

# SOMMARIO

## SAGGI

### LA PROPOSTA DI REGOLAMENTO SULL'IA DELLA COMMISSIONE EUROPEA PRESENTATO IL 21.4.2021 (COM (2021) 206 FINAL) TRA MERCATO UNICO E COMPETIZIONE DIGITALE GLOBALE

di Franco Pizzetti

**Sommario:** 1. Inquadramento del tema. – 2. La difficoltà di “tenere insieme” l’obiettivo del Mercato Unico e quello del rafforzamento della capacità di competere a scala globale nella Digital Age. – 3. La struttura della UE come elemento essenziale anche nello sviluppo dell’epoca digitale. – 4. Il Regolamento sulla IA come snodo nel passaggio della UE dalla società predigitale a quella digitale. – 5. Il rafforzamento del ruolo della Commissione e la complessa governance posta alla base del Regolamento sulla Intelligenza Artificiale. – 6. Lo spazio riconosciuto agli operatori privati nel nuovo Regolamento. – 7. Qualche riflessione finale.

Il contributo analizza la proposta della Commissione europea relativa al Regolamento sull’IA, considerandola interessante e importante modello di nuovo approccio regolatorio nel quadro delle sfide che l’Unione europea è chiamata ad affrontare nella competizione globale. Da una parte, i tradizionali meccanismi previsti per la tutela del mercato unico europeo si basano su una regolazione uniforme e su procedure decisionali lunghe e complesse, con un forte ruolo degli Stati Membri; dall’altra, la competitività nel settore digitale è promossa da una regolazione duttile, snella e rapida nell’adeguarsi all’innovazione tecnologica. In questo senso, la proposta di Regolamento esaminata si segnala per un rafforzamento del ruolo e dei poteri delegati della Commissione, per una maggiore attenzione alle finalità perseguite piuttosto che alla minuziosità delle regole; per la valorizzazione dell’impact assessment e della responsabilità degli operatori, e per sistemi di governance settoriali, che andranno peraltro messi in equilibrio per evitare eccessive complicazioni.

*The essay analyzes the European Commission’s proposal for a Regulation on AI as an interesting and relevant model of a new regulatory approach in the framework of the European Union’s challenges in global competition. On the one hand, the European single market is based on a uniform regulation and lengthy and complex decision-making procedures, with a decisive role of Member States; on the other hand, competitiveness in the digital sector is promoted by a ductile regulation, streamlined and quick in adapting to technological innovation. In this sense, the proposal for Regulation strengthens the delegated powers of the Commission; is more focused on the purposes of the regulation rather than on the minutiae of the rules; enhances the impact assessment procedure and the responsibility of operators; creates sectoral governance systems, which will, however, have to be balanced to avoid excessive complications.*

### L’EFFETTIVITÀ DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI (DIRITTO ALL’OBLIO) NEL MONDO DIGITALE

di Camilla Della Giustina e Pierre de Gioia Carabellese

**Sommario:** 1. Introduzione. – 2. Il diritto all’oblio. – 3. Effettività o meno delle tutele apprestate. – 4. Raccordo sistematico.

Il diritto all’oblio, nato grazie all’elaborazione giurisprudenziale prima ancora che normativa, rinviene il proprio aggancio normativo nell’art. 17 del GDPR il quale contiene, a sua volta, un elenco in motivi, al ricorrere dei quali, l’interessato può vantare il diritto di ottenere, da parte del titolare del trattamento, la cancellazione dei dati personali che lo riguardano. Con questo breve contributo, dopo aver introdotto il dibattito sussistente in tema di diritto all’oblio, si affronterà la problematica dell’effettività della tutela apprestata dall’art. 17 GDPR al mondo digitale. Precisamente, l’aspetto che viene evidenziato, è che il mondo di Internet è programmato per aumentare la conoscenza e, di conseguenza, è impossibile trattare in senso proprio di cancellazione di dati immessi nel mondo digitale.

*The right to be forgotten, born thanks to the jurisprudential elaboration even before the regulation, finds its own normative engagement in art. 17 of the GDPR which contains, in turn, a list of reasons, at the recourse of which, the data subject can claim the right to obtain, by the controller, the deletion of personal data concerning him or her. With this brief contribution, after having introduced the discussion on the right to be forgotten, we will address the issue of the effectiveness of the protection provided by art. 17 GDPR in the digital world. Precisely, the aspect that is highlighted, is that the world of the Internet is programmed to increase knowledge and, consequently, it is impossible to treat in the proper sense of deletion of data entered into the digital world.*

---

 IL RICORSO A STRUMENTI INVESTIGATIVI A CD. CONTENUTO TECNOLOGICO. LA *DATA RETENTION* NEL PROCEDIMENTO PENALE ALLA LUCE DELLA GIURISPRUDENZA EUROPEA E DELLA (ONDIVAGA) GIURISPRUDENZA DI MERITO ITALIANA
 

---

di Alessandro Malacarne

**Sommario:** 1. Il progresso tecnologico e i dati esteriori delle comunicazioni. – 2. L'evoluzione della giurisprudenza sovranazionale. – 3. L'ultimo arresto della Corte di Lussemburgo: a) il problema relativo alla cd. efficacia diretta. – b) i cd. reati presupposto. – c) l'individuazione del titolare del potere autorizzatorio. – 4. La recente novella in materia di metadati di traffico telefonico e telematico: a) l'ipotizzata estensione delle ipotesi di cui all'art. 266 c.p.p. – b) l'indispensabile controllo dell'organo giurisdizionale.

La tematica relativa all'acquisizione e conservazione dei cd. dati esteriori delle comunicazioni è stata oggetto di una nuova, recente pronuncia della Corte di giustizia che ha contribuito a ravvivare il dibattito circa la compatibilità eurounitaria della disciplina prevista all'art. 132, Codice *privacy*. A seguito dell'arresto dei giudici europei, un intervento legislativo appariva ormai necessitato. Con il d.l. 30 settembre 2021, n. 132, il Governo si è fatto carico delle diverse istanze in materia ed ha modificato la normativa italiana mostrando così di aver recepito gli insegnamenti comunitari sia sotto il profilo della necessaria elencazione delle fattispecie di reato legittimanti l'accesso ai dati di traffico che con riguardo all'individuazione dell'organo titolare del potere acquisitivo degli stessi.

*The acquisition and conservation of the so-called "external data" of communications has recently been the object of a new Court of Justice's judgement which has rekindled the debate about the european compatibility of art. 132 of the Privacy Code. Following the Court's judgement, regulatory actions look necessary. The Government, by issuing the d.l. September 30th 2021, no. 132, has duly revisited the relevant Italian regulation. By doing so, the Government has proved to have successfully adopted the European guidelines from two perspectives: the necessary enumeration of crimes justifying the access to data and the identification of which authority has the power to access it.*

---

## ■ GIURISPRUDENZA

---

### EUROPEA

LA RESPONSABILITA' DEL GESTORE DI UNA PIATTAFORMA DI CONDIVISIONE DI VIDEO O DI UNA PIATTAFORMA DI *HOSTING* E DI CONDIVISIONE DI FILE AI SENSI DELLA DIRETTIVA 2000/31/CE. RILEVANZA DELL'INERZIA "INFORMATATA".

*Corte di Giustizia Ue; Grande Sezione; sentenza 22 giugno 2021, Cause Riunite C-682/18 E C-683/18*

commento di Alessandro La Rosa

**Sommario:** 1. Il caso de quo. – 2. La Direttiva 2019/790/UE sul diritto d'autore nel mercato unico digitale. – 3. La prima questione. Configurabilità di un "atto di comunicazione al pubblico" del gestore di una piattaforma online. – 4. Seconda e terza questione. Applicabilità dell'art. 14, paragrafo 1, della direttiva 2000/31 al gestore di una piattaforma di condivisione di video su internet. – 5. La responsabilità delle piattaforme online da inerzia "informata".

Il presente contributo esamina la recente pronuncia della Corte di Giustizia resa nelle cause riunite C-682/18 (*YouTube*) e C-683/18 (*Cyando*) relativa alla responsabilità dei gestori di una piattaforma online in caso di violazioni di diritti di proprietà intellettuale commesse dai loro utenti tramite tali piattaforme ai sensi dell'art. 3, paragrafo 1, della Direttiva Infosoc. A tal fine, verrà dapprima presentato il nuovo regime di responsabilità di alcuni gestori di piattaforme online introdotto dall'art. 17 della Direttiva (UE) 2019/790. Seguirà un'analisi dettagliata delle questioni oggetto di rinvio sottoposte al vaglio della Corte europea. Le riflessioni finali saranno dedicate all'individuazione degli effettivi confini tra responsabilità dei gestori di piattaforme online e il regime del c.d. *safe harbour*.

*This paper focuses on the recent EU judgment delivered in the joined cases C-682/18 (YouTube) and C-683/18 (Cyando), concerning Platform liability for copyright infringing user uploads under Article 3(1) of the InfoSoc Directive. To this end, an overview of the new copyright liability regime for certain online platforms provided for by Article 17 of the Directive on Copyright in the Digital Single Market will be first addressed. Then, the relevant questions referred to the CJEU will be analysed in details. Final remarks will concern the effective boundaries between platform's liability and the so called safe harbour regime.*

## COMPARATA

## IL CONTROLLO DEI LAVORATORI TRA STATUTO E GDPR: IL QUADRO ITALIANO E L'ESEMPIO DEI VICINI EUROPEI

*Tribunal Judiciaire de Versailles; sentenza 15 giugno 2021*commento di *Jacopo Liguori e Laura Camardelli*

**Sommario:** 1. Brevi premesse. – 2. Il caso di specie. – 3. La giurisprudenza delle corti europee e delle corti nazionali. – 4. Il quadro italiano. – 5. Alcune conclusioni e indicazioni pratiche.

Il tema del controllo dei lavoratori si lega in prima battuta ad una disciplina che potremmo definire risalente e questo non soltanto per un fattore meramente temporale, ma perché nel nostro ordinamento si è andato ad inserire, seppure a decenni di distanza, in un contesto normativo che ha una matrice molto precisa e storicamente definita. Non si può infatti ignorare che lo Statuto dei lavoratori discende da un preciso contesto politico e di politica del diritto che, per il tramite di Gino Giugni, si riversò in quel testo. Oggi, però, la pervasività delle tecnologie offre ai datori nuove e potenti possibilità di controllo sulle attività lavorative che, di per sé, potrebbero non ricadere nelle fattispecie vietate dallo Statuto, ma piuttosto sfruttarne le zone grigie create con il Jobs Act. Tali forme di controllo spesso passano dagli strumenti di lavoro e precisamente dal monitoraggio dei flussi di dati che lo svolgimento delle mansioni genera, se non addirittura da *wearables* atti specificamente a misurare e analizzare costantemente il comportamento e il rendimento dei lavoratori. Può dunque risultare utile analizzare come le norme rilevanti nel nostro ordinamento, siano esse giuslavoristiche, civilistiche o in materia di privacy, si intreccino e vadano a regolare, limitare o vietare tale controllo. Si tratta infatti di una disciplina stratificata e frammentata tra corpi normativi autonomi, dal combinato dei quali possono generarsi antinomie o quantomeno dubbi interpretativi. Il tema risulta di ancora maggior interesse se si considera quanto esso sia da anni sotto lo scrutinio delle autorità garanti e delle corti dei paesi europei: dal leading case *Bărbulescu* al più recente *Lopez Ribalda*, ai casi che hanno visto coinvolti *Lidl*, *Deutsche Bahn*, *Deutsche Telekom* e *H&M* in Germania fino al caso della divisione francese di *IKEA*.

*The topic of workers' control is first of all linked to a discipline that we could define long-standing - and this is not only due to a mere matter of time, but because in our legal system it has been inserted, albeit decades later, in a regulatory context that has a very precise and historically defined matrix. Indeed, it cannot be ignored that the "Statuto dei Lavoratori" stems from a precise political and legal policy context which, through Gino Giugni, was reflected in that text. Today, however, the pervasiveness of technologies offers employers new and powerful possibilities to control work activities that, in themselves, might not fall under the cases prohibited under the Statute, but rather exploit the grey areas created by the Jobs Act. These forms of control are often made thanks to work tools and precisely through the monitoring of data flows that the performance of tasks generates, if not even through wearables specifically designed to measure and constantly analyse the behaviour and performance of workers. It may therefore be useful to analyse how the applicable rules of our legal system, be they labour law, civil law or privacy law, intertwine and go to regulate, limit or prohibit such control. In fact, we witness a layered and fragmented discipline between autonomous bodies of law, the combination of which may give rise to inconsistencies or at least doubts on their interpretation. The subject is even more interesting if one considers how much it has been under the scrutiny of the data protection supervisory authorities and of the courts of European countries for years: from the leading case *Bărbulescu* to the more recent *Lopez Ribalda*, to the cases involving *Lidl*, *Deutsche Bahn*, *Deutsche Telekom* and *H&M* in Germany and the case of the French division of *IKEA*.*

## CIVILE

## LA CESSIONE NON AUTORIZZATA DEL "PERSONALITY CODE" CONTENUTO NEL DUPLICATO DI UNA CHIAVE ELETTRONICA E' TRATTAMENTO ILLECITO DI DATI PERSONALI?

*Corte di Cassazione; sezione I civile; ordinanza 7 luglio 2021, n. 19270*commento di *Mariangela Ferrari*

**Sommario:** 1. La fattispecie. – 2. Il concetto di dato personale a fini identificativi. – 3. Identità personale e digitale. – 4. Il trattamento dei dati.

La Cassazione, nell'osservanza della vecchia disciplina in materia di *privacy*, alla luce dell'ampio concetto di dato personale, ha attribuito tale valenza al *personality code* immagazzinato nella chiave elettronica di un autoveicolo, ritenendo così necessario disporre l'accertamento della illiceità o meno del trattamento operato dal concessionario che abbia consegnato il duplicato ad un soggetto (rivelatosi in seguito un truffatore) non autorizzato secondo le regole accettate in sede di conclusione del contratto dalle parti.

*The Italian Supreme Court has attributed the value of personal data to the "personality code" stored in the electronic key of a vehicle. It's necessary assess if the dealer, who delivered a duplicate to an unauthorized person (later revealed to be a scammer), is responsible for illegal treatment, when he doesn't respect the rules accepted at the conclusion of the contract by the parties.*

## RATING REPUTAZIONALE, TRASPARENZA DELL'ALGORITMO E VALIDITÀ DEL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

*Corte di Cassazione; sezione I civile; ordinanza 25 maggio 2021, n. 14381**commento di Andrea Parziale*

**Sommario:** 1. Introduzione. – 2. Il caso di specie e la sentenza del Tribunale di Roma. – 3. L'ordinanza della Cassazione tra classificazione reputazionale e validità del consenso. – 4. Alcune considerazioni tra GDPR e la Proposta di Regolamento sull'Intelligenza Artificiale.

Con l'ordinanza in commento, la Cassazione stabilisce il principio per cui, nel caso di una piattaforma *web* preordinata all'elaborazione di profili reputazionali, la validità del consenso al trattamento dei dati personali è subordinata alla conoscibilità, da parte dell'interessato, dello schema esecutivo dell'algoritmo sotteso e dei suoi elementi costitutivi. Dopo aver valutato il possibile ruolo del principio in esame nell'economia della disciplina del GDPR in tema di trattamenti automatici, il presente contributo argomenta che tale principio è, in effetti, suscettibile di applicarsi a tutti i trattamenti di dati a base algoritmica, imponendo al titolare di garantire, per la validità del consenso dell'interessato, non una generica trasparenza dell'algoritmo, ma più esattamente una sua spiegabilità e intellegibilità da parte dell'interessato. Infine, vengono evocati i limiti del suddetto principio in relazione ai sistemi, sempre più diffusi, di Intelligenza Artificiale, anche alla luce della Proposta di Regolamento formulata in proposito dalla Commissione europea.

*By ordinance no. 14381/2021, the Italian Corte di Cassazione established the principle according to which, in the case of a reputation rating web platform, the validity of the consent to the processing of personal data is subject to the knowledge, by the data subject, of the executive scheme of the underlying algorithm and its constituent elements. After having assessed the possible role of the principle in question in the GDPR rules on automatic processing, the essay argues that this principle may, in fact, apply to all algorithmic-based data processing operations, requiring the data controller to ensure the validity of the data subject's consent not through a generic transparency of the algorithm, but more precisely through its "explainability" and intelligibility by the data subject themselves. Finally, the limits of the aforementioned principle are evoked in relation to the increasingly widespread AI systems, also in the light of the European Commission's Proposal for a Regulation on Artificial Intelligence.*

## TUTELA DELLA RISERVATEZZA: I DATI PERSONALI DEVONO ESSERE UTILIZZATI SOLO SE INDISPENSABILI

*Corte di Cassazione; sezione I civile; ordinanza 26 aprile 2021, n. 11020**commento di Annamaria Doria*

**Sommario:** 1. Il caso concreto. – 2. Il principio di minimizzazione: framework normativo. – 3. La difficile scelta dei soli dati necessari alla finalità. – 4. Diritto alla riservatezza e alla tutela dei dati personali e diritto di difesa: antagonismo e bilanciamento – 5. Risarcibilità del danno da illecito trattamento dei dati personali. – 6. Osservazioni conclusive.

La Suprema Corte ha ribadito che il trattamento delle informazioni personali è lecito purché avvenga nel rispetto del criterio di minimizzazione, dovendo essere utilizzati solo i dati indispensabili, pertinenti, limitati a quanto necessario rispetto alle finalità. La divulgazione di informazioni "eccedenti" comporta il risarcimento del danno, grave e serio che si identifica con le conseguenze della lesione dell'interesse tutelato.

*The Supreme Court reiterated that the processing of personal information is lawful as long as it takes place in compliance with the minimization criterion, since only the indispensable, pertinent data must be used, limited to what is necessary with respect to the purposes. The disclosure of "excess" information entails compensation for damage, serious and serious which is identified with the consequences of the damage of such injury.*

## LA COMUNICAZIONE A MEZZO PEC SENZA LA SENTENZA IN ALLEGATO IMPEDISCE LA DECORRENZA DEL TERMINE BREVE D'IMPUGNAZIONE. DAL RITO FORNERO SPUNTI PER QUALCHE RIFLESSIONE SULLE COMUNICAZIONI E LE NOTIFICAZIONI NELL'ERA DEL PROCESSO TELEMATICO

*Corte di Cassazione; sezione lavoro; sentenza 13 aprile 2021, n. 9647**commento di Pasquale Mazza*

**Sommario:** 1. Introduzione. – 2. Lo scopo della comunicazione. – 3. Le ragioni di diritto che sorreggono l'orientamento maggioritario e perché (secondo noi) non sarebbe plausibile una lettura di segno contrario. – 4. Varie altre situazioni in cui la comunicazione del provvedimento decisivo è messa sullo stesso piano della notificazione. L'equipollenza, però, non sempre presuppone l'integrale conoscenza del provvedimento – 5. Chi e come può provare il contenuto del messaggio di posta elettronica certificata.

Che la comunicazione integrale del provvedimento decisivo non possa equipararsi *quoad effectum* alla mera comunicazione di deposito è un'affermazione apparentemente ineccepibile. Eppure, nell'ambito del rito Fornero, la corte di legittimità è stata più volte chiamata a ribadire le ragioni di un orientamento che ormai viaggia sui binari della stabilità perché sorretto dalla logica del diritto processuale. Con le funzioni assunte oggi dalla comunicazione in vari altri contesti, rimangono tuttavia presenti ambiguità legate all'uso che si fa del messaggio di posta elettronica certificata, su cui il presente lavoro si sofferma brevemente con l'intento di discernere le differenze in un'area del vissuto processuale dai frequenti (e sovente inesorabili) risvolti preclusivi. I mezzi tramite cui fornire la prova della comunicazione ed il possibile rilievo d'ufficio della decadenza sono esaminati nel paragrafo conclusivo.

*In a decision issued by the Supreme Court of Cassation, it was sustained the principle according to which the deadline for challenging a judgment runs from the moment in which the party receives the service of the full text of the judgment. Indeed, it is not enough that the clerk only transmits the*

*operative part of a decision. The author, hence, draws inspiration to deepen the subjects of services by using the certified e-mail, time limits for filing appeals and the way to provide proof.*

#### FORMA SCRITTA, DOCUMENTO INFORMATICO ED EQUIVOCI INTERPRETATIVI

*Corte di Cassazione; sezione II civile; ordinanza 10 marzo 2021*

*commento di Matilde Ratti*

**Sommario:** 1. La decisione. – 2. Il point and click per la conclusione del contratto e come firma elettronica semplice. – 3. L'attuale disciplina del documento informatico con firma elettronica. – 4. La normativa applicabile all'epoca dei fatti. – 5. Forma scritta e firme elettroniche nello scenario europeo. – 6. Ulteriori riflessioni sulla forma del contratto e sulle operazioni in covered warrant. – 7. Considerazioni conclusive.

L'ordinanza affronta il tema dell'idoneità del documento informatico con firma elettronica semplice a integrare il requisito della forma scritta. Il caso ha ad oggetto un contratto di intermediazione finanziaria che veniva concluso tramite *point and click* nell'area personale dei clienti sul sito *web* della banca. Il giudice di primo grado dichiarava la nullità del contratto poiché carente del requisito della forma scritta, mentre la Corte di appello ribaltava l'esito della pronuncia sostenendo che, nel caso di specie, non fosse necessaria la firma elettronica qualificata o la firma digitale per la conclusione del contratto. L'ordinanza in commento conferma la decisione del giudice di appello, sostenendo che la normativa applicabile all'epoca dei fatti consentisse al giudice di valutare se i documenti informatici con firma elettronica semplice potessero integrare il requisito della forma scritta.

*The decision addresses the issue of determining the juridical value of an electronic document with a simple electronic signature and the possibility to consider it equivalent to a paper document. The case concerns the point-and-click acceptance of a financial contract. While the Tribunal challenged this method of signature, declaring the contract null and void as it lacked the requirement of the written form, the Court of Appeal overturned the ruling, stating that a qualified electronic signature or a digital signature was not strictly necessary for the conclusion of such a contract. This decision confirms the position of the Court of Appeal and establishes that the applicable law allowed the judge to assess whether electronic documents with simple electronic signatures could satisfy the written form requirement.*

#### IL DIRITTO A ESSERE SE STESSI SUL WEB

*Tribunale di Roma; sezione I civile; 9 febbraio 2021, n. 2297*

*commento di Antonio Musio*

**Sommario:** 1. I fatti di causa e la decisione del Tribunale di Roma. – 2. Il diritto all'immagine nel sistema civilistico. – 3. La tutela indiretta del diritto all'immagine. – 4. Dal diritto all'immagine al diritto ad essere se stessi. – 5. Il diritto a essere se stessi alla prova di internet.

Il Tribunale di Roma è tornato sul tema del diritto all'identità personale con riferimento alla pretesa di una famiglia di non veder accostata la propria immagine agli ideali di un certo orientamento ideologico. Nella specie, un'associazione politica aveva utilizzato l'immagine dei componenti del nucleo familiare trovata su *internet* al fine di promuovere una manifestazione pubblica in favore della famiglia. Secondo il giudice capitolino va riconosciuto il diritto al risarcimento del danno non patrimoniale in capo agli attori in conseguenza dell'omesso offuscamento dell'immagine nonostante la diffida rivolta all'associazione a procedere in tal senso. In particolare, sebbene non vi fosse ormai la possibilità di provvedere alla rimozione dei manifesti affissi in città, essendo la suddetta diffida arrivata solamente alcuni giorni prima dell'evento promosso, lo stesso non si potrebbe dire per quanto riguarda la rimozione dell'immagine dai siti *internet*. È da tale comportamento che deriva una lesione del diritto all'identità personale, inteso come il diritto di ogni persona a che la proiezione sociale della propria personalità non subisca travisamenti o distorsioni a causa dell'attribuzione di idee, opinioni o comportamenti differenti da quelli che ha manifestato nella vita di relazione.

*The Court of Rome returned to the issue of the right to personal identity with regard to the claim of a family not to see its image linked to the ideals of a certain ideological orientation. In this case, a political association had used the image of the family members found on the internet in order to promote a public demonstration in favor of the family institution. According to the judge, the right to compensation for non-pecuniary damage suffered by the plaintiffs must be recognized as a result of the omitted obscuration of the image despite the warning in this sense addressed to the association. In particular, although it was no longer possible to remove the posters affixed in the city, since the aforementioned warning arrived only a few days before the promoted event, the same could not be said with regard to the removal of the image from the websites. It is from this behavior that a violation of the right to personal identity derives, understood as the right of each person to have the social projection of his or her personality not being misrepresented or distorted due to the attribution of ideas, opinions or behaviors different from those that he or she manifested in the relational life.*

## LE VULNERABILITÀ IN AMBIENTE DIGITALE. L'AMMINISTRAZIONE DI SOSTEGNO QUALE STRUMENTO DI TUTELA?

*Tribunale di Ravenna; sentenza 30 gennaio 2021, n. 102**commento di Anna Anita Mollo*

**Sommario:** 1. La fattispecie oggetto di giudizio: l'evoluzione tecnologia e la capacità di autodeterminazione dell'individuo (utente). – 2. La prodigalità, le truffe affettive in rete e le misure di protezione più adeguate. – 3. Il romantic scam e l'istituto dell'amministrazione di sostegno. – 4. La vulnerabilità nell'era delle tecnologie digitali: quale tutela? – 5. Conclusioni.

Il presente contributo ha ad oggetto l'effettività della tutela offerta dal nostro ordinamento giuridico verso nuove forme di vulnerabilità, tali in quanto sviluppate nel contesto digitale, della rete *Internet* in particolare. La sentenza in commento analizza una fattispecie giuridica particolare, relativa a vere e proprie truffe affettive realizzate *online*, definite nell'ambito della giurisprudenza penale "*romantic scam*"; respingendo la richiesta di inabilitazione dei familiari della vittima, il giudice adito ha ritenuto di applicare la misura di protezione dell'amministrazione di sostegno, ritenendola più adeguata al caso di specie e rinviando la causa al giudice tutelare competente; nelle more, per evitare un vuoto di protezione, il giudice ha provveduto a nominare un amministratore di sostegno provvisorio. L'autore esamina l'impatto che l'uso distorto della rete può determinare sulle categorie giuridiche della capacità e delle volontà dei soggetti che operano nello spazio virtuale, interrogandosi sulla possibilità che siano le particolari caratteristiche dello strumento (e le modalità di relazionarsi) ad indurre gli utenti a sviluppare forme di fragilità che nella vita reale restano celate.

*The contribution aims to address the effectiveness of the protection offered by our legal system against new forms of vulnerability, such as they are developed in the digital context. The sentence in question analyzes a particular legal case defined "romantic scam"; by rejecting the request of the victim's family members, the court seised that in this case the most adequate protection measure is the support administration. The author examines the impact that the distorted use of Internet can determine on the categories of ability and will of the subjects operating in the virtual space, wondering about the possibility that may be the tool (and the ways of relating) to induce users to develop forms of fragility that remain hidden in real life.*

## PENALE

## SFIDE "ESTREME" TRA MINORI E SOCIAL NETWORK: ISTIGAZIONE AL SUICIDIO?

*Tribunale di Milano; sez. IX penale; sentenza 19 maggio 2021; n. 5678**Tribunale di Milano; sez. G.I.P.; decreto di archiviazione 21 marzo 2021**commento di Beatrice Panattoni*

**Sommario:** 1. Le vicende oggetto delle pronunce del Tribunale di Milano. – 2. Il caso della Blue Whale challenge. – 3. Blue Whale challenge e blackout challenge: stesso fenomeno sociale ma diverse qualificazioni giuridiche del fatto. – 4. Blackout challenge: comportamenti rimproverabili o riprovevoli? – 5. La dimensione collettiva del fenomeno.

Tra gli utenti più giovani dei *social network* si sono diffuse pratiche, percepite dagli stessi quali "sfide" o "giochi", estremamente pericolose e dannose, in grado di violare beni giuridici di primaria importanza quali la tranquillità psico-fisica e la libertà d'autodeterminazione dei minori, così come la loro stessa incolumità. Gli addebiti di responsabilità penale configurabili in questi casi pongono questioni differenti a seconda della tipologia di "sfida" a cui la vittima ha partecipato, essendo alcune di esse caratterizzate da una portata offensiva più chiara ed evidente rispetto ad altre, e coinvolgendo in modo diverso gli utenti della rete, i quali possono trovarsi parte di rapporti intersoggettivi diretti con un altro soggetto determinato, oppure in nodi della rete *social* dove le forme comunicative si sostanziano nel caricamento di contenuti multimediali diretti verso un numero indeterminato di utenti o *follower*.

*Practices extremely dangerous and harmful have widespread among the youngest users of social networks. Even though they can violate legal goods of primary importance such as psycho-physical tranquility and freedom of self-determination of minors, as well as their own safety, they are perceived as "challenges" or "games" by the participants. The forms of criminal responsibility that can be configured in these cases pose different issues depending on the type of "challenge" in which the victim has participated, being some of them characterized by a clearer and more evident harm compared to others, and involving in a different way the users, who can be part of inter-subjective relationships directed to another specific subject, or nodes of the social network in which the communicative forms are substantiated in the uploading of multimedia contents directed to an indeterminate number of users or followers.*



## L'EVOLUZIONE APPLICATIVA DELLA DIFFAMAZIONE VIA E-MAIL NELL'ERA DELLO SMART-WORKING

*Corte di Cassazione; sezione V penale; sentenza 8 aprile 2021, n. 13252**commento di Pierluigi Zarrà*

**Sommario:** 1. Il casus decisis. – 2. Il delitto di diffamazione e la configgente relazione con l'ingiuria: il discrimen dell'assenza della vittima. – 3. Prerogative essenziali per la configurazione del delitto di diffamazione: il riferimento colloquiale implicito all'interessato e la riconoscibilità logico-deduttiva del diffamato. – 4. La comunicazione con più persone e la divulgazione delle frasi denigratorie per mail: la diffamazione via web nell'era Covid-19. – 5. "Da remoto" ed "in presenza": le modalità di realizzazione dell'offesa. Spunti riflessivi conseguenti alla pandemia.

Il presente contributo si sofferma sulla penale responsabilità a titolo di diffamazione, ascrivibile in capo a chi condivide una conversazione privata con contenuti diffamatori, inoltrando per e-mail tale discussione a soggetti terzi – nello specifico dieci persone – in una mailing list in cui era presente la stessa persona offesa, indicando le generalità di quest'ultimo. In considerazione di ciò, si giunge a tale assunto: se l'espressione offensiva è proferita nel corso di una riunione da remoto, in cui sono collegate più persone, alla quale partecipa l'offeso, ricorrerà l'ipotesi depenalizzata dell'ingiuria; talora gli epiteti offensivi siano contenuti in una comunicazione scritta, rivolta all'offeso ed ad altri destinatari non presenti, contestualmente al momento in cui è proferita l'offesa, ricorrono i presupposti costitutivi per il delitto di diffamazione.

*This contribution focuses on the criminal liability for defamation, ascribable to those who share a private conversation with defamatory contents, forwarding by e-mail such discussion to third parties – specifically ten people – in a mailing list in which the offended person was present, indicating the personal details of the latter. In view of this, we arrive at this assumption: if the offensive expression is uttered during a remote meeting, in which several people are connected, in which the offended person participates, the decriminalized hypothesis of insult will occur. If the offensive epithets are contained in a written communication, addressed to the offended party and to other recipients who are not present, at the same time as the offence is uttered, the conditions for the crime of defamation are met.*

## SEQUESTRO PROBATORIO DEL REPERTO DIGITALE E MANIFESTAZIONI DISTORSIVE DELL'ATTIVITÀ DI INDAGINE

*Corte di Cassazione; sezione VI penale; sentenza 19 marzo 2021, n. 10815**commento di Vincenzo Gramuglia*

**Sommario:** 1. Premessa. – 2. La vicenda. – 3. L'oggetto del sequestro probatorio di dati e sistemi informatici. – 4. Restituzione del dispositivo e impugnabilità del provvedimento di sequestro. – 5. L'utilizzo abusivo del sequestro probatorio per scopi di natura meramente "esplorativa". – 6. La dimensione trasversale del principio di proporzionalità. – 6.1. segue: ... e la sua influenza sul contenuto della motivazione del provvedimento di sequestro. – 7 Note conclusive.

Con la pronuncia in commento, la Corte di cassazione è tornata sul tema del sequestro probatorio di dati e sistemi informatici. A fronte di un utilizzo "esplorativo" dello strumento di ablazione, contrastante con la *ratio* dell'istituto, la Corte ha rimarcato l'importanza di assicurare la proporzionalità del provvedimento attraverso l'adempimento di un rigoroso onere di motivazione.

*This paper aims to analyze one of the last judgments of the Supreme Court of Cassation concerning the evidence seizure of computer systems and digital evidence. This specific case, dealing with an "exploratory" use of the instrument of ablation, is considering by the judges in contrast with the ratio of the institution and it was the occasion for the Supreme Court to underline the importance to make seizure order complying with the principle of proportionality by the fulfillment of a strict burden of motivation.*

## ADESCAMENTO DI MINORI IN RETE E PRINCIPIO DI OFFENSIVITÀ. L'ELEMENTO DEL "PERICOLO CONCRETO" E L'INDISTINTO CONFINE CON IL TENTATIVO DEI REATI-FINE

*Corte di Cassazione; sezione III penale; sentenza 9 febbraio 2021, n. 5039**commento di Luca D'Agostino*

**Sommario:** 1. Il caso sottoposto all'attenzione della Corte – 2. Il reato di adescamento di minorenni – 3. La natura di pericolo concreto del reato di adescamento di minorenni e il rapporto con il tentativo dei reati fine – 4. Considerazioni conclusive.

Il contributo riflette sulla configurazione del delitto di adescamento di minorenni come reato di pericolo concreto, soffermandosi in particolare sul rapporto tra la condotta descritta dall'art. 609-undecies c.p. e il tentativo dei reati fine. Dopo aver evidenziato alcuni passaggi critici nell'argomentazione della sentenza annotata, l'Autore sostiene che la questione relativa alla violazione del principio di offensività dovrebbe essere esaminata con maggiore attenzione, considerando i limiti esegetici a una lettura del dolo specifico in termini oggettivi.

*The essay deals with the criminal offence of "solicitation of children for sexual purposes" (Article 609-undecies of Italian Criminal Code) focusing on the nature of such crime and its relationship with the attempt of committing sexual exploitation or crimes related to child pornography. After highlighting the most critical issues argued by Italian Supreme Court, the Author suggests that the Court should consider carefully the principle of offensiveness, because the specific intent required by Art. 609-undecies is not able to give evidence that the victim has been somehow endangered.*

## AMMINISTRATIVA

START-UP INNOVATIVE NON COSTITUITE CON ATTO PUBBLICO: QUALI EFFETTI DOPO LA SENTENZA N. 2643 DEL 2021 DEL CONSIGLIO DI STATO?

*Consiglio di Stato; sezione VI; sentenza 29 marzo 2021, n. 2643*

*commento di Antonino Mazza Labocchetta*

**Sommario:** 1. Il caso. – 2. Il quadro normativo. – 3. Il decreto ministeriale del 17 febbraio 2016: attuativo o “innovativo” della fonte primaria? – 4. Le perplessità suscitate dalla sentenza del Consiglio di Stato. – 5. Il controllo del notaio previsto dall’art. 25 del C.A.D. – 6. I riflessi della sentenza n. 2443 del 2021 del Consiglio di Stato sulle startup già costituite. – 6.1. Perdita dei requisiti di start-up innovativa. – 6.2. L’art. 39-septies del d.l. n. 77 del 2021: è sanatoria? – 7. Considerazioni conclusive.

Il lavoro si propone di evidenziare che, contrariamente a quanto ritenuto dal Consiglio di Stato, è vero che il controllo effettuato in sede di registrazione non interviene, come previsto dalle direttive (UE) 2009/101 e 2017/1132, «all’atto della costituzione» e, quindi, in un momento *preventivo*, ma è anche vero che l’ottica nella quale il legislatore, con l’art. 4, comma 10-bis, del d.l. n. 3 del 2015, si è mosso è quella di favorire, in via derogatoria rispetto all’art. 2463 c.c., la nascita delle start-up innovative attraverso l’introduzione di una modalità di costituzione alternativa rispetto a quella ordinaria, e più snella. L’ipotesi derogatoria, introdotta dal legislatore, giustifica l’eliminazione del controllo preventivo notarile e il suo spostamento nella fase della registrazione della società. Il lavoro esamina, inoltre, gli effetti derivanti dalla sentenza sulle start-up non costituite nella forma dell’atto pubblico. Al fine di evitare la nullità degli atti costitutivi e degli statuti, è intervenuto il legislatore con l’art. 39-septies del d.l. n. 77 del 2021 che, confermando la validità delle start-up costituite in via telematica, sembra dare all’art. 2, comma 2, del decreto ministeriale 17 febbraio 2016 una lettura conforme alle direttive.

*The work aims to highlight that, contrary to what the Council of State believed, it is true that the control carried out during registration does not intervene, as required by Directive (EU) 2009/101 and 2017/1132, «at the time of constitution» and, therefore, in a preventive moment, but it is also true that the perspective in which the legislator, with art. 4, paragraph 10-bis, of the legislative decree no. 3 of 2015, the move was to favor, by way of derogation from art. 2463 of the Italian Civil Code, the birth of innovative start-ups through the introduction of an alternative and more streamlined method of incorporation than the ordinary one. The derogation hypothesis, introduced by the legislator, justifies the elimination of the notarial preventive control and its displacement in the registration phase of the company. The work also examines the effects deriving from the ruling on start-ups not established in the form of a public deed. In order to avoid the nullity of the articles of association and statutes, the legislator intervened with art. 39-septies of the legislative decree no. 77 of 2021 which, confirming the validity of start-ups established electronically, seems to give art. 2, paragraph 2, of the ministerial decree of 17 February 2016, a reading in compliance with the directives.*

I LIMITI ALLA DOCUMENTAZIONE SUSCETTIBILE DI OSTENSIONE. LA FINE DEL GIORNALISMO INVESTIGATIVO?

*T.a.r. Lazio; sezione III; sentenza 18 giugno 2021, n. 7333*

*commento di Rossella Bucca e Vincenzo Colarocco*

**Sommario:** 1. Il caso di specie. – 2. Dall’accesso classico all’accesso civico generalizzato: un percorso guidato dal faro della “trasparenza”. – 3. L’accesso civico generalizzato. – 4. L’accesso documentale. – 5. Punti di contatto e differenze con il diritto di accesso dell’interessato di cui all’articolo 15 del Regolamento UE 2016/679. – 6. I limiti all’ostensione documentale in rapporto all’attività giornalistica. – 7. Conclusioni.

Con la sentenza in commento i Giudici del Tribunale Amministrativo Regionale per il Lazio si pronunciano in merito alla questione afferente alla delimitazione della documentazione suscettibile di ostensione, affermando che anche l’attività preparatoria di acquisizione e raccolta delle informazioni per la realizzazione di un servizio giornalistico può costituire oggetto di ostensione quando rappresenti mezzo utile per la difesa di un interesse giuridicamente rilevante. Il presente contributo offre una disamina sui presupposti di ammissibilità dell’accesso civico e documentale con un focus sui limiti alla documentazione oggetto di ostensione nell’ambito dell’attività giornalistica.

*With the judgement in question, the Judges of the Regional Administrative Court for Lazio rule on the question relating to the delimitation of the documentation susceptible to display, stating that the preparatory activity of acquiring and collecting information for the realization of a journalistic service can also be object of ostension when it represents a useful means for the defense of a legally relevant interest. This contribution is intended to provide a general overview of the eligibility conditions for civic and documentary access with a focus on the limits to the documentation object of ostension in the context of journalistic job.*



## PRASSI

## LA VALUTAZIONE DEGLI INDIRIZZI INTERNET PROTOCOL (IP)

di Roberto Moro Visconti

**Sommario:** 1. Gli indirizzi IP. – 2. Da IPv4 a IPv6. – 3. Profili di valutazione. – 3.1. La valutazione dei beni immateriali. – 3.1.1. Approccio del costo. – 3.1.2. Approccio reddituale/finanziario. – 3.1.3. Approccio di mercato. – 3.2. La valutazione degli indirizzi IP.

Un indirizzo IP (*Internet Protocol*) è una sequenza di numeri o di caratteri alfabetici che permette di individuare anche geograficamente un elaboratore connesso in rete, indispensabile sia per ricevere sia per inviare dati; il protocollo IP regola l'interconnessione tra reti. Secondo la versione IPv4, l'indirizzo IP di ogni calcolatore è costituito da 32 bit e permette l'indirizzamento di circa 4 miliardi (2<sup>32</sup>) di elaboratori. La crescita delle dimensioni di Internet ha reso però insufficiente questo numero ed è stata così definita una nuova versione, IPv6, che aumenta la lunghezza dell'indirizzo a 128 bit. La valutazione degli indirizzi IPv4, in fase di esaurimento, si basa essenzialmente su un valore di mercato desumibile da aste condotte su piattaforme digitali.

*An IP (Internet Protocol) address is a sequence of numbers or alphabetic characters that allows a computer connected to the network to be identified geographically, which is essential for both receiving and sending data; the IP protocol regulates the interconnection between networks. According to the IPv4 version, each computer's IP address is made up of 32 bits and allows the addressing of about 4 billion (2<sup>32</sup>) computers. The growth in the size of the Internet, however, has made this number insufficient and a new version, IPv6, has been defined, which increases the length of the address to 128 bits. The valuation approach of IPv4 addresses, which are currently being exhausted, is essentially based on a market value that can be inferred from auctions conducted on digital platforms.*

## CATENA DI CUSTODIA, PROVA DIGITALE E TECNOLOGIA BLOCK-CHAIN

di Giulio Soana

**Sommario:** 1. Introduzione. – 2. Volatilità, modificabilità e transnazionalità. Le chiavi di volta del rischio digitale. – 3. Catena di custodia e prova digitale. Un binomio necessario. – 4. La legge 48/2008 di attuazione della Convenzione di Budapest – 5. Block-chain e RegTech. Un'introduzione. 6. Il caso di studio: block-chain per la catena di custodia. – 7. Ricadute processuali ed extraprocessuali. – 8. La Hangzhou Judicial Block-chain Platform. – 9. Conclusione.

Le peculiari caratteristiche della prova digitale ed il suo pervasivo utilizzo per l'accertamento penale richiedono l'impiego di nuove tecniche che permettano di garantirne l'integrità e comprensibilità per gli attori processuali; in particolare, la catena di custodia, elemento cruciale per garantire la correttezza metodologica della prova scientifica, può giocare un ruolo centrale in questo sforzo. Tale aggiornamento delle tecniche forensi è oltretutto legislativamente demandato a seguito dell'introduzione della l. 48/2008. In quest'ottica, la tecnologia block-chain può essere implementata quale strumento di registrazione e conservazione della catena di custodia; l'attitudine di tale tecnologia a questo scopo è stata d'altro canto già dimostrata dalla sua prima adozione da parte dell'Hangzhou Internet Court in Cina. Il presente contributo analizza, da una prospettiva prettamente giuridica, le potenzialità di una tale implementazione nell'ordinamento italiano.

*The characteristics of the digital evidence and its pervasive use as means to establish criminal responsibility call for new techniques to guarantee its integrity and comprehensibility for the parties; the chain of custody plays a crucial role in guaranteeing the methodological soundness of the scientific evidence, and can, therefore, be a fundamental piece in this effort. This update of the techniques is law-mandated following the introduction of the l. 48/2008. Within this framework, block-chain can be implemented as a means to register and store the chain of custody; the aptness of this technology is, furthermore, witnessed by its adoption by the Hangzhou Internet Court in China. The article analyses, from a legal perspective, the risk and opportunities of this implementation within the Italian legal system.*

## LE LINEE GUIDA DEL GARANTE PER LA PROTEZIONE DEI DATI E DELL'AUTORITÀ NAZIONALE ANTICORRUZIONE IN TEMA DI BILANCIAMENTO FRA PRIVACY E TRASPARENZA

di Alice Incerti

**Sommario:** 1. Privacy e trasparenza amministrativa: due discipline complementari. – 2. Le prime linee guida del Garante per la protezione dei dati personali e dell'Autorità Nazionale Anticorruzione in materia di trattamento di dati personali, contenuti in atti e documenti amministrativi, effettuato per finalità di pubblicità e di trasparenza sul web da soggetti pubblici e sull'attuazione degli obblighi di pubblicità contenute nel Codice della trasparenza. – 3. Riflessioni conclusive.

A seguito dell'introduzione del Codice della trasparenza, il Garante per la protezione dei dati personali e l'Autorità Nazionale Anticorruzione sono intervenuti con apposite linee guida al fine di operare l'arduo bilanciamento fra il diritto alla privacy e il principio della trasparenza amministrativa.

*Following the introduction of the Transparency Code, the Data Protection Authority and the National Anti-Corruption Authority intervened with specific guidelines in order to carry out a difficult balance between the right to privacy and the principle of administrative transparency.*