



I “diritti digitali” dei dipendenti pubblici nell’ordinamento spagnolo

ALESSANDRA ALBANESE

Università di Firenze
già Professoressa associata
di Diritto Amministrativo
alessandra.albanese@unifi.it

JOSEFA CANTERO MARTÍNEZ

Università di Castilla-La Mancha
Professoressa ordinaria
di Diritto Amministrativo
Josefa.cantero@uclm.es

ABSTRACT

This work analyzes the so-called “digital rights” of public employees in Spain, which are none other than the classic fundamental rights adapted to an increasingly digitized work environment.

The Spanish legal system reacted belatedly and only to expressly protect the right to privacy of public employees with respect to the use of digital devices made available to them by the Administration and the use of video surveillance and geolocation systems.

Other fundamental rights that could be influenced by technological advances are not expressly mentioned, nor are other possible areas that should be subject to protection indicated, such as the use of artificial intelligence systems, biometrics, data analysis, or social networks, etc.

Keywords: Digital rights; Right to privacy; Digital devices; Video cameras; Geolocation

<https://doi.org/10.60923/issn.2421-2695/23504>

I “diritti digitali” dei dipendenti pubblici nell’ordinamento spagnolo¹

SOMMARIO: 1. Introduzione: la privacy del dipendente di fronte a un’amministrazione panottica. – 2. L’uso di sistemi di videosorveglianza, geolocalizzazione e registrazione audio da parte dell’amministrazione. – 3. L’accesso ai computer e agli altri dispositivi elettronici messi a disposizione del dipendente. – 4. Alcune carenze dell’attuale quadro giuridico dei diritti digitali in ambito amministrativo. – 4.1. La complessità della tecnica dei rinvii normativi. – 4.2. L’assenza di un regime abilitante specifico e chiaro per l’Amministrazione. – 4.3. L’apparente universalizzazione del regime giuridico dei diritti digitali: un’assimilazione fittizia tra dipendenti pubblici e lavoratori del settore privato. – 4.4. L’obsolescenza normativa di fronte ai progressi tecnologici. – 5. In conclusione: la sfida di positivizzare i nuovi diritti emergenti sulla base degli orientamenti della Carta dei diritti digitali.

1. Introduzione: la privacy del dipendente di fronte a un’amministrazione panottica

I progressi tecnologici hanno comportato il riconoscimento di importanti poteri di sorveglianza e controllo per l’Amministrazione e una limitazione dei diritti fondamentali dei dipendenti pubblici, in particolare del diritto alla privacy. Ciò avviene quando l’Amministrazione utilizza dispositivi di videosorveglianza o di geolocalizzazione che le consentono di vedere praticamente tutto ciò che fanno i propri dipendenti o quando controlla l’uso che essi fanno dei dispositivi digitali che essa stessa mette a loro disposizione come strumenti di lavoro. Dispositivi tecnologici quali computer, tablet, telefoni fissi e cellulari, nonché gli account di posta elettronica, compresi quelli istituzionali, consentono non solo lo svolgimento delle funzioni lavorative, ma anche la memorizzazione di dati di carattere personale. Possono contenere agende di contatti, file privati, credenziali bancarie, file multimediali, comunicazioni private, ecc. È normale che i dipendenti pubblici possano utilizzare questi dispositivi per scopi privati, soprattutto se non esiste alcun divieto espresso o limitazione al loro utilizzo, il che presuppone una certa tolleranza nei confronti di tale utilizzo e l’esistenza di una ragionevole aspettativa di riservatezza nei confronti di interferenze da parte del datore di lavoro.

I progressi tecnologici ci mostrano nuovi aspetti dell’Amministrazione quando agisce in qualità di datore di lavoro, che devono ancora essere adeguatamente disciplinati dal diritto amministrativo. L’Amministrazione è diventata una sorta di “grande fratello

⁽¹⁾ *Questo lavoro è stato realizzato nell’ambito dell’accordo tra l’ente pubblico Red.es e l’Università di Castilla-La Mancha per promuovere l’attuazione della Carta dei diritti digitali nel campo dei diritti digitali nell’ambiente lavorativo e aziendale C039/23-OT.*

(2)” che vede tutto, un’Amministrazione “panottica (3)”, che può utilizzare le nuove tecnologie per provare facilmente la commissione di infrazioni amministrative e avviare procedimenti disciplinari nei confronti dei propri dipendenti. Allo stesso modo, seguendo la dottrina del diritto del lavoro (4), si potrebbe dire che dispone anche di nuovi poteri “computazionali” o di direzione algoritmica che le consentono di conoscere enormi quantità di dati sui propri dipendenti, di elaborarli, di creare profili o persino di adottare decisioni nella gestione del personale basate sull’utilizzo di sistemi di Intelligenza Artificiale (IA).

L’utilizzo di tutte queste tipologie di tecnologia da parte dell’Amministrazione può avere un impatto significativo sui diritti fondamentali dei dipendenti pubblici (5). Può influire sul loro diritto alla riservatezza delle comunicazioni (art. 18.3 CE), sul diritto alla protezione dei dati (art. 18.4 CE) e, in particolare, sul diritto alla privacy (art. 18.1 CE). Quest’ultimo diritto è gravemente leso quando l’amministrazione datrice di lavoro si avvale di determinati strumenti tecnologici quali la videosorveglianza, la geolocalizzazione, i sistemi di registrazione audio o quando accede direttamente ai computer o ad altri dispositivi digitali messi a disposizione dei propri dipendenti per controllarne l’utilizzo. Come sottolineato dalla sentenza del Tribunal Constitucional 173/2011, del 7 novembre, i dati ottenuti da un computer possono forse essere considerati irrilevanti se presi isolatamente. Tuttavia, se analizzati nel loro insieme, possono fornire un profilo altamente descrittivo della personalità del titolare che incide

(2) L. Rodríguez Fernández, *Robots, algoritmos y trabajos*, El País, 2023, in www.iustel.com//diario_del_derecho/noticia.asp?ref_iustel=1232476&utm_source=D&utm_medium=email&utm_campaign=17/4/2023&utm_popup=

(3) J. Mercader Uguina, *Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?*, *Relaciones laborales: Revista crítica de teoría y práctica*, 2001, 1, 665-686 y *En busca del empleador invisible: algoritmos e inteligencia artificial en el derecho digital del trabajo*, *El Cronista del Estado Social y Democrático de Derecho*, 2022, 100, 136-145.

(4) A. Todolí Signes, *La inteligencia artificial no te robará tu trabajo, sino tu salario. Retos del Derecho del Trabajo frente a la dirección algorítmica*, *El Cronista del Estado Social y Democrático de Derecho*, 2022, 100, 151. Definisce la direzione algoritmica come un insieme diversificato di strumenti tecnologici e tecnici che consentono di strutturare le condizioni di lavoro e gestire la forza lavoro.

(5) Sono dipendenti pubblici coloro che svolgono funzioni retribuite nella Pubblica Amministrazione al servizio dell’interesse generale. Questa categoria di “dipendenti pubblici” comprende i funzionari pubblici e il personale contrattualizzato dell’Amministrazione. Questa categoria è disciplinata negli artt. 8 ss. del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (TREBEP). I funzionari sono legati all’amministrazione in virtù dell’atto amministrativo di nomina, sono soggetti a un rapporto statutario disciplinato dal diritto amministrativo e le loro controversie sono di competenza della giurisdizione contenzioso-amministrativa (Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa). Il personale contrattualizzato dell’Amministrazione è legato a quest’ultima tramite un contratto di lavoro di tipo privatistico. Tuttavia, è caratterizzato dal fatto che alcuni istituti fondamentali, come l’accesso all’Amministrazione, i diritti, il regime disciplinare, ecc., sono regolati anche dalle norme del TREBEP. Per quanto non previsto dal TREBEP, essi sono disciplinati dalla legislazione sul lavoro, dettata dal Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET). Sono soggetti a un ambito giurisdizionale diverso, la giurisdizione sociale, al pari dei lavoratori del settore privato (Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social).

sull'individualità della persona e che, pertanto, deve essere degno di protezione nei confronti di terzi e dei poteri pubblici (STS del 29 settembre 2023, Sezione contenzioso-amministrativo, Sezione seconda, n. 1207/2023).

Il diritto alla privacy personale è un diritto fondamentale sancito dall'articolo 18.1 della Costituzione spagnola (CE) e, di conseguenza, gode del massimo grado di protezione previsto dall'ordinamento spagnolo. È vincolante per tutti i poteri pubblici, può essere regolato solo da una “legge organica ⁽⁶⁾” che deve rispettarne il contenuto essenziale ed è suscettibile di tutela dinanzi al Tribunale costituzionale (articolo 53 CE). In quanto derivato dalla dignità della persona (art. 10.1 CE), implica l'esistenza di un ambito proprio e sottratto all'azione e alla conoscenza degli altri, necessario, secondo i canoni della nostra cultura, per mantenere una qualità minima della vita umana. Al fine di preservare tale spazio riservato, il diritto alla privacy conferisce alla persona il potere giuridico di imporre a terzi il dovere di astenersi da qualsiasi ingerenza nella sfera intima e il divieto di fare uso di quanto conosciuto senza il suo consenso (Sentenza del Tribunal Constitucional 170/2013 del 7 ottobre).

Ebbene, di fronte alle nuove sfide poste dall'uso della tecnologia nell'ambiente di lavoro, che riguardano in modo significativo il complesso dei diritti alla riservatezza e alla tutela dei dati personali, l'ordinamento giuridico spagnolo ha reagito in modo tardivo e modesto, adeguando solo il diritto fondamentale alla privacy. Tale adeguamento è stato realizzato in modo congiunto per tutti i dipendenti, siano essi lavoratori di un'azienda privata, funzionari pubblici o personale dell'Amministrazione. Tuttavia, il grado di protezione finale di questi diritti può variare in modo significativo in funzione dello sviluppo che ne verrà dato in seguito attraverso la contrattazione collettiva, il cui regime giuridico e la cui portata sono molto diversi nel settore della pubblica amministrazione. È stata la legge organica 3/2018, del 5 dicembre, sulla protezione dei dati personali e la garanzia dei diritti digitali, a riconoscere e regolamentare questi nuovi “diritti digitali” nell'ambito dell'amministrazione.

Infatti, la quattordicesima disposizione finale della suddetta Legge Organica ha ampliato l'elenco dei diritti di cui all'articolo 14 del Regio Decreto Legislativo 5/2015, del 30 ottobre, che approva il testo riformato della Legge sullo Statuto Base dei Dipendenti Pubblici (in di seguito, TREBEP). Tale disposizione contiene i diritti individuali di tutti i dipendenti pubblici, siano essi funzionari o impiegati pubblici, e la lettera h) sanciva già il diritto alla privacy personale sin dalla sua formulazione originaria. Il legislatore organico, tuttavia, ha ritenuto che tale menzione non fosse sufficiente a tutelare il dipendente pubblico di fronte ai progressi tecnologici e ha aggiunto una nuova lettera all'articolo 14, la lettera j bis), per riconoscere loro specificamente il diritto alla

⁽⁶⁾ Le leggi organiche sono leggi previste dall'articolo 81 della Costituzione spagnola che si caratterizzano perché la loro approvazione richiede la maggioranza assoluta del Congresso dei deputati in una votazione finale sull'insieme del progetto. Questa categoria speciale è riservata alla regolamentazione dei diritti fondamentali e delle libertà pubbliche, all'approvazione degli Statuti di autonomia delle Comunità autonome, al regime elettorale generale e agli altri casi previsti dalla Costituzione.

privacy “nell’uso dei dispositivi digitali messi a loro disposizione e in relazione all’uso di dispositivi di videosorveglianza e geolocalizzazione”, rinviando direttamente alla disciplina dettata dalla legislazione vigente in materia di protezione dei dati personali e garanzia dei diritti digitali ⁽⁷⁾. Questo rinvio si riferisce agli articoli 89 e seguenti della Legge Organica 3/2018, che attribuiscono espressamente all’Amministrazione i nuovi poteri di sorveglianza e supervisione tecnologica dei propri dipendenti pubblici. Le nuove norme hanno dato contenuto sostanziale a questa nuova versione digitale del diritto alla privacy, stabilendone i requisiti, le garanzie e definendo i tratti essenziali del suo regime giuridico. In realtà, si tratta sostanzialmente di un adeguamento del diritto fondamentale alla privacy e del diritto alla protezione dei dati personali (anche se quest’ultimo non è espressamente menzionato) al nuovo ambiente di lavoro digitalizzato. Tuttavia, con il progresso delle tecnologie dell’informazione e della comunicazione, questo regime sta diventando rapidamente obsoleto.

Sebbene la norma riconosca anche il diritto alla disconnessione digitale, in questo lavoro mi concentrerò solo sulla tutela del diritto alla vita privata del dipendente pubblico e agli orientamenti della giurisdizione contenzioso-amministrativa, che fa rinvio direttamente alla giurisprudenza elaborata dalla giurisdizione sociale sulla validità dei diritti fondamentali nell’ambito lavorativo.

2. L’uso di sistemi di videosorveglianza, geolocalizzazione e registrazione audio da parte dell’Amministrazione

Lo Statuto fondamentale dei dipendenti pubblici non contiene norme specifiche a fronte di questo importante potere amministrativo. È riconosciuto solo il diritto dei dipendenti pubblici al rispetto della privacy in relazione all’uso di strumenti di videosorveglianza e geolocalizzazione. Non viene espressamente menzionata la protezione contro la registrazione audio. Le condizioni per il loro utilizzo sono contenute negli articoli 89 e 90 della Legge Organica 3/2018, che universalizza il regime giuridico per l’utilizzo di questi strumenti. Tali norme riconoscono al datore di lavoro, sia esso un imprenditore o un’amministrazione pubblica, il potere di controllare e sorvegliare i propri dipendenti attraverso l’uso dei dispositivi di videosorveglianza, di geolocalizzazione o di registrazione audio sul luogo di lavoro. Quanto maggiore è l’invasione della privacy del dipendente, tanto maggiori sono le precauzioni e le garanzie stabilite dal legislatore. Così, ad esempio, la registrazione dei suoni sarebbe ammessa solo quando sussistono rischi rilevanti per la sicurezza degli impianti, dei beni e delle persone e nel rispetto del principio di proporzionalità e di intervento minimo.

⁽⁷⁾ Con lo stesso contenuto, la sua tredicesima disposizione finale aggiungeva un nuovo articolo 20 bis al testo coordinato del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET), in cui riconosceva i diritti dei lavoratori alla privacy in relazione all’ambiente digitale e alla disconnessione.

La formulazione di queste disposizioni, a mio avviso, presenta importanti difetti di tecnica giuridica. Sebbene la lettera j.bis) dell'art. 14 del TREBEP si riferisca solo al diritto alla privacy (art. 18.1 CE), con l'utilizzo di queste tecnologie è direttamente interessato anche il diritto alla protezione dei dati di cui all'art. 18.4 CE che, come stabilito dalla sentenza della Corte Costituzionale 292/2000, del 30 novembre, garantisce alle persone il potere di controllo sui propri dati personali, sul loro utilizzo e destinazione, al fine di impedirne il traffico illecito e lesivo della dignità e dei diritti dell'interessato. D'altra parte, per il trattamento delle immagini ottenute tramite sistemi di telecamere o videocamere o per la geolocalizzazione del dipendente, le norme rimandano esplicitamente a quanto previsto dall'articolo 20.3 dello Statuto dei lavoratori (ET) e dalla normativa in materia di pubblico impiego, purché tali funzioni siano esercitate nell'ambito del loro quadro giuridico e nei limiti ad esso inerenti. In ambito lavorativo privato, l'articolo 20.3 del ET riconosce i poteri di direzione e controllo aziendale e autorizza il datore di lavoro ad adottare le misure che ritiene più opportune per la sorveglianza e il controllo dei propri lavoratori al fine di verificare l'adempimento dei loro obblighi e doveri lavorativi. Tuttavia, in ambito pubblico non esiste una norma simile che riconosca espressamente tali poteri all'Amministrazione. Manca il quadro giuridico che abiliti tale potere, che consenta di inquadrarlo correttamente e limitarlo solo ai casi in cui sussista una causa che giustifichi tale ingerenza nei diritti fondamentali del dipendente, garantendo un uso legale, lecito, proporzionato e trasparente di questo tipo di controlli.

In questi casi, l'Amministrazione dovrà informare preventivamente, in modo espresso, chiaro e conciso, i propri dipendenti e i loro rappresentanti in merito a tale misura. Tuttavia, se la telecamera riprende in flagranza la commissione di un atto illecito, si riterrà adempiuto l'obbligo di informazione quando sia presente almeno il dispositivo di cui all'articolo 22.4 della legge organica stessa, vale a dire sia stato apposto un adesivo o un dispositivo informativo in un luogo sufficientemente visibile che identifichi almeno l'esistenza del trattamento, l'identità del responsabile e la possibilità di esercitare i diritti previsti dagli articoli da 15 a 22 del RGPD. In altre parole, la norma prevede una regola generale di informazione specifica per i dipendenti pubblici e un'eccezione in caso in cui il dipendente sia stato ripreso in flagranza dell'illecito, nel qual caso è sufficiente l'informazione generica prevista per tutte le persone in generale con i suddetti adesivi informativi. La giurisprudenza, tuttavia, ha trasformato l'eccezione in regola generale, poiché considera sufficiente l'esistenza dell'adesivo per ritenere adempiuto l'obbligo di informazione.

Le garanzie sono rafforzate nel caso in cui si utilizzi la tecnologia di geolocalizzazione, poiché l'invasione della sfera giuridica del dipendente è ancora maggiore. In questo caso, i dipendenti pubblici e, se del caso, i loro rappresentanti devono essere informati in anticipo, in modo esplicito, chiaro e inequivocabile, dell'esistenza e delle caratteristiche di tali dispositivi, informandoli anche del possibile

esercizio dei diritti di accesso, rettifica, limitazione del trattamento e cancellazione. Il requisito dell’informazione, in questa ipotesi, non ammette alcuna eccezione.

La giurisprudenza del Tribunal Constitucional ha mantenuto nelle sue ultime sentenze una posizione eccessivamente flessibile in merito agli obblighi di informazione del datore di lavoro, che ha comportato una chiara svalutazione del diritto all’informazione del lavoratore ⁽⁸⁾.

Infatti, nella sentenza STC 29/2013, dell’11 febbraio, relativa alle registrazioni all’Università di Sevilla, il Tribunal Constitucional ha ritenuto necessario che i lavoratori vengano informati espressamente della finalità di controllo sul rispetto delle condizioni di lavoro e dell’esistenza di telecamere installate dal datore di lavoro, anche ai fini dell’irrogazione di eventuali sanzioni disciplinari. Tuttavia, successivamente il giudice costituzionale ha cambiato criterio con la sentenza STC 39/2016, del 3 marzo, allentando sensibilmente i criteri e ritenendo che fosse sufficiente il dovere di informazione generica sulla presenza delle telecamere installate per la sicurezza dei locali, ritenendo che il consenso sia implicito nell’accettazione del contratto di lavoro, che implica il riconoscimento del potere direttivo del datore di lavoro e che tale potere del datore di lavoro sia direttamente correlato al diritto alla proprietà privata (art. 33 CE) e al diritto alla libertà di impresa (art. 38 CE). Nel caso di specie, l’azienda aveva apposto l’apposito cartello informativo nella vetrina del negozio in cui prestava servizio la lavoratrice licenziata, per cui il Tribunale ha ritenuto che si potesse presumere che quest’ultima fosse a conoscenza dell’esistenza delle telecamere e dello scopo per cui erano state installate.

Questa giurisprudenza è stata recentemente confermata dalla sentenza del Tribunal Constitucional 119/2022, del 29 settembre, che avalla anche la legittimità di un licenziamento a fronte di un fatto qualificato come irregolare dalla direzione dell’azienda. Sono state esaminate le telecamere di sicurezza installate nei luoghi di contatto con il pubblico e si è verificato che uno dei lavoratori aveva tenuto un comportamento illecito, vendendo un prodotto senza registrarlo in cassa. I lavoratori non avevano ricevuto informazioni preventive ed espresse sull’installazione delle telecamere e sul loro eventuale utilizzo a fini disciplinari. Tuttavia, l’installazione del sistema di videosorveglianza era segnalata in un luogo visibile dell’azienda, mediante un cartello conforme alla normativa vigente in materia di protezione dei dati da oltre cinque anni, e un altro lavoratore era già stato licenziato anni prima per un motivo simile.

In altre parole, questa giurisprudenza applica una presunzione diretta di conoscenza di tali informazioni da parte del lavoratore, il che non è previsto dalla legislazione organica, che richiede invece determinate condizioni affinché l’informazione sia considerata valida: informazione preventiva, espressa, chiara e concisa. Incomprendibilmente, la giurisprudenza costituzionale si discosta dall’obbligo

⁽⁸⁾ M.A. Cabellos Espiérrez, *El derecho a la protección de datos personales ante la videovigilancia en el ámbito laboral: la progresiva devaluación en la jurisprudencia constitucional de la obligación de informar al trabajador*, *Revista Vasca de Administración Pública*, 2024, 128-I, in <https://doi.org/10.47623/ivap-rvap.128.2024.1.01>

di informare specificamente il lavoratore in merito alla finalità del trattamento e riduce notevolmente gli standard di tutela dei diritti dei lavoratori.

In ambito amministrativo, la stessa questione è stata trattata nella sentenza del Tribunal Supremo del 26 aprile 2021, Terza Sezione, Contenzioso-amministrativo, Sezione 4, Sentenza 557/2021, in merito al caso di una funzionaria dell'Agenzia statale dell'amministrazione tributaria (AEAT) che era stata sanzionata con 8 mesi di sospensione dal servizio e dallo stipendio per aver eluso i controlli orari, come era stato dimostrato da una registrazione.

Le immagini registrate dalla videocamera dimostrano l'attività svolta dalla ricorrente per eludere il sistema di controllo orario, essendo stata ripresa mentre cercava di evitare di essere individuata, mentre ometteva le proprie registrazioni o sostituiva o falsificava le registrazioni di un altro funzionario ⁽⁹⁾. La sentenza pone la questione se, nell'ambito della Pubblica Amministrazione, l'uso di sistemi di videosorveglianza, installati in modo permanente e con finalità generali di sorveglianza e sicurezza, richieda di informare preventivamente, in modo espresso e inequivocabile, i dipendenti pubblici in merito alla finalità di controllo dell'attività lavorativa di tale sistema e, di conseguenza, in merito al suo possibile utilizzo per l'irrogazione di sanzioni disciplinari. La sentenza è importante perché applica direttamente al settore della funzione pubblica la giurisprudenza elaborata dal Tribunal Constitucional in relazione all'ambito aziendale, compiendo uno sforzo significativo per trasferire la terminologia e l'argomentazione giuridica utilizzata in ambito lavorativo privato al settore della funzione pubblica.

Infatti, essendo l'immagine un dato personale che identifica o rende identificabile una persona, il suo trattamento necessita di una base giuridica, ma tale base non si trova nel consenso del funzionario, bensì «nel contratto di lavoro e nei poteri legali di controllo concessi al datore di lavoro». Ne consegue, quindi, che per utilizzare questi sistemi di videosorveglianza non è necessario il consenso del funzionario, dato che la base giuridica deriva dalla sua nomina ⁽¹⁰⁾. Poiché il principio di minimizzazione di cui all'articolo 5 del RGPD richiede che i dati personali trattati siano adeguati, pertinenti e

⁽⁹⁾ La sentenza prosegue sulla scia della giurisprudenza della STEDH del 17 ottobre 2019 (numeri 1874/13 e 8567/13) (causa López Ribalda II), in cui è stato affrontato l'uso di telecamere di sorveglianza nascoste sul luogo di lavoro e la loro relazione con i diritti alla privacy dei dipendenti. In questo caso, diverse lavoratrici di un supermercato sono state licenziate dopo essere state riprese a loro insaputa da telecamere di videosorveglianza nascoste nel locale, installate dal proprietario perché sospettava che alcune dipendenti stessero rubando prodotti, senza che queste fossero a conoscenza della sorveglianza. La sentenza è rilevante perché stabilisce che il diritto alla privacy dei lavoratori non è assoluto e può essere limitato in determinati contesti, in particolare quando sussiste un legittimo interesse dell'azienda, come la protezione della proprietà. Tuttavia, il giudice sottolinea anche la necessità di un equilibrio tra la sicurezza del datore di lavoro e i diritti fondamentali del lavoratore.

⁽¹⁰⁾ Il valore del consenso di un dipendente pubblico come base giuridica quando l'amministrazione intende trattare i suoi dati è piuttosto limitato, dato lo squilibrio di potere che spesso si crea nei rapporti tra le due parti, che impedisce che il consenso possa essere considerato libero. Così le Linee guida 05/2022 del Comitato europeo per la protezione dei dati (CEPD) sull'uso del riconoscimento facciale nel settore delle forze di polizia, versione 2.0, elaborate il 26 aprile 2023, in www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_es.pdf

limitati in relazione alle finalità per cui sono trattati, è stato sollevato il dubbio se tale trattamento, previsto per motivi di sorveglianza della sicurezza del luogo di lavoro, possa essere utilizzato per una finalità diversa, ovvero per l'esercizio del potere disciplinare dell'Amministrazione. Il Tribunal Constitucional ha ritenuto che la regola generale del consenso al trattamento dei dati personali, quali le registrazioni, trovi un'eccezione nella necessità di salvaguardare lo svolgimento del rapporto di servizio, che deriva dallo speciale regime giuridico proprio dei funzionari pubblici, vale a dire da un rapporto di tipo pubblicistico che richiede di garantire l'adempimento di specifici obblighi, pur tenendo sempre conto della proporzionalità.

La sentenza compie un importante sforzo argomentativo per trasferire in blocco all'ambito dell'Amministrazione la giurisprudenza elaborata nell'ambito del diritto del lavoro in materia di poteri di vigilanza e supervisione del datore di lavoro, nonostante che nel settore pubblico non esista una disposizione esplicita come quella dell'articolo 20.3 dell'ET, che attribuisca all'Amministrazione i poteri di sorveglianza e supervisione digitale e nonostante che, ovviamente, non siano applicabili i diritti di libertà d'impresa (articolo 38 CE) e di proprietà privata (articolo 33 CE) utilizzati dalla giurisprudenza della giurisdizione sociale in questo ambito. Pertanto, il Tribunal Supremo ha affermato che, «va considerato che ci si trova in presenza di un rapporto di particolare soggezione del funzionario pubblico all'Amministrazione, e che tale acquisizione di immagini non è stata effettuata mediante l'installazione di nuove telecamere appositamente installate per la funzionaria ricorrente, ma che la commissione dell'infrazione è stata accertata, tra l'altro, con le telecamere esistenti, già note alla ricorrente, come dimostra l'esecuzione di manovre volte ad eludere il controllo delle condizioni di lavoro, quali l'orario di lavoro giornaliero. Tutto ciò con una forte presenza dell'interesse generale a fronte di questo tipo di comportamenti, per cui la loro generalizzazione, oltre a ledere l'immagine dell'Amministrazione come organizzazione al servizio della comunità, comprometterebbe il corretto funzionamento dell'istituzione. Pertanto, la raccolta delle informazioni ordinarie, mediante telecamere installate in termini generali nell'edificio, volte a verificare la sicurezza e la sorveglianza, ma anche il rispetto delle condizioni di lavoro, non richiede una comunicazione preventiva, concreta e specifica, del loro successivo utilizzo nei confronti dei funzionari pubblici coinvolti, vale a dire una comunicazione sulla finalità specifica del loro utilizzo, in caso di eventuali procedimenti disciplinari».

La stessa argomentazione è stata utilizzata dal Tribunal Superior de Justicia de la Comunità Valenciana del 17 febbraio 2023, Sezione Contenzioso-Amministrativo, Sezione 2ª, che ha sanzionato un funzionario con 2 giorni di sospensione dal lavoro e dallo stipendio per essersi assentato dal posto di lavoro per più di due ore, superando la mezz'ora di pausa. Egli chiedeva l'annullamento della sanzione sulla base del fatto che le prove ottenute tramite videocamera - registrazioni - non potevano essere considerate valide in quanto i funzionari del Corpo Nazionale di Polizia (CNP) non erano stati informati che potevano essere utilizzate come prove nei procedimenti disciplinari, in

violazione dell'articolo 89 della Legge Organica 3/2018, del 5 dicembre. Secondo la Corte, non era necessario un avviso specifico e preventivo ai funzionari del CNP per l'utilizzo delle immagini a fini disciplinari su fatti accaduti nella stazione di polizia, quando i funzionari stessi ne erano già a conoscenza.

3. L'accesso ai computer e agli altri dispositivi elettronici messi a disposizione del dipendente

L'attribuzione esplicita all'Amministrazione del potere di accedere ai computer e agli altri dispositivi elettronici messi a disposizione dei dipendenti si trova nell'articolo 87 della Legge Organica 3/2018. Esso consente alla Amministrazione di accedere ai contenuti derivanti dall'uso dei mezzi digitali messi a disposizione dei propri dipendenti al solo scopo di controllare l'adempimento degli obblighi lavorativi o statutari e di garantire l'integrità di tali dispositivi. Tale autorizzazione consentirebbe all'Amministrazione di accedere al contenuto di computer, tablet, telefoni cellulari, e-mail o altri dispositivi digitali che essa stessa ha messo a disposizione dei propri dipendenti. Sebbene l'articolo 14.j.bis) menzioni solo il diritto alla privacy, è evidente che con tale accesso può essere lesa anche il diritto fondamentale alla segretezza delle comunicazioni ⁽¹¹⁾.

Anche in questi casi sono previste determinate garanzie. Devono essere stabiliti preventivamente i criteri di utilizzo dei dispositivi digitali, rispettando in ogni caso gli standard minimi di protezione della privacy in conformità con gli usi sociali e i diritti riconosciuti dalla Costituzione e dalla legge. La norma prevede limitazioni a tale potere di sorveglianza per proteggere la privacy del dipendente e dispone in modo imperativo che l'elaborazione dei criteri di utilizzo di tali mezzi avvenga con la partecipazione dei rappresentanti dei lavoratori, che è indispensabile (STS del 6 febbraio 2024, Sezione del Lavoro, Sezione 1^a). Se l'uso per fini privati è ammesso, per l'accesso al dispositivo digitale è necessario che siano specificati con precisione gli usi autorizzati e che siano stabilite garanzie per preservare la privacy dei dipendenti. Come garanzia essenziale, è necessario determinare i periodi in cui i dispositivi possono essere utilizzati per tali fini privati e informare i dipendenti di tali criteri di utilizzo.

Su alcune di queste questioni si è già pronunciata la giurisprudenza. Nella sentenza dell'Audiencia Nacional (Tribunale Nazionale) del 6 febbraio 2024, Sezione 7^a, il caso riguardava l'accesso al computer di un funzionario dell'AEAT (Agenzia statale dell'amministrazione tributaria), che era stato utilizzato a fini disciplinari e aveva comportato la sua sospensione dal servizio e dallo stipendio per dieci mesi. Il

⁽¹¹⁾ A questo proposito si può consultare la sentenza della Corte europea dei diritti dell'uomo del 3 aprile 2007 (caso Copland contro Regno Unito), che ha ritenuto in via preliminare che “le e-mail inviate dal luogo di lavoro” rientrano nell'ambito di protezione dell'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, in quanto possono contenere dati sensibili che incidono sulla vita privata e sul rispetto della vita privata (paragrafi 41 e 44).

funzionario aveva commesso numerose infrazioni amministrative che l'Amministrazione aveva potuto verificare dopo aver analizzato il suo computer. La Sezione del Tribunale nella sentenza richiamata ricorda che non esiste un diritto assoluto alla privacy rispetto ai dati contenuti nei computer messi a disposizione del funzionario dall'Amministrazione, ma che tale diritto è strumentale allo svolgimento delle attività proprie della funzione svolta. Pertanto, se sussiste il sospetto di un uso improprio delle apparecchiature informatiche, mediante il compimento di azioni che potrebbero costituire un'infrazione amministrativa, come nel caso in esame, è opportuno che l'amministrazione acceda a tali apparecchiature per acquisire le prove necessarie ad accertare le azioni illecite del funzionario. In questo caso esisteva un'istruzione interna dell'Amministrazione che dava indicazioni sull'uso del computer, avvertiva della possibilità di essere ispezionati e precisava che i risultati avrebbero potuto essere inseriti in un fascicolo disciplinare o utilizzati in un procedimento giudiziario.

Di particolare interesse è la sentenza del Tribunal Supremo del 7 ottobre 2024, Sezione contenzioso-amministrativo, Sezione 3^a, (ric. 6949/2022), che ha affrontato la questione se l'accesso ai contenuti del computer di un funzionario violi il diritto alla protezione dei dati sancito dall'articolo 18.4 della Costituzione spagnola. In questo caso, è stata dichiarata illegittima la prova fornita dal Comune di Algemesí per sanzionare la propria dipendente, tesoriera del Comune. Sono stati rinvenuti alcuni documenti nella stampante e nella memoria del suo scanner che potevano far supporre che la dipendente svolgesse attività professionali per un'azienda privata durante l'orario di lavoro, attività che non avevano nulla a che vedere con le sue funzioni di tesoriera né erano compatibili con esse. Il sindaco ha ordinato al dipartimento informatico di indagare sui documenti del computer personale di lavoro per chiarire i fatti. L'informatico, senza bisogno di accedere fisicamente al computer con la password di amministratore, ha ispezionato il computer e copiato diverse cartelle di documenti personali relativi ad attività private che sono state registrate su un DVD, dai quali risultava che la dipendente stava effettivamente lavorando per una società privata, ma erano state anche copiate informazioni personali particolarmente sensibili e dati sanitari.

L'azione del Comune è stata compiuta senza rispettare i diritti dei propri dipendenti e la loro ragionevole aspettativa di privacy. In questo caso, il Comune non aveva informato preventivamente i dipendenti dell'utilizzo delle apparecchiature informatiche, avvertendoli dell'esistenza di misure di controllo o di sorveglianza del computer sulle comunicazioni dei dipendenti. Inoltre, non era stato nemmeno rispettato il principio di proporzionalità nell'accesso, poiché il Comune ha avuto accesso a tutte le cartelle e i file senza discriminare il loro contenuto, in modo particolarmente invasivo, ispezionando dati sanitari e altri dati sensibili e documenti privati della ricorrente. Il Tribunale ha affermato che il rapporto di lavoro pubblico è un rapporto “statutario”, di diritto pubblico, che colloca il funzionario in una posizione di particolare assoggettamento, delimitata e disciplinata da una normativa specifica, ma che ciò non esclude né impedisce che siano impartite istruzioni ai dipendenti pubblici che precisino

in cosa consiste l'uso corretto dei mezzi informatici, nonché la portata del controllo che può essere esercitato su di essi.

La sentenza è importante perché dichiara espressamente che la giurisprudenza elaborata dalla sentenza della Corte europea dei diritti dell'uomo (CEDU) del 5 settembre 2017, nella causa *Barbulescu* 2, è applicabile anche al settore del pubblico impiego. Inoltre, analizza l'articolo 14, j) bis del TREBEP, trasferendo direttamente la giurisprudenza elaborata in materia di lavoro al settore della pubblica amministrazione. Si fa esplicito riferimento all'interpretazione data dal Tribunal Supremo, Sezione Sociale, dell'8 febbraio 2018 (Rec. 1121/2015) e alla sua analisi sulla “aspettativa di privacy” per il trattamento dei dati personali quando si accede al computer di un dipendente pubblico. Partendo da ciò, la Corte respinge la tesi avanzata dal Comune ricorrente sull'inesistenza di un'aspettativa di privacy del funzionario, in virtù dell'esistenza di un rapporto speciale di assoggettamento tra il funzionario e l'Amministrazione e della natura speciale del computer e della stampante come beni di dominio pubblico.

La Corte chiarisce inoltre che il rapporto di subordinazione speciale tra il funzionario e l'Amministrazione implica una situazione di dipendenza maggiore rispetto a quella che si verifica nei rapporti di subordinazione generale, ma non arriva all'esclusione di un diritto fondamentale che non trova specifico fondamento giuridico nella natura giuridica pubblica del Comune ricorrente, poiché i principi generali del diritto alla protezione dei dati sono applicabili sia agli enti pubblici che a quelli privati, anche se in alcuni casi la normativa pubblicistica può influire sul trattamento effettuato. Le particolarità dell'Amministrazione pubblica, che esistono, riguardano fondamentalmente la non sottoponibilità del Comune alle sanzioni previste per le violazioni della normativa sulla protezione dei dati, ma il fatto che il soggetto trasgressore sia un'amministrazione pubblica non comporta la scomparsa del diritto fondamentale di cui all'articolo 18 della Costituzione spagnola o all'articolo 8 della Carta europea dei diritti umani.

4. Alcune carenze dell'attuale quadro giuridico dei diritti digitali in ambito amministrativo

Il quadro normativo applicabile ai diritti digitali del personale al servizio delle amministrazioni pubbliche è caratterizzato da complessità e frammentazione, poiché è disperso in diverse disposizioni legislative. Da un punto di vista tecnico, tale regime presenta notevoli carenze, sia nella sua concezione che nella sua capacità di rispondere alle nuove sfide poste dalla trasformazione digitale del settore pubblico.

La normativa attuale offre una protezione esplicita solo in relazione al diritto alla privacy e all'utilizzo da parte dell'Amministrazione di tre sistemi specifici: la videosorveglianza, la geolocalizzazione e l'uso di dispositivi digitali. Esclude altri diritti fondamentali ugualmente esposti all'uso dei suddetti fenomeni tecnologici, come il diritto alla protezione dei dati personali o il segreto delle comunicazioni, e non menziona

altre tecnologie che possono avere un impatto su tali diritti, come la biometria, l'analisi dei dati e dei social network, la profilazione, ecc. Particolare preoccupazione suscita il crescente utilizzo di sistemi di intelligenza artificiale nei processi di gestione e di decisione in materia di personale, poiché il quadro normativo vigente appare chiaramente insufficiente.

Queste carenze tecniche e limitazioni evidenziano la necessità di una revisione integrale del regime giuridico, che consenta un aggiornamento e una sistematizzazione dei diritti digitali adeguati alle nuove realtà tecnologiche.

4.1. La complessità della tecnica dei rinvii normativi

Il quadro dei diritti riconosciuti dal TREBEP manca di completezza e chiarezza, il che determina automaticamente una situazione di incertezza giuridica. Si basa su un modello di rinvio tra norme che pone l'operatore giuridico di fronte a un complesso puzzle normativo che deve essere ricomposto. Il punto di partenza è senza dubbio la lettera j) bis dell'articolo 14 del TREBEP, che riconosce il diritto alla privacy rispetto all'uso di determinate tecnologie, ma questo è solo il primo pezzo del puzzle.

Il secondo tassello indispensabile del puzzle è la legislazione organica sulla protezione dei dati, il cui titolo X è dedicato alla “garanzia dei diritti digitali”. Questa norma, come abbiamo sottolineato, disciplina negli articoli da 87 a 91 i diritti digitali in ambito lavorativo, con totale indipendenza dalla natura pubblica o privata del datore di lavoro. Essa impone requisiti e limiti all'Amministrazione al fine di preservare il diritto alla privacy dei propri dipendenti, garantendo loro, in ogni caso, un diritto strumentale all'informazione sui criteri di utilizzo di questi strumenti digitali. A sua volta, questo quadro deve essere integrato dalla contrattazione collettiva, che può rafforzare il quadro di protezione di questi diritti, anche se il suo ruolo è molto diverso nel settore pubblico e in quello privato, come vedremo di seguito.

Per maggiore completezza, sono state emanate alcune norme settoriali dalle quali potrebbe derivare una certa configurazione del presunto diritto all'informazione algoritmica. Ad esempio, un altro tassello di questo puzzle potrebbe essere rappresentato dall'articolo 23.1 della legge 15/2022, del 12 luglio, integrale per la parità di trattamento e la non discriminazione, che fa riferimento ad alcuni aspetti essenziali che l'Amministrazione deve tenere in considerazione quando utilizza algoritmi per il processo decisionale. La legge si applica all'intelligenza artificiale e alla gestione massiva dei dati (art. 3.1.o) e rimanda, in generale, alla Strategia Nazionale per l'Intelligenza Artificiale, e alla Carta dei Diritti Digitali e alle iniziative europee in materia. Sottolinea la necessità che le amministrazioni pubbliche favoriscano l'attuazione di meccanismi affinché gli algoritmi coinvolti nel processo decisionale utilizzato nelle amministrazioni pubbliche tengano conto dei criteri di minimizzazione dei pregiudizi, trasparenza e responsabilità, ove tecnicamente fattibile. Tali meccanismi devono includere la loro

progettazione e i dati di addestramento e tenere conto delle conseguenze del loro potenziale impatto discriminatorio. A tal fine, devono promuovere la realizzazione di valutazioni d’impatto che determinino l’eventuale discriminazione. Inoltre, nel secondo paragrafo si sottolinea che «le amministrazioni pubbliche, nell’ambito delle loro competenze in materia di algoritmi coinvolti nei processi decisionali, daranno priorità alla trasparenza nella progettazione e nell’attuazione e alla capacità di interpretazione delle decisioni adottate dagli stessi». Tuttavia, pur rappresentando un notevole passo avanti, la normativa descritta presenta ancora alcune lacune. Non si pronuncia in modo sufficientemente imperativo né sancisce esplicitamente i diritti a favore dei cittadini, ma ha un carattere marcatamente programmatico e astratto quando si tratta di stabilire obblighi giuridicamente vincolanti ⁽¹²⁾.

Allo stesso tempo, sarebbe necessario tenere conto di altre normative elaborate dalle Comunità Autonome dalle quali potrebbero derivare alcuni diritti anche per i dipendenti pubblici, qualora tali sistemi fossero utilizzati nella gestione del personale. In questi casi, il grado di protezione dipenderà dalla Comunità Autonoma in cui il dipendente presta servizio. Per citare solo uno degli esempi più recenti, possiamo richiamare l’articolo 48 della Legge 4/2025, dell’11 luglio, sulla semplificazione, snellimento e digitalizzazione amministrativa in Castilla-La Mancha, che riconosce il diritto a una “esposizione delle motivazioni della decisione adottata in un linguaggio comprensibile, con l’indicazione dei dati utilizzati, dei criteri di automazione utilizzati e della logica di funzionamento del sistema” o il diritto di ricevere informazioni sui “dati utilizzati nella procedura, nonché sui criteri di utilizzo del sistema di Intelligenza Artificiale”. Inoltre, nel definire i requisiti per l’uso dell’IA, precisa che i servizi e le azioni che fanno uso di sistemi di IA non possono costituire di per sé decisioni o atti amministrativi senza la convalida umana, salvo che si tratti di atti che non richiedono una valutazione soggettiva delle informazioni o delle circostanze concorrenti o un’interpretazione di carattere giuridico. Nella misura in cui si tratta di un obbligo per l’Amministrazione, se ne può dedurre il diritto all’intervento umano nel processo decisionale attraverso l’IA (art. 45).

Infine, nell’ambito della regolamentazione dell’IA nei procedimenti amministrativi, si ravvisa anche la necessità di riconoscere nuovi diritti digitali, affinché i diritti fondamentali delle persone interessate non subiscano alcuna lesione a causa dell’utilizzo di tali tecnologie.

Tutto ciò ci pone di fronte a un quadro giuridico molto complesso e frammentato che, inoltre, deve essere analizzato alla luce dell’interpretazione data dalla prolifica giurisprudenza sociale del Tribunal Supremo, che è stata recepita in blocco dalla giurisprudizione contenzioso-amministrativa e dalla giurisprudenza del Tribunale

⁽¹²⁾ A. Lertxundi, *El impacto de la digitalización en los derechos fundamentales del personal empleado público en España*, *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 2020, 18, 38 ss. in www.ivap.euskadi.eus/contenidos/informacion/18_revgp/eu_def/Lertxundi_38_53.pdf

Costituzionale e dalla Corte Europea dei Diritti dell’Uomo sui diritti fondamentali nel campo dei rapporti di lavoro.

4.2. L’assenza di un regime specifico e chiaro che abiliti l’Amministrazione

Nel settore della funzione pubblica si riscontrano alcuni problemi giuridici per la configurazione teorica del modello di amministrazione digitale e per l’applicazione all’Amministrazione della giurisprudenza costituzionale elaborata sulla limitazione dei diritti fondamentali nell’ambito lavorativo privato. Sebbene i diritti digitali di cui si è trattato in precedenza siano emersi come reazione alle nuove facoltà di sorveglianza e controllo digitale dell’Amministrazione, tuttavia nel pubblico impiego non esiste una norma simile all’articolo 20.3 del Testo Unico del Lavoro, che attribuisca in modo esplicito tali poteri di direzione all’Amministrazione. Esiste solo un codice di condotta dei dipendenti pubblici, contenuto nell’articolo 54 del TREBEP, applicato attraverso l’esercizio del potere disciplinare, che consente all’Amministrazione di sanzionare i propri dipendenti quando commettono un’infrazione amministrativa (articoli 93 e seguenti).

Inoltre, non è possibile invocare gli articoli 33 e 38 della Costituzione spagnola per giustificare i poteri di vigilanza dell’Amministrazione rispetto all’operato dei propri funzionari. Infatti, per giustificare la limitazione dei diritti fondamentali nell’ambito lavorativo privato, la giurisprudenza del Tribunal Constitucional ha collegato il potere direttivo del datore di lavoro previsto da una norma di legge ai diritti costituzionali alla proprietà privata e alla libertà di impresa (STC 39/2016, del 3 marzo e STC 119/2022, del 29 settembre). Questo collegamento ha permesso di costruire un contrasto fittizio fra diritti, attribuendo all’art. 20.3 dell’ET un collegamento con i due precetti costituzionali citati, per dedurre, successivamente, un conflitto tra diritti fondamentali e altri diritti e beni costituzionali anch’essi meritevoli di tutela, conflitto che, di conseguenza, deve essere risolto con la tecnica della ponderazione tra diritti e con l’applicazione del principio di proporzionalità. Come evidenziato da alcune opinioni critiche formulate contro questa giurisprudenza, la concezione espressa dal Tribunal Constitucional finisce per trasformare i poteri di vigilanza e controllo aziendale sanciti dall’articolo 20.3 dell’ET in una fonte costituzionale, quando in realtà l’articolo in questione non è altro che una semplice norma legislativa che disciplina il rapporto contrattuale.

In ogni caso, l’argomentazione del Tribunal Constitucional è inapplicabile al settore pubblico, poiché non è possibile invocare la proprietà privata e la libertà di impresa per giustificare la limitazione dei diritti fondamentali dei dipendenti pubblici. La mancanza di un’esplicita attribuzione di poteri di vigilanza e controllo digitale non impedisce di riconoscere che anche l’Amministrazione ha interesse a garantire il buon funzionamento dell’azione amministrativa, poiché ciò è necessario affinché essa

adempia con obiettività ed efficacia alla sua funzione di servire l'interesse pubblico (art. 103 CE) e che, di conseguenza, tale compito può essere assolto solo prevedendo meccanismi per verificare che i propri dipendenti adempiano ai propri obblighi professionali con la necessaria diligenza. Come sottolineato dalla citata sentenza del Tribunal Supremo del 26 aprile 2021, esiste un forte interesse pubblico nei confronti di questo tipo di comportamenti per evitare che venga compromessa l'immagine dell'Amministrazione come organizzazione al servizio della comunità e che venga leso il principio di efficacia, che richiede il corretto funzionamento dell'istituzione.

4.3. L'apparente universalizzazione del regime giuridico dei diritti digitali: un'assimilazione fittizia tra dipendenti pubblici e lavoratori del settore privato

Il legislatore spagnolo ha scelto di prevedere un regime giuridico unitario e universale in materia di diritti digitali, applicabile sia al pubblico impiego che ai rapporti di lavoro nel settore privato, senza tenere conto delle peculiarità proprie dell'esercizio della funzione pubblica e del ruolo della contrattazione collettiva. Tuttavia, in questo disegno il legislatore sembra essersi dimenticato delle peculiarità del regime dei funzionari pubblici, di ciò che in Spagna chiamiamo “funzione pubblica”.

A seguito di questa omissione, e nonostante l'intento unificatore del sistema, la disciplina dettata dal TREBEP per i propri funzionari in regime pubblicistico è più povera di quella applicabile ai lavoratori delle imprese private e persino di quella applicabile al proprio personale assunto in regime privatistico. Tale disparità non sembra essere molto ragionevole.

In ambito lavorativo privato sono stati riconosciuti nuovi diritti che non esistono nel settore pubblico. È il caso del diritto all'informazione algoritmica previsto dalla legge 12/2021, del 28 settembre, che modifica il testo coordinato della legge sullo statuto dei lavoratori, approvata con regio decreto legislativo 2/2015, del 23 ottobre, per garantire i diritti dei lavoratori addetti alla distribuzione nell'ambito delle piattaforme digitali, che ha modificato l'articolo 64 dello Statuto dei lavoratori e ha aggiunto il diritto del comitato aziendale di essere informato dal datore di lavoro sui parametri, le regole e le istruzioni su cui si basano gli algoritmi o i sistemi di intelligenza artificiale che influenzano il processo decisionale che può incidere sulle condizioni di lavoro, l'accesso e il mantenimento del posto di lavoro, compresa l'elaborazione di profili professionali. Tuttavia, non esiste una disposizione analoga per gli algoritmi che potrebbero influire sui dipendenti pubblici e tale mancanza costituisce una grave violazione del principio di universalità del regime giuridico dei diritti digitali.

La soluzione a questo problema passa attraverso una modifica della legislazione di base sul pubblico impiego che riconosca espressamente questo nuovo diritto digitale agli organi di rappresentanza dei funzionari pubblici, ovvero ai delegati del personale e ai comitati del personale (art. 39 TREBEP). Ciò potrebbe essere realizzato aggiungendo

una nuova lettera all’elenco delle funzioni affidate a questi organi dall’art. 40.1 del TREBEP per attribuire ai dipendenti pubblici un diritto all’informazione algoritmica simile a quello previsto dall’art. 64 dell’ET.

Allo stesso modo, il ruolo attribuito alla contrattazione collettiva nella definizione e nella tutela dei diritti digitali rivela una notevole omissione in relazione al personale pubblico. Sebbene la regolamentazione dei diritti nell’ambiente di lavoro digitale si presenti con un approccio universalistico e apparentemente uniforme, l’intervento della contrattazione collettiva, determinante nel settore privato, può dare luogo a significative asimmetrie nel suo sviluppo normativo. In questo contesto, si può affermare che il legislatore ha completamente trascurato la specificità del “regime statutario” pubblicistico dei dipendenti pubblici, omettendo qualsiasi disposizione che garantisca la loro adeguata integrazione in questo processo di riconoscimento e garanzia dei diritti digitali.

Il legislatore ha completamente dimenticato i dipendenti pubblici in relazione a quest’ultimo aspetto. L’articolo 91 della Legge Organica 3/2018 descrive il sistema di protezione digitale dei dipendenti rimandando direttamente ai contratti collettivi, che possono prevedere garanzie aggiuntive per i diritti e per le libertà riguardanti il trattamento dei dati personali dei lavoratori e per la salvaguardia dei diritti digitali nell’ambito lavorativo. Sebbene tale normativa si riferisca letteralmente solo ai contratti collettivi del settore privato, si potrebbe interpretare questo richiamo come estensibile anche agli accordi e ai patti dei funzionari pubblici per la tutela dei loro diritti digitali.

Tuttavia, se così fosse - dato che si tratta dell’interpretazione teleologica più ragionevole - non sarebbe superfluo che il legislatore organico stesso introducesse un riferimento diretto alla realtà dei funzionari, dato che esistono differenze molto importanti tra la contrattazione collettiva nel settore pubblico e in quello privato.

Infatti, il regime giuridico del personale pubblico è soggetto a una rigorosa riserva di legge ai sensi dell’articolo 103.3 della Costituzione spagnola. A differenza di quanto avviene nel settore privato, dove la norma giuridica funge da livello minimo di garanzia del diritto, suscettibile di miglioramento attraverso la contrattazione collettiva, nel settore pubblico la contrattazione collettiva non opera come meccanismo di sviluppo o ampliamento dei diritti. La legge non funge da piattaforma minima che può essere migliorata mediante convenzione. È concepita come una fase obbligatoria all’interno della procedura di elaborazione normativa, limitata ai termini previsti dall’articolo 37.1 del TREBEP ⁽¹³⁾.

In questo contesto, gli accordi e i patti dei dipendenti pubblici possono riguardare solo le materie espressamente elencate in tale disposizione, senza alcun margine per affrontare nuove dimensioni dei diritti del lavoro, come quella dei diritti

⁽¹³⁾ Questo precetto stabilisce l’elenco delle materie oggetto di negoziazione e indica chiaramente che tali materie “saranno oggetto di negoziazione, nei rispettivi ambiti e in relazione alle competenze di ciascuna Amministrazione Pubblica e con la portata legalmente applicabile in ciascun caso”. Non esiste nella PA la libertà di negoziazione prevista dallo Statuto dei Lavoratori.

digitali. Sebbene il TREBEP imponga all'Amministrazione l'obbligo di negoziare in buona fede, tale requisito è strettamente limitato alle materie legalmente definite, il che impedisce di incorporare, attraverso il dialogo sociale, proposte specifiche relative al settore digitale. Di conseguenza, la presunta parità di diritti richiederebbe riforme di ampia portata e, come minimo, una legge che ampli l'elenco delle materie oggetto di negoziazione, mediante l'inserimento esplicito di una nuova lettera nell'articolo 37.1 del TREBEP che consenta di affrontare in modo specifico la protezione e lo sviluppo dei diritti digitali nell'ambito del pubblico impiego.

4.4. L'obsolescenza normativa di fronte ai progressi tecnologici

L'attuale quadro di protezione dei diritti digitali dei dipendenti delle amministrazioni pubbliche è molto carente. La normativa è in ritardo rispetto allo sviluppo tecnologico, limitandosi a contemplare espressamente una serie ridotta di strumenti quali i sistemi di videosorveglianza, la geolocalizzazione o l'uso di dispositivi digitali, senza prevedere in modo specifico altre tecnologie emergenti che consentono anch'esse una sorveglianza e un controllo digitale molto intenso. È il caso, ad esempio, dei sistemi di identificazione biometrica, che consentono di verificare in modo affidabile l'identità del dipendente pubblico nel registro delle presenze e di controllare la sua effettiva presenza sul posto di lavoro ⁽¹⁴⁾. Queste tecniche, potenzialmente invasive, possono compromettere i diritti fondamentali del dipendente, senza che nell'ordinamento spagnolo esista una disposizione espressa che legittimi questo trattamento dei dati personali, ne regoli i limiti, le condizioni d'uso o le garanzie necessarie ⁽¹⁵⁾. Come sottolineato dall'Agenzia spagnola per la protezione dei dati, l'utilizzo di dati biometrici può comportare anche la deduzione di molteplici dati sanitari del dipendente. Infatti, i sistemi biometrici basati sul riconoscimento facciale possono trattare dati che consentono di estrarre informazioni sanitarie. Alcuni sistemi di identificazione tramite impronte digitali consentono la registrazione di parametri quali la temperatura o la pressione sanguigna, mentre le analisi biometriche della voce umana

⁽¹⁴⁾ Per quanto riguarda i problemi legati all'uso di questa tecnologia nell'ambito dell'amministrazione, rimando a J. Cantero Martínez, *Los derechos digitales del empleado público ante las transformaciones tecnológicas y el uso de la LA en los procesos de gestión de personas*, 2025, 28, *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 54 ss.

⁽¹⁵⁾ Le tecnologie che utilizzano dati biometrici sono collegate in modo permanente e irrevocabile all'identità di una persona; pertanto, hanno un impatto diretto o indiretto su una serie di diritti e libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea che possono andare oltre la privacy e la protezione dei dati, come la dignità umana, la libertà di circolazione, la libertà di riunione, ecc. Pertanto, le Linee guida 05/2022 del Comitato europeo per la protezione dei dati (CEPD) sull'uso del riconoscimento facciale nel settore delle forze di polizia, versione 2.0, del 26 aprile 2023, concludono che il sistema di riconoscimento facciale non soddisfa i requisiti di necessità e proporzionalità e costituisce un'ingerenza sproporzionata nei diritti fondamentali delle persone.

possono raccogliere più di cento parametri diversi relativi alla salute, che, tra gli altri, rilevano problemi fisici o psicologici ⁽¹⁶⁾.

A differenza della cosiddetta “amministrazione elettronica”, che è consistita fondamentalmente nella sostituzione della carta con mezzi elettronici e nell’automazione di alcune fasi delle procedure amministrative per consentirne l’elaborazione a distanza, la cosiddetta “amministrazione digitale” implica un ulteriore passo avanti nell’utilizzo degli strumenti tecnologici e, peraltro, in modo intensivo e dirompente ⁽¹⁷⁾. Attraverso i registri, l’amministrazione accumula un’enorme quantità di dati sui propri dipendenti pubblici che potrebbe elaborare e utilizzare attraverso lo sviluppo di algoritmi per creare profili e adottare e motivare decisioni gestionali in materia di valutazione delle prestazioni, carriera, assegnazione di posti o determinazione delle componenti retributive legate al rendimento e alle prestazioni dei propri dipendenti ⁽¹⁸⁾.

Tra tutte le tecnologie, l’IA rappresenta una delle rivoluzioni più significative degli ultimi tempi ⁽¹⁹⁾. I sistemi di IA sono quei sistemi in grado di elaborare un’enorme quantità di dati e informazioni in modo simile a un comportamento intelligente, che generalmente comprende aspetti di ragionamento, apprendimento, percezione, previsione, pianificazione o controllo ⁽²⁰⁾. A differenza di quanto accadeva con altre tecnologie dell’informazione precedenti, l’IA è caratterizzata dalla capacità di apprendere e agire con un certo grado di autonomia. Come previsto dall’articolo 3.1 del Regolamento sull’intelligenza artificiale (RIA), Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio approvato il 13 giugno 2024, un «sistema di IA» è un sistema basato su una macchina progettato per funzionare con diversi livelli di autonomia e in grado di mostrare capacità di adattamento dopo l’implementazione e che, per obiettivi espliciti o impliciti, deduce dalle informazioni in ingresso che riceve il modo di generare risultati in uscita, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare ambienti fisici o virtuali.

Dal punto di vista tecnico, l’IA consentirebbe all’Amministrazione di elaborare profili dei propri dipendenti pubblici e persino di riconoscere e gestire le loro emozioni ⁽²¹⁾, il che potrebbe essere uno strumento rilevante, ad esempio, per l’assegnazione dei

⁽¹⁶⁾ Agencia Española de Protección de Datos, Guía sobre el tratamiento de control de presencia mediante sistemas biométricos, novembre 2023, 13-14, in www.aepd.es/guias/guia-control-presencia-biometrico.pdf

⁽¹⁷⁾ E. Gamero Casado, *El tránsito hacia la Administración digital (o la historia interminable). Su conexión con el desarrollo económico y social*, 2022, a cura di Antonio Cerrillo Martínez D., 37.

⁽¹⁸⁾ R. Galindo Caldes, *Transformación digital local y función pública: aspectos organizativos*, 2023, 16, *Estudios de Relaciones Laborales*, Diputación de Barcelona, 15 ss.

⁽¹⁹⁾ Estrategia de Inteligencia Artificial 2024, Ministerio para la Transformación Digital y de la Función Pública, 2024, in https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.pdf

⁽²⁰⁾ Definizione utilizzata dalla Raccomandazione dell’UNESCO sull’etica dell’intelligenza artificiale, adottata dalla Conferenza Generale il 23 novembre 2021.

⁽²¹⁾ Il considerando 18 del RIA lo definisce come un sistema di IA destinato a distinguere o dedurre le emozioni o le intenzioni delle persone fisiche sulla base dei loro dati biometrici (felicità,

posti di lavoro o per la progettazione di percorsi formativi o di carriera professionale. La profilazione è definita all’articolo 4, paragrafo 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (regolamento sulla protezione dei dati), come qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di dati personali provenienti da fonti diverse per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti relativi al rendimento professionale, alla situazione economica, alla salute, alle preferenze personali, agli interessi, all’affidabilità, al comportamento, all’ubicazione o agli spostamenti di tale persona fisica. Tuttavia, l’impatto sui diritti fondamentali dei dipendenti è talmente rilevante che il RIA vieta direttamente l’uso della biometria per l’identificazione delle emozioni o la sorveglianza a distanza nell’ambito dei rapporti di lavoro.

Sono diverse le istituzioni pubbliche locali che possono essere interessate da queste trasformazioni tecnologiche. Si pensi, ad esempio, alla progettazione stessa dei posti di lavoro, alla loro robotizzazione, all’uso dell’IA come strumento di gestione delle risorse umane (per organizzare i processi di mobilità, la carriera professionale o la valutazione delle prestazioni) o semplicemente come importante “aiuto funzionale” del dipendente nello svolgimento delle sue mansioni, che gli consente di essere più produttivo ed efficiente ⁽²²⁾.

L’utilizzo dell’IA nel settore pubblico comporta anche un aumento dei rischi di errore o discriminazione e può contenere pregiudizi ⁽²³⁾. Non sorprende infatti che alcuni documenti ufficiali abbiano persino proposto che l’utilizzo di sistemi di IA sia accompagnato da un’importante riflessione sulla necessità di istituire procedure di sorveglianza algoritmica - che evitino errori e pregiudizi - e dalla creazione di un nuovo corpo di “ispettori algoritmici” ⁽²⁴⁾.

Sebbene il RIA sia stato emanato principalmente per favorire il mercato, la sua disciplina è perfettamente consapevole dei rischi che l’utilizzo dei sistemi digitali può

tristezza, indignazione, sorpresa, disgusto, imbarazzo, entusiasmo, vergogna, disprezzo, soddisfazione e divertimento, ecc.). Il considerando 44 ne vieta l’uso nell’ambiente di lavoro, non solo per le carenze della sua base scientifica e per la sua scarsa affidabilità, ma anche per l’impatto che può avere sul diritto alla vita privata e sul diritto alla parità di trattamento dei lavoratori.

⁽²²⁾ V. Almonacid Lamelas, *IA y Recursos Humanos: aplicaciones prácticas en las Administraciones públicas*, post publicado su Nosoloytos 3 ottobre 2024, in <https://nosoloytos.wordpress.com/2024/10/03/ia-y-recursos-humanos-10-aplicacionespracticas-en-las-administraciones-publicas/>

⁽²³⁾ I sistemi di IA possono riflettere le preferenze, le priorità e i pregiudizi (inconsi) dei loro creatori. Il problema è che i dati che alimentano i sistemi di IA possono essere imprecisi, incompleti o contenere errori o materiale irrilevante. I dati possono essere influenzati da pregiudizi. Il pregiudizio dell’IA nel settore dell’impiego pubblico è una differenza sistematica nel trattamento di determinate persone o gruppi, ad esempio stereotipi, pregiudizi o favoritismi, rispetto ad altri attraverso algoritmi di IA.

⁽²⁴⁾ Ministerio para la Transformación Digital y de la Función Pública, Consenso para una Administración abierta. Proyecto LIP 1: IA generativa y espacio de datos, INAP, 2024, 10, in www.inap.es/documents/10136/2342224/GT1-%20IAGenerativaYEspaciosDeDatos.pdf/5ae519f3-fad5-ac66-ffa7-068b73eec720

comportare per i diritti dei lavoratori, in particolare per il diritto alla privacy e alla protezione dei dati. Pertanto, sia l'articolo 6 del RIA che il suo allegato III hanno considerato come sistemi ad alto rischio tutti i sistemi che comportano la profilazione di persone fisiche, quelli destinati ad essere utilizzati per l'assunzione o la selezione di dipendenti, in particolare per pubblicare annunci di lavoro specifici, analizzare e filtrare le candidature e valutare i candidati.

Ebbene, di fronte ai rischi posti da queste nuove realtà tecnologiche, è necessario riflettere sul modo in cui esse possono influire sui diritti dei dipendenti pubblici. Per il momento si può affermare che disponiamo di un quadro normativo frammentato, incompleto e soprattutto obsoleto rispetto alle grandi sfide e ai rischi che l'IA può comportare nella gestione dell'impiego pubblico. Forse dovremmo avanzare verso il riconoscimento esplicito di nuovi diritti di natura digitale, come ad esempio il riconoscimento del diritto all'informazione algoritmica, ovvero il diritto di conoscere il codice sorgente e il funzionamento degli algoritmi utilizzati dall'amministrazione nella gestione del proprio personale in modo che sia comprensibile per gli interessati; il diritto a non essere oggetto di discriminazione a causa di pregiudizi dell'algoritmo; il diritto del dipendente di partecipare attraverso i propri rappresentanti o individualmente al processo decisionale sull'utilizzo dei sistemi di IA; il diritto all'intervento umano nel processo decisionale amministrativo che riguarda il dipendente; il diritto alla formazione o all'alfabetizzazione in materia di IA ⁽²⁵⁾, ecc. Questo quadro giuridico è ancora tutto da costruire.

5. In conclusione: la sfida di positivizzare i nuovi diritti emergenti sulla base degli orientamenti della Carta dei diritti digitali

Come abbiamo sottolineato, la costruzione giuridica dei diritti digitali realizzata nel TREBEP per i dipendenti pubblici è ormai superata rispetto alle importanti sfide poste dai progressi tecnologici. Il quadro giuridico vigente non è riuscito a stare al passo con la complessità e la portata dei nuovi strumenti digitali, creando un divario tra la realtà tecnologica e la risposta normativa, in particolare per quanto riguarda la tutela dei diritti fondamentali del personale al servizio delle amministrazioni pubbliche.

⁽²⁵⁾ L'articolo 4 del RIA prevede l'obbligo dell'Amministrazione di adottare misure volte a garantire che i propri dipendenti e le altre persone incaricate per loro conto del funzionamento e dell'utilizzo dei sistemi di IA abbiano un livello sufficiente di alfabetizzazione in materia di IA. L'alfabetizzazione in materia di IA deve fornire ai dipendenti interessati i concetti necessari per prendere decisioni informate in relazione ai sistemi di IA e per comprendere in che modo le decisioni adottate con l'ausilio dell'IA avranno un impatto su di loro (considerando n. 20 del RIA). A. Todolí Signes, *Entra en vigor la obligación de «alfabetización» en materia de IA de las empresas hacia sus trabajadores vía Reglamento IA*, post del 19 febbraio 2025, in Blog Argumentos en Derecho Laboral, <https://adriantodoli.com/2025/02/19/entra-en-vigor-la-obligacion-de-alfabetizacion-en-materia-de-ia-de-las-empresas-hacia-sus-trabajadores-via-reglamento-ia/>

È necessario aggiornare e ripensare il modello di tutela affinché questi nuovi processi di cambiamento tecnologico siano accompagnati da un quadro normativo adeguato, che garantisca la sicurezza giuridica e i diritti dei dipendenti ⁽²⁶⁾. A tale fine assume un ruolo essenziale la Carta de Derechos Digitales approvata dal Consiglio dei ministri spagnolo nel luglio 2021, che è stata adottata in attuazione della misura n. 28 della Strategia nazionale per l'intelligenza artificiale al fine di creare fiducia nei cittadini sull'uso dell'IA e con l'intento di stabilire un quadro etico e normativo che rafforzi la protezione dei diritti dei cittadini ⁽²⁷⁾. Sebbene questo documento non abbia carattere normativo, tuttavia definisce il quadro di riferimento che il governo spagnolo deve tenere in considerazione per progredire in questo campo, poiché sollecita direttamente il governo ad adottare le disposizioni opportune per garantire l'efficacia dei diritti digitali nell'ambiente di lavoro ⁽²⁸⁾.

La Carta delinea un quadro dinamico e attento alla dimensione umana del fenomeno digitale, che consente di garantire la protezione dei diritti individuali e collettivi dei cittadini nel settore digitale. Come previsto dal RIA, essa richiede che, in ogni caso, lo sviluppo e l'uso di algoritmi e di qualsiasi altro procedimento equivalente nell'ambito lavorativo siano sottoposti a una valutazione d'impatto relativa alla protezione dei dati personali, che dovrà includere nella sua analisi i rischi connessi ai principi etici e ai diritti relativi all'uso dell'intelligenza artificiale contenuti nella suddetta Carta. Vengono presi in considerazione, in particolare, i rischi riferiti alla prospettiva di genere e il divieto di qualsiasi forma di discriminazione diretta o indiretta, con particolare attenzione ai diritti di conciliazione. La Carta riconosce il diritto dei rappresentanti legali dei lavoratori ad essere informati con adeguato anticipo dei cambiamenti tecnologici che si verificheranno e consente inoltre di poter stabilire garanzie aggiuntive di tali diritti attraverso la contrattazione collettiva.

Il punto 4 della Carta disciplina i diritti nel mondo del lavoro per garantire la dignità e i diritti fondamentali dei lavoratori negli ambienti digitali. Alcuni di questi diritti sono già espressamente sanciti dall'articolo 14.j.bis) del TREBEP. L'aspetto più

⁽²⁶⁾ Cortés abad O., *Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración Pública*, 2020, 18, *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 54 ss., <https://burjcdigital.urjc.es/items/71e5631c-2e63-4869-9fca-026dce4fecae>

⁽²⁷⁾ <https://espanadigital.gob.es/lineas-de-actuacion/carta-de-derechos-digitales>

⁽²⁸⁾ Allo stesso modo, è degna di nota la Dichiarazione europea sui diritti e principi digitali per il decennio digitale del Parlamento europeo, del Consiglio e della Commissione, pubblicata nella Gazzetta ufficiale dell'Unione europea il 23 gennaio 2023, (C 23/01), che mira a stabilire il quadro globale che deve guidare questi processi di trasformazione digitale, che devono essere basati sui valori europei e sui diritti fondamentali dell'UE, porre le persone al centro, riaffermare i diritti umani universali e andare a beneficio di tutte le persone, delle imprese e della società nel suo complesso. Sebbene tale documento abbia solo carattere dichiarativo, definisce gli obiettivi da raggiungere, che dovranno tradursi in una serie di diritti di natura digitale per tutti i lavoratori e, quindi, anche per i dipendenti pubblici. Sottolinea inoltre la necessità di garantire che le decisioni importanti che riguardano i lavoratori siano soggette a supervisione umana e che, in generale, essi siano informati del fatto che stanno interagendo con sistemi di intelligenza artificiale. In altre parole, viene stabilito ciò che è stato definito “riserva di umanità”.

importante di questo documento è, a mio avviso, che inquadra e limita i poteri di sorveglianza e supervisione digitale dell'Amministrazione e che estende l'ambito oggettivo e materiale di applicazione dell'articolo 14.j.bis).

La Carta sottolinea infatti la necessità di riconoscere come un diritto del dipendente l'uso lecito, leale, proporzionato e trasparente dei controlli digitali aziendali, nonché il diritto di ricevere dal datore di lavoro i mezzi tecnologici necessari per svolgere la propria attività senza che i lavoratori debbano mettere a disposizione di quest'ultimo i mezzi di loro proprietà; il documento riconosce inoltre il diritto di venire informati sulla politica di utilizzo di tali dispositivi digitali, compresi i criteri per un eventuale utilizzo a fini privati.

Nell'intento di estendere l'ambito di protezione dei diritti digitali, la Carta riconosce ai dipendenti non solo il diritto alla protezione della vita privata e familiare, ma anche il diritto all'onore, all'immagine, alla protezione dei dati e alla segretezza delle comunicazioni anche in relazione all'utilizzo da parte della p.a. di strumenti di monitoraggio, di sistemi biometrici, di analisi e processi decisionali in materia di risorse umane e relazioni industriali, e in particolare in relazione all'analisi dei social network, prevedendo anche l'obbligo di informare i rappresentanti legali dei lavoratori dell'uso di tali dispositivi o strumenti.

Le misure sopra indicate sarebbero idonee a risolvere alcune delle carenze tecniche giuridiche dell'attuale quadro normativo. Infatti, le informazioni fornite dovrebbero soddisfare i parametri, le regole e le istruzioni su cui si basano gli algoritmi o i sistemi di intelligenza artificiale che influenzano il processo decisionale che possono incidere sulle condizioni di lavoro, sull'accesso e sul mantenimento dell'occupazione, compresa la profilazione. Allo stesso tempo, si fa riferimento anche alla necessità di garantire i diritti dei lavoratori rispetto all'uso da parte del datore di lavoro di procedure di analisi dei dati, intelligenza artificiale e, in particolare, quelle previste dalla legislazione in materia di utilizzo di decisioni automatizzate nei processi di selezione del personale.

Altrettanto degna di nota è anche la Dichiarazione europea sui diritti e principi digitali per il decennio digitale del Parlamento europeo, del Consiglio e della Commissione, pubblicata nella Gazzetta ufficiale dell'Unione europea il 23 gennaio 2023, (C 23/01), che mira a delineare il quadro globale che deve guidare i processi di trasformazione digitale, in modo che siano basati sui valori europei e sui diritti fondamentali dell'UE, fra i quali: porre le persone al centro, riaffermare i diritti umani universali e andare a beneficio di tutte le persone, delle imprese e della società nel suo complesso.

Sebbene tale documento abbia solo carattere dichiarativo, così come la Carta dei diritti digitali spagnola, indica gli obiettivi da raggiungere e stabilisce la tabella di marcia per sviluppare questa materia. Le linee guida tracciate dalla Dichiarazione europea dovrebbero tradursi nel riconoscimento di una serie di diritti di natura digitale per tutti i lavoratori e, quindi, anche per i dipendenti pubblici.

La Dichiarazione sottolinea inoltre la necessità di garantire che le decisioni importanti che riguardano i lavoratori siano prese con l'intervento e la supervisione umana e che, in generale, essi siano informati del fatto che stanno interagendo con sistemi di intelligenza artificiale. In altre parole, viene previsto ciò che è stato definito “riserva di umanità” ⁽²⁹⁾.

In definitiva, è urgente che il legislatore statale spagnolo avvii un processo di chiarimento e aggiornamento integrale del regime giuridico dei diritti digitali nel settore dell'impiego pubblico, prendendo come riferimento gli orientamenti contenuti nella Carta dei diritti digitali del 2021 e nella Dichiarazione europea dei diritti e dei principi digitali del 2023. Solo attraverso questo lavoro di concretizzazione normativa sarà possibile adattare efficacemente i diritti fondamentali dei dipendenti pubblici alle profonde e incessanti sfide poste dalla trasformazione digitale delle amministrazioni pubbliche.

⁽²⁹⁾ Per approfondire l'argomento, v. J. Ponce Solé, *Límites jurídicos de la toma de decisiones discrecionales automatizadas mediante inteligencia artificial: racionalidad, sabiduría y necesaria reserva jurídica de humanidad en el ámbito digital*, *Revista General de Derecho Administrativo*, 2024, 66.

Bibliografía

- Almonacid Lamelas V., *LA y Recursos Humanos: aplicaciones prácticas en las Administraciones públicas*, Nosoloaytos, 2024, in <https://nosoloaytos.wordpress.com/2024/10/03/ia-y-recursos-humanos-10-aplicaciones-practicas-en-las-administraciones-publicas>
- Cabellos Espiérrez M. Á., *El derecho a la protección de datos personales ante la videovigilancia en el ámbito laboral: la progresiva devaluación en la jurisprudencia constitucional de la obligación de informar al trabajador*, in *Revista Vasca de Administración Pública*, 2024, 128-I, in <https://doi.org/10.47623/ivapr vap.128.2024.1.01>
- Cantero Martínez J., *Los derechos digitales del empleado público ante las transformaciones tecnológicas y el uso de la LA en los procesos de gestión de personas*, in *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 2025, 28.
- Cortés Abad O., *Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración Pública*, in *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 2020, 18, in <https://burjcdigital.urjc.es/items/71e5631c-2e63-4869-9fca-026dce4fecae>
- Lertxundi Lertxundi A., *El impacto de la digitalización en los derechos fundamentales del personal empleado público en España*, in *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 2020, 18, in www.ivap.euskadi.eus/contenidos/informacion/18_rev gp/eu_def/Lertxundi_38_53.pdf
- Galindo Caldés R., *Transformación digital local y función pública: aspectos organizativos*, Estudios de Relaciones Laborales, Diputación de Barcelona, 2023, 16.
- Gamero Casado E., *El tránsito hacia la Administración digital (o la historia interminable). Su conexión con el desarrollo económico y social*, in *Administración digital*, diretta da A. Cerrillo Martínez - Dykinson, 2022.
- Mercader Uguina J., *Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?*, in *Relaciones laborales: Revista crítica de teoría y práctica*, 2001, 1, 665-686
- Mercader Uguina J., *En busca del empleador invisible: algoritmos e inteligencia artificial en el derecho digital del trabajo*, in *El Cronista del Estado Social y Democrático de Derecho*, 2022, 100, 136-145.
- Ponce Solé J., *Límites jurídicos de la toma de decisiones discrecionales automatizadas mediante inteligencia artificial: racionalidad, sabiduría y necesaria reserva jurídica de humanidad en el ámbito digital*, in *Revista General de Derecho Administrativo*, 2024, 66.
- Rodríguez Fernández L., *Robots, algoritmos y trabajos*, El País, 2023, in www.iustel.com//diario_del_derecho/noticia.asp?ref_iustel=1232476&utm_source=D&utm_medium=email&utm_campaign=17/4/2023&utm_popup=1
- Todolí Signes A., *La inteligencia artificial no te robará tu trabajo, sino tu salario. Retos del Derecho del Trabajo frente a la dirección algorítmica*, in *El Cronista del Estado Social y Democrático de Derecho*, 2022, 100, 151.
- Todolí Signes A., *Entra en vigor la obligación de «alfabetización» en materia de LA de las empresas hacia sus trabajadores vía Reglamento LA*, post de 19 de febrero de 2025, in *Blog Argumentos en Derecho Laboral*, in <https://adriantodoli.com/2025/02/19/entra-en-vigor-la-obligacion-de-alfabetizacion-en-materia-de-ia-delas-empresas-hacia-sus-trabajadores-via-reglamento-ia/>