

SOMMARIO

SAGGI

IL “DIGITAL OMNIBUS”: SEMPLIFICAZIONE (O DEREGOLAMENTAZIONE) DEL CONTESTO DIGITALE EUROPEO?

di Enzo Maria Tripodi

3

Il 19 novembre 2025 la Commissione europea ha pubblicato la proposta di regolamento sulla semplificazione dell'*acquis* digitale europeo (c.d. “Digital Omnibus”) che costituisce uno strumento che racchiude modifiche tecniche alla legislazione digitale dell’Unione Europea. La legislazione digitale, infatti, secondo quanto argomentato nella proposta stessa, appare frammentata, con duplicazioni e complessità amministrativa. L’obiettivo dichiarato, pertanto, è quello di ridurre la complessità, armonizzare le disposizioni non allineate e alleggerire i costi di conformità per imprese, amministrazioni pubbliche e cittadini. Il *Digital Omnibus* riguarda, in particolare, il GDPR e la Direttiva *ePrivacy*; il regime della circolazione e sfruttamento dei dati; l’introduzione di un meccanismo unico di notifica degli incidenti sulla sicurezza; l’abrogazione del Regolamento P2B sulla trasparenza delle piattaforme online. A seguito dell’operazione di “consolidamento” vengono conseguentemente abrogati il Regolamento (UE) 2018/1807 (*Free Flow of Non-Personal Data*), il Regolamento (UE) 2019/1150 (P2B), superato dal *Digital Services Act* (DSA) e dal *Digital Markets Act* (DMA), il Regolamento (UE) 2022/868 (*Data Governance Act*), assorbito nel *Data Act* e la Direttiva (UE) 2019/1024 (*Open Data Directive*), trasposta nel citato *Data Act*. Il “pacchetto” di modifiche comprende anche un provvedimento specifico per l’IA (il *Digital Omnibus on IA*) che propone una revisione al Regolamento sull’IA di recente emanato dall’Unione europea e non ancora entrato in vigore in tutte le sue previsioni. La proposta prevede, tra l’altro: a) la proroga – in attesa dell’adozione dei necessari standard tecnici – dei termini di attuazione per i sistemi ad alto rischio (la decorrenza degli obblighi per i sistemi di IA, di cui all’All. III, sarà posticipata al 2 dicembre 2027. Per i sistemi di IA ad alto rischio, di cui all’All. I, l’applicazione è rinviata al 2 agosto 2028; b) l’armonizzazione della classificazione dei rischi (rispetto, ad esempio, al trattamento dei set di dati di addestramento, ai requisiti di qualità dei dati, ai controlli sui bias); c) la facoltatività e non più l’obbligo della formazione interna (tranne per chi utilizza sistemi ad alto rischio) con l’invito agli Stati membri ad incoraggiare le aziende a qualificare volontariamente i propri dipendenti in materia di IA; d) la riduzione degli obblighi di documentazione di gestione della qualità per le *Small Mid-Cap Enterprises* che vengono parificate alla PMI. Una valutazione del quadro complessivo delle modifiche proposte non è agevole poiché, accanto ad operazioni di “accorpamento” ragionato delle disposizioni (è il caso del *Data Act*), in altri casi la “semplificazione”, in realtà, modifica gli stessi concetti di riferimento, finendo per incidere sul livello della tutela (come nel caso delle modifiche al GDPR), oppure si presta ad una lettura politica in cui l’Unione europea smantella alcuni capisaldi regolamentari (come per l’AI Act), a tutto vantaggio delle *Big Tech* nordamericane, nonostante – a parole – dichiari di favorire le imprese europee.

On 19 November 2025, the European Commission published its proposal for a regulation on the simplification of the European digital *acquis* (the so-called “Digital Omnibus”), which is an instrument that contains technical amendments to European Union digital legislation. Indeed, digital legislation, as stated in the proposal itself, appears fragmented, with duplications and administrative complexity. The stated objective, therefore, is to reduce complexity, harmonize disaligned provisions, and reduce compliance costs for businesses, public administrations, and citizens. The *Digital Omnibus* focuses, in particular, on the GDPR and the *ePrivacy Directive*; the regime for data circulation and exploitation; the introduction of a single security incident notification mechanism; and the repeal of the P2B Regulation on transparency of online platforms. Following the “consolidation” operation, Regulation (EU) 2018/1807 (*Free Flow of Non-Personal Data*), Regulation (EU) 2019/1150 (P2B), superseded by the *Digital Services Act* (DSA) and the *Digital Markets Act* (DMA), Regulation (EU) 2022/868 (*Data Governance Act*), absorbed into the *Data Act* and Directive (EU) 2019/1024 (*Open Data Directive*), transposed into the aforementioned *Data Act*, are consequently repealed. The package of amendments also includes a specific provision for AI (the *Digital Omnibus on IA*) which proposes a revision to the AI Regulation recently enacted by the European Union, which has not yet entered into force in all its provisions. The proposal includes, among other things: a) the extension – pending the adoption of the necessary technical standards – of the implementation deadlines for high-risk systems (the start date of the obligations for AI systems, referred to in Annex III, will be postponed to 2 December 2027. For high-risk AI systems, referred to in Annex I, application is postponed to 2 August 2028); b) the harmonization of risk classification (with respect, for example, to the processing of training datasets, data quality requirements, and bias checks); c) the optional nature of internal training (except for those using high-risk systems) with an invitation to Member States to encourage companies to voluntarily qualify their employees in AI; d) the reduction of quality management documentation requirements for *Small Mid-Cap Enterprises*, which are treated as SMEs. An overall assessment of the proposed changes is not easy. In addition to thoughtful “consolidation” of provisions (as in the case of the *Data Act*), in other cases the “simplification” actually modifies the underlying concepts, ultimately impacting the level of protection (as in the case of the changes to the GDPR). Or it lends itself to a political interpretation in which the European Union dismantles certain regulatory cornerstones (as with the AI Act), to the advantage of North American *Big Tech*, despite claiming to favor European companies.

AMBITO DI APPLICAZIONE E PRINCIPI GENERALI DELLA LEGGE 23 SETTEMBRE 2025, N. 132, RECANTE “DISPOSIZIONI IN MATERIA DI INTELLIGENZA ARTIFICIALE”

di Fortunato Costantino

17

Il contributo propone un’analisi sistematica delle disposizioni di apertura della legge 23 settembre 2025, n. 132, recante “Disposizioni in materia di intelligenza artificiale”, esaminandone il ruolo all’interno del più ampio quadro giuridico europeo in materia di regolazione dell’IA. Attraverso l’analisi delle finalità, dell’ambito di applicazione, delle definizioni e dei principi generali, l’articolo

ricostruisce la funzione strutturante dei primi tre articoli quali clausole di sistema, idonee a orientare l'interpretazione e l'attuazione della disciplina. L'indagine mette in luce le principali implicazioni applicative e le criticità potenziali di una normativa chiamata a operare in un contesto tecnologico caratterizzato da elevata dinamicità, nonché le tensioni emergenti tra esigenze di certezza del diritto, tutela dei diritti fondamentali e promozione dell'innovazione. I rilievi conclusivi sono dedicati alla valutazione del possibile impatto del c.d. Digital Omnibus, il pacchetto legislativo presentato dalla Commissione europea il 19 novembre 2025, considerato quale fattore di possibile ridefinizione degli assetti regolatori digitali dell'Unione, e delle potenziali ricadute sulla legge n. 132/2025, concepita come norma di raccordo e integrazione nel sistema europeo multilivello della governance dell'intelligenza artificiale.

This article offers a systematic analysis of the opening provisions of Law No. 132 of 23 September 2025 on artificial intelligence, examining their role within the broader European legal framework governing AI. By focusing on the law's objectives, scope of application, definitions and general principles, the contribution reconstructs the structural function of the first three articles as system-setting clauses capable of guiding interpretation and enforcement. The analysis highlights the practical implications and potential criticalities of a national AI regime designed to operate in a rapidly evolving technological environment, as well as the emerging tensions between legal certainty, fundamental rights protection and innovation-oriented regulation. The concluding section assesses the potential impact of the Digital Omnibus legislative package presented by the European Commission on 19 November 2025, considering its capacity to reshape EU digital regulatory arrangements and its direct and indirect effects on Law No. 132/2025, conceived as a coordinating and integrative instrument within the EU's multilayered system of artificial intelligence governance.

LA RESPONSABILITÀ GENITORIALE NELLA COMPLESSITÀ DELL'ECOSISTEMA DIGITALE. RIFLESSIONI ALLA LUCE DELLA LEGGE N. 132/2025 SULL'INTELLIGENZA ARTIFICIALE

di Ilaria Garaci

35

Il contributo esamina il ruolo degli esercenti la responsabilità genitoriale nella prevenzione dei rischi sistemici legati all'uso degli strumenti digitali da parte dei minori, nell'ambito di un contesto tecnologico profondamente trasformato dallo sviluppo dei sistemi di intelligenza artificiale c.d. generativa. L'analisi, in particolare, esplora il modo in cui si concretizzano i doveri genitoriali di protezione e di cura alla luce dell'attuale quadro giuridico (con specifico riferimento alla legge n. 132 del 2025 sull'intelligenza artificiale), tenendo conto della difficoltà di conciliare le esigenze di protezione di soggetti vulnerabili quali sono i minori di età, con il loro diritto all'autodeterminazione nel contesto digitale.

This paper examines the role of those exercising parental responsibility in preventing systemic risks associated with the use of IT tools by minors, in a technological context that has been profoundly transformed by the development of so-called generative artificial intelligence systems. In particular, the analysis explores how parental duties of protection and care are fulfilled in light of the current legal framework (with specific reference to Law No. 132 of 2025 on artificial intelligence), taking into account the difficulty of reconciling the need to protect vulnerable individuals, such as minors, with their right to self-determination in the digital context.

RES LOQUENTES E ANDROIDI: DAL SERVO ROMANO AGLI SCHIAVI ROBOT DEL XXI SECOLO. PROSPETTIVE GIURIDICHE E FILOSOFICHE, TRA DIRITTO ROMANO E ARTIFICIAL INTELLIGENCE ACT DELLA UE.

di Alessandro del Ninno

45

La Roma antica inquadrava lo schiavo come *res loquens*: pur essendo persona fisica, il servo non aveva capacità giuridica autonoma. Soggetto alla dominica potestas del padrone – esercitata su di lui come su un oggetto – lo schiavo poteva amministrare un *peculium*, ma ogni contratto o illecito ricadeva in capo al dominus. Strumenti come la *manumissio* (liberazione formale) e l'*actio noxalis* (responsabilità del padrone per le azioni del servo) regolavano formalmente lo status, senza però mai attribuire al servo alcuna soggettività giuridica: in sostanza era un essere umano trattato come cosa. Analogamente, il Regolamento (UE) 2024/1689 (AI Act) definisce i sistemi di intelligenza artificiale come entità automatizzate che producono output – contenuti, previsioni, decisioni, raccomandazioni – capaci di influenzare gli ambienti fisici o virtuali. Tuttavia, analogamente allo schiavo romano, anche gli androidi intelligenti – sempre più vicini a passare dai laboratori di sperimentazione ai mercati e alle case degli esseri umani – rimangono giuridicamente *res*: strumenti o prodotti tecnologici soggetti a obblighi di sicurezza piuttosto che soggetti di diritto autonomi. Se è vero che in sede europea si è persino ipotizzato di elevare robot e IA a “persone elettroniche”, il quadro normativo vigente resta profondamente antropocentrico. In effetti, come rileva la dottrina moderna, gli ordinamenti occidentali considerano ancora l'uomo «fulcro della società», relegando le entità non umane a oggetti di tutela e controllo (ad es. attraverso rigorose certificazioni e responsabilità dei fornitori). L'AI Act attuale prosegue – in un certo senso – il percorso iniziato dal diritto romano: definisce con precisione obblighi e rischi per chi produce o impiega IA avanzate, ma non scalfisce il paradigma che concepisce l'androide intelligente come bene da governare, più che come soggetto con diritti. Questo parallelismo storico-giuridico illumina profili condivisi: entrambi i sistemi – antico e moderno – riflettono un approccio giuridico antropocentrico, in base al quale solo l'essere umano è titolare effettivo di diritti, mentre gli altri “parlanti” sono visti come *res* con diritti mediati dai dominus/deployer. L'obiettivo comparatistico e critico del saggio è proprio far emergere queste analogie: mettere a confronto norme e istituti antichi e moderni (*res loquens* verso sistemi IA, dominica potestas verso obblighi di governance dell'IA, *peculium* verso risorse algoritmiche, *manumissio* verso meccanismi di disabilitazione, ecc.) per riflettere su come giuridicamente sia stata gestita nel tempo la soggettività di entità intelligenti non umane (o non considerate umane) e quali sono le prospettive regolatorie, filosofiche e sociali che ci attendono.

Ancient Rome framed the servus as a res loquens: although a human being in physical terms, the slave lacked any autonomous legal capacity. Subject to the dominica potestas of the master—exercised over him as over an object—the slave could administer a peculium, yet every contract or delict was ultimately attributable to the dominus. Instruments such as manumissio (formal liberation) and actio noxalis (the master's liability for the slave's wrongful acts) formally regulated the status of servitude, without ever recognizing to the slave any genuine legal subjectivity: in substance,

he was a human being treated as a thing. Analogously, Regulation (EU) 2024/1689 (AI Act) defines artificial intelligence systems as automated entities generating outputs—content, predictions, decisions, recommendations—capable of influencing physical or virtual environments. However, much like the Roman slave, intelligent androids—now approaching the transition from research laboratories to human markets and households—remain in law *res*: technological instruments or products subject to safety obligations rather than autonomous subjects of rights. Even though the European debate has at times contemplated the notion of granting robots and AI systems the status of “electronic persons,” the prevailing regulatory framework remains profoundly anthropocentric. As modern legal doctrine observes, Western legal systems still consider man the “axis of society,” relegating non-human entities to the realm of objects of regulation and control (for instance, through strict certification regimes and provider liability). In this sense, the current *AI Act* continues the trajectory initiated by Roman law: it precisely defines duties and risks for those who produce or deploy advanced AI, yet it does not disturb the paradigm that conceives the intelligent android as a good to be governed, rather than as a holder of rights. This historical-legal parallel highlights shared structural profiles: both the ancient and the modern systems reflect an anthropocentric legal approach under which only the human being is a genuine right holder, while other “speaking entities” are regarded as *res* endowed with derivative rights mediated by their respective dominus or deployer. The comparative and critical purpose of this essay is precisely to unveil these analogies: to juxtapose ancient and modern legal constructs (*res loquens* vs. AI systems, *dominica potestas* vs. AI governance obligations, *peculium* vs. algorithmic resources, *manumissio* vs. deactivation mechanisms, etc.) so as to reflect on how legal systems have historically managed the subjectivity of intelligent non-human (or non-recognized human) entities, and to explore the regulatory, philosophical, and societal perspectives that lie ahead.

I NUOVI BENI IMMATERIALI DIGITALI ALLA LUCE DEL DIRITTO PRIVATO EUROPEO: IL CASO DEI DATI PERSONALI

di Giovanni Maria Tosi

61

Lo studio affronta il tema dei nuovi beni digitali alla luce della recente normativa europea sui contratti di fornitura di contenuti digitali e servizi digitali, comprese le informazioni e i dati personali, valorizzando la licenza d'uso come modello contrattuale atipico. Lo sviluppo di nuovi beni digitali dovuto al progresso tecnologico e alla frammentazione del quadro normativo può essere ricondotto a unità costruendo una tassonomia dei nuovi beni immateriali digitali che tenga conto del superamento del dogma della logica dominicale.

The study addresses the issue of new digital goods in light of the recent European regulations on contracts for the supply of digital contents and digital services, including information and personal data, emphasizing the license agreement as an atypical contractual model. The development of new digital goods due to technological progress and regulatory fragmentation can be brought to unity by constructing a taxonomy of new digital intangible goods that takes into account the overcoming of the dogma of dominical logic.

LEGGE 89/2025: LO SPAZIO DEI PRIVATI. PROFILI DI RESPONSABILITÀ CIVILE

di Ivan Fino

71

Il contributo ricostruisce la L. 89/2025 quale esito della crescente centralità dei rapporti tra privati nello spazio. Il Titolo IV appronta, per i danni arrecati a terzi sulla superficie terrestre e agli aeromobili in volo, una responsabilità a titolo oggettivo, con esimenti tassative e applicazione dell'art. 1227 c.c. Per gli eventi lesivi cagionati nello spazio, l'inquadramento dell'imputazione resta rimesso alle categorie codicistiche, aprendo alla sussunzione delle attività spaziali nell'alveo dell'art. 2050 c.c. In questo quadro, sul piano interno, il massimale di copertura previsto potrebbe determinare, in assenza di garanzie pubbliche, una possibile insufficienza soddisfattoria ove il danno ecceda la soglia; tensione che, insieme ad asimmetrie rispetto alle soluzioni accolte in altri ordinamenti e alla non più differibile adozione di decreti attuativi idonei a graduare obblighi e coperture per classi di rischio, costituisce uno dei principali profili problematici della disciplina.

The article reconstructs Law No. 89/2025 as the outcome of the growing centrality of private-law relations in outer space. Title IV establishes, for damage caused to third parties on the Earth's surface, a strict-liability regime, with exhaustively listed defences and the application of Article 1227 of the Italian Civil Code. For harmful events occurring in outer space, the framework instead refers back to the Civil Code categories, opening the way to subsuming space activities under Article 2050 (hazardous activities). Against this background, the statutory insurance cap may, in the absence of public guarantees, result in a potential shortfall in compensation where the damage exceeds the threshold; this tension—together with misalignments vis-à-vis other legal systems and the need for implementing decrees capable of calibrating obligations and coverage by risk classes—constitutes one of the main problematic aspects of the regime.

GIURISPRUDENZA

EUROPEA

NATURA PERSONALE DEI DATI PSEUDONIMIZZATI: LA CGUE RIBADISCE CHE VA VALUTATA IN RELAZIONE AL SINGOLO CASO

Corte di Giustizia Ue; sezione prima; sentenza 4 settembre 2025, causa C-413/23 P

commento di Giovanni Polimeni

87

93

Il presente contributo prende in esame un'importante pronuncia della Corte di Giustizia dell'Unione europea intervenuta nell'ambito di una controversia sorta tra il Comitato Unico di Risoluzione e il Garante Europeo per la Protezione dei Dati personali ri-

guardo la trasmissione dei dati raccolti presso gli interessati a un soggetto terzo non indicato nell'informativa. Sul tema dei requisiti previsti dall'art. 3 del Regolamento 2018/1725 per classificare come dato personale un'informazione, i giudici hanno chiarito che le opinioni personali riguardano necessariamente coloro che le hanno espresse. Sul requisito dell'identificabilità, i dati pseudonimizzati non vanno considerati a priori personali ma vanno valutate le circostanze di ogni singolo caso; inoltre, anche qualora per un terzo i dati pseudonimizzati non avessero natura personale, il titolare del trattamento deve adempiere al dovere di informare l'interessato dell'eventuale trasmissione dei suoi dati ad altri soggetti.

This essay ribution examines an important judgment of the Court of Justice of the European Union delivered in the context of a dispute between the Single Resolution Board and the European Data Protection Supervisor concerning the transmission of data collected from data subjects to a third party that had not been mentioned in the information notice. With regard to the requirements laid down in Article 3 of Regulation 2018/1725 for classifying information as personal data, the judges clarified that personal opinions necessarily relate to the individuals who expressed them. As for the requirement of identifiability, pseudonymised data should not be regarded as personal a priori, but the circumstances of each individual case must be assessed; moreover, even if pseudonymised data were not considered personal for a third party, the controller must still comply with the obligation to inform the data subject of any possible disclosure of his or her data to other entities.

CIVILE

DATA BREACH E FASCICOLO SANITARIO ELETTRONICO: LA CASSAZIONE INDIVIDUA IL TITOLARE DEL TRATTAMENTO.

Corte di Cassazione; sezione prima; ordinanza 15 ottobre 2025, n. 27558

commento di Sergio Perrotta

99
102

Con l'ordinanza in commento, la Corte di Cassazione affronta il tema dell'individuazione della figura del titolare del trattamento dei dati personali nell'ambito del fascicolo sanitario elettronico. La Corte riconosce la Provincia autonoma come titolare del trattamento in ragione di quanto previsto dalla normativa nazionale in tema di fascicolo sanitario elettronico, escludendo che detta qualifica debba essere attribuita, con riferimento a specifiche finalità, all'Azienda sanitaria.

In the order under examination, the Italian Supreme Court engages with the issue of the identification of the data controller within the framework of personal data processing. Relying on the national regulatory scheme governing the Electronic Health Record, the Court qualifies the Province as the data controller, thereby excluding that such status may be attributed to the Local Health Authority.

SCAMBIO DI MESSAGGI SU WHATSAPP: ACCORDO PREMATRIMONIALE?

Tribunale di Catanzaro; sezione seconda; sentenza 17 luglio 2025 n. 1620

commento di Francesco Molinaro

107
112

Lo scritto, partendo da una sentenza del Tribunale di Catanzaro che ha ritenuto valido un accordo ricavato da una chat WhatsApp – in cui il marito, in attesa del divorzio, si impegna a pagare tutto il mutuo della casa familiare in cambio della rinuncia della moglie ad ogni pretesa economica – si concentra sia sulla annosa questione della nullità dei patti prematrimoniali, sia su quella, più recente, relativa alla possibilità di considerare la piattaforma di messaggistica istantanea come un valido strumento di contrattazione tra privati.

The article, starting from a ruling by the Court of Catanzaro that upheld the validity of an agreement reached via WhatsApp chat – in which the husband, awaiting divorce, undertook to pay the entire mortgage on the family home in exchange for his wife's waiver of any financial claims – focuses both on the long-standing issue of the invalidity of prenuptial agreements and on the more recent issue of whether instant messaging platforms can be considered a valid tool for negotiations between private individuals.

RESPONSABILITÀ DEI GENITORI NELL'USO DEI SOCIAL NETWORK DA PARTE DI MINORI INCAPACI

Tribunale di Brescia; sezione prima; sentenza 4 marzo 2025, n. 879

commento di Vittoria Barone

121
122

L'autrice prende in esame la sentenza del Tribunale di Brescia n. 879/2025, con cui i genitori di una minore dichiarata incapace sono stati condannati al risarcimento dei danni derivanti dalla creazione di profili social falsi e dalla diffusione, tramite tali canali, di immagini manipolate a sfondo sessuale e di contenuti diffamatori. La decisione si colloca in un contesto giurisprudenziale di crescente attenzione verso la responsabilità genitoriale nell'era digitale e offre l'occasione per approfondire i rapporti tra norme civilistiche, disciplina penalistica e strumenti di tutela introdotti dal legislatore in materia di cyberbullismo. In particolare, l'analisi si concentra su tre direttrici principali: da un lato, l'inquadramento normativo della responsabilità dei genitori ex artt. 2047 e 2048 c.c.; dall'altro, il rilievo assunto dalle prove informatiche nei giudizi di responsabilità civile connessi a condotte online; infine, le difficoltà derivanti dal deficit di competenze digitali degli adulti e il necessario bilanciamento tra doveri di vigilanza e diritto alla riservatezza dei minori. A completare il quadro, vengono offerti alcuni spunti di diritto comparato, con riferimento alle esperienze francese, tedesca e spagnola, che consentono di collocare la pronuncia bresciana entro una prospettiva sovranazionale.

This essay examines the judgment of the Brescia Court of First Instance (No. 879/2025), which held the parents of an incapable minor liable for damages arising from the creation of fake social media profiles and the dissemination, through those profiles, of digitally manipulated sexualized images and defamatory content. The decision situates itself within a broader case law trend that increasingly addresses parental liability in the

digital age and provides an opportunity to explore the interaction between civil law provisions, criminal law offences, and the protective measures introduced by the Italian legislature in relation to cyberbullying. The analysis develops along three main lines: first, the normative framework of parental liability under Articles 2047 and 2048 of the Civil Code; second, the pivotal role played by digital evidence in civil liability cases involving online misconduct; and third, the challenges posed by parents' lack of digital competence and the need to balance duties of supervision with minors' rights to privacy. The discussion is further enriched by a comparative perspective, drawing on French, German and Spanish experiences, thereby situating the Brescia judgment within a wider transnational context.

SULLE RIPRODUZIONI INFORMATICHE DI CONTRATTI E RICEVUTE: VALIDITÀ PROBATORIA E DEGRADAZIONE A PRESUNZIONI SEMPLICI

Tribunale di Napoli Nord; sezione seconda; 25 gennaio 2025, n. 308

commento di Giulia Pomi

131

133

Il presente contributo prende in esame uno dei due snodi su cui poggia l'opposizione ad un decreto ingiuntivo da parte di una srl resasi destinataria di un servizio di accertamento dei presupposti per accedere ad alcuni bonus fiscali. In particolare, l'opposizione è proposta per invalidità delle prove attestanti l'esistenza e il quantum del credito e per conseguente infondatezza della pretesa creditoria. Infatti, l'attribuzione dell'incarico, adduce la srl opponente, non è certificata; questa inoltre disconosce i documenti forniti in fotocopia e le ricevute telematiche emesse dall'ente a cui, per effetto del servizio dell'opposto, era stata trasmessa la documentazione necessaria per i bonus. Qui si innesta il rigetto dell'opposizione all'ingiunzione, pronunciata nell'ambito di un giudizio volto ad accertare l'esistenza del credito tramite prove valide che consentono di fondare la pretesa. Conformemente alla regola generale, l'onere probatorio ricade sul convenuto che, dovendo provare l'esistenza del suo credito, opera in giudizio come attore con il relativo onere della prova. Questo onere risulta soddisfatto grazie al disconoscimento delle riproduzioni informatiche proposto dalla s.r.l., mancante dei requisiti idonei e quindi degradate a presunzioni semplici. È sulla validità probatoria attribuita ai documenti informatici dal filone giurisprudenziale orbitante intorno all'art. 2712 c.c. che l'autrice svolge le sue riflessioni, anche alla luce della disciplina del d.lgs. 7 marzo 2005, n. 82, c.d. CAD e del raccordo di questo con la disciplina codicistica.

This paper examines one of the two pivotal issues underlying the opposition to an injunction filed by a limited liability company (LLC) that had been the recipient of a service aimed at verifying the requirements for accessing certain tax incentives. In particular, the opposition was brought on the grounds of the invalidity of the evidence attesting to the existence and amount of the credit, and the consequent unfoundedness of the creditor's claim. Indeed, according to the opposing company, the assignment of the task was not duly certified; moreover, it contested both the documents submitted in photocopy and the electronic receipts issued by the institution to which, as a result of the opposing party's service, the documentation necessary for the bonuses had been transmitted. This is where the rejection of the opposition to the injunction comes into play, issued within proceedings aimed at establishing the existence of the credit through valid evidence capable of supporting the claim. In accordance with the general rule, the burden of proof lies with the defendant who, having to prove the existence of its credit, assumes the role of plaintiff in the proceedings. This burden is deemed satisfied by virtue of the objection raised by the LLC against the electronic reproductions, which lacked the necessary requirements to be reduced to mere circumstantial evidence. The Author takes a position on the evidentiary value attributed to electronic documents by the line of case law revolving around Article 2712 of the Civil Code, also considering the framework set forth by the legislative decree No. 82 of 7 March 2005, the Digital Administration Code, and its coordination with the codified provisions.

PENALE

LA MESSAGGISTICA ISTANTANEA NEL PROCEDIMENTO PENALE: EVOLUZIONE DELLA NOZIONE DI CORRISPONDENZA E GARANZIE COSTITUZIONALI

Corte di Cassazione; sezione quarta; sentenza 24 settembre 2025, n. 31878

commento di Stefano Aterno e Paola Patriarca

143

145

Le "nuove" tecnologie della comunicazione, quali la messaggistica istantanea (ad esempio, posta elettronica e WhatsApp), impongono una revisione della tradizionale nozione di "corrispondenza" nel procedimento penale, al fine di garantire un'effettiva attuazione delle garanzie costituzionali poste a tutela della sua libertà e segretezza. La riflessione muove dalla sentenza della Corte di Cassazione, 24 settembre 2025, n. 31878, che sembra aver definitivamente recepito e consolidato il principio affermato dalla Corte costituzionale con la sentenza, 27 luglio 2023, n. 170, riconoscendo dignità di "corrispondenza" alle comunicazioni intercorse tra soggetti determinati mediante i nuovi strumenti telematici, anche quando esse siano già state ricevute e lette dal destinatario. Nel presente contributo, senza alcuna pretesa di esaustività, gli Autori analizzano le modalità di acquisizione della messaggistica istantanea nel processo penale, muovendo dall'ampliamento della nozione di corrispondenza e dalle conseguenze che ne derivano, sino all'individuazione delle forme del sequestro dei dispositivi e dei supporti informatici nei quali la corrispondenza digitale è contenuta.

Communication technologies, such as instant messaging (for example, email and WhatsApp), require a reconsideration of the traditional notion of "correspondence" in criminal procedure, in order to ensure the effective implementation of the constitutional guarantees protecting its freedom and secrecy. This analysis is prompted by Judgment no. 31878 of 2025 of the Italian Court of Cassation, which appears to have definitively embraced and consolidated the principle affirmed the previous year by the Italian Constitutional Court in Judgment no. 170 of 2023, recognising the status of "correspondence" to communications exchanged between identified parties through new telematic means, even when such communications have already been received and read by the addressee. In this contribution, the Authors examine the methods for acquiring instant messaging communi-

cations in criminal proceedings, starting from the expanded notion of correspondence and the consequences flowing therefrom, and extending to the identification of the appropriate procedures for acquiring the devices and information media in which digital correspondence is stored.

DIRITTO D'AUTORE E DOLO SPECIFICO: LA CASSAZIONE RIBADISCE L'ASSENZA DI REATO SENZA FINE DI LUCRO

Corte di Cassazione; sezione terza, sentenza 4 settembre 2025, n. 30279

commento di Olimpia Barresi

153

154

Il presente contributo esamina una recente pronuncia della Corte di Appello di Reggio Calabria che ha confermato la condanna del ricorrente per il reato di cui all'art. 171-ter della l. n. 633 del 1941, per aver trasmesso una partita di campionato di Serie A su più apparecchi televisivi all'interno di un esercizio commerciale, rendendola visibile alla clientela mediante l'utilizzo di una smart card destinata a uso domestico. La decisione si colloca in linea di continuità con i più recenti arresti giurisprudenziali in materia di tutela penale del diritto d'autore e si sofferma, in particolare, sull'interpretazione della fattispecie incriminatrice, con particolare riferimento all'elemento soggettivo del dolo specifico. La pronuncia in commento si inserisce, inoltre, in un più ampio contesto sistematico, nel quale il diritto penale è chiamato a confrontarsi con la persistente presenza di fattispecie inadeguate, che impongono oggi una rilettura restrittiva e orientata al principio di offensività, al fine di delimitare l'area della rilevanza penale e prevenire indebite estensioni dell'intervento punitivo.

This contribution examines a recent ruling by the Court of Appeal of Reggio Calabria, which upheld the conviction of the appellant for the offense under Article 171-ter of Law No. 633 of 1941, for broadcasting a Serie A football match on multiple television sets within a commercial establishment, making it visible to customers through the use of a smart card intended for domestic use. The decision is consistent with recent case law on the criminal protection of copyright and focuses, in particular, on the interpretation of incriminated conduct, with special attention to the subjective element of specific intent. The ruling under discussion also fits within a broader systemic context, in which criminal law must contend with the persistent presence of inadequate statutory provisions, which today require restrictive reading guided by the principle of offensiveness, in order to delineate the scope of criminal liability and prevent undue expansions of punitive intervention.

REVENGE PORN E PIATTAFORME DIGITALI: ESTENSIONE DELLA TUTELA PENALE NEI RAPPORTI CONTRATTUALI TRA CREATOR E FAN

Corte di Cassazione; sezione quinta; ordinanza, 2 settembre 2025, n. 30169

commento di Riccardo Lanzo

163

166

Il presente contributo prende in esame l'Ordinanza n. 30169 del 2 settembre 2025 (ud. 12 giugno 2025) della Corte di Cassazione, Sezione V Penale, proponendosi di analizzare l'art. 612-ter c.p. nel peculiare contesto della Piattaforma di contenuti per adulti OnlyFans. La Suprema Corte estende il concetto di "contenuti privati" alle foto e ai video condivisi a pagamento con i Fan e stabilisce una sorta di "automatismo" tra la violazione degli obblighi contrattuali (es. screen recording) e la lesione della sfera privata tutelata dalla norma incriminatrice. Il consenso del Creator, inoltre, deve considerarsi limitato alla mera visualizzazione del singolo utente: la successiva diffusione a terzi configura il difetto di consenso richiesto per l'integrazione del delitto de quo. La pronuncia, dunque, rafforza in modo significativo la tutela della libertà di autodeterminazione sessuale, affermando che la dimensione economica del contenuto non affievolisce la protezione del bene giuridico. L'Ordinanza conferma, dunque, la capacità della norma di presidiare anche i nuovi contesti digitali e contrattuali, nonostante il legislatore del 2019 abbia pensato l'art. 612-ter c.p. come strumento di tutela contro le condotte di "revenge porn".

This article examines Decision no. 30169 of September 2, 2025 (hearing of June 12, 2025) issued by the Italian Supreme Court with the aim of analyzing article 612-ter of the Italian Criminal Code within the specific context of the adult content platform OnlyFans. The Court extends the concept of "private content" to encompass videos and photos shared for a fee with Subscribers/Fans, thereby establishing a form of automatic connection between the breach of contractual obligations (e.g., unauthorized screen recording) and the violation of the private sphere. Furthermore, the Creator's consent must be deemed limited solely to the individual user's viewing: the subsequent dissemination to third parties constitutes the defect of consent required for the offense to be established. The ruling, therefore, significantly strengthens the safeguard of the freedom of sexual self-determination, asserting that the content's economic dimension does not diminish the protection afforded to the legally protected interest. The Decision confirms the provision's capacity to govern new digital and contractual environments, notwithstanding the fact that the 2019 legislature conceived article 612-ter c.p. primarily as a protective measure against "revenge porn" conduct.

AMMINISTRATIVA

ACCESSO DOCUMENTALE E INTELLIGENZA ARTIFICIALE: L'AFFERMAZIONE DELLA "RISERVA DI UMANITÀ" NELL'ERA DIGITALE

Consiglio di Stato; sezione sesta; sentenza 5 giugno 2025

commento di Filippo Lorè

171

173

Il contributo esamina la decisione assunta dal Consiglio di Stato che individua un principio di legalità secondo il quale l'accesso documentale, con conseguente estrapolazione di dati, non può essere negato per l'incapacità (e presunta impossibilità) dell'Amministrazione di identificare il processo decisionale dell'algoritmo nel definire un procedimento di erogazione di contributi (aiuti), collegati al possesso di beni patrimoniali di privati. La decisione in commento, nel respingere l'appello e nell'annotare, in caso di

ricorso all'Intelligenza Artificiale, i principi di conoscibilità e compressibilità, non esclusività e non discriminazione della decisione algoritmica, invoca l'accessibilità all'algoritmo da parte del soggetto che partecipa ad una procedura amministrativa, dove l'IA non si limita ad accelerare la decisione, bensì determina la scelta concludendo il procedimento, incidendo, in linea diretta, il destinatario dell'azione amministrativa.

This article examines the decision taken by the Council of State, which identifies a principle of legality according to which access to documents, with consequent data extraction, cannot be denied due to the Administration's inability (and presumed inability) to identify the algorithm's decision-making process in defining a procedure for the disbursement of grants (aid) linked to the ownership of private assets. The decision in question, by rejecting the appeal and noting, in the event of recourse to Artificial Intelligence, the principles of knowability and compressibility, non-exclusivity, and non-discrimination of algorithmic decision-making, invokes accessibility to the algorithm by the party participating in an administrative procedure, where AI does not merely accelerate the decision, but rather determines the choice by concluding the procedure, directly impacting the recipient of the administrative action.

IURA NOVIT IA?

T.A.R. Lombardia, Milano, sezione quinta, 21 ottobre 2025, n. 3348

commento di Eugenio Prosperetti

185

188

La sentenza del TAR Lombardia in commento interessa per la censura all'avvocato patrocinante per aver citato numerosi riferimenti di giurisprudenza risultati non corretti e inesistenti, risultati poi generati ed inventati dall'IA. Linee guida ordinistiche e specifici obblighi dell'AI Act e della nuova Legge italiana sull'IA consentono di indirizzare la questione. Il commento analizza le conseguenze in termini di responsabilità che derivano dalla violazione di tali obblighi.

The Lombardy Regional Administrative Court ruling in question is noteworthy for its criticism of the lawyer who introduced the case for citing numerous references to case law that were found to be incorrect and non-existent, which resulted having been made up by generative AI. Professional association guidelines and specific obligations under the AI Act and the new Italian law on AI provide guidance on this issue. The commentary analyzes the consequences in terms of liability arising from the violation of these obligations.

L'ACCESSO AL CODICE SORGENTE NEI CONCORSI PUBBLICI: NOTE CRITICHE A MARGINE DI UNA RECENTE PRONUNCIA DEL GIUDICE AMMINISTRATIVO

T.A.R. Sicilia, Catania, sezione prima, 1° settembre 2025, n. 2555

commento di Carla Cozzi

193

194

Il contributo esamina il tema dell'accesso al codice sorgente dei software utilizzati nelle procedure concorsuali, alla luce delle esigenze di trasparenza e di tutela difensiva dei partecipanti. L'analisi si sofferma sulla qualificazione giuridica del software impiegato dall'amministrazione e sul rapporto tra accesso e riservatezza. Ne emerge una lettura critica dei limiti opposti all'ostensibilità del codice sorgente.

The contribution examines access to the source code of software used in public recruitment procedures in light of transparency requirements and the defensive needs of candidates. It focuses on the legal qualification of administrative software and on the relationship between access rights and confidentiality. The analysis offers a critical reading of the limits commonly invoked to deny disclosure of source code.

PRASSI

ATTI DIGITALI DEGLI STATI GENERALI DEL DIRITTO DI INTERNET E DELLA INTELLIGENZA ARTIFICIALE V EDIZIONE

a cura di Giuseppe Cassano e Francesco Di Ciommo

199

