo interesse pubblico alla conoscenza dell'accadimento; la continenza, consistente nella correttezza formale dell'esposizione.

In un'ottica di continuità dell'*iter* intrapreso dai giudici di ultima istanza, la sentenza del '98 ha segnato il primo di una serie di interventi giurisprudenziali nel cui novero giova richiamare una statuizione del 2008 [13] tramite la quale si prevede perentoriamente che il fondamento dell'oblio è da rinvenire nell'art. 2 Cost., quale forma di estrinsecazione del diritto alla riservatezza, dal quale però si differenzia per il fattore temporale [14].

Difatti, il diritto all'oblio attrae nella propria sfera di afferenza informazioni non più riservate, delle quali però si vuole evitare una nuova pubblicazione, stante l'inutilità sociale della riproposizione delle stesse.

Dunque, è proprio alla luce di tali osservazioni che alcuni teorici hanno espresso la volontà di annoverare il diritto all'oblio fra i diritti di nuovo conio che, sebbene non siano esplicitamente contemplati dalla Costituzione, tutelano comunque in maniera significativa la personalità dell'individuo garantita dall'art. 2 della Carta fondamentale [15].

3.1 Segue: l'espansione del diritto all'oblio

Preso atto del panorama giurisprudenziale connotato dal crescente interesse nei confronti di un concetto di oblio ormai non più così estraneo agli interpreti delle scienze giuridiche, a partire dal 2012 [16] si susseguono molteplici pronunce dalle quali si evince l'ampliamento della definizione del "*droit all'oubli*".

In un primo provvedimento si asserisce che un giornalista possa divulgare i

[13] Cass., 09.06.2008, n. 5658, in *Mass. Giur. it.*, 2008.

[14] E. LIGI, *Il diritto alle vicende e la sfera della personalità*, in *Foro it.*, 1955, volume 1, 394 ss.; E. CARNELUTTI, *Diritto alla vita privata*, in *Rivista trimestrale di diritto pubblico*, 1955, volume 1, pagg. 3 ss.; V. ZENO-ZENCOVICH, *Una svolta giurisprudenziale nella tutela della riservatezza*, in *Diritto dell'informazione e dell'informatica*, 1986, volume 1, 934 ss.; M. LOSANO, I *progetti di legge italiani sulla riservatezza di dati personali*, relazione presentata al convegno Integrazione di informatica e diritto, atti del convegno, FAST, Milano 1983, 1-15.

[15] T.E. FROSINI, *Il diritto all'oblio e la libertà informatica*, in *Il diritto dell'informazione e dell'informatica*, n. 4/5, 2012, nonché in *Libertè Egalitè Internet*, Napoli, 2016, 120 ss.; F.C. SALVADORI, *Il diritto all'oblio tra diritto alla riservatezza e diritto di cronaca*, in *Dialoghi*, 2013, volume 4, 141-157.

[16] Cass., 12.10.2012, n. 17408, in *Mass. Giur. it*., 2012.

dati personali sensibili di un individuo purché l'informazione risulti "essenziale" secondo quanto previsto dal relativo codice deontologico [17].

Nello stesso anno il Supremo Collegio [18] si è occupato di una vicenda che ha condotto i giudici di legittimità alla valorizzazione dell'art. 11 del summenzionato codice deontologico, che richiede, in sede di divulgazione di notizie inerenti al passato, l'ossequiosa osservanza dell'informazione dei principi di proporzionalità, di pertinenza e di non eccedenza.

Il nucleo fondamentale comune ad entrambi i casi attiene alla possibilità che il diritto all'informazione di cui all'art. 21 Cost., laddove concerna un interesse pubblico, possa prevalere sul diritto alla riservatezza. La legittimità della divulgazione, tuttavia, permarrà soltanto finché la notizia venga opportunamente aggiornata.

Da ciò si evince che laddove, invece, tale aggiornamento non sia avvenuto oppure che la connessione fra ripubblicazione di un accadimento ed interesse pubblico sia impropria, allora il diritto *ex* art. 21 Cost. dovrà soccombere rispetto al diritto alla riservatezza ("subspecie" di diritto all'oblio).

Come accennato all'inizio del presente lavoro, la tematica del "diritto ad essere dimenticati" ha coinvolto diverse branche dell'ordinamento giuridico e, difatti, in ambito penale particolare attenzione (e scalpore) ha destato la pubblicazione su un noto quotidiano nazionale di un fatto di sangue passato che ha visto come protagonista Vittorio Emanuele di Savoia. Infatti, in occasione della cerimonia di riapertura della Reggia di Venaria, alla quale aveva presenziato il figlio dell'ultimo Re d'Italia, veniva riproposto sul suddetto giornale l'uccisione da parte di quest'ultimo perpetrata ai danni di un altro uomo.

In tal caso, i giudici di piazza Cavour [19] hanno chiarito che il diritto all'oblio deve soggiacere all'interesse della collettività ad essere informata sugli accadimenti da cui dipende la formazione dei propri convincimenti, i quali, nella vicenda di specie, non possono essere messi in secondo piano, stante la notorietà del personaggio di primario rilievo coinvolto.

---

[17] Cfr. Codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (art. 25 legge n. 675/96). In particolare si guardi l'art. 6 rubricato "essenzialità dell'informazione" ai sensi del quale:

"1. La divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti.

2. La sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica.

3. Commenti e opinioni del giornalista appartengono alla libertà di informazione nonché alla libertà di parola e di pensiero costituzionalmente garantita a tutti".

[18] Cass., 12.10.2012, n. 17408, in *Mass. Giur. it*., 2012.

[19] Cass., 03.08.2017, n. 38747, in *Mass. Giur. it.*, 2017.

4. Il riconoscimento del “diritto alla cancellazione" da parte dei giudici eurounitari

Analizzata la “galassia” giurisprudenziale italiana nella quale è nato e si è sviluppato il “diritto ad essere dimenticati”, ora occorre rilevare come la tematica dell’oblio sia stata costellata da diverse pronunce anche in ambito sovranazionale, una delle quali in particolare ha tracciato il sentiero per il riconoscimento espresso di tale diritto a livello eurounitario.

In chiave ermeneutica si è cercato di individuare le radici del diritto all’oblio nell’art. 8 CEDU [20] che sancisce il rispetto alla vita familiare in combinato disposto con l’art. 7 della Carta di Nizza, il cui art. 8 [21], poi, disciplina la protezione dei dati personali non a caso inserito nel titolo relativo alle “libertà” [22].

Una tutela, seppure indiretta, si rinveniva nella direttiva 95/46/CE (abrogata dal GDPR n. 679/2016) al cui art. 12 lett. b) veniva riconosciuto all’interessato per la prima volta nella storia del diritto europeo un vero e proprio “diritto alla cancellazione” dei propri dati personali [23].

Come accennato ad inizio capitolo, una sentenza in particolare ha destato clamore giacché ha consacrato il riconoscimento del diritto all’oblio in ambito unionale.

---

[20] “*1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*

2. Non può esservi ingerenza di una autorità pubblica nell’esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell’ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui”.

[21] *“1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un’autorità indipendente”.

[22] F. Di Ciommo, *Diritti della personalità tra media tradizionali e avvento di internet*, in G. Comandè (a cura di), *Persona e tutele giuridiche*, Torino, 2003, *passim*; A. Mantelero, *Attività di impresa in Internet e tutela della persona*, Cedam, Padova, 2004, 146 ss. V., inoltre, G. Ramaccioni, *La protezione dei dati personali e il danno non patrimoniale*, Jovene, Napoli, 2017, 242 ss.; G. De Gregorio e R. Torino, *Privacy, protezione dei dati personali e big data*, in E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Lefebvre, 2019, 478 ss.

[23] Sul punto v. D. Poletti e M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (a cura di), *Privacy Digitale*, cit., 369 ss.

Il riferimento è al caso "Google Spain"[24], tramite cui i giudici europei hanno cercato di individuare un punto di equilibrio fra l'interesse all'informazione ed i diritti fondamentali della persona[25].

La vicenda vedeva come protagonista un cittadino spagnolo, il quale digitando il proprio nome sul motore di ricerca Google rinveniva diversi articoli concernenti un fatto passato che lo riguardava avente ad oggetto un pignoramento avvenuto nei suoi confronti in ordine alla riscossione coattiva di tributi previdenziali da parte del Fisco spagnolo.

Egli lamentava l'assenza di attualità delle notizie ancora presenti su *Internet* dal momento che aveva già compiutamente estinto tale debito in seguito al regolare svolgimento dell'esecuzione forzata da lui subita.

Presentava pertanto ricorso al fine di ottenere la cancellazione dei vari articoli *online* che descrivevano tale vicenda.

La Corte di Giustizia, investita della causa, emana una serie di principi fondamentali. Innanzitutto, essa afferma il "diritto alla cancellazione" delle informazioni personali attinenti a vicende passate che non rivestano più alcun interesse pubblico.

Difatti, il fine che si vuole perseguire consiste nella possibilità per il singolo individuo di non rivenire (in misura talvolta anche copiosa) articoli in rete, tramite la digitalizzazione del proprio nome, che lo riguardino in relazione a quella specifica vicenda e ciò prescindendo da eventuali danni effettivi che gli potrebbero essere arrecati da tale situazione.

Inoltre, i giudici europei affermano che il "diritto alla cancellazione" delle informazioni personali sarebbe legittimo "*non soltanto se i dati sono inesatti, ma anche se sono inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, oppure non aggiornati o conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si impegna per motivi storici, statistici o scientifici*".

---

[24] CGUE, 13.05.2014, C-131/12, ECLI:EU:C:2014:317, disponibile su http://curia.europa.eu.

[25] T.E. Frosini, O. Pollicino, G. Finocchiaro, G. Caggiano, P. Piroddi, G. Sartor, M. Viola De Azevedo Cunha, A. Mantelero, S. Sica, V. D'Antonio, C. Comella, G.M. Riccio, R. Flor, F. Pizzetti, in G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, RomaTrE-Press, Roma, 2015, http://romatrepress.uniroma3.it/ojs/index.php/oblio; F. Fontanelli, *The Mythology of Proportionality in Judgments of the Court of Justice of the European Union on Internet and Fundamental Rights*, in *Oxford Journal of Legal Studies*, 2016, n. 3, 630-660; D. Miniussi, *Il "diritto all'oblio": i paradossi del caso Google*, in *Rivista italiana di diritto pubblico comunitario*, 2015, n. 1, 209-234; E. Bassoli, *Il diritto all'oblio nella recente giurisprudenza della Corte di giustizia*, http://www.pensareildiritto.it/il-diritto-alloblio-nella-recente-giurisprudenza-della-corte-di-giustizia/; H. Kranenborg, *Google and the Right to be Forgotten*, in *European Data Protection Law Review*, 2015, n. 1, 70-79; T. Scannicchio, *Tutela della privacy: motori di ricerca e diritto all'oblio*, in *Giur. it*., 2014, n. 6, 1323-1325.

Dunque, siffatto diritto promana dagli artt. 7 e 8 della Carta di Nizza testé riportati, in virtù dei quali esso tendenzialmente prevarrebbe sull'interesse economico del motore di ricerca a pubblicare la notizia, salvo che quest'ultima non rivesta una particolare rilevanza in termini di interesse della collettività in ragione, ad esempio, dalla carica pubblica rivestita dal protagonista della vicenda [26].

Sul punto, infatti, la Corte di Giustizia stabilisce che "*anche nel caso in cui il trattamento di dati personali effettuato dal motore di ricerca Internet sia lecito, il soggetto titolare dei suddetti dati può rivolgersi direttamente al gestore del motore di ricerca quale titolare del trattamento per vedere riconosciuto il proprio diritto all'oblio ed ottenere così la rimozione del dato contestato, dovendo tuttavia dimostrare l'inadeguatezza di questo, la non pertinenza o l'eccessività rispetto alle finalità di indicizzazione*".

In relazione al "caso Google", i giudici europei riconoscono concretamente nei confronti dell'interessato il diritto alla cancellazione degli articoli *online* inerenti a quella specifica vicenda. Le motivazioni che accordano tale "beneficio" al ricorrente risiedono nella non attualità delle informazioni, essendo decorsi ormai molti anni dall'accadimento, ed inoltre nel fatto che egli non rivesta alcuna carica di interesse pubblico.

Nel solco tracciato dalla sentenza esaminata si registrano due ulteriori pronunce dei giudici eurounitari. Con la prima la Corte di Giustizia, nel caso "*Google c. CNIL*" [27], ha sancito che non vi è l'obbligo per il gestore del motore di ricerca di procedere alla deindicizzazione, relativa al soggetto richiedente, anche nei paesi extra-europei. Si tenga conto che tale operazione consiste specificamente nella cancellazione dalla rete telematica di tutti gli articoli afferenti a quella determinata persona.

Tale statuizione ha lasciato non poche perplessità considerato che limitando l'oblio nei confini continentali si lascerebbe il "vaso di Pandora" ancora parzialmente scoperchiato [28].

Nella seconda delle sentenze testé menzionate [29] ("*caso Facebook"*), i giudici unionali segnano un ulteriore passo in avanti nell'ottica del riconoscimento

---

[26] Sul punto v. CGUE (Grande Camera), 24.09.2019, C-507/2017, ECLI:EU:C:2019:772; CGUE (Grande Camera), 24.09.2019, C-126/2017, ECLI:EU:C:2019:773, disponibili su http://curia.europa.eu.

[27] CGUE, 24.09.2019, C-507/17, ECLI:EU:C:2019:772, disponibile su http://curia.europa.eu.

[28] A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, 419; sul punto si veda anche C. PERLINGIERI, *Gli accordi tra i siti di social networks e gli utenti*, in *Rass. dir. civ.*, 2015, 115.

[29] CGUE, 03.10.2019, C-18/18, ECLI:EU:C:2019:821, disponibile su http://curia.europa.eu.

del diritto all'oblio a livello mondiale e sembrerebbero aver colmato la lacuna lasciata dal *dictum* precedente. Lo scrutinio di tale vicenda ha condotto la Corte di Giustizia ad affermare che le autorità giudiziarie nazionali dei singoli paesi dell'U.E. hanno il potere di ordinare al noto *social network Facebook* di eliminare qualsiasi articolo *online d*a cui possa derivare un nocumento per il soggetto interessato alla cancellazione. Il profilo innovativo della questione di cui trattasi risiede nella circostanza che tale espunzione non opera soltanto all'interno del perimetro unionale, ma si estende al mondo intero [30].

Ebbene, alla luce dei sensazionali sviluppi avvenuti sul tema anche da parte della giurisprudenza sovranazionale si può fornire una definizione del diritto all'oblio, già cara ad alcuni studiosi [31], quale espressione peculiare del diritto alla riservatezza e del legittimo interesse a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria persona.

5. Art. 17 GDPR n. 679/2016: la regolamentazione del diritto all'oblio nella sua natura "composita"

La sentenza della Corte di Giustizia sul "caso Google" ha segnato la strada maestra ai fini dell'espresso riconoscimento del diritto all'oblio da parte del legislatore euronitario, il quale lo ha compiutamente disciplinato all'art. 17 del Regolamento Generale sulla Protezione dei Dati dell'U.E. del 27 aprile 2016, n. 679, c.d. GDPR [32].

Il "diritto alla cancellazione" si colloca in un'ottica di piena coerenza con l'art. 1 del testo legislativo di cui trattasi che annovera la protezione delle informazioni personali fra i diritti fondamentali della persona [33].

Il summenzionato art. 17 contempla le tre declinazioni del diritto all'oblio: il diritto ad essere dimenticato e a non vedere danneggiati onore e reputazione per

---

[30] In questo senso v. G. RESTA, *Diritti fondamentali e diritto privato nel contesto digitale*, in F. CAGGIA e G. RESTA (a cura di), *I diritti fondamentali in Europa e il diritto privato*, Roma Tre-Press, Roma, 2019, 128 ss.; cfr. AGCM, 11.5.2017, n. 26597, WhatsApp-Trasferimento Dati a Facebook, in Bollettino n. 18/2017, 57, nonché AGCM, 11.5.2017, n. 26596, WhatsApp-Clausole Vessatorie, in Bollettino n. 18/2017.

[31] T.E. FROSINI, *op. cit.*; A.L. VALVO, *Il diritto all'oblio nell'epoca dell'informazione digitale*, in *Studi sull'integrazione europea*, X (2015), 347-357; R. SERAFINO, *I diritti della personalità*, Cedam, Padova, 2013, 70 ss.

[32] Attuato nell'ordinamento legislativo italiano per mezzo del D.lgs. 10 agosto 2018, n. 101.

[33] E. MOSTACCI, *La soft law nel sistema delle fonti: uno studio comparato*, Milano, 2008, 70 ss.; A. SOMMA, *Soft law sed law: diritto morbido e neocorporativismo nella costruzione dell'Europa dei mercati e nella distruzione dell'Europa dei diritti*, 2008, in *Rivista critica del diritto privato*, 437 ss.

la reiterazione di pubblicazione di notizie inizialmente (e legittimamente) divulgate; la pretesa alla corretta e aggiornata contestualizzazione della notizia originariamente pubblicata sul sito sorgente; il diritto e la pretesa alla deindicizzazione dei dati [34].

Infatti, il diritto dell'interessato affinché il titolare del trattamento proceda alla cancellazione dei suoi dati personali potrà avvenire purché essi non siano più necessari per le ragioni per le quali sono stati raccolti [35].

La nuova disciplina, quindi, attribuisce un ruolo preminente al titolare del trattamento poiché questi, laddove sussista il diritto all'oblio, deve necessariamente eliminare il dato personale [36]. Inoltre, egli in attuazione del principio di ragionevolezza, come noto derivante dall'art. 3 Cost., deve informare anche gli altri eventuali titolari del trattamento che sono in possesso dei dati personali dell'interessato affinché provvedano a cancellarli [37].

A tal riguardo, riprendendo alcuni profili già inseritisi nel solco tracciato dal c.d. "codice privacy" [38], viene precisato che il soggetto che richiede l'eliminazione deve essere sempre necessariamente identificato o quantomeno identificabile.

Infatti, come ritenuto da alcuni studiosi [39], il diritto all'oblio si rapporta ad un altro diritto della personalità di nuova emersione: quello all'identità personale. Laddove venga nuovamente divulgata una notizia appartenente al passato, è indispensabile tenere conto dell'identità della persona e di ciò che la stessa è diventata, non potendo la riproposizione della notizia alterare la personalità attuale dell'individuo [40].

---

[34] S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?*, in *federalismi.it*, 2018; D. BARBIERATO, *Osservazioni sul diritto all'oblio e la (mancata) novità del Regolamento UE 2016/679 sulla protezione dei dati personali*, in *Resp. civ. e previd.*, 2017, 2100 ss.

[35] Sul punto cfr. S. SASSI, *Diritto transnazionale e legittimazione democratica*, Milano, 2018, 56 ss.

[36] R. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leggi civili commentate*, 2017, 1023 ss.

[37] L. GATT, R. MONTANARI, I. A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, 339.

[38] Codice in materia di protezione dei dati personali, D.lgs. 30 giugno 2003, n. 196.

[39] Sul punto ampiamente S. RODOTÀ, *Il diritto di avere diritti*, Editori Laterza, Bari, 2013.

[40] L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016, 263; E. STRADELLA, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?*, in *Rivista dell'Associazione Italiana dei Costituzionalisti*, 2016, n. 4.

Alla luce delle considerazioni fin qui svolte, l'aspetto che presenta maggiore pregnanza, specialmente ai fini del presente articolo, risiede nella circostanza in base alla quale il diritto all'oblio non è assoluto, bensì deve essere oggetto di bilanciamento con gli altri diritti fondamentali con i quali si pone in conflitto.

6. I delicati rapporti fra il "diritto ad essere dimenticati" ed il diritto di cronaca: criteri di bilanciamento in chiave costituzionale

Alla luce di siffatta ricostruzione normativa e giurisprudenziale, foriera di non poche perplessità è stata la questione attinente al bilanciamento dei valori costituzionali che vengono in rilievo in caso di conflitto fra il diritto di cronaca, come noto posto al servizio dell'interesse pubblico all'informazione (art. 21 Cost.), ed il diritto all'oblio, finalizzato, invece, alla tutela della riservatezza della persona [41].

Tale *vexata quaestio è* stata analizzata di recente in ordine al "caso Venditti" [42], concernente il contenzioso sorto fra il famoso cantante ed una nota trasmissione televisiva.

Lo scrutinio dei profili dirimenti per la questione in esame avviene alla luce del GDPR n. 679/2016, nonché della giurisprudenza eurounitaria (in particolare con riguardo al "caso Google Spain") e di quella interna (prevalentemente della Cassazione) [43].

In primo luogo si rileva che il diritto all'oblio può soccombere rispetto all'altrettanto fondamentale diritto di cronaca soltanto nel caso in cui quest'ultimo presenti determinati requisiti.

Essi sono individuati nel contributo arrecato ad un dibattito pubblico; nell'interesse effettivo ed attuale alla diffusione della notizia; nell'elevato grado di notorietà del soggetto rappresentato; nella modalità posta in essere per acquisire l'informazione, che deve essere connotata da verità ed in ultimo nella preliminare comunicazione circa la sua diffusione.

---

[41] G. CITARELLA, *"Diritto all'oblio" e rilevanza del tempo*, in *Responsabilità Civile e Previdenza*, 2016, III, 583; L. BUGIOLACCHI, *Quale responsabilità per il motore di ricerca in caso di mancata deindicizzazione su legittima richiesta dell'interessato?*, in *Responsabilità civile e previdenza*, 2016, II, 571 ss.; sul punto, si vedano anche G. SCORZA, *Corte di giustizia e diritto all'oblio: una sentenza che non convince*, in *Corr. giur.*, 2014, 1471; A. MANTELERO, *Diritto all'oblio e pubblicità del registro delle imprese*, in *Giur. it.*, 2015, 265.

[42] Cass., (ord.) 20.03.2018, n. 6919, in *Mass. Giur. it.*, 2018.

[43] A. SALARELLI, *Ancora sul diritto all'oblio: cosa cambia dopo la sentenza della Corte di Giustizia Europea contro Google*, consultabile su *JLIS.it*, Vol. 6, n. 1; O. POLLICINO, *"Google rischia di "vestire" un ruolo para-costituzionale",* in *Il Sole24Ore,* 15 maggio 2014.

In assenza di tali caratteristiche lo scorrere del tempo determinerà un'ineludibile violazione del diritto all'oblio.

Ebbene, il provvedimento sul "caso Venditti" è stato preso in considerazione nell'ordinanza interlocutoria con la quale la Cassazione rimetteva la trattazione una causa alle Sezioni Unite [44] che sarebbe di lì a poco divenuta una pietra miliare in tema di oblio [45].

La vicenda concerneva un omicidio perpetrato da un uomo nei confronti della moglie al quale era seguita la condanna a 12 anni di reclusione, regolarmente scontata dal reo in questione. Tuttavia, dopo molti anni, un giornale pubblicava nuovamente tale accadimento, di fatto rendendo vani gli sforzi di risocializzazione del protagonista del delitto, che intanto si era reinserito nel contesto sociale avendo anche trovato lavoro [46].

Alla luce di tali premesse l'ordinanza di rimessione si concentra sul contemperamento fra il diritto all'oblio e quello di cronaca.

Quest'ultimo rappresenta un diritto pubblico soggettivo che trova le sue radici nell'art. 21 Cost. ed i cui limiti, affinché non soccomba rispetto al diritto alla riservatezza, sono costituiti dall'utilità sociale dell'informazione, dalla verità oggettiva e dalla forma dell'esposizione che deve essere rispettosa della dignità individuale.

Tale diritto si differenzia da quello di critica dal momento che quest'ultimo si manifesta tramite congetture che quindi non assumono rilevanza al di fuori dell'orbita meramente soggettiva di chi lo esercita.

Il diritto all'oblio, invece, afferma la Cassazione che "*è collegato, in coppia dialettica, al diritto di cronaca e prevale su quest'ultimo quando non vi sia più un'apprezzabile utilità sociale ad informare il pubblico; ovvero la notizia sia diventata falsa in quanto non aggiornata o, infine, quando l'esposizione dei fatti non sia stata commisurata all'esigenza informativa ed abbia arrecato un vulnus alla dignità dell'interessato*".

I supremi giudici ritengono "*ormai indifferibile l'individuazione di univoci criteri di riferimento che consentano agli operatori del diritto (ed ai consociati) di conoscere preventivamente i presupposti in presenza dei quali un soggetto ha diritto di chiedere che una notizia, a sé relativa, pur legittimamente diffusa in*

---

[44] Cass., (ord.) 05.11.2018, n. 28084, in *Mass. Giur. it.*, 2018.

[45] G. FINOCCHIARO, *Le Sezioni Unite sul diritto all'oblio*, in *Giust. civ.*, 29 luglio 2019; V. CUFFARO, *Una decisione assennata sul diritto all'oblio*, in *Corr. giur.*, 2019, 1189 ss.; D. MUSCILLO, *Oblio e divieto di lettera scarlatta*, in *Danno e resp.*, 2019, 611 ss.

[46] A tal riguardo si tenga presente che la funzione della pena, ad oggi, è fortemente improntata sulla funzione rieducativa che la stessa deve espletare in ossequio al III comma dell'art. 27 Cost. ("*Le pene non possono consistere in trattamenti contrati al senso di umanità e devono tendere alla rieducazione del condannato*").

passato non resti esposta a tempo indeterminato alla possibilità di una nuova divulgazione".

Dunque, in base a tali presupposti le Sezioni Unite, in via preliminare, affermano che il caso di cui trattasi rientra nella prima delle tre accezioni accordate all'oblio in seno all'art. 17 GDPR n. 679/2016, ossia quella attinente al diritto ad essere dimenticato e a non vedere danneggiati onore e reputazione per la reiterazione di pubblicazione di notizie inizialmente (e legittimamente) divulgate.

Notevolmente interessante la distinzione che il Collegio effettua fra il diritto di cronaca e quello alla rievocazione storiografica di un fatto.

Nel primo assume fondamentale rilevanza la contestualizzazione del fatto divulgato in un determinato periodo di tempo, considerato che anche in relazione ad un evento passato possono subentrare dei nuovi elementi che di fatto gli consentono di riacquisire il connotato dell'attualità, funzionale ad un legittimo espletamento del diritto di cronaca.

Laddove manchi tale requisito dell'attualità, allora la rievocazione di un accadimento risalente nel tempo costituirà mero esercizio di un'attività di storiografia, la quale consiste proprio nella rievocazione di fatti che hanno riguardato la vita di un popolo.

Essa, tuttavia, quand'anche costituisse un'attività utile per la collettività non può di certo essere ammantata delle stesse garanzie costituzionali previste per il diritto di cronaca.

A tal riguardo, è opportuno rilevare, infatti, che quello di cronaca non è un diritto senza limiti, ed anzi esso deve essere ineludibilmente ancorato a precisi canoni di meritevolezza costituiti, come precedentemente esaminato, dall'utilità sociale dell'informazione, dalla verità oggettiva dei fatti, la cui esposizione deve pur sempre risultare rispettosa della dignità umana della persona cui si rivolge.

Pertanto si è ritenuto che il diritto all'oblio possa soccombere rispetto al diritto di cronaca soltanto in presenza di talune condizioni, fra le quali è possibile annoverare la natura pubblica dell'interesse suscitato dal dibattito relativo alla diffusione di una notizia concernente un determinato individuo, stante la sua notorietà.

A tal riguardo, le Sezioni Unite, però, hanno fornito copiose e più dettagliate argomentazioni inerenti all'individuazione di criteri di riferimento che consentano agli operatori del diritto di conoscere preventivamente i presupposti in presenza dei quali un soggetto ha diritto di chiedere che una notizia, a sé relativa, non resti esposta a tempo indeterminato alla possibilità di nuova divulgazione.

La sentenza, che ha costituito il risultato del perseguimento di tale finalità, ha esaminato la questione nella sua completezza, delineando in premessa un quadro sintetico della normativa sia nazionale che europea, procedendo, quindi,

alla disamina degli artt. 2, 3, 21 Cost., nonché della legge sulla stampa, del "codice privacy" e del testo unico dei doveri del giornalista [47].

La questione di diritto che viene portata all'attenzione delle Sezioni Unite consiste nella legittimità della ripubblicazione di quanto è stato già a suo tempo divulgato senza contestazioni.

A tal riguardo, occorre rilevare che la corretta premessa dalla quale bisogna muovere, al fine di indicare quale sia la linea di confine fra diritto di cronaca e diritto all'oblio, è che quando un giornalista pubblica nuovamente una notizia già divulgata, che all'epoca rivestiva un interesse pubblico, egli non sta esercitando il diritto di cronaca, quanto il diritto alla rievocazione storiografica di quei fatti.

Tuttavia, ciò non esclude che in relazione ad un evento del passato possano intervenire elementi nuovi tali per cui la notizia ritorni di attualità, di modo che diffonderla nel momento presente rappresenti ancora una manifestazione del diritto di cronaca.

In assenza di siffatti elementi, però, divulgare di nuovo una notizia del passato costituisce espletamento di un'attività per l'appunto storiografica, la quale, evidentemente, non può beneficiare della stessa garanzia costituzionale contemplata per il diritto di cronaca.

Sul punto, è necessario verificare se vi sia un particolare interesse a divulgare il nominativo della persona destinataria della notizia, che la stessa non vuole diffondere per rispetto del diritto all'oblio.

Infatti, è ben possibile che l'accadimento inerente a quel determinato individuo poteva suscitare il pubblico clamore dei fatti, divenendo, invece, irrilevante successivamente.

Dunque, al fine di dirimere la problematica attinente alla individuazione dei criteri di bilanciamento in ordine ai valori costituzionali venuti in rilievo in caso di conflittualità sorta fra diritto all'oblio (quale estrinsecazione del più generale diritto alla riservatezza) e diritto di cronaca, le Sezioni Unite hanno fornito pregnanti delucidazioni finali.

I giudici di piazza Cavour hanno chiarito che riproporre fatti del passato costituisce comunque espressione della libertà accordata ai giornalisti in virtù dell'art. 21 Cost.

Tuttavia, deve essere premura del giudice di merito, chiamato ad occuparsi del caso concreto, valutare la sussistenza dei requisiti di attualità, pubblicità e concretezza dell'indicazione degli elementi suscettibili di individuare specificamente il soggetto interessato dalla notizia.

Ebbene, il diritto di cronaca prevale sul diritto alla riservatezza ("subspecie"

[47] Approvato dal Consiglio nazionale di categoria il 26.01.2016.

di diritto all'oblio) soltanto nel caso in cui l'identificazione del soggetto protagonista della vicenda passata si giustifichi in virtù della notorietà relativa al ruolo pubblico rivestito da quest'ultimo.

Invece, laddove tale ultima connotazione di notorietà pubblica non sia rinvenibile, allora il diritto di cronaca risulta soccombente rispetto al diritto all'oblio.

Infatti, la preminenza di quest'ultimo deriva dalla volontà di evitare che il diritto di cronaca, esercitato mediante la ripubblicazione dell'ormai trascorsa vicenda, si riveli funzionale soltanto alla lesione della dignità della persona umana.

A tal riguardo, infatti, si evidenzia che risulterebbe particolarmente gravoso per la reputazione del destinatario dell'attività giornalistica trovarsi costantemente sotto l'imperitura "spada di Damocle" costituita, appunto, dalla ripubblicazione di quell'accadimento passato.

7. Riflessioni conclusive

Al termine dell'analisi svolta è possibile affermare che attualmente il diritto all'oblio ha acquisito piena autonomia concettuale, nonostante la sua natura composita, ed è stato espressamente riconosciuto a livello legislativo, nonché efficacemente applicato a livello giurisprudenziale sia in ambito nazionale che eurounitario.

La eminente rilevanza attribuita a tale diritto si evince prevalentemente dalla sua inclusione nei diritti (di nuovo conio) della personalità di cui l'art. 2 Cost. ne rappresenta l'invalicabile presidio.

Tuttavia, in un contesto come quello attuale in cui si parla di "società dell'informazione" (stante oltretutto la macroscopica pregnanza che ha assunto *Internet n*el mercato delle notizie), ad oggi è necessario contemperare il suesposto "diritto ad essere dimenticati" con il diritto di cronaca espressamente tutelato dall'art. 21 Cost.

Tale operazione di bilanciamento deve essere sempre effettuata in virtù dei principi di uguaglianza e di proporzionalità dal momento che, secondo una mirabile statuizione del Giudice delle leggi[48], non può esservi un decremento di tutela di un diritto fondamentale se ad esso non fa riscontro un corrispondente incremento di tutela di altro interesse di pari rango.

Dunque, è proprio in tale ottica che si colloca il bilanciamento fra oblio e cronaca attuato in concreto dalle Sezioni Unite. Infatti, alla luce di una Carta fondamentale che non individua una gerarchia di diritti fondamentali, spetta al giudice effettuare in concreto tale contemperamento.

[48] C. Cost., 20.06.2013, n. 143, disponibile su https://www.cortecostituzionale.it.

A tal riguardo nel presente articolo si è rilevato che, proprio nel rispetto dei canoni di eguaglianza e proporzionalità, il diritto all'oblio non può essere ritenuto sempre prevalente rispetto al diritto di cronaca. Difatti, occorrerà avere riguardo della ontologica differenza dei casi concreti in cui tali diritti vengono in rilievo e sarà altresì necessario individuare una giusta proporzione fra il sacrificio sotteso alla soccombenza dell'uno o dell'altro e il diritto che si intende tutelare.

La Corte di Cassazione non a caso in premessa ha affermato la non assolutezza del diritto "ad essere dimenticati", il quale senz'altro deve prevalere laddove non vi sia alcun interesse per la collettività alla riproposizione di un fatto che, se ripubblicato, potrebbe determinare un nocumento nei confronti del relativo protagonista. Parimenti, invece, dovrà soccombere dinanzi al diritto di cronaca (quando non si manifesta come mera storiografia) laddove, vista la caratura pubblica del richiedente l'eliminazione dell'informazione, vi sia un interesse pubblico alla divulgazione.

In conclusione del presente lavoro si può intuire questa estenuante corsa volta ad ottenere la cancellazione della propria persona dalla memoria collettiva laddove si aneli, giustamente, alla non riproposizione di eventi sgradevoli del proprio passato.

In un (infernale) gioco di "pesatura" dei diritti si voglia tenere conto, in una dimensione che esula dall'universo giuridico, che talvolta (quasi come all'epoca della *damnatio memoriae* romana) l'essere dimenticati può costituire un abisso incolmabile. "*L'oblio è una seconda morte che le anime grandi temono più della prima*" (Stanislas de Boufflers, in *Pensées, saillies et bons mots*, 1816).

LA VALUTAZIONE DELLA PROPORZIONALITÀ DELLE MISURE CHE LIMITANO I DIRITTI FONDAMENTALI DELLA PRIVACY NELLE NUOVE LINEE GUIDA DEL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

THE ASSESSMENT OF THE PROPORTIONALITY OF THE MEASURES THAT LIMIT THE PRIVACY FOUNDAMENTAL RIGHTS IN THE NEW GUIDELINES OF THE EUROPEAN DATA PROTECTION SUPERVISOR

SERGIO GUIDA

Independent Researcher, Data Governance & Privacy Sr Mgr

DANILO TOZZI

Consulente legale e DPO presso Studio Legale de Lima Souza

Abstract:

Il Garante europeo della protezione dei dati (sin d'ora "GEPD") ha avuto modo di osservare attentamente la dimensione che la protezione dei dati personali sta acquisendo negli ultimi anni nello spazio economico europeo, riconoscendo una ormai crescente attenzione operata dal legislatore in tutti gli stati membri ed in tutti i settori politici e in quasi tutte le iniziative condotte dalla Commissione Europea. Tale attenzione non è dovuta solo ad una maggiore consapevolezza dell'opinione pubblica, ma al fatto che la grande capacità di elaborazione dei dati permessa dalla tecnologia, impatta in modo considerevole sulla vita di ogni singolo cittadino. In questo quadro, in linea con lo sviluppo del Necessity Toolkit del 2017, che aveva delimitato l'ambito di operatività del concetto di necessità delle limitazioni ai diritti fondamentali, il GEPD ha adottato a dicembre 2019 le «Linee guida sulla proporzionalità», che definiscono ulteriormente il contenuto e lo scopo dei diritti garantiti dalla Carta fondamentale e dal Regolamento generale sulla protezione dei dati (sin d'ora «GDPR»), sviluppando un'analisi legale atta alla realizzazione di un vero e proprio test di proporzionalità da applicare al trattamento dei dati personali, con la realizzazione di una lista di controllo pratica per valutare la proporzionalità delle nuove misure legislative.

The European Data Protection Supervisor (EDPS) has been carefully observing the dimension that personal data protection has acquired in recent years in the European eco-

nomic area, recognizing a growing attention paid by the legislator in all states members, all political sectors and in almost all the initiatives conducted by the European Commission.
This attention is not only due to a greater awareness of public opinion, but to the fact that the huge data processing capacity allowed by technology causes a significant impact on each individual citizen's life. In this context, in line with the development of the 2017 Necessity Toolkit, which had delimited the scope of the concept of the need for limitations to fundamental rights, the EDPS adopted in December 2019 new «Proportionality guidelines».
These rules further define the content and purpose of the rights guaranteed by the Basic Charter and by the GDPR, developing a deep legal analysis aimed at creating a real proportionality test and practical tools to help assess the compliance of proposed EU measures that would impact the fundamental rights to privacy and the protection of personal data.

Parole-chiave: GEPD; Test di necessità e test di proporzionalità; Linee guida sulla proporzionalità.

Key-words: *EDPS; Necessity Toolkit; Proportionality Guidelines.*

Introduzione

Le nuove linee guida del Garante europeo della protezione dei dati (GEPD)[1] sulla valutazione della proporzionalità «mirano a fornire ai responsabili politici, degli strumenti pratici di valutazione della conformità delle misure UE proposte

[1] Le norme per la protezione dei dati nelle istituzioni dell'UE, nonché i compiti del Garante europeo della protezione dei dati (GEPD), sono stabiliti nel nuovo Regolamento (UE) 2018/1725. Queste norme sostituiscono quelle stabilite dal Regolamento (CE) n. 45/2001. Il GEPD è un'autorità di controllo indipendente sempre più influente con la precipua responsabilità di monitorare il trattamento dei dati personali da parte delle istituzioni e degli organi dell'UE, fornire consulenza sulle politiche e sulla legislazione che impattano sulla privacy e cooperare con autorità simili per garantire una protezione coerente dei dati. Le Linee guida sono state pubblicate il 19/12/2019.

che potrebbero avere un impatto sui diritti fondamentali della privacy e sulla protezione dei dati personali come delineata dalla Carta dei diritti fondamentali dell'Unione europea» [2].

Come si legge nella Press Release, «Wojciech Wiewiórowski, GEPD, ha dichiarato che: "Qualsiasi proposta di limitazione del diritto alla protezione dei dati personali deve essere conforme al diritto dell'UE. Ciò significa garantire che tale limitazione sia necessaria e proporzionale. Le nostre Linee guida sulla proporzionalità, combinate con il Necessity Toolkit pubblicato nel 2017 ("Necessity toolkit on assessing the necessity of measures that limit the fundamental right to the protection of personal data" [3], NdA), mirano a rendere la valutazione della necessità e della proporzionalità più rapida e semplice per i responsabili politici, aiutandoli a garantire che tutte le nuove proposte dell'UE rispettino il diritto fondamentale alla protezione dei dati personali» [4].

Il GDPR «si basa sull'articolo 8 [5] della Carta dei diritti fondamentali dell'Unione europea e sull'articolo 16 [6] del Trattato sul funzionamento dell'Unione europea, in base ai quali tutte le persone hanno il diritto alla protezione dei propri dati personali: l'UE deve pertanto emanare una legislazione conforme in tal senso e qualsiasi provvedimento in restrizione di tali diritti deve rispettare determinati criteri (i) deve essere previsto dalla legge; (ii) deve rispettare l'essenza del diritto fondamentale in questione e (iii) deve essere sia necessario che proporzionale, tenendo conto non solo degli obiettivi della misura stessa, ma anche della necessità di proteggere i diritti e le libertà in generale» [7].

Basandosi sulla giurisprudenza pertinente e sui recenti pareri legislativi del GEPD e sui commenti formali, le linee guida sulla proporzionalità del GEPD e

---

[2] Cfr. EDPS, *Press Release «EDPS publishes new Proportionality Guidelines aimed at making privacy-friendly policymaking easier»*, 18/12/2019, in https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-publishes-new-proportionality-guidelines_en.

[3] Il Toolkit, pubblicato in data 11.04.2017 risponde alle richieste, da parte delle istituzioni UE, di orientamento in merito requisiti derivanti dall'articolo 52, paragrafo 1, della Carta, in cui si afferma che ferma qualsiasi limitazione, deve sempre essere esercitato il diritto alla protezione dei dati personali (articolo 8 della Carta), diritto «necessario» per un obiettivo di interesse generale o per proteggere i diritti e le libertà altrui.

[4] Cfr. EDPS, *Press Release «EDPS publishes new Proportionality Guidelines aimed at making privacy-friendly policymaking easier»*, 18/12/2019, cit.

[5] R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Il Mulino - Bologna, 2001.

[6] P. COSTANZO, *Testi normativi per lo studio del diritto costituzionale italiano ed europeo. Vol.1*, Giappichelli, Torino, 2017.

[7] Cfr. EDPS, *Press Release «EDPS publishes new Proportionality Guidelines aimed at making privacy-friendly policymaking easier»*, 18/12/2019, cit.

il Necessity Toolkit «forniscono orientamenti pratici per aiutare ad affrontare queste dimensioni chiave sin dall'inizio del processo legislativo» [8] [...] «per assicurare che i diritti fondamentali siano sempre adeguatamente tutelati» [9].

1. Lo scopo delle Linee guida e come usarle

I diritti fondamentali, sanciti dalla Carta dei diritti fondamentali dell'Unione europea (di seguito «la Carta»), fanno parte dei valori fondamentali dell'Unione europea, che sono anche stabiliti nel Trattato sull'Unione europea (di seguito «TUE»): tra questi vi sono i diritti fondamentali alla privacy e alla protezione dei dati personali sanciti dagli articoli 7 e 8 della Carta che devono essere rispettati dalle istituzioni e dagli organi dell'UE anche quando elaborano e attuano nuove politiche o adottano nuove misure legislative. Anche altre norme sui diritti fondamentali svolgono un ruolo influente nell'ordinamento giuridico dell'UE, in particolare, quelle stabilite nella Convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. Le condizioni per eventuali limitazioni all'esercizio dei diritti fondamentali sono tra le caratteristiche più importanti della Carta perché determinano la misura in cui i diritti possono essere effettivamente goduti.

La necessità e la proporzionalità [10] di una misura legislativa che comporta una limitazione dei diritti fondamentali alla privacy e alla protezione dei dati personali sono un duplice requisito essenziale a cui devono conformarsi tutte le misure proposte che comportano il trattamento di dati personali. Tuttavia, garantire che la protezione dei dati diventi parte integrante del processo decisionale dell'UE richiede non solo una comprensione dei principi espressi nel quadro giuridico e nella giurisprudenza pertinente, ma anche la messa in campo di un'attenzione pratica e creativa volta alla soluzione di problemi complessi.

La Corte di giustizia dell'Unione europea (di seguito «CGUE») ha riconosciuto che la legislazione dell'UE deve spesso raggiungere diversi obiettivi di interesse pubblico, i quali a volte possono essere contraddittori, rendendo necessaria la messa a punto di un giusto equilibrio da raggiungere con i diritti fondamentali tutelati dall'ordinamento giuridico dell'UE. Tali diritti e interessi, come sancito dalla Carta, possono comprendere: il diritto alla vita (articolo 2) e all'integrità della persona (articolo 3); il diritto alla libertà e alla sicurezza (arti-

[8] Ibidem.

[9] Ibidem.

[10] AA.VV., *FRA Handbook, Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level, Guidance*, May 2018.

colo 6); libertà di espressione (articolo 11); libertà di condurre un'impresa (articolo 16); il diritto di proprietà, compresa la proprietà intellettuale (articolo 17); il diritto di accesso ai documenti (articolo 42). [11]

Le Linee guida sono state sviluppate per coadiuvare i legislatori dell'UE [12], una volta individuate le misure che incidono sulla protezione dei dati e le priorità e gli obiettivi alla base di tali misure, nel trovare soluzioni che minimizzino il conflitto tra le varie priorità e che possano definirsi armonizzate secondo un principio di proporzionalità. [13] Esse offrono una metodologia pratica e dettagliata per valutare la proporzionalità delle nuove misure legislative, fornendo spiegazioni ed esempi concreti.

Il GEPD osserva che, negli ultimi anni, la protezione dei dati personali è sempre più riconosciuta come una dimensione che deve essere considerata dal legislatore in tutti i settori politici e per quasi tutte le iniziative condotte dalla Commissione. Ciò non è dovuto solo a una maggiore consapevolezza dell'opinione pubblica, ma alla grande capacità di elaborazione dei dati e al notevole impatto sulla vita di ogni singolo cittadino.

È essenziale sottolineare che la necessità e la proporzionalità, sebbene strettamente collegate tra loro (entrambe le condizioni devono essere soddisfatte dalla legislazione), comportano due prove diverse. Ciò è reso evidente nella sezione III delle Linee guida dove viene elaborata la lista di controllo pratica per la proporzionalità, in base alla quale viene fornita la prima visione olistica del flusso di lavoro complessivo cui i legislatori sono chiamati. Le Linee guida consistono in un'introduzione, che ne definisce il contenuto e lo scopo, un'analisi legale del test di proporzionalità applicato al trattamento dei dati personali e in una lista di controllo pratica per valutare la proporzionalità delle nuove misure legislative. La checklist è il nucleo delle Linee guida e può essere utilizzata autonomamente.

---

[11] L'operazione che nelle nostre coordinate ordinamentali si traduce nel bilanciamento operato dal legislatore e sul cd. meta-bilanciamento della Consulta, v. G. ZAGREBELSKY, *Il diritto mite. Leggi diritti giustizia*, Einaudi, Torino, 1992, e R. BIN, *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzionale*, Giuffrè, 1992; v. anche F. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Giappichelli, 1995, pp. 94-103.

[12] Cfr. «Le Linee guida del GEPD, che rientrano nella cosiddetta "soft law", non avendo natura di regolamento vincolante, hanno il solo scopo di aiutare le istituzioni e i legislatori dell'UE a valutare la conformità delle nuove misure con la protezione dei dati personali, garantita dalla Carta dei diritti fondamentali, articoli 7 e 8 e dal GDPR» in A IANNOTTI DELLA VALLE, *The EDPS publishes the new Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data,* European Journal of Privacy Law & Technologies, 15/01/2020, in www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=36.

[13] Sull'ampio panorama delle linee guida v. anche B. PASTORE, *Soft law, gradi di normatività, teoria delle fonti* in Lavoro e diritto 17.1 (2003): 5-16.

Gli orientamenti si basano sulla giurisprudenza della CGUE, sulla Corte europea dei diritti dell'uomo (di seguito, «CEDU»), sui pareri del GEPD e del gruppo di lavoro «Articolo 29» (di seguito, «WP29») nonché su linee guida dell'European Data Protection Board (di seguito, «EDPB»).

Insieme al Necessity Toolkit, le Linee Guida forniscono un approccio comune alla valutazione della necessità e della proporzionalità delle misure legislative in relazione al diritto alla privacy e alla protezione dei dati personali. [14]

2. Il test di proporzionalità applicato alla privacy e alla protezione dei dati personali

2.1. Il test di proporzionalità nella valutazione della legalità di qualsiasi misura proposta che implichi il trattamento di dati personali

L'articolo 8 della Carta sancisce il diritto fondamentale alla protezione dei dati personali. Il diritto non è assoluto e può essere limitato, a condizione che le limitazioni siano conformi ai requisiti di cui all'articolo 52, paragrafo 1, della Carta. La stessa analisi si applica al diritto al rispetto della vita privata sancito dall'articolo 7 della Carta. [15]

Per essere lecita, qualsiasi limitazione all'esercizio dei diritti fondamentali tutelati dalla Carta deve quindi rispettare i seguenti criteri:

- deve essere prevista dalla legge;
- deve rispettare l'essenza dei diritti;
- deve conseguire obiettivi di interesse generale riconosciuti dall'Unione o la necessità di proteggere i diritti e le libertà altrui;
- deve essere necessaria – sulla scorta del focus disciplinato dal *Necessity Toolkit;*
- deve essere proporzionata: il fulcro di queste Linee guida.

Pertanto, la proporzionalità in senso lato (come indicato dalla CGUE) comprende sia la necessità che l'adeguatezza (proporzionalità in senso stretto) di una misura, vale a dire la misura in cui esiste un legame logico tra la misura e il

[14] CGUE, *Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010, paras. 89 und 86.

[15] M. Panebianco, *Repertorio della Carta dei diritti fondamentali dell'Unione europea: annotato con i lavori preparatori e la giurisprudenza delle alte Corti europee e della Corte costituzionale italiana*, Milano, 2001.

(legittimo) obiettivo perseguito. [16]

Affinché una misura rispetti il principio di proporzionalità, i vantaggi derivanti dalla misura non dovrebbero essere compensati dagli svantaggi che la misura comporta rispetto all'esercizio dei diritti fondamentali. Pertanto tale criterio «limita le autorità nell'esercizio dei loro poteri richiedendo di raggiungere un equilibrio tra i mezzi utilizzati e l'obiettivo previsto (o il risultato raggiunto)» [17]. Quest'ultimo elemento (l'equilibrio da raggiungere) descrive la proporzionalità in senso stretto in termini di adeguatezza e costituisce il test di proporzionalità che è l'oggetto delle Linee guida e che dovrebbe essere chiaramente distinto dalla necessità sia dal punto di vista concettuale che pratico.

2.2. Chiarimenti sul rapporto tra proporzionalità e necessità

Come specificato nel Necessity Toolkit, «la necessità implica una valutazione combinata e basata sui fatti dell'efficacia della misura per l'obiettivo perseguito e se sia meno invasiva rispetto ad altre opzioni per raggiungere lo stesso obiettivo» [18]. Il test di necessità dovrebbe essere considerato come il primo passo a cui deve conformarsi una misura proposta che comporta il trattamento di dati personali, sicché una misura che non si è dimostrata necessaria non dovrebbe essere proposta a meno che e finché non sia stata modificata per soddisfare il requisito della necessità: in altre parole, la necessità è una condizione preliminare per la proporzionalità.

Quindi, una volta che una misura legislativa è ritenuta necessaria, dovrebbe essere esaminata in base alla sua proporzionalità. Un test di proporzionalità generalmente implica la valutazione di quali «salvaguardie» dovrebbero accompagnare una misura al fine di ridurre i rischi, posti dalla misura prevista per i diritti e le libertà fondamentali delle persone interessate, a un livello accettabile/proporzionato.

---

[16] Scivoloso ma necessario il confronto con il concetto di proporzionalità quale categoria amministrativistica, su cui v. A. SANDULLI, *La proporzionalità dell'azione amministrativa*. Cedam (Wolters Kluwer Italia), 1998; sul fronte costituzionalistico v. anche M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana. Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola*. Roma: Palazzo della Consulta. 2013, o G. SCACCIA, "*Il principio di proporzionalità*" in S. MANGIAMELI (a cura di), *L'ordinamento europeo. II. L'esercizio delle competenze* , Milano, Giuffre 2006 : 225-274.

[17] EUROPEAN COURT OF HUMAN RIGHTS-ECHR, Case of Szabo and Vissy v. Hungary, paragraph 73.

[18] Riprendendo molti degli argomenti trattati dal WP29, *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation*, 13/5/2013.

Un altro fattore da considerare nella valutazione della proporzionalità di una misura proposta è l'efficacia delle misure esistenti oltre a quella proposta. Se esistono già misure per uno scopo simile o uguale, la loro efficacia dovrebbe essere sistematicamente valutata nell'ambito della valutazione della proporzionalità. Senza una tale valutazione circa l'efficacia delle misure esistenti che perseguono uno scopo simile o uguale, il test di proporzionalità per una nuova misura non può essere considerato debitamente eseguito.

2.3. Conclusione: proporzionalità nella legislazione sulla protezione dei dati. Un concetto "basato sui fatti" che richiede una valutazione caso per caso da parte del legislatore dell'UE

La comparsa di un requisito di proporzionalità è stata considerata uno degli sviluppi più sorprendenti dell'ultimo decennio nella legislazione europea sulla protezione dei dati: il trattamento dei dati deve essere proporzionato rispetto allo scopo legittimo perseguito e deve riflettere in tutte le fasi del trattamento un giusto equilibrio tra tutti gli interessi in gioco.

Al centro della nozione di proporzionalità si trova l'esercizio di una attività di bilanciamento [19]che richiede la ponderazione dell'intensità dell'interferenza rispetto all' importanza dell'obiettivo raggiunto nel contesto dato. Pertanto, la chiarezza della misura che limita i diritti fondamentali alla privacy e/o alla protezione dei dati è un prerequisito per l'identificazione dell'interferenza della norma in esame. Il peso dell'interferenza, a sua volta, è necessario per verificare se l'impatto su questi diritti fondamentali è proporzionato all'obiettivo perseguito. Come affermato dalla CGUE, quella di proporzionalità è una valutazione concreta, condotta caso per caso, un'analisi da condurre sempre contestualmente alla progettazione di una norma e che non può aver luogo senza aver prima identificato il contesto della misura in esame.

L'apparato delle Linee guida mira ad aiutare il legislatore a porsi la giusta serie di domande, tenendo conto delle questioni più pertinenti e ricorrenti in materia di protezione dei dati [20]. La seguente lista di controllo mira anche a stimo-

[19] Ancora sul punto v. G. PINO, *Conflitto e bilanciamento tra diritti fondamentali. Una mappa dei problemi, Ethics & Politics, vol.1*, Palermo, 2006.

[20] Cfr. «Fornendo una procedura pratica "step by step" per soddisfare la "proporzionalità" delle misure, possiamo fare riferimento a queste Linee guida del 2019 come a un "Proportionality Toolkit" » in A. IANNOTTI DELLA VALLE, *The EDPS publishes the new Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data,* European Journal of Privacy Law & Technologies, 15/01/2020, in www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=36, cit.

lare il cd. pensiero «out of the *b*ox», portando a scelte *ex ante* innovative e aiutando nel monitoraggio e nella valutazione *ex post* delle misure da adottare.

3. Lista di controllo per la valutazione della proporzionalità di nuove misure legislative

3.1. Descrizione generale del flusso di lavoro

La valutazione generale della necessità e della proporzionalità (visione sinottica) è la seguente:

Test 1. Per quanto riguarda la necessità (test di necessità), i passaggi ("Step") raccomandati nel Necessity Toolkit sono:

1. descrizione fattuale della misura da introdurre;
2. identificazione dei diritti fondamentali e delle libertà limitati dal trattamento dati da porre in essere;
3. definizione degli obiettivi della misura;
4. scelta dell'opzione più efficace e meno invasiva.

Test 2. Per quanto riguarda poi la proporzionalità (test di proporzionalità), i passaggi indicati nel Proportionality Toolkit sono i seguenti:

1. valutare l'importanza dell'obiettivo e in che modo la misura possa raggiungerlo;
2. valutare lo scopo, l'estensione e l'intensità dell'inferenza ingenerata dalla misura;
3. procedere ad un equo bilanciamento della misura;
4. se la misura non è proporzionata, identificare ed introdurre le adeguate clausole di salvaguardia.

Qui lo Step 2, ovvero «valutare la portata e l'intensità dell'interferenza in termini di impatto effettivo della misura sui diritti fondamentali della privacy e della protezione dei dati» è l'altra fase chiave del test di proporzionalità.

Ricordando che i diritti e le libertà fondamentali limitati dalla misura sono già stati identificati nella seconda fase del test di necessità (test 1), in questa fase vanno riconsiderati questi diritti e libertà fondamentali al fine di accertare, ancora *ex ante,* ma in concreto, come sarebbero interessati dalla limitazione. In effetti, la misura non dovrebbe imporre un onere sproporzionato ed eccessivo alle persone colpite dalla limitazione in relazione all'obiettivo perseguito.

È importante notare che l'impatto può essere «minore» per l'individuo in questione, ma comunque significativo o altamente significativo per la società

nel suo complesso (impatto sugli individui vs. impatto sulla società nel suo insieme). Esempi ipotetici potrebbero riguardare:

• danno al processo elettorale e politico (uso improprio di dati per manipolazione politica [21]);
• profilazione illegale e discriminazione che causano sfiducia nei confronti delle autorità pubbliche;
• effetto agghiacciante sulla libertà di espressione a causa di una sorveglianza omnicomprensiva o altri effetti negativi sulla libertà delle persone derivanti da un sistema di profilazione e valutazione pervasivo ed attuato sistematicamente.

Come si vede, l'impatto di questa fase riguarda anche il potenziale effetto dannoso della misura su una base più ampia di quella della protezione della privacy, includendo quindi i rischi per altri diritti fondamentali. Ciò è in linea con l'approccio adottato dal GDPR che si riferisce esplicitamente e in più occasioni ai «rischi per i diritti e le libertà delle persone fisiche», sottolineando così il fatto che un effetto dannoso per il diritto alla privacy è spesso indissolubilmente legato ad altri diritti fondamentali, quali la libertà di espressione e la libera circolazione e ai principi generali del diritto dell'UE come quello di non discriminazione.

4. Guida operativa

L'impatto della norma dovrebbe essere sufficientemente descritto per consentire una chiara comprensione della portata e del livello dell'interferenza sui diritti fondamentali della privacy e della protezione dei dati personali che si viene a creare. È particolarmente importante identificare con precisione:

• l'impatto della misura: valutando le limitazioni del campo di applicazione della misura stessa, il numero di persone colpite, l'esistenza di intrusioni collaterali, ovvero di interferenze con la privacy di persone diverse dai soggetti direttamente coinvolti dalla misura che si intende porre in essere;
• l'estensione della misura: in che termini viene limitato il diritto fondamentale, la quantità di informazioni che vengono raccolte, per quanto tempo le informazioni vengono raccolte, in che termini la misura in esame richiede la raccolta e l'elaborazione di categorie speciali di dati;

[21] Celebre lo scandalo Facebook/Cambridge Analytica. Su cui C. CADWALLADR, E. GRAHAM-HARRISON *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,* in The Guardian 17/3/2018; J. ISAAK, MJ. HANNA, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, Computer 51.8 (2018): 56-59.

• il livello di invadenza della misura: tenendo conto della natura dell'attività soggetta al provvedimento restrittivo, del contesto, se si tratta ovvero della profilazione delle cd. persone interessate o meno, se il trattamento comporta l'uso di un sistema decisionale automatizzato (parzialmente o completamente) con una marginalità più o meno nota di errori;

• se la misura riguarda persone vulnerabili o meno.

Nei casi in cui gli impatti non possono essere (anche parzialmente) accertati in anticipo, potrebbe essere utile applicare il cosiddetto principio precauzionale. Come esempio di applicabilità di questo principio, si potrebbe suggerire al legislatore, secondo tutte le circostanze rilevanti del caso, di adottare un approccio incrementale, optando per l'uso di uno strumento IT già sperimentato e verificato.

5. Procedere alla valutazione del saldo equo della misura

Quando il legislatore ha raccolto tutte le informazioni richieste ed eseguito una valutazione circa l'importanza, l'efficacia e l'efficienza della misura e valutato tutte le sue possibili interferenze con la privacy e la protezione dei dati personali, arriva il momento di bilanciare (*rectius* equilibrare) ulteriormente l'emanando provvedimento con le ragioni della sua emanazione.

In pratica, il principio di proporzionalità richiede di stabilire un equilibrio tra la portata e la natura dell'interferenza e le ragioni dell'interferenza (i bisogni), tradotte in obiettivi effettivamente perseguiti dalla misura. La CGUE ha sottolineato che «sono in discussione numerosi diritti e libertà fondamentali protetti dall'ordinamento dell'Unione europea, la valutazione della possibile natura sproporzionata di una disposizione del diritto dell'Unione europea deve essere effettuata al fine di conciliare i requisiti della protezione di questi diversi diritti e libertà e un giusto equilibrio tra loro».

In altre parole, il principio funge da strumento per bilanciare gli interessi in conflitto secondo uno standard razionale nei casi in cui la precedenza non è data a priori a nessuno di essi. Occorre rispondere ad almeno altre due domande. In primo luogo, occorre verificare se esiste una situazione di asimmetria delle informazioni: sono state raccolte tutte le informazioni pertinenti e sono state eseguite valutazioni sia sui benefici che sui costi della misura?

Poi, è necessario confrontare i vincoli imposti alla privacy e alla protezione dei dati con i benefici (esercizio di bilanciamento): le misure previste per soddisfare l'obiettivo rispondono in modo proporzionato all'esigenza posta alla base della proposta legislativa, in considerazione di tutte le limitazioni che questa comporta alla protezione dei dati e al diritto alla privacy?

Infine, è necessario conservare (registrare ed archiviare) tutta la documentazione pertinente ottenuta o prodotta durante l'esercizio della valutazione di bilanciamento. Tale documentazione dovrebbe essere pertinente e sufficiente a fornire l'adeguata giustificazione per la misura in esame, che è poi l'obiettivo finale della valutazione posta in essere.

Conclusioni

Appare proficuo a questo punto concludere con due esempi pratici tratti dalle Linee guida analizzate.

ESEMPIO 1: Tele2 Sverige AB (CGUE, C-203/15 e C-698/15, ECLI: EU: C: 2016: 970) [22]

Il risultato della valutazione della proporzionalità (definita «necessità rigorosa») in Tele2 è negativo. La Corte sottolinea i fattori che hanno determinato la sua valutazione negativa: in particolare, tali fattori riguardano la mancanza di relazione tra i dati che devono essere conservati e la minaccia per la pubblica sicurezza, in contrasto con l'obiettivo della misura (v. punto 106 della sentenza). Al contrario, la Corte ha anche espressamente stabilito le caratteristiche della misura proporzionata. In particolare, la misura «deve, in primo luogo, stabilire regole chiare e precise che disciplinino la portata e l'applicazione di tali misure di conservazione dei dati e l'imposizione di garanzie minime, in modo che le persone i cui dati sono stati conservati abbiano garanzie sufficienti per un'efficace protezione dei loro dati personali contro il rischio di un loro uso improprio. Tale normativa deve, in particolare, indicare in quali circostanze e in quali condizioni una misura di conservazione dei dati può essere adottata come misura preventiva, garantendo in tal modo che tale misura sia limitata a quanto strettamente necessario. In secondo luogo, [...] la conservazione dei dati deve [...] soddisfare criteri oggettivi, che stabiliscano una connessione tra i dati da conservare e l'obiettivo perseguito. In particolare, si deve dimostrare che tali condizioni sono tali da circoscrivere, in pratica, l'estensione di tale misura e, quindi, il pubblico interessato dalla stessa».

[22] Cfr. EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., 33-34.

ESEMPIO 7: Linee guida per la videosorveglianza del GEPD [23]

«Lo stesso approccio, consistente nel trovare l'ottimizzazione dell'interferenza sul diritto alla privacy e alla protezione dei dati personali con l'obiettivo perseguito dalla misura (ad esempio, la sicurezza dei locali), è applicato nelle Linee guida del GEPD sulla video-sorveglianza: utilizzando un approccio pragmatico basato sui principi gemelli di selettività e proporzionalità, i sistemi di videosorveglianza possono soddisfare le esigenze di sicurezza rispettando al contempo la nostra privacy. Le telecamere possono e devono essere utilizzate in modo intelligente e devono solo indirizzare i problemi di sicurezza specificamente identificati, riducendo così al minimo la raccolta di filmati non pertinenti. Ciò non solo riduce al minimo le intrusioni nella privacy, ma aiuta anche a garantire un uso più mirato e, in definitiva, più efficiente, della videosorveglianza».

In tale ottica, appare altamente esemplificativa di tutto il complesso processo retrostante l'affermazione dell'EBDP secondo cui «la videosorveglianza non è di default una necessità quando esistono altri mezzi per raggiungere lo scopo sottostante. Altrimenti rischiamo un cambiamento nelle norme culturali che porta all'accettazione della mancanza di privacy come principio generale» [24].

In sintesi entrambi gli esempi ci ricordano come «le scelte progettuali in ambito tecnologico non dovrebbero imporre le nostre interazioni sociali e la struttura delle nostre comunità, ma piuttosto sostenere i nostri valori e diritti fondamentali» [25].

[23] Cfr. EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., 31.

[24] Cfr. EDPB, *Guidelines 3/2019 on processing of personal data through video devices*, Adopted on 10 July 2019, 5.

[25] Cfr. EDPS, *Verso una nuova etica digitale Dati, dignità e tecnologia*, 11/9/2015, 12.

LO *SMART WORKING*, DA PRATICA SPERIMENTALE A *MODUS OPERANDI* ORDINARIO: PROBLEMATICHE GIURIDICHE E APPLICATIVE

THE SMART WORKING, FROM EXPERIMENTAL PRACTICE TO ORDINARY MODUS OPERANDI: LEGAL AND APPLCATION PROBLEMS

Luigi Izzo

Praticante Avv. del Foro di Napoli e Cultore della materia in Diritto delle Nuove Tecnologie – Università degli Studi di Napoli Suor Orsola Benincasa

Abstract:

Da secoli la modalità ordinaria di impiego prevede la presenza fissa del lavoratore sul luogo allo stesso assegnato, a prescindere dall'ambito lavorativo di riferimento. Eppure, dopo i primi impulsi dovuti all'esigenza di tutelare particolari categorie "deboli" di lavoratori, l'attuale emergenza dovuta alla pandemia da COVID-19 ha imposto un ripensamento del paradigma lavorativo mediante un utilizzo sempre più esteso delle modalità di "lavoro agile", sia nelle imprese che negli uffici amministrativi. Ciò, tuttavia, impone di prendere in considerazione una serie di problematiche che spaziano dalla privacy alla tutela del lavoratore di per sé.

For centuries, the ordinary method of employment has required the permanent presence of the worker in the assigned workplace, regardless of the specific working environment. Nonetheless, after the first impulses due to the need to protect particular "weak" categories of workers, the current emergency due to COVID-19 pandemic has imposed a rethinking of the working paradigm through an ever-expanding use of the "smart working", both in the business and in the administrative sectors. However, it requires to consider several concerns, ranging from privacy issues to the protection of the worker himself.

Parole-chiave: Lavoro agile; COVID-19; TIC; Protezione dei dati personali.

Key-words: *Smart Working; COVID-19; ICT; Data Protection.*

Introduzione

Il c.d. "lavoro agile" (così è stata tradotta nella nostra lingua l'espressione anglosassone "*smart working"*) è una nuova realtà lavorativa, già molto diffusa prima dell'attuale crisi globale ma che solo in tempi molto recenti ha ottenuto un vero e proprio riconoscimento giuridico da parte del legislatore mediante l'approvazione della l. 22 maggio 2017, n. 81, la quale è il prodotto di un *iter i*niziato nel 2014 con la presentazione del disegno di legge Mosca. Riconoscimento che, in molti ambiti, aveva avuto il sapore di una mera sperimentazione, oggi culminata nell'adozione forzata di questo approccio versatile verso il lavoro.

All'interno della legge sopra menzionata, specificamente all'art. 18, co. 1 [1], si rinviene una compiuta descrizione di tale nuova modalità lavorativa, che dovrebbe migliorare la competitività delle imprese, pensata per una miglior conciliazione degli impegni lavorativi con le esigenze di vita sociale del singolo [2] e per la quale si prevede:

– che vi sia accordo tra le parti;

– che non vi siano precisi vincoli di orario e di luogo, così sussistendo la possibilità di lavorare alternativamente da locali aziendali ovvero private e suddividendo il carico lavorativo tra tot ore in sede e tot ore fuori sede;

– che possono essere *eventualmente* utilizzati strumenti tecnologici (PC, tablet, laptop, ecc.);

– che si rispetti il limite di durata massima, sia giornaliero che settimanale, così come definito dalla legge e dalla contrattazione collettiva.

Di sicuro si è in presenza di un *modus operandi* nettamente differente rispetto a quello consolidato e proprio per questo si temeva l'impatto dirompente e innovativo di tale novella legislativa, soprattutto ove si consideri che tramite questa si espande l'area dell'autonomia privata relativamente ai profili del luogo e soprattutto dell'orario di lavoro [3], così ponendo il lavoratore fuori dai confini

---

[1] Art. 18, co. 1, l. 81/2017 – "*Le disposizioni del presente capo, allo scopo di incrementare la competitività e agevolare la conciliazione dei tempi di vita e di lavoro, promuovono il lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva*."

[2] WASCHKE, *Smart working, conciliare le esigenze di lavoratori e azienda*, in *Il Sole 24 Ore*, 3 luglio 2018, disponibile su *https://www.diritto24.ilsole24ore.com.*

[3] SPINELLI, *Tempi di lavoro e di non lavoro: quali tutele per il lavoratore agile?*, in *Giustizia Civile.com*, 31 agosto 2018.

dei poteri datoriali con riguardo a questi aspetti [4] e a quelli ad essi correlati [5], come la distribuzione del carico di lavoro e la definizione di un vero e proprio diritto alla disconnessione [6].

Inoltre, a differenza delle normali modalità di impiego subordinato (perché il lavoro agile è, nonostante le apparenze, soggetto alla forma lavorativa della subordinazione) si fornisce meno rilevanza alla quantità di ore e al luogo fisico in cui queste sono consumate, attribuendo maggior importanza, piuttosto, ai risultati conseguiti [7] dallo *smart worker*.

Sussistono, pertanto, delle vere e proprie differenze tra lo "*smart working"* e il similare (ma, appunto, non coincidente) "telelavoro" che, per essere comprese, richiedono uno sguardo alla nozione di quest'ultimo [8] dalla quale si desume la regolarità del lavoro "fuori sede" e dell'utilizzo delle tecnologie informatiche, elementi già di per sé sufficienti a tracciare un netto solco tra le due fattispecie, reso ancor più ampio dalla presenza di una maggior autonomia individuale nell'ambito del "lavoro agile" [9].

Ma, ancora, sussiste una ulteriore particolarità dello *smart working* da prendere in considerazione ai fini di una sua maggior distinzione: l'estrema (per gli standard odierni, beninteso) flessibilità che al momento non è dato rinvenire nel "telelavoro" e che in diversi accordi precedenti all'emergenza pareva essere oltretutto assente data la presenza di numerose imposizioni da parte dei datori di lavoro [10], probabilmente proprio nel tentativo di recuperare parte di quei poteri datoriali persi con questa innovazione.

---

[4] CALDERARA, *Il "lavoro agile" nella l. n. 81 del 2017: prospettive d'indagine*, in *Giustizia Civile.com*, 20 giugno 2018, 5-6.

[5] *Ivi*, 9-10.

[6] Diritto, tra l'altro, previsto espressamente dall'art. 19, co. 1 l. 81/2017, il quale, però, rimanda all'accordo tra le parti relativamente all'aspetto della sua disciplina. Ossia, trattasi di fatto di un diritto quasi "vuoto" che va riempito con quanto deciso dal datore di lavoro e dal suo subordinato.

[7] FALASCA, *Con lo smart working accordi modellati dalle parti firmatarie*, in *Il Sole 24 Ore*, 8 novembre 2017, disponibile su *https://www.diritto24.ilsole24ore.com.*

[8] Nozione chiaramente definita all'interno dell'art. 1, co. 1 dell'Accordo Quadro sul Telelavoro del 9 giugno 2004, il quale così statuisce: "*Il telelavoro costituisce una forma di organizzazione e/o di svolgimento del lavoro che si avvale delle tecnologie dell'informazione nell'ambito di un contratto o di un rapporto di lavoro, in cui l'attività lavorativa, che potrebbe anche essere svolta nei locali dell'impresa, viene regolarmente svolta al di fuori dei locali della stessa.*".

[9] SANTORO PASSARELLI, *Lavoro etero-organizzato, coordinato, agile e telelavoro: un puzzle non facile da comporre nell'impresa in via di trasformazione*, in *WP C.S.D.L.E. "Massimo D'Antona".IT,* 2017, n. 327, 16.

[10] BOTTINI e MOROSINI, *Smart working, accordi non sempre validi. A partire dall'orario di lavoro*, in *Il Sole 24 Ore*, 25 settembre 2017, disponibile su *https://www.diritto24.ilsole24ore.com.*

Tuttavia, va detto che, seguendo il DUNI [11], il "telelavoro", per quanto differente dal "lavoro agile", presenta, come caratteristica comune, la possibilità di far eseguire le mansioni lavorative a distanza rispetto al luogo di lavoro. Pertanto, lo si potrebbe definire quasi un antenato dell'attuale *smart working,* il cui fondamento normativo era dato dall'art. 4 della legge n. 191/1998 [12], che ha avuto completa attuazione con il D.P.R. n. 70 del 1999.

1. La diffusione dello *smart working*

Le caratteristiche di siffatta modalità lavorativa son tali da rendere il lavoro agile un vero e proprio *game changer,* tuttavia non adeguatamente apprezzato da molte (troppe) Piccole e Medie Imprese come pure da larga parte della stessa Pubblica Amministrazione nonostante l'approvazione di una normativa specifica. Questo ha frenato la diffusione del lavoro agile e provocato un esteso ritardo, che si è dovuto recuperare in tutta fretta allo scoppio della pandemia.

1.1. Lo scenario pre-pandemia

Al fine di rendere meglio l'idea dell'atteggiamento tenuto da tanti nei confronti dello *smart working p*uò essere fatto un paragone con quanto accadde con lo sviluppo dei *radar* negli anni '30 e '40, strumento tatticamente (e strategicamente) utilissimo che fu palesemente ignorato dai vertici politici e militari del nostro Paese, salvo poi dover correre ai ripari a conflitto già avviato [13].

Ecco, si potrebbe dire che allo stesso modo sia andata con questa ulteriore innovazione, mal recepita (se non perfino ostacolata) immediatamente dopo la

---

[11] DUNI, *Il progetto nazionale di teleamministrazione pubblica, in "L'informatica giuridica e il Ced della Corte di Cassazione"*, atti del Convegno presso l'Univ. di Roma "La Sapienza", 27-29 nov. 1991, Milano 1992.

[12] Art. 4, co.1, l. 191/1998 – "*Allo scopo di razionalizzare l'organizzazione del lavoro e di realizzare economie di gestione attraverso l'impiego flessibile delle risorse umane, le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 3 febbraio 1993, n. 29, possono avvalersi di forme di lavoro a distanza. A tal fine, possono installare, nell'ambito delle proprie disponibilità di bilancio, apparecchiature informatiche e collegamenti telefonici e telematici necessari e possono autorizzare i propri dipendenti ad effettuare, a parità di salario, la prestazione lavorativa in luogo diverso dalla sede di lavoro, previa determinazione delle modalità per la verifica dell'adempimento della prestazione lavorativa*."

[13] PODDIGHE, *Il radar nella seconda guerra mondiale: una guerra tecnologica e una occasione perduta*, disponibile su *aidmen.it*.

sua disciplina e che ora, a emergenza oramai in corso, viene vista sempre più come il rimedio a cui ricorrere il prima possibile per consentire una limitata ripresa economica e il funzionamento del complessivo apparato amministrativo nel rispetto del divieto di assembramento. Si è deciso, quindi, di adottare su base generalizzata questo nuovo approccio.

Tuttavia, immediatamente dopo l'adozione della normativa di base, come si può immaginare, sono state emanate delle linee guida che di fatto né hanno frenato la diffusione, quale, ad esempio, quella di prevedere un obiettivo minimo pari ad appena il 10% dei dipendenti da porre in *smart working p*er quanto concerne la Pubblica Amministrazione, quota indicata da una direttiva dell'allora Ministro Marianna Madia [14] da raggiungere, peraltro, in "soli" 3 anni, attraverso, di fatto, un processo di sperimentazione.

Target che, relativamente alle caratteristiche dell'impiego presso la Pubblica Amministrazione [15], fu giudicato pure irrealistico da alcuni [16] ma, vedendo quanto avvenuto esattamente 3 anni dopo, questa soglia sarebbe da considerare quasi lo *standard* minimo per garantire il funzionamento degli uffici pubblici in tempo di emergenza.

Al tempo stesso, invece di cercare di attivare progetti di *smart working* nei confronti di ogni dipendente, pubblico o privato, che fosse in grado di usufruirne così velocizzandone l'implementazione su scala molto più vasta, si è deciso di imporre solamente dei criteri di precedenza [17] che garantissero una corsia preferenziale a precise categorie di lavoratori. Intento sicuramente lodevole, non c'è dubbio alcuno, ma la misura certamente non favoriva una accelerazione generalizzata nell'adozione di questa modalità lavorativa.

Qual è stato il risultato finale di tale atteggiamento verso il lavoro agile? La risposta è semplice, ad ottobre 2019 (esattamente alla vigilia dell'*outbreak* virale di Wuhan) dai dati dell'Osservatorio Smart Working risultava che sia la P.A. che le P.M.I., queste ultime parimenti refrattarie all'idea di dover ripensare le modalità di impiego dei propri dipendenti, erano estremamente in ritardo rispetto ad altri comparti [18], tant'è vero che i progetti di *smart working* del pubblico impiego avevano un effettivo impatto su appena il 12% della popolazione complessiva dei dipendenti con una scelta orientata dalle motivazioni prettamente

[14] Direttiva n. 3 del 2017, disponibile su *funzionepubblica.gov.it.*

[15] Caratterizzato da un forte "schematismo" (Cass., 11 maggio 2010, n. 11405) che lo distingue nettamente rispetto all'impiego nelle aziende private.

[16] TAMPIERI, *Il lavoro agile nella pubblica amministrazione: opportunità o illusione?*, in *Giustizia Civile.com*, 2018, 9.

[17] Art. 1, co. 486, L. n. 145/2018(cd. Legge di Bilancio 2019).

[18] CASADEI, *Smart working, mancano all'appello Pmi e Pa*, in *Il Sole 24 Ore*, 30 ottobre 2019, disponibile su *https://www.diritto24.ilsole24ore.com.*

famigliari di questi e, invero, una percentuale identica era stata ottenuta per i progetti delle P.M.I., a dimostrazione di quanto sia difficile accettare di dover ripensare il modo di lavorare in alcuni ambienti.

Eppure, è uno strumento, questo, che anche la P.A. avrebbe dovuto accettare senza eccessive remore (se non quella di garantirne una corretta ed effettiva applicazione) al fine di completare quel processo di digitalizzazione della stessa già da tempo avviato, così concretizzando il concetto di Amministrazione Digitale (o anche *e-government)* che prevede il sostanziale "trasferimento" dei procedimenti amministrativi dagli sportelli fisici a quelli telematici. Stesso discorso valga per le P.M.I., che avrebbero potuto capire per tempo come gestire le mansioni di tipo amministrativo "fuori sede" senza ritrovarsi in affanno in seguito.

Quindi, trattasi di uno strumento che, se prima era visto solamente come una soluzione per risparmiare risorse e tempo nei procedimenti amministrativi (sia pubblici che aziendali) e in grado di conciliare le esigenze lavorative con quelle personali dei dipendenti (si pensi, per esempio, alle necessità familiari), oggi assume quasi le vesti di una vera e propria *arma strategica,* necessaria al fine di garantire il funzionamento del Sistema Paese in un momento di emergenza.

Per contro, vi è stato chi è stato sufficientemente lungimirante, come i dirigenti del gruppo Generali, i quali già due anni prima dell'inizio della crisi sono stati in grado di riprogettare completamente tutto e di avviare un'adozione sempre più ampia del lavoro agile, al punto da adottarlo per ben 1.000 dipendenti tra Milano e Roma in poco tempo [19] ed estenderlo poi a numerosi lavoratori di Mogliano Veneto, Torino e Trieste nel 2018 [20]. Infatti, come accertato dall'Osservatorio Smart Working, ben il 58% delle grandi e medie imprese aveva già adottato in modo diffuso questo approccio e superato la fase della sperimentazione, dato che in queste aziende il lavoro agile era già una realtà diffusa e consolidata.

1.2. Le reazioni all'emergenza

Come noto, a fine febbraio di quest'anno si è giunti alla proclamazione dello stato di emergenza su tutto il territorio nazionale in seguito alla diffusione del nuovo coronavirus (denominato SARS-CoV-2), geneticamente simile a quello della SARS del 2003 [21] ma da questi differente e apparentemente più lieve, in

[19] Comunicato stampa del gruppo Generali datato 19 ottobre 2017, disponibile su https://asset.generali.it/267831/10-19_CS_Smart-working-Generali-Italia.pdf.

[20] Comunicato stampa della FISAC CGIL datato 25 giugno 2018, disponibile su https://www.fisac-cgil.it/75903/generali-firmato-accordo-su-smart-working.

[21] Sul punto si veda al link https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it.

quanto la SARS dell'epoca era caratterizzata da un tasso di mortalità pari al 9,6% degli infetti e da una minore capacità di trasmissione rispetto all'attuale variante riscontrata in Cina nel dicembre dello scorso anno [22].

Il problema riguarda proprio questa maggior capacità di infezione del ceppo oggigiorno circolante, che ha comportato proprio la necessità di ridurre i contatti sociali, obbligando allo stop generalizzato di molte attività e al massiccio ricorso allo s*mart working* nelle aziende e negli uffici, sia pur con tutti i disagi che comporta un cambio di passo così repentino [23].

Innanzitutto, il rapido ricorso allo stesso (specialmente nelle zone inizialmente colpite dall'epidemia) ha costretto il Governo a operare una prima deroga relativa alla previsione che richiede un accordo scritto tra il datore di lavoro e il dipendente, disponendo con il D.P.C.M. del 23 febbraio 2020 che sia sufficiente una mera autocertificazione che attesti la provenienza del lavoratore da una delle zone all'epoca a rischio, con ciò eleggendolo *de facto* a strumento imprescindibile per la continuazione dell'attività lavorativa e facendo venire meno (almeno temporaneamente) la volontarietà che lo ha contraddistinto.

Questo, in combinazione con un'ulteriore diffusione dei dati relativi all'utilizzo del lavoro agile nelle P.M.I., "accusate", guarda caso, di essere perfino più arretrate dei pubblici uffici [24], ha innescato, poi, una vera e propria corsa all'attivazione di quante più posizioni possibili sotto forma di *smart working* e, come logica conseguenza, ciò ha portato molti a interrogarsi su questioni che hanno immediatamente trovato spazio sui giornali del settore, quali l'applicazione del codice disciplinare [25], gli strumenti di controllo digitale delle prestazioni (e annesse preoccupazioni per la privacy del lavoratore) [26], la flessibilità nella scelta

---

[22] ISS, *Coronavirus, più casi della Sars ma più bassa letalità. Il commento di Gianni Rezza*, su *iss.it*, 3 febbraio 2020.

[23] GABANELLI e QUERZÈ, *Coronavirus, smartworking obbligatorio per tutti ma ad 11 milioni di italiani manca la connessione*, su *corriere.it*, 15 marzo 2020.

[24] ROMANI, *Ora lo Smart Working diventa necessario*, su *Diritto24*, 26 febbraio 2020 e CASADEI e MELIS, *Lo smart working oltre l'emergenza: una sfida per le Pmi*, in *Il Sole 24 Ore*, 2 marzo 2020, disponibile su *https://www.diritto24.ilsole24ore.com.*

[25] Sul punto cfr. MARRAFFINO, *Il codice disciplinare in sede vale anche fuori*, su *Il Sole 24 Ore*, 9 marzo 2020, disponibile su *https://www.diritto24.ilsole24ore.com*, che prende le mosse dalla Sent. n. 6022/2018 del Tribunale di Roma dove è stato riconosciuto il licenziamento per giusta causa nei confronti del "*lavoratore che aveva pubblicato su Facebook la e-mail di invettive inviata al proprio superiore gerarchico, colpevole di «mettere bocca» o «questionare» sulle modalità di lavoro in giornata di smart working. Alla e-mail dai toni accesi seguivano altri post sui social network, tutti a carattere offensivo e svilente nei confronti dell'azienda, che sono stati considerati diffamatori dal giudice.*".

[26] FALASCA, *Lo smart working ammette verifiche su pc e posta digitali*, in *Il Sole 24 Ore*, 9 marzo 2020, disponibile su *https://www.diritto24.ilsole24ore.com.*

degli orari e luoghi della prestazione [27], la sicurezza informatica [28], il ruolo del *Data Protection Officer n*elle aziende [29].

Ai decreti e agli articoli giornalistici, nel marasma informativo di quei giorni, poi, faceva immediatamente seguito il 9 marzo 2020 un avviso dell'INAIL contenente una informativa sulla sicurezza dei lavoratori ai sensi dell'art. 22, co. 1, l. 81/2017 [30], nella quale erano indicati numerosi comportamenti e accorgimenti da adottare per un lavoro agile in sicurezza.

Questo, nell'ambito delle imprese. Per quanto concerne l'adozione massiva di siffatta modalità lavorativa nella Pubblica Amministrazione, invece, si deve partire dalla circolare del 4 marzo 2020 a firma Dadone [31] con cui si è dato un primo forte impulso allo *smart working,* passando dalla sua sperimentazione all'adozione in via ordinaria, in uno scenario dove, secondo il rapporto dell'anno precedente [32], il 43% dei lavoratori ritiene che questa modalità operativa non sia applicabile alla propria realtà e che il procedimento amministrativo cartaceo e la gestione tramite faldoni e fascicoli non consente il lavoro agile. Il 27%, poi, non percepisce i benefici ottenibili e il 21% solleva il problema delle procedure poco digitalizzate (a volte differenti perfino all'interno di una stessa amministrazione) nonché l'assenza di una adeguata tecnologia, per esempio di banda di rete di comunicazione, tutti segnali di una P.A. poco "digitale" [33]. Ciononostante, dopo nemmeno un mese dalla prima circolare attuativa (o meglio, *esortativa)*, Palazzo Vidoni fa uscire i primi risultati di un monitoraggio tendente a verificare l'andamento dei pubblici enti circa l'implementazione dello *smart working,* da cui emerge che addirittura l'83% del personale della P.A. centrale sarebbe impiegato mediante tale modalità.

Si vede, pertanto, come entrambe le anime del Paese, quella pubblica e quella privata, abbiano saputo, in tempi relativamente brevi, digitalizzarsi in maniera estesa al fine di evitare un blocco totale.

---

[27] BOTTINI, *Flessibilità per orari e luoghi: il nodo chiave degli accordi*, in *Il Sole 2 Ore*, 2 marzo 2020, disponibile su *https://www.diritto24.ilsole24ore.com.*

[28] CASTROREALE, PEREGO e PONTI, *Smart working, come garantire sicurezza informatica e privacy*, su *Agendadigitale.eu*, 2 marzo 2020.

[29] PEREGO e PONTI, *Il ruolo del DPO nell'emergenza coronavirus (e non solo): indicazioni operative*, su *cybersecurity360.it*, 13 marzo 2020.

[30] Disponibile sul sito *inail.it* nella sezione comunicativa dedicata ad avvisi e scadenze.

[31] Disponibile su *funzionepubblica.gov.it.*

[32] MANCA, *Lo smart working nella PA: cos'è e com'è (complicato) farlo nella realtà*, su *Agendadigitale.eu*, 5 marzo 2020.

[33] CAPOZZI, *Coronavirus, lo Stato non è digitale e le mille lingue della Pubblica amministrazione frenano lo smart working*, su *ilfattoquotidiano.it*, 14 marzo 2020.

2. Problematiche giuridico-applicative

È evidente come il lavoro agile sia divenuto una vera e propria panacea per le aziende, sia pur ponendo diverse problematiche in ordine alla privacy [34].

Questo aspetto concerne specialmente i lavoratori in quanto il datore di lavoro, ai sensi dell'art. 21, l. 81/2017 deterrebbe un potere di controllo che rischia di porre serie lesioni alla sfera privata dei suoi dipendenti. Non solo, dacché questi potrebbe, attraverso intromissioni e pressioni nel processo decisionale relativo all'orario di lavoro, rendere *de facto* ineffettivo il diritto alla disconnessione e tentare di stabilire una vera e propria disponibilità illimitata del subordinato, così configurando una intrusione indebita nel tempo di non lavoro e, quindi, nella sfera personale del lavoratore, ledendone anche la privacy (di cui il diritto alla disconnessione è, in pratica, una sfaccettatura) [35].

Al tempo stesso, va considerato come sia stato implementato frettolosamente il lavoro agile al fine di minimizzare i danni economici, però facendo affidamento spesso e volentieri sui *device* informatici di personale proprietà degli impiegati in luogo di quelli forniti dalle imprese, al fine di accorciare i tempi (e magari abbassare i costi) ma in tal modo aumentando i rischi di involontari *leak* informativi e di attacchi ai sistemi e così ponendo a rischio il patrimonio informativo aziendale.

2.1. La privacy dei lavoratori

Nell'analisi del rischio derivante da un uso errato dei poteri datoriali di controllo è bene considerare che detti poteri sono strettamente correlati alla necessità di far rispettare un codice disciplinare e di applicare le relative sanzioni.

Di conseguenza, si pone una prima domanda a cui rispondere, ossia se si configuri, per lo *smart worker, u*n differente codice disciplinare (e relative sanzioni) da rispettare rispetto a un normale dipendente in azienda, problematica cui non si può non fornire una risposta negativa, soprattutto qualora le violazioni del lavoratore agile siano connesse ai doveri fondamentali collegati al rapporto di lavoro [36]; soprattutto violazioni dei doveri fondamentali, certamente, ma al

---

[34] LANFRANCHI, *Smart working a prova Gdpr, come arginare i rischi privacy*, su *agendadigitale.eu*, 13 marzo 2020.

[35] SPINELLI, *op. cit.*, 7, 2018.

[36] Trib. Roma, Sent. n. 6022/2018, dove è stato affrontato il caso di un lavoratore in *smart working*, licenziato disciplinarmente poiché, nel corso di uno scambio di e-mail nonché attraverso l'utilizzo di post pubblicati su Facebook, aveva rivolto ai superiori gerarchici ed ai colleghi offese immotivatamente gravi, così configurando un uso scorretto di internet e dei *social network*.

tempo stesso non solo quel genere di violazioni sono passibili di essergli contestate. Infatti, è lecito ritenere che, al fine di non creare disparità tra lo *smart worker* e i dipendenti in azienda, si applichino le stesse sanzioni e le medesime previsioni disciplinari generalmente indicate nei vari contratti collettivi [37]. Ragion per cui i poteri di controllo sul lavoratore agile, sia pur con le peculiarità dovute al caso specifico, tenderanno ad essere esercitati con la stessa "intensità" che si avrebbe nei confronti di quanti espletano le proprie mansioni dai locali aziendali. Questo, però, rischia di invadere la sfera individuale del lavoratore in maniera assai più rilevante, considerato il diverso contesto ambientale dove si lavora e la differente (certamente più flessibile e discontinua) modalità di gestione dell'orario di lavoro [38].

Proprio in considerazione di questi aspetti, allo stato attuale e prescindendo dalla sottoscrizione di un accordo scritto cui si è rinunciato almeno per la durata di questa emergenza [39], va notato come sia ugualmente necessario, per l'azienda, disciplinare [40]:

– il rispetto degli orari di lavoro, configurando anche il diritto – dovere dei dipendenti alla disconnessione;
– l'utilizzo degli strumenti elettronici, siano essi aziendali o personali;
– l'esercizio del potere direttivo e di quello di controllo, anche da remoto;
– ipotesi specifiche di infrazioni disciplinari che possano essere commesse dal lavoratore agile.

Infatti, anche se viene meno la necessità di un accordo individuale, lo stesso vanno seguiti, come richiesto dalla normativa emergenziale, i principi sottesi allo *smart working* presenti negli articoli dal n. 18 al n. 23 che impongono la regolamentazione dei profili di cui sopra affinché non si registrino abusi da parte dei datori di lavoro, disciplina cui si potrebbe provvedere quantomeno mediante

---

[37] MARRAFFINO, *Il codice disciplinare in sede vale anche fuori*, in *Il Sole 24 Ore*, 9 marzo 2020, disponibile su *https://www.diritto24.ilsole24ore.com.*

[38] CAFIERO e PEZZALI, *Lo smart working da "Covid19" non è smart working*, in *Diritto24*, 7 aprile 2020, disponibile su *https://www.diritto24.ilsole24ore.com.*

[39] Vedasi l'art. 2, co. 1, lett. r) del D.P.C.M. 8 marzo 2020, che così dispone: "*la modalità di lavoro agile disciplinata dagli articoli da 18 a 23 della legge 22 maggio 2017, n. 81, può essere applicata, per la durata dello stato di emergenza di cui alla deliberazione del Consiglio dei ministri 31 gennaio 2020, dai datori di lavoro a ogni rapporto di lavoro subordinato, nel rispetto dei principi dettati dalle menzionate disposizioni, anche in assenza degli accordi individuali ivi previsti; gli obblighi di informativa di cui all'art. 22 della legge 22 maggio 2017, n. 81, sono assolti in via telematica anche ricorrendo alla documentazione resa disponibile sul sito dell'Istituto nazionale assicurazione infortuni sul lavoro;*".

[40] FURLAN, *Smart working e problematiche applicative nel periodo di emergenza COVID-19*, in *Diritto24*, 3 aprile 2020, disponibile su *https://www.diritto24.ilsole24ore.com.*

una informativa diretta ai lavoratori [41], dal momento che allo stato attuale ben poco supporto può essere fornito dai sindacati.

Ma, in concreto, come si può attuare il potere di controllo? Di sicuro vanno rispettati i limiti fissati dagli articoli 2, 3 e 4 dello Statuto dei lavoratori. L'ultimo di questi articoli, in particolare, ha una certa rilevanza quando si parla di lavoro agile, perché fissa un divieto di installazione e uso di apparecchiature tecnologiche e sistemi che rendano il datore di lavoro in grado di controllare a distanza lo svolgimento dell'attività lavorativa del dipendente, a meno che il ricorso a questi apparecchi non venga preventivamente concordato con un accordo sindacale o ottenga l'autorizzazione dell'Ispettorato territoriale del lavoro e a condizione che vengano impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale [42].

La norma, nata nel 1970, grazie a una interpretazione evolutiva da parte della giurisprudenza e del Garante della Privacy è giunta a comprendere anche gli strumenti di controllo digitalizzato della prestazione lavorativa, che spaziano dai sistemi di rilevazione della posizione sino a quei software che monitorano in maniera costante l'uso che viene fatto di Internet [43].

Pertanto, diviene impossibile verificare per mezzo delle tecnologie digitali cosa stia facendo il dipendente in un dato momento della giornata, atteggiamento che sarebbe pure contrario alla logica del lavoro agile. Però, si deve notare che lo Statuto ha subito una parziale deroga da parte del Jobs Act del 2015 [44], il quale dispone che queste restrizioni non si applichino agli "strumenti di lavoro" e che i dati e le informazioni ottenuti tramite gli strumenti di controllo a distanza siano utilizzabili "ai fini del rapporto di lavoro" solo a condizione che sia stata data al lavoratore abbia ricevuto una adeguata informativa in merito.

Di conseguenza, rispetto alla situazione ante-Jobs Act non sussiste più un divieto totale di controllo, anzi! Per esempio, qualora vi siano sospetti fondati che lo *smart worker* commettendo degli illeciti disciplinari ovvero sussistano esigenze organizzative e di gestione e protezione dei dati [45], possono benissimo essere svolti controlli mirati, anche a distanza, a patto che rispettino il principio di proporzionalità, non siano invasivi e che riguardino beni dell'azienda [46] (il PC

---

[41] MACCHIONE, *Il lavoro agile ai tempi del Coronavirus*, in *Giustizia Civile.com*, 14 aprile 2020.

[42] BENATTI e COLOMBA, *Tutela della privacy alla prova dello smart working: linee guida*, su *cybersecurity360.it*, 25 marzo 2020.

[43] FALASCA, *op. cit.*

[44] Art. 23, D.lgs. n. 151/2015.

[45] BAGNATO, *Coronavirus e smart working: cosa si può fare e cosa non si può fare?*, su *altalex.com*, 24 marzo 2020.

[46] Infatti, la giurisprudenza della Suprema Corte (Cass., Sent. n. 22313/2016) afferma la ne-

fornito dal datore, la casella di posta aziendale), rispetto ai quali va anticipatamente chiarito a tutti i dipendenti, mediante apposita informativa [47], che gli strumenti aziendali non possono essere usati per motivi non attinenti alle proprie mansioni proprio perché potrebbero essere oggetto di indagini aziendali. Al tempo stesso, dovendo generalmente usare programmi e piattaforme (anche su PC personali dei dipendenti) che possono eventualmente soddisfare la necessità di controllo da parte del datore, quest'ultimo deve garantire che siano stati osservati i principi di *privacy by design* e *privacy by default* [48] nella progettazione del *software.*

2.2. La tutela del patrimonio informativo dell'azienda

Con riferimento ai rischi che corre l'azienda stessa, va evidenziato come lo *smart worker i*mprovvisato possa costituire una vera e propria falla nella struttura digitale di una azienda [49]. Infatti, nella stragrande maggioranza dei casi, per i lavoratori sono stati predisposti sistemi di collegamento a distanza improvvisati, spesso con l'uso di *device* non aziendali bensì di proprietà dei dipendenti o addirittura dei loro familiari. Pertanto, sarebbero strumenti digitali potenzialmente inappropriati ai fini dello svolgimento delle mansioni lavorative in quanto spesso e volentieri risultano privi di sistemi operativi aggiornati e misure di sicurezza adeguate, caratteristiche che connotano, invece, la gestione e l'utilizzo dei dispositivi di proprietà aziendale. A ciò si aggiunga pure che a buona parte del personale è stato dato accesso ai sistemi e programmi aziendali senza fornire una informativa che abbia istruzioni specifiche relativamente all'utilizzo degli

---

cessità di «*rispettare la libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali dettata dal D.lgs. n. 196 del 2003, i principi di correttezza, di pertinenza e non eccedenza di cui all'art. 11, comma 1, del Codice; ciò, tenuto conto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o di dati di carattere sensibile (cfr. sul punto Cass. civ., 5 aprile 2012, n. 5525 e n. 18443 del 1° agosto 2013)*» nell'effettuare i controlli sul lavoratore. Allo stesso modo il Garante Privacy con provvedimento 1° febbraio 2018 n. 53, disponibile su https://www.garanteprivacy.it/pdf?p_p_id=PdfUtil&p_p_lifecycle=2&p_p_state=normal&p_p_mode=view&p_p_resource_id=%2Foffering%2FprintPDF&p_p_cacheability=cacheLevelPage&_PdfUtil_articleId=8159221, ha ritenuto illecito ai sensi della normativa in materia di privacy il trattamento dei dati effettuato dal datore su un account di posta elettronica aziendale proprio perché era eccessivamente sproporzionato.

[47] Il Garante Privacy, sempre nel provvedimento del 1° febbraio 2018 n. 53, ritenne illegittimo un controllo che, oltre ad essere sproporzionato era anche effettuato senza previa informativa per i dipendenti.

[48] BENATTI e COLOMBA, *op. cit.*

[49] MAIOLETTI, *Smart working: di necessità virtù – le regole a tutela della privacy*, su *Diritto24*, 7 aprile 2020.

stessi e alle misure di sicurezza da adottare e rispettare [50].

Queste problematiche, poi, vengono ulteriormente amplificate dal fatto che le connessioni di cui usufruiscono i dipendenti non sono affatto quelle di tipo chiuso, quali le reti *intranet* aziendali che son collegate al *web* e al tempo stesso protette per mezzo di *firewall* e di sistemi di criptazione dei dati, bensì le più comuni reti domestiche, che sono potenzialmente in grado di far avere numerose informazioni a terzi estranei proprio per il minor impegno necessario al fine di "bucarne" i protocolli di sicurezza.

È evidente come sia preferibile che i dispositivi di lavoro vengano forniti dal datore di lavoro, così che abbiano sistemi operativi aggiornati e adeguate misure di sicurezza, quali antivirus e *firewall.* Però, qualora non sia attuabile un programma di forniture aziendali (come ora, in piena emergenza) o si preferisca consentire l'accesso attraverso strumenti di proprietà dello *smart worker,* sarà necessario implementare adeguate *policy* BYOD ("*Bring Your Own Device"*, l'approccio attualmente più diffuso) [51] attraverso le quali verificare quali siano i livelli di sicurezza che detti dispositivi dei dipendenti dovranno avere e stabilir-

---

[50] Infatti, tra le attività *prodromiche* all'attivazione di un rapporto di *smart working*, che in condizioni "normali" sarebbero rispettate, rientrano le seguenti: "*Predisposizione di una policy aziendale recante una serie di elementi essenziali che rispondono agli obblighi di informativa facenti capo al datore di lavoro. Il datore deve indicare specifiche linee guida di comportamento – oltre ai basilari doveri di diligenza – per garantire una corretta esecuzione della prestazione lavorativa nel pieno rispetto delle misure di sicurezza e alla luce della necessaria cooperazione dello Smart worker. In particolare, deve suggerire accorgimenti e regole in tema di utilizzo e ricovero degli strumenti di lavoro; di gestione della password; di operatività dell'Antivirus; di conservazione di file e documenti; di protezione dei dispositivi portatili; di utilizzo di Internet e della posta elettronica. Deve, inoltre, indicare in via preventiva le conseguenze disciplinari in caso di violazione delle regole di comportamento e fornire informazioni circa eventuali attività di monitoraggio – che devono attenersi ai principi di necessità, correttezza, pertinenza e non eccedenza – (indicando modalità, finalità e soggetti autorizzati a procedervi) e la conservazione dei relativi dati. Valutazione preventiva – e obbligatoria – di impatto sulla protezione dei dati (ex art. 35 GDPR), ossia predisposizione di una procedura – soggetta a continua revisione – volta a descrivere un singolo trattamento di dati ovvero più trattamenti analoghi in termini di natura, ambito, contesto, finalità e rischi, al fine di valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di adottare tutte le misure di sicurezza idonee ad affrontarli. Predisposizione di una specifica procedura in caso di data breach (ex artt. 33, 34 GDPR) di cui devono essere adeguatamente informati i lavoratori, dovendo gli stessi dare tempestiva informazione al datore di lavoro nel caso in cui si verifichi – nell'ambito della loro attività – una violazione dei dati personali oggetto di trattamento che ponga a rischio i diritti e le libertà delle persone fisiche; predisposizione di un'adeguata informativa privacy – aderente ai dettami degli artt. 12 e 13 GDPR – da fornire al lavoratore circa il trattamento dei suoi dati personali raccolti mediante gli strumenti utilizzati e i software dai quali può derivare la possibilità di controllo da parte del datore di lavoro.*" (BENATTI e COLOMBA, *op. cit.,* 2020).

[51] FRATINI e LECCHI, *Smart working e tutela del know how*, su *Diritto24*, 4 maggio 2020.

ne le relative modalità di utilizzo, le quali prevedano l'utilizzo di precise credenziali di autenticazione atte a consentire all'utente l'accesso solo ai dati allo stesso riservati e magari stabilendo l'installazione di *software* di segregazione dei dati e delle informazioni, in modo da evitare una commistione tra i dati aziendali e quelli privati [52].

Da un punto di vista tecnico, al fine di limitare i rischi derivanti da un approccio BYOD, le principali soluzioni alle quali il datore di lavoro può far ricorso, senza trascurare la continua formazione digitale dello *smart worker,* sono: le reti VPN (Virtual Private Network), i *software* che sfruttano il Cloud (Cloud Computing, ovverosia Nuvola Informatica) e l'ACL (Access Control List), mirata a limitare il rischio di accesso non autorizzato con conseguente diffusione e/o perdita e distruzione dei dati aziendali. Al tempo stesso dovrebbe essere stilato un vero e proprio codice di condotta digitale da seguire nell'utilizzo di dispositivi per il collegamento da remoto, nel quale inserire regole come:

– non lasciare incustodito o in un qualsiasi modo accessibile il dispositivo;
– non allontanarsi dalla postazione di lavoro senza aver prima posto in sospensione, sbloccabile solo con password, il dispositivo;
– curare gli aggiornamenti per tutti gli antivirus e i software installati;
– limitare il salvataggio in locale dei dati a casi eccezionali e limitatissimi, avendo cura, venuta meno la necessità, di eliminare tali dati dalla memoria interna;
– regolamentare, qualora sia consentito, l'utilizzo di dispositivi esterni di archiviazione dati quali *pen drive* e *hard disk e*sterni;
– emanare una apposita informativa per rendere edotti i lavoratori dei rischi derivanti da attività di hackeraggio o *phishing* di cui potrebbero essere vittime e sui comportamenti da adottare per neutralizzare tali violazioni;
– rammentare le regole fornite per la gestione di possibili *leak* di dati personali e aziendali (c.d. *data breach)*.

2.3. Una possibile maggior diffusione del DPO

Considerato un tale scenario di partenza è istintivo immaginare che, insieme allo *smart working,* raggiunga una ulteriore importanza anche la figura del *Data Protection Officer* (DPO), il quale dovrebbe essere maggiormente diffuso e coinvolto nella creazione delle *policy a*ziendali nel suo ambito operativo, anche al fine di evitare eventuali sanzioni per una gestione totalmente *fai-da-te* dei dati

[52] MAIOLETTI, *op. cit.*

sensibili, siano essi personali ovvero aziendali [53].

Ad esempio, prendendo come base la necessità di gestire e strutturare nel migliore dei modi il lavoro agile, pare assai opportuno che un DPO si coordini con l'area IT dell'azienda per un monitoraggio complessivo e per organizzare il presidio informatico e la gestione dell'accesso contemporaneo di più lavoratori operanti da remoto.

Al tempo stesso, tale soggetto dovrebbe monitorare anche la sicurezza informatica aziendale al fine di prevenire eventi di *data breach e*, al riguardo, le caselle di posta elettronica aziendali potrebbero vedere il costante presidio del DPO ovvero di qualche altro soggetto autorizzato all'interno dell'Organizzazione, che potrebbe attraverso le stesse segnalare un simile evento e spingere i dipendenti a porre in atto le procedure previste per tali ipotesi.

Inoltre, il DPO dovrebbe gestire le procedure di *backup* dei dati nonché operare una valutazione in merito alla resilienza degli uffici dell'area IT, i quali dovrebbero avere una certa "ridondanza" non tanto in termini di strumenti digitali quanto, piuttosto, in termini di dipendenti disponibili, così da avere tale organo sempre funzionante anche nel malaugurato caso che uno degli addetti non sia in grado di espletare le proprie mansioni per motivi di salute (si immagini, per esempio, che venga infettato proprio dal nuovo coronavirus) [54].

Al tempo stesso, una siffatta figura sarà indispensabile non solo per proteggersi (o rimediare) da determinati rischi per la durata dell'emergenza, bensì anche per il futuro assestamento delle aziende dacché il lavoro agile diventerà quasi sicuramente la norma per numerosi lavoratori (si pensi che in appena due mesi si è raggiunto il milione di *smart worker* in Italia e che il report dell'Osservatorio ne registrava poco meno di 600.000 a fine 2019), obbligando a rivedere e rimodulare la gestione di tale modalità di lavoro, così da renderla più sicura e affidabile.

Conclusioni

Sembra che questo virus abbia offerto al nostro Paese una irripetibile opportunità per poter ripensare il complesso dei modelli socioeconomici e produttivi, che tanto hanno sofferto proprio perché non erano adeguatamente preparati ad assorbire un tale *shock.* Si potrebbe quasi dire che vada ormai adottata a livello generalizzato quella capacità tipica dei militari di essere flessibili e *leader* al

[53] COLOMBO, *Strumenti per prevenzione diffusione Covid19: sanzioni in caso di privacy fai da te*, in *laborproject.it*, 27 aprile 2020.

[54] PEREGO e PONTI, *op. cit.*

tempo stesso, così da poter gestire in modo migliore, più avanti, non solo le problematiche quotidiane ma anche e soprattutto quelle più critiche, risolvendo le vulnerabilità dell'azienda, prendendo le opportunità per tempo (quale, appunto, quella di introdurre il lavoro agile) ed evitando che ci si trovi in difficoltà in futuro [55].

Al tempo stesso, però, l'utilizzo esteso dello *smart working h*a dimostrato anche come sia doveroso sviluppare a livello generalizzato una vera e propria cultura della che tenda alla tutela della *privacy* dei singoli *e* alla protezione dei dati sensibili in senso generale, obiettivo conseguibile non solo mediante l'operato del legislatore ma anche e necessariamente attraverso uno sforzo congiunto che veda nuovamente protagonisti le imprese, i sindacati e i lavoratori, così da sviluppare una normativa regolamentare realmente applicabile e applicata da tutti gli attori del lavoro agile.

Solo attraverso questo grande sforzo sarà possibile sfruttare appieno gli aspetti positivi di siffatta modalità lavorativa minimizzandone, al contempo, i rischi che questa necessariamente comporta.

[55] Non è un caso che Amazon, per la logistica, punti fortemente su militari, sia in servizio che congedati (LUNA, *Soldato Amazon*, in *rep.repubblica.it*, 13 febbraio 2020).

HAVE COLLABORATED TO THIS ISSUE OF THE *EJPLT*

ADRIÁN PALMA ORTIGOSA – Assistant Researcher at Universidad de Sevilla

ALDO IANNOTTI DELLA VALLE – Ph.D. – candidate in 'Humanities and Technologies' at Università degli Studi Suor Orsola Benincasa di Napoli

ANNA IRENE CESARANO – Ph.D. – candidate at Università degli Studi Suor Orsola Benincasa di Napoli

DANILO TOZZI – Legal Caunsel and DPO at Studio Legale de Lima Souza

DOMENICO FAUCEGLIA – Ph.D. at Università di Roma Tor Vergata, Lawyer

FEDERCO SERGIO – Teaching Assistant in Tax Law at Università degli Studi Suor Orsola Benincasa di Napoli

LIVIA AULINO – Ph.D. candidate at Università degli Studi Suor Orsola Benincasa di Napoli, Member of the Editorial Team of EJPLT

LUIGI IZZO – Treinee Lawyer and Teaching Assistant in New Technology Law at Università degli Studi Suor Orsola Benincasa di Napoli

MAI-BRIT CAMPOS NIELSEN – LL.M. at the University of Edinburgh

MARCO BERGAMO – Lawyer in Naples

MARÍA BOCIO JARAMILLO – Assistant Researcher at Seville University

MARIA CRISTINA GAETA – Postdoctoral Research Fellow in Privacy Law at Università degli Studi Suor Orsola Benincasa di Napoli, Coordinator of the Editorial Team of EJPLT

MARIO TRIGGIANI – Teaching assistant in Private Law at Università degli Studi Suor Orsola Benincasa di Napoli

RAFFAELE SERPE – Lawyer in Naples

RICCARDO BERTI – Lawyer at Zumerle Law Firm

SERGIO GUIDA – Independent Researcher, Data Governance & Privacy Sr Mgr

SIMONA LATTE – Legal Counsel e Web Marketing Manager

VALERIA MANZO – Lawyer in Naples and Ph.D. (c) at Università della Campania Luigi Vanvitelli, Member of the Editorial Team of EJPLT