



ANNO III, N. 3-4, 2013



## **Democrazia e Sicurezza - Democracy and Security Review**

Direttore responsabile: Salvatore Bonfiglio

Redazione: c/o il Laboratorio Multimediale e di Comparazione Giuridica - via G. Chiabrera, 199 - 00145 Roma - Università degli Studi "Roma Tre".

Rivista iscritta presso il Tribunale di Roma, n. 373/2011 del 5 dicembre 2011.

ISSN: 2239-804X

### **Scientific Board**

Domenico Amirante (Seconda Università degli Studi di Napoli); Fabrizio Battistelli (Università degli Studi di Roma "La Sapienza"); Paolo Benvenuti (Università degli Studi "Roma Tre"); Salvatore Bonfiglio (Università degli Studi "Roma Tre"); Roberto Borrello (Università degli Studi di Siena); Gerardo Cautilli (Direzione Centrale degli Istituti di Istruzione - Ministero dell'Interno); Francesco Clementi (Università degli Studi di Perugia); Rosario Garcia Mahamut (Universitat Jaume I - Castellón); Hermann Groß (Hessische Hochschule für Polizei und Verwaltung); Andrew Hoskins (University of Glasgow); Martin Innes (Cardiff University); Luis Jimena Quesada (Universidad de Valencia); Luis Maria Lopez Guerra (juge de la Cour Européenne des Droits de l'Homme-Strasbourg); Stelio Mangiameli (Direttore dell'ISSIRFA-CNR); Maria Luisa Maniscalco (Università degli Studi "Roma Tre"); Kostas Mavrias (Università degli Studi di Atene); Lina Panella (Università degli Studi di Messina); Otto Pfersmann (Université Paris-Sorbonne); Artemi Rallo Lombarte (Universitat Jaume I - Castellón); Angelo Rinella (LUMSA); Cheryl Saunders (Melbourne Law School); Roberto Sgalla (Scuola Superiore di Polizia-Direttore); Giovanna Spagnuolo (Isfol-Italy); Alessandro Torre (Università degli Studi di Bari "Aldo Moro"); Matthew C. Waxman (Columbia Law School).

### **Editorial staff**

Coordinators of the section: Mario Carta (Note); Valentina Fiorillo, Cristina Gazzetta e Massimo Rubechi (Osservatorio sulla normativa); Giulia Aravantinou Leonidi, Caterina Bova e Pamela Martino (Osservatorio sulla giurisprudenza); Valerio Sarcone e Francesco Soluri (Osservatorio degli operatori della sicurezza); Massimo Pellingra Contino, Laura Giobbi e Valeria Rosato (Focus); Maria Flavia Casatelli (Recensioni)

Assistant Editors: Francesca Fanti



## INDICE

Editoriale

*The Right Not to Be Criminalized*  
di Salvatore Bonfiglio

Saggi

*Privacy e sicurezza*  
di Licia Califano

Note

*La costruzione di un efficace sistema tunisino di protezione dei diritti umani*  
di Stefania Spada

*Il ruolo delle forze armate croate nella difesa dell'ambiente*  
di Alessandra Carloni





## EDITORIALE



## THE RIGHT NOT TO BE CRIMINALIZED

Salvatore Bonfiglio

### 1. The systemic deficiencies in the asylum procedure and reception conditions for asylum seekers

On 6 May 2009, to 35 nautical miles south of Lampedusa (Agrigento), that is, within the Maltese Search and Rescue Region of responsibility, migrants were intercepted by three ships by the Italian Revenue Police (Guardia di finanza) and the Coastguard. The occupants of the intercepted vessels were transferred onto Italian military ships and returned to Tripoli. Migrants alleged that during that voyage the Italian authorities did not inform them of their real destination and took no steps to identify them. The persons intercepted should have to be informed in an appropriate way so that they can express any reasons for believing that disembarkation in the proposed place would be in breach of the principle of non-refoulement. The UNHCR stated that the principle of non-refoulement involved procedural obligations for States. Furthermore, the right of access to an effective asylum procedure conducted by a competent authority was all the more vital when it involved “mixed” migratory flows, in the framework of which potential asylum seekers must be singled out and distinguished from other migrants. The rejections on the high seas, according to a recent decision of the European Court of Human Rights (*Hirsi and other c. Italy*, February 23, 2012), are unable to distinguish between simple illegal immigrants and asylum seekers. And

this is very serious because «the right to have rights» (Arendt) should be at the global level as «a lawful incarnation of the right of asylum»<sup>1</sup>.

1.1 In asylum there are significant differences between national provisions and their application. For this reason, while in the past the Treaty of Amsterdam provided only the adoption of minimum standards, now the Article 78 of the Treaty on the Functioning of the European Union (TFEU) goes beyond the regulatory model of harmonization, establishing a uniform *status* of asylum valid in the European Union.

The European Council remains committed to the objective of establishing a common area of protection and solidarity based on a common asylum procedure and a uniform *status* for those granted international protection. According to the European Council: «The development of a Common Policy on Asylum should be based on a full and inclusive application of the 1951 Geneva Convention relating to the Status of Refugees and other relevant international treaties. Such a policy is necessary in order to maintain the long-term sustainability of the asylum system and to promote solidarity within the Union. Subject to a report from the Commission on the legal and practical consequences, the Union should seek accession to the Geneva Convention and its 1967 Protocol»<sup>2</sup>.

<sup>1</sup> E. Larking, 'Human rights, the right to have rights, and life beyond the pale of the law', in *Australian Journal of Human Rights*, vol. 18, n. 1, 2012, p. 77. The High Court of Australia rules that using the outcome of an ASIO (Australian Security Intelligence Organisation) security assessment to deny a refugee a protection visa is invalid.

<sup>2</sup> European Council, The Stockholm programme – An open and secure Europe serving and protecting citizens (2010/C 115/01).

1.2 In some EU countries, such as Greece, there is a systemic deficiency in the asylum procedure and reception conditions for asylum seekers. The Court of Human Rights (*M.S.S. c. Belgium and Greece*, January 21, 2011) ruled not only that the Hellenic Republic had violated Article 3 of the ECHR because of the existential conditions of detention of the applicant on its territory, and Art. 13 of the ECHR in conjunction with the said Article 3, because of shortcomings in the asylum procedure followed for the applicant, but also that the Kingdom of Belgium had violated Art. 3 of the ECHR, exposing the plaintiff to risks related to the deficiencies of the asylum procedure in Greece and existential conditions of detention contrary to that Article. On the other hand, it must be said that in 2010 Greece was the entry point for about 90% of illegal migrants, so that the burden borne by that Member State in reason of this great flux was out of proportion to that sustained by other EU Member States and the Greek authorities were physically unable to cope with it. For this reason must prevail solidarity between the EU countries, according to the most recent case law of the European Court of Justice and as required by Regulation (EU) No. 439/2010 of the European Parliament and the Council of 19 May 2010, establishing the European Asylum Support Office. The function of this office is to strengthen practical cooperation between EU countries on asylum, supporting the countries of the EU in which asylum and reception systems are disproportionately subject to strong pressures, in particular because of their geographical or demographic situation characterized by the sudden arrivals of a large number of non-EU citizens who may be in need of international protection. It not is surprising, therefore, that the

European Asylum Support Office was opened in Valletta Harbour, Malta – the southern border of the EU – with the decision 2010/762/UE of the Representatives of the Member States, meeting on the 25 February 2010. The Office, which helps also to improve the implementation of the Common European Asylum System (CEAS), must support the EU countries by coordinating asylum support teams, as well as actions on the initial analysis of asylum applications and the rapid creation of adequate reception facilities.

## 2. Administrative detention of irregular migrants

It has been said that the Italian law-maker has adopted some unlawful provisions in order to address the complex phenomenon of immigration, often with public safety measures. Although not declared unconstitutional, other provisions adopted and still in force are difficult to implement, ineffective and useless. This is the case of the rules introduced by Law 15.07.2009, n. 94. The main novelty of this law is to have introduced into the Italian legal system a new crime, that of illegal immigration<sup>3</sup>. There is therefore a real turning point in the regulatory system on immigration: the violation of the rules

4

<sup>3</sup> T. Catananti T., 'I reati in materia di immigrazione dopo la legge n. 94 del 2009, in *Rivista dell'Associazione italiana dei Costituzionalisti*, del 02.07.2010, p. 1; C. Renoldi C., 'I nuovi reati di ingresso e di permanenza illegale dello straniero nel territorio dello Stato', in *Dir. imm. citt.* XI, 4-2009, p. 38 e ss; M. Donini, 'Il cittadino extracomunitario da oggetto materiale a tipo d'autore nel controllo penale dell'immigrazione', in *Quest. Giust.*, 2009, p.127 e ss.

concerning the entry and residence in the territory of the State, up until now punished by expulsion, is raised to criminal illicit. The criminalization of illegal status is likely to devalue the fundamental liberal principle of the criminal law of the fact – based on Article 25, paragraph 2, of the Italian Constitution – according to which the penalty may be lawfully provided only with respect to material facts and not prejudicial to the legal interests than mere subjective personal conditions, such as those of migrants.

The Law 15.07.2009, n. 94, punishes the illegal entry into the territory of the State, which classifies illegal entry as a crime to commit instantly, by passing illegally the borders. But this first provision of law is useless, because the problem is not so much the entry (which in most cases is legal), but the permanence of illegal non-EU (citizens of non-EU countries). In addition, a final assessment of the ineffectiveness of the financial penalty: illegal immigrants without a residence permit do not have the resources to pay the penalty, because certainly they do not have a regular job.

Italian law-maker has adopted another ineffective provision, which allowed the extension of the time of detention in Centers for Identification and Expulsion (CIE) for up to eighteen months, in order to allow the identification and expulsion procedure. When they were opened in Italy, with the Law Turco-Napolitano of 1998, under the name of the detention centers (CPT), the maximum limit of detention was thirty days. The limit then became sixty days in 2002 with the Bossi-Fini law. The so-called security package in 2009 had already tripled the limit from two to six months. The decree 23 June 2011, No 89, once again, extended the duration of the detention from six

to eighteen months, in art. 3 on "Changes and additions to Legislative Decree 25 July 1998, No 286 implementing Directive 2008/115/EC "European Parliament and the Council of 16 December 2008 laying down rules and procedures applicable in Member States for returning citizens of third countries whose stay is illegal. In fact, the Directive 2008/115/EC - Return of third-country nationals illegally staying - provides for administrative detention of irregular migrants for up to 18 months. Of course, in regulating the manner and timing of the return of third-country nationals illegally staying, it stipulates the gradual series of administrative actions, favoring voluntary departure of foreigners irregularly and, above all, conceiving the detention as a last resort. However, it is desirable to amend the EU and Italian regulatory framework to provide for a shorter duration of the maximum period of detention and the identification of modern and effective tools for establishing the identity and nationality or for the acquisition of documents.

6

Detention cannot actually turn into a sort of alternative to prison detention, because of its long duration; but personal liberty is inviolable and more important than securing of borders. For this reason administrative detention is a legitimate limitation of personal autonomy only if required for a short duration aiming to the identification and the departure of irregulars and, as such, if it is not violating the right not to be criminalized as irregular<sup>4</sup>. According to the European Court of Human Rights, the principle of proportionality requires that the detention of nationals illegally staying or extradition procedure

<sup>4</sup> Dennis J. Baker, *The Right Not to be Criminalized*, Ashgate, Farnham, Surrey, UK 2011.

does not go beyond a reasonable time, it does not exceed the time required to reach the goal pursued (see, inter alia, *Saadi v. United Kingdom*, January 29, 2008). Can it be assumed for illegal immigrants detained in the identification centers a stay which exceeds the 20 or 35 days provided for foreign asylum seekers without identification or who have escaped the border control? Maybe. Certainly a stay for up to 18 months in the identification centers cannot be considered reasonable. Furthermore, adequate reception facilities for unaccompanied minors should always be provided, ensuring that they are not imprisoned and that they are kept separate from adults.

Any person may dispose of (or deliberately put at risk) his freedom, while every political institution may take legitimate and effective measures in proportion to the losses suffered by the social community due to misconduct, and yet, in the Constitutional State as each person cannot dispose of his dignity, so the authority is obliged to respect the very value of human dignity.





**SAGGI**





# Privacy e sicurezza

di Licia Califano<sup>1</sup>

Sommario: 1. Riservatezza e sicurezza: definire i contorni per bilanciare. - 1.1 I fondamenti costituzionali della tutela della riservatezza. - 2. Il quadro europeo in tema di riservatezza e protezione dati. - 3. La sicurezza come fine e la riservatezza come (ostacolo nel) mezzo. - 3.1 La videosorveglianza a fini di tutela della sicurezza urbana. - 3.2 Il trattamento dei dati biometrici a fini di sicurezza. - 4. La riservatezza come fine e la sicurezza come mezzo: alcune riflessioni incrociate su cybercrime, reati contro la privacy e “cyberbullismo”. - 5. Riflessioni conclusive

1

## 1. Riservatezza e sicurezza: definire i contorni per bilanciare

Affrontare un tema quale “privacy e sicurezza” è senza dubbio estremamente complesso, sia per l’ampiezza e l’eterogeneità delle possibili declinazioni di entrambi i concetti

<sup>1</sup> Le opinioni espresse nel presente scritto sono del tutto personali e non impegnano in alcun modo l’Autorità Garante. L’A. intende ringraziare Giuseppe Busia, Claudio Filippi, Luigi Montuori e Biancamaria Sabatini dell’Ufficio dell’Autorità per aver letto e fornito utili osservazioni su una prima versione del presente lavoro, così come Antonio Caselli del medesimo Ufficio per la documentazione fornita. La responsabilità di quanto scritto rimane interamente dell’Autrice.



che per la difficoltà insita nel tentativo di trovare un bilanciamento tra i due. Nel descrivere il binomio "sicurezza e privacy" è utile partire da un presupposto, ovverosia l'intima connessione che esiste tra queste due tematiche, sia da un punto di vista generale che all'interno dell'ordinamento italiano in particolare. In tal senso basti pensare che il primo strumento legislativo introdotto in Italia a tutela della riservatezza (legge n. 675/1996 recante norme a Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) venne di fatto "imposto" al nostro Paese come pre-requisito per aderire al sistema Schengen e consentirne la completa applicazione sul territorio nazionale e questo al fine di poter fruire dei vantaggi legati agli scambi commerciali nel quadro di una politica di sicurezza comune<sup>2</sup>.

A differenza di quanto avviene nella Carta dei diritti fondamentali dell'Unione europea (art. 6), la sicurezza nell'ordinamento italiano non ha una precisa codificazione costituzionale in grado di suffragarne senza dubbio alcuno il rango di diritto fondamentale. Pur avendo essa differenti declinazioni costituzionali, ed essendo stata da alcuni definita addirittura come diritto di libertà<sup>3</sup>, occorre valutare con attenzione se questa sia da considerarsi come semplice «interesse della collettività» o anche come diritto dell'individuo

<sup>2</sup> G. GARDINI, *Le regole dell'informazione*, Bruno Mondadori, Milano, 2009, p. 246.

<sup>3</sup> C. MOSCA, *La sicurezza come diritto di libertà*, Cedam, Milano, 2012.



per se<sup>4</sup>. Questo vale tanto per il volto repressivo della sicurezza – che mira principalmente a mantenere lo status quo – quanto per quello maggiormente propositivo ovverosia che impegna le autorità pubbliche nella rimozione degli ostacoli che si pongono agli individui nella realizzazione e nel godimento dei propri diritti fondamentali<sup>5</sup>.

Per altro verso, sebbene la possibilità che la sicurezza entri nel gioco del bilanciamento<sup>6</sup> dipenda senza dubbio dalla sua qualificazione come diritto costituzionale o meno e, in ogni caso, dalla definizione della sua “dimensione costituzionale”<sup>7</sup>, anche una sua riduzione in termini di “bisogno elementare” solleva comunque dei delicati problemi in relazione alla possibilità che in nome della sicurezza si pongano limiti all’esercizio di diritti fondamentali, come la tutela della riservatezza.

La riservatezza – secondo elemento del nostro binomio lessicale e concettuale, e sul quale ci si soffermerà maggiormente – è segnata da una peculiarità di fondo: essa si presenta infatti come uno dei diritti di più difficile definizione, forse proprio per l’intrinseca pluralità contenutistica che la caratterizza. Essa, in primo luogo, assume una dimensione socio-relazionale, delineandosi come una sorta di “diritto alla

<sup>4</sup> G. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, in G. COCCO (a cura di), *I diversi volti della sicurezza*, Giuffrè, Milano, 2012, pp. 17-80 (anticipato nel 2009 in [www.associazionedeicostituzionalisti.it](http://www.associazionedeicostituzionalisti.it)).

<sup>5</sup> *Ibidem*.

<sup>6</sup> Su questo aspetto non si può che rinviare ampiamente al contributo di Alessandro Pace nel presente volume.

<sup>7</sup> T. GIUPPONI, *Le dimensioni costituzionali della sicurezza*, Libreria Bonomo, Bologna, 2010.



solitudine” rectius “diritto ad essere lasciati da soli” (right to be left alone di matrice anglosassone). In questo caso la tutela della riservatezza presuppone forme e modalità di protezione giuridica di quella particolare sfera delle vicende umane che si qualifica normalmente come vita privata o intima, in tal senso meritevole di tutela giuridica nei confronti di ingiustificate interferenze o altre indebite forme di indiscrezione provenienti dall'esterno<sup>8</sup>.

Gli ordinamenti giuridici hanno sentito il bisogno di garantire i cittadini dalle indebite interferenze (sia da parte di soggetti pubblici che di altri soggetti privati) nell'intimità privata, escludendo la diffusione di dati, fatti e informazioni che possano toccare un individuo nello sviluppo della sua area strettamente riservata e personale.

La protezione giuridica della sfera della riservatezza ha tuttavia registrato una progressiva evoluzione ordinamentale che coinvolge la fonte costituzionale, l'assetto normativo interno, comunitario e internazionale e, infine, la giurisprudenza costituzionale, comunitaria e ordinaria. Tale evoluzione è stata consequenziale rispetto ai profondi mutamenti connessi a quelle che Stefano Rodotà nel suo *Tecnologie e diritti* definisce: «nuove dimensioni della raccolta e del trattamento delle informazioni»<sup>9</sup>. Si tratta di una tendenza determinata da «fenomeni interdipendenti tra loro» quali: da

<sup>8</sup> G. M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in P. RIDOLA, R. NANIA (a cura di), *I diritti costituzionali*, Giappichelli, Torino, 2006, vol. II, pp. 617 ss.

<sup>9</sup> S. RODOTÀ, *Tecnologie e diritti*, il Mulino, Bologna, 1995.



un lato, le nuove modalità di raccolta dati automatizzate tramite l'ausilio dell'informatica, dall'altro, il bisogno di dati, sempre crescente, da parte delle istituzioni pubbliche e private. Si tratta di un'enorme mole di dati connessi alla vita, alla sfera privata, alla salute, al pensiero politico, al credo religioso di un individuo che, collegate tra loro, sono in grado di "profilare" (si usa qui questa espressione in senso atecnico) un individuo.

La riservatezza si distacca così dall'individuo fisico per estendersi alle informazioni e ai dati che a questo stesso individuo si riferiscono e di cui offrono una rappresentazione<sup>10</sup>. Dalla dimensione socio-relazionale si passa così a definire la riservatezza anche sulla base dei contenuti informativi dell'individuo, e sulla necessità di difenderlo dai molteplici casi in cui sarebbe possibile configurare un controllo sui cittadini tramite i loro dati personali<sup>11</sup>. Si è dunque passati dal «diritto alla riservatezza» quale garanzia offerta dall'ordinamento al «diritto alla protezione dei dati personali», configurando così un nuovo diritto, in grado di tutelare i flussi informativi connessi ai dati personali in ogni settore pubblico e privato, estendendo o comunque declinando in termini più ampi il concetto di riservatezza.

In questo contesto, oggi in particolare, è centrale il ruolo svolto da un apposito apparato autoritativo, il Garante per la protezione dei dati personali, cui è attribuito un complesso di funzioni pubbliche direttamente connesse all'obiettivo di

<sup>10</sup> G. GARDINI, *op. cit.* p. 240.

<sup>11</sup> G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), *I diritti in azione*, il Mulino, Bologna, 2007, p. 353.



tutelare il «diritto» di ogni individuo alla «protezione dei dati personali che lo riguardano» (articolo 1 del Codice privacy, d.lgs 196/2003).

Tuttavia, come si anticipava, tale protezione giuridica non assorbe per intero la tematica della riservatezza ma ne costituisce piuttosto una esplicitazione parziale. Ciò è specificato dallo stesso Codice che, all'articolo 2, indicando le finalità alla base della sua adozione, afferma che esso è rivolto a garantire che il trattamento dei dati personali si svolga «nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato con particolare riferimento alla riservatezza, all'identità e al diritto alla protezione dei dati personali» (articolo 2, comma 1). Si tratta, dunque, di una disposizione che accentua il rilievo della situazione giuridica soggettiva (il diritto alla protezione dei dati personali), la quale viene accostata a principi di rango costituzionale quali dignità dell'uomo, identità personale e riservatezza.

In linea con tali premesse la tutela della riservatezza si è sviluppata principalmente intorno a tre direttrici: a) qualità delle informazioni soggette a tutela; b) strumenti individuali di tutela; c) area di insistenza della privacy.

Con riguardo al primo aspetto occorre sottolineare che il Codice privacy tutela non soltanto fatti attinenti all'immagine del soggetto, alle sue abitudini familiari, alla sua reputazione sociale ma anche dati relativi all'opinione politica, alle convinzioni religiose, all'appartenenza sindacale, alla vita sessuale (cd. dati sensibili).

In secondo luogo, lo "strumentario" in mano al singolo si arricchisce di nuove facoltà: accanto alle norme che





regolamentano comunicazione e diffusione dei dati, vi sono una serie di attività che rientrano tutte nel più ampio potere di controllo sui propri dati personali e che ricomprendono il diritto di accesso ai propri dati personali presso chi li detiene, il diritto di opporsi al loro trattamento, il diritto a ottenere il blocco o la cancellazione di dati trattati in violazione di legge. Tutto ciò si articola grazie al ruolo del Garante che decide su ricorsi, reclami e segnalazioni del cittadino, così come è in grado di attivarsi d'ufficio.

In terzo luogo, l'area di insistenza della privacy si estende alla protezione di qualsiasi turbativa volta non solo a carpire informazioni, ma anche ad arrecare una qualsiasi forma di disturbo (es: molestie telefoniche), giungendo così a una sorta di «diritto ad essere lasciati in pace» fino al «diritto all'oblio» (cd. privacy storica)<sup>12</sup>. Da qui deriva proprio l'intrinseca pluralità contenutistica della nozione di riservatezza e delle pretese di rango costituzionale ad essa collegate. In tal modo viene confermata la qualificazione del diritto alla riservatezza quale vero e proprio diritto della personalità, diradando i dubbi circa il suo fondamento costituzionale: ormai è sempre più diffusa la convinzione circa la riconduzione del diritto in



<sup>12</sup> Da ultimo sul tema: F. PIZZETTI, *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013; G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Il diritto dell'informazione e dell'informatica*, n. 3/2010, pp. 391 – 404. In una differente prospettiva V. MAYER SCHÖNBERGER, *Delete: the virtue of forgetting in the digital age*, Princeton University press, 2009.



questione alla copertura costituzionale fornita anzitutto dall'articolo 2 della Costituzione quale fattispecie aperta<sup>13</sup>.

### 1.1 I fondamenti costituzionali della tutela della riservatezza

Come anticipato, la Costituzione italiana non tratta esplicitamente del diritto alla riservatezza; tantomeno si occupa della protezione dei dati personali, diritto, come si è visto, di ben più recente nascita ed affermazione. Più correttamente osserviamo che la riservatezza non viene esplicitamente trattata come tutela della sfera intima della persona, così come la riconoscono le carte internazionali (Dichiarazione Onu del 1948), europee (Cedu del 1950) e più strettamente comunitarie (Carta di Nizza del 2000 e Tdue come modificato dal Trattato di Lisbona).

Questa assenza non è tanto da ascrivere all'insussistenza di esigenze di tutela della privacy all'epoca dell'Assemblea costituente: in altri ordinamenti (Regno Unito, ma soprattutto Stati Uniti) il dibattito era già piuttosto sviluppato, e sia la dottrina che le corti avevano già offerto i primi strumenti giuridici in proposito. Semmai, sembra più corretto ravvisarsi «una certa arretratezza rispetto ai problemi “reali” che andavano emergendo, tanto da far ritenere che gli occhi dei costituenti fossero rivolti più al passato che all'avvenire»<sup>14</sup>.

<sup>13</sup> A. BARBERA, *Sub art. 2*, in G. BRANCA (a cura di) *Commentario della Costituzione*, Bologna, Zanichelli editore, Roma, 1975.

<sup>14</sup> A. BARBERA, *op. cit.*, p. 53.



L'evidente lacuna della Costituzione del 1948 tuttavia non scalfisce la sua forza, insita in quella vitale capacità di assorbire e dare "tono costituzionale" alle esigenze che man mano si fanno largo nella società: e quando il processo di consapevolizzazione di questi interessi civili e sociali giunge ad effettiva maturazione, allora diventa possibile riconoscere copertura costituzionale anche a situazioni inizialmente escluse da considerazione.

Ciò nondimeno si ricorre a quei principi di rilievo costituzionale che, collocando il pieno sviluppo della persona umana al centro dei fini che devono essere perseguiti dai poteri pubblici e riconoscendo nonché garantendo i diritti inviolabili dell'uomo, possono consentire una lettura favorevolmente sistematica delle disposizioni costituzionali che, più o meno direttamente, appaiono collegate alla tutela della sfera della riservatezza. Si tratta, in primo luogo, delle disposizioni che garantiscono in modo inequivocabile specifiche sfere di libertà individuale dall'altrui ingerenza: l'inviolabilità della libertà personale (art. 13), intesa non soltanto dal punto di vista strettamente fisico-materiale ma anche come libertà morale; l'inviolabilità del domicilio (art. 14); l'inviolabilità della libertà e della segretezza della comunicazione (art. 15). Queste rappresentano tutte situazioni giuridiche soggettive di vantaggio che sono primaria e fondamentale specificazione del principio personalista posto dall'articolo 2 della Costituzione.

Possono altresì essere utilmente ricordati i casi in cui la Costituzione fa espresso riferimento a situazioni, rapporti e comunque ambiti di attività umane giuridicamente protetti da interferenze esterne. È questo il caso del diritto all'esercizio





privato del culto religioso (art. 19), la libertà di manifestazione del pensiero (art. 21), il diritto al nome (art. 22), l'inviolabilità del diritto di difesa (art. 24), i diritti della famiglia come società naturale (art. 29), il rispetto della persona umana nell'assoggettamento ai trattamenti sanitari obbligatori (art. 32).

Ma è specificamente l'articolo 2 Cost., nella sua accezione di clausola a "fattispecie aperta"<sup>15</sup>, a consentire al diritto alla riservatezza di trovare posto tra i diritti fondamentali della persona, in particolare nella sua accezione di vero e proprio diritto della personalità. Si tratta di una lettura ormai unanimemente condivisa in letteratura, e che deve la sua affermazione soprattutto grazie all'influenza che il già citato quadro giuridico sovranazionale ha progressivamente esercitato sul nostro ordinamento.

Invero, il recepimento delle indicazioni di provenienza internazionale deve il suo merito alle riflessioni condotte già negli anni '60-'70 da dottrina non propriamente costituzionalistica, bensì in gran parte civilistica (si pensi ad Auletta, De Cupis, Pugliese o Cataudella), ma senza dimenticare altresì il contributo della scuola penalistica (come Bricola, Vassalli o Mantovano). In quegli anni anche la giurisprudenza ha iniziato a dare voce all'esigenza di protezione della riservatezza.

Ed è stata proprio la Corte di Cassazione, nel 1975 (sulla scia anche di quanto detto dalla Corte cost. con la sent. n. 38/1973), a cogliere tutti questi segnali e ad imprimere una svolta fondamentale nel processo di "digestione" di questa nuova

<sup>15</sup> *Ibidem.*



esigenza di tutela da parte dell'ordinamento giuridico. Con la sent. n. 2129 del 1975, infatti, la Cassazione, nell'offrire tutela alla principessa Soraya dall'invasività dei fotografi scandalistici, ha fornito un'eccellente summa del diritto alla riservatezza, definendolo come la «tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori del domicilio domestico, non hanno per terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti».

E nel fare questo, la Suprema corte costruisce un sistema costituzionale di tutela della privacy, che nasce sì dai principi fondamentali contenuti negli artt. 2 e 3 Cost., ma che tange anche altre fattispecie che di volta in volta possono essere chiamate in causa, in virtù della loro naturale predisposizione a proteggere la persona umana e a promuoverne lo sviluppo: si pensi, oltre ai citati artt. 14 e 15 Cost., all'art. 13 che è alla base dell'habeas corpus, all'art. 29 come cuore della tutela dell'intimità familiare, o all'art. 41 che si occupa della persona nella sua attività professionale e imprenditoriale.

È questa la chiave di volta che la dottrina costituzionalistica ha infine accettato e poi utilizzato per giungere ad una più compiuta elaborazione scientifica – benché nella diversità delle sensibilità mostrate e delle sfaccettature cui si è dato risalto (tra i tanti, si pensi a Pace, Modugno, Salerno, Baldassarre, Cerri). E cioè la constatazione che la riservatezza, per utilizzare un concetto coniato dalla Corte suprema Usa, vive nella “penombra” delle disposizioni costituzionali, in grado di



interessare la Costituzione come sistema di tutela dei diritti fondato sulla centralità della persona umana.

In questo percorso si è inserita anche la Corte costituzionale. Dopo il citato pronunciamento del 1973, sarà poi la n. 139/1990, a riconoscere come «i principi a tutela della privacy individuale (...) sono diffusi, pressoché in forma analoga, in tutti gli ordinamenti giuridici delle nazioni più civili». Successivamente il giudice delle leggi ha fornito anch'esso una lettura del diritto alla riservatezza quale diritto ad uno spazio vitale libero da interferenze sgradite, in connessione con altre fattispecie costituzionali: in particolare, con la segretezza delle conversazioni private (sentt. n. 366/1991 e n. 81/1993 sulle intercettazioni telefoniche) e con l'inviolabilità del domicilio (sent. n. 135/2002 sulla videosorveglianza), andando così oltre la Corte di Cassazione nel caso Soraya e trasformando la privacy da diritto di pochi a diritto di tutti<sup>16</sup>.

<sup>16</sup> *A latere* si segnala che un ultimo e più recente contributo, ancorché più enigmatico, da parte della giurisprudenza costituzionale è giunto con la celebre sent. n. 1/2013 – mediante la quale la Consulta ha dato ragione al Presidente Napolitano nel conflitto con la Procura di Palermo sulle intercettazioni che lo riguardavano. In un *obiter dictum* si cita tra i «valori e diritti di rilievo costituzionale» la «tutela della riservatezza su dati sensibili». Non è chiaro come debba essere letto questo passaggio, poiché è inserito all'interno di un ragionamento che si occupa di altro (cioè la riservatezza "speciale" da riconoscere al Presidente della Repubblica al fine dell'esercizio delle funzioni che la Costituzione gli attribuisce), e anche perché non viene debitamente approfondito. Tuttavia, si potrebbe presagire che la Corte ha inteso lasciare in sospenso il discorso, lanciando un sasso nella discussione e rinviando a data da destinarsi una sua più compiuta elaborazione, la quale senza dubbio dovrebbe condurre a ragionare sulla tutela del dato personale in sé e non solo del dato sensibile ovvero sia quello riconducibili a stati di salute o all'espressione di orientamenti politici, sessuali o ideologici. Evidenzia



Quanto descritto finora, tuttavia, si riferisce all'idea di privacy considerata come mera riservatezza, ossia della tutela della sfera privata della persona, nell'ambito di quella che si è definita "dimensione socio-relazionale". Tuttavia non si deve dimenticare quanto affermato in premessa, ovvero che essa rileva anche sul piano della protezione dei dati personali. Così come inequivocabilmente affermato dalle carte internazionali e dalla nota disciplina interna di settore, l'articolo 2 del Codice privacy, quale precipitato legislativo finale di tale cornice di garanzia. E della piena compatibilità di questo testo normativo con il dettato costituzionale ne è certa pure la Corte costituzionale che, con la sent. n. 271/2005, in primo luogo ha riconosciuto la (legittima) discendenza comunitaria dell'atto in questione; in secondo luogo ne ha ascritto la competenza alla potestà legislativa esclusiva dello Stato (perlopiù attraverso la voce "ordinamento civile").

È la giurisprudenza costituzionale a non aver ancora compiuto quell'equazione che, al contrario, si rinviene, sulla scorta delle sollecitazioni comunitarie, all'interno del citato articolo 1 del Codice della privacy. Nella società dell'informazione l'enorme mole di dati personali che vengono quotidianamente diffusi e scambiati fa sì che si debba giungere a parlare di vero e proprio diritto alla protezione dei dati personali come strumentale alla tutela della riservatezza. Un'equazione che a livello europeo, come si vedrà a breve, è

questo passaggio M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parlamentari e di politica costituzionale*, n. 176/2012 in corso di pubblicazione.



stata stabilita da lungo tempo e ha trovato codificazione all'interno dell'articolo 8 della Carta dei diritti fondamentali dell'UE.

## 2. Il quadro europeo in tema di riservatezza e protezione dati

La disciplina della riservatezza in ambito europeo ci aiuta a chiarire alcune necessarie distinzioni concettuali, solo in parte già anticipate. In primo luogo occorre specificare che il modello europeo di tutela della riservatezza si distingue da quello degli Stati Uniti, cui si deve l'originaria affermazione del termine "privacy"<sup>17</sup>.

In questo senso – è ormai noto ma vale la pena rimarcarlo – il concetto di "privacy" e quello di "riservatezza" non sono tra loro perfettamente sovrapponibili e non rappresentano due termini tra loro interscambiabili. La privacy nell'accezione americana ha rappresentato il perno giuridico intorno al quale la Corte suprema statunitense ha costruito una tutela dell'autodeterminazione individuale che travalica il concetto della riservatezza tout court per diventare condizione di libertà nelle scelte di vita personali ed intime<sup>18</sup>. È cosa risaputa che l'aborto sia stato ammesso per la donna in virtù dei privacy rights nella storica sentenza *Roe v. Wade* del 1973, ma

<sup>17</sup> S. BRANDEIS, L. WARREN, *The right to privacy*, in 4 *Harvard Law Review* 193, 1890.

<sup>18</sup> G. TIBERI, *op. cit.*, p. 350.



analogo ragionamento è valso per l'uso di materiale pornografico o il rifiuto di trattamenti sanitari obbligatori<sup>19</sup>.

Come si è detto, nella tradizione costituzionale europea la riservatezza nasce prima di tutto come possibilità per l'individuo di preservare una particolare sfera intima e personale, proteggendo i propri fatti privati dalla divulgazione o, comunque, di scegliere modi e tempi di una certa diffusione. In altre parole una sorta di diritto al riserbo. Per altro verso in particolare a causa dell'evoluzione tecnologica e della crescente informatizzazione dei rapporti autorità pubblica-cittadino stanno ulteriormente allontanando il modello statunitense da quello europeo. L'affermazione di un «diritto alla protezione dei dati personali» si pone in maniera conflittuale – se non addirittura antitetica – rispetto alla concezione americana di privacy, secondo la quale il dato personale è patrimonio della persona e il suo uso è sindacabile solo nel caso in cui esso abbia provocato dei danni<sup>20</sup>. Sono stati, tra le altre cose, esemplificativi delle differenze interpretative tra tradizione americana ed europea in tema di privacy e tutela dei dati personali i casi noti come PNR e Swift, frutto dell'iniziativa unilaterale delle autorità USA nell'ambito della lotta al terrorismo internazionale<sup>21</sup>.

<sup>19</sup> LEVINSON, *Privacy*, in K. HALL, J. ELY, J. GROSSMAN (edited by), *The Oxford Companion to the Supreme Court of the United States*, Oxford- New York, Oxford University Press, (2<sup>nd</sup> ed.), 2005.

<sup>20</sup> G. TIBERI, *op. cit.*, p. 350.

<sup>21</sup> In generale sul caso cfr. F. CLEMENTI, G. TIBERI, *Sicurezza interna, diritti e cooperazione internazionale nella lotta al terrorismo: i casi PNR e Swift*, in *Astrid online*, 2013.



Proprio sull'evoluzione e specificazione della tutela della riservatezza in tutela dei dati personali si trova, al contrario, la principale e specifica novità della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza). All'articolo 8, difatti, si stabilisce che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano; i dati dovranno essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. È altresì previsto per ciascuno il diritto di accesso ai dati che lo riguardano e che sono stati raccolti, nonché un "diritto alla rettifica". Si tutela, dunque, separatamente rispetto al diritto alla vita familiare (che invece la Carta di Nizza colloca all'articolo 7), la tutela dei dati personali come diritto fondamentale.

Volendo tralasciare la distinzione tra diritto "costruito" e non "riconosciuto"<sup>22</sup>, la rilevanza del data protection è prima di tutto frutto della necessità di armonizzare le differenti discipline statali affermatesi sin dai primi anni settanta (si trattò di una prima "stagione" a cui presero parte Svezia, Germania, Austria, Danimarca, Norvegia, Islanda e Lussemburgo)<sup>23</sup>. Da qui è nata, con ritardo rispetto a molti ordinamenti statali, l'esigenza di adottare la direttiva 95/46/CE del 1995 relativa al trattamento dei dati personali e alla loro libera circolazione. Ad essa sono poi seguite la direttiva 97/66/CE (sul trattamento dei dati personali e tutela della vita privata nel settore delle telecomunicazioni), la direttiva 2002/58/CE (sul trattamento dei

<sup>22</sup> Cfr. D. CALDIROLA, *Il diritto alla riservatezza*, Cedam, Padova, 2006.

<sup>23</sup> G. GARDINI, *op. cit.*, p. 245.



dati personali nel settore delle comunicazioni elettroniche) e le più recenti direttive 2009/136/EC (in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche) e 2009/140/C (in materia di reti e servizi di comunicazione elettronica).

Peraltro, se nella direttiva “madre” la tutela dei dati è ancora, in ultima analisi, funzionale al perseguimento di finalità economiche sottese all’insieme dell’ordinamento comunitario, la svolta della Carta di Nizza sta nella previsione della tutela del diritto in sé e per sé. In ragione di ciò, sarà significativo vedere come questi aspetti verranno ad essere evidenziati dalla Corte di Giustizia dopo che il Trattato di Lisbona ha introdotto il principio della giuridicizzazione della Carta di Nizza.

Un intervento che, come suggerito dalle Spiegazioni relative alla Carta (2007/C 303/02), è stato fondato sulle seguenti disposizioni normative: sulla direttiva 95/46/CE, sull’articolo 286 (ora articolo 16 del Trattato sul Funzionamento dell’Unione europea), sull’articolo 8 della Cedu e sulla Convenzione del Consiglio d’Europa sulla protezione dei dati personali nei trattamenti automatizzati (108/1981).

In ambito Cedu, occorre sottolineare come l’articolo 8 della Convenzione tuteli un insieme complesso di distinte sfere dell’autonomia personale: la vita privata, la vita familiare, il domicilio e la corrispondenza. In via generale i giudici di Strasburgo hanno ritenuto che queste sfere, per quanto distinte, non siano tra loro reciprocamente escludenti. Nello specifico, dunque, in materia di dati personali il Consiglio d’Europa si è mosso in un primo momento ritenendo insufficiente l’articolo 8 della Convenzione a tutelare nello specifico gli individui a



fronte dei rischi posti dalla tecnologia informatica, concependo ben presto una Convenzione ad hoc, la numero 108 del 1981 per la «protezione degli individui rispetto al trattamento automatizzato dei dati personali». La protezione dei dati personali nell'ordinamento Cedu, dunque, è frutto dell'interpretazione dell'articolo 8 della Carta alla luce della Convenzione del 1981. Quest'ultima, per quanto ancora molto sbilanciata sul lato della libertà di informazione, è stata a livello europeo uno dei primissimi tentativi di fornire un «minimo comune denominatore» nel data protection in Europa, un livello basilare di tutela del dato personale poi mutuato a livello comunitario<sup>24</sup>.

Si rinviene, ad ogni modo, una relazione stretta tra tutela della vita privata e protezione dei dati personali nella stessa giurisprudenza della Corte Edu, con la quale riconosce la tutela dei dati personali come ulteriori fattispecie tutelata dall'articolo 8 della Cedu (Leander c. Svezia del 26 marzo 1987; Z. c. Finlandia del 25 febbraio 1997; Amman c. Svizzera del 16 febbraio 2000).

In linea con la ragion d'essere della stessa Corte di Strasburgo chiamata ad esprimersi in materia di diritti fondamentali, la tutela dei dati personali emerge dalla giurisprudenza Cedu prima di tutto come tutela dei diritti degli individui da ingerenze eccessive da parte di soggetti privati e pubblici nella sfera dell'autonomia personale<sup>25</sup>.

<sup>24</sup> G. TIBERI, *op. cit.* pp. 360 ss.

<sup>25</sup> *Ibidem.*



Sul versante del diritto dell'Unione europea, la prospettiva della Corte di Lussemburgo è, almeno in origine, differente, poiché si innesta prima di tutto sul principio della libera circolazione dei dati personali, alla luce del principio della libera circolazione di merci, beni e servizi tutelata dal Trattato Cee. Solo successivamente – e comunque anche prima dell'adozione della direttiva madre – i giudici comunitari gettano le basi per mutuare la giurisprudenza della Cedu sulla protezione dei dati fino ad arrivare alle due significative sentenze del 2003, in cui alla fine si accoglie appieno la concezione di tutela dei dati così come interpretata dalla Corte di Strasburgo (Causa Rundfunk del 20 maggio 2003 e Lindquist del 6 novembre 2003), pur riservandosi i giudici comunitari di sindacare anche sulle interpretazioni della direttiva madre in potenziale contrasto con l'articolo 8 della Cedu. Peraltro da questo punto di vista interessanti saranno gli sviluppi a cui si potrà assistere a seguito di due fondamentali novità introdotte dal Trattato di Lisbona e agli effetti che queste potrebbero sortire nella giurisprudenza italiana ed europea: la giuridicizzazione della Carta di Nizza, da un lato, e l'adesione dell'UE al sistema convenzionale Cedu, dall'altro.

### **3. La sicurezza come fine e la riservatezza come (ostacolo nel) mezzo**

Pasquale Costanzo all'interno del volume "Videosorveglianza e privacy" scrive: «Le nuove tecnologie dell'informazione e della comunicazione hanno invaso la nostra vita per il meglio come per il peggio. [omissis] Sta però di fatto che ciascuno di noi, a meno che non viva in territori deserti o



isolati, ogni giorno è, come si dice in gergo, tracciato decine di volte»<sup>26</sup>. Il progredire della tecnologia e le emergenze che in determinati momenti storici possono verificarsi sono fattori che incrementano la richiesta di sicurezza ma al contempo i rischi nella tutela della riservatezza. È quindi corretto domandarsi se per perseguire efficacemente le politiche di sicurezza, pubblica e nazionale, debba essere sempre e comunque necessario restringere lo spazio dei diritti di libertà. In altre parole, quella tra privacy e sicurezza deve essere sempre una relazione inversamente proporzionale per cui più sicurezza equivale a meno privacy?<sup>27</sup> O non è piuttosto superata una visione che vede la tutela della riservatezza come ostacolo alla sicurezza? Attraverso alcuni esempi pratici sottoposti all'esame del Garante, si cercherà di argomentare che un bilanciamento – e non un gioco a somma zero – nella maggior parte dei casi è possibile, sia quando il bene primario da tutelare è la sicurezza, sia quando, al contrario, le maggiori preoccupazioni sono rivolte alla tutela della riservatezza. Al fondo di entrambe le questioni è innegabile che vi sia il fine ultimo della tutela dell'individuo e della sua sfera personale.



<sup>26</sup> P. COSTANZO, *Videosorveglianza e internet*, in M. MANETTI, R. BORRELLO (a cura di), *Videosorveglianza e privacy*, Angelo Pontecorboli editore, Firenze, 2010.

<sup>27</sup> G. BUTTARELLI, *La cooperazione fra i servizi di intelligence*, in G. AMATO, E. PACIOTTI (a cura di), *Verso l'Europa dei diritti*, il Mulino, Bologna, 2005, p. 176.



### 3.1 La videosorveglianza a fini di tutela della sicurezza urbana

Il fenomeno della videosorveglianza presenta degli ambiti di applicazione molto vasti ed eterogenei. Pur in questa eterogeneità, essi sono riconducibili primariamente a due finalità: da un lato, la sicurezza pubblica e urbana nonché la prevenzione e controllo di fenomeni criminosi e vandalici sia in ambito pubblico (piazze, strade, luoghi pubblici) che privato (condomini e aree comuni); dall'altro, l'incolumità del personale in ambito lavorativo e la protezione del patrimonio aziendale.

Per questi motivi, quando si affronta il tema della videosorveglianza occorre essere consapevoli del fatto che esso si intreccia con una serie di altri ambiti di intervento normativo quali le norme in materia di sicurezza pubblica e urbana, con particolare riferimento alle politiche degli enti locali, la legislazione giuslavoristica, la disciplina dei condomini (peraltro da poco aggiornata dalla legge 220/2012 con nuove norme proprio sui sistemi di videosorveglianza, art. 7 che inserisce il nuovo 1122-ter nel codice civile) e, infine, le norme in materia di protezione dei dati personali.

Difatti, per quanto appaia ormai come un elemento acquisito e scontato, è bene ricordare che le immagini tracciate attraverso le apparecchiature di registrazione sono pienamente qualificabili come dati personali, dal momento che rendono possibile l'identificazione dei singoli individui. Come il Garante ha avuto modo di chiarire all'interno del suo provvedimento generale: «la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (art. 4, comma 1, lett. b), del Codice). È considerato



dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione»<sup>28</sup>.

Il provvedimento appena citato è stato adottato nell'aprile 2010 dall'Autorità Garante per far fronte alle rilevanti modifiche normative apportate dal cd. "pacchetto sicurezza" del Governo Berlusconi. Tra le misure del "pacchetto sicurezza" approvate dal Governo Berlusconi rilevano, ai nostri fini, quelle che prevedono la possibilità (indirettamente nel primo caso, direttamente nel secondo) per i sindaci dei comuni di installare sistemi di videosorveglianza per le finalità di tutela della sicurezza urbana: l'articolo 6 del decreto legge n. 92 del 2008 (conv. con modificazioni dalla legge 125 del 2008) e l'articolo 6, comma 7 del decreto legge n. 11 del 2009 (conv. con modificazioni dalla legge 38 del 2009). Disposizioni queste<sup>29</sup> che rinviano al concetto di sicurezza urbana, la cui definizione è stata poi esplicitata all'interno di un decreto del Ministero dell'interno (D. M. 5 agosto 2008)<sup>30</sup>. Tale decreto ha definito la sicurezza urbana come «un bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le



<sup>28</sup> Punto 2, Provvedimento generale dell'8 aprile 2010, pubb. In G.U. n. 99 del 29 aprile 2010, doc. web n. 1712680.

<sup>29</sup> La prima ha notoriamente modificato l'art. 54 del TUEL in materia di ordinanze contingibili e urgenti dei sindaci, disposizione poi dichiarata illegittima dalla Corte costituzionale nella sentenza 115/2011.

<sup>30</sup> Cfr. in generale A. PAJNO (a cura di), *La sicurezza urbana*, Maggioli, Sant'Arcangelo di Romagna, 2010.



condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.».

Per altro verso è fuori discussione che il trattamento di dati personali effettuato da un soggetto istituzionale tramite un sistema di videosorveglianza deve evidentemente sottostare ai principi di liceità, necessità, proporzionalità e finalità<sup>31</sup>, tutti già rinvenibili peraltro nella intelaiatura stessa del Codice privacy.

Sebbene non obbligatoria per i Comuni che impiegano videosorveglianza a tutela della sicurezza urbana, il Garante comunque ha sottolineato l'importanza di rendere l'informativa<sup>32</sup>; per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione dei dati è di sette giorni, eventualmente estendibili, a fronte delle 24 ore concesse agli altri soggetti. Permangono invece gli obblighi in capo a tutti i soggetti, pubblici e privati, quali la verifica preliminare<sup>33</sup>, l'autorizzazione del Garante (nel caso di trattamento dei dati sensibili) e la notificazione al Garante (per le attività di cui all'art. 37 del Codice privacy).

<sup>31</sup> A. FROSINI, *La disciplina generale della videosorveglianza nell'ordinamento italiano*, in M. MANETTI, R. BORRELLO (a cura di), *op. cit.*

<sup>32</sup> Punto 5.1, Provvedimento generale dell'8 aprile 2010, pubb. In G.U. n. 99 del 29 aprile 2010, doc. web n. 1712680.

<sup>33</sup> Indispensabile in tutti i casi in cui i trattamenti tramite videosorveglianza comportano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare ai sensi dell'art. 17 del Codice.



Al giorno d'oggi si può constatare la realizzazione di una connessione tra piattaforme tecnologiche differenti in grado di realizzare una interoperabilità tra vari sistemi. Uno di questi esempi di interoperabilità è rappresentato dalla cd. "videosorveglianza intelligente". Si tratta di sistemi che non si limitano a captare delle immagini ma in qualche modo le classificano, segnalando eventi ritenuti "anomali", individuati tramite la corrispondenza a dei parametri inseriti in un software (il tutto tramite degli algoritmi). Non di rado poi questi sistemi sono anche connessi tramite la rete ad altre banche dati.

Descritto lo scenario, si passi ora all'analisi del caso di specie. A tal fine risulta utile analizzare un caso molto particolare, qualche tempo fa all'attenzione del Garante: una istanza di verifica preliminare relativa proprio a un sistema di videosorveglianza intelligente in un centro urbano.

Il sistema è costituito da una serie di videocamere fisse che, al verificarsi di un comportamento anomalo, fanno scattare un allarme ottico/acustico sul monitor installato nella control room, situata presso la centrale operativa della polizia locale. L'allarme ha lo scopo di attirare l'attenzione dell'operatore di polizia locale, che provvede a verificare la bontà del segnale e valuta le opportune azioni da intraprendere. L'"evento anomalo" in grado di attivare la spia consiste nella sosta prolungata di uno o più soggetti presso una certa area, che è virtualmente delimitata da una linea di interdizione. Gli obiettivi così virtualmente perimetrati sono monumenti (in passato già colpiti da atti vandalici o occupazioni abusive), e sedi istituzionali. Nella richiesta di verifica preliminare è



specificato che la registrazione delle immagini, riguardante una superficie limitata, si attiva in caso di permanenza prolungata, ovvero sia oltre un certo numero prestabilito di secondi (a seconda dei siti controllati 30 o 60 secondi). Un sistema di questo tipo intuitivamente presenta due possibili criticità in relazione alla tutela, da un lato, della libertà di circolazione degli individui e, dall'altro, alla sfera di riservatezza dei passanti (occorre precisare che già era installato un sistema di videosorveglianza tradizionale). Quello che il Garante si è pertanto chiesto è così riassumibile: un sistema del genere limita la libera scelta di ammirare, per tutto il tempo che si vuole, una fontana monumentale o un palazzo d'epoca in piena notte, nel silenzio della città e senza traffico e turisti? Vi è o meno un'invasione della sfera intima e personale del soggetto che decide di sostare dinanzi a un monumento?

In tal senso è stato di aiuto un precedente deciso dal Garante il 7 aprile 2011 e relativo a un sistema, molto simile, di videosorveglianza intelligente della Fontana del Nettuno in Piazza della Signoria a Firenze<sup>34</sup>. Alla luce di ciò, il sistema sopra descritto è stato ritenuto proporzionato, e quindi ammissibile, in considerazione delle finalità istituzionali di sicurezza urbana, alla luce della dichiarata inadeguatezza delle misure alternative di controllo (perlopiù a causa della scarsità di personale e dei numerosi atti vandalici già avvenuti).

Il Garante, dunque, ha ritenuto che si potesse dare risposta positiva alla verifica preliminare per una serie di ragioni. La prima di queste è che la permanenza prolungata dei soggetti

<sup>34</sup> Doc. web n. 1811897, provvedimento n. 140 del 7 aprile 2011.



presso i luoghi indicati conduce solo ad un richiamo all'operatore situato presso la control room, senza che siano automaticamente attivate altre funzionalità né interventi da parte di forze di polizia. Rimane dunque inalterato un passaggio "cognitivo" di tipo umano: è l'operatore, preallertato dal segnale, a verificare la situazione nel monitor e a ponderare di volta in volta cosa fare. In secondo luogo sono del tutto escluse funzioni quali la capacità di rilevare i percorsi, l'analisi audio, la geolocalizzazione, il riconoscimento tramite incrocio con altri dati o confronto con campioni di dati così come ulteriori funzionalità eventualmente legate al comportamento dell'interessato ripreso.

In altre parole, si è cercato un bilanciamento che tenesse conto sia della tutela di libertà fondamentali come quella di circolazione, sia delle necessità oggettive di incremento dell'efficacia dell'azione di controllo territoriale da parte di un soggetto istituzionale. Si è quindi affermato che, sulla base degli elementi acquisiti, «questo tipo di trattamento non comporta, in concreto, un pregiudizio rilevante per l'interessato, idoneo a determinare effetti particolarmente invasivi sulla sua sfera di autodeterminazione e, più in generale, sui suoi diritti e libertà fondamentali.» Le caratteristiche specifiche del sistema in esame, infatti, nel rilevare la presenza prolungata dell'interessato nell'area adiacente determinati siti monumentali e sedi istituzionali puntualmente segnalati, producono l'effetto esclusivo di richiamare l'attenzione dell'operatore di polizia locale addetto alla centrale operativa, al fine di favorirne un eventuale tempestivo intervento.



Il Garante, inteso sia come Collegio che come Ufficio, ha saputo collocarsi come tutore dei diritti dei cittadini, senza chiudersi su posizioni anacronistiche rispetto a possibili nuove applicazioni della tecnologia a servizio di quegli stessi cittadini.

### 3.2 Il trattamento di dati biometrici a fini di sicurezza

L'articolo 4 del Codice privacy (comma 1, lettera c), definisce "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato. L'Autorità Garante ha chiaramente stabilito in più occasioni che la raccolta e la registrazione di impronte digitali e dei dati biometrici utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione sono a tutti gli effetti operazioni di trattamento di dati personali. Operazioni di identificazione sono solitamente connesse ad esigenze di tutela della sicurezza di luoghi, beni, persone o informazioni. Di norma le tecniche volte all'accertamento dell'identità personale e, quindi, al reperimento di dati identificativi, si basano sull'utilizzo delle password oppure su supporti materiali (badge, tessere elettroniche). Tuttavia questi strumenti possono essere facilmente "dimenticati", ceduti, sottratti, smarriti o contraffatti, offrendo così un minor grado di certezza e affidabilità rispetto ad altre tecniche quali quelle biometriche, che, basandosi su caratteristiche del corpo o comportamentali di un individuo, non sono riproducibili e rimangono nell'esclusiva disponibilità dell'interessato.

Questo tipo di dati è funzionale a consentire all'individuo, una volta identificato, l'accesso a sistemi informativi e banche dati (accesso logico), oppure a luoghi specifici ad ingresso



ristretto e controllato (accesso fisico) oppure svolge una funzione meramente facilitativa (abilitazione all'accesso di una biblioteca, una palestra).

Soprattutto nei casi di cd. "accesso logico" è interessante notare a latere come si sia in presenza di un'ulteriore possibile declinazione del binomio "privacy e sicurezza": infatti, ci si trova dinanzi ad una misura di sicurezza che utilizza dati personali (biometrici) per difendere altri dati personali contenuti nei sistemi informativi o nelle banche dati. Si veda in questo senso, in attuazione degli articoli da 33 a 36 del Codice privacy, il Disciplinare tecnico in materia di misure minime di sicurezza in relazione al sistema di autenticazione informatica.

In considerazione della peculiarità della biometria e della particolare invasività che questa tecnica comporta, è necessario stabilire delle misure di sicurezza per tutelare i dati conservati e trattati dal sistema biometrico. Questo deve avvenire tramite la conservazione in forma criptata e, ove possibile, su dispositivi personali (smart card) piuttosto che su dispositivi centralizzati<sup>35</sup>. Questi accorgimenti tecnici fanno sì che le caratteristiche biometriche di un individuo siano confrontabili con il modello registrato al momento del cd. enrollment (la registrazione). L'impronta una volta misurata viene "tradotta" in un template, criptata e conservata sulla card ad uso esclusivo dello stesso soggetto. Così facendo si evita la creazione di banche dati centralizzate e si riduce il rischio che i dati biometrici possano

<sup>35</sup> Gruppo Articolo 29, Parere WP193 sugli sviluppi nelle tecnologie biometriche adottato il 27 aprile 2012.



essere impiegati in contesti potenzialmente lesivi per l'interessato stesso (come per esempio il furto di identità).

Tra le tecnologie biometriche più diffuse si ricordano prima di tutto quelle cd. fisiche o statiche quali la geometria del reticolo venoso della mano, la lettura dell'iride, il riconoscimento facciale e vocale ma soprattutto la rilevazione di impronte digitali e la geometria della mano e delle dita. Le impronte digitali vengono rilevate tramite la registrazione della peculiare disposizione delle creste e delle valli cutanee presenti sui polpastrelli delle mani. Le caratteristiche delle impronte, come si anticipava, vengono tradotte in un template tramite degli algoritmi, in una maniera generalmente non reversibile. La geometria della mano, invece, si basa sulla rilevazione delle caratteristiche geometriche bidimensionali o tridimensionali della mano e delle dita. La principale differenza rispetto alle impronte digitali, consiste nel fatto che le caratteristiche della mano di un individuo non sono descrittive al punto da risultare univocamente associabili ad un unico soggetto e, di conseguenza, l'utilizzo di questa biometria è particolarmente utile per finalità di identificazione in comunità circoscritte e ristrette.

Dall'altro vi sono anche tecniche biometriche "comportamentali o dinamiche" ovverosia basate su valutazioni comportamentali dell'individuo come la firma (e la lettura grafometrica di essa), o l'emissione della voce. In questi casi appare naturalmente più elevato l'indice di rischio nel trattamento del dato personale, dal momento che dalle suddette caratteristiche dinamiche è più facile attivare una profilazione comportamentale dell'individuo.



Le tecnologie basate sull'elaborazione dei dati contenuti nel DNA, pur non rappresentando strettamente una forma di biometria, sono comunque ad essa assimilabili per il tipo di problematiche che sollevano<sup>36</sup>, con particolare riguardo in questo caso anche alla definizione di dati sensibili poiché idonei a rivelare l'origine razziale o lo stato di salute (si veda art. 4, comma 1 lettera d del Codice privacy).

I dati biometrici in generale sono dunque dati personali e per la loro stessa natura possono comportare notevoli rischi per la vita privata delle persone<sup>37</sup>.

Pertanto, tali dati possono essere oggetto di trattamento soltanto in presenza di una base giuridica e solo se il trattamento è adeguato, pertinente e non eccedente rispetto alle finalità per le quali vengono rilevati e/o successivamente trattati<sup>38</sup>.

In questo ambito la giurisprudenza Cedu si è concentrata più sulla conservazione dei dati biometrici, piuttosto che sul loro prelievo. Si ricorda in particolare la sentenza *Marper c. The United Kingdom* del 4 dicembre 2008 che ha dichiarato illegittima la normativa statale che consentiva l'illimitata conservazione dei dati di persone poi non condannate. I due accusati, poi assolti, avevano richiesto invano la distruzione



<sup>36</sup> Cfr. *Biometric-based technologies* Rapporto OCSE 28 aprile 2004.

<sup>37</sup> G. BUSIA, *La protezione dei dati personali*, in G. AMATO, E. PACIOTTI, *op. cit.*, p. 163.

<sup>38</sup> Gruppo Articolo 29, Parere WP80 adottato il 1 agosto 2003 e successivamente Parere WP193 sugli sviluppi nelle tecnologie biometriche adottato il 27 aprile 2012.



delle impronte digitali, dei campioni DNA e dei profili DNA acquisiti in relazione alle accuse. La Corte ha ritenuto sproporzionata l'ingerenza nella vita privata, non riscontrando il giusto equilibrio tra interessi pubblici e privati.

In Europa questo genere di trattamenti è difatti consentito in applicazione di precise disposizioni normative quali il regolamento istitutivo di Eurodac per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino in materia di asilo (CE n. 2725/2000 del Consiglio, dell'11 dicembre 2000), oppure il regolamento istitutivo del sistema di informazione VIS (regolamento CE n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti. Si tratta dunque di attività specifiche connesse fra loro nel quadro normativo complessivo volto al rafforzamento dello spazio di libertà, sicurezza e giustizia nell'Unione europea e nello specifico al Programma dell'Aia<sup>39</sup>.

A queste misure si può accostare la legge n. 85 del 2009 con la quale l'Italia ha ratificato il Trattato di Prum che ha incrementato la mole di informazioni anche basate su dati biometrici che possono essere scambiate tra le varie forze di polizia europee allo scopo di contrastare il terrorismo, la

<sup>39</sup> Cfr. in generale G. AMATO, E. PACIOTTI, *op. cit.*



criminalità transfrontaliera e la migrazione illegale e che ha istituito in Italia la banca dati nazionale del DNA<sup>40</sup>.

Nella giurisprudenza costituzionale italiana merita di essere menzionata la sentenza n. 238/1996 che ha dichiarato illegittima una norma del codice di procedura penale che consentiva il prelievo ematico coattivo, senza precisare i casi ed i modi in cui una misura del genere può essere adottata. In senso parzialmente differente la Corte di Cassazione che, al contrario, ha considerato prove ammissibili per l'accertamento del reato di guida in stato di ebbrezza i risultati di un prelievo ematico eseguito in una struttura pubblica di pronto soccorso, anche in assenza del consenso dell'interessato<sup>41</sup>.

Tuttavia non è sull'utilizzo di sistemi biometrici per finalità di contrasto al terrorismo, controllo dei traffici transfrontalieri, controllo dell'immigrazione e contrasto al crimine che qui ci si intende soffermare. Dall'osservatorio privilegiato dell'Autorità si registra sempre più frequentemente l'applicazione della biometria non per ragioni immediatamente riconducibili alle esigenze di sicurezza pubblica e di perseguimento dei reati bensì per motivazioni genericamente riconducibili alla sicurezza di beni, luoghi o persone: in altre parole, come si anticipava, si tratta di casi in cui si verifica l'applicazione della



<sup>40</sup> Cfr. in generale R. BORRELLO, *Il trattamento dei dati personali da parte delle forze di polizia*, in R. BORRELLO, A. FROSINI, M. MANETTI, *Attività delle forze di polizia e trattamento dei dati personali*, Maggioli, Sant'Arcangelo di Romagna, 2012.

<sup>41</sup> Corte di Cassazione IV Sez. pen. 16 maggio 2012, n. 26108.



biometria per la mera sostituzione di badge e tesserini elettronici.

Il Codice privacy riconosce la peculiarità dei dati biometrici e, soprattutto, vi ricollega dei rischi specifici per la tutela dei diritti fondamentali e per la dignità degli interessati. Per queste ragioni è stabilito che il trattamento di dati biometrici debba essere sottoposto a verifica preliminare da parte del Garante (artt. 17 e 55) e debba essere sempre obbligatoriamente notificato al Garante stesso (art. 37 e combinato disposto degli articoli 39 e 55), fatta eccezione per i casi in cui esso è impiegato in un sistema di autenticazione informatica, la quale costituisce, come si è visto, una misura minima di sicurezza (conformemente ai requisiti tecnici indicati dalle regole 1-11 dell'Allegato B) al Codice di cui all'art. 34, comma 1, lett. a)).

In considerazione della peculiarità di questi dati e visto l'impiego della biometria soprattutto in circostanze che coinvolgono gioco forza anche i lavoratori (si pensi alle aree aeroportuali oppure alle banche), l'Autorità Garante ha stabilito una serie di parametri per il loro utilizzo nell'ambito del lavoro privato<sup>42</sup> e pubblico<sup>43</sup>.

Accanto alle rilevanti implicazioni giuslavoristiche, resta fermo, ovviamente, anche che la conformità del trattamento biometrico alla disciplina di protezione dei dati deve essere

<sup>42</sup> 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, deliberazione del 23 novembre 2006, doc. web n. 1364939.

<sup>43</sup> Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, deliberazione del 14 giugno 2007, doc. web n. 1417809.



valutata tenendo presente sempre i principi di necessità, liceità e proporzionalità stabiliti dal Codice (artt. 3 e 11).

In ambito privato l'utilizzo di dati biometrici può essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili", in considerazione della natura delle attività che vi vengono svolte. Ci si riferisce, ad esempio, a processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore. In questa ottica il Garante ha ritenuto lecito l'impiego della biometria per l'accesso solo ad alcune aree riservate di un'azienda operante nel settore avionico ed elettronico<sup>44</sup>; oppure lecito è stato dichiarato l'uso della biometria per l'identificazione del personale nelle banche per l'accesso ristretto ad un'area particolare della sede per garantire sia la sicurezza del personale della direzione sia la riservatezza di documenti e fascicoli, nonché la protezione di alcune opere d'arte (15 giugno 2006)<sup>45</sup>. Ma, per esempio, si è ritenuta illecita la raccolta e l'utilizzo di impronte digitali dei clienti per l'accesso ad una palestra, nella misura in cui per fini di «natura essenzialmente amministrativa» l'impiego di mezzi meno invasivi come badge e schede elettroniche era certamente da preferire<sup>46</sup>.

<sup>44</sup> Doc. web n. 1202254, provvedimento del 23 novembre 2005.

<sup>45</sup> Doc. web n. 1306098, provvedimento del 15 giugno 2006.

<sup>46</sup> Doc. web n. 1894570, provvedimento del 16 febbraio 2012.



Analogamente in ambito pubblico la biometria può essere impiegata solo per particolari esigenze di controllo dell'accesso a speciali aree dei luoghi di lavoro in cui si debbano assicurare elevati e specifici livelli di sicurezza. Questo può avvenire, secondo le Linee guida, principalmente per due ordini di motivi: a) in aree dove vengono svolte attività con particolare carattere di segretezza, ovvero prestate da personale selezionato e impiegato in attività che comportano la necessità di trattare informazioni rigorosamente riservate (es. accesso a sale operative ove confluiscono segnalazioni afferenti alla sicurezza anticrimine; aree adibite ad attività inerenti alla difesa e alla sicurezza dello Stato; ambienti di torri di controllo aeroportuali); b) aree riservate alla conservazione di oggetti di particolare valore o la cui disponibilità deve essere ristretta ad un numero circoscritto di dipendenti in quanto un loro utilizzo improprio può determinare una grave e concreta situazione di rischio per la salute e l'incolumità degli stessi o di terzi (es. ambienti ove sono custodite sostanze stupefacenti o psicotrope).

Sulla base delle Linee guida e dei principi del Codice è stato ritenuto lecito l'impiego della geometria della mano per l'accesso alla sala operativa di una Sovraintendenza archeologica dove confluivano le segnalazioni afferenti alla sicurezza anticrimine ed antincendio dei siti archeologici di competenza della Amministrazione; ma, al contrario, non è stato ritenuto proporzionale e indispensabile, rispetto alle finalità dichiarate, un sistema di rilevazione delle impronte digitali installato da un'azienda di trasporto pubblico che aveva limitato in tal modo l'accesso ai locali dove erano custodite le banche dati aziendali. La decisione del Garante in questo caso



ha tenuto conto di due elementi. In primo luogo il fatto che i dati che risultano conservati si sostanziano in informazioni che solitamente sono trattate negli uffici amministrativi di qualsiasi azienda e, in secondo luogo, i soggetti pubblici (datori di lavoro in generale) che intendono verificare la presenza in servizio dei dipendenti tramite la biometria hanno mancato di dimostrare al Garante che le finalità di controllo non possano essere realizzate con sistemi meno invasivi, nel rispetto dei principi di necessità e di proporzionalità<sup>47</sup>.

Provando a riassumere, fino ad oggi i punti fermi nella prassi del Garante in merito al dato biometrico sono i seguenti: a) per giustificare l'utilizzo della biometria non sono sufficienti generiche esigenze di sicurezza, non adeguatamente motivate e suffragate; b) l'uso è consentito solo per accesso a ben delimitate aree all'interno di un luogo di lavoro più ampio, e comunque occorre sempre rapportare la finalità con il principio di proporzionalità del trattamento; c) il dato biometrico non è ammesso per finalità di controllo delle presenze dei lavoratori (a fini di controllo della condotta e per misurazione della retribuzione e degli straordinari), a meno che i datori di lavoro non dimostrino preventivamente che le finalità di controllo non possano essere realizzate con sistemi meno invasivi, nel rispetto dei principi di necessità e di proporzionalità.

Rispetto a questa impostazione viene in particolare rilievo un caso che recentemente il Garante ha analizzato e nel quale, in via del tutto eccezionale, si è deciso di discostarsi in parte dal suddetto orientamento, nel tentativo di ricercare un differente

<sup>47</sup> Doc. web n. 1779745 e n. 1779758, provvedimenti del 17 novembre 2010.



bilanciamento tra istanze di sicurezza più generali e tutela della sfera della riservatezza<sup>48</sup>.

La particolarità di questo caso consiste nel fatto che il sistema di rilevamento biometrico (si trattava di geometria della mano) era finalizzato a garantire la certa identificazione dei dipendenti, sia nel caso di quelli soggetti a misure alternative della pena sia nel caso dei cd. incensurati. Questo perché l'azienda in questione operava in una realtà difficile caratterizzata da un alto tasso di criminalità organizzata, con elevato rischio di infiltrazioni camorristiche. A ciò si aggiunga che un quarto del totale dei dipendenti era rappresentato da soggetti che fruivano di misure alternative alla detenzione, rispetto ai quali l'azienda è chiamata a comunicare a una molteplicità di soggetti ("Procura della Repubblica", "Tribunale", "Polizia di Stato"), su loro richiesta, informazioni certe e veritiere circa l'effettiva presenza in servizio.

Accanto a questo l'azienda ha anche fatto presente l'esigenza di eliminare il meccanismo basato sui badge e tesserini elettronici per evitare i casi di ritorsioni o intimidazioni nei confronti di alcuni dipendenti qualora questi non intendessero prestarsi ad eventuali pratiche fraudolente (scambio del badge per effettuare timbrature al posto dei colleghi di lavoro). Tali circostanze sono state appurate anche in occasione di tutta una serie di pronunce del giudice di primo grado che ha riconosciuto in questo caso la necessità di introdurre sistemi di controllo delle presenze più sicuri e affidabili di quelli basati su supporti elettronici.

<sup>48</sup> Doc. web n. 2354574, provvedimento del 10 gennaio 2013.



Quanto appena descritto rende l'idea della peculiarità del caso e ha perciò indotto il Garante a valutare, in deroga alle citate Linee guida del 23 novembre 2006, come necessario e proporzionato il trattamento dei dati della geometria della mano dei lavoratori; questo anche in ragione dell'effettiva necessità di una continua reperibilità degli interessati (in tal senso, Cass. 5 marzo 2003, n. 18140) e delle finalità perseguite dal titolare, ritenute lecite dalla giurisprudenza di merito che si era in precedenza pronunciata sulla medesima fattispecie.

In un passaggio significativo della giurisprudenza richiamata e, in qualche modo, fatta propria dal Garante come punto di partenza del proprio intervento «la teorica compromissione del diritto alla riservatezza [sarebbe] in ogni caso ridimensionata alla luce delle esigenze di ordine pubblico e sicurezza sul luogo di lavoro sottese all'impiego del sistema biometrico»<sup>49</sup>.

Sono stati molti i dubbi sollevati relativamente a questo aspetto. Ci si è interrogati sulla reale sussistenza e sul fondamento giuridico di un "obbligo di custodia" da parte del datore di lavoro sui dipendenti in regime di semi-libertà, dal momento che un preciso obbligo di legge in tal senso avrebbe potuto far propendere la decisione di bilanciamento a favore del datore di lavoro. In secondo luogo ci si è chiesti se fosse possibile perseguire le medesime finalità di controllo con modalità meno invasive della sfera personale. Quale è da questo punto di vista la reale efficacia del dato biometrico, considerato che quel tipo di sistema assicura la presenza del

<sup>49</sup> Trib. Napoli 21 aprile 2011, citato nel provvedimento.



lavoratore in quel determinato momento presso il sistema di rilevamento ma non è in grado di dare certezze in merito alla presenza del lavoratore nell'arco dell'intera giornata lavorativa?

In via del tutto derogatoria rispetto al proprio orientamento generale, il Garante ha limitato l'impiego del dato biometrico alle sole circostanze appena descritte, basandosi per l'appunto sull'interpretazione delle esigenze di tutela dell'ordine pubblico e di sicurezza del luogo di lavoro poste in particolare rilievo dalla giurisprudenza che già si era espressa sul caso.

In altre parole, si è trattato di una deroga ai suesposti principi generali in presenza di circostanze oggettive che imponevano un ribilanciamento a favore delle esigenze di sicurezza. Prova ne è che in un caso del gennaio 2013, relativo ad un comune in provincia di Napoli, che pure presentava alcune affinità con quanto appena descritto, il Garante ha confermato la sua precedente prassi, ritenendo illecito l'impiego di un sistema biometrico per il solo accertamento delle presenze dei lavoratori, una volta verificato che il comune non aveva neanche provato ad adottare misure di controllo meno invasive e più proporzionali<sup>50</sup>.

<sup>50</sup> Trattamento di dati biometrici per finalità di rilevazione delle presenze dei dipendenti: verifica preliminare richiesta dal Comune di Boscoreale doc. web n. 2304669, provvedimento del 31 gennaio 2013.



#### 4. La riservatezza come fine e la sicurezza come mezzo: alcune riflessioni incrociate su cybercrime, reati contro la privacy e "cyberbullismo"

La diffusione della tecnologia informatica, quel complesso "sistema di sistemi"<sup>51</sup> noto come *Information Communication Technology* (ICT), porta con sé dei problemi di rilevanza costituzionale a cui tuttora si cerca di dare risposta. La prima e forse più rilevante questione è fino a che punto sia possibile limitare la libertà di informazione esercitata tramite internet. Per rispondere a questa domanda occorre partire da una premessa: l'esercizio di un potere censorio sui contenuti e sui dati immessi in rete (ivi compresi quelli volti a creare una profilazione dell'interessato) incide sulla libertà di espressione che trova espresso riconoscimento e garanzia oltre che negli articoli 21 e 15 della Costituzione italiana, anche nella Cedu (art. 10) e nella Carta di Nizza (art. 11). È pacifico che la garanzia offerta da tali disposizioni trova piena applicazione anche con riguardo alla comunicazione a mezzo internet.

A fronte di ciò diviene sempre più importante il ruolo svolto dagli intermediari o *Internet Service Provider* (ISP) e crescenti sono gli interrogativi rispetto a una loro responsabilità sui

<sup>51</sup> F. PIZZETTI, *Dati e diritti nell'epoca della comunicazione elettronica*, in F. PIZZETTI (a cura di), *I diritti nella "rete" della rete*, Giappichelli, Torino, 2013, p. 7.



contenuti pubblicati o su un loro possibile ruolo di intermediazione<sup>52</sup>.

Sulla base di tali premesse non vi è dubbio che il blocco e la rimozione di contenuti caricati in rete anche da parte di un ISP costituisca una illegittima interferenza sulla libertà di informazione. D'altra parte l'esercizio di ogni diritto fondamentale trova un limite nell'esigenza di evitare illegittime interferenze su altri interessi meritevoli di tutela. Pertanto, anche la diffusione su internet di informazioni può essere limitata al fine di evitare la violazione del diritto d'autore, della tutela dei dati, dell'onore o della reputazione dei singoli. Interventi a tutela di questi diritti non devono essere lasciati al caso o a interventi dell'intermediario ma, al contrario, è necessario un intervento del legislatore nel tenere insieme in bilanciamento le differenti libertà. Molte e significative riflessioni – che in questa sede è solo possibile accennare – sono sollecitate in tema di bilanciamento tra diritto d'autore e tutela dei dati personali dal noto caso Peppermint, dal nome della casa discografica tedesca che chiese un ingente risarcimento danni a numerosi utenti che avevano condiviso file musicali nei siti *peer to peer*. In quell'occasione il Garante per la privacy assunse una posizione molto netta a favore della tutela dei dati degli utenti italiani, arrivando anche a costituirsi in giudizio dinanzi il Tribunale di Roma nella causa intentata dalla casa

<sup>52</sup> Cfr. M. VIGGIANO, *Internet e "privacy": immunità o responsabilità del "provider"? Un problema di diritto pubblico*, in A. PACE, R. ZACCARIA, G. DE MINICO (a cura di), *Mezzi di comunicazione e riservatezza*, Jovene, Napoli, 2008.



discografica tedesca e adottando un provvedimento di divieto nei confronti della stessa<sup>53</sup>.

Il rischio che nel “cyberspazio” possano configurarsi contenuti o comportamenti illeciti che necessitano di intervento da parte dell'autorità pubblica, aumenta a dismisura con i social network, i quali si distinguono per un'ampissima gestione individuale e autonoma nei contenuti, in grado di trasformare, a seconda delle circostanze, gli utenti tanto in autori quanto in vittime di comportamenti illeciti.

L'uso di reti informatiche per integrare fattispecie di reati definibili per l'appunto come reati informatici, reati cibernetici, o con il ben più noto termine *cybercrime* trova la principale disciplina sistematizzazione all'interno della Convenzione Consiglio d'Europa fatta a Budapest il 23 novembre 2001, ratificata dal nostro Paese tramite la legge 18 marzo 2008, n. 48, il cui articolo 10 peraltro ha modificato in termini sostanziali anche alcune disposizioni del Codice della privacy (articolo 132)<sup>54</sup>. Gli illeciti che rientrano nella Convenzione sono, a titolo esemplificativo, l'accesso illegale ad un sistema informatico, l'attentato all'integrità sia del sistema che dei dati, la frode informatica, nonché tutti i reati relativi alla pornografia infantile e quelli connessi alla proprietà intellettuale.

<sup>53</sup> *Peer-to-peer*: illecito “spiare” gli utenti che scambiano *file* musicali e giochi (Peppermint), provvedimento del 28 febbraio 2008, doc. *web* n. 1495246.

<sup>54</sup> Cfr. F. ERAMO, *L. n. 48/2008 sulla criminalità informatica. Aspetti generali e ricadute sulla tutela dei minori dalle insidie telematiche*, in *Famiglia e diritto*, n. 1/2009, pp. 93-103.



Non ancora pienamente organica appare, invece, la disciplina del *cybercrime* a livello comunitario, nonostante il fondamentale lavoro svolto dal Centro Europeo di Criminalità Informatica (EC3) all'interno di EUROPOL e dallo *European Network and Informatic Agency* (ENISA), entrambi nati con l'obiettivo di incrementare la cooperazione tra gli Stati membri su sicurezza delle reti e delle informazioni.

In generale comunque la tipologia di abusi sui diritti fondamentali che possono ritrovarsi in rete, e i cui rischi specifici aumentano in relazione all'uso dei social network, sono generalmente riconducibili a differenti beni giuridici o interessi penalmente protetti<sup>55</sup>. È dunque possibile tentare una classificazione che individui le seguenti tipologie: a) reati connessi alla diffusione e fruizione di materiale pedopornografico; b) ingiurie e diffamazioni, istigazione all'odio razziale, apologia di reati a danno dei minori; c) violazioni del diritto d'autore sulle opere protette; d) in generale tutte quelle fattispecie di illecito penale che possono configurarsi da parte di soggetti che utilizzano internet e i social network come strumento in sé di organizzazione e preparazione dell'illecito (terrorismo, prostituzione, traffici illeciti); e) violazioni della riservatezza e reati contro la privacy, furto o manipolazione di dati (*data diddling* e *data leakage*). A questi poi si potrebbe aggiungere la cd. "riservatezza informatica", ricondotta dal Tribunale costituzionale tedesco, nella rilevante e interessante sentenza del 27 febbraio 2008 BvR



<sup>55</sup> Cfr. sul tema L. PICOTTI, *Diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giurisprudenza di merito*, n. 12/2012, pp. 2522-2546.



370/0, tra i diritti della personalità. Questa ultimissima categoria di abusi sui diritti fondamentali rinvenibili in rete, consente di invertire l'ordine dei fattori fin qui seguito: se finora si sono analizzati casi in cui la sicurezza era l'interesse da tutelare anche a detrimento della riservatezza, ora si provi a invertire l'ordine dei fattori, ponendo la riservatezza e i dati personali al centro degli sforzi di tutela dell'ordinamento.

In relazione alle violazioni della privacy penalmente rilevanti, il nostro Codice prevede una specifica fattispecie, ovverosia il «delitto di trattamento illecito di dati personali» (art. 167).

A tal proposito ha destato grande scalpore la vicenda nota come "Google-Vivi down", connessa alla pubblicazione sul sito di condivisione Google Video di un video che ritraeva dei giovani bulli che vessavano un ragazzo disabile, mentre pronunciavano frasi ingiuriose nei confronti della loro vittima e nei confronti dell'Associazione Vivi Down. Non essendo possibile esaurire in questa sede l'analisi dei numerosi profili di interesse di tale vicenda, ci si limiterà a formulare delle considerazioni mirate sui profili di tutela della riservatezza.

Il Tribunale di primo grado<sup>56</sup> ha ravvisato una responsabilità di tipo penale proprio ai sensi dell'art. 167 del Codice della privacy in capo ai tre manager di Google Italia.

L'orientamento della sentenza di primo grado è stato tuttavia ribaltato nella sentenza d'appello<sup>57</sup>, nella quale i manager, condannati in primo grado, sono stati assolti perché

<sup>56</sup> Tribunale di Milano, 12 aprile 2010.

<sup>57</sup> Corte d'appello di Milano, dep. 27 febbraio 2013.



la Corte ha affermato che non è imputabile all'hoster o ISP "un potere/dovere di verifica preventiva" sui contenuti caricati dagli utenti: il dolo specifico richiesto dall'articolo 167 del Codice non è rinvenibile e, dunque, il fatto non sussiste.

Il caso presenta numerosi e sostanziali profili di rilevanza con riguardo alla tutela – rafforzata, trattandosi di minori – della protezione dei dati personali diffondibili online ma al tempo stesso ci permette di estendere il ragionamento alla tipologia di bene giuridico che occorre tutelare.

In questo caso più della riservatezza in sé e per sé vi è forse una questione di tutela della dignità della persona. In tale contesto il diritto all'onore, il diritto all'immagine, il diritto alla riservatezza e con esso quello alla protezione dei dati personali sono funzionali alla tutela della dignità della persona<sup>58</sup>. Tuttavia la principale debolezza della sentenza di primo grado sta proprio nel fatto che, in assenza di un quadro normativo in grado di enucleare le responsabilità in capo ai provider, la riservatezza e le norme sulla privacy sono state forzatamente impiegate per raggiungere il fine della dignità dell'individuo e della sua sicurezza.

Il caso appena illustrato ci permette di formulare alcune osservazioni supplementari sulle situazioni di potenziale pericolo per i minori che utilizzano internet e social network. La facilità con cui i minori al giorno d'oggi utilizzano questi strumenti è stupefacente, dal momento che per i più giovani, i

<sup>58</sup> M. TIMIANI, *Nello spazio (e al tempo) di internet, quale natura per il diritto alla privacy?*, su A. PEREZ MIRAS, G. TERUEL LOZANO, E. C. RAFFIOTTA (a cura di), *Nuevas exigencias de tutela de los derechos de la persona*, Aranzadi, Madrid, in corso di pubblicazione.



cosiddetti «nativi digitali», la rete non è solo uno strumento di lavoro o di svago bensì è «parte dell'ambiente» dove si ritrovano fin dalla nascita<sup>59</sup>.

Un minore che naviga online si espone facilmente ad abusi e, al tempo stesso, può diventare egli stesso autore di abusi e illeciti. Nel primo caso si pensi alla fattispecie della diffusione di contenuti illegali (pedopornografia) o pericolosi per i bambini (videogiochi violenti) oppure al desolante fenomeno del *grooming*, l'adescamento dei minori attraverso la rete<sup>60</sup>. Alcune di queste fattispecie di reato sono contemplate all'interno della già citata Convenzione di Budapest, altre hanno trovato adeguata disciplina in Italia, in primis nella legge 6 febbraio 2006, n. 38 recante Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet. Altro passo importante è stata la ratifica della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, sottoscritta a Lanzarote il 25 ottobre 2007, (legge 1 ottobre 2012, n. 172) così come di grande rilievo la recente direttiva 2011/92/UE sulla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile.

Tuttavia, al tempo stesso i minori una volta avuto accesso facile al mondo digitale e alla possibilità di condividere contenuti sulla rete, possono trasporre essi stessi condotte

<sup>59</sup> S. CALZOLAIO, *Internet e minori. Rassegna tematica per una indagine giuridica*, in *La tutela dei minori di fronte ai "media"*, Quaderni del Co.re.com. Emilia-Romagna, Bologna, 2012, p. 105.

<sup>60</sup> Cfr. L. MUSSELLI, *Internet e minori*, in *Dir. Informatica*, n. 6/2011, pp. 727 ss.



lesive della dignità altrui dal mondo reale allo spazio virtuale, come nel caso del cd. "cyberbullismo" o "bullismo hi-tech". Questo nuovo tipo di bullismo, contrariamente a quanto si sarebbe portati a pensare, è in realtà molto più invasivo del suo analogo nel mondo reale: la persecuzione della vittima è continua e neanche le mura di casa rappresentano più un luogo sicuro. La vittima di cyberbullismo è continuamente perseguitata tramite l'invio di sms minacciosi, di e-mail offensive e minacciose, coperte dalla vergogna generata dalla pubblicazione di fotografie personali, da commenti volgari ed offensivi in rete, da forum di discussione e da altri episodi simili.

Il cyberbullismo, al pari del bullismo tout court, non trova attualmente una disciplina specifica all'interno dell'ordinamento italiano. Ciò nonostante su questo fenomeno l'attenzione del Garante è stata sempre molto elevata, e si è concretizzata per il momento in interventi che si potrebbero definire di moral suasion e sensibilizzazione su un uso responsabile dei social network, così come in ambito scolastico il Garante ha fatto sempre ben presente che la diffusione di immagini video e foto tramite smartphone e tablet è possibile solo con il consenso dell'interessato.

Di tutti questi sforzi ne è testimonianza, da ultimo, la lettera che il Presidente Soro ha inviato in occasione della Giornata europea della protezione dei dati personali 2013 al Ministro dell'Istruzione per avviare delle iniziative comuni a riguardo.

Spesso il cyberbullismo genera dei problemi di tutela della riservatezza in relazione alla diffusione che di questi eventi viene fatta sulla stampa, tirando in causa così le norme che



disciplinano la tutela del minore e dei suoi dati personali in potenziale conflitto con il diritto di cronaca. Il Codice della privacy e il codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (allegato A1 al Codice privacy) pongono delle chiare garanzie a tutela dei minori. Il codice di deontologia all'articolo 7 stabilisce che il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca e che l'eventuale pubblicazione di notizie e immagini relative a minori dovrà avvenire secondo i principi e i limiti stabiliti dalla "Carta di Treviso". Trattasi di uno strumento di autoregolamentazione adottato dall'Ordine dei giornalisti e dalla Federazione Nazionale Stampa Italiana e che è stato recentemente aggiornato con riguardo a internet e al giornalismo on line e multimediale<sup>61</sup>.

L'Autorità Garante è dunque spesso intervenuta nei confronti dei mezzi di informazione per riaffermare le norme a tutela delle garanzie per i minori sopra descritte. Per citare un esempio tanto triste quanto significativo: nel febbraio 2010 molti quotidiani on line e organi di informazione vari pubblicarono la notizia di un gruppo su Facebook chiamato "Giochiamo al bersaglio con i bambini down", a cui era associata la foto di un neonato sulla cui fronte, tramite fotoritocco, era scritta un'offesa. L'Autorità ha immediatamente ricordato alle testate giornalistiche l'obbligo di rispettare in



<sup>61</sup> L'aggiornamento è stato formalizzato dalla delibera del Garante della Privacy, Doc. web n. 1357821, delibera n. 49 del 26 ottobre 2006.



particolare il principio dell'essenzialità dell'informazione (art. 137 del Codice), nonché tutti gli obblighi presenti nel codice di deontologia a tutela dei minori e ha, infine, richiamato tutte le testate a prestare particolare attenzione nel prelevare informazioni o fotografie tratte dalla rete, in particolare se riguardanti minori.

Quanto appena descritto è la dimostrazione di come il binomio "privacy e sicurezza" possa essere declinato anche nel senso che il dato personale in sé e le sue differenti espressioni, in quanto connesse alla dignità individuale, possono essere l'oggetto primario di un'azione finalizzata a disciplinare la rete, rendendola più sicura e regolamentandola nelle sue differenti articolazioni.

### 5. Riflessioni conclusive

In un convegno svoltosi a fine marzo a Genova, l'ex presidente dell'Autorità, Stefano Rodotà, nel commentare uno studio fornito dal gruppo statunitense Boston Consulting, ha spiegato come i dati personali degli oltre 500 milioni di abitanti dei 27 Paesi dell'Unione Europea nel 2020 avranno un valore commerciale stimato attorno ai 1.000 miliardi di euro, pari all'8% del Pil europeo, un tesoro «nascosto dal fortino della privacy». La privacy, continuava Rodotà, deve «continuare a esistere, è un campo di battaglia planetario», dal momento che molti grandi interessi pubblici e privati vogliono impadronirsi delle informazioni personali. Queste parole, evidenziano la rilevanza commerciale dei dati personali, fanno suonare un campanello di allarme, perché chiaramente svelano la principale minaccia che mina la tutela della riservatezza al



giorno d'oggi: l'idea che il dato personale possa essere scambiato al pari di qualsiasi bene e servizio, perdendo così il rango di diritto fondamentale. Ovvero l'idea che i dati identificativi di un individuo possano essere oggetto di una transazione commerciale, generando problematiche che travalicano i confini della sola società della comunicazione<sup>62</sup>.

Questo mutamento rappresenta, soprattutto per gli ordinamenti europei, la nuova sfida in tema di riservatezza e *data protection* e richiede forse un'inversione del paradigma fin qui seguito, tale da consentire che si parli di vera e propria "sicurezza dei dati personali" piuttosto che di "tutela dei dati personali dalle esigenze di sicurezza". Tuttavia anche in questa nuova ottica la privacy come diritto fondamentale trova la sua forza nell'apparire come una sorta di diritto polifunzionale in grado di offrire una tutela a tutto tondo dell'individuo, il quale è nella società dell'informazione costantemente esposto con riferimento ai propri dati personali<sup>63</sup>. E proprio il rafforzamento di questo diritto è l'obiettivo principale delle nuove proposte della Commissione europea di un rinnovato quadro giuridico europeo in materia di protezione dei dati. Un pacchetto di intervento presentato il 25 gennaio 2012 e costituito da un regolamento che andrà a sostituire la direttiva 95/46/CE, e una Direttiva che dovrà disciplinare i trattamenti per finalità di

<sup>62</sup> F. BERNABÈ, *Libertà vigilata, privacy, sicurezza e mercato nella rete*, Laterza, Roma-Bari, 2012.

<sup>63</sup> Cfr. M. MURGO, *Diritti di libertà*, in P. GIANNITI (a cura di), *I diritti fondamentali nell'Unione Europea – la Carta di Nizza dopo il Trattato di Lisbona*, Zanichelli editore, 2013, pp. 761 ss.



giustizia e di polizia (attualmente esclusi dal campo di applicazione della direttiva 95/46/CE).

Il "pacchetto protezione dati", a seguito delle innovazioni introdotte dal Trattato di Lisbona, dovrà essere adottato attraverso la procedura di co-legislazione, che vede il contributo paritario del Parlamento europeo e del Consiglio dell'Unione europea. Molte le innovazioni presenti nella direttiva, a partire dal diritto alla portabilità dei dati, (indispensabile per mantenere il controllo delle proprie informazioni (molto rilevante nel tecnologia del *cloud computing* ad esempio) o il riconoscimento del diritto all'oblio.

Non mancano certo le preoccupazioni e i punti criticabili, evidenziati dalla gran parte delle Autorità garanti europee, Italia compresa, quali gli ulteriori poteri che vengono concessi alla Commissione europea, la poca chiarezza di alcune disposizioni che rischiano di generare dubbi interpretativi nonché un nuovo sistema sanzionatorio eccessivamente rigido. Tuttavia il passaggio forse più significativo del nuovo regolamento è il principio dell'applicazione del diritto Ue anche alle imprese che operano fuori dell'Unione Europea, se i trattamenti di dati personali riguardano i cittadini europei. L'affermazione del principio della territorialità del cittadino a cui i dati appartengono è – oltre ad un prevedibile punto di contrasto con l'impostazione americana – una rilevante novità che amplierà gli strumenti a disposizione delle Autorità europee per tutelare i dati personali dei propri cittadini. Uno strumento per rendere la privacy più sicura.





**NOTE**



## LA COSTRUZIONE DI UN EFFICACE SISTEMA TUNISINO DI PROTEZIONE DEI DIRITTI UMANI

di Stefania Spada

### 1. Introduzione

La Tunisia è stato uno dei primi Paesi africani a creare – conformemente ai cd. Principi di Parigi<sup>1</sup> – un’istituzione nazionale<sup>2</sup> incaricata di promuovere e proteggere i diritti umani ovvero il Comité Supérieur des Droits de l’Homme et des Libertés Fondamentales (CSDHLF), istituito dal decreto n. 54-1991 del 7 gennaio 1991 che lo definisce come un organo consultivo incaricato di assistere il Presidente della Repubblica in tutte le attività riguardanti la tutela dei diritti umani e delle libertà fondamentali.

Quest’organismo pubblico, sin dalla data della sua istituzione, è stato formalmente incaricato – in rapporto di complementarità con altri organi quali, per esempio, le ONG –

<sup>1</sup> Il testo dei Principi di Parigi è consultabile sul sito

<sup>2</sup> E. Decaux, *Le dixième anniversaire des principes directeurs des Institutions Nationales des Droits de l’Homme dits « Principes de Paris »*, in *Droits fondamentaux*, n° 3, janvier – décembre 2003, pp. 11- 29, consultabile sul sito [www.droits-fondamentaux.org](http://www.droits-fondamentaux.org).

di verificare e garantire che a livello nazionale<sup>3</sup> fossero tutelati i diritti umani.

L'efficacia della sua azione nel contesto tunisino è stata oggetto di numerose critiche già immediatamente dopo la sua istituzione tanto è vero che si è messa in discussione<sup>4</sup>, più volte nel corso degli anni, la conformità della sua composizione e del suo metodo d'azione ai Principi di Parigi<sup>5</sup>.

Al fine di soddisfare la richiesta di molteplici attori internazionali<sup>6</sup> di rendere il funzionamento del CSDHLF conforme ai suddetti principi è stata emanata il 16 giugno 2008 la legge n° 2008-37: tale legge presenta alcune evidenti lacune che hanno impedito di fatto al Comitato di svolgere in maniera soddisfacente il proprio ruolo e, di conseguenza, di godere dell'atteso e auspicato riconoscimento sia a livello nazionale che a livello internazionale.

2

<sup>3</sup> Per una panoramica sui trattati internazionali in materia di diritti umani ratificati dalla Tunisia e sul grado di promozione e protezione degli stessi nel Paese fino al 2011 si rinvia a *European Parliament- Directorate General for external policies of the Union policy department, Human Rights concerns in Tunisia*, January 2011, consultabile sul sito <http://europa.eu>.

<sup>4</sup> Si vedano i diversi rapporti redatti dal *Sous-comité d'accréditation* che è un'articolazione interna del *Comité international de coordination des institutions nationales pour la protection et la promotion des droits de l'homme* (CIC) che è incaricato di valutare la conformità delle Istituzioni nazionali ai Principi di Parigi.

<sup>5</sup> Sul punto si veda il rapporto intitolato, *Evaluer l'efficacité des institutions nationales des droits de l'homme*, 2005, *Conseil international pour l'étude des droits humains*, Versoix, Suisse, spec. p. 6-7.

<sup>6</sup> Si veda a titolo esemplificativo il *Rapport et recommandations de la session du Sous-comité d'accréditation (SCA)*, Ginevra, 16-18 novembre 2009, consultabile sul sito <http://nhri.ohchr.org>.

**2. La necessaria ma (forse) non sufficiente modifica della legge che disciplina il funzionamento del Comité Supérieur des Droits de l'Homme et des Libertés Fondamentales**

Il CSDHLF – a tenore della richiamata legge del giugno 2008 e a dispetto di quanto stabilito dai Principi di Parigi – non ha dato prova di essere un organo indipendente, così come richiesto alle istituzioni nazionali incaricate di promuovere e proteggere i diritti umani, anche perché il provvedimento normativo che disciplina l'esercizio della sua funzione – che consiste nel garantire il rispetto dei diritti umani a livello nazionale – da un lato, non prevede per i suoi membri alcuna ipotesi di immunità e, dall'altro, stabilisce che gli stessi siano nominati dal Presidente della Repubblica secondo una procedura, peraltro, poco trasparente.

Di fatto, dunque, il Comitato ha esercitato la suddetta funzione – fino al dicembre 2010 – come fosse una sorta di longa manus del Presidente a danno dell'efficacia del sistema tunisino di protezione dei diritti umani. Tutto ciò ha reso evidente l'inadeguatezza del modus operandi del Comitato, che si sostanziava nella stesura di rapporti annuali concernenti l'implementazione della politica statale avente ad oggetto la promozione e protezione dei diritti umani e nella partecipazione a manifestazioni a livello nazionale e internazionale sul tema, anche alla luce delle rivendicazioni degli attori della rivoluzione dei gelsomini.

È emersa, quindi, l'urgenza di rendere l'istituzione nazionale incaricata di promuovere e proteggere i diritti umani non solo conforme ai Principi di Parigi, ma anche adatta a svolgere le proprie attribuzioni in un nuovo contesto socio-politico.

Della suddetta necessità si è fatto interprete, in un primo momento, il nuovo Presidente del Comitato, eletto il 5 settembre del 2011, che ha presentato – al fine di «promouvoir les droits de l'Homme et les libertés fondamentales et publiques, de concrétiser les objectifs de la Révolution, à travers la mise en place de structures nationales garantissant la dignité et la citoyenneté responsable et la reconstruction de l'Etat sur des bases démocratiques saines, de garantir la réussite de la Révolution et de consolider la place des droits de l'Homme et des libertés fondamentales et publiques»<sup>7</sup> – un progetto di decreto legge finalizzato a creare una «nouvelle institution adaptée à la Tunisie du 14 Janvier»<sup>8</sup> ovvero alla Tunisia della Rivoluzione.

Il progetto presentato al Presidente della Repubblica, infatti, prevedeva la sostituzione del Comité Supérieur des Droits de l'Homme et des Libertés Fondamentales con una nuova istituzione nazionale che – come il Conseil National des Droits de l'Homme previsto all'art. 161 della Costituzione marocchina – dovesse trovare un riconoscimento espresso nella Carta costituzionale e, inoltre, in evidente rottura con i criteri di

<sup>7</sup> Così si legge nel preambolo del progetto. Si rinvia a *Conseil Supérieur des Droits de l'Homme et des Libertés, Rapport 2011*, consultabile sul sito <http://www.droitsdelhomme.org.tn/fr/>.

<sup>8</sup> Si rinvia alla nota precedente.

composizione previsti per il Comitato, dovesse essere composta – secondo gli articoli 33 e 34 del progetto – da membri indipendenti dai partiti politici e ai quali fosse riconosciuta l’immunità funzionale.

Tuttavia, il detto progetto non è stato approvato e, di conseguenza, il Comitato non è stato sostituito dal Conseil National des Droits de l’Homme.

Della necessità, non soddisfatta, di modificare il modus operandi del Comitato, però, si è fatto interprete il Ministro dei Diritti Umani e della Giustizia transizionale che, in data 2 aprile 2013, ha richiesto all’OSCE/ODIHR e, congiuntamente, alla Commissione di Venezia un parere sulla conformità della legge n° 2008-37 con gli standard<sup>9</sup> internazionali dettati in materia. Tale parere è stato

<sup>9</sup> Che sono non soltanto quelli definiti di già citati Principi di Parigi ma anche quelli fissati nei seguenti documenti: UN Commission on Human Rights, *Human Rights Resolution 2005/74: National Institutions for the Promotion and Protection of Human Rights*, 20 April 2005, E/CN.4/RES/2005/74, consultabile sul sito <http://www.refworld.org/docid/45377c883.html>; OHCHR *Background Information on National Human Rights Institutions (NHRIs)* consultabile sul sito <http://www.ohchr.org/en/countries/nhri/pages/nhrimain.aspx>; *The International Coordinating Committee for National Human Rights Institutions (ICC)* <http://nhri.ohchr.org/EN/Pages/default.aspx>; *New Chart of the status of NHRIs del febbraio 2013* e consultabile sul sito [http://nhri.ohchr.org/EN/News/Lists/News/Attachments/104/Chart%20of%20the%20Status%20of%20NHRIs%20\(11%20Feb%202013\).pdf](http://nhri.ohchr.org/EN/News/Lists/News/Attachments/104/Chart%20of%20the%20Status%20of%20NHRIs%20(11%20Feb%202013).pdf); *Handbook on the establishment and accreditation of National Human Rights Institutions in the European Union* dell’ottobre 2012; *Recommendation No. R (97) 14 of the Committee of Ministers to member states on the establishment of independent national institutions for the promotion and protection of Human Rights* <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&%20InstranetImage=567349%20%20&SecMode=1&DocId=578706&Usage=2>.

adottato durante la sua novantacinquesima sessione plenaria tenutasi il 14 e 15 giugno 2013 (parere n. 724/2013). In esso vengono suggerite le modifiche da apportare alla legge che disciplina le modalità di composizione e funzionamento del Comitato al fine di renderlo efficace, realmente indipendente e pluralistico<sup>10</sup>.

A tal fine si suggerisce di prevedere per i suoi membri – fino ad ora nominati dal Presidente della Repubblica per tre anni rinnovabili – un unico mandato lungo e la nomina da parte del Parlamento, di inserire per gli stessi l’immunità funzionale e di modificare il *modus operandi*.

La legge, dunque, dovrebbe essere modificata in modo da ampliare e rafforzare i poteri del Comitato, in particolare attribuendo al Comitato il compito di rendere pareri e raccomandazioni su tutti gli argomenti concernenti la promozione e la protezione dei diritti umani non solo su richiesta del Presidente ma anche di propria iniziativa.

Secondo gli esperti internazionali, infatti, il Comitato dovrebbe poter verificare il seguito dato alle proprie raccomandazioni dalle differenti autorità, svolgere delle indagini d’ufficio o anche su richiesta dei singoli individui, e disporre di strumenti adeguati per ottenere qualsiasi

<sup>10</sup> Per un approfondimento sulle suddette caratteristiche che devono connotare le Istituzioni nazionali di protezione dei diritti umani si veda la Risoluzione 20/14 emanata dal Consiglio dei diritti umani della Nazioni Unite.

informazione utile a svolgere efficacemente il suo ruolo di garante dei diritti umani.

La protezione dei diritti suddetti passa, però, attraverso un consolidamento della cultura del rispetto dei diritti umani nel paese e, in tale prospettiva, compito essenziale del Comitato è di garantire che le decisioni prese nelle sedi internazionali in merito ai diritti umani e ratificate dal Governo tunisino trovino un'adeguata implementazione a livello nazionale. Nel parere, inoltre, si specifica che la legge del 2008 dovrà necessariamente essere modificata nella parte in cui prevede che il Presidente della Repubblica designa i 15 membri e il Presidente del Comitato, per poter rendere quest'organo pluralista come espressamente richiesto dai Principi di Parigi: a tal fine si suggerisce di creare una procedura di selezione e designazione dei membri aperta ai diversi gruppi sociali, in modo tale che il Comitato, la cui previsione dovrebbe essere oggetto di costituzionalizzazione, sia espressione delle diverse componenti della società civile tunisina, o in alternativa che alcuni membri siano designati dal Parlamento e altri dal Presidente della Repubblica.

### **3. L'Instance des droits de l'Homme nei lavori dell'Assemblea nazionale costituente**

Il parere n. 724/2013 è stato adottato a pochi giorni di distanza dalla pubblicazione del quarto, e forse ultimo, progetto di Costituzione, quando durante i dibattiti svoltisi

in seno alla commissione costituente, incaricata di redigere la parte del testo costituzionale riguardante le differenti Istanze costituzionali<sup>11</sup>, si era già affrontata la questione inerente la creazione di una Istituzione nazionale che fosse idonea a proteggere in maniera efficace e conformemente agli standards internazionali i diritti umani.

L'art. 125 del progetto di Costituzione, infatti, costituzionalizza l'Instance des droits de l'homme che è uno dei cinque organi costituzionali indipendenti<sup>12</sup> – da istituire nella Tunisia post-rivoluzionaria – accumulati dalle caratteristiche descritte dall'art. 122<sup>13</sup>.

<sup>11</sup> Si era discusso in merito alle attribuzioni delle cinque diverse Istanze costituzionali da istituire ovvero *l'Instance des médias, l'Instance du développement durable et des droits des générations futures, l'Instance nationale des droits de l'Homme, l'Instance de la bonne gouvernance et de la lutte contre la corruption*.

<sup>12</sup> Nel progetto di Costituzione presentato nel dicembre 2012, successivamente in parte modificato, è stato introdotto un articolo che enumera le caratteristiche di tutte le Istanze costituzionali da istituire. Devono, cioè, essere indipendenti, dotate di personalità giuridica e autonomia amministrativa e finanziaria e devono operare al fine di rinforzare la democrazia e attuare gli obiettivi della rivoluzione tunisina.

<sup>13</sup> L'art. 122 dell'ultimo progetto di Costituzione tunisina dispone che : « *Les instances constitutionnelles indépendantes oeuvrent au renforcement de la démocratie. Elles sont dotées de la personnalité juridique et de l'autonomie financière et administrative. Elles sont élues par l'Assemblée du peuple à laquelle elles présentent leur rapport annuel et devant laquelle elles sont responsables. Tous les organes de l'État se doivent de leur porter assistance dans la réalisation de leur mission. La loi fixe la composition de ces instances, leur organisation, ainsi que les modalités de leur contrôle.* ». Sulle osservazioni fatte dagli esperti della Commissione di Venezia a questa previsione normativa si rinvia a *Commission européenne pour la démocratie par le droit, Observations sur le projet final de*

L'Instance des droits de l'homme, a tenore dell'art. 125 del testo costituzionale in fieri, è un organo che, composto da membri indipendenti eletti con un mandato di sei anni non rinnovabile, «veille au respect et à la promotion des libertés et des droits de l'Homme et fait des propositions dans le sens du développement du système des droits de l'Homme. ».

L'Instance des droits de l'homme nell'assetto costituzionale della Tunisia del 15 gennaio 2011 avrebbe, altresì, il potere di indagare sui casi di violazione dei diritti umani e dovrebbe essere obbligatoriamente consultato su tutti i progetti di legge presentati in materia di diritti umani: tale organo, pertanto, nell'ipotesi in cui dovesse essere approvato l'ultimo dei progetti di Costituzione presentato, si sostituirà all'attuale Comité Supérieur des Droits de l'Homme et des Libertés Fondamentales. A tal fine sarà necessaria l'approvazione di un'apposita legge che ne disciplinerà la composizione, l'organizzazione e le modalità di controllo per la cui redazione il parere reso dalla Commissione di Venezia e dall'OSCE/ODIHR, che già in parte è stato recepito per la redazione della disposizione costituzionale, potrebbe essere di indubbia utilità.

## IL RUOLO DELLE FORZE ARMATE CROATE NELLA DIFESA DELL'AMBIENTE

### UNA NUOVA PROSPETTIVA DI SVILUPPO SOCIALE

Alessandra Carloni

*Introduzione* - 1. Il rapporto tra difesa e ambiente: verso un'ecologia militare? - 2. Attività di difesa e tutela ambientale nel paradigma croato - 2.1. L'incontro tra ricerca scientifica, tutela ambientale e protezione civile - 2.2. Le Forze Armate come attore di sviluppo sociale - 2.3. Il "patrocinio militare" alle campagne di sensibilizzazione ambientale - 3. Il caso del Poligono di Slunj - *Conclusioni*.

#### *Introduzione*

Parlare di Forze Armate in qualità di attore di sviluppo sociale è un esercizio teorico che il presente saggio intende proporre in riferimento al contesto nazionale croato. La prolifica attività di ricerca ad opera dei sociologi del paese, incentrandosi sulla trasformazione dell'organizzazione militare croata e sulle relazioni con il mondo civile, ha fornito alcuni spunti di riflessione sul potenziale detenuto dalle Forze Armate in tal senso.

I nuovi ruoli attribuiti ai militari in funzione di protezione civile hanno favorito un frame di interazione con la popolazione assai differente rispetto al passato, avvicinando le Forze Armate ai valori tipicamente postmoderni che vedono il personale militare socialmente attivo ed orientato sempre più verso un'etica *constabulary* (ovvero di protezione, appunto). Questa nuova immagine del soldato è stata più volte utilizzata dalla politica per scopi strumentali alla legittimazione delle attività di sicurezza, sia quelle praticate all'interno dei confini nazionali, sia quelle svolte in teatri operativi esteri. In Croazia,

dove la cultura militare conferisce alle Forze Armate un ruolo assai rilevante nel contesto pubblico, ciò è avvenuto trasformando i militari in una sorta di “sponsor” per le buone pratiche, un sigillo da apporre alle politiche governative in garanzia delle finalità di sicurezza collettiva che esse intendono perseguire. La promozione di una nuova consapevolezza ecologica, con la relativa assegnazione di compiti in materia di sostenibilità e protezione degli ambienti naturali, rientra in questa strategia politica che orna di aspetti innovativi l’esperienza metamorfica delle Forze Armate nazionali. In siffatte circostanze, queste ultime svolgono la duplice funzione di proteggere la collettività e di accompagnarne il processo di sviluppo civico, assurgendo a caso di studio estremamente interessante per la sociologia militare.

Nella congiuntura internazionale odierna, conquistata la membership europea, quello della tutela ambientale è uno dei temi maggiormente in auge nel dibattito pubblico croato, tallone d’Achille di tutti i governi post autoritari. Il mancato adeguamento ai dettami di Bruxelles sul tema dei rifiuti, ad esempio, espone la Croazia al duro sistema sanzionatorio europeo, costringendo la politica a correre ai ripari. Non potendo contare su un efficace meccanismo di armonizzazione tra legge e cultura civica, per sensibilizzare la popolazione al tema della corretta gestione dei rifiuti e della preservazione del patrimonio naturale, i poteri alti hanno dunque puntato su un testimonial d’eccellenza, le Forze Armate, per magnetizzare l’attenzione dell’opinione pubblica incentivandone l’adeguamento agli standard europei.

La questione, che molto verte sulla valorizzazione economica delle proprie bellezze naturali ai fini turistici, si intreccia con le annose vicende del Poligono di esercitazione militare di Slunj, al centro di una vivace protesta innescata proprio per gli effetti che tale sito avrebbe sugli equilibri ambientali.

Dunque, il comparto militare si trova doppiamente esposto in relazione ai temi ecologici: da una parte, è divenuto una vera

e propria agenzia di socializzazione dello stato, fornendo servizi di educazione civica, dall'altra, in virtù della sua tradizionale funzione bellica, è finito nell'occhio del ciclone di una querelle che ha per oggetto le relazioni tra attività di difesa e ambiente.

Il rapporto tra difesa e ambiente: verso un'ecologia militare?

Nella società globale del rischio, così come definita da Beck<sup>1</sup>, il multitasking operativo adottato dall'organizzazione militare assolve al delicato compito di fornire servizi di sicurezza ad ampio spettro, tentando di rispondere alle molteplici e variegatae istanze di protezione avanzate dalla cittadinanza. Così, l'alterazione semantica subita dal concetto di sicurezza ha raggiunto la deriva della tutela ecologica, fagocitando gli aspetti della giurisprudenza (legati al diritto di vivere in un ambiente sano e al diritto alla salute) e arricchendo la sequela di rischi a cui le società postmoderne sono esposte. La crucialità di questo aspetto è rinvenibile in ogni genere di attività umana, che dall'economia alla difesa impone specifici parametri di pianificazione e che, di conseguenza, ha comportato una profonda modifica della sensibilità collettiva in tema ambientale, divenendo al contempo fattore di sviluppo e di vulnerabilità sociale.

3

Che tale parametro fosse di vitale importanza non è cosa nuova: a partire dal 1949, con l'adozione del Protocollo addizionale della Convenzione di Ginevra, passando per la conferenza ONU di Rio de Janeiro del 1992, il tema della tutela ambientale nelle attività umane, comprese quelle militari e di difesa, ha assunto un rilievo crescente nel dibattito internazionale.

Anche in sede Nato, già nel 1969, l'istituzione del CCMS (Committee on the Challenges of Modern Society), inaugurava una nuova stagione di sensibilità ecologica, richiedendo ad ogni

<sup>1</sup> Beck U., (2000), *La società del rischio. Verso una seconda modernità*, tr. it., Carocci, Roma.

stato membro di contribuire alla ricerca scientifica sulla sostenibilità ambientale delle attività militari. Tale prassi è poi confluita in una politica organica che, con la “Nato Military Principles and Policies for Environmental Protection” del 2003 e del 2011, ha stabilito i principi della protezione ambientale dal punto di vista militare, annoverando tra i compiti dei comandanti della Nato l’applicazione di misure di tutela ambientale per la prevenzione dell’inquinamento, la gestione dei rifiuti, la conservazione e protezione della flora e della fauna<sup>2</sup>.

Che le attività di difesa siano strettamente connesse all’ambiente, dunque, è un dato formalmente acquisito, le cui conseguenze hanno modificato la struttura organizzativa delle Forze Armate, influenzandone la pianificazione e l’operatività sia in tempo di pace che in tempo di guerra.

Se però la letalità degli eventi bellici è un dato incontrovertibile, meno visibile, seppure innegabile, è l’alterazione degli equilibri ambientali provocata dalla mera presenza di strutture militari e da tutta la serie di attività che gravita intorno ad esse.

Uno studio pubblicato sulla celebre rivista “Armed Forces and Society”<sup>3</sup>, approcciando alla questione in termini olistici, ha classificato tre possibili modi per correlare l’ambiente al sistema di difesa: il primo riguarda lo sviluppo di armi e tecnologie sempre più distruttive ed i danni che queste producono nella fase di sperimentazione ed utilizzo nella formazione del personale. Il secondo è collegato alla cosiddetta “guerra ambientale”, ovvero a quelle strategie tese alla modifica

<sup>2</sup> L’attuazione di questa politica è supportata da una serie di accordi di standardizzazione (STANAG), dall’operato dell’Allied Command Operations (ACO) e dell’Allied Command Transformation (ACT) e, per il settore ricerca e sviluppo, dalle scuole Nato di Oberammergau e Ingolstadt, Germania, e dal Nato Undersea Research Centre (NURC) di La Spezia.

<sup>3</sup> Si veda in proposito Foster, Gregory D. (2001), *Environmental Security: The Search for Strategic Legitimacy*, Armed Forces and Society 27(3).

intenzionale di un sistema ecologico (meteo, ionosfera, magnetosfera, ecc.) e o l'attivazione di eventi sismici per provocare intenzionalmente la distruzione fisica, economica e psico-sociale di una popolazione (o anche la sua migrazione geografica) per fini tattico bellici. Il terzo ambito di correlazione afferisce alla serie di cambiamenti e alterazioni all'ambiente causati dalla presenza di strutture militari (attraverso attività addestrative, uso delle infrastrutture civili per il trasporto materiali, inquinamento acustico, ecc). Ciascuno di questi aspetti, strettamente collegati alle attività dei poli di esercitazione o ricerca militare, è oggetto di specifiche analisi in seno al sistema di difesa di ogni stato (ad opera di diversi tipi di agenzie, servizi di intelligence e di geografia militare), ma i dettagli di tali attività, per ovvie ragioni di sicurezza nazionale, restano per lo più segregati negli archivi confidenziali degli stati.

Come suggerito da alcuni studiosi<sup>4</sup>, ciò depone in senso sfavorevole all'affermazione di una "ecologia militare", ovvero di una disciplina a sé stante che possa concretamente svolgere attività di ricerca scevra da interessi di parte. Gli studi scientifici in questione, pertanto, non possono che restare appannaggio del sistema di difesa degli stati, riuscendo solo in parte rispondere alla necessità di tutelare la popolazione civile dai danni che le sofisticate tecnologie militari possono apportare all'ambiente fisico in cui agiscono. Non solo: le loro finalità genericamente definibili belliche, e l'altissimo potenziale distruttivo da esse detenuto, possono generare sentimenti collettivi di timore o resistenza nei confronti dei militari, oscurando l'immagine innovativa che i nuovi compiti civili hanno loro attribuito.

Ciò che è possibile evidenziare, per contro, sono specifiche contingenze in cui la ricerca in campo militare può attivare

<sup>4</sup> Prebilić et Ober, (2005), *Defence system and ecology. The North Atlantic Treaty Organization role*, *Polemos* 8, (1-2).

circuiti proficui nelle percezioni di una determinata collettività, laddove venga inserita in un più vasto progetto a sostegno dello sviluppo e della sicurezza umana.

## **2. Attività di difesa e tutela ambientale nel paradigma croato**

### **2.1. L'incontro tra ricerca scientifica, tutela ambientale e protezione civile**

È ormai tendenza diffusa in tutta l'area euroatlantica di estendere il concetto di difesa da parte delle forze militari anche alla sfera dell'ambiente naturale, considerato come un obiettivo sensibile suscettibile di esser depauperato da comportamenti impropri oppure minacciato da azioni di terrorismo ecologico. Questa duplice disposizione fornisce un topic di elevato interesse per la società croata, che richiede particolare accortezza in sede di pianificazione politica, soprattutto in ragione del fatto che i 2/3 del PIL nazionale derivano dai turisti che in milioni, ogni anno, visitano la Croazia attirati dalle sue ricchezze naturali.

Afferendo a diverse sfere della sicurezza sociale, ed essendo strettamente connessa alle attività economiche, i governi croati hanno incluso la tutela dell'ambiente nella pletera dei nuovi compiti delle Forze Armate, impegnandole sempre più frequentemente nella bonifica di territori particolarmente inquinati, nelle situazioni di catastrofe naturali o nel controllo di aree sensibili, oltre che nelle campagne di sensibilizzazione ambientale, di cui vedremo a breve.

Come accennato in precedenza, l'incontro tra sicurezza postmoderna e prassi ecologica riguarda, oltre quegli aspetti generalmente definibili di protezione civile, anche tutta una serie di progetti di ricerca scientifica. Questi, oltre alla sofisticazione di tecniche distruttive, sono altresì finalizzati alla difesa del territorio e dei cittadini da una serie di minacce che, direttamente o indirettamente, riguardano l'ambiente. Secondo

la gerarchia stabilita dal Ministero della Difesa della Repubblica di Croazia<sup>5</sup>, al primo posto vi è il terrorismo e la necessità di prevenire (o difendersi da) eventuali attentati perpetrati con armi chimiche, batteriologiche e atomiche. Segue la difesa delle infrastrutture tecniche fondamentali (acqua, energia, comunicazioni, ecc.), con la tutela del patrimonio naturale e paesaggistico, suscettibile di divenire bersaglio di attacchi ecologici. Al quarto posto si trova il degrado dell'ambiente naturale, (con i processi quali la desertificazione, l'erosione del suolo, l'inquinamento delle falde acquifere, gli incendi e l'esaurimento delle fonti di energia non rinnovabile); un aspetto non strettamente connesso alle attività militari ma che, al pari di qualunque attacco nemico, influenza direttamente non solo le opportunità di sviluppo e sicurezza della società, ma anche i rapporti con le altre comunità politiche.

Coniugare la necessità di protezione sociale con l'avanzamento dei livelli tecnico scientifici è dunque una delle strategie di difesa attuata dalla Repubblica croata che, adattando i progressi della scienza alle nuove sfide della sicurezza postmoderna anche dal punto di vista ambientale, ha offerto all'opinione pubblica una visione della ricerca scientifica in campo militare in qualità di servizio che lo stato rende alla collettività.

Questo sodalizio tra ecologia e ricerca è stato sancito anche dal Consiglio Nazionale della Scienza, che ha posto la tutela dell'ambiente in cima alla classifica delle priorità scientifiche in Croazia e che opera a stretto contatto con il Ministero della Difesa. Una simile scelta è più che fondata: da una parte, con la prevenzione, la società croata può ancora eludere fenomeni di degradazione ambientale, conservando le proprie prerogative in campo turistico; dall'altra, partendo dalla necessità di preservare l'ambiente, si creano nuove roccaforti di

<sup>5</sup> Rogić I., Mišetić A., Smerić T., (2009), *Hrvatska Vojska kao čimbenik društvenog razvitka –mišljenja hrvatske javnost*, Zagreb, Institut društvenih znanost Ivo Pilar.

razionalizzazione dello sviluppo e, di conseguenza, anche nuovi paradigmi di sviluppo sociale.

La sinergia con il mondo scientifico, integrando diversi aspetti della sicurezza con la tutela dell'ambiente e valorizzando le finalità civili dell'attività di ricerca nel settore della difesa, ha creato le condizioni per stimolare nuovi approcci nelle relazioni civili militari, proponendo all'opinione pubblica un'organizzazione militare multiforme e *multitask*, spendibile nelle strategie di sicurezza e sviluppo nazionali.

## 2.2 Le Forze Armate come attore di sviluppo sociale

La tradizionale affezione della popolazione civile nei confronti dei militari, in Croazia, ha spronato la ricerca sociale ad approfondire la qualità delle relazioni tra le due sfere, cimentandosi in uno studio<sup>6</sup> pioneristico teso ad evidenziare le conseguenze della trasformazione funzionale della organizzazione militare ed i suoi effetti sia sull'opinione pubblica che sui processi di sviluppo nazionale in senso ampio.

La ricerca, realizzata nel 2008 attraverso la somministrazione di alcuni questionari<sup>7</sup>, ha evidenziato come, sebbene non in maniera onnicomprensiva, la gran parte della popolazione consideri positivamente la presenza dei militari nei propri territori e le loro attività di natura civile, confermando la tendenza, verificatasi nel resto del mondo occidentale, ad accogliere positivamente i nuovi ruoli attribuiti alle Forze Armate.

Al contempo, la dislocazione di unità mimetiche nell'intero territorio, così come determinato dal "Piano di sviluppo a lungo

<sup>6</sup> Ibidem.

<sup>7</sup> Il campione consta di 3420 cittadini, intervistati nel mese di aprile del 2008, da un'équipe di sociologi dell'Istituto per le Scienze Umane Ivo Pilar.

termine per le Forze Armate 2006-2015<sup>8</sup>”, ha di fatto creato diversi punti di riferimento per i cittadini, in vece del potere centrale che rappresentano, aumentando i livelli di sicurezza collettivi. Ciò è vero soprattutto nelle zone rurali, tradizionalmente e culturalmente contrapposte a quelle urbane: territori abbandonati sono, infatti, terreno fertile per il radicamento di *malpractices*, sia di tipo parapolitico che criminale, le quali possono fomentare semi di intolleranza e devianza sociale. Per di più, tali territori possiedono una memoria storica di particolare spessore per il processo di riconciliazione interetnico, in quanto proprio le zone rurali semi abbandonate, tra il 1991 ed il 1995, sono state teatro di molteplici incursioni serbe.

In questo specifico contesto territoriale, la sicurezza locale influenza necessariamente il meccanismo che determina le trasformazioni strutturali della società in generale, divenendone condizione essenziale, e l’allargamento delle funzioni militari alla promozione di un maggiore decoro urbano, alla costruzione di infrastrutture ed alla tutela dell’ambiente può contribuire alla diffusione di particolari sensibilità civiche ed ecologiche, assurgendo a volano di sviluppo sociale.

Simili considerazioni sono avallate dall’analisi dei dati emersi dallo studio poc’anzi menzionato, laddove si focalizza l’attenzione sui ruoli dei militari nei diversi contesti della protezione civile, ambientale, infrastrutturale, ecc., e nella valutazione delle alterazioni socio culturali che tale innovazione ha prodotto. Avendo la possibilità di scegliere la propria risposta su una scala che va dal “non sono assolutamente favorevole” al “sono assolutamente favorevole”, in relazione a tali nuove funzioni è emerso un consenso da parte degli intervistati largamente condiviso.

<sup>8</sup> Cfr. <http://www.morh.hr/hr/zakoni-i-strategije/zakoni/zakon-o-obrani-republike-hrvatske.html>, 16 giugno 2013.



COMPITI	Absolutamente contrario	Contrario	Favorevole	Absolutamente favorevole	Non posso valutare	Non rispondo
Mantenimento della sicurezza interna (compiti di polizia)	16,6	14,7	36,7	23,3	8,3	0,3
Controllo internazionale degli armamenti	9	14	42,8	23,3	10,2	0,6
<b>Aiuti in caso di catastrofi naturali nel paese</b>	<b>2</b>	<b>2,6</b>	<b>31,3</b>	<b>60,3</b>	<b>3,6</b>	<b>0,2</b>
Aiuti in caso di catastrofi naturali al di fuori del paese	2,8	6,4	38,1	47,7	4,7	0,3
<b>Difesa ambientale</b>	<b>3,5</b>	<b>7,1</b>	<b>33,6</b>	<b>50,3</b>	<b>5,1</b>	<b>0,4</b>
<b>Compiti cerimoniali</b>	<b>6,9</b>	<b>13,5</b>	<b>40,8</b>	<b>31</b>	<b>7,5</b>	<b>0,2</b>
<b>Costruzione/ manutenzione di infrastrutture civili</b>	<b>7</b>	<b>12,2</b>	<b>29,7</b>	<b>44</b>	<b>6,9</b>	<b>0,2</b>
Sostituzione di impiegati civili in caso di scioperi	39,8	21,2	17,9	8,6	12,1	0,4
Controllo delle frontiere	6,1	10,3	41	36,3	5,9	0,4
Lotta al terrorismo	1,5	3,6	28,9	61,4	4,3	0,4
Lotta al traffico di droga	4	4,6	28,6	57,6	4,9	0,3
Protezione e difesa del territorio	0,6	1,9	20,2	73,3	3,6	0,5

Tab. 1. Compiti delle Forze Armate nella valutazione dell'opinione pubblica, dati in percentuale (2008)

Le operazioni di soccorso in caso di catastrofe naturale in teatro domestico sono ampiamente accettate (91,6% del totale, sommando le risposte favorevoli con quelle assolutamente favorevoli), mentre quelle di difesa dell'ambiente registrano un 83,9% dei consensi (adottando la stessa formula aggregatrice). Altro quesito di estremo interesse in questa sede è quello inerente il consenso dell'opinione pubblica in merito alla

partecipazione delle Forze Armate nella costruzione/manutenzione di infrastrutture civili (73,7% di gradimento)<sup>9</sup>.

Sebbene sia chiaro che al momento delle rilevazioni gli intervistati non abbiano ancora maturato un'opinione organica sulle Forze Armate in qualità di attore di sviluppo sociale, (la riforma della difesa, con la conversione funzionale dei militari, è stata varata nel 2002, mentre lo studio è del 2008), le loro risposte alle singole questioni suggeriscono l'origine di una tendenza positiva in tal senso. Nel quesito successivo, infatti, si esplicitava la richiesta di valutazione del ruolo di sviluppo sociale dei militari sotto il punto di vista locale, regionale e nazionale.

<b>Come valutate nel complesso il ruolo delle Forze Armate nello sviluppo sociale?</b>							
	Molto negativo	Abbastanza negativo	Né positivo né negativo	Abbastanza positivo	Molto positivo	Non so valutare	Non rispondere
Livello nazionale	2,2	6,4	<b>33,9</b>	33,2	8,6	15,3	0,4
Livello regionale	2,7	7,6	<b>34,3</b>	30,6	7	17,4	0,4
Livello locale	3,1	7,6	<b>35,2</b>	28,8	6,8	18	0,5

Tab. 2. Le Forze Armate come attore di sviluppo sociale nell'opinione pubblica, dati in percentuale 2008

Malgrado una porzione niente affatto esigua di consensi, le risposte fornite dagli intervistati indicano che nel sentire comune non si sia affermata una piena consapevolezza del potenziale di sviluppo detenuto dalle Forze Armate nelle dinamiche nazionali. Andando ad osservare le cifre relative ai tre livelli di analisi, invero, le percentuali più alte si stanziano su un valore neutro (a livello nazionale 33.9%, regionale 34.3%, locale 35.2%), sebbene non di molto rispetto a quelle che attestano una valutazione "abbastanza positiva" (rispettivamente 33.2%, 30.6% e 28.8%).

<sup>9</sup> Degno di nota è il fatto che tali percentuali siano di poco inferiori a quelle inerenti il tradizionale ruolo dei militari nella difesa del territorio (93,5% dei consensi).

Nel passo successivo si è voluto evidenziare, indipendentemente da questi livelli, come è considerato, nel complesso, il ruolo delle Forze Armate nello sviluppo sociale; i ricercatori hanno dunque scremato le risposte neutre e incerte, considerando solo quelle che attestano posizioni positive o negative, ovvero quelle espresse da cittadini in possesso di un'opinione chiara al riguardo. Da questo esercizio di focalizzazione è emerso che il ruolo delle Forze Armate come attore di sviluppo sociale (a livello nazionale) è accolto positivamente dagli intervistati con un grado di istruzione inferiore (86%), anziani (86%) orientati politicamente a destra (87.2%), provenienti da centri extra urbani (86.6%). Per contro, assumono un atteggiamento negativo gli intervistati con un grado di istruzione superiore (80%), giovani (75.9%), politicamente orientati a sinistra (76.2%) e residenti nei centri urbani (80.8%).

La stessa scrematura è stata eseguita anche sulle risposte fornite in riferimento al contesto locale e regionale, con il risultato che l'identikit degli intervistati è rimasto pressoché inalterato.

Da ciò si può dedurre che il grado di urbanizzazione, l'età, l'istruzione e l'orientamento politico siano fattori determinanti per la percezione dei militari in qualità di soggetti promotori di sviluppo.

La polarizzazione della società croata secondo lo schema centro periferia, pertanto, si manifesta anche nei risultati di tale studio, palesando lo steccato culturale che separa i due volti del paese e la necessità di attuare strategie politiche capaci di raggiungere trasversalmente la popolazione civile. Proprio nelle periferie, infatti, l'età media e la migrazione giovanile sono inesorabilmente in aumento, e le forze centrifughe che governano questi territori ancorano modelli, memorie e culture a vecchi schemi, ostacolando l'avanzare dei processi di modernizzazione e di inclusione sociale.

### 2.3 Il “patrocinio militare” alle campagne di sensibilizzazione ecologica

Se è vero che le Forze Armate perdono appeal nei confronti delle nuove generazioni, mantenendolo ben saldo nei confronti delle vecchie, i governi del paese, impegnati in una vastissima opera riformatrice, hanno ritenuto opportuno sfruttare il comparto militare, colonna portante della legittimazione statale, per enfatizzare il messaggio innovatore delle proprie campagne sociali, puntando sulle fasce di popolazione maggiormente emarginate e, al contempo, mostrando ai più scettici una nuova immagine sociale del militare, con lo scopo di accattivarsene le simpatie. L'ampio consenso di cui godono le Forze Armate croate, perciò, ha fornito l'occasione ai governi di issare lo stendardo militare laddove vi fosse la necessità di attirare l'attenzione del grande pubblico, valorizzando così una serie di esperienze politico sociali determinanti per il raggiungimento degli standard europei.

Tali esperienze sono rinvenibili in una varietà di eventi nazionali che hanno celebrato l'operato delle Forze Armate trasformandole in una sorta di “sponsor” per le buone pratiche. Esempi recenti sono individuabili nella riqualificazione di alcuni spazi urbani a Vukovar, città ricordata per il celeberrimo assedio serbo, oppure in giornate dedicate alla sensibilizzazione per la raccolta differenziata dei rifiuti, o anche nelle vastissime opere di bonifica dei fondali marini.

A Vukovar, dove l'indolenza della politica ha consentito che interi isolati fossero lasciati inagibili o strutturalmente decadenti per anni, la pesante eredità della guerra ha trovato nei suoi stessi protagonisti le figure chiave del proprio riscatto. Gli ingegneri militari sono stati impegnati a lungo nella riqualificazione degli spazi urbani della città, progettando gli adeguamenti strutturali e occupandosi della demolizione degli edifici fatiscenti, ottemperando così al duplice compito di fornire dei servizi alla cittadinanza e completare il proprio programma di formazione accademica. La stessa opera di

riassetto è stata replicata nelle aree limitrofe, interessando circa altri cento comuni e coinvolgendo così quella fascia di popolazione spesso rimasta ai margini delle iniziative politiche.

La presenza di mezzi militari nelle opere di valorizzazione di spazi e giardini pubblici e lo stesso utilizzo di strumenti tradizionalmente votati alla distruzione per finalità sociali arricchiscono di simbolismo il messaggio indirizzato alla collettività, ormai chiamata ad intendere le Forze Armate come una forza pubblica deputata alla sicurezza ed al benessere collettivo.

Se la riqualificazione degli assetti urbani da parte del personale militare è attività certamente pionieristica, altrettanto può dirsi della partecipazione dello stesso a momenti dedicati all'educazione civica in funzione ecologica. L'Esercito croato, infatti, è stato scelto come *testimonial* della giornata di sensibilizzazione al problema dello smaltimento dei rifiuti, iniziativa promossa dal governo croato nella scorsa primavera. Elevando l'immagine del militare ad esempio da seguire, e pubblicizzando il soldato in mimetica impegnato nella differenziazione di carta, vetro, plastica e materiale organico, la Croazia ha così creato una vera e propria strategia di marketing per il proselitismo della cultura ecologica.

Rientra nello stesso progetto di educazione la grandissima eco mediatica che ogni anno contraddistingue l'imponente opera di pulizia dei fondali marini operata dai sommozzatori della Marina Militare. In primavera, una squadra di militari subacquei raggiunge i luoghi ad alta attrazione turistica e, avendo cura di informare preventivamente la stampa, procede alla rimozione di tonnellate di rifiuti e relitti. Tale iniziativa viene debitamente pubblicizzata per attirare l'attenzione di visitatori stranieri e autoctoni che, in quantità crescente, restano affascinati dalle bellezze costiere della Croazia, scegliendola come meta ove trascorrere le vacanze. Il grande interesse a tutelare il patrimonio ecologico, di guisa, risulta altresì funzionale allo sviluppo del turismo, vero motore economico del paese.

Se da una parte questa sequenza di attività rientra in uno specifico progetto di sviluppo socio economico a livello nazionale, dall'altra, è da considerarsi come una politica mirata alla tutela del "brand" militare, per renderlo a tutti gli effetti una risorsa spendibile in una pluralità di circostanze e tutelarlo dalle vicende spinose che recentemente lo hanno investito.

### 3. Il caso del Poligono di Slunj

Come è emerso anche dallo studio riportato in precedenza, esiste una porzione di popolazione che non subisce in maniera acritica il fascino militare e che verosimilmente fornisce il bacino di utenza del movimento di protesta contro il campo di esercitazione "Eurgen Kvaternik", anche conosciuto come Poligono di Slunj.

Sono molti i movimenti ecologisti, quali Green Network (Zelena mreža) e la costola croata della PCAP International (Prevention of Cruelty to Animals and Plants), nati all'indomani della fine della guerra, che hanno la finalità comune di porre fine ai presunti effetti dannosi che le attività militari producono sull'ambiente circostante il Poligono. Secondo le loro denunce, tali effetti si tradurrebbero nell'inquinamento delle falde acquifere, nei dissesti all'edilizia popolare e nell'aumento del tasso di tumori nella comunità locale. Per quest'ultimo aspetto, in particolare, si sospetta che la causa sia riconducibile alle radiazioni sprigionate dalle deflagrazioni degli ordigni bellici a scopo esercitativo.

La PCAP, in proposito, ha effettuato degli studi<sup>10</sup> sulla popolazione residente nei dintorni del Poligono, intervistando, nei mesi di agosto e settembre 2006, un campione di 154 famiglie. Il 40 % di esse asseriva di aver subito danni strutturali alle proprie abitazioni a causa delle esplosioni e, in circa una su tre, si registrava la presenza di un malato di tumore. Tra i

<sup>10</sup> Per un resoconto completo si veda <http://www.jutarnji.hr/cak-500-hektara-poligona-u-slunju-zagadeno-teskim-metalima/155984/>, 7 giugno 2013.

cittadini era diffusa la convinzione che le moltissime malattie “inspiegabili” che in diverse occasioni hanno colpito gli allevamenti di bovini, suini e pollame, fossero collegate alle attività del sito militare, e che la presenza di rarità faunistiche nel vicino Parco naturale dei laghi di Plitvice (patrimonio dell’Unesco), fossero minacciate alla stessa stregua.

Una situazione nient’affatto distesa che ha mobilitato la società civile in diverse azioni di protesta. La più famosa, probabilmente, è stata quella organizzata contro la Nato in occasione di un’esercitazione congiunta tra Croazia e Stati Uniti, nel 2007. Allora, al coro di dissenso civile si unì quello di alcuni rappresentanti del mondo scientifico che denunciarono la presenza, all’interno dei missili sganciati dagli americani a scopo esercitativo, di uranio impoverito. Progressivamente, la partecipazione di scienziati e ricercatori alle attività di dissenso ha assunto continuità, avviando così una vera e propria azione di lobbying mirata alla predisposizione di adeguati strumenti di contenimento degli effetti dannosi del Poligono ed, in ultima istanza, alla chiusura dello stesso.

16

L’iniziale minimizzazione del problema da parte delle istituzioni ha trovato nel muro di opposizione scientifico-popolare un’omogeneità tale da non consentire il procrastinarsi di atteggiamenti indolenti. Per cui, proprio dal 2007, il governo croato ha istituito un sistema di monitoraggio sulle condizioni del suolo, dell’aria e delle falde acquifere nei dintorni del Poligono, procedendo periodicamente alla valutazione dell’impatto ambientale prodotto dalle attività del campo di esercitazione. Particolari rilievi vengono effettuati per stimare gli effetti acustici delle esplosioni sulla salute umana e faunistica, ma anche per determinare eventuali conseguenze delle vibrazioni procurate dal trasporto dell’equipaggiamento militare<sup>11</sup>.

<sup>11</sup> Questo argomento, in particolare, è stato oggetto di precise disposizioni legislative che prevedono la corresponsione di un equo indennizzo per i danni alle abitazioni private.

Regolarmente, i dati vengono pubblicizzati attraverso il sito del Ministero della Difesa croato<sup>12</sup>, accompagnati da relazioni tecniche che, nelle loro considerazioni, tengono debitamente conto della qualità delle esercitazioni svolte nei periodi antecedenti i rilievi e della loro connessione con i risultati delle analisi.

Il caso del Poligono di Slunj è una querelle tutt'altro che archiviata, suscettibile di gettare nocimento sull'immagine delle Forze Armate e di svilire le molteplici funzioni in materia di educazione civica che ad oggi la politica ha loro attribuito. Conseguentemente, si delinea una doppia esposizione mediatica dell'immagine sociale del militare dalla prospettiva ecologica, la cui evoluzione, tutt'ora in essere, assumerà fisionomie ancora da definire allorché le strettoie di Bruxelles produrranno i relativi effetti. Le questioni pendenti sulla gestione e smaltimento dei rifiuti, non ancora conformi ai parametri imposti dall'Unione, sono infatti al centro dei dibattiti pubblici croati, su cui si attende il prossimo abbattimento della scure sanzionatoria europea, ed i militari, ormai appannaggio delle politiche ecologiche, conseguentemente subiranno un ritorno negativo in termini di immagine.

### *Conclusioni*

Valutando le circostanze odierne, è possibile asserire che il campo di formazione e sviluppo di politiche ecologiche ad opera delle Forze Armate croate sia determinato dalle specifiche influenze sull'ambiente che queste esercitano e dal ruolo di attore ecologico che, progressivamente, stanno acquisendo nel panorama sociale del paese. In questo frangente, i militari rappresentano una corporazione specifica che

<sup>12</sup> I cui prospetti sono consultabili all'indirizzo web: <http://www.morh.hr/hr/morh-u-zajednici/ekologija/ekologija.html>, 20 giugno 2013.

tecnicamente e organizzativamente cerca di sviluppare un proprio profilo in rapporto alla protezione dell'ambiente, fornendo una liaison tra necessità politiche e nuove sensibilità ecologiche sempre più in crescendo nel paese. La cooperazione sinergica tra mondo scientifico, militare e civile ha perciò integrato su vari livelli la risposta dello stato alle molteplici esigenze della sicurezza contemporanea, razionalizzando le strategie politiche in senso polivalente attingendo dalle proprie risorse culturali.

In questo senso la politica si è avvalsa delle Forze Armate, rappresentanti di alto rango delle istituzioni, per promuovere comportamenti e prassi atti ad elevare il livello socio culturale del paese, ormai 28 membro UE.

Il coinvolgimento delle periferie, ancora inclini a manifestazioni di scetticismo etnico ed ancora legate ad un'immagine bellica dei militari, rientra nel piano di educazione civica promossa dai governi croati e nella volontà di escogitare strategie politiche in grado di raggiungere in maniera trasversale l'intera popolazione.

L'utilizzo dell'icona militare ha diverse chances per dimostrarsi idonea ad incentivare un mutamento intrinseco nei valori e negli stili di vita della società civile, poiché in grado di catturare l'attenzione di una vasta porzione del popolo, conservando le vesti mitiche proprie della cultura militare e proiettandole nei nuovi scenari odierni, in cui la moltiplicazione delle esigenze pubbliche e private, unite all'internazionalizzazione della vita politica, hanno imposto l'adozione di strategie scaltre. Pertanto, l'ascesa del militare a soggetto promotore di sviluppo, attingendo dal patrimonio simbolico culturale nazionale, risulta sicuramente efficiente dal punto di vista economico e foriero di efficacia anche dalla prospettiva della società civile, evidentemente incline a deporre la propria fiducia nell'operato delle Forze Armate.

In definitiva, considerata in qualità di processo in fieri, la mutazione funzionale del personale militare, passato dalla tradizionale difesa del territorio a quella "atipica" del

*Note*

patrimonio naturale e divenuto appannaggio della politica per la promozione di nuovi stili di vita ecologici, ha sicuramente arricchito la fase metamorfica delle relazioni civili militari in Croazia, assurgendo a modello di sviluppo potenzialmente spendibile anche in altri contesti nazionali.



