

## Intelligenza Artificiale nei rapporti di lavoro: tra regolazione e sfide future

CHIARA CICCIA ROMITO\*

SOMMARIO: 1. L'intelligenza Artificiale nel mercato del lavoro. – 2. Il problema dell'opacità algoritmica e l'esercizio del diritto di accesso e opposizione da parte del lavoratore. – 3. La Proposta di Regolamento sull'Intelligenza Artificiale: i limiti.

### 1. *L'Intelligenza Artificiale nel mercato del lavoro*

L'ingresso dell'Intelligenza Artificiale (d'ora in avanti I.A.) nel mercato del lavoro rappresenta una delle principali sfide poste dall'evoluzione tecnologica. Il rapporto di lavoro sta venendo influenzato dall'ingresso dei sistemi di I.A., che alterano i classici rapporti negoziali in esso e sollevano profonde riflessioni sullo *status* e i diritti del prestatore di lavoro.

Uno dei rischi intrinseci relativi all'I.A. nel mondo del lavoro dipende direttamente dalla natura stessa dei sistemi di I.A., soprattutto in riferimento all'utilizzo di codici algoritmici complessi, che sfruttano reti neurali strutturate, e al loro funzionamento.

Più il sistema è complesso, e quindi performante, più il sistema rischia di essere opaco e, conseguentemente, difficile da comprendere.

Questa complessità, tipica dei sistemi di *deep learning*, potrebbe impattare in maniera negativa sui principi di trasparenza e sui diritti dei lavoratori, oltre a lederne la dignità.

\* Avvocato in Modena ha conseguito il diploma di specializzazione per le professioni legali e il perfezionamento in Criminalità informatica e investigazioni digitali. Collabora con la Cattedra di Informatica giuridica dell'Università degli Studi di Milano, Dipartimento di Scienze giuridiche "Cesare Beccaria", Facoltà di Giurisprudenza come cultore della materia e Residential Affiliate dell'Information Society Law Center – ISLC. È Dottoranda di Ricerca in Lavoro, Sviluppo e Innovazione, Università degli Studi di Modena e Reggio Emilia – Fondazione Marco Biagi.

Lo stesso *draft* del Regolamento “AI Act”, pubblicato il 21 aprile 2021<sup>1</sup>, nella relazione alla proposta al punto 3.5 avverte che «con le sue caratteristiche specifiche (ad esempio opacità, complessità, dipendenza dai dati, comportamento autonomo) l’I.A. può incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell’Unione Europea e in particolare sul diritto alla dignità umana».

Si ricorda che anche Rodotà aveva qualificato il lavoro uno degli ambiti in cui la dignità umana trova espressione<sup>2</sup>. Il lavoro è il contesto nel quale il lavoratore, ma prima di tutto l’uomo, esprime le sue capacità e la sua libertà (anche economica) partecipando alla costruzione del principio solidaristico contenuto nell’art. 2 della nostra Costituzione e realizzando la sua personalità: giacché è solo con il lavoro che è possibile affrancarsi dalle necessità materiali e godere delle libertà civili.

Tali sistemi ben potrebbero incidere sulle libertà del lavoratore e portare a una discriminazione indiretta e per lo più sconosciuta al lavoratore stesso, ignaro di essere oggetto di una sorveglianza costante, capillare e spesso inserita nel processo lavorativo stesso.

Oggi le sperimentazioni che sfruttano la potenza dell’I.A. sono numerose. Il mercato è testimone di varie applicazioni dell’I.A. (tra le quali, a titolo esemplificativo, la selezione del personale). Le stesse trovano particolare fortuna poiché consentono di diminuire i tempi di selezione e combinare una serie di informazioni con le *skills* ricercate dalle Società<sup>3</sup>.

Già nel 2015 Amazon aveva testato un sistema di *recruitment* intelligente. La sperimentazione era, però, stata interrotta dopo che i risultati avevano portato alla selezione di soli candidati di sesso maschile. Il risultato espresso dalla macchina “intelligente” derivava da una fase, quella di raccolta dei dati, antecedente alla selezione vera e propria. La mac-

<sup>1</sup> Cfr. *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull’Intelligenza artificiale (legge sull’Intelligenza Artificiale) e modifica alcuni atti legislativi dell’Unione*, 21.04.2021.

<sup>2</sup> Cfr. S. Rodotà, *Antropologia dell’uomo dignitus*, Lezione tenuta nell’Aula Magna dell’Università di Macerata, 6 ottobre 2010.

<sup>3</sup> Secondo il sito *researchmarket.com*, l’impiego dei sistemi di I.A. nelle attività di *recruiting* è destinato a crescere nei prossimi cinque anni in maniera esponenziale. Ad oggi, le aziende sperimentatrici di questa tecnologia sembrano essere influenzate positivamente dai risultati prodotti per il risparmio in termini di costi e di tempo rispetto ai metodi tradizionali.

*Intelligenza Artificiale nei rapporti di lavoro: tra regolazione e sfide future*

L'articolo intende indagare sull'applicazione dei sistemi di Intelligenza Artificiale nel mercato del lavoro, e in particolare, approfondire le norme relative alla protezione dei dati personali in riferimento ai processi decisionali automatizzati in riferimento al grado di esperibilità dei diritti riconosciuti al lavoratore. Oltre alla disamina relativa alle norme del Regolamento europeo 679/2016, il presente articolo si pone l'obiettivo di analizzare la proposta di Regolazione sull'Intelligenza Artificiale pubblicata lo scorso 21 aprile 2021 per comprendere se la sua attuazione sia in grado di proteggere gli interessi in gioco nel contesto lavorativo.

*Artificial intelligence in labor relations: between regulation and future challenges*

The article aims to investigate the application of Artificial Intelligence in the labor market, and in particular, to delve into the norms related to the protection of personal data in reference to automated decision-making processes with regard to the degree to which the rights granted to the worker are exercisable. In addition to the examination related to the rules of the European Regulation 679/2016, the present article aims to analyze the proposed Regulation on Artificial Intelligence published last April 21, 2021 to understand whether its implementation is able to protect the interests at stake in the labor market.

## Ruoli e rapporti tra i soggetti coinvolti nel trattamento dei dati personali nel settore del gas naturale

MARIAGRAZIA BERARDO\*

Sommario: 1. Introduzione. – 2. Figure e ruoli dei soggetti coinvolti nel trattamento dei dati personali alla luce del GDPR e delle Linee Guida dell’EDPB n. 7/2020. – 3. I titolari del trattamento. – 4. I contitolari del trattamento. – 5. I responsabili del trattamento. – 6. I sub-responsabili. – 7. La qualificazione giuridica dei soggetti coinvolti in attività di trattamento di dati personali nel settore del gas. – 8. Le società del gruppo. – 9. Dipendenti e fornitori. – 10. Il medico competente e l’OdV. – 11. Le società terze di vendita del gas. – 12. L’Acquirente Unico. – 13. Conclusioni.

### 1. *Introduzione*

Il settore del gas si caratterizza per la presenza di una filiera articolata, che vede coinvolti numerosi soggetti sia nelle varie fasi di cui la stessa si compone sia, di conseguenza, nel trattamento dei dati personali a queste connesso. Da ciò deriva l’importanza per le imprese operanti nel settore di adottare sistemi di *data governance* idonei a garantire un’adeguata tutela dei dati e di inquadrare correttamente i ruoli di tutti i soggetti che, a vario titolo, sono coinvolti nel relativo trattamento, così da regolamentare in modo adeguato i rapporti e determinare i rispettivi obblighi e responsabilità in conformità a quanto previsto dal Regolamento (UE) 2016/679 (“GDPR”).

Dopo un breve *excursus* normativo, il presente contributo si concentrerà sulla qualificazione ai fini privacy dei principali soggetti coinvolti nell’attività di distribuzione e vendita di gas naturale (anche alla luce dei provvedimenti dell’autorità garante italiana per la protezione dei dati personali - “Garante”).

\* Avvocato iscritto all’ordine di Torino dal 2018.

2. *Figure e ruoli dei soggetti coinvolti nel trattamento di dati personali alla luce del GDPR e delle Linee Guida dell'EDPB n. 7/2020*

Ponendosi in sostanziale continuità con la previgente Direttiva 95/46/CE (“Direttiva”) e con il Codice della Privacy – D.lgs. n. 196/2003 – con cui la stessa era stata recepita in Italia, anche il GDPR individua e definisce i ruoli dei soggetti coinvolti nel trattamento dei dati personali, introducendo (*rectius* formalizzando) quelli dei contitolari, degli incaricati e dei sub-responsabili del trattamento<sup>1</sup>, dettagliando per ciascuno i rispettivi obblighi e il contenuto minimo degli accordi tra questi intercorrenti.

Quattro sono le figure principali:

- (i) il titolare del trattamento (art. 4, n. 7 e artt. 24-25 GDPR), ossia «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»<sup>2</sup>, su cui ricade una responsabilità generale<sup>3</sup> sui trattamenti posti in essere direttamente o da altri per suo conto, con il conseguente onere di adottare misure tecniche e organizzative adeguate alla natura e ai rischi di tali trattamenti e di dimostrarne la conformità al GDPR;
- (ii) i contitolari (art. 26 GDPR), figura che ricorre nel caso in cui le finalità e i mezzi del trattamento siano determinati congiuntamente da due o più titolari, i quali sono tenuti a regolamentare tramite uno specifico accordo interno le rispettive responsabilità;
- (iii) il responsabile del trattamento (art. 4, n. 8 e artt. 28 – 29 GDPR), ossia «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro

<sup>1</sup> Il concetto di contitolari del trattamento era già previsto dalla Direttiva, ma è stato organicamente disciplinato per la prima volta solo con il GDPR. Le figure degli incaricati (interni) e dei sub-responsabili del trattamento costituiscono invece una novità, dato che entrambe, non erano previste dalla Direttiva, seppur riconosciute in alcuni Stati membri e/o nella prassi operativa (per esempio, l'incaricato del trattamento era riconosciuto esclusivamente in Italia).

<sup>2</sup> Cfr. art. 4, n. 7 GDPR.

<sup>3</sup> In forza del principio di *accountability* (ossia di responsabilizzazione) ex art. 5, par. 2 GDPR, il titolare del trattamento è infatti giuridicamente responsabile del rispetto dei principi generali che, a norma del primo paragrafo dello stesso articolo 5, devono essere alla base di ogni trattamento (*i.e.* liceità, correttezza e trasparenza, finalità, qualità dei dati – ossia pertinenza, adeguatezza e non eccedenza – esattezza dei dati, conservazione sulla base della finalità e sicurezza).

*Ruoli e rapporti tra i soggetti coinvolti nel trattamento dei dati personali nel settore del gas*

La corretta qualificazione del ruolo dei soggetti coinvolti nelle operazioni di trattamento di dati personali è un presupposto fondamentale di una privacy *compliance* conforme al Regolamento (UE) 2016/679, specie per le aziende operanti in settori che, come quello del gas, si caratterizzano per la presenza di una filiera articolata.

Prendendo le mosse dal dettato normativo del GDPR e, soprattutto, dai recenti preziosi chiarimenti forniti dall'*European Data Protection Board* con le linee guida n. 1/2020 e dal Garante della privacy italiano, nel presente contributo si esamineranno le caratteristiche dei ruoli di titolare, contitolari, responsabile, sub-responsabile ed incaricati del trattamento dei dati personali, per poi concentrarsi sulla qualificazione ai fini privacy dei principali soggetti coinvolti nell'attività di distribuzione e vendita di gas naturale.

*Roles and relations between actors involved in the processing of personal data in the gas sector*

The correct qualification of the actors involved in the processing of personal data is an essential requirement for a privacy compliance in accordance with the Regulation (EU) 2016/679, especially for those companies operating in sectors which have an articulated supply chain (such as the gas sector).

Starting from GDPR and paying particular attention to the recent important clarifications provided by the European Data Protection Board with the guidelines n. 1/2020 as well as by the Italian national privacy supervisory authority, this paper will analyse the concepts of data controller, joint controller, data processor and sub-processor and will then focus on the privacy qualification of the main actors involved in distribution and sale of natural gas.

## La sorveglianza datoriale nell'era digitale

SIMONA KLIMBACHER\*

SOMMARIO: 1. Premessa. – 2. La normativa applicabile alla sorveglianza datoriale. – 3. Base giuridica e consenso. – 4. L'informativa. – 5. Gli adempimenti necessari per il datore di lavoro. – 6. Considerazioni conclusive.

### 1. *Premessa*

Il termine “sorveglianza” è divenuto di grande attualità nell'era digitale, caratterizzata da un crescente utilizzo di dispositivi informatici che consentono nuove forme di “controllo remoto”.

La sorveglianza di uno spazio specifico – fisico o elettronico – viene attuata per molteplici fini, tra cui prevalentemente la protezione della vita, della salute e della proprietà. Le sue caratteristiche tipiche sono il monitoraggio, il tracciamento, il controllo e l'osservazione sistematica dei comportamenti altrui. Si tratta quindi di un'attività che comporta l'inevitabile raccolta e conservazione di molteplici dati e informazioni su tutte le persone che entrano nello specifico spazio oggetto di monitoraggio; ne consegue che quanto più ampio sarà lo spazio monitorato, tanto maggiore risulterà il pericolo di un uso improprio di tali dati, soprattutto nei casi di sorveglianza sistematica e automatizzata e, quindi, continua nel tempo.

Nella presente trattazione verrà analizzato il fenomeno della sorveglianza in ambito lavorativo – con specifico riferimento alla disciplina della protezione dei dati che ne derivano – anche alla luce delle recenti e significative evoluzioni nelle modalità tipiche di svolgimento delle prestazioni lavorative, che vedono il progressivo passaggio da un luogo fisi-

\* Avvocato in Milano e New York, LL.M. (Fordham University School of Law). Collaboratrice presso la Cattedra di Informatica Giuridica dell'Università degli Studi di Milano e International Research Fellow del Centro di Ricerca in Information Society Law (ISLC).

co delimitato (es. l'ufficio) ad uno spazio indefinito, virtuale, nel quale il lavoratore comunica da remoto con il proprio datore di lavoro.

La diffusione del c.d. "lavoro agile" ha subito una decisa accelerazione nel periodo dell'emergenza sanitaria causata dalla pandemia Covid-19. L'indagine condotta dal Ministero del lavoro e delle politiche sociali nel contesto dell'introduzione del *Protocollo Nazionale sul Lavoro in Modalità Agile*<sup>1</sup> ha evidenziato che il ricorso al lavoro agile è più che raddoppiato rispetto al periodo pre-pandemico ed è diventato un tassello sempre più strutturale nell'organizzazione del lavoro.

In tale contesto, anche la sorveglianza datoriale si evolve verso nuove forme. Si passa infatti da una sorveglianza pensata e attuata prevalentemente con dispositivi dislocati presso i luoghi di lavoro (es. telecamere) all'utilizzo – più o meno manifesto – di strumenti digitali che consentono il controllo a distanza dell'attività dei lavoratori.

Basti pensare alle possibilità di accesso, da parte del datore di lavoro, agli strumenti messi a disposizione del lavoratore per rendere la propria prestazione lavorativa o professionale, quali computer, tablet e smartphone, dove qualsiasi operazione attuata dal lavoratore può essere potenzialmente oggetto di controllo da parte del datore di lavoro, mediante accesso alla posta elettronica (per conoscere i destinatari della posta inviata, ricevuta e i relativi contenuti), alla navigazione in internet (per conoscere i siti visitati e il tempo trascorso sul web), al disco del computer (per conoscere i dati processati, conservati ed eliminati), fino ad arrivare al GPS installato su un *device* (per conoscere gli spostamenti, le abitudini di guida, lo stato psico-fisico nel condurre un veicolo aziendale) e alle fotocamere (per conoscere le espressioni facciali rispetto ai *pattern* predefiniti).

In proposito, è stato osservato come grazie ad alcuni *software* il datore di lavoro possa di fatto esercitare un "pieno controllo" sull'insieme dei dati di carattere sia lavorativo che personale dei dipendenti<sup>2</sup>. D'altra parte, molto spesso è la stessa tecnologia "consegnata" al lavoratore a essere

<sup>1</sup> Il Protocollo, sottoscritto in data 7 dicembre 2021, è divenuto pienamente operativo a partire dal 1° settembre 2022 al termine della fase dello *smart working* emergenziale.

<sup>2</sup> Cfr. G. ZICCARDI, "Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatiche giuridiche", «Labour&Law Issues», vol. 2, n. 1, 2016, pp 55-59.



*La sorveglianza datoriale nell'era digitale*

Nell'era digitale la sorveglianza datoriale si evolve anche in ragione della diffusione di nuove forme di lavoro (*smart*, ibrida) e dell'utilizzo di tecnologie sempre più complesse e invasive.

Il presente articolo esamina la disciplina vigente in materia di controlli a distanza dei lavoratori, con specifico riferimento alla disciplina della protezione dei dati che ne derivano.

Dopo un *excursus* dell'evoluzione normativa in tema di controlli a distanza, viene analizzata la distinzione tra “strumenti di controllo” e “strumenti di lavoro” utilizzati dal lavoratore per rendere la propria prestazione lavorativa, con specifico riferimento ai principali strumenti tecnologici in dotazione ai dipendenti. Particolare attenzione è dedicata all'importanza di un'adeguata informativa ai lavoratori riguardo alle modalità di utilizzo degli strumenti tecnologici e di effettuazione dei controlli.

Viene quindi analizzato il “doppio ruolo” del datore di lavoro, quale garante della sicurezza e produttività della propria realtà lavorativa ma anche quale garante dei diritti fondamentali di ciascun lavoratore attraverso l'implementazione di procedure interne efficaci e trasparenti.

Si delineano infine, i principali adempimenti a carico del datore di lavoro, anche alla luce delle recenti disposizioni introdotte dal Decreto Trasparenza.

*Employer surveillance in the digital age*

In the digital age, surveillance by employers is evolving due to the adoption of new working models (smart, hybrid) and to the use of highly sophisticated and invasive technology.

This article examines the current legal framework applicable to the remote monitoring of workers with specific reference to data protection regulations.

Following a brief outline of the applicable laws and regulations on remote surveillance, the article analyses the differences between “monitoring tools” and “working tools” used by employees to perform their job, with a specific focus on the most common technology equipment supplied by employers.

Special attention is given to the need to adequately inform employees on the proper use of the digital equipment supplied and the cases in which monitoring in the workplace may apply.

Further, the article analyses the “dual role” of the employer as the guarantor both of the security and productivity of the business, as well as of the fundamen-

tal rights of each employee through the enforcement of internal transparent and effective procedures.

Finally, the main duties of the employers are outlined, also in light of the recent provisions introduced by the so-called Decree “Trasparenza”.

# PUBBLICA AMMINISTRAZIONE DIGITALE

## CAD, bugie e dibattito: il documento informatico in una prospettiva penalistica

DONATO EUGENIO CACCAVELLA, SILVIA PELLEGRINI\*

SOMMARIO: 1. Il CAD (decreto legislativo 7 marzo 2005, n. 82). – 2. Le regole tecniche: l'art. 71 del CAD e le Linee Guida AgID. – 3. Casi reali: quando il documento è veramente informatico? – 3.1. Il documento informatico: essere o non essere, questo è il dilemma. – 4. Conclusioni: l'intricato quadro fra Codice penale e Codice dell'Amministrazione Digitale.

### 1. *Il CAD (decreto legislativo 7 marzo 2005, n. 82)*

Il Codice dell'Amministrazione Digitale definisce il documento informatico come «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti», in contrapposizione al documento analogico, «rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti». Il Regolamento eIDAS n. 910/2014 definisce il documento elettronico come «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva». Per comprendere

\* Donato Eugenio Caccavella è laureato in Matematica presso l'Università di Bologna. Autore di articoli sul tema dell'informatica forense e della data protection, attualmente è Professore a contratto di Digital Forensics e di Sicurezza dei Sistemi Informativi presso l'Università degli Studi di Milano e di Digital Forensics Sanitaria presso l'Università degli Studi di Bologna. Svolge attività di consulenza in BIT4LAW relativamente all'informatica forense per conto di Autorità giudiziarie ed enti privati. Ricopre il ruolo di DPO in alcune società private.

\* Silvia Pellegrini è laureata in Giurisprudenza presso l'Università di Bologna, in cui ha conseguito successivamente il Master in Diritto delle Nuove Tecnologie e Informatica Giuridica. Ha terminato la pratica forense e il tirocinio ex art. 73 presso la Procura della Repubblica di Bologna. Insignita del Premio di Laurea "L'Europa che sarà 2022" della Regione Emilia-Romagna per la tesi di laurea in Diritto del Lavoro e Diritto dell'Unione Europea, svolge attività di consulenza in Diritto Europeo e Diritto delle nuove tecnologie presso la Regione Emilia-Romagna e presso BIT4LAW.

re correttamente il documento informatico, è opportuno analizzare con attenzione gli artt. 20, 21, 22 e 23 del CAD. All'art. 20 si stabilisce che il documento informatico ha valore di forma scritta, ai sensi dell'art. 2702 c.c., se vi è apposta la firma digitale o altro tipo di firma elettronica qualificata, che – in ogni caso – attesti la paternità dell'autore e che rispetti le caratteristiche di integrità e sicurezza. Anche nell'art. 21 del CAD si afferma che l'atto che rispetti i requisiti di cui all'art. 2702 del c.c. debba essere firmato con firma elettronica avanzata, qualificata o digitale; in aggiunta, si sottolinea come qualsiasi altro atto pubblico redatto su documento informatico debba essere firmato con firma qualificata o digitale. Viene abbandonato, quindi, il principio di non discriminazione tecnologico presente prima della riforma del 2017. All'art. 22, si illustrano le caratteristiche delle copie informatiche di documenti analogici, ovvero si analizza la formazione del documento informatico dei casi in questione. Si individuano tre livelli graduali di parametri per cui una copia informatica possa avere l'efficacia probatoria della forma scritta. In primo luogo, si sostiene che le copie informatiche assumono valenza probatoria se formati ai sensi dell'art. 20; poi se la conformità fra copia informatica e il suo originale analogico è attestata da un notaio o da un altro Pubblico Ufficiale a ciò autorizzato, secondo le regole tecniche di cui all'art. 71. In ultima analisi, come parametro residuale, si afferma che le copie informatiche hanno la stessa efficacia probatoria dell'originale analogico se non espressamente disconosciute. Infine, all'art. 23, oltre a quanto già detto per l'art. 22, si affronta l'argomento della copia analogica di documento informatico e di come la sua autenticità possa essere attestata e si introducono nuovi strumenti tecnologici come l'apposizione di un contrassegno che rimandi all'originale documento informatico, che sostituisce in tutto la necessità di apposizione di una firma.

Per una disanima il più possibile accurata, nel paragrafo successivo si analizzeranno l'art. 71 CAD e le Linee Guida AgID.

*CAD, bugie e dibattimento: il documento informatico in una prospettiva penalistica*

La presente trattazione mira a delineare gli elementi fondamentali del documento informatico all'interno del processo penale. Tale esigenza deriva da un continuo aumento di casi giudiziari in cui è necessario apprezzare quale sia la natura giuridica di file creati in ambito informatico e se tali file siano dotati dei requisiti tecnici del documento informatico. Perciò, in quest'elaborato, si compirà un'analisi approfondita di quanto disposto dal Codice dell'Amministrazione Digitale (d.lgs. 82 del 2005), che rappresenta lo strumento principale in materia di apprezzamento delle caratteristiche di documento informatico, con particolare riferimento agli artt. 20, 21, 22, 23 e 71; si analizzeranno le linee guida AgID e si sintetizzeranno due casi giudiziari che hanno portato a questa analisi giuridico-tecnica ad essere un tema quanto mai attuale e sempre più rilevante.

*CAD, lies and trial: the electronic document in a criminalistic perspective*

The purpose of this paper is to outline the fundamental elements of the electronic document within the criminal process. This requirement stems from a continuous increase in judicial cases in which it is necessary to assess the legal nature of files created in an IT environment and whether those files are equipped with the technical requirements of the electronic document. Therefore, in this paper, we will carry out a thorough analysis of the provisions of the Code of Digital Administration (d.lgs. 82/2005), which is the main tool for evaluating the characteristics of the electronic document, with particular reference to articles 20, 21, 22, 23 and 71; AgID guidelines will be analysed and two judicial cases, that have led to this legal-technical analysis, will be summarised, since this topic has proven an increasingly relevant issue.

## Tre ostacoli al voto elettronico in Italia: pregiudizi, contraddizioni del sistema, carenza di cultura digitale

EDOARDO COLZANI\*

SOMMARIO: 1. Il dibattito sul voto elettronico in Italia. – 2. Sperimentazioni e proposte di legge sul voto elettronico. – 3. Tre ostacoli al voto elettronico in Italia. – 3.1. L'illusione del voto sicuro. Una questione di fiducia. – 3.2. Una contraddizione nel sistema: voto elettronico elettivo *vs* voto elettronico deliberativo. – 3.3. Ripensare i meccanismi di voto per rendere effettivo il diritto di voto.

### 1. *Il dibattito sul voto elettronico in Italia*

Il presente contributo si propone una ricognizione dei principali aspetti connessi al tema del voto elettronico in ambito pubblico<sup>1</sup>, al fine di fornire al lettore una ricostruzione dei problemi ancora irrisolti e dei pregiudizi che impediscono lo sviluppo di tale forma di votazione all'interno del sistema italiano<sup>2</sup>. Ad oggi, nel dibattito pubblico, la scarsa alfabetizzazione digitale e normative che spesso ignorano la reale natura delle tecnologie impediscono di comprendere i benefici portati da questo *medium*, antepoendo a essi i possibili rischi e sollevando, peraltro, obiezioni circa la possibilità che le istituzioni sulle quali si è fatto affidamento per così lungo tempo siano ancora abbastanza forti e flessibili da

\* Avvocato, Dottore di Ricerca in Filosofia del Diritto.

<sup>1</sup> Al di fuori dell'ambito pubblico, sistemi di *e-voting* e *i-voting* trovano spazio nell'ambito societario, associativo, etc.

<sup>2</sup> Negli ultimi mesi vi sono state diverse occasioni in cui la stampa e le forze politiche si sono confrontate su questioni relative ai sistemi di voto elettronico. In particolare, in riferimento alla scelta della regione Lombardia di utilizzare una piattaforma di voto elettronico per il c.d. "Referendum Autonomia", e per il caso delle violazioni alla piattaforma Rousseau del Movimento 5 Stelle che hanno condotto, addirittura, a un intervento del Garante della Privacy.

poter gestire i cambiamenti in corso in un'ottica di libertà e democrazia<sup>3</sup>. Come si cercherà di dimostrare, infatti, nonostante le varie sperimentazioni effettuate, sono ancora diffusi dei preconcetti sul voto elettronico, e più in generale sui rapporti tra democrazia e nuove tecnologie, che sino a ora hanno impedito passi avanti nel dibattito pubblico. Eppure, si tratta di una sfida che ci impongono le nuove tecnologie e che non possiamo ignorare<sup>4</sup>. In questo senso, peraltro, vi è nei confronti del nostro ordinamento la sollecitazione anche dell'Europa. A partire da un progetto di sviluppo di origine europea, l'*E-POLL*<sup>5</sup>, il Ministero si impegna nella realizzazione di attività volte ad aumentare la partecipazione dei cittadini agli appuntamenti elettorali, permettendo loro di votare anche senza recarsi direttamente ai classici seggi, ma tramite delle postazioni appo-

<sup>3</sup> Cfr. G. ZICCARDI, "Democrazia elettronica e libertà dei dati tra sistemi elettorali e WikiLeaks", «Ciberspazio e diritto», vol. 12, n. 1, 2011, pp. 5-20.

<sup>4</sup> Gianmarco Gometz traccia un bilancio delle effettive capacità innovatrici delle ICT nei confronti della democrazia individuando quattro criteri di valutazione: l'espressività (cioè la capacità di veicolare una intenzione politica chiara ed esaustiva), la sicurezza (da brogli e manipolazioni, oltre che da interferenze esterne), l'influenza (cioè la ampiezza e varietà delle questioni su cui le decisioni votate possono incidere), l'accessibilità (fruibilità delle tecnologie da parte di chi ha diritti politici). Secondo Gometz, le ICT avrebbero il pregio di accrescere l'espressività e l'influenza del suffragio popolare, permettendo di particolareggiare l'indirizzo politico espresso nel voto; gli elettori avrebbero altresì la strumentazione per esprimersi più volte nel merito, rendendo così manifesta la loro volontà su un maggior numero di questioni. Non sfuggono, tuttavia, all'autore i problemi connessi all'ICT, rappresentati essenzialmente da una diffusa incompetenza nell'uso delle tecnologie e dai problemi relativi alla sicurezza dell'ICT. Cfr. G. GOMETZ, *Democrazia elettronica. Teoria e tecniche*, Pisa, Edizioni ETS 2017.

<sup>5</sup> *E-POLL* è un progetto transnazionale di ricerca e sviluppo tecnologico co-finanziato dalla direzione generale per la società dell'informazione della Commissione dell'Unione europea nell'ambito del programma *IST (Information Society Technologies)* del quinto programma quadro. Partner del progetto, che vede la presenza di due Paesi membri dell'Unione e di un Paese candidato, sono: il Ministero dell'Interno, Siemens informatica e Ancitel. Il progetto di voto elettronico denominato *E-Poll*, il cui nome completo è *Electronic polling system for remote voting operations*, ha l'obiettivo di semplificare le operazioni di voto attraverso l'integrazione di soluzioni tecnologiche di avanguardia, di indicazioni per l'innovazione normativa a livello europeo e di un modello organizzativo che risulta essere di grande efficacia senza introdurre nel sistema particolari complessità gestionali per tutte le fasi di voto: preparazione del voto, identificazione e autenticazione (con garanzia di riservatezza), autorizzazione, trasmissione del voto (in situazione di sicurezza), conteggio dei voti e comunicazione dei risultati.



*Tre ostacoli al voto elettronico in Italia: pregiudizi, contraddizioni del sistema, carenza di cultura digitale*

Il presente contributo propone una ricognizione dei principali aspetti connessi al tema del voto elettronico in ambito pubblico, al fine di fornire al lettore una ricostruzione dei problemi ancora irrisolti e dei pregiudizi che impediscono lo sviluppo di tale forma di votazione all'interno del sistema italiano. L'Autore, anche sulla base di un raffronto con esperienze straniere, evidenzia come la carenza di adeguata consapevolezza digitale sia di ostacolo a una seria riflessione sul tema.

*Three obstacles to e-voting in Italy: bias, contradictions in the system, lack of digital culture*

The paper focuses on electronic voting system and its application in the Italian legal system. Italian Constitutional principles and the lack of digital awareness represent, according to the Author, the main obstacle to the development of the electronic vote in Italy which is still considered unsecured.

## SOCIAL NETWORK E CASI GIUDIZIARI

## Le richieste social di revisione delle vicende giudiziarie. Considerazioni generali e casi pratici

GUGLIELMA VACCARO\*

SOMMARIO: 1. Considerazioni generali. I principi codificati nella Costituzione e l'interpretazione dell'opinione pubblica sui social network. – 2. La richiesta mediatica di riapertura di una vicenda giudizialmente conclusa è possibile? – 2.1. Il caso “Emme Team” e il cosiddetto “Metodo Cantone”. – 2.2. Il caso della scomparsa di Denise Pipitone e la richiesta di riapertura delle indagini. – 2.3. Il caso “Garlasco” e la difesa di Alberto Stasi. – 3. Conclusioni. Un gigantesco divano virtuale. L'ansia di partecipazione e il rischio del capro espiatorio.

### 1. *Considerazioni generali. I principi codificati nella Costituzione e l'interpretazione dell'opinione pubblica sui social network*

Sulle attuali piattaforme social, a proposito di casi di cronaca maggiormente dibattuti, è frequente imbattersi nelle locuzioni “Non in mio nome” e “Verità e Giustizia”. Tali espressioni, contenute in un commento a un articolo e talvolta precedute dal simbolo del cancelletto, in modo che si trasformino in un *hashtag*<sup>1</sup> unificatore di contenuti, manifestano, da parte di chi le utilizza, la non condivisione, il dissenso rispetto a provvedimenti giuridici che hanno messo la parola fine, a livello giudiziario, a una vicenda che ha generato interesse e partecipazione nell'opinione

\* Avvocato, da anni approfondisce questioni legate al ruolo dei social nella cronaca, intervenendo talvolta nelle discussioni per una migliore osservazione del fenomeno. Le opinioni espresse nel presente contributo, in mancanza di diverso riferimento, sono di responsabilità esclusiva dell'Autore e non riflettono necessariamente le posizioni dei soggetti coinvolti a vario titolo nei casi oggetto del presente studio.

<sup>1</sup> In alcuni motori di ricerca e, in particolare, in siti di *microblogging*, parola o frase (composta da più parole, scritte unite), preceduta dal simbolo cancelletto (#), che serve per etichettare e rintracciare soggetti di interesse (definizione del Vocabolario Treccani, rinvenibile al link <https://www.treccani.it/vocabolario/ricerca/hashtag/>).

pubblica, ovvero quello che, con una espressione entrata nel linguaggio comune, si definisce un “processo mediatico”.

Come noto, secondo quanto previsto dall’art. 27, comma 2, della Costituzione, un imputato è considerato non colpevole sino a condanna definitiva, vale a dire fino all’esito del terzo grado di giudizio emesso dalla Corte di Cassazione, oppure sino a quando non sono decorsi i termini previsti dalla legge per promuovere l’azione di impugnazione di una decisione formalizzata nel grado precedente<sup>2</sup>. In caso di rigetto dell’impugnazione o in difetto di azione nei termini previsti dalla legge, la sentenza passa in giudicato e la condanna assume valore di *status* giuridico consolidato. La *ratio* della previsione normativa è chiara: assicurare, in un’ottica di rispetto dei diritti fondamentali dell’individuo, che un soggetto si possa definire colpevole solo quando si è completato l’*iter* attraverso cui i magistrati, in veste di rappresentanti dello Stato, indipendenti e imparziali, hanno accertato al di là di ogni ragionevole dubbio le responsabilità per l’atto illecito contestato.

Rimedio eccezionale per cambiare una condizione così “cristallizzata” è l’istituto della revisione, prevista dagli artt. 629 e ss. del Codice di procedura penale, a norma dei quali è ammessa in ogni tempo a favore dei condannati, nei casi determinati dalla legge, la revisione delle sentenze di condanna o delle sentenze emesse ai sensi dell’articolo 444, comma 2<sup>3</sup>, o dei decreti penali di condanna diventati irrevocabili, anche se la pena è stata eseguita o è estinta.

La revisione, in quanto mezzo straordinario di “ribaltamento” di una sentenza di condanna definitiva, presuppone requisiti precisi e prevede che il soggetto condannato o altri soggetti previsti dalla legge<sup>4</sup> e della sua difesa:

<sup>2</sup> Cfr. art. 27 Costituzione: «La responsabilità penale è personale. L’imputato non è considerato colpevole sino alla condanna definitiva. Le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione del condannato [cfr. art. 13, comma 4]. Non è ammessa la pena di morte».

<sup>3</sup> Si tratta delle norme che regolano l’applicazione della pena su richiesta, un accordo tra imputato e Pubblico Ministero che, nel linguaggio comune, è più noto con il termine di “patteggiamento”.

<sup>4</sup> I soggetti legittimati alla richiesta di revisione sono, oltre al condannato, un prossimo congiunto ex art. 307 comma 4 c.p., il tutore del condannato, l’erede o il prossimo congiunto del condannato deceduto, nonché il Procuratore Generale della Corte d’Ap-

*Le richieste social di revisione delle vicende giudiziarie. Considerazioni generali e casi pratici*

Oggetto del presente contributo è l'analisi dell'interazione tra gli attuali sistemi di comunicazione e lo sviluppo di vicende giudiziarie di grande risonanza mediatica, il cui *iter* giudiziario si è concluso tra dubbi, perplessità e polemiche. Le vicende portate ad esempio costituiscono una "fotografia" del momento, in un flusso di notizie in costante aggiornamento, che costituiscono la fonte bibliografica preminente.

*Social requests for review of court cases. General considerations and practical cases*

The subject of this paper is the analysis of the interaction between the current communication systems and the development of judicial events of great media coverage, whose judicial process ended with doubts, perplexities and controversies.

The events taken as an example constitute a "photograph" of the moment, in a constantly updated stream of news that constitute the preminent bibliographic source.