UNIVERSITÀ DEGLI STUDI ROMA TRE
COLLANA CRISPEL
SEZIONE DI DIRITTO PUBBLICO ITALIANO ED EUROPEO
diretta da Franco Modugno
Collettanee
7

INNOVAZIONE TECNOLOGICA E VALORE DELLA PERSONA

Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679

a cura di

Licia Califano e Carlo Colapietro

Prefazione di Paolo Aquilanti

Editoriale Scientifica
Napoli

Il presente volume è stato pubblicato con il contributo del CRISPEL e del Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tre nonché con il contributo del Dipartimento di Giurisprudenza (DIGIUR) dell'Università degli Studi di Urbino Carlo Bo.

Via San Biagio dei Librai, 39 – 80138 Napoli

www.editorialescientifica.com

ISBN 978-88-9391-264-8

INDICE

XVII *Prefazione*
Paolo AQUILANTI

XXIII *Introduzione*

PRIMA PARTE
IL REGOLAMENTO EUROPEO
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

3 *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*
Licia CALIFANO

1. Origine, natura giuridica e strumenti di tutela di un diritto fondamentale: la protezione dei dati personali 3 - 2. La scelta dello strumento *self executing* e i suoi effetti in ambito europeo e nazionale 17 - 3. I principi ispiratori della nuova normativa tra conferme di un modello consolidato e novità che rafforzano l'esercizio del diritto 24 - 4. Il principio di responsabilizzazione ovvero il passaggio ad una logica di tutela preventiva quale approccio sostanziale ai doveri del titolare 34 - 5. La responsabilizzazione dei titolari e l'aspetto sanzionatorio 40 - 6. Lo schema informativa-consenso tra riaffermazione e consapevolezza dei limiti intrinseci 47

57 *Le origini ed il contesto*
Giulio M. SALERNO

1. Breve introduzione ai rapporti costituzionalmente delineati tra il nostro ordinamento, la UE e la CEDU 57 - 2. L'evoluzione integrata e progressiva delle competenze e delle discipline europee in materia di protezione e di corretto trattamento dei dati personali 63 - 3. Il ruolo della Corte di giustizia dell'Unione europea sulla disciplina della protezione dei dati personali 72 - 4. Qualche conclusione sull'evoluzione della dimensione costituzionale della protezione dei dati di carattere personale 81

85 *I principi generali del trattamento dei dati personali e i diritti dell'interessato*
Carlo Colapietro, Antonio Iannuzzi

1. Premesse e finalità del Regolamento. La funzione di indirizzo interpretativo dei *considerando* 85 - 2. L'ambito di applicazione del Regolamento 91 - 3. Le definizioni: la nozione dinamica del dato personale oggetto di protezione 98 - 4. L'autodeterminazione informativa ed i principi del trattamento dei dati personali 106 - 5. Il consenso informato ed il consenso dei minori "nativi digitali" 115 - 6. I diritti dell'interessato e la loro tutela 122 - 7. Il diritto all'oblio 126

137 *La responsabilità e la sicurezza del trattamento*
Simone Calzolaio, Laura Ferola, Valentina Fiorillo, Edoardo Alberto Rossi, Matteo Timiani

1. Gli effetti del Regolamento europeo sui titolari del trattamento. Considerazioni introduttive 137 - 2. Il titolare, il contitolare e il responsabile del trattamento 142 - 3. Il responsabile della protezione dei dati (RPD) 154 - 4. La funzione dei codici di condotta e delle certificazioni 162 - 5. La pianificazione dinamica della protezione dei dati: *privacy by design* e *privacy by default* 170 - 6. La pianificazione dinamica della protezione dei dati: valutazione di impatto e consultazione preventiva 175 - 7. Il modello dinamico di sicurezza del trattamento: prevenzione e reazione alle violazioni 186 - 8. Il modello europeo di "protezione transfrontaliera" dei dati personali 195

203 *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*
Lorenzo Chieffi

1. Innovazioni tecnologiche e tutela dei diritti fondamentali nei più recenti sviluppi del diritto europeo 203 - 2. Il ruolo del diritto nella protezione dei dati sensibili 210 - 3. Il dato sensibile nel Regolamento europeo 2016/679 214 - 4. (*segue*) Il trattamento dei dati genetici 221 - 5. Nuovi ambiti di protezione dell'autodeterminazione informativa 226 - 6. Il consenso informato al trattamento dei dati sensibili 230 - 7. Il controllo sulla circolazione dei dati sensibili 236 - 8. La regolamentazione dell'accesso ai dati sensibili 242 - 9. Eccezioni e deroghe al divieto di trattare i dati sensibili 246 - 10. Il trasferimento dei dati sensibili a Paesi terzi. I necessari *standard* di sicurezza 252 - 11. La violazione della riservatezza dei dati sensibili. Le conseguenze di tipo sanzionatorio 255 - 12. Considerazioni conclusive. Prospettive di adeguamento della normativa statale alla nuova disciplina regolamentare europea 260

267 *L'indipendenza del Garante*
Andrea Patroni Griffi

1. Una premessa sull'indipendenza delle Autorità di controllo: oltre l'imparzialità dell'amministrazione 267 - 2. Un'indipendenza diversa rispetto a quella dei giudici. Un possibile parallelismo con i giudici costituzionali o con

le giurisdizioni speciali? 274 - 3. Le *misure* dell'indipendenza delle Autorità di controllo nel Regolamento europeo 2016/679 sulla protezione dei dati 282 - 4. Le *misure* dell'indipendenza delle Autorità di controllo per la protezione dei dati nei singoli ordinamenti nazionali 291 - 5. (*segue*) La scelta di costituzionalizzare la garanzia di indipendenza dell'Autorità di controllo. Il caso della Grecia 301 - 6. Il giusto equilibrio nella scelta dei garanti: alcune riflessioni conclusive 304

311 *Regolamento UE 2016/679 e rapporto di lavoro*
Arturo MARESCA, Silvia CIUCCIOVINO, Ilario ALVINO

1. L'impatto del Regolamento UE 2016/679 nel campo dei rapporti di lavoro 312 - 2. I tratti di specialità della protezione dei dati personali dei lavoratori nel rapporto di lavoro e nel mercato del lavoro 314 - 3. La portata del principio di responsabilizzazione del titolare del trattamento nel rapporto di lavoro tra Regolamento UE 2016/679 e obbligo generale di protezione dei lavoratori di cui all'art. 2087 c.c. 323 - 4. La nuova dimensione organizzativa della protezione dei dati personali: analogie e differenze con la dimensione organizzativa della tutela della salute e sicurezza sul lavoro 327 - 5. La figura del *data protection officer*: rapporto con il datore di lavoro e posizione nella gerarchia aziendale 330 - 6. I principi applicabili al trattamento dei dati personali nel rapporto di lavoro alla luce del Regolamento UE 2016/679 334 - 7. L'impatto del Regolamento UE 2016/679 sugli orientamenti dell'Autorità per la protezione dei dati personali e sulle indicazioni da questa espresse nelle linee guida in materia di trattamento dei dati personali nel rapporto di lavoro 343 - 8. Il nuovo art. 4, L. 300/1970 alla luce del Regolamento UE 2016/679 345 - 9. La (ri)definizione e sistematizzazione dei c.d. controlli difensivi 350 - 10. Condizioni di legittimità dei controlli a distanza: l'accordo sindacale e l'autorizzazione amministrativa 354 - 11. Le esenzioni riservate agli strumenti utilizzati per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze 356 - 12. Controlli legittimi e utilizzabilità dei dati acquisiti per la gestione del rapporto di lavoro 362 - 13. L'informazione trasparente al lavoratore come condizione per l'utilizzabilità dei dati raccolti dal datore di lavoro 364

367 *La transizione verso il nuovo sistema delle fonti europee di protezione dei dati personali*
Massimo RUBECHI

1. Dal Codice al Regolamento: strumenti e modelli di implementazione e armonizzazione 367 - 2. I margini di intervento degli attori istituzionali statali: i vincoli di carattere generale, gli interventi necessari, facoltativi, la sfida dell'armonizzazione 374 - 3. Le prospettive attuative negli altri Stati dell'Unione europea (*cenni*) 387 - 4. Considerazioni di sintesi 393

PARTE SECONDA

PROTEZIONE E SICUREZZA NEI PRINCIPALI SETTORI DI TRATTAMENTO DEI DATI PERSONALI

397 *I trattamenti in ambito pubblico nell'era della digitalizzazione e della trasparenza*
Stefano TOSCHEI

1. Il mutevole significato del termine trasparenza nell'ordinamento nazionale 397 - 2. L'istituto della trasparenza tra principi comunitari e disposizioni normative di recepimento 408 - 3. Traiettorie fondamentali della tutela dei dati personali nel nostro ordinamento 413 - 4. Il difficile bilanciamento tra tutela della riservatezza e diritto alla conoscibilità 417 - 5. L'era della digitalizzazione dell'azione pubblica, il fenomeno dei *Big data* e le garanzie dei diritti coinvolti 430

441 *I dati relativi alla salute e i trattamenti in ambito sanitario*
Guerino FARES

1. Inquadramento del tema 441 - 2. Il trattamento dei dati concernenti la salute nel Regolamento UE 2016/679: definizioni 452 - 3. I presupposti di liceità del trattamento e le coordinate assiologiche dei *considerando* 455 - 4. L'impatto del Regolamento sul sistema salute: la portata dell'art. 9 461 - 5. Il piano patologico, fra diritto europeo ed ordinamento nazionale: il vizio di omesso trattamento 466 - 6. (*segue*) Il vizio di trattamento indebito 474 - 7. Considerazioni conclusive 478

491 *I trattamenti nel settore dell'istruzione e a fini di ricerca (scientifica, storica, statistica)*
Erik LONGO

1. Introduzione 491 - 2. Trattamento dei dati personali c. libertà di ricerca 493 - 3. Dalla Direttiva del 1995 al Codice privacy 497 - 4. Il Regolamento UE 2016/679: introduzione e principio della "limitazione della finalità" 499 - 5. (*segue*) Principi e regole applicabili ai trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici 501 - 6. Garanzie e deroghe applicabili ai trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici 503 - 7. I trattamenti nel settore dell'istruzione 506 - 8. Considerazioni conclusive 507

509 *Trattamento dei dati personali e libertà di espressione e di informazione*
Marco OROFINO

1. Il lento riconoscimento costituzionale del diritto alla riservatezza e la sua successiva attrazione nell'ambito del diritto alla protezione dei dati personali 509 - 2. L'impatto delle nuove tecnologie sulla libertà di espressione e sul diritto alla protezione dei dati personali nonché sul loro rapporto 516 - 3. Il rapporto tra libertà di espressione e di informazione e diritto alla protezione dei dati

personali nella Direttiva 95/46/CE 518 - 4. Il rapporto tra libertà di espressione e di informazione e diritto alla protezione dei dati personali nel Codice di protezione dati 520 - 5. La "giurisprudenza" del Garante riguardo al rapporto tra diritto di cronaca e protezione dei dati personali 522 - 6. Il nuovo Regolamento UE 2016/679: la disciplina delle limitazioni e delle deroghe alla normativa in materia di protezione dati a tutela della libertà di espressione e di informazione 527 - 7. Il diritto all'oblio tra giurisprudenza della Corte europea ed art. 17 del Regolamento 529 - 8. Diritto alla rettifica e istituto della rettifica 533 - 9. Brevi osservazioni conclusive 536

539 *I dati personali di natura religiosa, tra scelte individuali e trattamento confessionale collettivo*
Alberto Fabbri

1. Aspetti inclusivi 539 - 2. L'evoluzione della normativa 544 - 3. La disciplina attuale e la sua *ratio* 546 - 4. La previsione di «idonee garanzie» e loro natura 552 - 5. Le autorizzazioni del Garante 557 - 6. La nuova regolamentazione europea, spunti critici 559 - 7. Strutture di natura religiosa e rilevanza statale 564 - 8. Ambiti di applicazione del diritto alla protezione dei dati religiosi, tra vecchi e nuovi scenari 567

573 *Profilazione e trattamento dei dati personali*
Olga Sesso Sarti

1. La profilazione e il trattamento dei dati personali tra vecchie e nuove sfide 573 - 2. Il quadro europeo ed interno prima del Regolamento UE 2016/679 579 - 3. La Raccomandazione del Consiglio d'Europa e il Regolamento europeo: due testi a confronto e un primo richiamo al «rapporto» tra profilazione e processo decisionale automatizzato 585 - 4. I principi che riguardano il trattamento di profilazione e i diritti dell'interessato nei diversi ambiti normativi. Il diritto ad essere informati ed il diritto di accesso: spunti di riflessione sul richiamo «alla logica utilizzata» 589 - 5. I diritti di rettifica, di cancellazione e di limitazione del trattamento 596 - 6. I riflessi della profilazione sul diritto alla portabilità dei dati 598 - 7. Il diritto di opposizione 600 - 8. Il processo decisionale automatizzato e la profilazione 603 - 9. Profilazione e sicurezza. La valutazione di impatto sulla protezione dei dati e la consultazione preventiva. Il ruolo del *data protection officer* 613 - 10. Il lungo cammino della profilazione nei provvedimenti del Garante per la protezione dei dati personali. Il richiamo al contesto europeo: i pareri del WP29. Uno sguardo d'insieme 619

629 *I trattamenti nel settore bancario, finanziario e assicurativo*
Chiara Alvisi

Premessa 629 - Sezione I - *I trattamenti nel settore bancario e finanziario* 631 - 1. Protezione dei dati personali e segreto bancario 631 - 2. Tipologie di dati

trattati in ambito bancario e finanziario 636 - 3. La base giuridica del trattamento bancario e finanziario dei dati personali 640 - 4.Tipologie di trattamenti in ambito bancario e finanziario che si legittimano su basi giuridiche diverse dal consenso 641 - 5. (*segue*) I trattamenti dei gestori e dei partecipanti ai sistemi di informazioni creditizie. La Centrale dei Rischi presso la Banca d'Italia. I Sistemi di informazioni creditizie privati 650 - 6. Il consenso dell'interessato 666 - 7. I trattamenti illeciti di dati bancari e finanziari 668 - 8. *Accountability* e responsabilità degli intermediari finanziari 670 - 9. (*segue*) I codici di condotta 676
SEZIONE II - *Il trattamento dei dati personali in ambito assicurativo* 678 - 1. Il problema della catena assicurativa: obblighi informativi, raccolta del consenso, ripartizione delle responsabilità 678 - 2. Pluralità di interessati 682 - 3. Gli obblighi legali di *disclosure* a carico del contraente e il problema della privacy genetica nelle assicurazioni sanitarie e spese mediche 683 - 4. La profilazione della clientela da parte delle compagnie assicuratrici. Le profilazioni obbligatorie. Trattamenti tramite dispositivo c.d. scatola nera ed *event data recorder* 686
SEZIONE III - *L'esercizio dei diritti riconosciuti all'interessato nei settori bancario ed assicurativo* 693 - 1. Le novità in tema di diritti 693 - 2. Diritto di accesso ai dati personali e portabilità nel settore assicurativo 700 - 3. Diritto di accesso e portabilità nel settore bancario 703

709 *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*
Pietro MILAZZO

1. Gli antecedenti della Direttiva UE 2016/680 709 - 2. La Direttiva UE 2016/680: alcuni profili problematici 722 - 3. Il contenuto della Direttiva: i principi, i diritti dell'interessato, gli obblighi del titolare, la sicurezza dei trattamenti e i trasferimenti dei dati nei Paesi terzi 726 - 4. Il primo impatto della Direttiva UE 2016/680 nell'ordinamento italiano 737

741 *Prospettive de iure condendo della protezione dei dati personali nel settore delle comunicazioni elettroniche, tra Regolamento generale 2016/679 e futuro Regolamento e-Privacy*
Guido SCORZA

1. La privacy nelle comunicazioni elettroniche: un'eccezione che si avvia a diventare la regola 741 - 2. L'ambito di applicazione del Regolamento e-Privacy 745 - 3. La riservatezza delle comunicazioni elettroniche e la conservazione dei dati 752 - 4. La tutela delle informazioni conservate nei dispositivi degli utenti finali 756 - 5. La prestazione del consenso e la centralità dei browser 760 - 6. Privacy, servizi di comunicazione interpersonale e *direct marketing* nel Regolamento e-Privacy 765

771 *Abstract*

INDEX

XVII *Preface*
Paolo AQUILANTI

XXIII *Introduction*

PART ONE
THE EUROPEAN REGULATION
ON THE PROTECTION OF PERSONAL DATA

3 *The Regulation EU/2016/679 and the construction of a uniform European standard model for privacy and data protection*
Licia CALIFANO

1. Origin, legal nature and guarantees for a fundamental right: the protection of personal data 3 - 2. The choice of the self executing instrument and its effects at European and national level 17 - 3. The guiding principles of the new legislation between confirmation of a consolidated model and novelties which strengthen the exercise of the law 24 - 4. The principle of accountability and the shift to preventive protection as a substantial approach to the duties of the controller 34 - 5. The accountability of controller and sanctions 40 - 6. The information-consent scheme between reaffirmation and awareness of intrinsic limits 47

57 *The origins and the context*
Giulio M. SALERNO

1. Brief introduction to the constitutionally delineated relations between our legal system, the EU and the ECHR 57 - 2. The integrated and progressive evolution of European competences and disciplines for the protection and the correct processing of personal data 63 - 3. The role of the Court of Justice of the European Union in regulating the protection of personal data 72 - 4. Some conclusions on the evolution of the constitutional dimension of personal data protection 81

85 *General principles relating to processing of personal data and the rights of data subject*
Carlo Colapietro, Antonio Iannuzzi

1. Background and purposes of the Regulation. The interpretative address function of the recitals 85 - 2. The scope of the Regulation 91 - 3. Definitions: the dynamic concept of personal data 98 - 4. Informational self-determination and the principles of personal data processing 106 - 5. Consent and consent of "digital native" children 115 - 6. The rights of the data subject and their protection 122 - 7. The right to be forgotten 126

137 *Accountability and security of processing*
Simone Calzolaio, Laura Ferola, Valentina Fiorillo, Edoardo Alberto Rossi, Matteo Timiani

1. The effects of the European Regulation on data subjects. Introductory considerations 137 - 2. The controller, the joint controller and the processor 142 - 3. The data protection officer (DPO) 154 - 4. The function of codes of conduct and certifications 162 - 5. Dynamic data protection planning: privacy by design and privacy by default 170 - 6. Dynamic data protection planning: data protection impact assessment and prior consultation 175 - 7. The dynamic model in security of processing: prevention and response to violations 186 - 8. The European model of "cross-border" data protection 195

203 *Protecting the confidentiality of sensitive data: the new European frontiers*
Lorenzo Chieffi

1. Technological innovation and protection of fundamental rights in the latest developments in European law 203 - 2. The role of law in the protection of sensitive data 210 - 3. Sensitive data in the European Regulation 2016/679 214 - 4. (*continuing*) The processing of genetic data 221 - 5. New areas of protection for informational self-determination 226 - 6. Informed consent to the processing of sensitive data 230 - 7. Monitoring the circulation of sensitive data 236 - 8. Regulation of access to sensitive data 242 - 9. Exceptions and derogations from the prohibition on processing of sensitive data 246 - 10. The transfer of sensitive data to third countries. The necessary security standards 252 - 11. Breach of the confidentiality of sensitive data. The sanctioning consequences 255 - 12. Concluding considerations. Prospects for adapting state regulations to the new European regulatory framework 260

267 *6. The independence of the* Garante
Andrea Patroni Griffi

1. A brief premise about supervisory Authorities and the principle of independence: beyond the impartiality of the administration 267 - 2. An independence different from the judicial one. A possible parallelism with constitutional judges or special jurisdictions? 274 - 3. The measures of

independence of supervisory Authorities in the European Data Protection Regulation 2016/679 282 - 4. Measures to ensure the independence of supervisory Authorities in individual national systems 291 - 5. (*continuing*) The choice to constitutionalise in the legal system the guarantee of independence of the supervisory Authority. The case of Greece 301 - 6. The right balance in the choice of guarantors: concluding considerations 304

311 *Regulation EU 2016/679 and employment relations*
Arturo MARESCA, Silvia CIUCCIOVINO, Ilario ALVINO

1. The impact of EU Regulation 2016/679 in the relations between employer and employee 312 - 2. The specialty of protection of workers personal data in the relations with the employer and in the job market 314 - 3. The scope of the principle of accountability of the data controller in the employment relationship between EU Regulation 2016/679 and the general obligation to protect workers as per art. 2087 c.c. 323 - 4. The new organisational dimension of personal data protection: similarities and differences with the organisational dimension of occupational health and safety protection 327 - 5. The new figure of the data protection officer: relationship with the employer and position in the company hierarchy 330 - 6. The principles applicable to the processing of personal data in the employment relationship in the light of EU Regulation 2016/679 334 - 7. The impact of EU Regulation 2016/679 on the Authority's guidelines for the protection of personal data and the indications expressed by the Authority in its guidelines on the processing of personal data in the employment relationship 343 - 8. The new art. 4 l. 300/1970 in the light of EU Regulation 679/2016 345 - 9. The (re)definition and systematization of defensive controls 350 - 10. Conditions for the legitimacy of remote controls: trade union agreement and administrative authorisation 354 - 11. Exemptions reserved for tools used to render work performance and for recording access and attendance 356 - 12. Legitimate controls and usability of acquired data for managing employment relationships 362 - 13. Transparent information to the worker as a condition for the usability of the data collected by the employer 364

367 *Transition to the new system of European data protection sources of law*
Massimo RUBECHI

1. From the Privacy Code to the Regulation: tools and models for implementation and harmonisation 367 - 2. The scope for intervention of State institutional actors: general constraints, necessary and optional measures, the challenge to harmonisation 374 - 3. Implementation in other EU Member States (an outline) 387 - 4. Summary considerations 393

PART TWO
PROTECTION AND SECURITY IN THE MAIN SECTORS OF PERSONAL DATA PROCESSING

397 *Public processing in the age of digitalization and transparency*
Stefano TOSCHEI

1. The changing meaning of the term transparency in national law 397 - 2. Transparency in Community principles and transposing legislation 408 - 3. Fundamental trajectories of personal data protection in our system 413 - 4. The difficult balance between protection of confidentiality and the right to knowingness 417 - 5. The era of digitization of public action, the Big Data phenomenon and the guarantees of the rights involved 430

441 *Personal data concerning health and health care*
Guerino FARES

1. Framing of the theme 441 - 2. The processing of personal data concerning health in Regulation EU/2016/679: definitions 452 - 3. Conditions for the lawfulness of treatment and axiological coordinates of the recitals 455 - 4. The impact of the Regulation on the health system: the scope of Article 9 461 - 5. The pathological plan, between European law and national law: the flaw of "non-processing" 466 - 6. (*continuing*) The flaw of undue processing 474 - 7. Concluding considerations 478

491 *Processing in the field of education and research (scientific, historical, statistical)*
Erik LONGO

1. Introduction 491 - 2. Processing personal data vs. freedom of research 493 - 3. From the 1995 Directive to the Privacy Code 497 - 4. Regulation EU/2016/679: introduction and principle of "purpose limitation" 499 - 5. (*continuing*) Principles and rules applicable to storage of personal data for the public interest, for scientific or historical research or for statistical purposes 501 - 6. Guarantees and derogations applicable to storage of personal data for the public interest, for scientific or historical research or for statistical purpose 503 - 7. Processing of personal data in the field of education 506 - 8. Concluding considerations 507

509 *Processing of personal data and freedom of expression and information*
Marco OROFINO

1. The slow constitutional recognition of the right to privacy and its subsequent attraction to the area of the right to protection of personal data 509 - 2. The impact of new technologies on freedom of expression and the right to protection of personal data and their relationship 516 - 3. The relationship between freedom of expression and information and the right to protection of personal

data in Directive EC/95/46 518 - 4. The relationship between freedom of expression and information and the right to protection of personal data in the Privacy Code 520 - 5. The Garante's "jurisprudence" on the relationship between the right to chronicle and protection of personal data 522 - 6. The new Regulation 2016/679: the regulation of limitations and derogations from data protection regulations to protect freedom of expression and information 527 - 7. The right to be forgotten between the case-law of the European Court and Article 17 of the Regulation 529 - 8. The right to rectification and the rectification 533 - 9. Brief concluding remarks 536

539 *Personal data of religious nature, between individual choices and collective confessional*
Alberto FABBRI

1. Inclusive aspects 539 - 2. Developments in legislation 544 - 3. The current framework and its rationale 546 - 4. The provision of 'appropriate safeguards' and their nature 552 - 5. The Authorisations by the *Garante* 557 - 6. The new European regulation, critical observations 559 - 7. Religious structures and state importance 564 - 8. Areas of application of the right to religious data protection, between old and new scenarios 567

573 *Profiling and processing of personal data*
Olga SESSO SARTI

1. Profiling and processing of personal data between old and new challenges 573 - 2. The European and internal framework before the European Regulation 579 - 3. The Council of Europe Recommendation and the European Regulation: two texts in comparison and a first note on the relation between profiling and automated decision-making 585 - 4. Principles relating to profiling and the rights of the data subject in the different regulatory frameworks. The right to be informed and the right of access: some ideas about "the logic involved" 589 - 5. The rights of rectification, erasure and restriction of processing 596 - 6. Reflections of profiling on the right to data portability 598 - 7. The right to object 600 - 8. Automated decision-making and profiling 603 - 9. Profiling and security. The data protection impact assessment and prior consultation. The role of the *data protection officer* 613 - 10. The long path of profiling in the measures of the Garante the european context: the opinions of the WP29. An overview 619

629 *Processing of personal data in the banking, financial and insurance sector*
Chiara ALVISI

Premise 629 - SECTION I - *Processing in the banking and financial sector* 631 - 1. Protection of personal data and bank secrecy 631 - 2. Types of data processed in the bank and financial sector 636 - 3. The legal basis for the banking and financial processing of personal data 640 - 4. Types of processing in the banking and financial sector which are based on legal bases other than

consent 641 - 5. (*continuing*) Processing by operators and participants in credit information systems. The Central Risk Office at the Bank of Italy. The private credit information systems 650 - 6. The consent of the data subject 666 - 7. Illegal processing of banking and financial data 668 - 8. Accountability and liability of financial intermediaries 670 - 9. (*continuing*) Codes of conduct 676
SECTION II - *The processing of personal data in the insurance sector* 678 - 1. The problem of the insurance chain: information requirements, consent building, distribution of responsibilities 678 - 2. Multiple data subjects 682 - 3. Policyholder's legal disclosure obligations and the issue of genetic privacy in health insurance and medical expenses 683 - 4. Customer profiling by insurance companies. Compulsory profiling. Processing through black box device and event data recorder 686
SECTION III - *The exercise of the rights granted to the data subject in the bank and insurance sectors* 693 - 1. The main news concerning data subject's rights 693 - 2. The right of access to personal data and the right to portability in the insurance sector 700 - 3. The right of access and portability in the bank sector 703

709 *Directive EU 2016/680 and the protection of personal data in the field of public security and criminal justice*
Pietro MILAZZO

1. Background of Directive EU 2016/680 709 - 2. Directive EU 2016/680: some problematic profiles 722 - 3. The content of the Directive: the principles, the rights of the data subject, the obligations of the data controller, the security of the processing and transfer of data in third countries 726 - 4. The first impact of Directive EU 2016/680 on the Italian legal system 737

741 *Perspectives de iure condendo of the protection of personal data in the electronic communications sector, between General Regulation 2016/679 and future Regulation e-Privacy*
Guido SCORZA

1. Privacy in electronic communications: an exception that starts to become the rule 741 - 2. The scope of the ePrivacy Regulation 745 - 3. Confidentiality of electronic communications and data retention 752 - 4. Protection of information stored in end-users' devices 756 - 5. Consent and browser centrality 760 - 6. Privacy, interpersonal communication services and direct marketing in the e-Privacy Regulation 765

771 *Abstract*

Arturo Maresca, Silvia Ciucciovino, Ilario Alvino*

Regolamento UE 2016/679 e rapporto di lavoro

SOMMARIO: 1. L'impatto del Regolamento UE 2016/679 nel campo dei rapporti di lavoro. – 2. I tratti di specialità della protezione dei dati personali dei lavoratori nel rapporto di lavoro e nel mercato del lavoro. – 3. La portata del principio di responsabilizzazione del titolare del trattamento nel rapporto di lavoro tra Regolamento UE 2016/679 e obbligo generale di protezione dei lavoratori di cui all'art. 2087 c.c. – 4. La nuova dimensione organizzativa della protezione dei dati personali: analogie e differenze con la dimensione organizzativa della tutela della salute e sicurezza sul lavoro. – 5. La figura del *data protection officer*: rapporto con il datore di lavoro e posizione nella gerarchia aziendale. – 6. I principi applicabili al trattamento dei dati personali nel rapporto di lavoro alla luce del Regolamento UE 2016/679. – 7. L'impatto del Regolamento UE 2016/679 sugli orientamenti dell'Autorità per la protezione dei dati personali e sulle indicazioni da questa espresse nelle linee guida in materia di trattamento dei dati personali nel rapporto di lavoro. – 8. Il nuovo art. 4, L. 300/1970 alla luce del Regolamento UE 2016/679. – 9. La (ri)definizione e sistematizzazione dei c.d. controlli difensivi. – 10. Condizioni di legittimità dei controlli a distanza: l'accordo sindacale e l'autorizzazione amministrativa. – 11. Le esenzioni riservate agli strumenti utilizzati per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze. – 12. Controlli legittimi e utilizzabilità dei dati acquisiti per la gestione del rapporto di lavoro. – 13. L'informazione trasparente al lavoratore come condizione per l'utilizzabilità dei dati raccolti dal datore di lavoro.

* Arturo Maresca è Professore ordinario di Diritto del lavoro nella Sapienza - Università di Roma; Silvia Ciucciovino è Professore ordinario di Diritto del lavoro nell'Università degli Studi Roma Tre; Ilario Alvino è Professore aggregato di Diritto del lavoro nell'Università degli Studi Roma Tre. Il presente lavoro è frutto della riflessione comune e della collaborazione dei tre Autori; tuttavia, i paragrafi da 1 a 5 sono stati redatti da Silvia Ciucciovino, i paragrafi 6 e 7 sono stati redatti da Ilario Alvino e i paragrafi da 8 a 13 sono stati redatti da Arturo Maresca.

1. *L'impatto del Regolamento UE 2016/679 nel campo dei rapporti di lavoro*

Il trattamento dei dati personali nell'ambito del rapporto di lavoro presenta peculiarità tali da attenuare la forza autoapplicativa della fonte regolamentare europea, normalmente dotata di efficacia diretta orizzontale.

L'art. 88 del Regolamento UE 2016/679, infatti, consente agli Stati membri di prevedere con legge o tramite contratti collettivi «norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro». Quindi per tutti i profili del rapporto di lavoro – nella fase di assunzione, esecuzione e cessazione – è consentito agli Stati membri di apportare modifiche e adattare la disciplina del Regolamento al contesto nazionale.

Non è irrilevante che il riconoscimento della specialità della materia lavoristica sia ricollegato non soltanto ad esigenze di tutela e protezione dei lavoratori (parità e diversità sul posto di lavoro, salute e sicurezza, godimento dei diritti e vantaggi sul posto di lavoro), ma parimenti ad esigenze gestionali e di difesa degli interessi del datore di lavoro (pianificazione e organizzazione del lavoro, protezione della proprietà del datore di lavoro e dei suoi clienti, cessazione dei rapporti di lavoro).

Gli interessi peculiari di cui sono portatrici entrambe le parti del rapporto di lavoro giustificano la possibilità di filtrare la diretta applicazione del Regolamento attraverso opportuni interventi di adattamento delle regole.

Non si tratta di facoltà di deroga. Sembra chiaro, infatti, che l'adozione di discipline «più specifiche» consenta un adattamento, una declinazione, una puntualizzazione delle norme europee comunque volta a garantire («assicurare») la protezione dei diritti e delle libertà con riguardo al trattamento dei dati dei lavoratori dipendenti. La finalità delle eventuali discipline nazionali non può, quindi, essere diretta ad immettere negli ordinamenti nazionali un'attenuazione delle garanzie per i lavora-

tori se da ciò dovesse scaturire una riduzione, sul piano sostanziale, dei diritti e delle libertà previste dal Regolamento.

L'adattamento alle peculiarità tipiche connesse alla gestione dei rapporti di lavoro, d'altro canto, è molto ragionevole e diretto ad agevolare il trattamento di una rilevante mole di dati, molti dei quali anche sensibili, che con continuità tutti i datori di lavoro, pubblici e privati, a prescindere dalla dimensione aziendale, si trovano inevitabilmente a dover trattare per ragioni contrattuali, previdenziali, assicurative, fiscali e di salute e sicurezza.

L'adozione a livello nazionale di discipline legali o contrattuali collettive sostitutive o specificative del Regolamento è ovviamente puramente eventuale, come si evince dal verbo «possono prevedere» utilizzato dall'art. 88 nel riferirsi all'intervento degli Stati membri su questa materia. Ne consegue che, in mancanza, di normative specifiche, troverà immediata e diretta applicazione la disciplina del Regolamento. Chiaro è, inoltre, che le discipline nazionali sono quelle adottate successivamente all'entrata in vigore del Regolamento e specificative di questo; mentre non si tratta di una norma di salvezza delle discipline nazionali precedenti al Regolamento, che devono essere passate al vaglio di compatibilità/conformità con la normativa regolamentare.

Tra le discipline previgenti, ovviamente, v'è il D.lgs. 30 giugno 2003 n. 196 – Codice in materia di protezione dei dati personali (nel prosieguo per brevità anche Codice), che non è abrogato dal Regolamento e rimane in vigore, almeno per le parti che non formano oggetto di nuova regolazione da parte della fonte europea, come meglio si vedrà per i singoli aspetti nel prosieguo.

È dato agli Stati membri un termine stringente entro il quale dare seguito alla possibilità di dettare discipline nazionali specifiche in materia di protezione dei dati personali dei lavoratori diverse da quelle immediatamente previste dal Regolamento, come si evince dal termine entro il quale adempiere al relativo obbligo di notifica alla Commissione delle disposizioni di legge adottate ai sensi dell'art. 88, paragrafo 1, fissato al 25 maggio 2018, salvo comunque l'obbligo di comunicazione tempestiva di ogni successiva modifica (art. 88, paragrafo 3).

Riguardo alla fonte contrattuale collettiva, appare difficile immaginare come ordinamenti nazionali, quali il nostro, dove i contratti collettivi sono privi di efficacia soggettiva *erga omnes* possano utilmente dare seguito alla previsione di cui all'art. 88, paragrafo 1, se non in contesti particolari e settorialmente; mentre sembra molto più appropriata all'uopo una fonte legislativa, magari frutto di intese concertative con le parti sociali.

Riguardo al livello di contrattazione collettiva, il *considerando* 155 fa espresso riferimento anche agli «accordi aziendali», fonte questa che comunque poteva ritenersi pienamente abilitata anche soltanto in base al generico riferimento operato dall'art. 88 ai contratti collettivi senza ulteriori specificazioni, che non consente evidentemente di escludere alcun livello contrattuale.

La *ratio* di una disciplina nazionale di specificazione è chiaramente quella di agevolare il trattamento della grande massa di dati personali che qualsiasi datore di lavoro pubblico e privato necessariamente si trova a trattare nella quotidiana gestione dei rapporti di lavoro, anche per adempiere ad obblighi stabiliti dalla legge o da contratti collettivi, così come per organizzare e gestire in modo efficiente il personale, ma anche per garantire trattamenti che tengano adeguatamente conto di particolari elementi soggettivi riferiti a fattori potenzialmente discriminatori o comunque legati a elementi di diversità oppure alla salute del lavoratore.

In ogni caso appare scarsamente realistico nell'attuale particolare congiuntura politica caratterizzata da elevata instabilità, che effettivamente il nostro Paese si avvalga in tempi così brevi della facoltà dischiusa dal Regolamento di dotarsi di una disciplina legislativa nazionale *ad hoc* in materia di trattamento dei dati dei lavoratori dipendenti.

2. *I tratti di specialità della protezione dei dati personali dei lavoratori nel rapporto di lavoro e nel mercato del lavoro*

La specialità della materia lavoristica per ciò che riguarda la tutela della riservatezza, il trattamento e la protezione dei dati non è certo una novità. Norme specifiche a protezione della sfera personale del lavoratore da intrusioni indebite del datore di lavoro nel rapporto di lavoro subordinato sono poste a presidio della libertà e dignità del lavoratore[1].

Basti pensare alle norme speciali che regolano il divieto di indagine sulle opinioni politiche, religiose e sindacali e su fatti non rilevanti ai fini

[1] Sul rapporto in generale tra normativa lavoristica e legislazione in materia di privacy v., tra gli altri: P. TULLINI (a cura di), *Web e lavoro*, Torino 2017; ID. (a cura di), *Tecnologie della telecomunicazione e riservatezza nel rapporto di lavoro*, Padova 2010; P. CHIECO, Privacy *e lavoro*, Bari 2000, 334; M. AIMO, *Privacy, libertà di espressione e rapporto di lavoro*, Napoli 2003; A. TROJSI, *Il diritto del lavoratore alla protezione dei dati personali*, Torino 2013; F. CARINCI, R. DE LUCA TAMIAJO, P. TOSI, T. TREU, *La tutela della privacy del lavoratore*, Torino 2000; A. SITZIA, *Il diritto alla privatezza nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova 2013.

della valutazione dell'attitudine professionale dei lavoratori (art. 8, L. 20 maggio 1970, n. 300); il divieto di effettuare accertamenti sulla salute del lavoratore e i limiti posti al controllo della idoneità fisica del lavoratore (art. 5, L. 300/1970) e alla sorveglianza sanitaria (D.lgs. 9 aprile 2008, n. 81); i limiti alle visite di controllo personale e a distanza mediante impianti audiovisivi (artt. 2, 3 e 4, L. 300/1970).

Ma alla medesima finalità di preservazione della sfera intima e personale dei lavoratori è indirizzata la normativa che vieta la discriminazione per motivi politici, sindacali, religiosi, di orientamento sessuale, legati alla razza e all'origine etnica, alle convinzioni personali e che pone quindi indirettamente un limite all'acquisizione ed al trattamento da parte del datore di lavoro di dati atti a rivelare simili fattori potenzialmente discriminatori (art. 15, L. 300/1970; D.lgs. 9 luglio 2003, n. 215; D.lgs. 9 luglio 2003, n. 216).

Peraltro la specificità della materia giuslavoristica è sempre stata riconosciuta dal legislatore della privacy che, infatti, tiene ferme le disposizioni dello Statuto dei lavoratori in materia di controllo a distanza (artt. 114, Codice; ma, già prima, l'art. 43 L. 675/1996), riconoscendo a queste una sorta di primato in funzione della specialità della materia lavoristica rispetto alle norme generali sulla protezione dei dati, ma anche implicando un non semplice incastro tra normativa generale in materia di protezione dei dati personali e disposizioni speciali giuslavoristiche.

La necessità connesse alla gestione dei rapporti di lavoro giustifica comunque alcune aree di esenzione legale dall'applicazione di limiti altrimenti generalmente applicabili nel trattamento dei dati personali.

Si può rammentare in proposito che il trattamento di dati sensibili riferiti all'adesione sindacale è esentato dall'applicazione delle garanzie (consenso scritto dell'interessato) di cui all'art. 26, comma 1, Codice (art. 26, comma 3, lett. b, Codice); mentre i dati sensibili riferiti ai lavoratori sono trattabili anche in mancanza di consenso sulla base dell'autorizzazione del Garante quando necessario per adempiere a specifici obblighi o compiti previsti dalla legge o altra fonte per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro, previdenza e assistenza (art. 26, comma 4, lett. d). Autorizzazione che ormai, di prassi, assume la forma di autorizzazione generale rilasciata annualmente dall'Autorità.

Si aggiunga che il Codice privacy qualifica espressamente di «rilevante interesse pubblico», e quindi come tali idonee a consentire il trattamento dei dati sensibili, altrimenti vietato, le finalità di gestione del rapporto di lavoro e di integrazione sociale dello straniero, dell'immigrato o

del profugo (art. 64, comma 2, lett. c); così come sono qualificate di «rilevante interesse pubblico» le attività svolte dal soggetto pubblico attinenti al supporto al collocamento e all'avviamento al lavoro (art. 73, comma 2, lett. i) e, più in generale, le attività svolte per finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato (art. 112).

A parte le disposizioni di espressa esenzione appena menzionate, le disposizioni speciali dettate in ambito giuslavoristico non valgono certo a restringere il campo di applicazione della normativa in materia di protezione dei dati personali e quindi si aggiungono a questa. In tale contesto al difficile bilanciamento tra esigenze operative e gestionali, da un lato, ed esigenze di protezione dei dati dei lavoratori dall'altro, sono dedicati i numerosi atti emanati dal Garante per risolvere singole questioni o per fornire linee guida di condotta o per fornire pareri sull'adozione di atti legislativi e regolamentari in materia di gestione del rapporto di lavoro o di funzionamento del mercato del lavoro.

Bisogna notare che la normativa relativa al funzionamento del mercato del lavoro è in continua evoluzione e numerose previsioni specifiche implicano il trattamento dei dati personali dei lavoratori da parte dei molteplici soggetti deputati ai servizi al lavoro e alle politiche attive del lavoro.

Su questo versante occorre innanzitutto ricordare l'art. 10, D.lgs. 10 settembre 2003, n. 276 che estende agli operatori del mercato del lavoro i limiti antidiscriminatori e i divieti di indagine su fatti non rilevanti ai fini dell'occupazione già previsti per i datori di lavoro.

L'art. 10 vieta, infatti, alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati «di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento dell'attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. È altresì fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti

alle loro attitudini professionali e al loro inserimento lavorativo». Il secondo comma aggiunge che le disposizioni di cui al primo comma non possono in ogni caso impedire «di fornire specifici servizi o azioni mirate per assistere le categorie di lavoratori svantaggiati nella ricerca di una occupazione».

Ulteriori disposizioni sono dettate con riferimento ai flussi informativi che debbono caratterizzare l'informatizzazione dell'incontro tra domanda e offerta di lavoro e la costituzione della borsa continua nazionale del lavoro (artt. 15 e 16, D.lgs. 276/2003)[2] e del sistema informativo unitario delle politiche del lavoro (art. 13, D.lgs. 14 settembre 2015, n.150), indispensabili al buon funzionamento del mercato del lavoro.

L'art. 6 del D.M. 13 ottobre 2004 intitolato al «Trattamento dei dati relativi all'incontro domanda offerta» estende il divieto di cui all'art. 10, D.lgs. 276/2003, nei confronti di tutti i soggetti che accedono alla borsa continua nazionale del lavoro.

La questione della protezione dei dati dei lavoratori in questo campo è molto delicata in quanto si deve tener conto dell'esigenza di carattere pubblicistico di garantire la libera accessibilità della borsa continua nazionale del lavoro da parte dei lavoratori e delle imprese e la necessità della libera consultabilità della stessa da un qualunque punto della rete (cfr. art. 15, comma 2, D.lgs. 276/2003). Ciò anche in relazione al principio di continua e diretta alimentazione della borsa da parte dei singoli lavoratori e delle imprese e dell'obbligo posto in capo agli operatori pubblici e privati, accreditati o autorizzati, di conferire alla borsa continua nazionale del lavoro i dati acquisiti, in base alle indicazioni rese dai lavoratori e a quelle rese dalle imprese riguardo l'ambito temporale e territoriale prescelto (art. 15, comma 3, D.lgs. 276/2003).

Si noti peraltro che la definizione, raccolta, comunicazione e diffusione dei dati deve permettere «la massima efficienza e trasparenza del processo di incontro tra domanda e offerta di lavoro, assicurando anche

[2] Cfr. il D.M. 13 ottobre 2004 istitutivo della borsa nazionale continua del lavoro, il cui art. 6 riguarda specificamente il trattamento dei dati relativi all'incontro domanda offerta. Stabilisce che i titolari del trattamento dei dati contenuti nella borsa continua nazionale del lavoro sono il Ministero del lavoro, le regioni e gli operatori. Inoltre i soggetti ai quali è consentita la consultazione della borsa continua nazionale del lavoro utilizzano le informazioni e trattano solo i dati pertinenti all'instaurazione di un rapporto di lavoro. Sugli standard tecnici della borsa continua nazionale del lavoro e dei relativi flussi informativi si v. anche D.M. 30 ottobre 2007 che ha sostituito gli allegati del D.M. 13 ottobre 2004. Per l'interferenza con la normativa sulla privacy si v. anche il Parere del Garante sullo schema di decreto in materia di «Borsa continua nazionale del lavoro» del 3 settembre 2004 [doc. web n. 1341395].

gli strumenti tecnologici necessari per la raccolta e la diffusione delle informazioni presenti nei siti internet ai fini dell'incontro tra domanda e offerta di lavoro» (art. 15, comma 4, lett. a) D.lgs. 276/2003).

L'art. 16, comma 2, D.lgs. 276/2003 stabilisce comunque che il trattamento dei dati personali ed i flussi informativi della borsa continua del lavoro debbano avvenire nel rispetto dei diritti dell'interessato previsti dalla normativa sulla privacy (all'epoca il riferimento era alle disposizioni di cui «all'art. 31, comma 2, della L. 31 dicembre 1996, n. 675»). E quindi occorre che gli standard tecnici delle soluzioni informatiche adottate siano configurati in modo tale da tener conto dei diritti dell'interessato con riferimento alla protezione dei dati personali e più in generale dei principi del Codice.

Va aggiunto che ad esigenze di massima trasparenza e leggibilità dei dati riferiti alle schede anagrafiche professionali dei lavoratori è indirizzata da ultimo la previsione dell'art. 13, comma 3, D.lgs. 150/2015 relativa al Sistema informativo unitario delle politiche del lavoro e che stabilisce che «allo scopo di certificare i percorsi formativi seguiti e le esperienze lavorative effettuate, l'ANPAL definisce apposite modalità di lettura delle informazioni» contenute nelle schede anagrafiche e professionali dei lavoratori «a favore di altri soggetti interessati, nel rispetto del diritto alla protezione dei dati personali di cui al D.lgs. 30 giugno 2003, n. 196».

Dunque si tratta pur sempre di tener conto dei diritti e principi della protezione dei dati personali nel dare attuazione ai principi che devono presiedere ai flussi informativi necessari al buon funzionamento del mercato del lavoro, assicurando la circolazione, accessibilità, trasparenza, interoperabilità delle banche dati.

In tale contesto si può ritenere comunque lecito, ai sensi degli artt. 73, comma 2, lett. i), e 112 del Codice, il trattamento dei dati sensibili dei lavoratori da parte dei soggetti pubblici in quanto connesso al supporto al collocamento e all'avviamento al lavoro ed a finalità di instaurazione di rapporti di lavoro.

In merito all'applicazione della normativa sulla protezione dei dati personali nel campo dei rapporti di lavoro, oggi il Regolamento va oltre quanto già acquisito con il Codice e, con una disposizione di carattere generale (art. 9), stabilisce che, quando si tratta di esercitare diritti, poteri, obblighi in materia di diritto del lavoro e sicurezza e protezione sociale, non vale il divieto di trattamento dei dati personali sensibili che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, così come il trattamento di dati genetici e dati biometrici (inseriti dal Regolamento nell'alveo dei dati sen-

sibili) intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

È esentato dal divieto generale altresì il trattamento reso necessario da finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (art. 9, paragrafo 2, lett. h), purché tali dati siano trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale. Il riferimento alla «capacità lavorativa» del dipendente, estrapolata dal contesto, potrebbe essere inteso come trattamento di dati riferiti anche al rendimento individuale, alla capacità relazionale, ad altre caratteristiche soggettive del lavoratore nell'esercizio della propria mansione; tuttavia la connotazione evidentemente sanitaria della disposizione fa preferire un'interpretazione più limitata, dove la «capacità» sembra piuttosto da intendere come idoneità psicofisica del lavoratore rispetto alla mansione da svolgere.

Il Regolamento prevede inoltre che gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento dei dati biometrici (art. 9, paragrafo 4), che – com'è noto – sempre più frequentemente trovano impiego anche nel campo della gestione dei rapporti di lavoro, ad esempio per rilevare presenze, accessi o per identificare e autorizzare determinati lavoratori a fare ingresso in determinate zone dell'impresa oppure ad utilizzare determinati strumenti di lavoro.

Al di là di queste disposizioni specifiche che tengono conto dei tratti di specialità della materia lavoristica, è possibile rinvenire nel principio di liceità (art. 6, paragrafo 1, lett. f), Regolamento) la base generale di legittimazione del trattamento dei dati dei lavoratori da parte del datore di lavoro, in quanto ciò è necessario per il perseguimento del legittimo interesse del titolare del trattamento, ossia del datore di lavoro, all'esercizio dei suoi poteri tipici e alla gestione del rapporto, pur nel bilanciamento con gli interessi, i diritti e le libertà fondamentali del lavoratore.

Il punto semmai è proprio questo, cioè il bilanciamento da realizzare di volta in volta tra i due concorrenti interessi – economico/organizzativi del datore di lavoro e alla riservatezza del lavoratore – muovendo però dalla premessa che il trattamento dei dati dei lavoratori è lecito nella misura in cui risulta necessario al perseguimento del legittimo interesse del datore di lavoro a gestire i rapporti di lavoro. Dunque, non è in discussione l'*an*, ma semmai il *quomodo* del trattamento dei dati, ovvero i limiti che lo devono caratterizzare.

Per quanto riguarda l'impatto del Regolamento sul quadro normativo

previgente in materia di protezione dei dati dei lavoratori, si può dire che, sul piano dei principi sostanziali della raccolta e trattamento dei dati, il Regolamento apparentemente si pone in linea di massima in continuità con il Codice, ribadendone i principi di base (liceità, correttezza, trasparenza, necessità), non senza apportare alcune specificazioni e innovazioni.

Se, però, ci si solleva ad un piano di valutazione più complessivo e sistematico, è possibile cogliere una prospettiva generale molto più avanzata del passato, in quanto nel Regolamento risalta in modo sicuramente più incisivo la configurazione della protezione dei dati personali come diritto fondamentale della persona e come tale incidente sulla sfera della dignità umana[3].

Come è stato opportunamente notato dalla dottrina[4], questa più avanzata configurazione è certamente tributaria dell'apporto interpretativo fornito dalla Corte di Giustizia negli ultimi decenni; che ha favorito la progressiva evoluzione della concezione a livello europeo del trattamento come presidio a salvaguardia dei diritti fondamentali. Non a caso il diritto ad un trattamento secondo il principio di lealtà, per finalità determinate e con il consenso dell'interessato è previsto anche dall'art. 8 della Carta dei diritti fondamentali di Nizza.

Guardando alla sfera dei rapporti di lavoro, se il bene/interesse in gioco, come conferma il quadro normativo vigente – anche in relazione alle nuove ed enormi potenzialità di raccolta e trattamento consentite dall'evoluzione tecnologica – riguarda in modo progressivamente crescente la persona del lavoratore, allora si comprende come esso si collochi tra i diritti e le libertà fondamentali e reclami strumenti di tutela adeguati anche nell'ambito del rapporto di lavoro.

A ben vedere questo diritto si avvicina molto, per la sua configurazione sostanziale e per le modalità di tutela disegnate dal legislatore, al diritto alla salute e sicurezza sul lavoro. Come questo, anche il diritto alla riservatezza e alla autodeterminazione informativa si configura come un diritto personalissimo del lavoratore attinente alla sfera della libertà e della personalità morale dello stesso. Ne consegue una dimensione e una titolarità eminentemente individuale ed inalienabile dei relativi diritti, che, in effetti, mal si prestano ad essere sintetizzati dall'azione sindacale, almeno nella sua accezione tradizionale.

[3] V. L. Califano in questo *Volume*; Id., *Privacy: affermazione e pratica di un diritto fondamentale*, Roma 2016.

[4] V. C. Colapietro, A. Iannuzzi in questo *Volume*; Id., *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Dir. lav. rel. ind.*, 2017, 439 ss.

Rispetto all'interesse sindacale, che notoriamente costituisce la sintesi degli interessi di una pluralità di lavoratori di cui il sindacato è esclusivo titolare, nel caso della riservatezza (così come della sicurezza) si può fondatamente ritenere che titolare dell'interesse rimanga esclusivamente il singolo lavoratore e che le strutture di rappresentanza sindacale difficilmente saranno in grado di sintetizzare, con mediazioni tipiche dell'azione sindacale, gli interessi di tutti i lavoratori rappresentati su questo versante, poiché a ben guardare si tratta di rappresentare una pluralità di interessi individuali non comprimibili e non negoziabili.

Forse questa difficoltà ontologica può contribuire a spiegare il perché il legislatore anche nella recente riforma dell'art. 4, L. 300/1970, sulla quale ci soffermeremo più avanti, abbia in larga misura sganciato la tematica dei limiti al controllo a distanza dei lavoratori dall'orbita dell'autorizzazione sindacale, per riportarla su un terreno più consono alla natura squisitamente personale del diritto in esame, quale è il rispetto del principio di informazione trasparente e più in generale il rispetto dei principi che presiedono alla riservatezza e protezione dei dati personali.

In tale contesto è razionale e del tutto consequenziale che nel nuovo quadro venutosi a delineare, arbitro del corretto esercizio dei poteri datoriali di controllo sia, non tanto il sindacato, quanto piuttosto il Garante.

Fatte queste premesse di carattere generale, venendo a considerare più specificamente l'impatto del Regolamento sui singoli principi che devono presiedere al trattamento dei dati, si può osservare come le corrispondenti previsioni del Codice risultano ormai assorbite dalla puntuale elencazione dei «principi applicabili al trattamento dei dati personali» effettuata dall'art. 5 del Regolamento. Principi che precisamente consistono nella «liceità, correttezza e trasparenza»; nella «limitazione della finalità»; nella «minimizzazione dei dati»; nell'«esattezza»; nella «limitazione della conservazione»; nell'«integrità e riservatezza».

Questi principi si connettono poi ad una sorta di super principio, che tutti li comprende, affermato dallo stesso art. 5, paragrafo 2, del Regolamento che è quello della «responsabilizzazione» del titolare del trattamento, su cui si tornerà più diffusamente nel paragrafo successivo.

Pur nella continuità con il passato, il Regolamento introduce comunque nuovi diritti sostanziali alcuni dei quali, nella gestione del rapporto di lavoro, appaiono di particolare rilievo, attesa la crescente mobilità tra impieghi cui sono destinati i lavoratori nelle attuali e future dinamiche del mercato del lavoro. Si tratta del diritto alla cancellazione, anche detto diritto all'oblio (art. 17) – frutto di una concezione molto più evoluta del diritto all'autodeterminazione informativa dell'interessato – nonché del di-

ritto alla portabilità dei dati (art. 20), con conseguente integrale o parziale possibilità per il lavoratore di ottenere il trasferimento da un titolare a un altro titolare dei propri dati senza impedimenti.

Si pensi agli importanti riflessi che siffatta previsione è destinata ad avere nella successione tra impieghi o tra diversi status soggettivi nel mercato del lavoro, così come nei fenomeni di esternalizzazione e integrazione collaborativa tra imprese (reti, gruppi, appalti) che implica anche il distacco e la circolazione dei lavorati tra imprese diverse.

Sotto il profilo dei rapporti con le pp.aa. e con gli operatori del mercato del lavoro questo implica anche che la gestione del portafoglio delle competenze, delle esperienze, ecc. debba essere effettuato con cautele compatibili con i principi del Regolamento.

Quanto alle modalità di raccolta e trattamento, il Regolamento apporta alcune modifiche agli adempimenti già previsti dal Codice privacy riferiti all'informativa, al consenso, al diritto di accesso, alla nomina del responsabile esterno.

Dal punto di vista del corretto adempimento degli obblighi datoriali vengono introdotte nuove prescrizioni come l'obbligo di prova, l'obbligo di protezione dei dati già dalla progettazione, l'obbligo di tenuta di un registro dei trattamenti svolti, l'obbligo di notifica delle violazioni all'interessato e al Garante, l'obbligo di valutare l'impatto dei trattamenti dei dati sulla privacy che non mancheranno di esplicare un impatto notevole nelle prassi gestionali ed amministrative di tutti i datori di lavoro.

Come meglio si vedrà nei paragrafi successivi è, comunque, sul piano dei modelli organizzativi e gestionali della protezione dei dati che il Regolamento promette il maggiore impatto rispetto alla normativa preesistente. Comporta infatti un'epocale evoluzione dell'approccio sostanziale al tema della tutela della riservatezza, segnando il passaggio da un modello statico ad un modello dinamico di protezione dei dati, così come il passaggio da una concezione della protezione per così dire prescrittiva e tecnica ad una concezione olistica, organizzativa e procedurale della tutela della riservatezza.

3. *La portata del principio di responsabilizzazione del titolare del trattamento nel rapporto di lavoro tra Regolamento UE 2016/679 e obbligo generale di protezione dei lavoratori di cui all'art. 2087 c.c.*

Come messo in luce nei capitoli introduttivi del presente volume, una delle principali innovazioni apportate dal Regolamento concerne il principio di responsabilizzazione del titolare che, per ciò che in questa sede rileva, determina una dilatazione crescente dell'obbligazione datoriale di protezione dei dati e della riservatezza nei confronti dei lavoratori.

La responsabilizzazione del titolare del trattamento, spesso ma non necessariamente coincidente con il datore di lavoro, è declinata in modo onnicomprensivo e rimessa alla valutazione appropriata dello stesso soggetto obbligato. Ne discende la difficoltà di configurare aprioristicamente le condotte dovute, essendo queste in molta parte rimesse alla valutazione preliminare e continua del titolare del trattamento.

Dal combinato disposto degli artt. 5 e 24 del Regolamento si evince, infatti, che il criterio della responsabilizzazione riguarda il rispetto di tutti i principi informatori del trattamento dei dati e comporta a carico del titolare una valutazione preventiva del contesto e delle finalità del trattamento, della probabilità e gravità dei rischi e, in funzione di questi elementi, comporta l'adozione di politiche adeguate in materia di protezione dei dati, oltre che di misure tecniche ed organizzative appropriate per garantire, ed essere in grado di dimostrare, il trattamento conforme al Regolamento.

Dette misure, inoltre, devono essere continuamente riesaminate ed aggiornate ove necessario, in un processo circolare e continuo che rinnova continuamente la responsabilità del titolare e dei vertici aziendali.

In base all'art. 82 del Regolamento la responsabilità del titolare è generale, riguarda il rispetto, per intero e nulla escluso, di quanto previsto dal Regolamento stesso e determina la risarcibilità del danno cagionato all'interessato, salvo che il titolare non dimostri che tale danno non sia a lui imputabile. Si presume, dunque, l'imputabilità fino a prova contraria. Viceversa, l'ambito della responsabilità risarcitoria del responsabile del trattamento è più circoscritta e vale esclusivamente in relazione agli obblighi specifici direttamente a lui addossati.

Il criterio di imputazione della responsabilità in questo ambito – analogamente a quanto avviene nella sfera della salute e sicurezza sul lavoro – ubbidisce al principio di effettività, in quanto segue la titolarità del trat-

tamento, che a sua volta compete, non certo in base a qualifiche formali o alla collocazione nell'organigramma aziendale, ma ad un criterio di effettività, a colui che ha la capacità giuridica di determinare in concreto le finalità e i mezzi del trattamento dei dati personali (cfr. art. 4, paragrafo 7, Regolamento); cioè a chi è nelle condizioni di poter incidere sul trattamento dei dati.

A motivo di ciò, potrebbe allora non aversi una sicura coincidenza tra il datore di lavoro in senso tecnico giuridico (cioè come parte del contratto di lavoro e capo dell'impresa) ed il titolare del trattamento dei dati ai sensi della normativa sulla privacy. Tanto è vero che può aversi contitolarità del trattamento da parte di più soggetti all'interno della medesima impresa o anche di soggetti appartenenti a realtà imprenditoriali differenti e che presentino le caratteristiche del (con)titolare dei dati, pur se formalmente estranei alla relazione contrattuale con il lavoratore (si pensi, ad esempio, al caso dell'appalto e della posizione del committente rispetto ai dipendenti dell'appaltatore).

Quanto appena detto evidenzia come il principio di responsabilizzazione riguardo al trattamento dei dati in parte si sovrappone ed in parte travalica la posizione di garanzia del datore di lavoro di cui all'art. 2087 c.c. La norma civilistica, per la sua conformazione generale e dinamica, è già di per sé in grado di fondare una responsabilità contrattuale nei confronti dei lavoratori dipendenti a carico del datore di lavoro, onerato di un obbligo di protezione generale, non soltanto della loro integrità psicofisica, ma anche della loro personalità morale e quindi della dignità personale[5].

È noto come nel diritto vivente il richiamo all'art. 2087 c.c., quale fondamento di una posizione di garanzia a contenuto generale del datore di lavoro nei confronti dei lavoratori subordinati, tende a far risalire al datore l'imputazione della responsabilità per violazioni dell'obbligo di protezione anche quando la condotta sia stata tenuta da soggetti diversi dal datore di lavoro, come dirigenti o preposti. Sotto il profilo della responsabilità, infatti, vi è una tendenza all'equiparazione della obbligazione di garanzia con quella di sorveglianza o vigilanza (*culpa in vigilando*), così il datore di lavoro è chiamato comunque a rispondere anche per la condotta di altri sui quali avrebbe dovuto esercitare poteri di organizzazione e controllo. Una dilatazione dell'ambito della responsabilità, questa, che viene proposta in giurisprudenza non soltanto sul piano civile ma anche

[5] L. MONTUSCHI, *Problemi del danno alla persona nel rapporto di lavoro*, in *Riv. it. dir. lav.*, 1994, I, 317 ss.

su quello penale, con criteri di imputazione non sempre rispettosi del principio di personalità[6].

Ai sensi dell'art. 2087 c.c. sul datore di lavoro grava un obbligo giuridico di impedimento, dovendo egli garantire l'incolumità fisica e la salvaguardia della personalità morale dei prestatori di lavoro. Nella norma si radicano doveri di corretta organizzazione primaria, consistenti nel predisporre mezzi e misure adeguate di protezione e doveri di organizzazione secondaria, sotto il profilo della sorveglianza continua sull'adozione di misure preventive da parte di preposti o singoli lavoratori.

La portata precettiva dell'art. 2087 c.c. si coglie quindi su un doppio piano, non soltanto in relazione alla adozione delle singole misure cautelari e preventive da parte del datore di lavoro, ma anche sul piano dell'organizzazione dell'impresa nel suo complesso, attraverso il suo governo, la programmazione, la pianificazione, la gestione.

L'art. 2087 c.c. ha poi una conformazione aperta e dinamica, in quanto chiama il datore di lavoro ad adottare tutte le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie a realizzare un'adeguata tutela. Ciò determina un elevato grado di incertezza riguardo alla portata della condotta dovuta, che assumerà spesso contorni precisi soltanto a posteriori grazie all'interpretazione giudiziale dopo che la violazione e la lesione si è realizzata[7].

La norma civilistica, in una lettura aggiornata ai nostri tempi, contempla al suo interno anche un obbligo di garanzia della riservatezza del lavoratore, in quanto tale riservatezza incide sull'integrità della personalità morale e sulla dignità del lavoratore; diritti, questi, che spetta al datore di lavoro preservare, adottando cautele e misure adeguate al contesto aziendale, all'esperienza e alla evoluzione tecnologica. Sotto questo profilo, si può dire che, con riferimento al trattamento corretto dei dati dei lavoratori, l'art. 2087 c.c. costituisce una norma di carattere generale, mentre la normativa sulla privacy (insieme con gli artt. 4 e 8, L. 300/1970) costituisce una *lex specialis* che, da un lato, specifica la portata della

[6] D. Piva, *La responsabilità del "vertice" per organizzazione difettosa nel diritto penale del lavoro*, Napoli 2011.

[7] R. Del Punta, *Diritti della persona e contratto di lavoro*, in *Dir. lav. rel. ind.*, 2006, 195 ss. Sulla tendenza ad un utilizzo in chiave riparatoria, anzichè preventiva dell'art. 2087, v. M. Aimo, *op. cit.*, 303 ss. Per una critica a questo approccio all'art. 2087 c.c. si v. E. Gragnoli, *L'obbligo di sicurezza e la responsabilità del datore di lavoro*, in F. Carinci (a cura di), *Il lavoro subordinato*, Tomo II, *Il rapporto individuale di lavoro: costituzione e svolgimento*, Trattato di diritto provato diretto da M. Bessone, Torino 2007, 443 ss.

norma civilistica con particolare riferimento all'ambito della protezione dei dati personali, e dall'altro declina la responsabilità con riferimento ad un ambito soggettivo più ampio di quello dell'art. 2087 c.c.

Infatti, il Codice ed il Regolamento trovano applicazione ben oltre l'ambito del lavoro subordinato, riguardando qualsiasi lavoratore a prescindere dalla tipologia, autonoma o subordinata, del contratto di lavoro stipulato e persino al di là dell'esistenza di un contratto di lavoro (si pensi, ad esempio, ai tirocini o al lavoro volontario o alle prestazioni di lavoro occasionale di cui all'art. 54-*bis*, D.l. 24 aprile 2017, n. 50, conv. in L. 21 giugno 2017, n. 96). Inoltre, la figura del titolare del trattamento, come già detto, non necessariamente coincide con quella formale di datore di lavoro, sicché la responsabilizzazione del titolare operata dalla normativa sulla privacy ha un campo di applicazione ben più ampio e articolato di quella cui mette capo l'art. 2087 c.c.

Peraltro i due nuclei normativi possono trovare concorrente applicazione. Ed invero, nel caso di lesione dei diritti dei lavoratori subordinati da parte del titolare del trattamento che non sia coincidente con il datore di lavoro, si avrà un'autonoma responsabilità del titolare ai sensi della normativa sulla privacy, ma si può ritenere che questa non valga ad esentare da responsabilità il datore di lavoro che potrebbe essere comunque chiamato a rispondere per violazione dell'obbligo generale di protezione, se non altro *sub specie* di *culpa in eligendo* e di *culpa in vigilando*, ai sensi dell'art. 2087 c.c.

Anche al di fuori dell'ambito di applicazione soggettivo di cui all'art. 2087 c.c., e dunque del lavoro subordinato, la normativa sulla privacy vale a predisporre un'adeguata responsabilizzazione a tutto tondo del titolare del trattamento dei dati personali nei confronti dei lavoratori interessati, con una presunzione di responsabilità del danneggiante da cui quest'ultimo si può liberare soltanto fornendo la prova che l'evento dannoso non gli è in alcun modo imputabile (art. 82, Regolamento; art. 15, Codice in combinato disposto con l'art. 2050 c.c.).

In ogni caso, dal punto di vista prevenzionistico, la responsabilità dell'art. 2087 c.c. condivide con il principio di responsabilizzazione del titolare del trattamento di cui alla normativa privacy diversi profili sistematici e di dettaglio. Basti pensare all'impostazione ampia e generale dell'obbligo di protezione; al doppio piano della responsabilità che si dipana tanto a livello tecnico-operativo tanto a livello gestionale ed organizzativo; alla strutturazione aperta e dinamica rimessa alla cautela e valutazione prudenziale del titolare; alla predilezione per uno schema di tutela preventiva anziché risarcitoria/riparatoria. Non va dimenticato, infatti,

che l'art. 2087 c.c. può fondare una responsabilità risarcitoria nei confronti dei lavoratori, ma questa è una conseguenza della violazione delle misure di prevenzione, che costituiscono il contenuto precettivo primario della disposizione.

Il Regolamento prevede espressamente che la responsabilizzazione consista non soltanto nell'obbligo di trattamento conforme ma anche nell'onere del titolare obbligato a «comprovarlo» (art. 5, paragrafo 2). In tale contesto gli strumenti dell'adesione ai codici di condotta o della certificazione sono espressamente considerati utili come mezzi probatori del rispetto, da parte del titolare, dell'obbligo della protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25, paragrafo 3) e da parte del responsabile del trattamento, degli obblighi su lui incombenti ai sensi dell'art. 28 (art. 28, paragrafo 5) e comunque degli obblighi a garanzia della sicurezza del trattamento (art. 33).

4. *La nuova dimensione organizzativa della protezione dei dati personali: analogie e differenze con la dimensione organizzativa della tutela della salute e sicurezza sul lavoro*

È stato ripetutamente evidenziato nel presente volume come il Regolamento abbia segnato un'importante modifica dell'approccio legislativo al tema della protezione dei dati personali, nella misura in cui ha immesso nell'ordinamento una concezione di organizzazione secondaria della protezione dei dati personali che si affianca a quella della prevenzione primaria. La prevenzione e sicurezza organizzativa si affianca così alla più tradizionale sicurezza tecnica già prevista dalla normativa previgente.

Con il Regolamento le misure organizzative di protezione dei dati e la procedimentalizzazione degli obblighi di sicurezza diventano parte integrante degli obblighi giuridici del titolare del trattamento e, per quanto qui particolarmente interessa, del datore di lavoro e dei soggetti da lui designati. Tutto ciò costituisce a sua volta fonte diretta di responsabilità civile e amministrativa per i soggetti obbligati alla predisposizione delle misure organizzative. Manca, invece, una diretta rilevanza penale della violazione della dimensione organizzativa della protezione dei dati, in quanto non è allo stato attuale prevista, diversamente dalla normativa relativa alla salute e sicurezza sul lavoro, la c.d. colpa di organizzazione con rilievo penale.

L'omessa adozione delle misure organizzative di protezione dei dati personali o la loro violazione non dà luogo neppure alla responsabilità

amministrativa degli enti ex D.lgs. 8 giugno 2001, n. 231 in quanto non rientra nel novero dei reati presupposto da cui discende siffatta responsabilità dell'ente ai sensi di detta normativa.

Tuttavia, il Regolamento per molti versi richiama alla mente, sul piano dei contenuti e dell'impostazione, i modelli di organizzazione e gestione (c.d. MOG) previsti dall'art. 6, D.lgs. 231/2001, la cui adozione ed efficace attuazione, in altri contesti si presume atta a prevenire la commissione di reati a vantaggio dell'ente. Così come richiama alla mente i sistemi di gestione della salute e sicurezza (c.d. SGSL) previsti dall'art. 30, D.lgs. 81/2008, che, pure, si presumono atti a prevenire i reati di omicidio colposo o lesioni gravi e gravissime commessi con violazione delle norme di sicurezza, con conseguente efficacia esimente della responsabilità amministrativa degli enti sostanzialmente riconducibile a tale responsabilità penale.

Il criterio di imputazione soggettivo sul quale è basata la responsabilità degli enti per i delitti in esame è appunto quello della c.d. colpa in organizzazione. Viene sanzionato, cioè, un modello di organizzazione aziendale che non si cura di prevenire il rischio reato da infortunio sul lavoro. L'omettere di prevedere e proceduralizzare regole organizzative idonee a prevenire la commissione di reati genera una colpa da organizzazione.

Nel caso della protezione dei dati personali la rilevanza penale delle trasgressioni è sì prevista dal Codice, e dunque riferita a singole violazioni dei principi e degli obblighi gravanti sui diversi soggetti tenuti al loro rispetto, ma il Regolamento non prevede ovviamente sanzioni penali e si limita a prescrivere l'adozione a livello nazionale di sanzioni effettive, proporzionate e dissuasive (art. 84). Ne consegue che quella parte innovativa del Regolamento che attiene appunto alla sicurezza organizzativa dei dati personali è attualmente sguarnita di rilevanza penale.

Sul piano delle sanzioni pecuniarie amministrative, però, il Regolamento non manca di rinviare agli ordinamenti nazionali l'adozione di sanzioni molto rilevanti in funzione di elementi e presupposti predeterminati. In particolare l'art. 83 connette la gravità e l'entità della sanzione anche al «grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32» (paragrafo 2, lett. d) oltre che dell'«adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42» (paragrafo 2, lett. j).

È dunque possibile tracciare una distinzione, anche sul piano sanzionatorio, tra violazioni di tipo operativo (violazione della sicurezza prima-

ria), rilevabili in corrispondenza dell'esercizio delle singole attività di raccolta o trattamento dei dati e violazioni di tipo organizzativo (violazioni della sicurezza secondaria); se non altro sul piano della tipologia ed entità delle sanzioni.

La visione della bontà organizzativa ai fini della protezione dei dati personali è da concepire, allora, in modo strumentale non tanto alla esenzione della responsabilità amministrativa degli enti o della responsabilità penale del titolare o del responsabile (come nei modelli ex art. 6 D.lgs. 231/2001 o nei modelli ex art. 30 D.lgs. 81/2008), quanto piuttosto in modo strumentale a garantire un'efficace osservanza di tutti gli obblighi imposti dalla normativa sulla privacy e ad attenuare il grado di responsabilità del titolare del trattamento e del responsabile del trattamento con conseguente riflesso di ridimensionamento delle sanzioni applicabili.

La predisposizione di un modello organizzativo e gestionale della privacy tende allora ad assumere la forma del dovere, quantomeno sotto il profilo della regolarità e della correttezza della gestione, piuttosto che del mero onere, in quanto appunto strumentale all'adempimento degli obblighi posti dal Regolamento e alla minimizzazione della responsabilità imputabile ai soggetti obbligati per le non conformità.

L'approccio organizzativo alla protezione dei dati è in effetti ispirato al principio della conformità, cioè del rispetto puntuale di tutti gli obblighi giuridici previsti dal Regolamento per ciascun soggetto responsabile e per ciascun adempimento gestionale e sostanziale, ma anche a quello del contenimento del rischio e delle conseguenti responsabilità.

Concorrono a delineare questo modello gestionale ed organizzativo una pluralità di previsioni che attengono: alla chiara definizione di ruoli e responsabilità (titolare, responsabile del trattamento, responsabile della protezione dei dati); alla predisposizione di politiche adeguate (art. 24, paragrafo 2); alla valutazione preventiva dei rischi e alla valutazione preventiva dell'impatto; all'adozione di misure tecniche ed organizzative per garantire la sicurezza dei dati e la prevenzione *by design* e *by default*; all'adozione di sistemi di registrazione continua dei trattamenti e delle non conformità; al riesame e alla valutazione dell'efficacia dei sistemi adottati e aggiornamento degli stessi (art. 24, paragrafo 1).

Come si vede si tratta di un vero e proprio approccio secondo la logica di processo circolare che connota tipicamente i modelli di organizzazione e gestione indirizzati al miglioramento continuo[8], che per essere

[8] Modelli di organizzazione e gestione che normalmente sono ispirati al classico ciclo di Deming (ciclo PDCA, acronimo dall'inglese *Plan, Do, Check, Act*) – articolato nelle

pienamente rispondenti al fine che si propongono, cioè di efficace prevenzione dei rischi e delle condotte illegittime, dovrebbero completarsi con efficaci sistemi di controllo interni tesi a rilevare e correggere le non conformità e con un riesame periodico dell'efficacia e funzionamento del modello organizzativo da parte dei vertici. In effetti in tale direzione è orientato l'art. 32, paragrafo 1, lett. d) che impone l'adozione di «una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento».

5. *La figura del data protection officer: rapporto con il datore di lavoro e posizione nella gerarchia aziendale*

Si è visto come nella catena organizzativa della protezione dei dati personali una figura del tutto nuova rispetto al passato sia rappresentata dal responsabile della protezione dei dati personali anche denominato *data protection officer* (di seguito per brevità RPD o DPO) cui sono dedicati gli artt. 37-39 del Regolamento. Rinviando ai contributi del presente volume specificamente dedicati a questa figura, ci si limiterà qui ad esaminare la posizione del DPO nella gerarchia aziendale, le qualità soggettive che deve possedere ed il rapporto che deve intercorrere tra il DPO ed i vertici aziendali. Su tali questioni alcune importanti indicazioni si ricavano dalle Linee guida sui responsabili della protezione dei dati (WP29 del 13 dicembre 2016[9]).

Riguardo al campo di applicazione delle disposizioni ed ai soggetti tenuti alla nomina del DPO[10], vale la pena qui soltanto ricordare che la gestione dei rapporti di lavoro ed il pagamento delle retribuzioni costitui-

quattro fasi di pianificazione, attuazione, controllo, reazione – volto al controllo e al miglioramento continuo dei processi e dei prodotti.

[9] Reperibile in *www.garanteprivacy.it*.

[10] L'art. 37, paragrafo 1, recita «Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10».

scono «funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali»[11]. Ne consegue che tali attività di per sé non integrano gli estremi dei presupposti applicativi dell'art. 37, paragrafo 1, lett. c).

Quanto alla designazione, si nota come questa debba avvenire da parte del titolare del trattamento e del responsabile del trattamento (art. 37, paragrafo 1). In base al tenore della norma non è chiarissimo se si tratti di un meccanismo di designazione congiunta ovvero alternativa. Le menzionate Linee guida del WP29 si sono espresse nel senso che la designazione sarà effettuata dal titolare quando i presupposti di cui all'art. 37, paragrafo 1, lett. a-c), riguardino l'azienda nel suo complesso, mentre sarà effettuata soltanto dal responsabile del trattamento se e nella misura in cui tali presupposti ricadano unicamente in un suo ambito di attività.

Nei casi previsti il DPO può essere nominato per la singola azienda o anche per più aziende appartenenti ad un gruppo imprenditoriale, a condizione che tale soggetto «sia facilmente raggiungibile da ciascuno stabilimento». Il Regolamento sembra privilegiare un criterio non formale, bensì sostanziale di individuazione del DPO. Non si fa una chiara distinzione tra azienda, stabilimento, unità produttiva. Ciò che conta per individuare l'obbligo non sembrano i confini formali dell'impresa, quanto l'area coperta dalla tipologia di trattamento che, appunto, fa scattare l'obbligo alla designazione del DPO in quanto ricadente in una delle lett. a-c) dell'art. 37, paragrafo 1. Tale area potrebbe per ipotesi riguardare una parte o tutta l'impresa, essere trasversale anche a più imprese (come nei gruppi) o amministrazioni, come nelle pp.aa. che, infatti, possono individuare un unico DPO, tenuto conto della loro struttura organizzativa e dimensione (art. 37, paragrafo 4).

Ciò che conta, in base al criterio di effettività, è l'operatività effettiva del DPO, la possibilità concreta di espletare i suoi compiti, l'agevole raggiungibilità dello stesso da parte degli interessati. Raggiungibilità che, ovviamente, non deve essere intesa in senso fisico-topografico, ma di agevole contatto e comunicazione; cosa che implica la messa a disposizione di mezzi di comunicazione idonei e l'utilizzo da parte del DPO della lingua degli interessati. Infatti il DPO deve poter essere contattato dagli interessati «per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti» (art. 38, paragrafo 4).

[11] *Linee guida sui responsabili della protezione dei dati* (WP29 del 13 dicembre 2016).

In ogni caso non ci può essere ambiguità sull'identità del DPO. I contatti dello stesso debbono essere resi pubblici agli interessati e comunicati all'Autorità garante. Nulla vieta che il DPO sia affiancato da uno o più collaboratori, ma rimane fermo il suo ruolo e la sua piena e diretta responsabilità nei confronti dei soggetti che lo hanno nominato e a cui dovrà rispondere del proprio operato, sebbene in una posizione di autonomia, nonché nei confronti degli interessati al trattamento dei dati e delle autorità ed enti esterni con i quali dovrà interfacciarsi.

Riguardo alle qualità soggettive è molto chiaramente previsto dall'art. 37, paragrafo 5, che la sua designazione avvenga «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39». È evidente allora che la competenza professionale non è da intendere in modo formale, come possesso di qualifiche o titoli di studio, ma deve essere declinata in concreto, dovendo tener conto anche delle prassi e della capacità di affrontare nel proprio ambito e settore le questioni specifiche connesse ai compiti di cui è investito, dunque in funzione dei trattamenti di dati da effettuare e della protezione richiesta per i dati personali oggetto di trattamento (cfr. *considerando 97*).

La verifica delle competenze professionali in esame spetta ovviamente al soggetto designante e non va condotta una volta tanto, ma rinnovata nel tempo, come chiaramente si evince dall'art. 38, comma 2, laddove pone in capo al soggetto designante l'obbligo di fornire il necessario sostegno al DPO nell'esecuzione dei suoi compiti, fornendogli «le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica».

Venendo a considerare la posizione del DPO nella gerarchia aziendale, anzitutto va notato che non è prescritto il suo necessario inserimento nella struttura aziendale. Il rapporto giuridico avente ad oggetto il suo incarico può essere compatibile con un rapporto di lavoro subordinato, un rapporto di lavoro autonomo od anche con un contratto di fornitura di servizi (art. 37, paragrafo 6). Può coesistere, inoltre, con altre funzioni già svolte per il medesimo titolare o responsabile del trattamento, purché non si configuri un conflitto di interessi (art. 38, paragrafo 6).

Dunque ciò che importa non è la natura della relazione giuridica in base alla quale l'attività di DPO viene prestata, mentre viene in rilievo la posizione concreta di potere che intercorre con il titolare o il responsabile del trattamento. Ed infatti la posizione del DPO si deve caratterizzare per

l'assenza di una subordinazione gerarchica con specifico riferimento alla funzione di protezione dei dati, cioè per l'assenza di un assoggettamento a potere altrui nell'espletamento dei propri compiti. La posizione del DPO è, dunque, quella di un'assoluta autonomia dal titolare e dal responsabile del trattamento come chiaramente prescrive l'art. 38, paragrafo 3, nonché il *considerando* 97 dove si prevede che i DPO «dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente».

Da un lato, infatti, il DPO non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti, dall'altro lato non può essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento in ragione dell'adempimento dei propri compiti. Inoltre egli riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

La posizione nella struttura aziendale è quella dunque caratterizzata da un rapporto diretto con il vertice aziendale; dalla piena autonomia nell'espletamento del proprio ruolo; dall'assenza di qualsiasi interferenza tra compiti svolti come DPO ed ulteriori eventuali compiti e funzioni svolte per la stessa azienda; da una relativa autonomia dai soggetti che lo hanno designato.

Relativa poiché è da escludere che il DPO non sia sottoponibile a controllo alcuno. È chiaro che i soggetti designanti devono accertarsi che il DPO svolga correttamente i propri compiti e sia costantemente idoneo all'espletamento del ruolo, sino all'eventuale revoca o rimozione qualora ciò non dovesse verificarsi. Ciò che è impedito dall'art. 38, paragrafo 3, sono le penalizzazioni di qualsiasi tipo o le interruzioni del rapporto che configurino comportamenti ritorsivi verso il DPO in ragione dell'adempimento dei propri compiti. Mentre ben diversa è la questione del conferimento e revoca della funzione che non può che rimanere di pertinenza del titolare e del responsabile quali soggetti tenuti all'osservanza del Regolamento e che ben potrà essere valutata tempo per tempo, anche in relazione alla adeguatezza e competenza dimostrata dal DPO nello svolgimento delle proprie funzioni.

Così come rimane del tutto impregiudicata la possibilità di gestire, modificare o estinguere il rapporto di lavoro del DPO ai sensi della normativa giuslavoristica per questioni diverse e del tutto indipendenti dal suo specifico ruolo di responsabile della protezione dei dati.

Il DPO deve inoltre essere dotato, a sua volta, delle condizioni, materiali, sostanziali e relazionali adeguate ai fini dell'espletamento del proprio ruolo. Il che significa non soltanto della possibilità di disporre delle

risorse anche finanziarie e temporali adeguate alla rilevanza del compito da svolgere, ma altresì della possibilità di interagire con adeguata autorità con il personale dell'azienda, di avere accesso diretto a informazioni e sorgenti di dati ed essere pienamente e continuamente coinvolto nelle strategie e nelle attività rilevanti di azienda che possono avere un impatto sul trattamento dei dati.

Da ciò si evince come non andrebbe sottovalutata l'utilità/opportunità di un posizionamento del DPO interno all'azienda, in grado di favorire la partecipazione e consapevolezza delle questioni che rientrano nelle sue competenze nonché la sua capacità di incidere con la dovuta autorità sui processi gestionali attinenti all'espletamento dei propri compiti. Chiaro è che tale eventuale inserimento – per le ragioni sopra esposte – dovrà avvenire in una posizione molto elevata e laterale rispetto alla linea gerarchica aziendale. Il DPO deve essere infatti dotato di autonomi poteri di iniziativa ed essere sottratto ad autorizzazioni di qualsiasi genere per poter svolgere le attività funzionali all'espletamento dei propri compiti.

La collocazione all'esterno dal perimento aziendale, d'altro canto, potrebbe fornire maggiori garanzie di indipendenza e qualificazione specialistica rispetto al ricorso a risorse umane interne. Ma anche in questo caso non vanno sottovalutati i possibili conflitti di interesse nel caso in cui il DPO esterno svolga tale funzione per diverse imprese in concorrenza tra loro e le difficoltà di interazione e rapporto diffuso con i diversi uffici e personale dell'impresa che il soggetto esterno inevitabilmente incontra in misura maggiore di un soggetto inserito all'interno della struttura aziendale.

6. *I principi applicabili al trattamento dei dati personali nel rapporto di lavoro alla luce del Regolamento UE 2016/679*

Dopo aver messo in rilievo la portata del principio di responsabilizzazione che il Regolamento pone alla base della nuova regolazione europea del trattamento dei dati personali e aver sottolineato l'impatto, valutato con le lenti del giuslavorista, che le nuove regole avranno sull'organizzazione imprenditoriale, è arrivato il momento di spostare l'attenzione sul quadro dei principi e delle regole che devono presiedere al trattamento dei dati personali nell'ambito della gestione dei rapporti di lavoro.

Analisi questa che, anche in questo caso, va affrontata con lo scopo primario di individuare gli elementi di eventuale novità apportati dal Re-

golamento all'impianto già definito dall'ormai abrogata Direttiva 95/46/CE.

Venendo immediatamente al merito della questione, come si è già messo in rilievo nei paragrafi precedenti, si può affermare che il Regolamento non rivoluziona quel quadro di principi e di regole; piuttosto lo fa proprio, sviluppandone alcuni profili, al contempo ampliando, per un verso, il ventaglio delle obbligazioni gravanti sul datore di lavoro e, per l'altro, riconoscendo nuovi diritti in capo ai lavoratori.

Il recepimento dell'impianto dei principi già dettati dalla Direttiva all'interno del Regolamento ha peraltro il non secondario effetto di rendere quei principi immediatamente vincolanti per tutti i soggetti operanti all'interno degli Stati membri. Ed infatti, come già messo in evidenza, mentre la Direttiva fissava dei principi la cui concreta attuazione era rimessa alle singole legislazioni nazionali tenute a varare le regole necessarie a renderli concretamente applicabili, il Regolamento non si limita a vincolare le istituzioni degli Stati membri, ma costituisce una fonte dotata di efficacia giuridica anche nei rapporti fra i soggetti privati, i quali sono dunque tenuti a rispettarne la disciplina. Ciò comporta che il Regolamento è destinato a travolgere le regole nazionali che siano con esso incompatibili.

Queste preliminari osservazioni spingono dunque ad approfondire il quadro dei principi che il Regolamento detta per il trattamento dei dati personali, con specifico riferimento ai rapporti di lavoro, in una duplice prospettiva.

Per un verso, l'indagine deve appurare quali elementi di innovazione il Regolamento abbia apportato a tale quadro.

Per l'altro, ci si deve interrogare circa l'impatto che gli elementi di novità eventualmente riscontrati potranno avere sulla disciplina nazionale che ha dato attuazione alla Direttiva del 1995 (quindi il Codice e, per quanto qui in particolare interessa, l'art. 4, L. 300/1970, poiché, pur non trattandosi di una disposizione attuativa di quella direttiva, fissa regole che direttamente toccano il diritto alla riservatezza dei lavoratori) e sugli orientamenti espressi dell'Autorità per la protezione dei dati personali, nonché sulle indicazioni da questa formulate nelle proprie linee guida in materia di trattamento dei dati personali nel rapporto di lavoro.

Quest'ultima parte dell'analisi assume una rilevanza altrettanto importante delle altre se si considera quanto disposto dall'art. 154, comma 1, lett. c), Codice, a mente del quale è conferito all'Autorità il compito di «*prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'art. 143*». Ciò significa che l'ordinamento ha conferito

al Garante il compito di tradurre in prescrizioni concrete le regole dettate dal Codice, identificando le misure che, alla luce dell'esperienza e del progresso tecnologico, appaiono funzionali a garantire la piena attuazione degli obiettivi di tutela della riservatezza a cui mirano le norme in materia di protezione dei dati personali. L'immediata conseguenza di tale ragionamento è che, nel sistema della protezione della privacy, le prescrizioni del Garante costituiscono atti dalla cui osservanza dipende la legittimità del trattamento dei dati. È dunque necessario chiedersi se l'impianto degli orientamenti interpretativi espressi dal Garante con specifico riferimento al trattamento dei dati nel rapporto di lavoro possa dirsi sopravvissuto al Regolamento, o se l'entrata in vigore di quest'ultimo richiederà degli adattamenti.

Così definite le prossime tappe dell'indagine da sviluppare, e prendendo le mosse dall'analisi delle novità relative al quadro dei principi ai quali deve essere ispirato il trattamento, appare essenziale subito esplicitare la prospettiva peculiare a partire dalla quale deve essere approfondito il contenuto che quei principi assumono se calati all'interno del rapporto di lavoro.

Ed infatti, se l'interesse principale che la regolazione della privacy è chiamata a soddisfare è quello di assicurare al soggetto un controllo sulla circolazione dei propri dati personali[12], con riferimento ai dati registrati dal datore di lavoro, questo interesse va considerato in una prospettiva ulteriore. Prospettiva ulteriore che muove dalla constatazione che, tramite i dati acquisiti in conseguenza dello svolgimento della prestazione lavorativa, il datore di lavoro potrebbe apprendere, per un verso, informazioni che non dovrebbe conoscere[13], e, per l'altro, dati che potrebbero essere utilizzati per ricostruire a distanza modalità, tempi e contenuti della prestazione svolta dal lavoratore durante l'orario di lavoro e non solo[14].

[12] Il lavoratore ha sicuramente interesse anche a che i suoi dati personali, acquisiti dal datore all'interno del rapporto, non vengano, ad esempio, illecitamente trasferiti a terzi. Si pensi, per fare un esempio, all'interesse che un'impresa con un elevato numero di dipendenti potrebbe avere a vendere ad una società terza i dati relativi all'accesso da parte dei dipendenti durante l'orario di lavoro a siti internet che non hanno nulla a che fare con lo svolgimento della prestazione lavorativa, ma dai quali possano evincersi informazioni circa la propensione al consumo e l'interesse all'acquisto di determinati prodotti.

[13] È sufficiente qui richiamare quanto prescritto dall'art. 8, L. 300/1970, a mente del quale «*è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore*».

[14] Il tema della ricostruzione dei contenuti della prestazione lavorativa è oggi ulterior-

Il rischio che gli interessi appena richiamati possano essere lesi da un trattamento illecito dei dati del lavoratore è, com'è noto, fortemente cresciuto nel corso degli anni recenti per effetto delle profonde innovazioni tecnologiche; innovazioni che hanno interessato direttamente il ventaglio degli strumenti utilizzati dal lavoratore o collegati con lo svolgimento della prestazione lavorativa. Strumenti che sono impiegati per perseguire obiettivi diversi, come si vedrà nella parte dedicata all'esame dell'art. 4, L. 300/1970, ma che hanno in comune la capacità di registrare non solo ogni elemento relativo alla prestazione svolta dal lavoratore, consentendone una ricostruzione completa, ma di acquisire anche dati relativi alle sue opinioni, ai suoi gusti, ai suoi spostamenti, ecc.

Acquisizione di dati che può realizzarsi, peraltro, non solo tramite gli strumenti forniti dal datore di lavoro per lo svolgimento della prestazione lavorativa, o per soddisfare esigenze connesse con l'attività del lavoratore, ma anche tramite gli strumenti di proprietà personale del lavoratore che sempre più possono essere impiegati per rendere la prestazione lavorativa. Tra queste ultime tecnologie, per richiamare un esempio indicativo, è utile ricordare il *Bring your own device (BYOD)*, il quale ha sollecitato un'attenzione particolare[15] in quanto consente di creare, sullo stesso dispositivo (di proprietà del dipendente), due ambienti diversi, contenenti rispettivamente dati personali e dati aziendali, che possono consentire all'utente anche di collegarsi alla intranet aziendale, utilizzandone dati ed applicazioni.

Tramite l'impiego di tecnologie come quella appena citata, si realizzano, dunque, inedite possibilità di accesso da parte del datore di lavoro a dati personali del lavoratore, mentre, d'altro canto, si pongono maggiori rischi per la sicurezza aziendale e quindi maggiori ragionevoli esigenze di controllo, poiché tale modalità di connessione con i server aziendali sollecita ad implementare strumenti adeguati a tutelare le informazioni presenti nella rete del datore di lavoro e ad ostacolare la divulgazione di dati riservati, tanto dell'azienda medesima quanto dei terzi che con questa vengano in contatto.

mente complicato dall'impiego delle nuove tecnologie che consentono al lavoratore di connettersi al server aziendale e svolgere la prestazione lavorativa utilizzando *devices* di proprietà personale, nonché dall'impiego delle tecnologie che consentono di svolgere la propria prestazione di lavoro da remoto, al di fuori del luogo di lavoro. Su questi profili v. *infra.*

[15] È sufficiente qui richiamare la specifica attenzione riservata all'impiego di questa tipologia dal WP29 all'interno della *Opinion 2/2017 on data processing at work (WP249)*, adottata l'8 giugno 2017 (v. il punto 5.4.2).

Sviluppando l'analisi nella prospettiva appena indicata e spostando l'attenzione sui principi dettati dal Regolamento per il trattamento dei dati personali, si può subito constatare che l'elenco dettato dall'art. 5 rispecchia sostanzialmente quello già contenuto nella Direttiva del 1995, cosicché anche il trattamento dei dati da parte del datore di lavoro dovrà avvenire nel rispetto degli stessi.

Se il quadro non viene alterato nella sua impostazione di fondo, è però importante osservare come: da un lato, a questi principi venga affiancata la codificazione di diritti nuovi della persona a cui i dati si riferiscano (come ad esempio il diritto all'oblio) il cui godimento deve essere garantito alla persona anche nell'ambito del rapporto di lavoro; e, dall'altro, alcuni dei principi già posti dalla disciplina previgente vengano rafforzati e arricchiti nel loro contenuto per effetto degli elementi innovativi apportati dal Regolamento alla impostazione di fondo che dovrà garantire la protezione dei dati personali a partire dal prossimo maggio del 2018.

Prendendo le mosse dall'analisi di questo secondo profilo e focalizzando l'attenzione sul trattamento dei dati personali del lavoratore, si può affermare che tra i principi che subiscono una indubbia valorizzazione all'interno del Regolamento sono annoverabili il principio di trasparenza e quello della minimizzazione nel trattamento dei dati personali.

Il principio di trasparenza si traduce principalmente nell'obbligo di fornire al lavoratore un'informativa completa, chiara, facilmente consultabile e comprensibile sui dati che possono essere oggetto di trattamento, sulle modalità di questo e sul periodo di conservazione dei dati medesimi. Il Regolamento peraltro, rispetto al passato, si preoccupa di elencare in modo tassativo i contenuti dell'informativa, tra i quali spiccano, per quanto qui in particolare interessa, la necessità che siano indicate le finalità che giustificano la registrazione dei dati e che sia predeterminato e comunicato il periodo di conservazione dei dati medesimi.

L'obbligazione informativa riguarda qualunque forma di trattamento dei dati personali che il datore di lavoro possa mettere in campo per la gestione del rapporto di lavoro; rispetto ad essa, quindi, il fondamentale obbligo informativo prescritto dall'art. 4, L. 300/1970, sul quale torneremo più avanti, costituisce una regola speciale. L'obbligo di informazione che il datore di lavoro deve fornire risulta quindi più ampio di quello definito dall'art. 4 e riguarda qualunque tipo di trattamento dei dati del lavoratore realizzato in azienda, anche se non connesso all'impiego degli strumenti tecnologici forniti dal datore di lavoro.

Strumentale e strettamente collegato al principio di trasparenza ap-

pena enucleato è poi l'obbligo, di nuova istituzione, della tenuta del registro del trattamento dei dati personali eseguiti dal titolare (art. 30, Regolamento). Un obbligo gravante sulle imprese con più di 250 dipendenti, ma che deve essere ritenuto vincolante anche per le imprese con un numero inferiore di dipendenti se il trattamento effettuato *«possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categoria particolari di dati di cui all'art. 9, par. 1»*. La formulazione appena riportata induce a suggerire una notevole attenzione nel determinare l'area di applicazione dell'obbligazione con riferimento al trattamento dei dati riferiti al lavoratore e trattati in ragione del rapporto di lavoro. Si può invero affermare che in molte occasioni il trattamento dei dati può non essere occasionale e soprattutto comporta spesso, soprattutto nelle imprese tecnologicamente più avanzate, l'impiego di strumenti funzionali alla realizzazione della prestazione lavorativa che possono consentire l'accesso ai dati contemplati dal primo paragrafo dell'art. 9 del Regolamento. È dunque altamente consigliabile prevedere sempre l'istituzione e la tenuta di un registro dei trattamenti dei dati del lavoratore, anche in aziende di dimensioni ridotte.

Di grande importanza è anche l'impatto che la nuova filosofia della protezione dei dati personali inaugurata dal Regolamento è suscettibile di produrre sull'attuazione del principio di minimizzazione del trattamento.

Tale principio risulta infatti valorizzato se considerato in rapporto al principio di responsabilizzazione, da un lato, e alla prescrizione della realizzazione di un sistema di *privacy by design* e *by default*, dall'altro.

Come già messo in rilievo più sopra e in altri contributi del presente volume, uno dei tratti caratterizzanti della disciplina dettata dal Regolamento, che ne rappresenta al contempo il maggior tratto di discontinuità rispetto alla disciplina dettata dalla Direttiva 95/46/CE, è infatti costituito dall'affermazione e valorizzazione del principio di responsabilizzazione del titolare e del responsabile del trattamento.

Principio in virtù del quale, titolare e responsabile sono tenuti non solo ad attuare (o almeno contribuire ad attuare) le misure ritenute utili a prevenire la violazione alle regole sul trattamento dei dati personali, ma altresì a monitorare costantemente i rischi che possono porsi rispetto a tale trattamento e a conseguentemente adattare le misure richieste dall'evoluzione tecnologica e dagli eventuali cambiamenti della struttura organizzativa che possano produrre un impatto sul trattamento.

La regola della «minimizzazione dei dati» – così ora espressamente denominata dal Regolamento (art. 5, paragrafo 1, lett. c), ma già presente

nella Direttiva 95/46/CE (art. 6, paragrafo 1, lett. c) – costituisce indubbiamente una delle espressioni della finalità prevenzionistica alla base del principio di *accountability*.

Il principio di minimizzazione dei dati richiede infatti al titolare del trattamento che i dati siano trattati (e, dunque, raccolti, memorizzati, organizzati, consultati e conservati) in maniera adeguata, pertinente e limitata a quanto necessario rispetto alle finalità perseguite con il trattamento.

Tale principio, come anticipato, non innovativo ma presente già nella normativa europea previgente e nella sua prassi applicativa, merita però un'attenzione specifica, poiché lo stesso assume un ruolo centrale nell'ambito della gestione dei rapporti di lavoro.

Da tale principio deve infatti evincersi l'obbligo del datore di lavoro, che abbia necessità di avvalersi di strumenti tecnologici all'interno della propria organizzazione, di installarli solo laddove sia assicurato che i dati relativi al lavoratore e alla prestazione da questi resa, registrati in conseguenza dell'impiego dello strumento da parte del prestatore di lavoro, siano acquisiti e trattati compatibilmente con quel principio.

Detto con altri termini e per maggiore chiarezza, lo strumento potrà essere utilizzato dall'imprenditore solo laddove esso sia strutturato, sin dal momento dell'installazione, in maniera tale che lo stesso registri, al momento del suo utilizzo, solo i dati essenziali a soddisfare una delle ragioni legittime che ne hanno consentito l'impiego, cosicché solo i dati necessari alla realizzazione di tali finalità, e non altri, siano effettivamente consultabili da parte del datore di lavoro.

Vedremo, poi, in sede di analisi dei contenuti dell'art. 4, L. 300/1970, come si debba oggi concludere che i dati registrati dagli strumenti tecnologici installati per finalità lecite siano utilizzabili per tutti i fini connessi al rapporto di lavoro e, quindi, ad esempio, anche per finalità disciplinari.

Per completare sul tema dei principi che debbono presiedere al legittimo trattamento dei dati personali è utile però precisare che il bilanciamento fra i vari interessi coinvolti non potrà che avvenire valutando caso per caso le potenzialità di accesso e gestione dei dati personali che sono proprie del singolo strumento tecnologico impiegato o comunque collegato allo svolgimento della prestazione lavorativa. Bilanciamento che può rilevarsi molto complicato da definire in concreto se si considera, come ormai chiarito nella giurisprudenza anche internazionale[16], che il datore di lavoro non può limitarsi a vietare al lavoratore l'impiego per scopi personali degli strumenti di lavoro al fine di fondare il proprio diritto ad in-

[16] Cfr. in particolare CEDU *Barbulescu v. Romania*, 61496/08, 5 settembre 2017.

terrogare tali dati. Come sottolineato dal WP29, invero, *«as good practice, the employer could offer alternative unmonitored access for employees. This could be done by offering free WIFI, or stand-alone devices or terminals* […] *where employees can excercise their legitimate right to use work facilities for some private usage»*[17]. Deve essere dunque riconosciuto al lavoratore, anche in ragione della fondamentale funzione di strumenti di socialità che oggi è rivestita da tecnologie come internet e la posta elettronica, un diritto a poterle impiegare moderatamente anche per esigenze personali durante l'orario di lavoro. Poiché l'apparato fornito dal datore di lavoro accresce, in ragione di ciò, la possibilità di acquisire dati personali del lavoratore, le modalità di registrazione, consultazione e interrogazione di questi dati devono dunque essere impostate, sin dall'origine, riducendo al minimo le facoltà di accesso a tali dati.

Infine, per quanto riguarda i diritti di nuovo conio, un'attenzione specifica per l'attuazione dei principi in materia di trattamento dei dati personali del lavoratore meritano il diritto all'oblio (art. 17) e il diritto alla portabilità dei dati (art. 20).

Il diritto all'oblio è strettamente collegato al principio di *«limitazione della conservazione»* (art. 5, paragrafo 1, lett. e), Regolamento), in virtù del quale il dato personale non deve essere conservato oltre il tempo necessario per la realizzazione delle finalità che ne hanno giustificato il trattamento. L'interessato ha dunque il diritto di ottenere dal titolare del trattamento la cancellazione dei dati che lo riguardano senza giustificato ritardo.

È però evidente che un simile diritto può non essere di facile soddisfazione in concreto, poiché molto difficile può essere la identificazione dei dati cancellabili rispetto a quelli conservabili quando si tratti di dati generati dal lavoratore attraverso l'impiego di strumenti forniti per lo svolgimento della prestazione lavorativa.

Un esempio particolarmente significativo può essere quello delle *e-mail* inviate dal dipendente nello svolgimento della prestazione lavorativa e che possono essere utili al datore di lavoro, per esempio, per dimostrare l'avvenuta stipulazione di un contratto con un cliente che invece la disconosca. La possibilità di reperire una simile informazione all'interno della corrispondenza elettronica scambiata potrebbe allora giustificare la conservazione integrale, almeno per i tempi del decorso della prescrizione ordinaria, per permettere al datore di lavoro di avere gli strumenti per una eventuale difesa del proprio diritto in sede giudiziaria; motiva-

[17] WP29 *Opinion 2/2017 on data processing at work (WP249)*, cit., punto 5.3.

zione, quest'ultima, espressamente annoverata dal Regolamento fra quelle che giustificano la conservazione, escludendo l'operatività del diritto all'oblio (art. 20, paragrafo 3, lett. e), Regolamento). D'altronde, a conferma di tale conclusione, potrebbe argomentarsi che una selezione fra la corrispondenza cancellabile e quella che il datore di lavoro ha il diritto di conservare richiederebbe un controllo sui contenuti di quella medesima corrispondenza, la cui fattibilità deve ritenersi incompatibile con la protezione accordata tanto dal Regolamento, quanto dalla disciplina nazionale ed in particolare dall'art. 4, L. 300/1970.

Per quanto riguarda il diritto alla portabilità dei dati, anch'esso deve essere ritenuto pienamente operante con riferimento ai dati acquisiti e generati nello svolgimento del rapporto di lavoro.

L'art. 20 del Regolamento riconosce invero tale diritto ogni qualvolta il trattamento trovi la sua ragione nell'esecuzione di un contratto di cui l'interessato è parte.

Il citato art. 20 attribuisce al diritto alla portabilità un duplice significato: il diritto dell'interessato a ricevere, in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati che lo riguardano; il diritto a trasmettere tali dati ad un terzo, o autonomamente o tramite colui che ha trattato i dati e che deve farsi carico del trasferimento.

Nella prospettiva specifica che interessa in queste pagine, bisogna chiedersi quali siano i dati comunicati e generati nell'ambito dello svolgimento del rapporto di lavoro che debbano essere fatti oggetto del diritto alla portabilità.

Per rispondere a tale quesito è utile tenere in considerazione due aspetti del diritto alla portabilità dei dati messi in evidenza dal WP29. Quest'ultimo ha invero evidenziato, in un suo parere, che, per un verso, il diritto alla portabilità dei dati riguarda i dati personali che possano essere utilizzati per scopi personali[18], e, per l'altro, che i dati portabili sono quelli che riguardano l'interessato e che sono stati forniti dall'interessato[19].

Con riferimento al primo requisito, la finalità specifica appena evidenziata consente, in prima battuta, di limitare la latitudine del diritto a tutti quei dati che il lavoratore possa utilizzare per scopi personali e nei quali non siano dunque toccati interessi del datore di lavoro o di terzi[20]. Si può così concludere che la portabilità non possa riguardare la

[18] *Linee guida sul diritto alla portabilità dei dati*, 5 aprile 2017, WP242 rev. 01, 5.
[19] *Linee guida sul diritto alla portabilità dei dati*, cit., 10.
[20] *Linee guida sul diritto alla portabilità dei dati*, cit., 12.

corrispondenza scambiata per ragioni lavorative, mentre potrebbe, ad esempio, riguardare la rubrica dei contatti, ma solo se riferibile in via esclusiva ai contatti personali lavoratore. La rubrica dei contatti acquisita nello svolgimento della prestazione lavorativa può invero avere un valore commerciale che il datore di lavoro può volere evidentemente preservare.

Per quanto riguarda il secondo requisito, sempre il WP29 ha concluso che tra i dati portabili devono essere inclusi anche quelli che siano stati forniti inconsapevolmente dall'interessato, perché ad esempio generati nello svolgimento della prestazione di lavoro attraverso, ad esempio, l'utilizzo di un dispositivo fornito dal datore (dati grezzi generati da un contatore intelligente o altri oggetti connessi alle registrazioni delle attività svolte, la cronologia della navigazione su un sito web o delle ricerche effettuate).

Non rientrerebbero nella categoria in questione invece i dati derivanti dalla successiva analisi dei dati raccolti e del comportamento dell'interessato.

Muovendo da quest'ultima osservazione, ci si deve chiedere, ad esempio, se siano «portabili» i dati relativi alla performance lavorativa che siano stati utilizzati nella decisione circa l'erogazione della retribuzione di risultato.

7. *L'impatto del Regolamento UE 2016/679 sugli orientamenti dell'Autorità per la protezione dei dati personali e sulle indicazioni da questa espresse nelle linee guida in materia di trattamento dei dati personali nel rapporto di lavoro*

Così ricostruiti i profili di maggiore novità apportati dal Regolamento al quadro dei principi che devono governare il trattamento dei dati personali nel rapporto di lavoro, si deve spostare l'attenzione sul secondo profilo di analisi più sopra enucleato e quindi chiedersi se tali elementi di novità comportino la necessità di un aggiornamento della legislazione nazionale (D.lgs. 196/2003) e degli orientamenti espressi dall'Autorità nei propri provvedimenti e nelle linee guida.

Non è facile fornire una risposta a tale quesito, che comunque richiederebbe, almeno per quanto riguarda i provvedimenti, un'analisi caso per caso prendendo in considerazione le peculiarità della fattispecie sottoposta all'esame del Garante.

Quello che si può tentare di fare in questa sede è una valutazione di respiro più generale riguardante i profili di novità che devono essere te-

nuti in considerazione nella valutazione della correttezza dell'operato del datore di lavoro rispetto al trattamento dei dati personali del lavoratore.

Esaminando il tema in questa prospettiva ed in considerazione del fatto che, come già detto, il Regolamento ha sostanzialmente recepito l'impianto dei principi già dettati dalla Direttiva, si può concludere che, con riferimento al rapporto di lavoro, conservino nel loro complesso validità le regole dettate dal Codice, il quale fa espressamente salva, agli artt. 114 e 115, la disciplina statutaria. Le regole ivi dettate, ed in particolare l'art. 4, L. 300/1970, vanno ovviamente interpretate conformemente alle disposizioni del Regolamento, ma tenendo conto delle specifiche esigenze implicate nello svolgimento del rapporto di lavoro come peraltro lo stesso Regolamento espressamente ammette all'art. 88. Art. 4 che, come anticipato e come meglio sarà messo in risalto più avanti, è stato recentemente riformato dal legislatore. In particolare, attesa la non sovrapponibilità delle regole dettate dall'art. 4 rispetto a quelle poste dalla disciplina della privacy, anche l'Autorità garante dovrà tener conto nei propri provvedimenti della regola, ora espressamente enunciata dalla disposizione statutaria, che consente l'utilizzabilità delle informazioni raccolte dagli strumenti di lavoro e non «a tutti i fini connessi al rapporto di lavoro».

Tenendo in considerazione tale importante precisazione, si può comunque constatare come conservino sicuramente un'efficace funzione di orientamento le linee guida definite in materia di utilizzo della posta elettronica e di internet[21], e non solo[22], soprattutto nella parte in cui vengono ricostruiti gli accorgimenti utili a prevenire, tanto l'utilizzo improprio da parte del lavoratore degli strumenti aziendali, quanto l'esigenza del datore di lavoro di consultare i dati registrati per far fronte ad esigenze organizzative e produttive.

Tali misure, anzi, appaiono perfettamente in linea con lo spirito di prevenzione del rischio che il Regolamento pone a base del nuovo sistema di regole tramite il principio di *accountability* e l'esigenza della realizzazione delle modalità di trattamento tramite i meccanismi della privacy *by design* e *by default*.

Le nuove regole europee comportano però la necessità – in coerenza

[21] Si tratta delle Linee guida del Garante per posta elettronica e internet (Provv. Garante 1 marzo 2007, doc. web n. 1387522).

[22] Cfr.: Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (Provv. Garante 23 novembre 2006, doc. web n. 1364939); Linee guida in materia di trattamento di dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (Provv. Garante 14 giugno 2007, doc. web n. 1417809).

con i sopra citati profili di novità apportati dal Regolamento – di accrescere la rilevanza che deve essere riconosciuta all'obbligo del datore di lavoro di installare strumenti che sin dall'inizio consentano solo il trattamento lecito dei dati personali, nonché all'obbligo del medesimo soggetto di informare il lavoratore del possibile trattamento.

Nel nuovo quadro di regole, invero, questi due principi appaiono essere quelli ai quali è principalmente affidata la soddisfazione del diritto del lavoratore, non solo a mantenere un controllo sul trattamento dei propri dati personali, ma anche a che sia assicurata la protezione della propria dignità personale evitando un controllo sistematico della prestazione lavorativa, ricostruibile a distanza, attraverso la consultazione dei dati registrati dagli strumenti informatici.

Una volta minimizzati i dati oggetto di registrazione ed assicurata la piena e completa informazione del lavoratore sulle possibili modalità del trattamento, appare pienamente coerente riconoscere, come fa l'art. 4, L. 300/1970, la utilizzabilità dei dati registrati dall'apparecchio, a tutti i fini connessi al rapporto di lavoro.

8. *Il nuovo art. 4, L. 300/1970 alla luce del Regolamento UE 2016/679*

Per completare il quadro deve essere ora dedicata opportuna attenzione al contenuto della principale disposizione, più volte evocata, che, nell'ambito della disciplina del rapporto di lavoro, interagisce, ed è sempre più destinata ad interagire, con le regole dedicate alla protezione dei dati personali del lavoratore: l'art. 4, L. 300/1970.

Questa disposizione non può essere ignorata nell'esame dei contenuti del Regolamento e dei profili di novità dallo stesso apportati se si considera, da un lato, che l'art. 4, L. 300/1970 è stato, storicamente, una delle prime norme del nostro ordinamento specificamente destinate a realizzare anche la tutela del diritto alla riservatezza nell'ambito speciale dei rapporti di lavoro, e, dall'altro, che quella disposizione è stata da ultimo profondamente riformata dall'art. 23, D.lgs. 14 settembre 2015, n. 151, per poi essere ulteriormente corretta dall'art. 5, comma 2, D.lgs. 24 settembre 2016, n. 185. È necessario dunque valutare se il nuovo bilanciamento fra l'interesse del datore di lavoro a consultare i dati registrati dagli strumenti tecnologici e quello del lavoratore a sottrarsi a qualunque forma di controllo a distanza sia compatibile con l'assetto realizzato dal Regolamento qui in esame.

Anticipando le conclusioni dell'indagine appena indicata, si può dire

che la disposizione statutaria appare pienamente compatibile con i contenuti del Regolamento sotto un duplice profilo.

Da un lato, l'art. 4 detta una disciplina che appare destinata ad integrarsi e non a sovrapporsi con le regole dettate dal Regolamento e dal Codice. In questo senso deve essere interpretato il richiamo, ora contenuto nell'art. 4 riformato, al «rispetto di quanto previsto dal D.lgs. 196/2003»; richiamo che traccia il confine tra le materie disciplinate direttamente dall'art. 4 e quelle rimesse alla disciplina di protezione dei dati personali, le quali concorrono a concretizzare la complessiva tutela del lavoratore in materia di controlli a distanza. Così, ad esempio, in materia di informazione adeguata al dipendente e di utilizzabilità dei dati raccolti a tutti i fini del rapporto di lavoro dovrà essere applicato quanto previsto dall'art. 4, comma 3 che in materia costituisce norma speciale rispetto a quella generale contenuta nell'art. 11, comma 2, Codice e ora negli artt. 12 e ss. del Regolamento. Invece uno degli aspetti non disciplinati nell'art. 4 riguarda la misura e modalità dei controlli a distanza che dovranno rispettare i principi sanciti dal Codice e ora dal Regolamento, in particolare con riferimento ai principi, più sopra ricordati, alla necessità e pertinenza, dalla non eccedenza e dalla temporanea conservazione dei dati raccolti. Principi la cui concreta applicazione dovrà confrontarsi con le previsioni dell'art. 4 nella parte in cui danno atto della operatività del controllo ammettendone la legittimità[23].

Dall'altro lato, si può anticipare che l'evoluzione subita dal testo dell'art. 4 è pienamente conforme ai principi di fondo, sopra esaminati, sui quali il Regolamento fonda la protezione dei dati personali del lavoratore.

Procedendo con ordine, va subito rilevato che le ragioni della recente modifica dell'art. 4, L. 300/1970[24] sono state tradizionalmente indivi-

[23] Molto raramente la giurisprudenza nel verificare la legittimità dei controlli a distanza del datore di lavoro ha affrontato questi temi, al riguardo v. Trib. Milano (Giud. Attanasio) 23 marzo 2015 e la sentenza di riforma App. Milano (Rel. Vitali) 4 agosto 2015, entrambe – per quanto consta – non edite.

[24] La nuova disposizione ha suscitato un ampio ed articolato dibattito. V., tra gli altri: P. TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino 2017, 45; A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel* nuovo *art. 4 dello Statuto dei lavoratori*, in *Riv. it. dir. lav.*, 2016, I, 513; G. PROIA, *Trattamento dei dati personali, rapporti di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza*, in *Riv. it. dir. lav.*, 2016, I, 547; C. ZOLI, *Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970*, in *Var. temi dir. lav.*, 2016, 635; E. BALLETTI, *I poteri del datore di lavoro tra legge e contratto*, Relazione alle Giornate di Studio Aidlass (Napoli, 16-17 giugno 2016), 40 del dattiloscritto; P. LAMBERTUCCI, *I poteri del datore di lavoro nello statuto dei lavoratori dopo l'attuazione del c.d.* Jobs Act *del 2015: primi spunti di*

duate nella obsolescenza della disciplina statutaria causata dalle nuove tecnologie e forse, ancor più, dall'imponente evoluzione della normativa generale in materia di tutela della riservatezza (in particolare, il Codice e la sua implementazione da parte del Garante). Opinione che, però, deve essere precisata aggiungendo che l'art. 4, pur risalente al 1970, venne replicato dal legislatore nel 2003, a dispetto della sua obsolescenza già allora conclamata, all'interno dell'art. 114 del Codice.

Quella disciplina era stata caratterizzata, però, sin dall'inizio, dal paradosso per cui la tutela in materia conseguiva non già all'operatività del meccanismo predisposto dal legislatore statutario (cioè il preventivo accordo sindacale o, in difetto, l'autorizzazione amministrativa), bensì alla sua mancata attuazione. Ciò poiché le imprese molto spesso neppure avviavano le trattative per concludere l'accordo previsto dall'art. 4, comma 2 ed i sindacati non si dolevano più di tanto di queste omissioni, forse anche con qualche sollievo per aver, così, evitato di essere coinvolti in negoziati di non facile gestione e sindacalmente poco interessanti.

A trarre occasionale vantaggio da tale situazione poteva essere, invece, il singolo lavoratore colpevole di un'infrazione disciplinare, magari anche di grave entità, ma documentabile soltanto utilizzando i controlli effettuati dal datore di lavoro in modo non conforme all'art. 4 e, per questo, non producibili in giudizio per provare la responsabilità del dipendente.

Quindi l'ipocrisia con la quale l'art. 4, comma 2 (vecchio testo) ha convissuto derivava proprio dalla manifesta inidoneità della norma a realizzare una tutela della riservatezza dei lavoratori.

In conclusione, si può dire che le modalità di realizzazione di questa

riflessione, in *Arg. dir. lav.*, 2016, 527; R. Del Punta, *La nuova disciplina dei contratti a distanza sul lavoro (art. 23 d.leg. n. 151/2015)*, in *Riv. it. dir. lav.*, 2016, I, 77; A. Bellavista, *Il nuovo art. 4 dello Statuto dei lavoratori*, in G. Zilio Grandi, M. Biasi (a cura di), *Commentario breve alla riforma "Jobs Act"*, Padova 2016, 717; M. Ricci, *I controlli a distanza dei lavoratori tra istanze di revisione e flessibilità «nel» lavoro*, in *Arg. dir. lav.*, 2016, 740; M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in *Arg. dir. lav.*, 2016, 484; L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, in *Riv. it. dir. lav.*, 2016, I, 369; A. Levi (a cura di), *Il nuovo art. 4 sui controlli a distanza*, Milano 2016; I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues*, 2016, v. 2, 3 ss.; V. Maio, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Arg. dir. lav.*, 2015, 1186; M.T. Salimbeni, *La riforma dell'art. 4 dello statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Riv. it. dir. lav.*, 2015, I, 589.

tutela finivano per trascurare l'interesse della generalità dei dipendenti alla loro riservatezza in se stessa considerata, proiettandosi invece sulle conseguenze disciplinari delle condotte illecite di singoli lavoratori riscontrate in violazione di tale disposizione.

Volgendo lo sguardo al nuovo testo dell'art. 4 se ne può percepire, in grandi linee, l'evoluzione isolando almeno tre profili che evidenziano i tratti di continuità e discontinuità rispetto alla norma statutaria, quanto ad interessi tutelati e tecniche di regolamentazione.

Il primo concerne l'approccio al tema dei controlli a distanza tecnologici che conferma la volontà del legislatore di assoggettare questi controlli a limiti specifici finalizzati a tutelare la riservatezza del dipendente, escludendo la liberalizzazione di tali controlli.

Il secondo riguarda, nel segno della discontinuità, forme e strumenti di realizzazione della tutela del lavoratore che si caratterizzano per il declino dell'accordo sindacale come condizione generale e sufficiente di legittimità dei controlli a distanza. Infatti, il bene della riservatezza del lavoratore viene garantito dal legislatore in forme più coerenti alla dimensione individuale e personale di tale diritto, con attenzione per le modalità e la misura del controllo da correlare alle funzioni che esso legittimamente può assolvere. Ciò in perfetta coerenza con l'impostazione data alla regolazione del trattamento dal Regolamento.

Il terzo profilo – che si pone in linea di sviluppo con quanto appena accennato – riguarda il raccordo, già più sopra anticipato, tra i controlli a distanza e l'utilizzabilità «delle informazioni raccolte [...] a tutti i fini connessi al rapporto di lavoro» (art. 4, comma 3). Un raccordo che chiarisce l'interazione funzionale dei poteri (in particolare, quelli di controllo e disciplinare) del datore di lavoro: da una parte il legittimo accertamento dell'infrazione e, dall'altra, la possibilità di sanzionarla.

Affianco a tali profili, va considerato che, pur in mancanza di una disposizione analoga a quella che si leggeva nel testo originario del comma 1 dell'art. 4, il nuovo testo continua a vietare al datore di lavoro di avvalersi di strumenti tecnologici per controllare a distanza la prestazione del dipendente, in quanto tali controlli sono ammessi «esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale» e, per converso, vietati in ogni altro e diverso caso.

L'opzione per il mantenimento anche nel nuovo art. 4, comma 1, del divieto statutario di controlli a distanza direttamente mirati sull'attività lavorativa e, quindi, l'esclusione del potenziamento tecnologico del potere di controllo del datore di lavoro va ricondotta e motivata con l'esigenza

di bilanciamento tra l'interesse del datore di lavoro di verificare l'esatta esecuzione della prestazione lavorativa, da una parte, e, dall'altra, la condizione di subordinazione del dipendente destinata altrimenti ad accentuarsi in forme più invasive e, per di più, connotate dal permanente disvalore per i controlli tecnologici realizzati dalla macchina sull'uomo[25].

Ai limitati fini del presente contributo è qui utile sottolineare la collocazione sistematica dei controlli riconducibili all'art. 4, comma 1, rispetto a quelli del comma 2 che, derivando dagli «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa» o da quelli «di registrazione degli accessi e delle presenze», sono sottratti all'applicazione del comma 1 dell'art. 4 (anche se assoggettati alle medesime tutele del comma 3) per espressa indicazione del legislatore.

Ciò avviene non già per una differenziazione delle due fattispecie che avrebbe indotto il legislatore a diversificare la disciplina applicabile, bensì per la ragione inversa: i controlli dell'attività lavorativa riconducibili al comma 2 dell'art. 4 sono effettuati da strumenti che, essendo adoperati per lavorare o accedere ai luoghi di lavoro, non possono per la loro stessa natura e funzione essere assoggettati ad una causale o motivazione che ne giustifica l'utilizzo né si potrebbe seriamente ipotizzare per essi la necessità di una preventiva autorizzazione sindacale o amministrativa[26], senza stravolgere il potere organizzativo del datore di lavoro che riguarda anche la scelta dei «mezzi» di cui il dipendente si avvale per svolgere la propria attività.

Si potrebbe, quindi, osservare che il comma 2 dell'art. 4 realizza una

[25] D'altronde è utile ricordare che la legge delega riguardava la «revisione della disciplina dei controlli a distanza» realizzati tramite «impianti» o «strumenti di lavoro», senza porre vincoli o stabilire criteri selettivi in funzione delle specifiche finalità del loro impiego, consentendo così al legislatore delegato di disciplinare tali controlli, «tenendo conto dell'evoluzione tecnologica», anche quando l'attività lavorativa fosse stata direttamente oggetto di essi, dovendo farsi comunque carico dell'imprescindibile contemperamento delle «esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore». La necessità di provvedere a tale contemperamento sta proprio a dimostrare che il controllo tecnologico non può ritenersi di per se stesso - e cioè prescindendo dalle modalità e dalla misura in cui avviene - sempre e comunque precluso perché lesivo della dignità o della riservatezza di chi lo subisce. Del resto, se così fosse, chiunque (consumatore, utente, ecc.) – e non solo il lavoratore – potrebbe invocare l'interdizione dei controlli a distanza che lo riguardano.

[26] La tesi era già sostenibile nel vigore dell'art. 4 nel testo statutario, v. da ultimo R. Del Punta, *op. cit.*, e, precedentemente, A. Maresca, S. Lucrezio Monticelli, *Tutela della riservatezza nei rapporti di lavoro: divieto di controllo a distanza e telelavoro*, in G. Santaniello (a cura di),*Trattato di Diritto Amministrativo*, vol. XXXVI, 2005, 537 ss. e, sul punto, 552.

sorta di presunzione assoluta della legittimità del controllo indotto dagli strumenti ivi previsti, attesa la funzione primaria da essi assolta di «rendere la prestazione lavorativa». Su questo aspetto toneremo più avanti.

9. *La (ri)definizione e sistematizzazione dei c.d. controlli difensivi*

Le considerazioni appena svolte consentono di mettere a fuoco alcune questioni che, specialmente nella fase applicativa della norma, hanno creato e potrebbero ancora creare incertezze e confusioni. Questioni di rilevante importanza per definire con chiarezza l'ambito della regolazione riservato alla disciplina in materia di privacy (Regolamento e Codice) rispetto a quello sul quale è destinato ad operare l'art. 4, L. 300/1970.

In questa logica, la prima questione, solo apparentemente banale, riguarda la distinzione tra esercizio del controllo a distanza ed utilizzo dei dati derivanti da tale controllo. Infatti, accade spesso che questi due aspetti vengano sovrapposti e percepiti come se fossero riconducibili ad un unico atto catalogabile come esercizio del potere di controllo. Ciò accade perché molto spesso l'avvenuto controllo, cioè l'acquisizione del dato, si manifesta in modo visibile soltanto quando si procede alla sua utilizzazione nei confronti del singolo lavoratore.

Per chiarire il punto occorre fare riferimento (almeno) a tre fasi cronologicamente e funzionalmente distinte: la prima riguarda l'acquisizione dei dati relativi all'attività lavorativa, come conseguenza automatica della tecnologia utilizzata dal dipendente per svolgere l'attività lavorativa; la seconda concerne la conservazione dei dati, cioè la loro memorizzazione; la terza – che è meramente eventuale – attiene all'utilizzazione dei dati per la gestione del rapporto di lavoro. La sequenza delle tre fasi connota e caratterizza la tipologia dei controlli tecnologici prevista dall'art. 4; controlli che, appunto, vengono definiti «a distanza» per segnare lo spazio di luogo o di tempo che intercorre tra il momento o il luogo in cui il dato inerente all'attività lavorativa viene a formarsi, quello della raccolta/acquisizione, quello della conservazione e, infine, dell'utilizzazione.

I limiti posti dal nuovo art. 4 scandiscono bene (e, comunque, più nitidamente di quanto avveniva con la norma statutaria) le tutele del lavoratore con riferimento alle varie fasi, tenendo conto che il controllo a distanza si configura esaustivamente nel momento in cui il dato viene acquisito (e memorizzato), anche prescindendo dalla sua utilizzazione che è solo eventuale.

Si potrebbe ulteriormente precisare che all'interno dell'art. 4 l'acquisizione del dato relativo all'attività lavorativa integra l'esercizio del potere di controllo secondo quanto stabilito dai commi 1 e 2; mentre il comma 3 detta le regole per l'utilizzazione del dato «a tutti i fini connessi al rapporto di lavoro» e ciò attiene non già al potere di controllo, bensì a quelli di gestione del rapporto di lavoro, in particolare (ma non solo) al potere disciplinare. Una distinzione che, peraltro, si riflette anche sul regime sanzionatorio previsto dall'art. 171, Codice che attribuisce rilievo penale alle violazioni dei soli commi 1 e 2 dell'art. 4 e non del comma 3.

Alla stregua delle considerazioni accennate non appare quindi possibile sostenere, ad esempio, che i limiti al potere di controllo posti dall'art. 4 troverebbero applicazione e si attiverebbero non già nel momento in cui lo «strumento» acquisisce il dato attinente all'attività lavorativa, ma soltanto quando tale dato, seppure già residente nella memoria di un server aziendale, viene esaminato per valutarne la rilevanza ai fini disciplinari, cioè nel caso della sua utilizzazione. La conseguenza di una simile impostazione sarebbe infatti paradossale: l'accordo sindacale o l'autorizzazione amministrativa dovrebbero essere richiesti soltanto se il datore di lavoro fosse interessato ad utilizzare il dato, mentre è proprio l'acquisizione di esso che pone il tema della tutela della riservatezza a presidio della quale opera l'art. 4. D'altronde una simile interpretazione si rivelerebbe incompatibile anche con quanto prescritto dal Regolamento ed in particolare con il principio di minimizzazione dei dati che impone che i dati siano acquisiti, a prescindere dalla loro successiva catalogazione, solo in quanto necessari alla realizzazione delle finalità legittime che hanno giustificato il trattamento.

Tenendo presente quanto appena esposto si può prendere posizione anche sui c.d. controlli difensivi.

Naturalmente la questione viene affrontata in questa sede soltanto per verificare l'affermazione ricorrente[27] per cui tale tematica sarebbe oggi superata perché ricompresa nel nuovo art. 4 e, in particolare, nella previsione contenuta nel comma 1 in ordine ai controlli finalizzati alla tutela del patrimonio aziendale, con la conseguenza che l'attivazione di controlli difensivi potrebbe oggi avvenire soltanto previo accordo sindacale o autorizzazione amministrativa[28].

[27] V., per tutti, P. LAMBERTUCCI, *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli "a distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014*, *WP CSDLE "Massimo D'Antona".IT, n. 255/2014*, e M.T. SALIMBENI, *op. cit.*, 589 ss.

[28] Così: E. BALLETTI, *op. cit.*, 40 del dattiloscritto; I. ALVINO, *op. cit*., 18.

Limitandoci a questo profilo si può inizialmente osservare che i c.d. controlli difensivi sono stati utilizzati dalla giurisprudenza per sostenere l'inapplicabilità dell'art. 4 (vecchio testo) e, quindi, la legittimità del controllo anche in assenza del preventivo accordo sindacale, atteso che oggetto del controllo sarebbe stata non già l'attività lavorativa, bensì l'illecito commesso in occasione della prestazione resa dal dipendente al datore di lavoro.

Questa tesi – mutuata da quella che ammette, ex art. 3 St. lav., i controlli occulti tramite agenzie investigative finalizzati ad accertare condotte penalmente rilevanti dei dipendenti durante il servizio[29] – sembra difficilmente armonizzabile con la regolamentazione dei controlli tecnologici contenuta nell'art. 4, proprio per le modalità di funzionamento di tali controlli.

Infatti mentre l'incarico affidato ad un'agenzia investigativa può essere circoscritto alle sole indagini necessarie ad accertare la condotta illecita del singolo dipendente ed essere considerato legittimo proprio perché così delimitato, viceversa il controllo tecnologico derivante, ad esempio, dall'utilizzo di un sistema informatico registra l'insieme di tutti i dati relativi all'attività lavorativa svolta indistintamente dalla generalità dei dipendenti senza alcuna selettività né soggettiva né oggettiva.

In questo caso, quindi, non si può configurare un controllo difensivo proprio perché il controllo non è focalizzato sull'attività illecita, ma indistintamente sulla prestazione lavorativa nel suo complesso resa da tutto il personale dipendente.

E non appare neppure possibile che tale qualificazione avvenga, per così dire a posteriori, cioè quando dall'analisi dei dati acquisiti riferita alla generalità dei lavoratori si riscontra una condotta illecita di un singolo dipendente[30]. Infatti, in questo caso il controllo a distanza è avvenuto quando sono stati acquisiti e memorizzati i dati relativi all'ordinaria attività lavorativa svolta dal personale dipendente ed a tale controllo trova si-

[29] Cfr., tra le più recenti, Cass., sez. lav., 4 dicembre 2014, n. 25674, in *Foro it.*, 2015, I, 1671.

[30] Per un esempio significativo di questo indirizzo giurisprudenziale v. Cass., sez. V pen., 12 luglio 2011, n. 34842, per la quale «sono utilizzabili nel processo penale le prove di reato acquisite nei confronti di un dipendente mediante videoriprese effettuate con telecamere installate all'interno del luogo di lavoro, ad opera del datore di lavoro, per esercitare un controllo a beneficio del patrimonio aziendale messo a rischio da possibili comportamenti infedeli dei lavoratori, perché le norme dello statuto dei lavoratori poste a presidio della loro riservatezza, non fanno divieto dei c.d. controlli difensivi del patrimonio aziendale e non giustificano, pertanto, l'esistenza di un divieto probatorio».

cura applicazione l'art. 4 la cui violazione rende illegittimo il controllo effettuato; senza alcuna possibilità che l'accertamento di comportamenti illeciti del dipendente in base ai dati complessivi già raccolti possa legittimare, con effetto retroattivo, il controllo ormai consumato.

Riprendendo le precisazioni svolte in precedenza, si può dire che l'accertamento dell'illecito del lavoratore avviene, invero, nella fase di utilizzo dei dati a fini disciplinari, da distinguere da quella del controllo a distanza che si è consumata precedentemente con l'acquisizione dei dati.

Ciò non esclude in assoluto la possibilità di attivare un controllo realmente difensivo attraverso strumenti tecnologici al di fuori dell'ambito di applicabilità dell'art. 4, ma ciò può avvenire quando il sistema informatico (o una sua funzione) viene tarato in modo tale da accertare soltanto condotte illecite del dipendente e non già l'attività lavorativa nel suo complesso: ad esempio un software mirato a verificare l'autore di reati informatici.

Le considerazioni appena svolte consentono di ribadire che anche il nuovo art. 4 non si applica ai controlli difensivi – nel senso, torno a precisare, dei controlli aventi ad oggetto condotte illecite – che, conseguentemente, potranno essere attivati anche senza accordo sindacale o autorizzazione amministrativa.

Seguendo questa che sembra l'impostazione preferibile del problema, si può aggiungere che la previsione (art. 4, comma 1) dei controlli sul patrimonio aziendale dovrebbe consentire di ricondurre i controlli difensivi nel loro originario e corretto alveo.

Ciò potrebbe avvenire distinguendo tra: A) controlli a difesa del patrimonio aziendale costituito dai beni materiali ed immateriali di cui l'imprenditore ha la proprietà o il godimento e che riguardano la generalità dei dipendenti (o parte di essi) nello svolgimento della loro normale attività lavorativa che li pone a contatto con tale patrimonio. Questi controlli dovranno avvenire nel rispetto delle previsioni dell'art. 4, comma 1, ma anche del comma 3; B) controlli difensivi in senso stretto, mirati ad accertare selettivamente condotte illecite – anche di aggressione al patrimonio aziendale – di cui si presume, in base ad indizi concreti, siano autori singoli (o alcuni) dipendenti, anche se ciò avviene in occasione dello svolgimento della prestazione lavorativa. In questo caso si tratta di indagini che, salvo quelle condotte direttamente dalle autorità di polizia o dalla magistratura (il che esclude ovviamente l'applicazione dell'art. 4), possono essere attivate dal datore di lavoro avvalendosi di idonei strumenti tecnologici. Questi controlli si collocano al di fuori dell'ambito applicativo dell'art. 4, non avendo ad oggetto l'attività del lavoratore.

Peraltro tale impostazione appare perfettamente coerente con l'impostazione data alla tutela dei dati personali dal Regolamento, poiché anche in questo caso la registrazione dei dati e il loro successivo trattamento verrebbe svolto in conformità ai principi di liceità e correttezza in quanto funzionali al contrasto e alla punizione di utilizzi illeciti degli strumenti tecnologici.

10. *Condizioni di legittimità dei controlli a distanza: l'accordo sindacale e l'autorizzazione amministrativa*

Esula dall'oggetto specifico di questo contributo, un'analisi puntuale dei contenuti dell'art. 4. Meritano però di essere ricordati alcuni tra gli aspetti più innovativi della disposizione i cui contenuti si affiancano e vanno letti in maniera coerente con le disposizioni del Regolamento.

Al riguardo, va innanzitutto considerato che l'accordo sindacale, diversamente da quanto accadeva precedentemente, può essere stipulato anche con le «associazioni sindacali comparativamente più rappresentative sul piano nazionale» quando i controlli a distanza riguardano «imprese con unità produttive ubicate in diverse province».

Il legislatore si è fatto carico del problema – ricorrente nella pratica – delle aziende plurilocalizzate che si avvalgono di sistemi di controllo a distanza identici da istallare nelle varie unità produttive. In questi casi sarebbe stato irragionevole imporre la moltiplicazione degli accordi per ogni unità produttiva, per di più con la possibilità di esiti diversificati, avendo ciascuna RSA/RSU, per l'unità produttiva ove è costituita, la facoltà di negare il consenso all'accordo che, invece, avrebbe potuto essere concluso in altre unità produttive.

Il primo punto da segnalare al riguardo è che la trattativa con le associazioni sindacali esterne, anziché con la RSA/RSU, costituisce un'alternativa facoltativa e non già l'attribuzione di una competenza esclusiva riconosciuta a tali associazioni e sottratta alle rappresentanze sindacali costituite nell'azienda. Si tratta, quindi, di una legittimazione concorrente che implica l'eventualità di un raccordo tra le due strutture sindacali secondo prassi che caratterizzeranno le relazioni sindacali di ogni singola azienda o valutazioni effettuate di volta in volta.

Da quanto accennato si può dedurre che se il datore di lavoro sollecitasse l'apertura della trattativa per stipulare l'accordo previsto dall'art. 4, comma 1, nei confronti di uno qualsiasi dei soggetti sindacali legittimati, l'eventuale rifiuto (anche se opposto soltanto per declinare la com-

petenza a favore di un diverso soggetto sindacale) varrebbe a configurare la condizione sufficiente per richiedere l'autorizzazione in via amministrativa, attesa la «mancanza di accordo».

Per quanto riguarda l'autorizzazione amministrativa – che può essere richiesta solo dopo aver negativamente sperimentata la via dell'accordo sindacale (depongono in tal senso la diversificazione dei termini utilizzati nel comma 1, art. 4: «in alternativa», «in mancanza») – le novità principali da segnalare sono almeno due, una esplicitata dal legislatore e l'altra implicita.

La prima riguarda la facoltà per le «imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali» dell'Ispettorato nazionale del lavoro di chiedere «in alternativa» a quest'ultimo un'unica autorizzazione.

A prescindere dall'evidente semplificazione che la nuova norma comporta, ciò avrà nel tempo anche un ulteriore effetto particolarmente significativo, perché man mano che l'Ispettorato nazionale del lavoro sarà chiamato ad esprimere le autorizzazioni si formerà, con riferimento agli «strumenti» di controllo a distanza aventi funzioni identiche o molto simili, una giurisprudenza che con i suoi precedenti – la cui uniformità dovrebbe essere assicurata dall'unicità del soggetto decisore a livello nazionale[31] – condizionerà i comportamenti delle imprese, ma anche dei sindacati e delle sedi territoriali dell'Ispettorato nazionale del lavoro.

Le considerazioni svolte mettono in luce l'altra implicazione indotta dal sistema a cui si è accennato per quanto riguarda i riflessi che potranno prodursi sulla posizione delle parti nella trattativa sindacale prevista dall'art. 4, comma 1.

Infatti mentre i sindacati potranno del tutto legittimamente richiedere che i dati acquisiti dal datore di lavoro a seguito dei controlli a distanza non siano utilizzabili a fini disciplinari[32], tale posizione non potrà essere

[31] Certamente i primi esiti non sono incoraggianti, anche se le iniziali difficoltà interpretative possono giustificare orientamenti divergenti. Ci si riferisce al parere reso il 10 maggio 2016 dalla Direzione interregionale di Milano «in merito a GPS da installare su autovetture aziendali» che riconduce tale sistema di controllo al comma 2 dell'art. 4 ed al provvedimento di segno opposto della DTL (ora ITL) di Latina dell'11 maggio 2016 che, poi, la stessa DTL corregge in data 13 luglio 2016 uniformandosi al parere della Direzione milanese, riconducendo nell'ambito dell'art. 4, comma 2 la geolocalizzazione impiegata per esigenze di lavoro.

[32] In linea con il documento unitario di Cgil, Cisl e Uil del 14 gennaio 2016 intitolato *Un moderno sistema di relazioni industriali. Per un modello di sviluppo fondato sull'innovazione e la qualità del lavoro* dove, con riferimento alla nuova disciplina dell'art. 4, si afferma l'opportunità di «definire contrattualmente, tramite accordi con la RSU/RSA o, in

assunta dalle sedi territoriali e dall'Ispettorato nazionale del lavoro essendo per essi impegnativa la previsione del comma 3 dell'art. 4 per la quale «le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro».

11. *Le esenzioni riservate agli strumenti utilizzati per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze*

Si può ora volgere lo sguardo al comma 2 dell'art. 4 che affranca dai limiti previsti dal comma 1 gli «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa», nonché gli «strumenti di registrazione degli accessi e delle presenze».

Come già accennato, il legislatore muove da una duplice consapevolezza relativa a tali «strumenti» che, da una parte, assolvono alla funzione primaria di consentire al dipendente di rendere la prestazione e, quindi, adempiere agli impegni contrattuali che devono conformarsi all'organizzazione del lavoro come predisposta dall'imprenditore, ma, dall'altra, hanno un'indubbia e rilevante capacità di controllo a distanza dell'attività lavorativa.

Conseguentemente il legislatore ha ritenuto, ragionevolmente, di non poter imporre vincoli potenzialmente interdittivi all'impiego di tali strumenti, dovendo piuttosto occuparsi di tutelare il dipendente per quanto riguarda le «informazioni raccolte» dal datore di lavoro tramite gli stessi strumenti, anche perché tali informazioni sono «utilizzabili a tutti i fini connessi al rapporto di lavoro». A tale necessità provvede il comma 3 dell'art. 4.

Muovendo da queste premesse, si deve affrontare il nodo problematico relativo all'identificazione degli «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa».

L'esame deve iniziare dalla relazione intercorrente tra gli «strumenti» del comma 1 e quelli del comma 2 dell'art. 4, per chiarire ciò che li differenzia: le loro caratteristiche morfologiche o piuttosto le finalità del loro impiego? La soluzione corretta appare quest'ultima, come suggerisce l'apertura del comma 2 quando avverte che «la disposizione di cui al comma 1 non si applica [...]»; precisazione necessaria, attesa l'insussi-

assenza, con le OO.SS., i meccanismi certi di preventiva informazione del lavoratore circa le regole interne e l'utilizzo dei dati acquisiti, alla luce delle nuove norme sui controlli a distanza ed escludendo, comunque, l'utilizzo dei dati per fini disciplinari».

stenza di una differenziazione ontologica tra tali «strumenti», per affermare l'inoperatività del comma 1 quando gli stessi «strumenti» siano utilizzati per le finalità del comma 2.

Quindi la distinzione tra comma 1 e 2 dell'art. 4 si coglie guardando alla funzione che gli «strumenti» assolvono nell'organizzazione predisposta dal datore di lavoro e non già alle loro caratteristiche oggettive.

Di qui alcune precisazioni.

La prima riguarda il termine «strumenti» che deve intendersi riferito alle due componenti di qualsiasi sistema informatico: l'hardware (dal computer, al *tablet*, allo *smartphone*, al *device*, ecc.) che consente l'accesso ai vari tipi di software e di applicativi che animano il sistema ed il suo funzionamento; senza di essi le apparecchiature resterebbero inerti, anche quanto alla generazione di controlli a distanza. Quindi la riconducibilità degli «strumenti» nel comma 1 o 2 dell'art. 4 deve avvenire in relazione non solo all'hardware, ma anche e prevalentemente al software, quindi ai programmi a cui accede il dipendente.

Da quanto ora accennato discende anche che gli «strumenti» di cui al comma 2 non si possono identificare con gli strumenti di lavoro nel significato più tradizionale del termine, cioè di attrezzi o dotazioni individuali assegnati a ciascun dipendente per lo svolgimento del proprio lavoro.

Anzi molto spesso tali strumenti si immedesimano con il/i sistema/i informatico/i di cui l'impresa si è dotata centralmente al quale si connettono i lavoratori utilizzando postazioni (periferiche) fisse o mobili per svolgere le attività di loro competenza.

L'art. 4, comma 2, non pone preclusioni per quanto riguarda gli strumenti informatici utilizzabili dai dipendenti e neppure limiti alla competenza ed alle valutazioni del datore di lavoro che, quindi, restano insindacabili anche in ragione della maggiore o minore incidenza di tali strumenti sulla riservatezza dei lavoratori[33]. Infatti il comma 2 dell'art. 4 riguarda tutti gli «strumenti» accomunati dal fatto oggettivo dell'impiego da parte del prestatore a seguito delle decisioni imprenditoriali prese, come già detto, dal datore di lavoro.

L'ambito di applicazione del comma 2 dell'art. 4 è contraddistinto anche dal fatto che gli «strumenti» devono servire al dipendente «per rendere la prestazione lavorativa». Una formulazione ampia all'interno

[33] Sul punto v. V. PINTO, *La flessibilità funzionale e i poteri del datore di lavoro. Prime considerazioni sui decreti attuativi del* Jobs Act *e sul lavoro agile*, in *Riv. giur. lav.*, 2016, I, 344 ss. e, sul punto, 348.

della quale non sembra possibile differenziare gli strumenti allorché siano utilizzati per organizzare oppure per eseguire la prestazione lavorativa, limitando a questi ultimi la previsione dell'art. 4, comma 2 e riconducendo gli altri al comma 1.

Si tratta, infatti, di una distinzione priva di riscontro testuale, in quanto l'art. 4, comma 2, prende in considerazione tutti gli strumenti che a vario titolo concorrono per consentire al lavoratore di «rendere la prestazione lavorativa» e ciò avviene ogni qualvolta lo stesso lavoratore si attiva per dare impulso al loro funzionamento, ma anche quando il dipendente se ne avvale (o vi accede) per acquisire dati utili per rendere tale prestazione.

Le precisazioni fin qui accennate consentono di affrontare una delle casistiche oggi più ricorrenti, quella dei sistemi di geolocalizzazione in uso al dipendente attivabili da un *tablet* o da uno *smartphone*; geolocalizzazione che appare opportuno prendere in considerazione anche per dare atto della pluralità di soluzioni prospettabili in relazione ai diversi usi di uno stesso strumento.

Il sistema di geolocalizzazione rientra tra gli strumenti previsti dal comma 2 dell'art. 4, quando è utilizzato, ad esempio, da un tecnico tenuto a rendere una prestazione lavorativa che comporta spostamenti da un luogo all'altro a seconda degli interventi da eseguire; interventi che la geolocalizzazione consente di realizzare con maggiore rapidità, segnalando al tecnico il luogo da raggiungere in quel momento più vicino (ed anche con minor disagio personale limitando gli spostamenti).

Ad una diversa conclusione si deve giungere quando la prestazione del lavoratore non è caratterizzata da alcuna mobilità territoriale, in questo caso il sistema di geolocalizzazione non è funzionale a rendere tale prestazione e, quindi, potrebbe rientrare nel comma 1 dell'art. 4 (con la conseguenza che sarebbe attivabile solo dopo l'accordo sindacale o l'autorizzazione dell'Ispettorato) sempre che sussista almeno una delle ragioni ivi previste: ad esempio la geolocalizzazione dell'auto condotta dal dipendente a tutela del bene aziendale.

Fin qui si è detto dei sistemi di geolocalizzazione che realizzano anche un controllo a distanza dell'attività del dipendente, ma potrebbe accadere che i dati acquisiti non siano accessibili al datore di lavoro il che esclude l'applicazione dell'art. 4; ad esempio quando il sistema è nella disponibilità della sola compagnia di assicurazione che, a fronte di questa dotazione (c.d. *black box*), riduce il costo della polizza.

Il collegamento operato dal comma 2 dell'art. 4 tra utilizzo degli «strumenti» e «prestazione lavorativa» consente di affrontare anche la questione relativa a quei controlli a distanza attivati dal datore di lavoro

in adempimento di obblighi posti dalla legge o da una Authority (Consob, Agcom, ecc.) a tutela degli interessi di terzi (ad esempio gli utenti di un servizio). Si tratta di casi, per limitarci solo a qualche riferimento, nei quali si deve procedere alla registrazione del colloquio telefonico nel corso del quale un dipendente raccoglie un ordine di borsa o conclude un contratto di fornitura di servizi con un utente.

In queste ipotesi la registrazione documenta non solo il contratto, ma anche l'operato del dipendente venendo così a configurare un controllo a distanza sull'attività lavorativa che sembra riconducibile nel comma 2 dell'art. 4, proprio perché la prestazione del lavoratore non potrebbe essere resa con una modalità diversa da quella che realizza il controllo a distanza dello stesso dipendente.

C'è poi da aggiungere che in questo caso la protezione dell'interesse dell'utente assume, secondo la valutazione espressa dall'ordinamento, carattere cogente e necessario, come tale inconciliabile con la previsione dell'art. 4, comma 1 che sottopone il controllo a distanza alla preventiva autorizzazione sindacale o dell'Ispettorato, non residuando in capo a questi soggetti alcun margine di valutazione in ordine all'attivazione del controllo ed essendo presidiata dal comma 3 (anche con il richiamo al Codice) la tutela dovuta al dipendente quanto alla sua esposizione al controllo.

Sulla scorta di questi spunti si può spostare l'attenzione su un profilo problematico relativo all'applicazione dell'art. 4, comma 2 quando si tratti di sistemi di sicurezza del lavoro il cui impiego è monitorato a distanza dal datore di lavoro con inevitabili implicazioni anche sul controllo dell'attività lavorativa.

In prima battuta tali sistemi sembrerebbero rientrare nella previsione del comma 1 dell'art. 4 che espressamente riguarda gli «strumenti» «per la sicurezza del lavoro». Ma se l'evoluzione tecnologica dovesse evidenziarne la particolare efficacia nel presidio della sicurezza del lavoratore – magari in alcuni contesti produttivi dove i rischi sono più elevati e tali da rendere necessario il potenziamento delle azioni di contrasto – si potrebbe ipotizzare che la sicurezza tecnologica così garantita al dipendente diventi una modalità della prestazione lavorativa obbligata ex art. 2087 c.c.

Si deve, inoltre, considerare che il comma 1 dell'art. 4 realizza – come in precedenza segnalato – un bilanciamento dei contrapposti interessi, del datore di lavoro al controllo e del dipendente alla riservatezza. Ma tale bilanciamento non può riguardare il caso in esame dove non si pone il tema della tutela degli interessi datoriali all'esercizio del potere di controllo sull'attività lavorativa, bensì quello dell'obbligo di favorire la sicurezza dei dipendenti nelle forme tecnologicamente più evolute.

In questa prospettiva si potrebbe, quindi, avviare una riflessione sul comma 1 dell'art. 4 per escluderne l'applicazione laddove il controllo a distanza non sia finalizzato a realizzare un interesse del datore di lavoro quale creditore della prestazione lavorativa, quanto piuttosto quello del dipendente assoggettato sì ad un controllo a distanza, ma a tutela della sua sicurezza. Questo primo passaggio consentirebbe, poi, di ricondurre al comma 2 dell'art. 4 (e sempre nel rispetto delle tutele del comma 3) il caso in esame trattandosi di controlli derivanti dall'impiego di strumenti necessari per rendere la prestazione lavorativa, in quanto ne garantirebbero la sicurezza.

Un ultimo cenno sempre relativo all'ambito di applicazione del comma 2 dell'art. 4 riguarda la distinzione tra i controlli a distanza derivanti dall'impiego di software «utilizzati dal lavoratore per rendere la prestazione lavorativa» e l'implementazione di uno di questi software con funzioni aggiuntive, specificamente attivate per misurare il livello quali-quantitativo della produttività del lavoratore.

Nel caso in esame i controlli a distanza riconducibili all'art. 4, comma 2 sono quelli che derivano, secondo una non facile indagine tecnica più che giuridica, da un software dotato di varie funzioni sviluppate in modo integrato per lo svolgimento dell'attività lavorativa, ma che realizzano simultaneamente anche un controllo della produttività del singolo dipendente.

Se, invece, quest'ultimo controllo (sulla qualità/efficacia della prestazione) è realizzato da uno sviluppo applicativo originato dallo stesso software che, però, acquisisce una sua autonoma e specifica operatività rispetto alle funzioni di cui si avvale il dipendente per rendere la prestazione lavorativa, il controllo non sarà vietato dall'art. 4 se persegue «esigenze organizzative e produttive» del datore di lavoro, ma richiede il preventivo accordo sindacale o l'autorizzazione dell'Ispettorato essendo riconducibile al comma 1.

Appare più agevole l'identificazione degli «strumenti di registrazione degli accessi e delle presenze» a cui si riferisce l'art. 4, comma 2.

Con questa norma il legislatore intende, probabilmente, prendere posizione rispetto ad un orientamento della giurisprudenza – non univoco, ma accolto anche dalla Cassazione[34] – che affermava l'applicabilità dell'art. 4 (vecchio testo) al sistema informatizzato di rilevazione delle presenze all'inizio ed alla fine dell'orario di lavoro, in quanto idoneo a realizzare un controllo a distanza sui tempi della prestazione dovuta dal la-

[34] Cass., sez. lav., 17 luglio 2007, n. 15892, in *Riv. giur. lav.*, 2008, II, 358 ss., con nota di A. BELLAVISTA, e per la giurisprudenza di merito Trib. Napoli 29 settembre 2010, in *Riv. it. dir. lav.*, 2011, II, 31 ss.; soluzione recentemente confermata da Cass., sez. lav., 13 maggio 2016, n. 9904, in *Giur.it.*, 2016, I, con nota di M. MARAZZA.

voratore, con la conseguenza che l'attivazione di tale sistema avrebbe dovuto essere preceduta dall'accordo sindacale o dell'autorizzazione amministrativa. Cosa che, peraltro, nella pratica avveniva molto raramente.

La norma vigente consente di ritenere superata tale questione equiparando i controlli delle presenze a quelli derivanti dagli strumenti di lavoro per i quali non occorre l'accordo sindacale o l'autorizzazione dell'Ispettorato del lavoro.

Semmai il problema interpretativo si può porre con riferimento al termine «presenze», perché il legislatore non precisa se si tratta soltanto di quelle che si registrano all'entrata ed in uscita e, quindi, lascia aperta la possibilità di un'interpretazione estensiva che consentirebbe l'utilizzo di strumenti in grado di monitorare a distanza la presenza mobile del dipendente anche all'interno dei luoghi di lavoro, vale a dire la mobilità e gli spostamenti effettuati dal lavoratore rispetto alla sua postazione.

Non credo che questa interpretazione – seppur letteralmente possibile – sia coerente con la *ratio* della norma che accomuna la registrazione degli accessi a quella delle presenze, evidenziando così che si tratta di due situazioni per le quali ricorre la medesima esigenza, cioè quella di acquisire un dato preciso relativo alla posizione del dipendente nel momento dell'accesso o di inizio o fine del lavoro; un dato che, attraverso il controllo, viene fissato nel tempo, tanto è vero che rispetto ad esso il legislatore ne prevede la «registrazione».

La rilevazione degli accessi può riguardare non soltanto l'ingresso in azienda (allorché si distingue dalla rilevazione dell'inizio dell'orario di servizio), ma anche il controllo di specifiche aree che, all'interno di uno stabilimento, sono riservate soltanto ad alcuni dipendenti, ad esempio per motivi di segretezza delle lavorazioni (oppure di sicurezza) che comportano l'esigenza di monitorare attraverso specifici varchi l'ingresso dei lavoratori.

Ci si potrebbe anche chiedere se il riferimento al controllo degli accessi di cui al comma 2 dell'art. 4, comprenda anche la connessione ai sistemi informatici aziendali.

L'estensione della regola prevista per gli accessi fisici anche a quelli informatici appare possibile sul piano interpretativo, anche se tale questione sembra assorbita e risolta alla stregua della prima parte del comma 2 nel cui ambito è più corretto ricondurre i collegamenti e le connessioni telematiche (ed i controlli a distanza che né conseguono) effettuati dal dipendente per realizzare la prestazione lavorativa.

12. *Controlli legittimi e utilizzabilità dei dati acquisiti per la gestione del rapporto di lavoro*

Nel comma 3 dell'art. 4 è racchiusa la tutela del dipendente destinata ad operare nella fase in cui, all'esito dei controlli a distanza legittimamente effettuati in conformità ai commi 1 e 2, il datore di lavoro si avvale dei dati acquisiti utilizzandoli «per tutti i fini connessi al rapporto di lavoro».

A ben vedere, quindi, la disposizione non riguarda l'esercizio del potere di controllo e le sue modalità, ma una fase successiva che si colloca a valle del controllo, anzi quando esso si è esaurito, essendo le «informazioni» entrate nella disponibilità del datore di lavoro che potrà utilizzarle, a distanza di tempo o di luogo dal momento della loro acquisizione.

I limiti posti dal legislatore nel comma 3 operano, quindi, con riferimento non esclusivamente al potere di controllo, ma anche alla gestione del rapporto di lavoro ed ai poteri che caratterizzano tale gestione, tra i quali pure quello disciplinare. Ben potendo il datore di lavoro avvalersi delle «informazioni», ad esempio, per valutazioni relative sia alla remunerazione della prestazione lavorativa in rapporto ai risultati raggiunti, sia alle competenze professionali del dipendente per il miglior impiego delle energie lavorative.

In altre parole la nuova norma opera un opportuno raccordo tra il potere di controllo tecnologico e gli altri poteri gestionali del datore di lavoro, venendo così a colmare una lacuna del vecchio art. 4 che, com'è noto, alimentava non poche incertezze applicative in ordine all'utilizzabilità dei dati derivanti dal controllo, potendosi ritenere che alla legittimità di tale controllo conseguisse ineluttabilmente la facoltà del datore di lavoro di avvalersene, ma anche, all'opposto, che il limite stabilito dal legislatore del 1970 ai controlli a distanza in funzione di «esigenze organizzative e produttive» o dettate «dalla sicurezza del lavoro» operasse pure con riferimento all'utilizzo dei dati acquisiti.

La questione si può ritenere oggi risolta con il comma 3 dell'art. 4 che incide in termini generali sulla posizione del datore di lavoro ogni qual volta decida di avvalersi dei dati raccolti. Decisione subordinata al rispetto delle condizioni («[...] a condizione [...]») indicate dal legislatore e più sopra ricordate, che tracciano il discrimine tra l'uso legittimo o illegittimo dei predetti dati.

Le considerazioni accennate sollecitano un duplice chiarimento per quanto concerne i soggetti destinatari della norma ed il momento in cui si configura l'utilizzabilità dei dati «a tutti i fini connessi al rapporto di lavoro».

Non c'è dubbio che il comma 3 dell'art. 4 riguarda il datore di lavoro, ma il suo raggio di azione appare più ampio perché in realtà coinvolge

tutti i soggetti a vario titolo competenti in materia di controlli tecnologici a distanza secondo la previsione del comma 1, si tratta: dei sindacati (RSU, RSA, ma anche dei sindacati comparativamente più rappresentativi a livello nazionale), dell'Ispettorato del lavoro (nazionale e territoriale) e dell'Autorità.

È, però, evidente che la norma non vincola i sindacati che ben potranno avanzare richieste per limitare i controlli o i loro effetti e tali richieste formeranno oggetto della trattativa con il datore di lavoro in funzione dell'eventuale accordo di cui al comma 1 (come già segnalato, ciò avverrà sicuramente con riferimento alla non utilizzabilità dei dati a fini disciplinari).

Diversamente si deve dire per l'Ispettorato e per il Garante per i quali la regola posta dal legislatore nel comma 3 dell'art. 4 risulta impegnativa e dovrà conformare il loro operato.

La seconda questione è più complessa e sottile, ma altrettanto rilevante.

Infatti si tratta di capire quando si configura (cioè dove inizia a porsi il tema del)l'utilizzazione dei dati da parte del datore di lavoro che potrà avvenire soltanto nel momento in cui si saranno realizzate le condizioni imposte dal legislatore nel comma 3. Ciò significa, in altre parole, tracciare il confine tra l'esercizio del potere di controllo (commi 1 e 2 dell'art. 4) e ciò che si pone a valle di esso.

In questa prospettiva – e riprendendo questioni già accennate – appare possibile far coincidere l'utilizzazione dei dati con l'esame e la valutazione degli stessi da parte del datore di lavoro. Si tratta di un'operazione distinta e distinguibile: infatti essa è prodromica rispetto all'altra relativa ai provvedimenti che saranno adottati dal datore di lavoro, ma è successiva alla raccolta e memorizzazione dei dati.

Seguendo questo ragionamento si potrebbe dire che il datore di lavoro deve ottemperare alle condizioni poste dal comma 3 dell'art. 4 soltanto nel momento in cui decide di procedere all'esame dei dati legittimamente raccolti attraverso il sistema di controllo a distanza. Infatti soltanto dal collegamento tra tali dati ed il singolo lavoratore scaturisce per quest'ultimo la necessità di fruire delle garanzie apprestate dal legislatore.

Ne consegue che il datore di lavoro è tenuto ad ottemperare alle condizioni poste dal comma 3 dell'art. 4 allorché procede ad analizzare e valutare i dati raccolti che, pur essendo nella sua disponibilità, solo in questo caso verranno evidenziati nel loro collegamento con la prestazione del singolo lavoratore, identificandosi in ciò il primo atto di utilizzo dei dati.

Riprendendo quanto già detto, la raccolta dei dati (cioè l'esercizio del

potere di controllo del datore di lavoro) dovrà avvenire nel rispetto del comma 1 dell'art. 4 (quindi previo accordo sindacale o autorizzazione dell'Ispettorato, salvi i casi riconducibili nel comma 2) a tutela della riservatezza della generalità dei lavoratori, mentre l'utilizzo dei dati postula l'«adeguata informazione» a protezione della posizione dei dipendenti che assume rilievo nel momento in cui il datore di lavoro decide di avvalersi di tali dati.

È necessario precisare che tale decisione non potrà riguardare *ad personam* un singolo dipendente, ma dovrà realizzarsi per tutti i dati acquisiti nei confronti dei lavoratori sottoposti al medesimo sistema di controllo a distanza, proprio perché in tal modo i dati vengono associati alla persona del prestatore di lavoro.

Sul piano applicativo le considerazioni svolte inducono ad ipotizzare la possibilità di un diverso approccio del datore di lavoro all'obbligo dell'«adeguata informazione» nei confronti del personale dipendente che in alcune occasioni (ad esempio per quanto attiene alla rilevazione delle presenze) sarà necessitata dall'utilizzazione routinaria di queste informazioni, mentre in altri casi avverrà se e quando il datore di lavoro intenderà avviare un esame dei dati raccolti, ma, beninteso, prima che tale esame venga esperito. Naturalmente l'ipotesi a cui si è accennato potrà porsi in concreto soltanto per quei dati che siano distinguibili e separabili, consentendo l'esame di alcuni di essi e non di altri.

13. *L'informazione trasparente al lavoratore come condizione per l'utilizzabilità dei dati raccolti dal datore di lavoro*

La ricostruzione del dato normativo, fin qui accennata nei suoi tratti essenziali, porta a ritenere che l'informazione dovuta dal datore di lavoro ex art. 4, comma 3 realizza una tutela della persona del dipendente fondata sulla trasparenza. Ciò nella convinzione che l'obbligo di rendere edotto il lavoratore in ordine ai controlli a cui è sottoposto costituisce la modalità più efficace per proteggerlo non dal controllo, già avvenuto nel rispetto dei limiti previsti dal legislatore (commi 1 e 2 dell'art. 4), ma dall'utilizzo dei dati per le potenziali ripercussioni sulla posizione del prestatore nell'ambito del rapporto di lavoro (per quanto riguarda i profili disciplinari, ma non soltanto questi).

Ciò sta a significare che l'interesse del lavoratore in tal modo salvaguardato dal legislatore non è quello alla riservatezza il cui presidio è affidato, come più sopra messo in rilievo, ai principi generali sanciti dal Regolamento e dal Codice ed al bilanciamento con il potere datoriale di con-

trollo realizzato dai commi 1 e 2 dell'art. 4, ma quello alla verificabilità del corretto procedimento di trattamento dei dati.

Infatti l'adeguata informazione imposta dal comma 3 dell'art. 4 implica la trasparente rappresentazione di tutto l'iter che va dalle modalità d'uso dello strumento di cui si avvale il dipendente alla raccolta dei dati relativi alla prestazione lavorativa. Ciò dovrebbe consentire al lavoratore di evidenziare errori o manipolazioni delle informazioni che il datore di lavoro intende utilizzare, acquisendo elementi per difendersi di fronte a tali controlli, proprio perché esercitati con modalità palesi e non occulte.

Tale prospettiva dà quindi ragione della natura speciale dell'art. 4 rispetto all'ambito oggetto di regolazione da parte del Regolamento. Specialità che comunque permette di riscontrare la convergenza sul valore di fondo delle due discipline identificabile nell'obbligo di informazione funzionale alla piena realizzazione anche dei principi in materia di protezione dei dati personali.

Il divieto di controlli occulti sulla prestazione lavorativa costituisce, quindi, il principio guida che accomuna nello Statuto dei lavoratori i controlli disciplinati dall'art. 3 con quelli dell'art. 4.

A questo punto ci si deve chiedere quali siano le modalità dell'«adeguata informazione» da rendere al lavoratore.

Partendo dalla scontata considerazione che l'informativa, proprio perché è tale, non richiede alcuna accettazione dei lavoratori che ne sono destinatari, le questioni che si pongono riguardano almeno due profili: il contenuto dell'informativa e le modalità con le quali la stessa deve essere portata a conoscenza del personale dipendente.

Quanto all'adeguatezza del suo contenuto i due riferimenti forniti dal legislatore – le «modalità d'uso degli strumenti» e l'«effettuazione dei controlli» – sembrano costituire un'endiadi utilizzata dal legislatore per chiarire le finalità stesse dell'informativa e, così, individuarne il contenuto necessario. I due riferimenti, quindi, devono essere considerati in modo concorrente e coordinato, nel senso che le modalità d'uso – delle quali occorre dare conto nell'informativa – sono quelle da cui consegue il controllo, cioè l'acquisizione dei dati relativi alla prestazione lavorativa del dipendente. Non si tratta, quindi, di redigere un manualetto di istruzioni per l'impiego dello strumento, ma di identificare le modalità del suo utilizzo che comportano l'acquisizione di dati relativi al lavoratore. In poche parole, spiegare come l'uso dello strumento si raccorda con il controllo che ne deriva.

La quantità delle informazioni da trasmettere al lavoratore non dovrà essere eccessiva, perché costituisce un dato di comune esperienza che la

sovrabbondanza non favorisce la conoscibilità e la comprensione delle stesse informazioni che, anzi, richiedono un'esposizione completa, ma sintetica.

Proprio per questo appare preferibile un'informazione mirata e non generalizzata, nel senso che tale informazione dovrà riguardare gli strumenti utilizzati (o utilizzabili) dal lavoratore che così vengono ad essere identificati con riferimento ai controlli cui è sottoposto ciascun dipendente (o gruppi di lavoratori che utilizzano gli stessi strumenti). Invece un'informativa rivolta alla generalità dei dipendenti e che riguardi complessivamente tutti gli strumenti impiegati nell'azienda potrebbe risultare non coerente con la finalità perseguita dal legislatore di consentire la puntuale conoscenza da parte del lavoratore dei controlli ai quali è assoggettato.

Quanto appena detto consente di passare al secondo punto, cioè le modalità con le quali l'informativa deve essere portata a conoscenza dei lavoratori con la consapevolezza della mancanza di un'indicazione espressa da parte del legislatore.

Per risolvere il quesito, e quindi comprendere le modalità della sua comunicazione (pubblicità), occorre partire dal contenuto dell'informazione. Se quest'ultimo non è generalizzabile per tutto il personale dipendente, in quanto gli strumenti impiegati dai lavoratori sono differenziati, i destinatari di essa saranno soltanto quei dipendenti che si avvalgono di determinati strumenti, ma non gli altri che impiegano strumenti diversi; l'estensione a questi ultimi dell'informativa dovuta ai primi potrebbe, addirittura, generare confusione.

Alla questione ora esaminata si aggiunge l'altra che riguarda la prova che il datore di lavoro dovrà fornire, in caso di contestazione in sede giudiziaria, in ordine all'adempimento degli obblighi di informazione di cui è gravato.

In questo caso la ricevuta della comunicazione effettuata nei confronti di ciascun lavoratore costituisce la prova documentale più sicura, anche se la trasmissione è stata effettuata in via telematica (con una *e-mail* o mediante lettura sul sito aziendale debitamente documentata). Ciò, però, non esclude che la prova possa essere fornita anche con riferimento a modalità diverse di comunicazione, ad esempio, mediante affissione in luoghi accessibili ai lavoratori interessati.