PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Manuale per Giornalisti

Autori: Iñigo de Miguel Beriain, Lorena Pérez Campillo (UPV/EHU)

Editore: Federico Caruso (OBC Transeuropa)

Tabella dei contenuti

1. Introduzione

Il mondo del giornalismo è un microcosmo molto particolare in termini di protezione dei dati. Anche se comporta la raccolta e la conservazione di enormi quantità di informazioni personali sotto forma di interviste, registri aziendali, fotografie e filmati, e la loro diffusione, il suo quadro normativo non è mai stato così chiaro. Così, non sorprende che quando si tratta di attività mediatica ci siano serie preoccupazioni legate alla protezione dei dati (Erdos, 2015, p.8). Infatti, la pubblicazione di informazioni relative a una persona identificata o identificabile potrebbe costituire un grave attentato alla sua privacy.

D'altra parte, è innegabile che il lavoro del giornalismo è essenziale per costruire un'opinione pubblica ben formata. Infatti, i lavoratori dei media sono spesso considerati come guardiani pubblici con un ruolo vitale in una società democratica. Hanno il dovere di diffondere informazioni e informare il pubblico su tutte le questioni di interesse collettivo, che il pubblico ha anche il diritto di ricevere (Linee guida sulla salvaguardia della privacy nei media, p.6). Quindi, i mass media hanno il dovere di riportare adeguatamente gli eventi che potrebbero essere di interesse pubblico, anche se questo potrebbe mettere a rischio i diritti di alcuni interessati a casua della pubblicazione stessa.

Quindi, ci sono due diritti fondamentali, la libertà di espressione e la privacy, che a volte si scontrano. Questo solleva una questione che può essere risolta solo dal loro corretto bilanciamento in ogni caso concreto. Quando il diritto alla protezione dei dati personali prevale sul diritto alla libertà di espressione e di informazione e viceversa? Questa è una questione che è già stata approfondita dal punto di vista giuridico. Tuttavia, l'approvazione 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 (General Data Protection Regulation, GDPR) e la protezione rafforzata dei diritti di protezione dei dati aprono la porta a nuovi dibattiti. Crediamo

che i giornalisti e le organizzazioni dei mass media dovrebbero essere consapevoli di questa situazione.

Questo manuale non mira a concentrarsi sugli aspetti teorici della questione, ma a fornire ai professionisti dell'informazione, giornalisti, redattori dell'informazione, direttori dei media, ecc., di meccanismi adeguati per garantire il rispetto degli standard minimi legali ed etici in termini di protezione dei dati, assicurando allo stesso tempo un adeguato esercizio della loro professione. Vale a dire, questo manuale si concentra su chiunque lavori in un'organizzazione legata ai media, poiché tutti potrebbero beneficiare delle esenzioni o deroghe derivanti dall'articolo 85.2 del GDPR.

I contenuti di questo manuale combinano diversi quadri normativi: da un lato, il regolamento dell'UE, principalmente il GDPR; dall'altro, il regolamento del Consiglio d'Europa attraverso la Convenzione europea dei diritti dell'uomo e la Convenzione per la protezione delle persone rispetto al trattamento automatico dei dati personali (Convenzione 108). Queste fonti sono completate dalla giurisprudenza della Corte europea dei diritti dell'uomo e della Corte europea di giustizia. Come ha dichiarato il Gruppo dell'articolo 29, "Un elemento importante che emerge dall'attuale situazione legislativa negli Stati membri è che i media, o almeno la stampa, sono tenuti a rispettare alcune norme che, sebbene non facciano parte della legislazione sulla protezione dei dati in senso proprio, contribuiscono alla protezione della vita privata delle persone. Tale legislazione e la spesso ricca giurisprudenza in materia conferiscono forme specifiche di ricorso che sono talvolta considerate un sostituto della mancanza di rimedi preventivi previsti dalla legislazione sulla protezione dei dati" (A29WP, pag. 7). Pertanto, la guida fornita in questo manuale è intesa a seguire la regolamentazione fornita da tutte le istituzioni citate.

Il manuale è diviso in varie parti. Nelle sue prime sezioni, espone il quadro giuridico sul giornalismo e le questioni di protezione dei dati in ambito UE. Le sezioni quattro e cinque, invece, si concentrano su come affrontare le principali questioni etiche che devono essere affrontate da un giornalista o da un'organizzazione mediatica nel quadro del GDPR e dei regolamenti del Consiglio d'Europa. Infine, gli allegati forniscono informazioni dettagliate sul balancing test e sul quadro normativo a livello di Stati membri.

DISCLAIMER: Questo documento ha lo scopo di aiutare i giornalisti ad affrontare il regolamento sulla protezione dei dati. Tuttavia, il suo contenuto non costituisce una consulenza legale, non intende essere un sostituto della consulenza legale e non deve essere considerato tale. È necessario chiedere una consulenza legale o un'altra consulenza professionale in relazione a qualsiasi questione particolare che voi o la vostra organizzazione potreste avere.

2. Il quadro giuridico riguardante la libertà di espressione e la protezione dei dati in ambito UE

Il quadro normativo riguardante il diritto alla libertà di espressione e il regime di protezione dei dati in Europa è principalmente legato ai sistemi giuridici del Consiglio d'Europa e dell'Unione Europea. Nel caso del Consiglio d'Europa, la regolamentazione è duplice. Da un lato, i principali diritti in gioco, il diritto alla libertà di espressione e il diritto alla privacy, fanno parte della Convenzione europea dei diritti umani. Il suo articolo 10.1 afferma che "Ogni persona ha diritto alla libertà di espressione. Questo diritto include la libertà di opinione e la libertà di ricevere e di comunicare informazioni e idee senza interferenze da parte della pubblica autorità e senza riguardo alle frontiere. Il presente articolo non impedisce agli Stati di esigere la concessione di licenze per le imprese di radiodiffusione, televisione o cinema". Ovviamente, questo diritto potrebbe essere limitato secondo le disposizioni del numero 2 di questa clausola. L'articolo 8, invece, si concentra sulla difesa della privacy, affermando che:

> "1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.
>
> 2. Non ci sarà alcuna interferenza da parte di un'autorità pubblica nell'esercizio di questo diritto, eccetto quella che è conforme alla legge e che è necessaria in una società democratica nell'interesse della sicurezza nazionale, della sicurezza pubblica o del benessere economico del paese, per la prevenzione di disordini o crimini, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui".

D'altra parte, la Convenzione per la protezione delle persone rispetto al trattamento automatico dei dati personali (Convenzione 108), anch'essa approvata dal Consiglio

d'Europa, regola le questioni di protezione dei dati. Infatti, al momento attuale è l'unico accordo internazionale giuridicamente vincolante sulla legge di protezione dei dati. Tuttavia, la Corte europea dei diritti dell'uomo non tratta casi sulle presunte violazioni di questa convenzione, poiché è solo legata alla Convenzione europea dei diritti dell'uomo.

Nel contesto dell'UE, il diritto alla libertà di espressione è stato incluso nell'articolo 10 della Carta dei diritti fondamentali dell'UE, che recita:

> "1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere e di comunicare informazioni e idee senza interferenze da parte della pubblica autorità e senza limiti di frontiera.
>
> 2. La libertà e il pluralismo dei media sono rispettati".

Invece, gli articoli 7 e 8 della Carta includevano il diritto alla privacy e il diritto alla protezione dei dati personali che lo riguardano. Attualmente, il quadro giuridico per la protezione dei dati è disegnato principalmente dal regolamento (UE) 2016/679 del GDPR. Le presunte violazioni del diritto dell'UE sono giudicate dalla Corte di giustizia dell'Unione europea (CJEU). Non c'è un pezzo equivalente di legislazione secondaria globale e completa sulla libertà di parola e sui media, soprattutto a causa della posizione della Commissione che l'UE non ha l'autorità di legiferare in questo settore (Biriukova, 6).

Il GDPR si applica ogni volta che qualcuno tratta (raccoglie, conserva, usa o divulga, per esempio) qualsiasi informazione su una persona vivente. Come osserva l'ICO, "non impedisce il giornalismo responsabile, in quanto i principi principali sono abbastanza flessibili da adattarsi alle pratiche giornalistiche quotidiane (...) Tuttavia, i media non sono automaticamente esenti e dovranno assicurarsi di dare qualche considerazione ai diritti di protezione dei dati degli individui. La responsabilità legale di solito ricade sull'organizzazione dei media in questione piuttosto che sui singoli dipendenti, anche se i giornalisti freelance hanno probabilmente i loro obblighi separati". Tuttavia, è bene tenere sempre a mente che i dipendenti delle organizzazioni dei media devono essere consapevoli delle loro responsabilità legali, in particolare il rispetto quotidiano, quando lavorano per il loro datore di lavoro.

3. L'"esenzione giornalistica" nel GDPR

3.1 Introduzione e sfondo

Il GDPR è il principale strumento giuridico riguardante le questioni di protezione dei dati a livello dell'UE. Contiene i principi generali e le regole che si applicano a tutti i trattamenti di dati personali all'interno dell'UE o che coinvolgono i cittadini dell'UE. All'interno delle sue disposizioni, è possibile trovare un riferimento specifico alle questioni in questione. Stiamo parlando della cosiddetta "esenzione giornalistica", come stabilito dall'articolo 85 del GDPR, che è riportata nella tabella sottostante.

Questa clausola è stata inclusa nel GDPR come soluzione per alleviare le tensioni tra la libertà di espressione e il diritto alla protezione dei dati. In effetti, mirava a codificare la necessità generale di bilanciare questi due diritti fondamentali. A colpo d'occhio, ha semplicemente lasciato nelle mani degli Stati membri la possibilità di esentare dalle regole e dagli obblighi specifici del GDPR coloro che esercitano la loro libertà di espressione per "scopi giornalistici" (Biriukova, 14).

Questa esenzione giornalistica non era una novità nel regolamento dell'UE. L'articolo 9 della direttiva sulla protezione dei dati del 1995, il predecessore del GDPR, includeva già una disposizione simile, che ha portato una certa divergenza nella regolamentazione di questa questione negli Stati membri dell'UE. Una raccomandazione del gruppo di lavoro dell'articolo 29 ha [1]riassunto la situazione dividendo gli stati membri in tre gruppi principali:

> "a) In alcuni casi la legislazione sulla protezione dei dati non contiene alcuna deroga esplicita all'applicazione delle sue disposizioni ai media. Questa è la situazione attuale in Belgio, Spagna, Portogallo, Svezia e Regno Unito.

1 Tuttavia, il gruppo di lavoro ha anche riferito che "Le differenze tra questi tre modelli non dovrebbero tuttavia essere sopravvalutate. Nella maggior parte dei casi, indipendentemente da qualsiasi deroga esplicita che possa esistere, la legislazione sulla protezione dei dati non si applica pienamente ai media a causa dello speciale status costituzionale delle norme sulla libertà di espressione e sulla libertà di stampa. Queste norme pongono un limite de facto all'applicazione delle disposizioni sostanziali sulla protezione dei dati o almeno alla loro effettiva applicazione. D'altra parte i dati ordinari". Vedi: Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, Legge sulla protezione dei dati e media, Raccomandazione 1/97, pagg. 6-7, in: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf.

b) In altri casi i media sono esentati dall'applicazione di diverse disposizioni della legislazione sulla protezione dei dati. Questa è la situazione attuale nel caso di Germania, Francia, Paesi Bassi, Austria e Finlandia. Deroghe simili sono previste dal progetto di legge italiano.

c) In altri casi i media sono esentati dalla legislazione generale sulla protezione dei dati e regolati da disposizioni specifiche sulla protezione dei dati. Questo è il caso in Danimarca per tutti i media e in Germania in relazione alle emittenti pubbliche, che non sono coperte da leggi federali o dei Länder sulla protezione dei dati, ma sono soggette a disposizioni specifiche sulla protezione dei dati nei trattati inter-Länder che le regolano".

Il GDPR ha introdotto solo piccoli cambiamenti in questo scenario. Di fatto, l'articolo 85 del GDPR fornisce un quadro d'azione molto ampio agli Stati membri. Devono capire la portata dell'esenzione giornalistica e le circostanze in cui si applica. Tuttavia, perché i loro sviluppi normativi siano validi, devono essere allineati con le disposizioni del GDPR e la Convenzione europea dei diritti umani (CEDU). Pertanto, si deve pensare alle regole da seguire nell'ambiente giornalistico da una doppia prospettiva. Da un lato, bisogna sempre tenere a mente una serie di regole che sono incorporate nel GDPR e/o nella CEDU e la giurisprudenza della Corte di giustizia europea e della Corte europea dei diritti dell'uomo. Queste devono essere rigorosamente seguite nella pratica di questa professione. D'altra parte, si deve considerare che ci possono essere alcune differenze tra gli Stati membri, a seconda del particolare quadro normativo. In ogni caso, non dovrebbero essere eccessive poiché i principi e le regole del GDPR e della CEDU devono essere sempre rispettati.

Tuttavia, è importante sottolineare che alcuni Stati membri non hanno aderito pienamente a questi standard. In Bulgaria, per esempio, la Corte costituzionale ha recentemente dichiarato incostituzionale l'approccio nazionale all'attuazione dell'articolo 85. Ciò era dovuto all'inclusione di un articolo nella legge sulla protezione dei dati personali che stabiliva 10 criteri per decidere se i giornalisti avessero rispettato l'equilibrio tra il diritto all'informazione e quello alla protezione dei dati personali. La Corte ha ritenuto che tali criteri fossero troppo vaghi e potessero creare un rischio di interpretazioni arbitrarie, circostanza che apriva la strada a un imprevedibile potere

interpretativo della Commissione per la protezione dei dati, non necessariamente nell'interesse pubblico per quanto riguarda l'informazione pluralistica sulle politiche e le attività del governo[2].

Inoltre, in Romania, il regolatore della protezione dei dati è stato criticato per aver usato il GDPR per mettere a tacere le voci critiche nei media nazionali. Nel novembre 2018, in Romania è stato riportato un caso che potrebbe servire a riflettere la tensione tra protezione dei dati e libertà di parola. Era legato a un articolo su uno scandalo di corruzione che coinvolgeva un politico e la sua stretta relazione con una società indagata per frode, pubblicato sulla pagina Facebook Rise Project di Bucarest. Qualche tempo dopo la pubblicazione, l'autorità rumena per la protezione dei dati (ANSPDCP) ha inviato una serie di domande ai giornalisti autori dell'articolo.

In teoria, questo era dovuto alla necessità di garantire un equilibrio tra il diritto alla protezione dei dati personali, la libertà di espressione e il diritto all'informazione. L'autorità ha ritenuto che i giornalisti di Rise avessero violato il GDPR pubblicando i video, le foto e i documenti - in sostanza, i dati privati dei cittadini rumeni - per sostenere le accuse dei giornalisti. Ai giornalisti sono state chieste informazioni che potessero rivelare le fonti dell'articolo, sotto l'annuncio che se non avessero collaborato, avrebbero potuto affrontare una sanzione fino a 20 milioni di euro (Warner, 2019).

Un gruppo di dodici organizzazioni per i diritti umani e i media ha reagito a questa richiesta inviando una lettera aperta all'ANSPDCP che chiedeva all'ANSPDCP di analizzare attentamente i casi del GDPR che potrebbero mettere in pericolo la libertà di espressione. Ha anche chiesto di mettere in atto un meccanismo urgente e trasparente per valutare i reclami che coinvolgono operazioni di trattamento dei dati per scopi giornalistici. Allo stesso tempo, sedici ONG per i diritti digitali hanno inviato una lettera al Comitato europeo per la protezione dei dati, con l'ANSPDCP e la Commissione europea in copia, chiedendo che il GDPR non venga usato impropriamente per minacciare la libertà dei media in Romania (Benezic, 2018). In seguito, alcuni parlamentari europei a Bruxelles hanno criticato il caso contro il Rise Project e hanno

2 La Corte costituzionale della Bulgaria respinge la clausola della legge sulla protezione dei dati, 17 novembre 2019, https://sofiaglobe.com/2019/11/17/bulgarias-constitutional-court-rejects-data-protection-law-clause-on-media/#:~:text=La%20corte costituzionale%20della%20Bulgaria%20ha%20rullato,che%20di%20protezione%20dei%20dati%20personali.

contestato l'interpretazione rumena dell'applicazione del GDPR. Infine, tutto questo ha portato a degli avvertimenti da parte della Commissione europea (Nielsen, 2018). Tuttavia, al momento attuale è difficile sapere cosa potrebbe accadere alla fine, dato che il caso è attualmente in corso.

Ci sono, tuttavia, alcuni altri Stati membri che hanno preso la strada opposta. Per esempio, la Svezia ha ritenuto che l'articolo 85 del GDPR dia uno spazio più ampio per le esenzioni agli Stati membri rispetto alla direttiva sulla protezione dei dati, anche perché non richiede che il trattamento sia effettuato "esclusivamente" per scopi giornalistici (una dicitura che era inclusa nella direttiva). Inoltre, il governo svedese ha sostenuto che il considerando 153 del GDPR afferma che il concetto di libertà di espressione deve essere interpretato in modo ampio. Su questa base, la nuova legge sulla protezione dei dati include esenzioni o deroghe più ampie rispetto alla legge sui dati personali del 1998 (McCullagh, 45).

3.2 La portata personale dell'esenzione

Cosa significa "scopi giornalistici"? Cosa significa "giornalismo"? Non c'è nulla di simile a una definizione di giornalismo nel regolamento, dato che è stato eliminato dalle prime bozze del GDPR[3]. Alcuni Stati membri hanno creato le proprie definizioni. La maggior parte di essi è abbastanza aperta, con la principale eccezione dell'Austria, che ha riservato l'esenzione esclusivamente alle "imprese mediatiche, ai servizi mediatici e ai loro dipendenti" (Cullagh, 2019, p.5).

Tuttavia, sembra abbastanza chiaro che il GDPR opta per un significato aperto e inclusivo del termine, che potrebbe essere applicabile anche se il regolamento nazionale non lo riflette. Infatti, nel caso[4] Buivids, la CGUE ha accettato che l'eccezione di giornalista fosse applicabile a un cittadino che ha pubblicato una registrazione video su Youtube, ha dimostrato che l'oggetto della registrazione e la sua pubblicazione era la

3 Infatti, la bozza recitava: "Gli Stati membri dovrebbero classificare le attività come "giornalistiche" ai fini delle esenzioni e delle deroghe da stabilire ai sensi del presente regolamento se l'oggetto di tali attività è la divulgazione al pubblico di informazioni, opinioni o idee, indipendentemente dal mezzo utilizzato per trasmetterle. Esse non dovrebbero essere limitate alle imprese mediatiche e possono essere intraprese a scopo di lucro o senza scopo di lucro" (Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM/2012/011, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52012PC0011).

4 CGUE, Sergejs Buivids contro Datu valsts inspekcija, C-345/17, 14 febbraio 2019.

divulgazione di informazioni, opinioni o idee al pubblico. Allo stesso modo, nel caso[5] Satamedia, la CGUE ha stabilito che le attività di raccolta e diffusione dei dati potrebbero anche essere considerate "giornalistiche", se il loro scopo è quello di divulgare al pubblico informazioni, opinioni o idee, indipendentemente dai mezzi utilizzati. Il fatto che il titolare fosse un'organizzazione non mediatica a scopo di lucro è stato considerato irrilevante per questi scopi.

Non è chiaro cosa succederebbe se un'organizzazione austriaca che potrebbe essere considerata come un'impresa mediatica o un servizio mediatico attuasse una delle deroghe o eccezioni previste dall'articolo 85. In qualche modo, questo creerebbe un conflitto tra il regolamento austriaco e il GDPR, che implora esplicitamente un'ampia estensione del concetto di giornalismo. A nostro parere, è probabile che l'interpretazione del GDPR prevarrebbe.

Tenendo questo in mente, sembra che una definizione ampia di giornalismo abbia molto più senso di una ristretta. Natalija Bitiukova ha scritto che "il giornalismo si riferisce alla produzione e alla distribuzione di informazioni e notizie a un numero indeterminato di persone per perseguire l'interesse pubblico e contribuire al dibattito pubblico" (Bitiukova, p.4). La sua formulazione funziona perfettamente con il GDPR, secondo noi.

Il giornalismo, quindi, deve essere definito come un'attività che copre tutta la produzione su notizie, attualità, affari di consumo o sport[6]. Questo perché l'esenzione copre le informazioni elaborate solo per il giornalismo. Il concetto può anche includere editori e redattori di blog o pagine web su Internet, poiché i commenti fatti su queste piattaforme dovrebbero essere considerati come una manifestazione della propria libertà di espressione. Naturalmente, questo non significa che ogni blog o commento pubblicato online sarà giornalismo, dal momento che alcuni blogger intendono semplicemente prendere parte a comuni interazioni sociali o altri usi ricreativi di

5 CGUE, Tietosuojavaltuutettu contro Satakunnan Markkinapörssi Oy e Satamedia Oy, C-73/07, 16 dicembre 2008

6 Secondo l'ICO, "Preso insieme con l'arte e la letteratura, riteniamo che è probabile che copra tutto ciò che è pubblicato in un giornale o una rivista, o trasmesso alla radio o alla televisione - in altre parole, l'intera produzione della stampa e dei mezzi di trasmissione, con l'eccezione della pubblicità a pagamento (...It would In a wide range of , into (, and of (and). breve, l'esenzione può potenzialmente coprire quasi tutte le informazioni raccolte o create come parte della produzione giornaliera della stampa e dei media radiotelevisivi, e notizie online comparabili o punti vendita di attualità. Tuttavia, le entrate pubblicitarie, la gestione delle proprietà, il debito finanziario, la circolazione o le relazioni pubbliche non sarebbero di solito considerate come giornalismo" (ICO, 29).

Internet. Inoltre, i motori di ricerca sono espressamente esclusi dal concetto e quindi dall'eccezione[7].

3.3 Trattamento dei dati personali: l'ambito materiale

Come mostrato, l'articolo 85 specifica che esenzioni o deroghe potrebbero essere applicabili a chiunque miri a divulgare al pubblico informazioni, opinioni o idee. Tuttavia, che tipo di dati potrebbero essere considerati tali? Quali dati personali possono essere trattati per scopi giornalistici senza dover rispettare il GDPR? Di nuovo, non c'è una risposta semplice a questa domanda. In linea di principio, gli Stati membri hanno voce in capitolo sulla portata materiale dell'esenzione per i giornalisti e le loro politiche non sono sempre le stesse. Ad esempio, l'articolo 7 della legge rumena n. 190/2018, che introduce deroghe per il trattamento dei dati personali per scopi giornalistici, offre solo tre scenari alternativi in cui i dati personali possono essere trattati per scopi[8] giornalistici:

1) se si tratta di dati personali che sono stati chiaramente resi pubblici dall'interessato;

2) se i dati personali erano strettamente connessi alla qualità di persona pubblica dell'interessato; o

3) se i dati personali sono strettamente connessi al carattere pubblico degli atti in cui è coinvolto l'interessato. Se si applica una di queste tre situazioni, il GDPR (tranne il capitolo sulle sanzioni) è completamente escluso dall'applicazione.

Questi tre scenari alternativi sono estremamente limitati rispetto all'attuale giurisprudenza della Corte di giustizia europea e della Corte europea dei diritti dell'uomo. Entrambe le corti considerano che ci sono diversi fattori che devono essere soppesati prima di un'analisi, i più importanti sono il contributo a un dibattito di

7 CGUE, Google SLSpain e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, C-131/12, 13 May 2014, par. 81

8 Denuncia alla Commissione UE da parte di The Association for Technology and Internet (ApTI), 2018, su: https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf

interesse pubblico da un lato e il danno alla vita privata degli interessati dall'altro. Pertanto, la legge romena non sembra effettuare una riconciliazione adeguata tra il diritto alla protezione dei dati personali e il diritto alla libertà di espressione e di informazione.

Il Regno Unito ha adottato un approccio totalmente diverso. Il suo Data Protection Act 2018 considera che l'eccezione giornalista si applica al trattamento dei dati personali quando sono soddisfatte tre condizioni cumulative:

- i dati in questione devono essere trattati in vista della pubblicazione di materiale giornalistico,
- il responsabile del trattamento deve ragionevolmente credere che, con particolare riguardo all'importanza particolare dell'interesse pubblico della libertà d'espressione, la pubblicazione sarebbe nell'interesse pubblico,
- e il responsabile del trattamento dei dati deve ragionevolmente credere che l'applicazione della disposizione GDPR elencata sarebbe incompatibile con il suo scopo giornalistico.

Questo approccio sembra molto più in linea con il quadro normativo.

3.4. La condizione per l'esenzione

Le esenzioni o deroghe previste dall'articolo 85 sono applicabili solo "se sono necessarie per conciliare il diritto alla protezione dei dati personali con la libertà di espressione e di informazione". Quando si applica questa necessità? Il considerando 153 fornisce indicazioni preziose per rispondere a questa domanda:

> *La legislazione degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, compresa l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente regolamento. Il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni da talune disposizioni del presente regolamento se necessario per conciliare il diritto alla protezione dei dati personali con il diritto alla libertà di espressione e d'informazione sancito dall'articolo 11 della Carta. Ciò dovrebbe applicarsi in particolare al trattamento dei dati personali nel settore audiovisivo e negli archivi di notizie e nelle biblioteche stampa. Pertanto, gli Stati membri dovrebbero adottare misure legislative che*

stabiliscano le esenzioni e le deroghe necessarie al fine di equilibrare tali diritti fondamentali.

Pertanto, il GDPR vuole garantire un adeguato equilibrio tra la protezione dei dati e il diritto alla libertà di espressione e di informazione, come sancito dall'articolo 11 della Carta[9]. Ecco perché le *deroghe o le esenzioni da alcune disposizioni del GDPR* si applicano solo *se necessario per conciliare il diritto alla protezione dei dati personali con il diritto alla libertà di espressione e di informazione*. Questa idea di bilanciare entrambi i diritti è stata approvata dalla giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia, che richiede un bilanciamento caso per caso ogni volta che c'è un reale conflitto tra tali diritti. Il punto chiave, tuttavia, è come procedere per farlo. L'ICO afferma che per farlo in modo adeguato, le organizzazioni dovrebbero prendere in considerazione:

- l'interesse pubblico generale della libertà di espressione,
- qualsiasi interesse pubblico specifico nella materia,
- il livello di intrusione nella vita privata di un individuo, incluso se la storia potrebbe essere perseguita e pubblicata in modo meno invasivo, e
- il danno potenziale che potrebbe essere causato agli individui. La guida esistente esposta nei codici di pratica dell'industria può aiutare le organizzazioni a pensare a ciò che è nell'interesse[10] pubblico.

In questo contesto, la nozione di interesse pubblico è particolarmente rilevante, secondo la giurisprudenza della Corte di giustizia dell'UE o della Corte europea dei diritti dell'uomo, come indicato in casi come Buivids[11] o Satakunnan contro la Finlandia[12]. Tuttavia, è difficile da definire. Infatti, la Corte europea dei diritti dell'uomo si è storicamente astenuta dal fornire una definizione di "interesse pubblico". Tuttavia, ha dichiarato, nel contesto dei casi[13] Von Hannover, che "un primo criterio essenziale è il contributo dato dalle foto o dagli articoli della stampa a un dibattito di interesse generale". Così, sembra che questa nozione copra "il dibattito pubblico, politico e storico, le questioni relative ai politici, il comportamento dei funzionari pubblici, le

9 Articolo 11. Libertà di espressione e di informazione

1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere e di comunicare informazioni e idee senza interferenze da parte della pubblica autorità e senza limiti di frontiera.

2. La libertà e il pluralismo dei media sono rispettati.

10 ICO, p. 34

11 CGUE, Sergejs Buivids contro Datu valsts inspekcija, C-345/17, 14 febbraio 2019, par. 60-61.

12 CEDU, Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia, App no 931/13, 21 luglio 2015.

13 CEDU, Von Hannover c. Germania (n. 2), ricorsi n. 40660/08 e 60641/08, 7 febbraio 2012, par. 109.

grandi corporazioni, i governi, le questioni legate al crimine. Tuttavia, anche altre questioni meno evidenti possono essere considerate di interesse pubblico o generale" (Biriukova, 21).

Per riassumere, ci sono alcune variabili che devono essere sicuramente presenti nella definizione di interesse pubblico, che deve comportare "un elemento di proporzionalità - non può essere nell'interesse pubblico interferire in modo sproporzionato o sconsiderato con i diritti fondamentali di privacy e protezione dei dati di un individuo. Se il metodo di indagine o i dettagli da pubblicare sono particolarmente intrusivi o dannosi per un individuo, sarà necessario un argomento di interesse pubblico più forte e specifico per giustificarlo, oltre all'interesse pubblico generale nella libertà di espressione" (ICO, 33). Infatti, l'interesse pubblico non può essere ridotto alla sete del pubblico di informazioni sulla vita privata degli altri o al desiderio del lettore di sensazionalismo o persino di voyeurismo, come la pubblicazione di dettagli sulle attività sessuali di un personaggio pubblico. Se l'unico scopo di un articolo è quello di soddisfare la curiosità dei lettori riguardo ai dettagli della vita privata di una persona, non si può ritenere che esso contribuisca a un qualsiasi dibattito di interesse generale per la società (Guidelines on Safeguarding Privacy in the Media, 12). Per esempio, nel caso Standard Verlags GmbH v. Austria (No.2), è stato giudicato che un giornale aveva violato la privacy delle persone interessate quando ha pubblicato un articolo che commentava le voci che la moglie dell'allora presidente austriaco voleva divorziare da lui e stava mantenendo stretti contatti con un altro politico. Secondo la Corte, i giornalisti non possono riportare inutili pettegolezzi sui matrimoni dei politici. Le linee guida sulla salvaguardia della privacy nei media sottolineano che "nel determinare se una persona è un personaggio pubblico, è di poca importanza per i giornalisti se una certa persona è effettivamente conosciuta dal pubblico. I giornalisti non possono essere limitati dalle affermazioni delle persone interessate che non sono effettivamente note al pubblico. Ciò che conta è se la persona è entrata nell'arena pubblica partecipando a un dibattito pubblico, essendo attiva in un campo di interesse pubblico o in un dibattito pubblico" (Guidelines on Safeguarding Privacy in the Media, 12-20). Una serie di esempi di sentenze prodotte dalla Corte europea dei diritti dell'uomo e raccolte nelle Linee guida è stata incorporata nella prossima tabella (i riferimenti completi sono inclusi nella sezione Fonti di informazione alla fine di questo manuale).

Queste considerazioni aprono la porta a un dibattito più ampio su come bilanciare l'interesse pubblico con il diritto alla privacy. Questo sarà analizzato nella sezione di questo manuale dedicata al legittimo interesse come motivo giuridico per il trattamento dei dati personali.

3.5 La portata materiale dell'eccezione

L'articolo 85 traccia un ampio campo di applicazione per le eccezioni e le deroghe, poiché menziona il capitolo II (principi), il capitolo III (diritti dell'interessato), il capitolo IV (titolare del trattamento e resposabile del trattamento), il capitolo V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), il capitolo VI (autorità di controllo indipendenti), il capitolo VII (cooperazione e coerenza) e il capitolo IX (situazioni specifiche di trattamento dei dati). Pertanto, le eccezioni e le deroghe potrebbero riguardare i *principi generali, i diritti dell'interessato, il titolare del trattamento e il resposabile del trattamento, il trasferimento di dati personali a paesi terzi o organizzazioni internazionali, le autorità di controllo indipendenti, la cooperazione e la coerenza, e situazioni specifiche di trattamento dei dati.*

Tuttavia, è essenziale notare che questa ampia portata non si applicherà necessariamente a tutti gli Stati membri dell'UE. La clausola afferma esplicitamente che gli Stati membri devono prevedere esenzioni o deroghe, ma non elenca tali eccezioni. Dichiara solo che *dovranno* per legge conciliare il diritto alla protezione dei dati personali con il diritto alla libertà di espressione e di informazione, incluso il trattamento per scopi giornalistici e di espressione accademica, artistica o letteraria.

Pertanto, la decisione sulle misure concrete da adottare appartiene agli Stati membri. Essi devono sviluppare tale quadro normativo e notificare alla Commissione le disposizioni adottate in materia di esenzioni o deroghe e, senza indugio, ogni successiva legge di modifica o emendamento che le riguardi. Al momento attuale (novembre 2020), non tutti gli Stati membri hanno sviluppato un tale quadro normativo. Nell'allegato II abbiamo incluso informazioni sul regolamento incorporato dagli stati membri dell'UE, compresi i dati in cui la modifica è stata introdotta. Tuttavia, potrebbe accadere che alcuni paesi abbiano cambiato il loro quadro giuridico in seguito.

3.6 Regolamento applicabile

In generale, i giornalisti dovrebbero cercare di evitare di inviare dati personali al di fuori dello Spazio economico europeo (SEE) senza una protezione adeguata. Ciò che conta come "protezione adeguata" dipenderà "dalla natura delle informazioni, dallo scopo del trasferimento e dalla posizione giuridica all'altro capo, tra le altre cose". Questo principio non impedirà la pubblicazione online, anche se questo rende le informazioni disponibili al di fuori del SEE. Se la pubblicazione è conforme alla DPA sotto altri aspetti (o è esente in quanto di pubblico interesse), sarà opportuno pubblicarla al mondo intero" (ICO, 26).

Cosa succede se i giornalisti hanno sede in uno Stato membro ma desiderano pubblicare contenuti in altri paesi o nello spazio web? Il GDPR afferma che "quando tali esenzioni o deroghe differiscono da uno Stato membro all'altro, si dovrebbe applicare la legge dello Stato membro a cui è soggetto il titolare". Questo potrebbe causare strane conseguenze. Per esempio, sembra che una pubblicazione di un editore (o blogger) con sede in Spagna potrebbe beneficiare di regole relativamente permissive sulla privacy delle "celebrità" lì, anche se la pubblicazione in questione sarebbe vietata se pubblicata da un editore francese e anche se la pubblicazione spagnola è facilmente (e direttamente online) accessibile dalla Francia. Inoltre, potrebbero persino beneficiare del fatto di avere sede in Spagna anche se la pubblicazione fosse in francese e diretta a un pubblico francese. Questo breve suggerimento sulla legge applicabile è insufficiente per l'ambiente online. A meno che questo non venga affrontato più specificamente nel successore della direttiva e-Privacy, potrebbe rendere l'ambiente legale per la libertà di parola molto poco chiaro, in particolare nell'ambiente digitale online (EDRI, 51).

4. GDPR applicato al giornalismo

4.1 Il GDPR in breve

Il GDPR mira a stimolare la creazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno, e al benessere delle persone fisiche (considerando 2). Essa mira a garantire un adeguato equilibrio tra la protezione dei dati e la privacy e alcuni altri diritti fondamentali, come la libertà di parola, per esempio.

Il regolamento si concentra principalmente sul trattamento dei dati personali, cioè "qualsiasi informazione su una persona vivente identificabile che è (o sarà) memorizzata su un computer o altro dispositivo digitale, o archiviata in un sistema organizzato in cui può essere facilmente trovata" (ICO, 2). Pertanto, si concentra su dati strutturati che rivelano informazioni su una persona vivente. Gli appunti scritti a mano non sono considerati dati personali, per esempio. Tuttavia, se qualcuno trasferisce quegli appunti su un computer e li organizza, diventano dati personali.

Allo stesso modo, le informazioni anonimizzate non sono dati personali, ma non devono essere confuse con le informazioni pseudonimizzate, cioè le informazioni che potrebbero essere collegate a una persona (vedi la concettualizzazione qui sotto). Anche le informazioni che si riferiscono a persone decedute non sono protette dal GDPR, anche se la loro pubblicazione può generare problemi legati al diritto all'onore o all'immagine pubblica. D'altra parte, il fatto che un dato sia pubblico o privato non cambia la sua natura di dato personale. Tuttavia, può avere conseguenze sulla liceità del suo trattamento.

4.2 Le basi legali per il trattamento dei dati

In generale, nessun dato personale può essere trattato se non su una base legale. L'articolo 6 del regolamento stabilisce fino a sei motivi giuridici che legittimano il trattamento, vale a dire:

1. l'interessato ha dato il consenso al trattamento dei suoi dati personali per una o più finalità specifiche
2. il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte o per prendere misure su richiesta dell'interessato prima della conclusione di un contratto
3. il trattamento è necessario per il rispetto di un obbligo legale al quale è soggetto il titolare
4. il trattamento è necessario per proteggere gli interessi vitali della persona interessata o di un'altra persona fisica
5. il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio dei pubblici poteri di cui è investito il titolare
6. il trattamento è necessario ai fini dei legittimi interessi perseguiti dal responsabile del trattamento o da un terzo, tranne quando su tali interessi prevalgono gli interessi o i diritti e le libertà fondamentali della persona interessata che richiedono la protezione dei dati personali, in particolare se la persona interessata è un bambino.

Ci sono tre basi legali per l'elaborazione che di solito si applicano ai giornalisti. Queste sono il consenso, l'interesse pubblico e l'interesse legittimo. Saranno esplorati in dettaglio nella sezione 5.3.

4.3 Le categorie speciali di dati

Alcuni dati sono protetti in modo speciale dal GDPR e i giornalisti devono essere estremamente attenti se vogliono trattarli. Queste categorie speciali comprendono: i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, e il trattamento di dati genetici, dati biometrici allo scopo di identificare in modo univoco una persona fisica, dati relativi alla salute o dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Un responsabile del trattamento può trattare tali dati solo se ha un motivo legale per procedere secondo l'articolo 6 del GDPR e si applica una delle circostanze che alleviano il divieto introdotto al loro trattamento dall'articolo 9.1. Le circostanze sono elencate nell'articolo 9.2 del GDPR. In linea di principio, il consenso esplicito da parte del soggetto che fornisce l'informazione o la divulgazione pubblica da parte delle persone a cui l'informazione si riferisce sembrano le circostanze più promettenti. In ogni caso, il responsabile del trattamento deve sempre considerare che, poiché questi tipi di dati sono particolarmente sensibili, dovrebbe rivelarli solo se sussiste un interesse pubblico sostanziale. Nella seguente tabella potete trovare una compilazione della Corte europea dei diritti dell'uomo fornita dalle linee guida sulla salvaguardia della privacy nei media, che raccoglie la giurisprudenza della Corte europea dei diritti dell'uomo

Riguardo a questo problema, l'ICO ha dichiarato che "se le informazioni sono 'dati personali sensibili' le organizzazioni devono anche soddisfare una delle seguenti condizioni:

- la persona ha dato il suo consenso esplicito
- l'informazione è già stata resa pubblica come risultato di passi che una persona ha deliberatamente preso. Non è sufficiente che sia già di dominio pubblico - deve essere la persona interessata che ha fatto i passi che l'hanno resa pubblica" (ICO, 41).

4.4 Diritti del soggetto e doveri del titolare

Infine, è essenziale ricordare che il GDPR fornisce agli interessati alcuni diritti essenziali che devono essere rispettati, a meno che non siano applicabili deroghe ed eccezioni. Questi includono:

- il diritto di accesso. L'interessato ha il diritto di ottenere dal responsabile del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, l'accesso ai dati personali e informazioni su questioni quali le finalità del trattamento, le categorie di dati personali interessati, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, ecc. (vedi articolo 15 del GDPR).

- Il diritto di rettifica. L'interessato ha il diritto di ottenere dal responsabile del trattamento, senza ingiustificato ritardo, la rettifica di dati personali inesatti che lo riguardano. Tenendo conto delle finalità del trattamento, la persona interessata ha il diritto di far completare i dati personali incompleti, anche mediante una dichiarazione supplementare.

- Diritto alla cancellazione ("diritto all'oblio"). L'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione dei dati personali che lo riguardano senza indebito ritardo e il responsabile del trattamento ha l'obbligo di cancellare i dati personali senza indebito ritardo quando si applicano le circostanze elencate nell'articolo 17 del GDPR.

- Diritto alla limitazione del trattamento. L'interessato ha il diritto di ottenere dal responsabile del trattamento la limitazione del trattamento quando l'esattezza dei dati personali è contestata dall'interessato, per un periodo che consenta al responsabile del trattamento di verificare l'esattezza dei dati personali; oppure il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece la limitazione del loro uso; oppure il responsabile del trattamento non ha più bisogno dei dati personali ai fini del trattamento, ma sono richiesti dall'interessato per l'accertamento, l'esercizio o la difesa di diritti legali; oppure l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa di verificare se i motivi legittimi del responsabile del trattamento prevalgono su quelli dell'interessato.

- Diritto alla portabilità dei dati. L'interessato ha il diritto di ricevere i dati personali che lo riguardano e che ha fornito a un responsabile del trattamento in un formato strutturato, di uso comune e leggibile a macchina.

Inoltre, ci sono due doveri essenziali di cui il titolare deve occuparsi secondo il GDPR:

- dovere di fornire all'interessato le informazioni, indipendentemente dal fatto che siano state raccolte presso di lui o meno. Ciò include informazioni sull'identità e i dati di contatto del responsabile del trattamento e, se del caso, del rappresentante del responsabile del trattamento, i dati di contatto del responsabile della protezione dei dati, se del caso, le finalità del trattamento a cui sono destinati i dati personali e la base giuridica del trattamento, ecc (vedi articoli 13 e 14 del GDPR)

- obbligo di notifica per la rettifica o la cancellazione dei dati personali o la limitazione del trattamento. Il responsabile del trattamento comunica la rettifica o la cancellazione dei dati personali o la limitazione del trattamento a ciascun destinatario a cui sono stati comunicati i dati personali, a meno che ciò risulti impossibile o implichi uno sforzo sproporzionato. Il responsabile del trattamento informa l'interessato su tali destinatari se l'interessato lo richiede.

4.5 I concetti principali

Ci sono diversi concetti che sono particolarmente rilevanti nel contesto del GDPR e i giornalisti devono essere consapevoli del loro significato. Questi sono:

- «Dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identifi- cativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- «Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la struttu- razione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- Per «pseudonimizzazione»: si intende il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- Per «archivio» si intende qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

- Per «titolare del trattamento» si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- Per «responsabile del trattamento» si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- Per «destinatario» si intende una persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comuni- cazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comuni- cazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

- Per «terzo» s'intende una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

- Per «consenso dell'interessato» si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'inte- ressato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

5. I principi applicati al giornalismo

5.1 Introduzione

Questa sezione mira a fornire alcuni consigli concreti ai giornalisti per affrontare le loro attività quotidiane. Utilizza un linguaggio semplice e facile da capire, che potrebbe essere compreso da un non esperto. È strutturata sulla base dei principi stabiliti dal GDPR. Questo è dovuto a un fatto semplice: il trattamento deve sempre rispettare questi principi, che sono il nucleo del GDPR. Ciò significa che anche se avete un motivo legale per trattare i dati personali, dovete rispettare questi principi fondamentali. Altrimenti, il vostro trattamento non sarebbe legittimo.

Nelle pagine seguenti, mostriamo questi principi e forniamo consigli su come affrontarli dal punto di vista di un giornalista. Questo consiglio incorpora le raccomandazioni del Consiglio d'Europa nelle sue Linee guida sulla salvaguardia della privacy nei media approvate congiuntamente nel giugno 2018 dal Comitato direttivo sui media e la società dell'informazione (CDMSI) e dal Comitato della Convenzione 108 (Convenzione sulla protezione dei dati del Consiglio d'Europa). Queste linee guida comprendono una raccolta di norme del Consiglio d'Europa (il Consiglio/CoE) e della Corte europea dei diritti dell'uomo (la Corte) riguardanti la protezione della privacy di personaggi pubblici e privati nei media. **Per favore, tenete sempre presente che questa parte del Manuale fornisce principalmente una guida su come affrontare i principi adottati dal GDPR da una prospettiva etica. Al fine di garantire un'adeguata conformità legale, è necessario seguire il regolamento prodotto dal corrispondente stato membro.**

5.2 Legalità, equità e trasparenza

Secondo l'articolo 5.1 (a) del GDPR, "I dati personali sono trattati in modo lecito, equo e trasparente nei confronti della persona interessata". Questo principio include tre diversi requisiti.

- Liceità. Il trattamento dei dati è lecito solo se una base di legittimità lo permette (vedi sezione 3.1). La maggior parte delle informazioni che un giornalista raccoglie sono dati personali. Quindi, ottenere informazioni significa spesso un trattamento di dati e, quindi, dovrebbe seguire i principi stabiliti dal GDPR. Questo significa che deve avere una base legale per trattare i dati e deve giustificare le ragioni per cui li raccoglie.

- Equità. Il concetto di equità è difficile da definire. Si riferisce al fatto che il trattamento deve essere conforme allo spirito del GDPR, non solo alla sua letteralità. In questo modo, permette di introdurre nell'applicazione del RGPD le disposizioni di altri regolamenti di particolare importanza quando si tratta di definire ciò che è considerato "giusto" all'interno dell'UE e dei suoi Stati membri, come la Carta dei diritti fondamentali dell'UE. In generale, tuttavia, si potrebbe affermare che la correttezza implica che si trattino le informazioni in modo da soddisfare le aspettative razionali degli interessati. L'ICO ha dichiarato che l'equità significa che "ove possibile i media dovrebbero raccogliere e utilizzare le informazioni sulle persone in modo equo e legale, e non causare alcun danno ingiustificato. I giornalisti saranno spesso in grado di raccogliere informazioni senza la conoscenza o il consenso del soggetto, ma sarà ingiusto ingannare attivamente le persone sull'identità o le intenzioni del giornalista" (ICO, 40).

- Trasparenza. Il principio di trasparenza cerca di garantire che tutte le parti interessate siano consapevoli di ogni trattamento dei loro dati personali e che possano accedere alle informazioni essenziali sul loro contenuto specifico. In generale, dovreste anche dire alla persona da cui state raccogliendo le informazioni, e alla persona su cui le informazioni riguardano (cioè l'interessato), chi siete e cosa state facendo con le loro informazioni. Se vi forniscono le informazioni per uno scopo concreto, non dovreste usarle per un altro scopo. A volte, notificare agli interessati il trattamento dei dati potrebbe compromettere l'attività giornalistica. A volte, per ottenere una storia, si usano metodi segreti intrusivi, come la sorveglianza. Tutte queste circostanze potrebbero essere accettabili, a condizione che non ci siano alternative più conformi ai principi di protezione dei dati e che la storia sia di pubblico interesse. In effetti, questo è il punto chiave: potete evitare di notificare al soggetto dei dati il trattamento se e solo nella misura in cui ciò renderebbe impossibile l'esercizio del giornalismo. In altre parole, dovete comunicare il trattamento agli interessati, a meno che non consideriate che così facendo non sareste in grado di costruire la storia. Una volta che questo non si applica più, si dovrebbe procedere con gli obblighi stabiliti dal GDPR. Come ha dichiarato l'ICO, "nel contesto del giornalismo, accettiamo che non sarà generalmente praticabile per i giornalisti prendere contatto con tutti coloro sui quali raccolgono informazioni. Sarà spesso giusto raccogliere informazioni su questioni di potenziale interesse giornalistico senza che il soggetto ne sia a conoscenza. Tuttavia, ci saranno casi in cui la correttezza può richiedere un contatto diretto con il soggetto di un'indagine importante, per offrirgli l'opportunità di presentare la propria versione della storia" (ICO, 40).

5.3 Scegliere una base legale per il trattamento

Ci sono tre basi legali per l'elaborazione che di solito si applicano al giornalismo. Queste sono il consenso, l'interesse pubblico e l'interesse legittimo.

Consenso. I dati possono essere trattati se le persone che sono oggetto delle informazioni hanno dato il consenso. Se le informazioni si riferiscono a più persone, il consenso deve essere dato da tutte. Il consenso deve essere libero, specifico e informato. Dobbiamo sottolineare che il semplice fatto che qualcuno abbia pubblicato dati personali in un sito pubblico, come il suo profilo Facebook, non significa che questi dati possano essere utilizzati senza il suo consenso o un'altra base legale. Il consenso deve coprire gli scopi del trattamento dei dati. Pertanto, se si desidera utilizzare i dati per uno scopo diverso da quello originariamente richiesto dalla persona interessata, è necessaria una base giuridica. Ci potrebbero essere delle eccezioni a questa regola, specialmente se il soggetto dei dati è un personaggio pubblico, ma in tali circostanze,

dovreste elaborare i dati sulla base del legittimo interesse, invece che del consenso. Secondo le linee guida sulla salvaguardia della privacy nei media, "i giornalisti dovrebbero, in linea di principio, ottenere il consenso della persona interessata nel momento in cui la foto viene scattata e non semplicemente se e quando viene pubblicata. Altrimenti un attributo essenziale della personalità (l'immagine) dipende da terzi e la persona interessata non ha alcun controllo su di essa" (p. 20).

Interesse pubblico. I dati possono essere trattati se sono necessari per l'esecuzione di un compito svolto nell'interesse pubblico. In effetti, questa è la base giuridica più raccomandabile se fai parte di un'istituzione pubblica che agisce come tale (se il consenso non è applicabile). Se sei un attore privato o se sei un'istituzione pubblica che lavora come attore privato, la base del legittimo interesse è più raccomandabile. Questo è dovuto al fatto che l'interesse pubblico non può legittimare il trattamento se non si considerano gli interessi della persona interessata, poiché l'informazione non è un diritto o un dovere assoluto. Tuttavia, se questo è il caso, l'interesse legittimo e il balancing test sono concetti che funzionano molto bene con il trattamento. Quindi, è consigliabile utilizzare l'interesse legittimo come base legale per il trattamento.

Interesse legittimo. Il trattamento è necessario per "interessi legittimi", a condizione che non causi un danno ingiustificato alla persona interessata. "Gli interessi legittimi includeranno gli interessi commerciali e giornalistici di un'organizzazione di media nel raccogliere e pubblicare materiale, così come l'interesse pubblico nella libertà di espressione e il diritto di sapere". Quindi, è un'ampia base giuridica che comprende l'interesse pubblico ma non solo l'interesse pubblico. Al fine di bilanciare tutti gli interessi coinvolti, si dovrebbe seguire una procedura in grado di garantire che l'interesse legittimo serva come base legale di elaborazione comprende tre fasi principali (Detrekői):

- in primo luogo, dovete identificare un test di interesse legittimo (perché la storia serve l'interesse pubblico)
- in secondo luogo, è necessario eseguire un test di necessità (come la pubblicazione di nomi e dati personali è necessaria per rendere l'articolo informativo)
- infine, è necessario effettuare un balancing test volto a dimostrare che l'interesse del pubblico a conoscere l'argomento trattato nella storia supera l'interesse dell'individuo a tenere i propri dati personali nascosti agli occhi del pubblico. Maggiore è il valore dell'informazione per il pubblico, più l'interesse di una

persona a essere protetta dalla pubblicazione deve cedere, e viceversa (Guidelines on Safeguarding Privacy in the Media, p.11).

Una descrizione estesa di un test di bilanciamento è inclusa nell'allegato I di questo documento. La giurisprudenza della Corte europea dei diritti dell'uomo è piuttosto ampia sull'equilibrio tra interesse pubblico e privacy (vedi Diritto alla protezione della propria immagine, in: https://www.echr.coe.int/documents/fs_own_image_eng.pdf). Un'eccellente sintesi della sua posizione è stata inclusa nella causa Kaboğlu e Oran V. Turchia: "In diverse sue sentenze la Corte ha riassunto i criteri rilevanti per bilanciare il diritto al rispetto della vita privata e il diritto alla libertà di espressione come segue: contributo a un dibattito di interesse pubblico, se la persona interessata è nota, l'oggetto della relazione, il comportamento precedente della persona interessata, il contenuto, la forma e le conseguenze della pubblicazione, nonché, se del caso, le circostanze del caso (vedi *Von Hannover* (no.2) [GC], citata, §§ 108-113, e *Axel Springer AG*, citata, §§ 89-95; si veda anche *Couderc e Hachette Filipacchi Associés*, citata, § 93). Se i due diritti in questione sono stati bilanciati in modo coerente con i criteri stabiliti dalla giurisprudenza della Corte, la Corte avrebbe bisogno di ragioni forti per sostituire il suo punto di vista a quello dei giudici nazionali (cfr. *Palomo Sánchez e altri c. Spagna* [GC], nn. 28955/06, 28957/06, 28959/06 e 28964/06, § 57, CEDU 2011)".

5.4 Limitazione dello scopo

I dati personali devono essere raccolti per scopi specifici, espliciti e legittimi e non devono essere trattati ulteriormente in modo incompatibile con tali scopi. In virtù di ciò, i dati possono essere trattati solo per determinati scopi, che devono essere esplicitamente indicati nella giustificazione del trattamento. Pertanto, dovreste sempre tenere a mente, per esempio, che non potete usare i dati che conservate nei vostri registri per scopi diversi da quelli che hanno giustificato il loro trattamento, a meno che non abbiate una base che serva da fondamento per il nuovo trattamento.

5.5 Minimizzazione dei dati

I dati personali devono essere "adeguati, pertinenti e limitati a ciò che è necessario in relazione agli scopi per cui sono trattati". Questo principio implica che "dovete avere abbastanza informazioni per fare il lavoro, ma non dovreste avere nulla di cui non avete

davvero bisogno". Si noti che questo principio tiene conto dello scopo. Poiché la natura del giornalismo richiede la raccolta e l'incrocio di grandi volumi di informazioni, accettiamo che le informazioni senza rilevanza immediata per una storia attuale possano essere giustificatamente conservate per un uso futuro se si riferiscono a una persona o a un soggetto di interesse giornalistico più generale" (ICO, 25).

5.6 Precisione

Secondo l'articolo 5.1(d), "i dati personali devono essere esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per garantire che i dati personali inesatti, tenuto conto delle finalità per cui sono trattati, siano cancellati o rettificati senza indugio".

L'accuratezza è sia un principio essenziale del GDPR che un valore chiave del giornalismo. Pertanto, i giornalisti devono prestare particolare attenzione a garantire che le informazioni pubblicate siano accurate. A questo scopo, è necessario controllare i fatti. Si può sostenere che solo le informazioni accurate funzionano bene con l'idea di promuovere l'interesse pubblico. Pertanto, le esenzioni e le deroghe dell'articolo 85 si applicano solo se l'informazione è accurata. Tuttavia, l "esenzione può essere disponibile se, per esempio, la storia è urgente nell "interesse pubblico e la breve scadenza rende molto difficile un controllo completo dell "accuratezza. Come per qualsiasi uso dell'esenzione, dovrete ancora dimostrare che qualcuno ad un livello appropriato ha pensato bene a quali controlli potrebbero essere possibili, se la pubblicazione potrebbe essere ritardata per ulteriori controlli, la natura dell'interesse pubblico in gioco e che la decisione di pubblicare è stata, quindi, ragionevole" (ICO, 14).

Inoltre, l'accuratezza implica che devono essere prese misure molto ragionevoli per garantire che i dati personali inesatti siano cancellati o rettificati senza indugio. Questo è essenziale, poiché le informazioni pubblicate potrebbero compromettere seriamente l'immagine pubblica o la vita privata di qualcuno. Secondo l'articolo 29 WP, "il diritto di replica e la possibilità di far correggere le informazioni false, gli obblighi professionali dei giornalisti e le speciali procedure di autoregolamentazione ad essi collegate, insieme alla legge che protegge l'onore (disposizioni penali e civili riguardanti la diffamazione)

devono essere presi in considerazione nel valutare come la privacy è protetta in relazione ai media" (A29WP, p. 7).

Pertanto, i giornalisti devono essere particolarmente attenti e cambiare le informazioni se si dimostra che non riflettono fedelmente la realtà. Questo, naturalmente, deve essere particolarmente considerato se le persone che richiedono la rettifica sono gli interessati, in conformità con il loro diritto di rettifica. Infine, dovreste sempre dichiarare se state esprimendo un'opinione o informando su un fatto. Questo è fondamentale perché il pubblico non interpreti male le informazioni.

5.6 Limitazione dello stoccaggio

Il principio di limitazione della conservazione significa che i dati sono "conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario al conseguimento delle finalità per le quali i dati personali sono trattati" (art. 5 GDPR). Nel contesto del giornalismo, questo significa che, una volta che hai i tuoi dati, devi prendere alcune decisioni riguardo alla loro conservazione e per quanto tempo. I dati sono beni molto preziosi per i giornalisti, dato che potrebbero spesso servire come materiale di fondo. Anche i dati di contatto sono una risorsa molto importante e i giornalisti di solito desiderano conservarli. In linea di principio, è possibile conservare questi dati per lunghi periodi o a tempo indeterminato. Il GDPR non impone un limite di tempo su quanto tempo si possono conservare i dati personali. Il principio della "limitazione della conservazione" impone solo che ci sia una buona ragione per conservare i dati. Supponendo che questo sia il caso, possono essere conservati a tempo indeterminato.

Tuttavia, come afferma l'ICO (ICO, 12), "dovreste rivedere le informazioni conservate di tanto in tanto per assicurarvi che i dettagli siano ancora aggiornati, pertinenti e non eccessivi per le vostre esigenze, e dovreste cancellare qualsiasi dettaglio di cui non avete più bisogno (ad esempio se un contatto ha cambiato il suo numero). Inoltre, il modo in cui conservate le informazioni o come le rivedete dovrebbe essere stabilito nelle politiche organizzative.

5.7 Integrità e riservatezza

I dati devono essere "trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illegale e contro la perdita, la distruzione o il danno accidentali, utilizzando misure tecniche o organizzative adeguate" (art. 5 GDPR). Questo principio ha lo scopo di evitare il trattamento non autorizzato o illecito e la perdita, la distruzione o il danneggiamento accidentale dei dati.

I dati che state conservando sono materiale sensibile. Pertanto, dovete fare del vostro meglio per evitare che vengano persi, rubati o usati male. Cercate di tenerli al sicuro facendo attenzione alle procedure e ai protocolli di sicurezza stabiliti dalla vostra organizzazione. In effetti, tutti i dipendenti di una media company dovrebbero conoscere e seguire le politiche e le procedure dell'organizzazione. Le informazioni dovrebbero essere bloccate, protette da password e criptate dove possibile. Bisogna essere particolarmente attenti alla sicurezza quando si è fuori dall'ufficio con documenti, telefoni o computer portatili contenenti dati personali.

La gamma di sicurezza necessaria non è fissata. In linea di principio, le misure di sicurezza potrebbero essere appropriate per assicurare che non avvenga alcun accesso illegale o per evitare perdite accidentali, distruzione o danni. I giornalisti dovrebbero considerare quanto siano sensibili o riservate le informazioni che detengono, il danno che potrebbe derivare dalla loro perdita o dall'uso improprio, la tecnologia disponibile e i costi coinvolti. Non devono avere una sicurezza all'avanguardia, ma dovrebbe essere adatta al livello di rischio. Le organizzazioni devono considerare le misure di sicurezza tecniche (elettroniche) e fisiche, le politiche e le procedure, la formazione e la supervisione del personale. Queste dovrebbero coprire il personale che lavora sia all'interno che all'esterno dell'ufficio. In ogni caso, le organizzazioni dovrebbero essere in grado di giustificare il livello di sicurezza adottato (ICO, 43).

5.8 Responsabilità

Secondo l'articolo 5.2 del GDPR, "Il responsabile del trattamento è responsabile ed è in grado di dimostrare il rispetto del paragrafo 1". Questa clausola stabilisce che il responsabile del trattamento non è solo responsabile della conformità con il GDPR, ma

dovrebbe anche essere in grado di dimostrare questa conformità. Pertanto, il titolare porta l'onere della prova per la conformità con il GDPR. Nel caso del giornalismo, potrebbe accadere che, di fatto, sia stata attuata una deroga ai diritti del soggetto. In questi casi, le organizzazioni o i giornalisti dovrebbero essere in grado di spiegare perché il rispetto delle disposizioni pertinenti non era compatibile con le finalità del giornalismo. A questo scopo, dovrebbero spesso dimostrare di aver eseguito un balancing test, considerando i diversi interessi in gioco. Affermare che la conformità non è una pratica industriale standard non sarebbe sufficiente in ogni caso. Mantenere una traccia di controllo nei casi che sono controversi o particolarmente suscettibili di rivelarsi controversi potrebbe essere uno strumento appropriato per dimostrare la responsabilità.

Come ha dichiarato Biriukova, "in primo luogo, l'impresa mediatica, un giornalista o essenzialmente chiunque voglia fare affidamento sull'esenzione dovrebbe stabilire l'interesse pubblico della pubblicazione prevista e, in secondo luogo, capire quali obblighi di protezione dei dati sarebbero, in quel caso, in conflitto con gli scopi giornalistici". Forse, quando si tratta di un'indagine giornalistica sulla corruzione governativa, un rifiuto di rivelare la fonte delle informazioni potrebbe essere facilmente difeso, tuttavia, altri scenari meno bianchi e neri (ad esempio, le notifiche di violazione), possono creare enigmi di conformità. Allo stesso tempo, è difficile concepire che, ad esempio, un cittadino giornalista effettuerebbe a priori un tale esercizio di bilanciamento. A meno che non vengano forniti orientamenti più dettagliati, codici di pratiche o di condotta, un approccio così sfumato rischia di rimanere in gran parte teorico e non operativo" (Biriukova, 22).

Dobbiamo anche tenere sempre presente che, in generale, il responsabile del trattamento dei dati non è un giornalista isolato, ma l'organizzazione in cui lavora. Pertanto, l'organizzazione è responsabile dell'attuazione di misure organizzative e politiche sul trattamento dei dati e la responsabilità. Infatti, l'organizzazione deve essere in grado di dimostrare che il trattamento dei dati è stato il risultato finale di un processo decisionale che ha considerato tutte le questioni in gioco. Le procedure potrebbero variare considerevolmente, a seconda del tipo di organizzazione e di informazioni, ma ci dovrebbe essere una sorta di procedura strutturata in ogni organizzazione. Inoltre, sarebbe bene sviluppare alcuni codici di condotta nel quadro

della professione di giornalista in ogni Stato membro. In effetti, il gruppo di lavoro dell'articolo 29 ha dichiarato che "nel valutare se le esenzioni o le deroghe sono proporzionate, si deve prestare attenzione all'etica esistente e agli obblighi professionali dei giornalisti, nonché alle forme di autoregolamentazione della supervisione fornite dalla professione" (A29WP, p.8).

Come afferma l'ICO, "in molte storie quotidiane può essere appropriato per il giornalista usare il proprio giudizio, ma storie di più alto profilo, intrusive o dannose richiedono probabilmente un maggiore coinvolgimento editoriale e una considerazione più formale dell'interesse pubblico. Le politiche organizzative dovrebbero essere usate per spiegare quando è richiesto un maggiore coinvolgimento editoriale. La nostra opinione è che è importante la convinzione al momento del trattamento. Il titolare dei dati deve essere in grado di dimostrare che aveva una convinzione sull'interesse pubblico, vale a dire che la questione dell'interesse pubblico è stata effettivamente considerata. Dovrebbe anche essere in grado di dimostrare che è stato considerato al momento del trattamento pertinente dei dati personali e non solo dopo l'evento. Se un giornalista inizialmente ritiene che una storia sarà di pubblico interesse, ma alla fine l'organizzazione decide di non pubblicarla, l'esenzione può ancora coprire tutte le attività giornalistiche intraprese fino a quel momento.

In secondo luogo, l'esenzione richiede solo una ragionevole convinzione. Questo dà molto più margine di manovra rispetto ad altre esenzioni e riflette l'importanza di un media libero e indipendente (ICO, 35). La seguente tabella mostra alcune misure incluse nelle linee guida sulla salvaguardia della privacy nei media che potrebbero servire alle organizzazioni che cercano di assicurare la conformità con la protezione dei dati.

6. Questioni aggiuntive

6.1 Richieste di accesso all'oggetto

L'accesso alle informazioni conservate dai giornalisti può essere molto importante, sia per i soggetti che coprono, sia per le altre persone. I primi, tuttavia, hanno un diritto di accesso che gli altri non hanno. L'articolo 85, tuttavia, permette agli Stati membri di limitare tale diritto. In questa sezione introdurremo alcune considerazioni su come questa limitazione è solitamente formulata. Nel fare ciò, ci concentreremo sia sul diritto

di accesso che sul diritto di non rivelare le fonti di informazione, che sono ampiamente riconosciuti in Europa.

Secondo l'articolo 15 del GDPR, l'interessato ha il diritto di ottenere dal responsabile del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, l'accesso ai dati personali e le informazioni riguardanti le finalità del trattamento, le categorie di dati interessati, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare destinatari in paesi terzi o organizzazioni internazionali, il periodo previsto per la conservazione dei dati personali, ecc.

Su questa base, un giornalista dovrebbe fornire agli interessati le informazioni che detiene su di loro, a meno che non ritenga che così facendo non sarebbe in grado di costruire la storia. In tali circostanze le eccezioni e le deroghe dell'articolo 85 prevarrebbero sul loro diritto di accesso. Inutile dire che questo accadrebbe solo sotto il presupposto che la storia sia di interesse pubblico. Più alto è l'interesse, più forte è il diritto di non rivelare l'informazione alla persona interessata. Molto spesso, potrebbe succedere che potreste fornire l'accesso ad alcune delle informazioni sul trattamento o sui dati personali utilizzati senza causare danni agli scopi della vostra indagine. Se questo è il caso, dovreste procedere senza indugio.

Il rifiuto di fornire le informazioni richieste potrebbe essere perfettamente giustificato anche dopo la pubblicazione della storia. Se avete forti ragioni per ritenere che ciò potrebbe essere contro l'interesse pubblico, se siete in grado di spiegare perché rispondere minerebbe le future indagini o pubblicazioni, o le attività giornalistiche più in generale, potreste rifiutare la richiesta. Ma dovrete sempre dare una buona ragione per opporvi. Infine, non dimenticate che non dovete includere alcuna informazione su altre persone a meno che non abbiano acconsentito, o che sia ragionevole fornirle senza il loro consenso.

6.2 Fonti riservate

Le fonti di informazione sono sacre per i giornalisti. Diversi strumenti internazionali garantiscono la loro adeguata protezione, tra cui la risoluzione sulle libertà giornalistiche e i diritti umani, adottata alla 4th Conferenza ministeriale europea sulla

politica dei mass media (Praga, 7-8 dicembre 1994) e la risoluzione sulla riservatezza delle fonti dei giornalisti del Parlamento europeo (18 gennaio 1994, Gazzetta ufficiale delle Comunità europee n. C 44/34). Inoltre, la raccomandazione n. R(2000) 7 sul diritto dei giornalisti di non rivelare le loro fonti di informazione è stata adottata dal Comitato dei Ministri del Consiglio d'Europa l'8 marzo 2000. Inoltre, in generale, la legislazione e la pratica interna degli Stati membri prevedono una protezione esplicita e chiara del diritto dei giornalisti di non rivelare informazioni che identificano una fonte, conformemente all'articolo 10 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Esiste quindi un quadro giuridico che permette ai giornalisti di non rivelare le loro fonti. Questo diritto può essere limitato solo alle condizioni menzionate dal principio 3(b) della raccomandazione n. R(2000) 7, cioè:

> "i. misure alternative ragionevoli alla divulgazione non esistono o sono state esaurite dalle persone o dalle autorità pubbliche che chiedono la divulgazione, e
>
> ii. l'interesse legittimo alla divulgazione supera chiaramente l'interesse pubblico alla non divulgazione, tenendo presente che:
>
> -è provato un requisito prioritario della necessità di divulgazione,
>
> -le circostanze sono di natura sufficientemente vitale e grave,
>
> -la necessità della divulgazione è identificata come risposta a un bisogno sociale urgente, e
>
> -Gli Stati membri godono di un certo margine di apprezzamento nel valutare questa necessità, ma questo margine va di pari passo con la supervisione della Corte europea dei diritti dell'uomo.
>
> c. I requisiti di cui sopra dovrebbero essere applicati in tutte le fasi di qualsiasi procedimento in cui il diritto di non divulgazione potrebbe essere invocato".

Infine, non dobbiamo dimenticare che rivelare una fonte implica anche il trattamento dei dati. E che la fonte è anche un soggetto di dati che ha i diritti conferiti dal GDPR. Pertanto, se la fonte è una persona fisica, sarà probabilmente in grado di preservare la

sua identità sulla base del GDPR. Infatti, se il soggetto di una storia fa una richiesta di accesso soggetto e questa potrebbe essere soddisfatta solo rivelando l'identità delle vostre fonti, potete procedere solo se la fonte acconsente, o se è ragionevole farlo, tutte le circostanze considerate. Se la fonte è un'organizzazione, le circostanze cambiano perché le organizzazioni non hanno dati personali. Quindi, i giornalisti devono fare affidamento sull'esenzione per il giornalismo per non rivelare l'identità della fonte se questa non è disposta a rivelare il suo nome o se non è appropriato rivelarlo.

6.3 Minori e popolazione vulnerabile

Dovete stare particolarmente attenti se volete elaborare dati riguardanti minori o popolazioni vulnerabili. In primo luogo, la base legale per tale trattamento potrebbe essere debole. Il consenso di un minore sarà valido solo se tale minore può fornirlo secondo il quadro giuridico dello Stato membro. Il GDPR stabilisce un'età minima, ma gli Stati membri hanno la facoltà di aumentarla. Pertanto, è necessario informarsi su questo. Se il minore o la persona vulnerabile non è in grado di dare il proprio consenso, i suoi rappresentanti legali dovrebbero fornirlo.

Se non è possibile ottenere un consenso informato, allora il trattamento dovrebbe essere basato sulla base del legittimo interesse. Tuttavia, l'interesse legittimo perseguito dal responsabile del trattamento non si applica "qualora su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare quando l'interessato è un minore". Pertanto, è altamente improbabile che il test di bilanciamento permetta il trattamento di dati personali corrispondenti a minori. A nostro parere, pensieri simili sono applicabili alle popolazioni vulnerabili.

Le linee guida sulla salvaguardia della privacy nei media includono una sintesi di due casi relativi ai minori.

- "Nel caso Kahn contro la Germania, le foto di due bambini di Oliver Kahn, un ex portiere della nazionale di calcio tedesca, e di sua moglie sono state pubblicate in una rivista. I giornalisti furono multati perché avevano violato il diritto alla privacy della famiglia. Tutte le foto mostravano i bambini in compagnia dei loro genitori o in vacanza, anche se l'oggetto dei servizi non erano i bambini stessi, ma piuttosto la relazione dei loro genitori e la carriera di Oliver Kahn.

- Nella causa Reklos e Davourlis contro la Grecia, lo scatto di foto di un neonato senza il consenso dei suoi genitori (nel reparto intensivo a cui solo il personale dell'ospedale avrebbe dovuto avere accesso) è stato considerato una violazione del diritto alla privacy anche se le foto non sono state pubblicate".

Si noti che quest'ultima frase è particolarmente rilevante, poiché si concentra sulla necessità di avere una base legale per il trattamento dei dati nel momento in cui le fotografie vengono fatte. La decisione di non pubblicarle evita solo un successivo trattamento illegale (pubblicazione), ma non rimedia alla precedente violazione del diritto alla privacy.

6.4 Punti da prendere in considerazione

Ci sono alcuni consigli che potrebbero servire come riassunto delle cose che dovete sapere sulla conformità della protezione dei dati. In generale, si dovrebbe sempre tenere a mente che:

- La pubblicazione di dati personali implica il trattamento dei dati. Pertanto, devi essere sicuro di essere autorizzato a mostrare questi dati prima di procedere a farlo. In quel momento devi avere una base legale che permetta il trattamento. In caso contrario, sarebbe illegale.

- Se i dati personali sono trattati per servire l'interesse pubblico ("scopi giornalistici"), è probabile che il trattamento non dovrà essere conforme ad alcuni o tutti gli articoli del GDPR. Al contrario, questo significa che se i dati personali sono raccolti, analizzati o altrimenti trattati per altri motivi, il GDPR si applicherà in pieno.

- La pubblicazione di informazioni sensibili potrebbe causare un danno considerevole alla vita privata del soggetto dei dati. Dovete essere sicuri che i benefici per l'interesse pubblico giustifichino tale danno. A questo scopo, dovete bilanciare gli interessi in gioco, considerando diversi livelli di intrusione nella vita privata della persona interessata. Solo quando le considerazioni di interesse pubblico prevalgono chiaramente contro la loro privacy vi è permesso di pubblicare queste informazioni.

- L'intervento di una redazione senior o l'uso del contributo di esperti potrebbe essere di grande aiuto per assicurare che questo requisito sia applicato. Non dimenticare mai che di solito i giornalisti interessati non sono così obiettivi nel bilanciare i diversi interessi coinvolti.

- Ricordate sempre che dovreste raccogliere solo i dati che sono rilevanti per la vostra indagine e che potrebbero essere di interesse pubblico. Se, per esempio, state indagando su un politico sulla base di una possibile pratica di corruzione e scoprite informazioni sensibili sul suo orientamento sessuale, non dovreste

trattarle, sempre che non siano rilevanti per la questione in questione. Questo è un requisito essenziale del principio di minimizzazione, un concetto chiave nel GDPR.

- In casi particolarmente controversi, dove non è del tutto chiaro se o in che misura l'"esenzione giornalistica" si applica al trattamento dei dati, si dovrebbe tenere una traccia di controllo per spiegare le considerazioni sulla protezione dei dati e si dovrebbe chiedere la consultazione dell'autorità di controllo principale (Biriukova, p.30)

- Precauzioni speciali devono essere adottate quando vengono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale, e il trattamento di dati genetici, di dati relativi alla salute o di dati relativi alla vita sessuale o alle condanne penali e ai reati o alle relative misure di sicurezza.

- I dati riguardanti la popolazione vulnerabile e specialmente i minori dovrebbero essere trattati solo se forti ragioni lo giustificano. Bisogna essere assolutamente sicuri che si applichino al trattamento concreto prima di procedere.

7. Domande e risposte

E l'uso secondario dei dati?

La risposta a questa domanda dipende da alcune questioni chiave. In primo luogo, se i dati sono stati raccolti sulla base di un interesse legittimo, un contratto o interessi vitali, possono essere utilizzati per un altro scopo, a condizione che il nuovo scopo sia compatibile con quello originale. Secondo l'articolo 6.4 del GDPR, si dovrebbe prendere in considerazione, tra l'altro:

a. qualsiasi legame tra gli scopi per i quali i dati personali sono stati raccolti e gli scopi dell'ulteriore trattamento previsto;
b. il contesto in cui i dati personali sono stati raccolti, in particolare per quanto riguarda la relazione tra gli interessati e il responsabile del trattamento;
c. la natura dei dati personali, in particolare se vengono trattate categorie speciali di dati personali, ai sensi dell'articolo 9, o se vengono trattati dati personali relativi a condanne penali e reati, ai sensi dell'articolo 10;
d. le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e. l'esistenza di garanzie adeguate, che possono includere la crittografia o la pseudonimizzazione.

Se si desidera utilizzare i dati per la statistica o la ricerca scientifica, non è necessario eseguire il test di compatibilità. Questi nuovi usi sono compatibili con lo scopo originale, secondo l'articolo 5.2 (b) del GDPR.

Se si trattano i dati sulla base del consenso delle persone interessate o in seguito a un requisito legale, non è possibile alcun trattamento ulteriore oltre a quello coperto dal consenso originale o dalle disposizioni di legge. Un ulteriore trattamento richiederebbe di ottenere un nuovo consenso o una nuova base legale.

Mi piacerebbe avere un focus sui soggetti coinvolti nella commercializzazione dei dati personali, una valutazione economica dell'ammontare di questo sistema di traffico globale

In linea di principio, la commercializzazione dei dati è possibile solo se non sono coinvolti dati personali. Nel caso in cui un set di dati mescoli entrambi i tipi di dati, il GDPR è applicabile. Quindi, la commercializzazione dei dati non sarebbe accettabile. I dati personali sono legati ai diritti. Non sono merci e non possono essere comprati o venduti. Vedi la parte delle linee guida PANELFIT dedicata ai dataset e la nostra Analisi Critica per ulteriori dati.

Conservazione/archiviazione dei dati, diritto all'oblio

In generale, i dati non dovrebbero essere conservati più a lungo di quanto strettamente necessario per gli scopi per cui sono stati raccolti. Se il titolare ritiene che potrebbero essere utili in futuro, dovrebbe giustificare questo assortimento. In ogni caso, dovrebbero essere conservati in un modo che funziona bene con i principi di minimizzazione e limitazione della conservazione. Così, dovrebbero essere resi anonimi o, almeno, pseudonimizzati quando possibile.

Il diritto all'oblio è regolato dall'articolo 17 GDPR. Se le condizioni di cui all'articolo 17.1 GDPR sono soddisfatte, il responsabile del trattamento "ha l'obbligo di cancellare i dati personali senza indebito ritardo". Tuttavia, questo non è un diritto assoluto. Le esenzioni dell'articolo 17.3 GDPR identificano i casi in cui questo obbligo non si applica. Una di queste condizioni è che il diritto "non si applica nella misura in cui il trattamento è necessario (...) per esercitare il diritto alla libertà di espressione e di informazione" (articolo 17.3 (a)). Come potremmo bilanciare entrambi i diritti e gli interessi -diritto alla cancellazione e diritto alla libertà di espressione e informazione? Secondo quanto spiegato dalla CGUE nella sentenza Google 2, l'articolo 17.3.a GDPR è "espressione del fatto che il di

ritto alla protezione dei dati personali non è un diritto assoluto ma (...) deve essere considerato in relazione alla sua funzione nella società ed essere bilanciato con altri diritti fondamentali, secondo il principio di proporzionalità".[14] La Corte "stabilisce espressamente l'esigenza di trovare un equilibrio tra i diritti fondamentali alla vita privata e alla protezione dei dati personali garantiti dagli articoli 7 e 8 della Carta, da un lato, e il diritto fondamentale della libertà d'informazione garantito dall'articolo 11 della Carta, dall'altro".[15] D'altra parte, la CEDU ha indicato nella sentenza "M.L. e W.W. vs Germania" del 28 giugno 2018, il che il bilanciamento degli interessi difficilmente potrebbe risolversi a favore di una richiesta di cancellazione avanzata nei confronti dell'editore originario la cui attività è al centro di ciò che la libertà di espressione mira a proteggere.[16] Quindi, in generale, il diritto all'oblio non si applica se impedisce l'esercizio del diritto all'informazione.

Raccolta di dati nelle indagini, archiviazione dei dati, trattamento dei dati da fonti confidenziali

Il segreto professionale è un valore fondamentale che non dovrebbe essere infranto sulla base della protezione dei dati. Molto probabilmente il vostro Stato membro ha adottato norme specifiche per definire i poteri delle autorità di controllo di cui all'articolo 58, paragrafo 1, lettere e) ed f), in relazione ai titolari del trattamento o ai responsabili del trattamento che sono soggetti, in virtù del diritto dell'Unione o degli Stati membri o di norme stabilite da organismi nazionali competenti, all'obbligo del segreto professionale o ad altri obblighi di segretezza equivalenti, ove ciò sia necessario e proporzionato per conciliare il diritto alla protezione dei dati personali con l'obbligo del segreto (cfr. articolo 90 del GDPR). Tali norme, tuttavia, si applicano soltanto ai dati personali che il titolare del trattamento o il responsabile del trattamento ha ricevuto o ottenuto nell'ambito di un'attività coperta da tale obbligo di segretezza.

Ricerca/indagine forense con apprendimento automatico e falsi risultati di tali approcci che riguardano i cittadini

14 CGUE, causa C-136/17, sentenza del 24 settembre 2019, punto 57.

15 CGUE, causa C-136/17, sentenza del 24 settembre 2019, punto 59.

16 Corte europea dei diritti dell'uomo (CEDU), "M.L. e W.W. contro la Germania", 28 giugno 2018.

I giornalisti sono tenuti a controllare attentamente l'accuratezza delle loro informazioni. I dati desunti sono dati personali, poiché forniscono informazioni su una persona identificabile. Tutti i diritti e i doveri stabiliti dal GDPR sono applicabili ad essi.

Strumenti specifici che potrebbero rendere più gestibile l'elaborazione dei dati

PANELFIT Handbook for Journalists and Guidelines potrebbe essere abbastanza utile per questi scopi.

Il ciclo di vita della gestione dei dati. Se si possono conservare i dati o, per esempio, le registrazioni delle interviste, quando bisogna cancellarli? Le migliori pratiche per separare ciò che può essere conservato indefinitamente e ciò che dovrebbe essere cancellato, e per prendersi il tempo di cancellare effettivamente le cose rilevanti dalle posizioni di backup dopo un numero x di anni

Non c'è niente come uno standard oggettivo di tempo di conservazione adeguato nel GDPR. Dipende totalmente dal fatto che la conservazione abbia senso o meno. Se si può dimostrare che la conservazione di tali dati è necessaria per lo scopo del trattamento, è possibile conservarli a tempo indeterminato. In ogni caso, dovrebbero essere conservati in un modo che funzioni bene con i principi di minimizzazione e limitazione della conservazione. Quindi, dovrebbero essere resi anonimi o, almeno, pseudonimizzati quando possibile.

Regolamento sulle informazioni sanitarie

"I dati personali che sono, per loro natura, particolarmente sensibili in relazione ai diritti e alle libertà fondamentali meritano una protezione specifica in quanto il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali" (Considerando 51 GDPR). I dati relativi alla salute sono considerati categorie speciali di dati personali. Secondo l'articolo 9.1, non possono essere trattati a meno che non si verifichi un'eccezione che permetta tale trattamento. Le eccezioni sono elencate nell'articolo 9.2.

Protezione delle immagini

Le immagini sono dati personali. Pertanto, è necessaria una base giuridica per trattare tali dati. Se le immagini corrispondono a più persone, la base giuridica dovrebbe applicarsi a tutti gli interessati. Per esempio, se la base dei dati è il consenso, si

dovrebbe avere il consenso di tutte le persone che sono ritratte nella fotografia o nel video. Naturalmente, l'interesse pubblico potrebbe essere un'ottima base legale per consentire il trattamento, ma dovreste bilanciare attentamente i diritti, le libertà e gli interessi in gioco. Per esempio, se poteste evitare l'identificazione di quelle persone che non sono essenziali per le informazioni, dovreste farlo, specialmente se si tratta di minori.

Come gestire i dati che sono pubblicamente disponibili in un formato non strutturato con lo scopo di compilare un nuovo set di dati che potrebbe eventualmente portare a informazioni preziose, ma anche danneggiare le persone vulnerabili (ad esempio lo scraping di dati personali [pubblici] da un social media)?

In generale, si dovrebbe sempre trovare una base giuridica adatta per il trattamento dei dati. Come già detto, l'interesse legittimo è, in assenza di consenso, il più adatto. Se stiamo parlando della popolazione vulnerabile, questo dovrebbe essere incluso in modo prominente nel balancing test. Il trattamento sarebbe legittimo solo se l'interesse pubblico è così forte da sopraffare l'interesse della persona interessata.

Lo scraping in quanto tale non introduce novità in questa regola di base. Anche se alcuni dati possono essere pubblici, questo non significa che potete usarli come volete. Nel caso di dati che sono espressi in una rete sociale, devi anche tener conto che sei anche un utente di quella rete. Pertanto, i Termini di servizio sono applicabili a voi. Questo in linea di principio non dovrebbe significare troppo, ma dovresti tenerlo a mente.

Informazioni dettagliate su questo sono disponibili qui:

Moreno Mancosu, Federico Vegetti, Cosa si può raschiare e *cosa è giusto raschiare: A Proposal for a Tool to Collect Public Facebook Data, Social media + Society*, Volume: 6 issue: 3, Article first published online: 31 luglio 2020; Edizione pubblicata: 1 luglio 2020, su: https://journals.sagepub.com/doi/full/10.1177/2056305120940703

Come comportarsi quando si vuole inviare un comunicato stampa all'indirizzo email professionale di un altro giornalista (supponendo di non aver avuto alcun contatto precedente). Si deve chiedere il permesso in anticipo (e come, se non via e-mail) o si deve presumere che abbiano interesse ad essere informati, quindi si

invia il comunicato stampa e si dà loro la possibilità di rinunciare? E per quanto riguarda le e-mail di follow-up?

In generale, è possibile inviare e-mail agli indirizzi professionali delle persone, a condizione che:

- hai una buona ragione per pensare che il destinatario possa beneficiare delle informazioni fornite dal comunicato stampa.
- dovreste informare il destinatario di quali dati personali state trattando, per quale scopo, e come possono rimuovere i loro dati dalla vostra mailing list, o cambiarli, nel caso in cui questa lista esista.
- Inoltre, non dovete trattare i dati personali dei destinatari (immagazzinamento, per esempio) più a lungo del necessario.

L'invio di follow-up non viola il GDPR se soddisfa i tre requisiti descritti nella risposta precedente. Il trattamento dei dati in caso di un messaggio di follow-up dovrebbe seguire le stesse regole di un messaggio preliminare.

8. Glossario (art. 4 GDPR)

1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identifi- cativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la struttu- razione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi,

l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comuni- cazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'inte- ressato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «**stabilimento principale**»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'ammini- strazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del

trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51

22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

23) «**trattamento transfrontaliero**»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([1]);

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Allegato I. Il test comparativo

Introduzione: Il balancing test nel contesto del legittimo interesse come base giuridica per il trattamento

L'interesse legittimo è una delle sei basi giuridiche per il trattamento dei dati personali indicate nell'articolo 6(1) del GDPR. Questa base giuridica richiede che i legittimi interessi del titolare o di eventuali terzi a cui vengono comunicati i dati prevalgano sugli interessi, i diritti e le libertà fondamentali degli interessati (articolo 6(1)(f). Per verificare che questo sia effettivamente il caso, i titolari possono fare uso di uno strumento chiamato test di bilanciamento, che è stato raccomandato dal gruppo di lavoro dell'articolo 29, per esempio[17]. Questo strumento è volto a garantire che gli interessi legittimi del responsabile del trattamento o di eventuali terzi a cui vengono comunicati i dati prevalgano sugli interessi e i diritti e le libertà fondamentali delle persone interessate.

Quando i diritti e le libertà fondamentali della persona interessata dalla protezione dei dati non hanno la precedenza?

L'esecuzione di un test di bilanciamento implica la considerazione di diversi fattori chiave che sono decisivi nel determinare quali interessi, libertà o diritti prevalgono, vale a dire[18]:

- la **natura e la fonte dell'interesse legittimo** - se il trattamento dei dati è necessario per l'esercizio di un diritto fondamentale, se è altrimenti di interesse pubblico o se beneficia del riconoscimento nella comunità interessata. È obbligatorio valutare l'eventuale pregiudizio subito dal responsabile del

17 A29WP, Parere 06/2014 sulla nozione di legittimo interesse del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Aprile 2014, pag. 24. All'indirizzo: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accesso 05 gennaio 2020

18 A29WP, Parere 06/2014 sulla nozione di legittimo interesse del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Aprile 2014, pag. 24. All'indirizzo: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accesso 05 gennaio 2020.

trattamento, da terzi o dalla comunità in generale se il trattamento dei dati non ha luogo.

- Il **potere e lo status delle due parti** (titolare o terza parte e soggetto dei dati). Per esempio, un datore di lavoro che intende trattare i dati di un dipendente è in una posizione più forte del dipendente. Se la persona interessata è un minore, i suoi interessi, diritti o libertà dovrebbero essere ponderati.

- La **natura dei dati**. Ai dati di categorie speciali, per esempio, dovrebbe essere dato maggior peso. Allo stesso modo, i dati che le persone possono considerare particolarmente "privati" (per esempio i dati finanziari), i dati dei bambini o i dati relativi ad altri individui vulnerabili dovrebbero essere adeguatamente ponderati.

- L'**impatto del trattamento sugli interessati**. A questo scopo, i titolari dovrebbero considerare se il trattamento potrebbe comportare un rischio elevato per i diritti e le libertà degli individui. Se questo è il caso, devono eseguire una DPIA.

- **Le ragionevoli aspettative degli** interessati su ciò che accadrà ai loro dati. I titolari dovrebbero essere in grado di dimostrare che una persona ragionevole si aspetterebbe il trattamento alla luce delle particolari circostanze applicabili. Se lo scopo e il metodo del trattamento non è immediatamente ovvio e c'è il potenziale per una gamma di opinioni ragionevoli sul fatto che le persone se lo aspetterebbero, i titolari potrebbero voler condurre qualche forma di consultazione, focus group o ricerca di mercato con gli individui per dimostrare le aspettative e sostenere la loro posizione. Se ci sono studi preesistenti riguardo alle ragionevoli aspettative in un particolare contesto, i titolari possono essere in grado di attingere a questi come parte della loro determinazione di ciò che gli individui possono o non possono aspettarsi[19].
- Il **modo in cui i dati sono trattati** (su larga scala, data mining, profiling, divulgazione a un gran numero di persone o pubblicazione);

- Le **garanzie aggiuntive** che potrebbero limitare l'impatto indebito sulla persona interessata, come la minimizzazione dei dati (ad es. rigorose limitazioni alla raccolta dei dati, o cancellazione immediata dei dati dopo l'uso) - misure tecniche e organizzative per garantire che i dati non possano essere utilizzati per prendere decisioni o altre azioni nei confronti degli individui ("separazione funzionale") - ampio uso di tecniche di anonimizzazione, aggregazione dei dati, tecnologie di miglioramento della privacy, privacy by design, valutazioni di impatto sulla privacy e la protezione dei dati; maggiore trasparenza, diritto generale e incondizionato di opposizione (opt-out), portabilità dei dati e misure correlate per responsabilizzare gli interessati, ecc

La questione della salvaguardia supplementare

19 ICO, Come applichiamo i legittimi interessi nella pratica? All'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Accesso: 15 gennaio 2020

Il Gruppo dell'articolo 29 ritiene che le misure di attenuazione e le garanzie, come le misure organizzative o tecniche adottate dal responsabile del trattamento per la protezione dei diritti delle persone interessate, debbano essere incluse nel test comparativo. Esiste tuttavia un approccio alternativo, secondo il quale l'articolo 6, paragrafo 1, lettera f), richiede un test di bilanciamento tra due valori, i legittimi interessi del responsabile del trattamento (o di un terzo) e gli interessi, i diritti e le libertà della persona interessata. Le misure di mitigazione e le garanzie non si adattano bene a nessuno di questi valori. Pertanto, non dovrebbero essere considerate. Altrimenti, supererebbero la parte dei responsabili del trattamento in quanto minerebbero l'importanza del possibile danno da causare agli interessi, ai diritti e alle libertà della persona interessata. Kamara e De Hert hanno fatto delle affermazioni convincenti su questo tema concreto, affermando che[20]

> *"L'inclusione di misure di attenuazione nella valutazione porterebbe a una rappresentazione dell'impatto effettivo previsto del trattamento sui diritti degli interessati, e permetterebbe ancora agli interessi legittimi di prevalere. Questo approccio non "punisce" il responsabile del trattamento che adotta misure di attenuazione e garanzie, non includendole nel test di bilanciamento. Al contrario, incoraggia il titolare a farlo. D'altra parte, si dovrebbe tenere a mente che il peso delle future misure di salvaguardia e di attenuazione è sempre rilevante per la loro realizzazione ed efficacia. Tali misure dovrebbero quindi essere considerate, ma non giocare un ruolo significativo nel determinare da che parte pende la bilancia."*

Alcuni esempi di test di bilanciamento

Esempio 1[21]

Caso: Il giornale Z sta considerando la pubblicazione di alcune fotografie che mostrano X, un attore, dopo essere stato arrestato per possesso di cocaina durante una parata pubblica. X è un personaggio pubblico famoso nel suo paese perché interpreta un

20 Kamara, Irene e De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. All'indirizzo: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf Accessed: 17 gennaio 2020

21 Fonte: A29WP, parere 06/2014 sulla nozione di legittimo interesse del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Aprile 2014, pag. 63. All'indirizzo: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accesso 05 gennaio 2020

poliziotto in una serie televisiva. Inoltre, ha concesso diverse interviste fornendo pubblicamente dati sulla sua vita privata.

Balancing test: i dati riguardano la vita privata dell'individuo piuttosto che la vita professionale. Condividere i dati potrebbe contribuire a un danno significativo per l'individuo. Tuttavia, c'è un interesse pubblico a condividere queste informazioni. L'aspettativa dell'attore che la sua privacy sia effettivamente protetta è stata ridotta dal fatto che ha rivelato dati della sua vita privata in diverse interviste. Il risultato per l'azienda che ha considerato tutti i fattori rilevanti deve essere che gli interessi dell'attore famoso non superano i suoi interessi legittimi nella pubblicazione delle fotografie, e il trattamento è legittimo sulla base di questi interessi legittimi.

Vedi: Axel Springer AG contro Alemania

Esempio 2[22]

Caso: Un datore di lavoro controlla l'uso di Internet durante l'orario di lavoro da parte dei dipendenti per verificare che non stiano facendo un uso personale eccessivo dell'IT dell'azienda. I dati raccolti includono file temporanei e cookie generati sui computer dei dipendenti, che mostrano i siti web visitati e i download effettuati durante l'orario di lavoro. I dati sono trattati senza previa consultazione degli interessati e dei rappresentanti sindacali/consiglio di lavoro dell'azienda. Inoltre, le informazioni fornite alle persone interessate su queste pratiche sono insufficienti.

Test di bilanciamento: La quantità e la natura dei dati raccolti è un'intrusione significativa nella vita privata dei dipendenti. Oltre alle questioni di proporzionalità, la trasparenza sulle pratiche, strettamente legata alle ragionevoli aspettative degli interessati, è anche un fattore importante da considerare. Anche se il datore di lavoro ha un interesse legittimo a limitare il tempo trascorso dai dipendenti a visitare siti web non direttamente pertinenti al loro lavoro, i metodi utilizzati non soddisfano il test di bilanciamento dell'articolo 7(f). Il datore di lavoro dovrebbe utilizzare metodi meno invasivi (ad esempio, limitando l'accessibilità di alcuni siti), che sono, come migliore

22 Fonte: ICO. Come applichiamo i legittimi interessi nella pratica? All'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Accesso: 15 gennaio 2020

pratica, discussi e concordati con i rappresentanti dei dipendenti, e comunicati ai dipendenti in modo trasparente.

FARE e NON FARE

Dos

- Verificare la natura dei dati trattati e prestare particolare attenzione alla protezione degli interessi, dei diritti e delle libertà dei bambini se sono in gioco
- Considerare le ragionevoli aspettative degli interessati
- Eseguire una DPIA se le circostanze lo consigliano

COSE DA FARE

- Non trattare i dati dei bambini se non è assolutamente necessario per raggiungere l'interesse perseguito
- Non elaborare i dati se il test di bilanciamento è inconcludente
- Non esitate a introdurre salvaguardie adeguate per minimizzare il pregiudizio agli interessi, ai diritti e alle libertà degli interessati

Lista di controllo

- I titolari si sono assicurati che gli interessi dell'individuo non prevalgano sugli interessi legittimi del titolare o di terzi.
- I responsabili del trattamento utilizzano i dati degli individui in modi che essi si aspettano ragionevolmente.
- I titolari non stanno usando i dati delle persone in modo molto intrusivo o in un modo che potrebbe causare loro danno, a meno che non abbiano una ragione particolarmente buona.
- I responsabili del trattamento non trattano i dati dei bambini o, se lo fanno, hanno preso ulteriori precauzioni per assicurarsi di proteggere i loro interessi.
- I titolari hanno preso in considerazione misure di salvaguardia per ridurre l'impatto dove possibile.
- I titolari hanno considerato se hanno bisogno di condurre una DPIA.

Ulteriori letture

- Ulteriori esempi di test di bilanciamento sono stati forniti dall'articolo 29WP e possono essere trovati nel loro parere 06/2014 sulla nozione di interessi legittimi del titolare ai sensi dell'articolo 7 della direttiva 95/46/CE
- A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
- EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 april 2017, at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. Accessed 5 May 2020
- ICO, How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/
- ICO, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Accessed 05 May 2020.
- Kamara, Irene and De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. At: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

Allegato II. Analisi comparativa del quadro normativo a livello degli Stati membri dell'UE

La fonte principale delle informazioni raccolte è l'analisi comparativa di Bird&Bird, tranne dove diversamente indicato.

Austria

Ultima revisione: 05.06.2018

L'articolo 9 dell'ADPA prevede disposizioni speciali riguardanti il trattamento dei dati personali nel contesto della libertà di espressione e di informazione. Secondo queste disposizioni, diversi regolamenti del GDPR (in particolare i suoi principi e i diritti degli interessati) non si applicano al trattamento dei dati personali per scopi giornalistici e per scopi scientifici, artistici o letterari.

Belgio

Ultima revisione: 13.09.2018

La sezione 16 della DPA permette il trattamento dei dati personali effettuato con mezzi adeguati per scopi giornalistici o per scopi di espressione accademica, artistica o letteraria. Le sezioni 17 e seguenti stabiliscono eccezioni agli obblighi di informazione (sezione 17), protezione della fonte e del contenuto delle informazioni (sezione 18), eccezioni al diritto di restrizione del trattamento (sezione 19), informazioni sulla rettifica e la cancellazione (sezione 20), e limitazione del diritto di opposizione (sezione 21).

Finlandia

Ultima revisione: 13.11.2018

Secondo la sezione 27 della legge sulla protezione dei dati, solo limitate disposizioni del GDPR si applicano al trattamento dei dati personali per scopi giornalistici o di espressione accademica, artistica o letteraria. Questo approccio mantiene la situazione come era sotto la legge abrogata sui dati personali.

Francia

Ultima revisione: 11.02.2019

Secondo il quadro normativo francese, quando i dati personali sono trattati a fini giornalistici, artistici o di espressione letteraria, non si applicano le disposizioni relative

all'informativa, ai trasferimenti di dati, ai diritti degli interessati, alla conservazione e al trattamento di categorie speciali di dati.

Germania

Ultima revisione: 23.05.2018

Il § 35 della nuova legge federale tedesca sulla protezione dei dati ("FDPA") esenta il responsabile del trattamento dall'obbligo di cancellare i dati personali quando la cancellazione è, in caso di trattamento non automatico dei dati, impossibile o possibile solo con uno sforzo sproporzionato e l'interessato ha un interesse minore alla cancellazione. § L'articolo 27(2) FDPA limita i diritti degli interessati con alcune ulteriori condizioni.

Irlanda

Ultima revisione: 07.06.2018

Ai sensi dell'articolo 43(1) della legge, il trattamento dei dati personali ai fini dell'esercizio del diritto alla libertà di espressione e di informazione, compreso il trattamento a fini giornalistici o di espressione accademica, artistica o letteraria, è esente dal rispetto di alcune disposizioni del GDPR qualora, tenuto conto dell'importanza del diritto alla libertà di espressione e di informazione in una società democratica, il rispetto di tali disposizioni sarebbe incompatibile con tali finalità. La Commissione per la protezione dei dati può rinviare all'Alta Corte, per la sua decisione, qualsiasi questione di diritto che implichi l'esame dell'eventuale esenzione del trattamento dei dati personali ai sensi dell'articolo 43(1).

Italia.

Ultima revisione: 25.10.2018

IDPA titolo XII - sezioni 136-137-138-139. Il codice di pratica sul trattamento dei dati personali & attività giornalistiche (allegato A.1 dell'IDPA) rimane in vigore. La compatibilità di questo codice con il GDPR sarà rivalutata dal Garante italiano per la protezione dei dati personali (di seguito, l'"Autorità"). L'Autorità dovrebbe rivederlo

prima della fine del calendario. Inoltre, l'Italia ha incorporato alcuni principi riguardanti l'esenzione giornalistica attraverso un codice etico, vale a dire

a) il requisito di evitare qualsiasi tipo di censura preventiva

b) l'esenzione del diritto all'informazione nella raccolta dei dati quando l'esercizio professionale lo richiede

c) il dovere del giornalista di rettificare senza indugio gli errori e le imprecisioni

d) la necessità di essere particolarmente attenti quando il trattamento riguarda dati specialmente protetti. In tali circostanze, il trattamento deve essere limitato a fatti di interesse pubblico incontestabile. Inoltre, deve essere limitato agli aspetti essenziali dell'informazione ed evitare riferimenti a persone non collegate. Anche nel caso di fatti che l'interessato può aver reso pubblici, o che sono apprezzati nel comportamento pubblico, il diritto di essere protetto è riservato

e) si suggerisce di ricercare l'"essenzialità" dell'informazione, la proporzionalità di ciò che si rende pubblico, in modo che si limiti a ciò che è essenziale in relazione al caso

f) quando si fa riferimento a una notizia relativa alla salute, si deve rispettare la dignità, il decoro e la vita privata della persona interessata, soprattutto quando si tratta di malattie gravi o terminali, astenendosi dal pubblicare dati analitici o di interesse strettamente clinico. Tuttavia, si può fare un'eccezione a questo requisito se, conformemente al principio di proporzionalità, se la persona interessata si trova in una posizione di particolare importanza pubblica. Lo stesso vale per le informazioni sulla vita sessuale.

I Paesi Bassi

Ultima revisione: 17.09.2018

L'articolo 41 della legge di esecuzione del GDPR prevede che l'ordine di esecuzione del GDPR non si applica quando i dati personali sono trattati esclusivamente per scopi giornalistici o per scopi di espressione accademica, artistica o letteraria. Inoltre, riassume una lista di capitoli e articoli del GDPR che non sono applicabili anche per questi scopi: (a) articolo 7(3), 11(2); (b) capitolo III; (c) capitolo IV (ad eccezione degli

articoli 24, 25, 28, 29 e 32); (d) capitolo V; (e) capitolo VI; e (f) capitolo VII. "L'art. 41 UAVG limita la portata di alcuni obblighi in relazione agli interessi generali (cogenti) in allineamento con l'art 23 GDPR. Pertanto, prevede eccezioni ai diritti dell'interessato e ai doveri del responsabile del trattamento. Il GDPR in parte (art. 12-21 e 34 GDPR) non si applica (nella misura in cui sia appropriato e proporzionato) al trattamento dei dati in vista - tra l'altro - di importanti obiettivi di interesse pubblico, la sicurezza pubblica, la protezione dell'interessato o dei diritti e delle libertà altrui; e/o la raccolta di crediti civili.

Spagna

Ultima revisione: 05.03.2019

L'SDPA non contiene alcun precetto giuridico che concilia la libertà d'espressione con la protezione dei dati. C'è solo un riferimento alla libertà d'espressione nell'articolo 85 che riguarda il diritto alla libertà d'espressione in Internet che tutti hanno.

Svezia

Ultima revisione: 06.09.2018

Data Protection Act paragrafo 1:7: il GDPR e il Data Protection Act non devono essere applicati nella misura in cui ciò violerebbe le leggi sulla libertà di espressione. La legge sulla protezione dei dati prevede che gli articoli 5-30 e 35-50 del GDPR non siano applicabili al trattamento dei dati personali per scopi giornalistici o per scopi di espressione accademica, artistica o letteraria.

Regno Unito

Ultima revisione: 23.05.2018

Il Data Protection Act 2018[23] del Regno Unito offre una visione più sfumata dei confini dell'esenzione, suggerendo che alcune delle disposizioni del GDPR non si

23 Vid. The UK Data Protection Act 2018, Schedule 2, Part 5, par. 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

applicherebbero al trattamento dei dati quando sono soddisfatte tre condizioni cumulative (Cain, 2018):

- i dati in questione devono essere trattati in vista della pubblicazione di materiale giornalistico,
- il responsabile del trattamento dei dati deve ragionevolmente credere che, tenuto conto in particolare dell'importanza particolare dell'interesse pubblico della libertà d'espressione, la pubblicazione sarebbe nell'interesse pubblico, e
- il responsabile del trattamento deve ragionevolmente credere che l'applicazione della disposizione GDPR elencata sarebbe incompatibile con il suo scopo giornalistico.

L'ICO del Regno Unito consiglia di considerare la seconda condizione - "interesse pubblico" - caso per caso, prendendo in considerazione i codici di condotta esistenti e bilanciando l'interesse pubblico nella materia con il livello di intrusione nella vita privata di un individuo. Non è sorprendente vedere "l'interesse pubblico" incluso come uno dei criteri, dato che appare in modo prominente nella giurisprudenza della Corte Europea dei Diritti dell'Uomo. Anche se la Corte europea dei diritti dell'uomo si è astenuta dal fornire una definizione di "interesse pubblico", ha riconosciuto questa nozione per coprire il dibattito pubblico, politico e storico, le questioni relative ai politici, il comportamento dei funzionari pubblici, le grandi corporazioni, i governi, le questioni legate al crimine. Tuttavia, anche altre questioni meno evidenti possono essere considerate di interesse pubblico o generale (Bitiukowa, 21).

Informazioni relative a esenzioni e deroghe in breve

La seguente tabella (Bitiukowa, 25) include un confronto aggiornato tra diversi stati membri dell'UE per quanto riguarda la regolamentazione delle eccezioni.

TABLE 3

The scope of the "Journalistic exemption" under the national law of the selected Member States

GDPR Article	Explanation of the Article	Sweden	United Kingdom	Lithuania	Romania
Article 5(1)(f)	Principle of integrity and confidentiality, which means that a data controller (e.g., a media undertaking) must put in place technical and organizational measures to ensure that the personal data it processes is protection from unauthorized disclosure, accidental loss, damage,etc.	Partially exempted[94] ***	Not exempted**	Not exempted	Exempted
Article 6	Lawfulness of processing, which means that each processing operation can only be considered lawful if a data controller can identify a lawful basis for it (consent, contract, public interest, etc.).	Exempted*	Exempted	Not exempted	Exempted
Articles 12-23	Rights of data subjects, meaning that the data controller should provide individuals with information about processing and respond to their requests.	Exempted	Partially exempted[95]	Exempted	Exempted
Article 28	Processor, which means that where a media undertaking outsources data processing to another entity (e.g., a data centre or a data analytics company), they must have a data processing agreement in place with it.	Exempted	Not exempted	Not exempted	Exempted

* **Not exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply with the rule** the content of which is explained in the second column.

** **Exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **does not have to comply with the rule** the content of which is explained in the second column.

*** **Partially exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply only with the certain aspects of the rule** the content of which is explained in the second column and in the relevant footnote.

Fonti di informazione

Bibliografia

Article 29 Working Party, RECOMMENDATION 1/97 Data protection law and the media. Adopted by the Working Party on 25 February 1997, at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf. Last visited: 17/10/2020.

BIRD & BIRD, Personal data and freedom of expression, At: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression. Last visited: 17/10/2020.

BENEZIC, Dollores, Romania May Be Using GDPR to Intimidate Journalists, Liberties, 2018, At: https://www.liberties.eu/en/news/politicians-in-romania-use-gdpr-to-intimidate-journalists/16384. Last visited: 17/10/2020.

BITIUKOVA, Natalija, Journalistic exemption under the european data protection law, Vilnius Institute for Policy Analysis, 2020, at: https://vilniusinstitute.lt/wp-content/uploads/2020/01/VIPA_Bitiukova_2020_v4_f.pdf. Last visited: 17/10/2020.

CAIN N. and COWPER-COLES, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25 May 2018, https://www.lexology.com/library/detail.aspx?g=b26433e1-0548-4a9d-8351-f720e737f811. Last visited: 17/10/2020.

CULLAGH K. et al, National adaptations of the GDPR, Luxembourg: Blogdroiteuropéen, 17 February 2019, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf. Last visited: 17/10/2020.

DETREKŐI, Zsuzsa, GDPR in Hungary: A Road to Hell?, At: https://medium.com/center-for-media-data-and-society/gdpr-in-hungary-a-road-to-hell-3b60718a0281. Last visited: 17/10/2020.

DRECHSLER L., The GDPR and Journalism. Protecting Privacy or a Break on Democratic Accountability?, 18 September 2018, https://brusselsprivacyhub.eu/publications/ws21.html. Last visited: 17/10/2020.

ECtHR, Guide on Article 8 of the European Convention on Human Rights, August 2020, at: https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Last visited: 17/10/2020.

EDRI, Proceed with caution, at: https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf. Last visited: 17/10/2020.

NIELSEN, Nikolaj. EU Warns Romania Not to Abuse GDPR Against Press, EU Observer (Nov. 12, 2018

REVENTLOW, Nani Jansen, Symposium on the GDPR and international law. Can the GDPR and freedom of expression coexist? At: https://www.researchgate.net/publication/338407067_Can_the_GDPR_and_Freedom_of_Expression_Coexist. Last visited: 17/10/2020.

The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, at: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf. Last visited: 17/10/2020.

WARNER, Bernhard, Online-Privacy Laws Come With a Downside, The Atlantic, 2019, at: https://www.theatlantic.com/ideas/archive/2019/06/europes-gdpr-elevated-privacy-over-press-freedom/590845/. Last visited: 17/10/2020.

Documenti del Consiglio d'Europa

Convention for the protection of individuals with regard to the processing of personal data

Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership

Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors

Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media

Declaration by the Committee of Ministers on the protection and promotion of investigative journalism (26 September 2007)

Resolution 2066 (2015), Media responsibility and ethics in a changing media environment, Parliamentary Assembly

Resolution 1843 (2011), The protection of privacy and personal data on the Internet and online media, Parliamentary Assembly

Resolution 1165 (1998), Right to privacy, Parliamentary Assembly

Resolution 1003 (1993), Ethics of Journalism, Parliamentary Assembly

La giurisprudenza della Corte Europea dei Diritti dell'Uomo

- A v. Norway, No. 28070/06, 9 April 2009
- Ageyev v. Russia, No. 7075/10, 18 April 2013
- Alkaya v. Turkey, No. 42811/06, 9 October 2012
- Armonienė v. Lithuania, No. 36919/02, 25 November 2008
- Axel Springer Ag v. Germany [GC], No. 39954/08, 7 February 2012
- Bédat v. Switzerland [GC], No. 56925/08, 29 March 2016
- Biriuk v. Lithuania, No. 23373/03, 25 November 2008 Björk Eiðsdóttir v. Iceland, No. 46443/09, 10 July 2012
- Bladet Tromsø and Stensaas v. Norway, No. 21980/93, 20 May 1999
- Bodrožić v. Serbia, No. 32550/05, 23 June 2009 Bohlen v. Germany No. 53495/09 and Ernst August von Hannover v. Germany No. 53649/09, 19 February 2015
- Couderc and Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015

- Dorothea Sihler-Jauch against Germany and Günther Jauch v. Germany, Nos. 68273/10 and 34194/11, 24 May 2016 (decision)
- Egeland and Hanseid v. Norway, No. 34438/04, 15 April 2009
- Erla Hlynsdóttir (No.2), No. 54125/10, 21 October 2014
- Feldek v. Slovakia, No. 29032/95, 12 July 2001 Flinkkilä and Others v. Finland, No. 25576/04, 6 April 2010
- Fürst-Pfeifer v. Austria, Nos. 33677/10 and 52340/10, 17 May 2016
- Guseva v. Bulgaria, No. 6987/07, 17 February 2015
- Hachette Filipacchi Associés v. France, No. 71111/01, 14 June 2007
- Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015
- Hachette Filipacchi Associés ("Ici Paris") v. France, No. 12268/03, 23 July 2009
- Haldimann and Others v. Switzerland, No. 21830/09, 24 February 2015
- Janowski v. Poland, No. 25716/94, 21 January 1999
- Khan v. Germany, No. 38030/12, 21 September 2016
- Khmel v. Russia, No. 20383/04, 12 December 2012
- Khuzhin and Others v. Russia, No. 13470/02, 23 October 2008
- Krone Verlag GmbH & Co. KG v. Austria, No. 34315/96, 26 February 2002
- Krone Verlag GmbH & Co KG and Krone Multimedia GmbH & Co KG v. Austria, No. 33497/07, 17 January 2012
- Leempoel & S.A. ED. Ciné Revue v. Belgium, No. 64772/01, 9 November 2006
- Lillo-Stenberg and Sæther v. Norway, No. 13258/09, 16 January 2014 Mitkus v. Latvia, No. 7259/03, 2 October 2012
- MGN Limited v. the United Kingdom, No. 39401/04, 18 January 2011
- Mosley v. the United Kingdom, No. 48009/08, 10 May 2011
- Müller v. Germany (Dec.), No. 43829/07, 14 September 2010
- Österreichischer Rundfunk v. Austria, No. 35841/02, 7 December 2006 Guidelines on Safeguarding Privacy in the Media 38
- Peck. V. United Kingdom, No. 44647/98, 28 January 2003 Pentikäinen v. Finland [GC], No. 11882/10, 20 October 2015 Reklos and Davourlis v. Greece, No. 1234/05, 15 January 2009 Renaud v. France, No. 13290/07, 25 February 2010
- Salihu and Others v. Sweden, No. 33628/15, 10 May 2016 (decision)
- Schweizerische Radio- und Fernsehgesellschaft SRG v. Switzerland, No. 34124/06, 21 June 2012

- Selistö v. Finland, No. 56767/00, 16 November 2004
- Standard Verlags GmbH v. Austria (No.2), No. 21277/05, 4 June 2009
- Standard Verlags GmbH v. Austria (No. 3), No. 34702/07, 10 January 2012
- Toma v. Romania, No. 42716/02, 24 February 2009
- Verlagsgruppe News GmbH v. Austria, No. 10520/02, 14 December 2006
- Von Hannover v. Germany, No. 59320/00, 24 June 2004
- Von Hannover v. Germany (No.2) [GC], Nos. 40660/08 and 60641/08, 7 February 2012
- White v. Sweden, No. 42435/02, 19 September 2006
- Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v. Austria (no.2), No. 62746/00, 14 November 2002 (decision)
- Y v. Switzerland, No. 22998/13, 06 June 2017

  Zvagulis v. Lithuania, No. 861