MARCO CUNIBERTI

DEMOCRAZIE, DISSENSO POLITICO E TUTELA DELL'ANONIMATO

SOMMARIO: 1. Dissenso politico e democrazia nella « società della sorveglianza ». — 2. Anonimato e libertà di espressione in una società "democratica". — 3. Tutela dell'anonimato e regimi non democratici: i « rifugiati digitali ». — 4. Contraddizioni e ambiguità dell'anonimato nella manifestazione del dissenso politico. — 5. Quali strumenti per difendere l'anonimato? La protezione delle fonti, la responsabilità e il ruolo degli intermediari. — 6. La necessità di procedimentalizzare la *disclosure* della fonte anonima.

1. Dissenso politico e democrazia nella « società della sorveglianza ».

Affrontare il tema dell'anonimato in rapporto ai concetti di dissenso politico e di democrazia significa abbandonare il terreno relativamente sicuro del rapporto tra anonimato e *privacy* per addentrarsi in quello, assai meno esplorato, del rapporto tra anonimato, manifestazione del pensiero e forme della partecipazione politica.

In questa prospettiva, a prima vista, il tema dell'anonimato come strumento di protezione del dissenso sembrerebbe non riguardare, se non in modo affatto marginale, un ordinamento che possa realmente definirsi democratico: da un lato, infatti, la necessità di proteggere l'anonimato di chi dissente è una esigenza che sembra porsi solo in contesti non democratici; d'altra parte, una effettiva protezione di qualche forma di anonimato pare configurabile solo in regimi democratici (o quanto meno rispettosi dei diritti fondamentali), posto che appare improbabile che un regime autoritario accordi una qualche forma di tutela in questo ambito.

* Il presente scritto riproduce, con l'aggiunta di note e con aggiornamenti, la relazione presentata al convegno '*Anonimato, diritti della persona e responsabilità in rete*' organizzato dal Dipartimento di diritto pubblico dell'Università di Milano, dal Dipartimento di scienze giuridiche dell'Università di Milano-Bicocca e dalla Fondazione Calamandrei l'11 novembre 2013. Il lavoro, prima della pubblicazione, è stato sottoposto all'esame della Direzione della Rivista.

Ne consegue che uno studio sull'anonimato come strumento di protezione del dissenso sarebbe possibile solo nei termini di una analisi degli strumenti — tecnici e giuridici — che chi vive ed opera all'interno di regimi democratici — gli unici nell'ambito dei quali possiamo immaginare all'opera forme di tutela giuridica dell'anonimato — può mettere a disposizione dei movimenti di opposizione che operano all'interno di regimi autoritari: ed è questa, infatti, la prospettiva in cui per lo più si pone chi, affrontando il tema dell'anonimato dalla prospettiva del suo collegamento con la libertà di espressione, tende a circoscriverlo al problema della protezione dei dissidenti all'interno di regimi autoritari [1].

Una analisi appena più approfondita, però, potrebbe svelare che le cose non stanno esattamente in questi termini semplici e (relativamente) tranquillizzanti, poiché, nella percezione dei movimenti che esprimono forme di dissenso in rete, la stessa linea di demarcazione che separa gli ordinamenti c.d. "democratici" da quelli che tali non sono è tutt'altro che netta.

Se si analizzano le tecniche di lotta e i linguaggi dei movimenti sociali in rete [2], o il pensiero dei protagonisti di vicende come quella di *Wikileaks* [3], ciò che colpisce è che non sembrano esistere enormi differenze, nelle aspettative così come nelle preoccupazioni nei riguardi delle nuove tecnologie della comunicazione, tra chi opera nel contesto di un regime autoritario e chi opera in contesti che siamo abituati a definire democratici: e in particolare la distinzione tende a sfumare nel momento in cui si pone l'accento sui rischi del controllo sulle attività politiche che si svolgono in rete, un controllo che appare sempre più pervasivo e indipendente dai contesti nazionali, in quanto affidato ad una complessa

[1] Si v. ad esempio la raccomandazione 3/97 del 3 dicembre 1997 del Gruppo di lavoro per la tutela delle persone fisiche con riguardo al trattamento dei dati personali (reperibile in *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_it.pdf*), intitolata « *Anonimato su internet* », dove, come esempio di situazioni in cui l'anonimato serve, oltre che alla tutela della riservatezza, anche a proteggere la libertà di espressione, si cita (pag. 5) il caso « dei dissidenti politici soggetti ad un regime politico totalitario che desiderano esprimere la loro opposizione al sistema politico in cui vivono e richiamare l'attenzione sulle violazioni dei diritti umani » (sulla raccomandazione, v. E. MORELATO, *Il principio di necessità del trattamento: espressione di un nuovo diritto della personalità o regola generale per il trattamento dei dati personali con strumenti informatici?*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale* (vol. XLVIII del *Trattato di diritto commerciale e di diritto pubblico dell'economia* diretto da F. Galgano, Padova 2008, 209 ss.).

[2] Basti, per tutti, il riferimento a uno dei più autorevoli sociologi della rete, che nelle sue recenti ricerche sui movimenti sociali in rete tratta, senza sostanziale soluzione di continuità, tanto delle rivolte avvenute nei paesi del Nord Africa a partire dal 2011, quanto dei movimenti di protesta sorti in Europa e negli USA a seguito della crisi economica del 2008 (come la c.d. « rivoluzione delle pentole » in Islanda, il movimento degli « *Indignados* » in Spagna, il movimento « *Occupy Wall Street* » negli USA: M. CASTELLS, *Reti di indignazione e speranza. Movimenti sociali nell'era di internet*, Milano 2012).

[3] Come espresso nel recente libro — intervista di J. ASSANGE, *Internet è il nemico*, Milano 2012.

rete di cui fanno parte individui singoli, grandi organizzazioni imprenditoriali e governi, e che si riassume in espressioni come « società della sorveglianza » [4] o nella più colorita (e inquietante) « stato transnazionale della sorveglianza » [5].

E in effetti, proprio il carattere transnazionale e non territoriale della rete è uno degli aspetti che finisce col mettere in crisi la fiducia nelle garanzie di riservatezza che fanno capo alle istituzioni (e alle costituzioni) nazionali: le recenti vicende del c.d. "*datagate*" hanno evidenziato, nel caso ve ne fosse bisogno [6], tutte le difficoltà che gli strumenti di protezione elaborati in ambito nazionale (ma lo stesso può dirsi per l'ambito europeo) incontrano nel difendere i cittadini (e le istituzioni stesse) dalla sorveglianza da parte di soggetti (pubblici e privati) che sfuggono al nostro sistema di tutele: grandi multinazionali, centrali di *intelligence*, organizzazioni di vario tipo, governative e non, che operano attraverso i confini nazionali e utilizzano strumenti sempre più sofisticati, spesso prodotti in occidente per essere poi messi a disposizione (per lo più, spesso a costi non particolarmente proibitivi) anche di regimi autoritari (e viceversa), o prodotti concepiti per contrastare la pirateria informatica o la pedo - pornografia *on line*, ma in realtà utilizzabili per qualsiasi scopo.

Si registra quindi, tra gli utenti più attenti e consapevoli, una diffusa e certo non immotivata percezione di come gli strumenti della sorveglianza si stiano evolvendo profondamente, diventando sempre più raffinati, multiformi e flessibili, e coinvolgendo anche i soggetti privati: l'architettura di internet, oggi, diversamente da quella degli inizi, è una architettura compatibile con la sorveglianza, che anzi la favorisce, e questo avviene nei regimi che si proclamano democratici come in quelli che tali non sono.

Tra le grandi illusioni relative ad internet che non sembrano

---

[4] Al riguardo, v. S. NIGER, *Sorveglianza e nuovi diritti di libertà*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato*, cit., 6, secondo cui « la sorveglianza è ormai la forma propria della società dell'informazione »: una sorveglianza tanto più pervasiva quanto più impercettibile, che si scopre solo quando « qualcosa va storto » (D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano 2002, 2 e ss.), e che affonda le proprie radici, oltre che negli interessi economici che innervano la rete, anche nella sempre maggiore richiesta di sicurezza che caratterizza la società contemporanea (l'A. cita sul punto Z. BAUMAN, *La solitudine del cittadino globale*, Milano 2003, 24 in particolare).

[5] L'espressione è utilizzata ad es. da J. ASSANGE, *Internet è il nemico*, cit., 148.

[6] E in effetti, la vicenda del c.d. "*datagate*" non è stata la prima in cui si sono evidenziati gli enormi rischi implicati nella possibilità di collaborazione tra governi e multinazionali nel controllo sulla circolazione dei dati: E. PELINO, *L'anonimato su internet*, in G. FINOCCHIARO (a cura di) *Diritto all'anonimato*, cit., 289 ss., ricorda ad es. che nel 2006 il Dipartimento della Giustizia USA chiese ai 4 principali motori di ricerca statunitensi di fornire dati relativi alle ricerche degli utenti, ai dichiarati fini di lotta contro la pedopornografia, e che solamente *Google* rifiutò di fornire i dati richiesti; altra vicenda emblematica, richiamata dall'A., è quella che vide protagonisti *Yahoo* ed il governo cinese, e in cui le informazioni fornite contribuirono all'arresto di un giornalista (Shi Tao), poi condannato a 10 anni per avere inviato negli USA delle mail contenenti presunti segreti di stato.

essere sopravvissute alla fine del secolo scorso, vi è senz'altro quella della non controllabilità della rete: l'illusione che esista una "natura" intrinseca, incorporata nella "architettura" della rete, che la rende di per sé refrattaria ad ogni controllo. Giustamente si denuncia il carattere ideologico di questo assunto [7]: l'architettura della rete non è data una volta per tutte, ma dipende dal modo in cui essa viene disegnata dai suoi creatori, dalle *élites* tecnologiche che la configurano, e che continuamente la rimodellano anche sulla base degli interessi economici sottostanti; sicché, quando parliamo di architettura della rete non ci riferiamo solo all'architettura tecnologica [8], ma ci dovremmo riferire anche a come gli interessi economici influiscono sulla struttura della rete [9].

In altri termini, se, come sembra difficilmente contestabile, la profilazione dell'utente è fondamentale per tutti i modelli di *business* legati al c.d. « *web* 2.0 » [10], nonostante tutto l'apparato giuridico che si può tentare di mettere in campo per limitare e contenere il fenomeno, pare realistico attendersi che anche la struttura tecnologica di internet finirà per evolversi in modo da rendere sempre più agevole la profilazione — e quindi, in pratica, la sorveglianza — dell'utente [11].

Formule come quella della « società della sorveglianza » o dello « stato transnazionale della sorveglianza », depurate dalle sfuma-

---

[7] C. Formenti, *Cybersoviet. Utopie postdemocratiche e nuovi media*, Milano 2008, 201 ss., osserva peraltro come il mito della rete refrattaria al controllo sia tuttora duro a morire, nonostante sia stato ormai apertamente ripudiato da autorevoli studiosi (certo non sospettabili di diffidenza o preconcetta ostilità verso le nuove tecnologie) come Manuel Castells o Lawrence Lessig.

[8] Che pure ha un indubbio rilievo, nel momento in cui denota una tendenza evidente ad abbandonare il carattere decentrato della rete e a favorire il controllo: si pensi alla diffusione del *Cloud*, e in generale alla tendenza a ritrasferire "al centro" l'intelligenza della rete, o al crescente rilievo ed utilizzo degli strumenti di geolocalizzazione.

[9] Come osserva S. Niger, *Sorveglianza e nuovi diritti di libertà*, in G. Finocchiaro (a cura di), *Diritto all'anonimato*, cit., 12, anche uno dei più convinti apologeti della rete come occasione di liberazione e di emancipazione è costretto ad ammettere che « la trasformazione della libertà e della *privacy* su Internet è una conseguenza diretta della sua commercializzazione. Il bisogno di rendere sicura e identificare la comunicazione per ricavarne profitti e il bisogno di proteggere i diritti di proprietà intellettuali in rete hanno condotto allo sviluppo di nuove architetture *software* che rendono possibile controllare la comunicazione tra computer. I governi del mondo sostengono queste tecnologie di sorveglianza e sono pronti ad adottarle per riprendere parte del potere che stanno perdendo » (M. Castells, *Galassia internet*, Milano 2006, 163).

[10] E tale situazione non pare destinata a mutare col passaggio allo scenario del c.d. « *web* 3.0 » o « *web* semantico », posto che sia possibile attribuire un significato univoco a tali espressioni.

[11] La formulazione accattivante di Y. Benkler, *La ricchezza della rete*, Milano 2007, 66, secondo cui « l'economia dell'informazione in rete reca con sé la promessa di proiettare la ricchezza della vita sociale al centro dell'economia e della produzione », in realtà rivela uno scenario preoccupante nel momento in cui la « ricchezza della vita sociale » appare misurabile integralmente in termini economici: collocata « al centro dell'economia e della produzione », la vita sociale risponde integralmente a logiche economiche, e ogni suo aspetto (tempo libero, relazioni sociali, relazioni affettive, creatività) diventa uno strumento per la produzione di utilità economiche.

ture un po' apocalittiche che indubbiamente le contraddistinguono, descrivono quindi efficacemente un sistema che supera i confini degli stati e rispetto al quale, ben vedere, nessuno può dirsi estraneo: stati democratici e stati autoritari, poteri pubblici e imprese private, per arrivare allo stesso privato cittadino, sempre pronto a barattare la propria *privacy* per usufruire di servizi gratuiti. Quanto più diffusamente le nuove tecnologie dell'informazione e della comunicazione sono utilizzate da cittadini e movimenti politici che praticano forme di dissenso rispetto ai modelli economici, culturali e politici dominanti, tanto più aumentano i rischi di controllo e di manipolazione, e ciò, è bene sottolinearlo, tanto nei regimi che possiamo definire autoritari o totalitari, quanto in quelli che siamo abituati a considerare compiutamente democratici.

2. Anonimato e libertà di espressione in una società "democratica".

Nonostante venga talora affermato il contrario [12], non sembrano potersi seguire, almeno sino ai loro esiti più radicali, quelle tesi che, ricollegando l'anonimato alla stessa garanzia della libertà di espressione, ne affermano il carattere di diritto fondamentale: se l'anonimato può giocare un ruolo fondamentale ove siano in gioco esigenze di protezione della *privacy*, esso non assurge a situazione tutelata in sé, e in tale senso non sembrano potersi invocare le garanzie fornite da altre disposizioni costituzionali, come l'art. 21 [13] o l'art. 2 [14] della costituzione repubblicana.

In effetti, quando si afferma che l'anonimato, o il diritto ad usare uno pseudonimo, fa parte integrante della libertà di espressione, si fa per lo più riferimento a una forma di anonimato debole

[12] Cfr. ad es. G. M. Riccio, *Diritto all'anonimato e responsabilità civile del provider*, in L. Nivarra, V. Ricciuto, *Internet e il diritto dei privati*, Torino 2002, 29.

[13] La stessa formulazione letterale dell'art. 21 cost. sembra escludere che la disposizione possa essere utilizzata per fondare un diritto alla manifestazione in forma anonima, sia dove fa riferimento alla libertà di manifestare il «*proprio*» pensiero (comma 1), sia dove ammette (comma 3) l'esistenza di disposizioni volte a imporre l'individuazione dei responsabili per le pubblicazioni a mezzo stampa (sul punto v., da ultimo, M. Betzu, *Regolare internet. La libertà di informazione e di comunicazione nell'era digitale*, Torino 2012, 144 ss.; ma sia consentito rinviare anche a M. Cuniberti, *Disciplina della stampa e dell'attività giornalistica e informazione in rete*, in Id. (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionale e pubblicistici*, Milano 2008, 240 ss.). Non dissimili sono, del resto, le indicazioni che possono trarsi dall'art. 10 della Convenzione europea dei diritti dell'uomo, che, nell'affermare che l'esercizio della libertà di espressione « comporta doveri e responsabilità », fa chiaramente intendere che tra le « formalità » e le « restrizioni » contemplate nel par. 10.2 possano trovare posto regole atte a consentire l'individuazione dei responsabili.

[14] Come osserva D. Tassinari, *Diritto all'anonimato e diritto penale: un (possibile) oggetto di tutela o un* vulnus *per il* law enforcement*?*, in G. Finocchiaro, *Diritto all'anonimato*, cit., 182 ss., l'anonimato assurge a bene tutelabile (o se si preferisce a diritto) solo in collegamento con il diritto alla *privacy*, (come « diritto strumentale alla protezione della privacy ») mentre non pare configurabile un diritto all'anonimato autonomo, in particolare facendo riferi-

o relativo [15]: ci si riferisce, insomma, al diritto di non rendere sempre e comunque nota al pubblico la propria identità, o di utilizzare uno pseudonimo, ma pur sempre nel contesto di un insieme di regole che consentono, in presenza di un utilizzo illecito della libertà di espressione, di individuare e sanzionare i responsabili [16].

Del resto, anche le più significative pronunce giurisdizionali che vengono comunemente richiamate per affermare l'esistenza di un "diritto all'anonimato", a ben vedere non si spingono al punto di affermare che la libertà di parola e di stampa prevalgano in termini assoluti sulla esigenza di individuare e perseguire gli autori di illeciti commessi attraverso la stampa o i *mass media* in generale [17].

Le cose non mutano in maniera significativa se dal mondo dei *mass media* tradizionali si passa a quello dei nuovi *media* [18]: se da

---

mento all'art. 2 cost. (che anzi sembra deporre nel senso opposto, laddove collega strettamente il riconoscimento dei « diritti inviolabili dell'uomo » al necessario adempimento dei « doveri inderogabili di solidarietà »).

[15] Anche in quello che è ad oggi il più ricco ed organico studio sul diritto all'anonimato, si muove dalla premessa che il diritto all'anonimato è un diritto « relativo »: in questo senso v. G. Finocchiaro, *Introduzione*, in G. Finocchiaro (a cura di), *Diritto all'anonimato*, cit., XVII ss., e Id., *Conclusioni*, *ivi*, 412, dove in particolare si osserva che « non esiste nell'ordinamento giuridico italiano un diritto generale all'anonimato, ma esso è declinato con riguardo a circostanze specifiche e funzionali a particolari esigenze di tutela » e si conia l'espressione « anonimato ragionevole », intesa come il massimo di tutela compatibile con le specificità del caso concreto (in senso analogo, v. già A. Candian, voce *Anonimato (diritto all')*, in *Enc. Dir.*, vol. II, Milano 1958, 499 ss.). Sulla relatività della nozione stessa di anonimato, v. E. Pelino, *La nozione di anonimo*, in G. Finocchiaro (a cura di), *Diritto all'anonimato*, cit., 31 ss.

[16] Il modello è insomma quello della disciplina della stampa, in cui è senz'altro riconosciuta la libertà di pubblicare uno scritto anonimo su un periodico, o di pubblicare un'opera avvalendosi di uno pseudonimo (diritto già riconosciuto dal r.d.l. 7 novembre 1925, n. 1950 e oggi, sia pure con formulazione più sfumata e legata al rapporto contrattuale con l'editore, dagli artt. 21 e 126 della l. n. 633 del 1941), ma a ciò si accompagnano norme stringenti sulla attribuzione della responsabilità in capo a direttore o editore (artt. 57 e 57-*bis* cod. pen.): sul punto, cfr. B. Cunegatti, *Anonimato e libertà di stampa*, in G. Finocchiaro, *Diritto all'anonimato*, cit., 254 ss.

[17] Così, le importanti affermazioni di principio contenute nella sentenza della Corte Suprema USA *McIntyre vs. Ohio Campaign Commission* (ma v. anche, per altri riferimenti alla giurisprudenza USA, M. Betzu, *Regolare internet*, cit., 142 e s.) se da un lato non hanno impedito alla giurisprudenza USA di elaborare soluzioni per sanzionare la diffamazione in forma anonima (cfr. P. Balboni, *Cenni giurisprudenziali e riflessioni sul quadro normativo italiano*, in G. Finocchiaro, *Diritto all'anonimato*, cit., 327 ss.), dall'altro neppure hanno impedito l'emanazione del *Patriot Act* e la pratica del controllo generalizzato e delle imposizioni a carico degli ISP; quanto alla Corte Suprema israeliana, è pur vero che essa, nella sua nota sentenza del 25 marzo 2010, ha riconosciuto l'esigenza di fornire all'anonimato una qualche forma di protezione giuridica, ma occorre ricordare che, nella medesima sentenza, da un lato si precisava che l'esigenza di tutelare l'anonimato viene comune meno laddove si tratti di individuare e perseguire l'autore di gravi illeciti, dall'altro non si escludeva la possibilità, da parte del legislatore, di dettare una disciplina volta a consentire l'individuazione del responsabile, anche per illeciti meramente civili (cfr. D. Bianchi, *Anonimato in Rete, libertà di espressione e identità personale. La Corte Suprema di Israele: l'anonimato rende internet ciò che è*, in *Persona e Danno* (*www.personaedanno.it*), 8 aprile 2010).

[18] Si veda, del resto, quanto si afferma nella già citata raccomandazione 3/97 del Gruppo di lavoro per la tutela delle

un lato l'utilizzo di questi ultimi si traduce in un incremento delle occasioni di manifestazione del pensiero in forma anonima, l'anonimato che contraddistingue la manifestazione del pensiero attraverso internet si configura per lo più come una situazione di fatto, non già come oggetto di una pretesa giuridicamente sanzionata [19], e ciò che può essere rivendicato, sul piano strettamente giuridico, è semmai una forma di anonimato relativo, limitato a specifiche e puntuali situazioni e tendenzialmente superabile in presenza della necessità di individuare i responsabili di attività illecite.

Se quindi, in linea generale, si può dire che la libertà di espressione non implica in assoluto la libertà di comunicare informazioni ed idee sottraendosi alla relativa responsabilità, tuttavia ci sono delle valide ragioni per cui la rivendicazione dell'anonimato, come strumento di protezione del dissenso, può trovare spazio anche all'interno di una società c.d. democratica.

Occorre innanzitutto avere chiara la percezione del contesto in cui ci si muove, caratterizzato dal progressivo costante affievolimento della distinzione tra spazio pubblico e spazio privato, e quindi tra comunicazione riservata e comunicazione pubblica: nel contesto tipico della "cittadinanza digitale", cioè di una cittadinanza disgregata e frammentata, che continuamente si ricostruisce all'interno di un numero potenzialmente infinito di "comunità di interesse", finisce per affievolirsi, se non per cancellarsi del tutto, la stessa nozione di uno "spazio pubblico" come nettamente distinto dalla sfera privata [20]. Ciò trova una precisa corrispondenza, nella comunicazione in rete, nella difficoltà di distinguere tra comunicazione in forma riservata e manifestazione del pen-

persone fisiche con riguardo al trattamento dei dati personali, relativa all'« *Anonimato su internet* » (pagg. 6-7): « come dichiarato correttamente nella "dichiarazione ministeriale di Bonn" (Dichiarazione della Conferenza ministeriale di Bonn sulle reti d'informazione globali, 6-8 luglio 1997), il principio da seguire deve essere che quando l'utilizzatore può scegliere di mantenere l'anonimato fuori della rete, tale possibilità deve sussistere anche sulla rete ».

[19] Se, come osserva E. PELINO (*L'anonimato su internet*, cit., 292), « il diritto di manifestare anonimamente il pensiero trova frequente occasione di manifestarsi nella pubblicazione di commenti ad articoli, a *post* (ossia aggiornamenti di *blog*), a filmati, e in generale in relazione a qualsiasi altro contenuto informativo pubblicato in rete » (l'A. cita in particolare, come « uno dei più cospicui esempi di anonimato positivo », l'esperienza di *Wikipedia*), è pur vero che (come correttamente osserva M. BETZU, *Regolare internet*, cit., 144) nulla lascia intendere che l'anonimato di tali forme di manifestazione del pensiero sia oggetto di una specifica tutela giuridica. Anche il gruppo di lavoro "Art. 29", quando, nel suo documento del 21 novembre 2000 sulla *Tutela della vita privata su internet*, afferma (pag. 67) l'esigenza consentire l'anonimato dell'utente che partecipa a « forum pubblici » di discussione, si riferisce ad un anonimato relativo, cioè opponibile agli altri utenti del medesimo gruppo di discussione e a terzi non qualificati, e cedevole a fronte della esigenza di individuare l'autore della comunicazione per finalità di repressione di gravi illeciti o di tutela dei diritti dei terzi.

[20] Cfr. sul punto le stimolanti riflessioni di C. FORMENTI, *Cybersoviet*, cit., 91 ss.

siero [21]: sino a che punto un documento, una informazione o una idea che viene condivisa nell'ambito di una delle infinite "comunità" che si formano in rete può rivendicare il diritto alla segretezza nei riguardi della generalità della opinione pubblica?

Se, come è chiaro, l'anonimato, ed anzi la segretezza, è una pretesa fondamentale e costituzionalmente tutelata quando si comunica riservatamente, e cessa di essere una situazione protetta quando si manifesta il pensiero, la possibilità di distinguere tra comunicazione riservata e manifestazione del pensiero presuppone che si individui con chiarezza uno spazio pubblico in cui le opinioni devono circolare e in cui si forma l'opinione pubblica: è proprio questo concetto, però, che i nuovi *media* mettono in crisi, favorendo la nascita, in luogo di uno "spazio pubblico" condiviso, di un numero potenzialmente infinito di spazi, solo parzialmente tra loro comunicanti, e di conseguenza di un numero potenzialmente infinito di "zone grigie" in cui la stessa distinzione tra comunicazione riservata e manifestazione del pensiero fa fatica ad operare.

In questo contesto, il fatto che un contenuto possa essere oggetto di condivisione e di discussione all'interno di una comunità di utenti, per quanto estesa questa possa essere, non autorizza automaticamente a concludere che lo stesso sia stato offerto alla fruizione e alla discussione della generalità della cittadinanza.

L'affievolimento della distinzione tra le due fondamentali modalità della comunicazione ha poi anche un altro fondamentale risvolto. Nello scenario dei *media* tradizionali, la distinzione tra comunicazione riservata e comunicazione pubblica si accompagnava a due modelli di garanzie ben distinti e consolidati: garanzia di segretezza per le comunicazioni private e per le scelte individuali in merito alle fonti di informazione, garanzia di libertà — e correlativa assunzione di responsabilità — per le comunicazioni pubbliche. In questo scenario, il fatto che a chi riteneva di esercitare la propria libertà di manifestazione del pensiero venisse chiesto di rendere riconoscibile la propria identità trovava la propria contropartita nella contrapposta garanzia della segretezza delle comunicazioni private e delle scelte individuali sulle fonti di informazione.

Così, il soggetto che operava la scelta sul tipo di comunicazione (pubblica o riservata) sapeva di poter contare su due distinti e contrapposti regimi di tutela: in tanto poteva accettare di doversi esporre nel momento in cui manifestava pubblicamente il proprio

[21] Su cui v. tra gli altri, da ultimo, M. Betzu, *Regolare internet*, cit., 108 ss., e M. Orofino, *L'inquadramento costituzionale del web 2.0: da nuovo mezzo per la libertà di espressione a presupposto per l'esercizio di una pluralità di diritti costituzionali*, in Aa. Vv., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Santarcangelo di Romagna 2013, 42 ss.

pensiero, in quanto sapeva di godere della garanzia della segretezza nelle sue comunicazioni riservate; non solo, ma anche le scelte che l'utente operava rispetto alle sue fonti di informazione erano coperte dalle garanzie della vita privata, sicché ognuno poteva vantare una ragionevole aspettativa ad esercitare la propria libertà di informarsi senza che le proprie inclinazioni e le proprie preferenze in questo ambito venissero esposte alla conoscenza di terzi, pubblici o privati.

Indipendentemente dal credito che si voglia prestare a quelle tesi che tendono a ricomprendere libertà di corrispondenza e libertà di manifestazione del pensiero all'interno di nuove situazioni giuridiche (dai contorni per la verità non sempre perfettamente definiti) come la « libertà della comunicazione » o la « libertà informatica » [22], è pur vero che il sistema delle garanzie, di cui fanno parte anche l'esclusione delle tutele giuridiche dell'anonimato e gli obblighi di trasparenza, o sta in piedi tutto insieme o cade tutto insieme: se non esiste più garanzia di reale segretezza delle comunicazioni riservate, e neppure delle scelte che il soggetto opera relativamente alle proprie fonti di informazione, come possiamo giustificare l'obbligo di identificazione dell'autore delle comunicazioni pubbliche?

Come si è detto, nel mondo dell'attivismo in rete è molto forte, per lo meno tra gli utenti più consapevoli e tecnologicamente preparati, la percezione di un forte incremento delle occasioni e degli strumenti di sorveglianza da parte di soggetti pubblici e privati: si tratta di preoccupazioni che, se talora sono sicuramente enfatizzate (magari ad arte, nel tentativo di sottrarsi a precise assunzioni di responsabilità in presenza di attività illecite), non sono affatto prive di fondamento, come dovrebbe essere evidente se si guarda, ad esempio, alla crescente integrazione tra *blog* e siti del più vario genere e i c.d. *social network* [23], al ricorso

[22] Il tentativo più impegnativo in questo senso è quello di A. Valastro, *Libertà di comunicazione e nuove tecnologie*, Milano 2001: sul punto v. le critiche di A. Pace, in A. Pace, M. Manetti, *La libertà di manifestazione del proprio pensiero*, Bologna 2001, 11 ss.; ad esiti non molto diversi conduce anche lo sviluppo impresso da T. E. Frosini (*Tecnologie e libertà costituzionali*, in questa *Rivista* 2003, 487 ss.) alla nozione di « libertà informatica » elaborata a suo tempo da V. Frosini (*La protezione della riservatezza nella società informatica*, in N. Matteucci (a cura di), *Privacy e banche dei dati*, Bologna 1981, 37 ss.), anch'essa sottoposta a critica da A. Pace, *op. cit.*, 159 ss.

[23] La crescente integrazione tra *blog*, siti e *social network* rappresenta uno strumento formidabile per aumentare le possibilità di profilazione dell'utente: non solo, ma grazie alla sempre maggiore interazione tra *mass media* tradizionali (a cominciare dalla televisione) e *social network* il controllo e la tracciabilità si estendono anche alle scelte relative alla visione di programmi televisivi, alla lettura di giornali, insomma a tutte le scelte che il soggetto compie relativamente alle proprie fonti di informazione. A ciò si aggiunge la crescente possibilità di profilazione dell'utenza fornita dalla diffusione della televisione via cavo e della tv *on demand* (che hanno suscitato le giuste preoccupazioni del Garante per la protezione

sempre più diffuso a strumenti di localizzazione dell'utente [24], alla gestione dei dati personali da parte di organizzazioni private dotate di grandi disponibilità economiche e di forte potere di influenza, e in grado di sottrarsi agevolmente ai vincoli imposti dalle costituzioni e dalla legislazione nazionale o regionale [25].

Il rischio di essere esposti a varie forme di rilevazione e di sorveglianza cresce, come è ovvio, man mano che l'utente della rete non si limita alla mera fruizione individuale (già peraltro esposta, come si è visto, a molteplici rischi di controllo), e, sfruttando al meglio le potenzialità offerte dal c.d. *web* 2.0, condivide contenuti e opinioni con altri utenti: se è proprio la condivisione ciò che consente di trasformare la mera fruizione passiva di contenuti ed idee in uno strumento di mobilitazione sociale, non si può ignorare il fatto che, non appena si introducono momenti di condivisione, il rischio dell'esposizione al controllo aumenta considerevolmente.

Non può quindi stupire che il ricorso a strumenti tecnologici che consentano di preservare l'anonimato in rete venga rivendicato, nel mondo dell'attivismo in rete, come una forma di legittima difesa contro il rischio della rilevazione e di una generalizzata sorveglianza, e che questo avvenga anche all'interno di ordinamenti che pure si qualificano come democratici.

Ma qual è il rischio implicato da queste accresciute possibilità di vigilanza e controllo? Se è vero che, in un regime che garantisca in modo relativamente ampio la libertà di informazione e di critica, il soggetto può aspettarsi un certo livello di protezione contro i tentativi (specie da parte dei pubblici poteri) di sanzionare l'espressione di opinioni sgradite, occorre però sempre tenere presente che i rischi di sorveglianza e controllo rispetto ai quali si invoca l'anonimato non provengono solo dal potere pubblico, ma anche dai privati, e che questo pone in modo pressante l'esigenza di una protezione dei soggetti deboli dai rischi di discriminazione e di ritorsioni (anche) da parte di soggetti privati in posizione di forza; si pensi, ad esempio, alle ritorsioni che può subire il lavoratore che critichi (magari su un *social network*) le politiche della propria azienda, o che segnali abusi, fenomeni di malcostume o comportamenti illegali [26].

---

dei dati personali: v. il provv. 3 febbraio 2005, in *Boll.* 2005, n. 58).

[24] Le cose peggiorano se da internet si passa alle altre piattaforme di comunicazioni digitale *wireless*, che sempre più utilizzano dispositivi progettati specificamente per consentire, tra l'altro, la localizzazione dell'utente.

[25] Sui rischi derivanti da « posizioni di controllo private » e dalla collaborazione tra governi e grandi multinazionali, v. E. Pelino, *L'anonimato su internet*, cit., 301 ss.

[26] Rispetto alla posizione del lavoratore, se da un lato non ci si può esimere dal chiedersi quale effettività possano ancora avere, nel mondo dei *social network*, norme come quelle dell'art. 8 dello Statuto dei lavoratori che vietano al datore di lavoro di fare indagini sulle opinioni politiche o sui

Rispetto a questo genere di rischi, l'anonimato rappresenta una forma (forse l'unica) di effettiva protezione: e se è vero che l'anonimato potrebbe anche fornire una comoda copertura per operazioni diffamatorie [27], il punto di equilibrio non può che rinvenirsi, come si avrà modo di vedere in seguito, in una equilibrata procedimentalizzazione delle richieste di *disclosure* dell'identità di chi diffonde informazioni attraverso la rete; richieste che dovrebbero passare attraverso il filtro preventivo di un giudice e di un contraddittorio, assicurando, ove possibile, anche a chi ha diffuso la notizia la possibilità di difendere le ragioni per cui preferisce mantenere l'anonimato.

Infine, dobbiamo considerare che il rischio implicato nella possibilità di monitorare le attività che gli utenti svolgono in rete non è solo quello della possibile ritorsione, da parte di poteri pubblici e privati, a fronte di opinioni e informazioni "sgradite", ma anche quello della profilazione e della manipolazione dell'u-

gusti e le inclinazioni o sulla vita privata dei dipendenti, il problema più serio appare la tutela da ritorsioni e discriminazioni del lavoratore che intenda denunciare comportamenti illeciti o scorretti all'interno dell'azienda. Negli USA, la problematica del c.d. *whistleblowing* è stata affrontata dal legislatore, dopo le gravi frodi finanziarie dei primi anni del nuovo millennio (come la vicenda *Enron*) con il *Sarbanes - Oxley Act* del 30 luglio 2002, che tra l'altro obbliga tutte le società quotate al *New York Stock Exchange* ad attivare linee riservate per la segnalazione di illeciti ed irregolarità, con la garanzia dell'anonimato per gli autori delle segnalazioni (sez. 806) e la previsione di specifiche forme di tutela contro eventuali misure ritorsive (cfr. G. Golisano, *Il whistleblowing nella giurisprudenza USA: illeciti d'impresa e posizione del lavoratore che li denuncia*, in *Il lavoro nella giurisprudenza* 2006, 937 ss.). In Europa (con l'eccezione del Regno Unito, dove è stato adottato il *Public Interest Disclosure Act* che reca previsioni analoghe), il tentativo di attivare simili meccanismi incontra difficoltà anche legate alla disciplina europea della protezione dei dati personali (cfr. A. Rodolfi, *Whistleblowing 2.0. Le "soffiate" tra opportunità di* community *etiche e problematiche giuridiche*, in *Cyberspazio e diritto*, 2011, n. 3, 289 ss.): con proprio parere del 1º febbraio del 2006, il Gruppo dei Garanti europei costituito ai sensi dell'art. 29 della direttiva 95/46/CE ha fornito alcune indicazioni per rendere i trattamenti di dati personali effettuati attraverso tali sistemi di segnalazione conformi ai princìpi europei in tema di *privacy*; per quanto riguarda l'Italia, il Garante per la protezione dei dati personali ha rivolto, in data 10 dicembre 2009, una segnalazione a Parlamento e Governo sulla opportunità di adottare una specifica disciplina sul punto, specialmente al fine di tutelare l'anonimato del denunciante a fronte di eventuali richieste di accesso provenienti dai soggetti denunciati. Allo stato, oggi l'unica forma di riconoscimento legislativo del fenomeno del *whistleblowing* (come strumento per segnalare fenomeni di malcostume all'interno della pubblica annninistrazione) è rappresentata dall'art. 1, comma 51 della legge n. 190 del 2012 (rubricato « *Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione* », che, introducendo l'art. 54-*bis* nel d. lgs. n. 165 del 2001, offre una qualche forma di tutela al « dipendente pubblico che segnala illeciti », prevedendo che, salve le ipotesi di responsabilità a titolo di calunnia o diffamazione, il pubblico dipendente che denuncia condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro non può essere sanzionato, licenziato o sottoposto a misure discriminatorie dirette o indirette, e ne salvaguarda in qualche misura anche l'anonimato.

[27] Simili preoccupazioni sono quelle che hanno indotto ad es. la *Commission Nationale de l'Informatique e des Libertés* a opporsi in diverse occasioni all'attivazione presso aziende con sede in Francia di linee riservate per segnalazioni sul modello di quelle previste dal *Sarbanes - Oxley Act*, evidenziando il rischio che il sistema si traducesse in un meccanismo di delazione permanente (G. Golisano, *Il whistleblowing*, cit., 944).

tente (anche a fini politici): in questa prospettiva, l'anonimato non è solo un modo per eludere le responsabilità che discendono dall'esercizio della libertà di espressione: esso è anche invocato come strumento di difesa, non solo dalla censura (nelle infinite possibilità, più o meno sotterranee, che la rete offre) e da possibili ritorsioni da parte di soggetti pubblici o privati, ma anche dagli enormi rischi di manipolazione e di condizionamento che le nuove tecnologie dell'informazione recano con sé [28].

3. Tutela dell'anonimato e regimi non democratici: i « rifugiati digitali ».

Se le considerazioni fin qui svolte consentono di comprendere per quali ragioni e entro quali limiti una relativa tutela dell'anonimato possa essere rivendicata anche all'interno di ordinamenti che si definiscono democratici, la dimensione in cui l'anonimato può svolgere un ruolo determinante, nella protezione del dissenso politico, è ovviamente quella dei regimi autoritari: quando ci si rapporta al problema del dissenso nei regimi non democratici, e al ruolo che in questo ambito possono svolgere le nuove tecnologie dell'informazione e della comunicazione, è bene, peraltro, guardarsi dal rischio di cadere in facili luoghi comuni e generalizzazioni.

Il primo luogo comune che occorre sfatare è quello secondo cui i regimi autoritari sarebbero per lo più regimi tecnicamente arretrati, disinformati e inclini solo a limitare l'accesso ad internet o a censurare l'espressione di opinioni sgradite, sicché basterebbe promuovere la diffusione delle nuove tecnologie, e metterle al riparo da interventi censori da parte delle autorità locali, per contribuire alla crisi dei regimi autoritari, al rafforzamento del dissenso e alla diffusione della democrazia [29].

Quando si enfatizza il ruolo determinante che i c.d. nuovi *media* avrebbero avuto nel contribuire alla caduta di alcuni regimi autoritari [30], effettivamente si evidenzia una sostanziale incomprensione e svalutazione delle potenzialità del mezzo da parte di quei regimi, ma si rischia di perdere di vista il fatto che, all'in-

[28] Cfr. S. Niger, *Sorveglianza e nuovi diritti di libertà*, cit. 12.

[29] Quanto una simile visione sia superficiale, sbagliata e fuorviante è messo bene in luce, da ultimo, da E. Morozov, *L'ingenuità della rete. Il lato oscuro della libertà di internet*, Torino 2011.

[30] Il caso più recente ed enfatizzato è ovviamente quello delle c.d. "primavere arabe", anche se, a distanza di qualche tempo, gli entusiasmi originari dovrebbero forse essere ridimensionati, sotto almeno due profili: in primo luogo, perché è tutto da dimostrare che il ruolo delle nuove tecnologie sia stato veramente determinante, dal momento che movimenti popolari che hanno portato al sovvertimento di regimi autoritari ci sono sempre stati, sin dagli albori della storia e in contesti tecnologici del tutto differenti (del resto, lo stesso M. Castells, *Reti di indignazione e speranza*, cit., 38 ss., evidenzia come al successo delle rivolte nordafricane abbiano concorso molteplici fattori, tra cui, oltre alle iniziative di singoli e di comunità di *hacker* e di ISP di altri paesi, un ruolo decisivo fu svolto anche

terno di numerosi regimi non democratici o solo parzialmente democratici, il rapporto tra i detentori del potere politico e i mezzi di comunicazione è assai più articolato e complesso.

Mano a mano che si diffonde la consapevolezza delle potenzialità dei c.d. nuovi *media*, si diffonde anche, da parte di quei regimi che perseguono l'obiettivo di imbrigliare, stroncare o comunque rendere inoffensiva ogni forma di dissenso politico, la consapevolezza che i c.d. nuovi *media* non sono solo potenziali veicoli di dissenso, ma anche efficaci strumenti per controllarlo e minimizzarne l'impatto, e per condizionare, manipolare o anestetizzare l'opinione pubblica.

In questa prospettiva, piuttosto che cercare (inutilmente) di ostacolare l'accesso ad internet (il che, tra l'altro, appare per lo più impraticabile anche per il rilevante costo economico che comporta) [31], un regime autocratico consapevole tenderà, piuttosto, a promuovere l'utilizzo delle nuove tecnologie, al fine di sfruttarne a proprio vantaggio tutte le potenzialità: la possibilità di distrarre la cittadinanza e di distoglierla dall'impegno politico, inondandola con dosi massicce di intrattenimento a buon mercato; la possibilità di esercitare una massiccia sorveglianza su tutto ciò che accade in rete, monitorando la comparsa di focolai di ribellione e rendendone più agevole il controllo e, ove occorra, la repressione; infine, la possibilità di disporre di uno strumento di propaganda diffusa e decentralizzata, assai più efficace di quella diffusa da *media* tradizionali apertamente filogovernativi [32].

Quindi, le strategie occidentali per sostenere il dissenso sono del tutto inadeguate nel momento in cui si rifugiano nella comoda illusione secondo cui basterebbe promuovere ed assicurare l'ac-

da *mass media* tradizionali, come l'emittente televisiva *Al Jazeera* e altre televisioni arabe, che continuarono a diffondere immagini e notizie delle contestazioni nonostante il tentativo delle autorità di passarle sotto silenzio); in secondo luogo, perché gli sviluppi successivi alla caduta dei regimi autoritari, almeno in alcuni paesi, sembrano confermare che, una volta conseguito l'obiettivo del rovesciamento del regime, il ruolo dei nuovi *media* nel promuovere forme democratiche di partecipazione è decisamente meno incisivo di quanto lo si voglia far apparire nelle fasi c.d. "rivoluzionarie". È del resto ormai una constatazione diffusa — e avvalorata da molteplici esperienze concrete — quella secondo cui le tecnologie dell'informazione, se possono svolgere un ruolo decisivo nel contribuire alla crisi di un regime autoritario e all'affermazione di nuovi equilibri politici, rivelano una assai minore efficacia nell'organizzare e costruire forme di partecipazione democratica in situazioni di "normalità".

[31] Come osserva ancora M. Castells, *Reti di indignazione e speranza*, cit., 42, alla base del fallimento del tentativo di oscuramento delle comunicazioni in rete compiuto dal governo egiziano ai tempi delle rivolte, conclusosi con la revoca del blocco dopo appena 5 giorni, ci furono anche, se non soprattutto, ragioni economiche: « secondo l'organizzazione per la cooperazione e lo sviluppo economico (OCSE), i cinque giorni di blocco dell'accesso ad internet provocarono una perdita di circa 90 milioni di dollari USA di ricavi in seguito all'arresto delle telecomunicazioni e dei servizi di internet, pari a circa 18 milioni al giorno e al 3-4 per cento del PIL annuo egiziano ».

[32] Per numerosi esempi in proposito, tratti soprattutto dall'esperienza dei paesi dell'est europeo e della Russia, ma anche di alcune aree del sud America e dell'estremo Oriente, v. ancora E. Morozov, *L'ingenuità della rete*, cit.

cesso alla rete, e ridurre al minimo la possibilità di interventi censori, per rafforzare i movimenti di opposizione: se, come pare, i pericoli sono molto più vari, articolati e sottili, varia, articolata e sottile deve essere una strategia che voglia fornire una qualche forma di sostegno al "dissenso digitale".

Sicuramente, uno degli strumenti attraverso cui i regimi democratici possono sostenere e promuovere il dissenso nei regimi non democratici può consistere nel mettere a disposizione spazi di espressione del dissenso (*blog*, siti di discussione e di informazione, spazi per pubblicazione di documenti e testimonianze, ecc.) allocati su *server* posti fuori dal controllo dei governi autoritari e dei loro servizi di sicurezza e polizia: occorrerà però che tali spazi siano protetti e gestiti con estrema cautela, anche dal punto di vista delle garanzie dell'anonimato, per evitare che si trasformino in preziose miniere di informazioni per l'*intelligence* dei regimi autoritari.

Non sembra fuori luogo chiedersi se simili spazi di dissenso politico, e i soggetti che, usufruendone, vengono a configurarsi come dei veri e propri « rifugiati digitali » [33], possano ricevere una speciale protezione, che includa anche l'anonimato sull'identità di chi pubblica e di chi li consulta: una interpretazione evolutiva della disposizione costituzionale in tema di asilo (art. 10, comma 3, cost.) potrebbe probabilmente fornire la copertura necessaria per un regime normativo anche derogatorio rispetto alle regole generali in tema di individuazione dei responsabili [34].

Sotto tale profilo, però, è sempre bene ricordare che le maggiori difficoltà provengono (ancora una volta) non solo e non tanto dal potere pubblico, quanto dagli stessi soggetti imprenditoriali privati, che appaiono spesso riluttanti a fornire adeguate garanzie, sia per il timore di ritorsioni, sia per il rischio di subire attacchi informatici che possono provocare un danno economico considerevole [35]: occorre insomma rendersi conto che oggi la censura nel *web* non viene dal solo potere pubblico, ma anche dai privati, che

[33] L'espressione è sempre di E. Morozov, *L'ingenuità della rete*, cit., 100 ss.

[34] Si pensi all'art. 17, comma 2, lett. *b*) del d. gls. n. 70 del 2003, che, in applicazione della facoltà consentita agli Stati dall'art. 15, comma 2, della direttiva 2000/31/CE, impone al *provider* l'obbligo di « fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite ».

[35] È ancora E. Morozov (*L'ingenuità della rete*, cit., loc. cit.) a segnalare come, per varie ragioni (timore di offrire ospitalità a terroristi, desiderio di evitare problemi giudiziari o ritorsioni commerciali, applicazione ottusa di restrizioni commerciali imposte nei confronti di paesi autoritari, ecc.), molti *provider* occidentali rifiutino addirittura di fornire ospitalità a cittadini di paesi autoritari. Lo stesso A. osserva anche come i siti dei c.d. "rifugiati digitali" spesso siano oggetto di attacchi informatici secondo il metodo DDOS (*distributed denial of service*): il sito viene "assalito" da migliaia di visitatori sino a renderlo inaccessibile agli altri utenti, arrecando ingenti danni al *provider* che lo ospita e costringendo ad una costosa operazione di ripristino. Se da un lato i costi di ripristino e di difesa sono tali

si auto — censurano per evitare danni economici o che censurano altri siti (mediante la pratica dei « *cyber* attacchi ») per ragioni commerciali o anche politiche [36].

4. Contraddizioni e ambiguità dell'anonimato nella manifestazione del dissenso politico.

Se per le ragioni viste possiamo affermare che una forma, almeno relativa, di tutela dell'anonimato può avere fondate giustificazioni, ci si deve guardare anche dal coltivare l'illusione che l'anonimato sia la soluzione di tutti i problemi: ci sono, in effetti, numerosi elementi di ambiguità e contraddizioni, che rendono il discorso sull'anonimato particolarmente complesso.

Innanzitutto occorre segnalare una ambiguità di fondo, spesso presente nel riferimento alla *privacy*: si invoca la *privacy* per sfuggire al controllo, ma spesso chi invoca la *privacy* lo fa nel momento stesso in cui la sta violando, ad esempio mettendo *on line* i dati identificativi di funzionari sospettati di aver commesso abusi, divulgando documenti che contengono dati personali, svelando informazioni riservate a vario titolo, dal segreto industriale al segreto professionale e d'ufficio.

A tale proposito, sembra nulla più che una comoda scappatoia la risposta che consiste nel cambiare i termini del problema, collegando l'alternativa tra tutela dell'anonimato e trasparenza non più al dualismo tra comunicazione riservata e manifestazione del pensiero, ma alla distinzione tra singoli cittadini e detentori del potere, all'insegna dello slogan che recita « *privacy* per i deboli, trasparenza per i potenti » [37]: e in effetti, una volta escluso — per le ragioni che abbiamo visto — che i « potenti » siano solo

---

che i *provider*, anche in paesi c.d. democratici, potrebbero essere disincentivati dall'offrire spazi del genere per mere ragioni economiche, d'altro canto l'attrezzatura necessaria per lanciare un attacco DDOS ha un costo relativamente contenuto, sicché attacchi del genere potrebbero essere lanciati anche dai privati (es. privati sostenitori di un regime autoritario) e non solo dagli stati: un esempio di censura che non proviene necessariamente da un potere pubblico, ma che produce gli stessi effetti della chiusura di un sito disposta dalle autorità, oltretutto senza nessuna precisa assunzione di responsabilità al riguardo. Per inciso, si assiste qui al singolare paradosso per cui la pratica dei c.d. « *cyber* attacchi », che è un classico strumento di lotta dell'attivismo digitale (come dimostra l'esperienza del collettivo *Anonymous*) e che talora, se limitata nel tempo, con scopi essenziahnente dimostrativi e senza rilevanti danni alle strutture attaccate, è stata ritenuta legittima (al pari di un "*sit in* digitale", che blocca temporaneamente l'accesso ad uno spazio pubblico) può essere utilizzata dagli stessi regimi autoritari per "dare in *outsourcing*" la censura e per colpire il dissenso.

[36] Assume così un particolare rilievo l'osservazione (fatta ad es. da P. Balboni, *Cenni giurisprudenziali*, cit., 333), secondo cui, per quanto un ISP non possa essere obbligato a rivelare i dati identificativi di un utente senza un ordine dell'autorità, peraltro non gli è nemmeno vietato di farlo (indipendentemente dal consenso dell'interessato, come ad esempio di fronte a richieste volte a far valere un diritto in sede giudiziaria: v. art. 24, comma 1, lett. *f*), d. lgs. 196/2003).

[37] Per richiamare ancora una espressione utilizzata in J. Assange, *Internet è il nemico*, cit., 133.

le strutture pubbliche, il problema è quello di capire chi sono i « deboli » e chi sono i « potenti », specie di fronte a soggetti che operano sotto la protezione dell'anonimato.

L'uso di tecniche di manipolazione e di propaganda particolarmente sofisticate e subdole può, in effetti, rendere quanto mai problematico differenziare la propaganda di governi o di grandi centri di potere privato dalla libera manifestazione di pensiero dei singoli cittadini [38], e tale difficoltà non può che essere aggravata, come è chiaro, proprio dal ricorso all'anonimato: si realizza quindi l'ulteriore ed ennesimo paradosso per cui l'anonimato, invocato come mezzo di protezione del dissenso, può essere anche uno strumento al servizio della propaganda, della disinformazione e del potere; proprio il ricorso all'anonimato può rendere particolarmente agevole effettuare operazioni di manipolazione del consenso, di disinformazione, di distruzione della reputazione di soggetti pubblici o privati.

Vi è poi un altro elemento di ambiguità, o meglio una contraddizione interna, rispetto alla pretesa all'anonimato rivendicata dai movimenti che operano attraverso la rete: questi movimenti, infatti, puntano molto sul concetto di condivisione, sulla trasparenza, sul rifiuto di qualsiasi *leadership* e sul carattere aperto ed assembleare, cioè esibiscono caratteristiche che postulano una struttura aperta, un elevato livello di trasparenza, e che potrebbero risultare incompatibili con un forte ricorso agli strumenti che garantiscono l'anonimato in rete [39].

Non è un caso che gli strumenti più utilizzati dai movimenti che utilizzano la rete come strumento di mobilitazione di massa siano i c.d. *social network*, cioè strumenti che, come uno dei più attenti studiosi dei mutamenti sociologici indotti dalle nuove tecnologie non ha mancato di sottolineare, sono radicalmente incompatibili con l'anonimato [40].

---

[38] V. ad es. la vivace descrizione di come, in Russia, le forze al governo abbiano saputo abilmente ed efficacemente integrare ed utilizzare a fini propagandistici la cultura digitale, in E. Morozov, *L'ingenuità della rete*, cit., 116 ss.

[39] Occorre qui operare un distinzione tra i movimenti di massa e le *élites* tecnologiche di avanguardia, incarnate da entità collettive come *Anonimous* e *Wikileaks* (anche se la struttura di quest'ultima organizzazione appare molto più centralizzata): queste ultime, pur professandosi del tutto contrari ad ogni forma di leaderismo e di avanguardia, di fatto esercitano proprio il ruolo delle avanguardie, di *élites* tecnologicamente avanzate e competenti che, sfruttando al meglio le potenzialità della rete, stimolano e in qualche modo orientano l'azione dei movimenti di massa, composti, invece, prevalentemente di cittadini che aspirano a condividere, e quindi non utilizzano le tecniche crittografiche quanto, piuttosto, i *social network*.

[40] Osserva M. Castells, *Reti di indignazione e di speranza*, cit., 194, che « la chiave per il successo di un *social network* non sta nell'anonimato, bensì, al contrario, nell'autopresentazione di una persona reale che sviluppa rapporti con altre persone reali. Si creano reti per stare con gli altri, e con altri che vogliamo avere vicini, avendo come criterio quello di includere persone che già si conoscono o che vorrennno conoscere ». Non può non suscitare, peraltro, qualche perplessità l'entusiasmo con cui

Se per le ragioni ora esposte la rivendicazione dell'anonimato rischia di entrare in conflitto con la cultura della condivisione che caratterizza i movimenti sociali in rete, depotenziando l'efficacia della loro azione, d'altro canto la pretesa all'anonimato appare in piena continuità con il netto rifiuto della idea di organizzazione che caratterizza i movimenti in rete, i quali agiscono in modo magmatico ed indifferenziato, rifiutando ogni *leadership* ed ogni forma di mediazione e di rappresentanza: resta da chiedersi, peraltro, se anche questo aspetto non rischi di depotenziare l'efficacia della loro azione, dando vita a forme di impegno discontinuo, a corrente alternata, evanescente, svincolato da una precisa assunzione di responsabilità [41].

In conclusione si può dire che, se esistono fondate ragioni per rivendicare qualche forma di tutela dell'anonimato in rete, d'altro canto occorre tenere presente che l'anonimato non è la soluzione di tutti i problemi, per diverse ragioni: in primo luogo, perché più si diffonde la rivendicazione dell'anonimato, più si rafforzano, per contrasto, le posizioni di coloro che auspicano l'estensione dei controlli e della sorveglianza; in secondo luogo, perché l'anonimato può coprire e agevolare anche il controllo e il condizionamento dell'opinione pubblica in rete; infine, perché l'anonimato restringe la condivisione, crea un clima di sospetto e di cospirazione permanente e generalizzato che impedisce a chi dissente di uscire allo scoperto, e alla lunga limita e indebolisce l'azione dei movimenti nella società [42].

5. Quali strumenti per difendere l'anonimato? La protezione delle fonti, la responsabilità e il ruolo degli intermediari.

Si rende a questo punto necessario interrogarsi sugli strumenti su cui l'ordinamento e i singoli possono fare affidamento per assicurare un adeguato bilanciamento tra l'esigenza di proteggere

l'Autore (*ivi*, 193 ss.) saluta la "svolta" avvenuta nel primo decennio del nuovo millennio, con l'emergere, appunto, del *web* 2.0 e dei c.d. *social network*, di cui si esaltano gli aspetti di spontaneità, lasciando decisamente in secondo piano il ruolo dei soggetti imprenditoriali che predispongono e gestiscono le relative piattaforme e degli interessi economici sottostanti.

[41] È ancora E. Morozov, *L'ingenuità della rete*, cit., 167 ss., che, in modo alquanto provocatorio, stigmatizza la pretesa a fare i dissidenti rifugiandosi dietro all'anonimato, paragonando quelli che definisce « dissidenti da poltrona », ai dissidenti dei regimi dell'est Europa degli anni settanta che, invece, proprio nel momento in cui rischiavano (e spesso subivano) la repressione, contemporaneamente rappresentavano un esempio e un punto di riferimento per i movimenti di opposizione.

[42] Senza tener conto dell'ulteriore problema, di grande interesse ma che richiederebbe ben altro spazio, della possibile applicazione, ai *network* anonimi in rete, dei divieti costituzionali delle associazioni segrete e delle associazioni che perseguono scopi politici mediante una organizzazione di tipo militare (su cui v. S. Sassi, *La libertà di associazione nel "nuovo ecosistema mediatico": spunti problematici sull'applicazione dell'art. 18 della costituzione. Il (recente) caso dell'associazione xenofoba* on - line, in *Rivista telematica giuridica dell'Associazione Italiana dei Costituzionalisti (www.associazionedeicostituzionalisti.it)*, n. 2/2013, 6 e s.).

l'anonimato e l'esigenza, almeno altrettanto rilevante (ed anzi, l'unica cui la costituzione attribuisce espressamente rilievo) di individuare e perseguire i responsabili di comportamenti illeciti.

Un primo interrogativo che occorre porsi concerne la liceità dell'utilizzo degli strumenti che la tecnologia mette a disposizione a chi voglia preservare il proprio anonimato in rete [43]: ci si deve chiedere, in altri termini, se il ricorso alla crittografia e alla cifratura, oggi sempre più esteso ed accessibile anche da chi non disponga di particolari conoscenze tecniche o di ingenti risorse economiche, possa o meno considerarsi un diritto per chi comunica attraverso gli strumenti telematici.

Sulla base del vigente quadro costituzionale, non pare vi siano margini per l'imposizione di divieti generalizzati all'utilizzo di simili strumenti: se è vero che essi possono essere utilizzati anche come copertura per attività illecite, è vero che lo stesso può dirsi di ogni spazio e di ogni strumento rispetto al quale la costituzione garantisce un ambito di segretezza e riservatezza [44].

Gli strumenti tecnici che proteggono la segretezza e l'anonimato delle comunicazioni *on line* hanno come obiettivo primario la protezione di un valore costituzionalmente protetto quale è la libertà e la segretezza della corrispondenza; ed anzi, proprio il ricorso a simili tecnologie, da parte di chi esercita la libertà di comunicazione attraverso la rete, può costituire un valido indice ai fini dell'inquadramento costituzionale dell'attività, tra le forme di comunicazione riservata soggetta alle garanzie dell'art. 15 cost. piuttosto che nell'area della manifestazione del pensiero di cui all'art. 21 cost. [45].

Il problema sorge, ovviamente, quando i materiali che circolano riservatamente divengono pubblici, e sono offerti alla conoscenza ed alla condivisione generalizzata della collettività: è in effetti questo il momento in cui si può porre il problema di contemperare la pretesa all'anonimato di un soggetto, che comunque intende dare la massima pubblicità a un'informazione o a un'idea, con l'esigenza dell'individuazione del responsabile, finalizzata alla

---

[43] Ad esempio, si può fare riferimento alla tecnologia TOR, oggi largamente utilizzata, e che consente, anche a chi non possieda conoscenze informatiche particolarmente approfondite o significative risorse economiche, di conservare un livello sufficientemente elevato di protezione dell'anonimato.

[44] Così, per esemplificare, il fatto che all'interno di un domicilio privato possano svolgersi attività illecite non legittima certo a mettere in discussione la sua inviolabilità; ancora, la corrispondenza rimane segreta indipendentemente da fatto che proprio avvalendosi di tale segretezza sia possibile compiere reati.

[45] Cfr. in questo senso le persuasive argomentazioni di M. Betzu, *Regolare Internet*, cit., 108 ss., che nel constatare l'inadeguatezza, rispetto alle tecnologie digitali, del tradizionale criterio ermeneutico di distinzione tra l'ambito di applicazione dell'art. 15 e dell'art. 21 cost. fondato sulla determinatezza dei destinatari, propone di attribuire rilievo decisivo, a tali fini, alle scelte del soggetto attivo, cd in particolare alla scelta di utilizzare modalità tali da rendere, o meno, il contenuto della comunicazione « conoscibile da parte di terzi estranei » (126).

protezione dei diritti dei terzi a fronte della diffusione di contenuti lesivi.

Nel problematico tentativo di raggiungere un punto di equilibrio tra questi contrapposti interessi, può essere di aiuto il riferimento al tema, assai caro come è noto alla giurisprudenza della Corte europea dei diritti dell'uomo, della protezione delle fonti giornalistiche [46]: è nella giurisprudenza in materia di protezione delle fonti, in effetti, che si rinviene oggi il punto più avanzato di equilibrio tra l'esigenza dell'anonimato e l'esigenza di tutelare i diritti dei terzi che, a vario titolo, possono essere messi in pericolo dalla indiscriminata diffusione di informazioni false.

Il ricorso alle categorie della protezione delle fonti presuppone, peraltro, che si valorizzi il ruolo che, nella relazione tra chi diffonde una notizia o un'idea e il destinatario della comunicazione, è svolto dall'intermediario, e in particolare da un intermediario *professionale*: presuppone, cioè, che si esca dalla prospettiva, alquanto semplicistica e molto probabilmente fuorviante, di chi continua a vedere nella comunicazione in rete una comunicazione che può fare a meno degli intermediari.

Come si è già avuto modo di accennare, la rete è sempre meno quella struttura leggera e "stupida" magistralmente descritta da Lessig [47], incapace di selezionare e distinguere i contenuti, e in cui le scelte fondamentali sono tutte compiute dai terminali, da chi immette e da chi riceve i dati: la circolazione delle informazioni e delle idee in rete passa sempre più attraverso l'intervento di grandi intermediari (a cominciare da motori di ricerca e *social network*) che organizzano, selezionano e gestiscono le informazioni e i dati in modo (spesso) indipendente dalle scelte del singolo utente [48]. In questo contesto, negare il ruolo degli intermediari significa solo creare le condizioni perché simili operazioni di selezione avvengano al di fuori di qualsiasi controllo, in modo non trasparente e rispondendo agli interessi e alle finalità più disparate: pensare che dietro l'intelligenza della rete ci sia solo l'« intelligenza collettiva » degli utenti, e non l'attività di soggetti consapevoli ed organizzati, e portatori di enormi interessi, innan-

[46] Sull'argomento, anche per una ricognizione della evoluzione della giurisprudenza della Corte europea in materia, v. G. E. Vigevani, *La protezione del segreto del giornalista al tempo di internet*, in *www.costituzionalismo.it*, 2011.

[47] Il termine « network sciocco » o « stupido » è utilizzato da L. Lessig (*Il futuro delle idee*, Milano 2001, 42), in contrapposizione all'idea di una rete « intelligente », per descrivere l'architettura tipica di internet (almeno per come si è configurata agli inizi), in cui tutte le funzioni complesse sono svolte dai terminali e la rete si limita a veicolare, nel modo più neutrale e semplice possibile, i pacchetti di dati, senza operare alcuna selezione o scelta di sorta.

[48] Come si è detto, tale processo di progressiva "espropriazione" delle funzioni complesse dalle "periferie" a vantaggio del "centro" (o meglio della rete in sé, attraverso l'integrazione dell'attività degli utenti nei grandi nodi che gestiscono la circolazione delle informazioni) sembra destinato ad incrementarsi, tanto più dà credito a come viene rappresentata la transizione al c.d. « *web* 3.0 ».

zitutto (ma non necessariamente solo) economici, si rivela una colossale ingenuità.

Al contrario, valorizzare il ruolo di una intermediazione professionale, che operi in maniera trasparente e sulla base di regole deontologiche riconosciute, significa non solo creare le condizioni per una fruizione consapevole del mezzo, ma anche, appunto, creare le condizioni per assicurare un adeguato contemperamento tra l'esigenza di anonimato e quella della massima diffusione di notizie attendibili e documentate.

La funzione degli intermediari professionali è infatti centrale sotto diversi aspetti: in primo luogo, perché l'intermediario può sottoporre ad una seria verifica l'attendibilità delle informazioni che vengono portate a conoscenza dell'opinione pubblica, evitando il rischio della disinformazione e della manipolazione; in secondo luogo, perché l'intermediario, oltre alla autenticità, verifica la rilevanza dei materiali e soprattutto li organizza, coordina e seleziona, al fine di renderli comprensibili per l'opinione pubblica ed evitare fraintendimenti; infine, perché il ricorso ad un intermediario professionale può rappresentare un efficace strumento per assicurare un adeguato livello di protezione delle fonti, fornendo contemporaneamente un centro di imputazione di responsabilità in relazione alla autenticità dell'informazione, alla sua rilevanza per l'interesse pubblico, alla sua corretta presentazione.

La giurisprudenza della Corte europea, come è noto, attribuisce grande rilievo alla garanzia della protezione delle fonti giornalistiche, come diritto-dovere del giornalista, e in particolare ne ha esteso progressivamente l'ambito oggettivo di applicazione: dalla proclamazione della contrarietà alla Convenzione dell'ordine, rivolto al giornalista, di rivelare il nominativo della propria fonte, si è giunti a mettere in dubbio la liceità di ogni azione, anche puramente intimidatoria, che possa mettere in pericolo l'anonimato della fonte o anche solo incrinare la fiducia, in altre potenziali fonti confidenziali, sul rispetto da parte del giornalista del vincolo di confidenzialità [49]; con riferimento invece all'estensione soggettiva della garanzia, occorre chiedersi se essa possa essere invocata anche da chi non sia qualificabile come giornalista professionista in senso stretto [50].

[49] V. sul punto G. E. Vigevani, *La protezione del segreto del giornalista*, cit., 5 ss., che osserva come, pur nel silenzio del legislatore, anche la giurisprudenza italiana sembra aver accolto, almeno in parte, le indicazioni della Corte europea, progressivamente estendendo la portata oggettiva della protezione.

[50] Sul punto, come è noto, il legislatore italiano ha operato una scelta oltremodo restrittiva, circoscrivendo la possibilità di opporre il segreto (art. 200 cod. proc. pen.) al solo « giornalista professionista », con esclusione, quindi, non solo dell'autore occasionale, ma anche di pubblicisti e praticanti; diverso (sin dalla sentenza *Goodwin*

Al riguardo, fermo restando che la delimitazione, operata dal nostro ordinamento, ai soli giornalisti iscritti all'albo come professionisti (con esclusione quindi dei praticanti e dei pubblicisti, oltre che di eventuali altre figure di operatori professionali dell'informazione) è sicuramente in contrasto con le indicazioni che vengono dalla Corte europea, d'altra parte non pare possa prescindersi dal richiedere, a chi voglia avvalersi del diritto-dovere di protezione delle fonti, una qualche forma di qualificazione professionale, pur se da accertarsi secondo criteri sostanziali e non meramente formali; occorre, cioè, che chi pretende di avvalersi della protezione delle fonti sia un soggetto che opera, nel mondo dell'informazione e della comunicazione, in modo professionale e non meramente occasionale.

E significativo che le raccomandazioni degli organismi del Consiglio d'Europa in materia di protezione delle fonti giornalistiche, pur ammettendo l'esigenza di non irrigidire in gabbie formali la definizione di giornalista, e di estendere la protezione a figure che in vario modo siano coinvolte nell'attività giornalistica pur non essendo giornalisti in senso stretto e a chi opera attraverso i nuovi *media* elettronici, tuttavia ribadiscano la necessità di richiedere un minimo di qualificazione professionale in capo a chi intende valersi del beneficio [51].

Tale limitazione, per quanto possa sembrare in contrasto con l'immediatezza del collegamento, da sempre operato dalla Corte

c. *Regno Unito* del 27 marzo 1996) è l'orientamento della giurisprudenza della Corte europea, che ha esteso l'ambito della tutela anche ad altri soggetti, pur senza arrivare ad una estensione indiscriminata a chiunque eserciti, anche occasionalmente, la libertà di espressione, e continuando a richiedere un minimo di professionalità (sul punto v. le osservazioni critiche di G. E. VIGEVANI, *La protezione del segreto del giornalista*, cit., 15, che, anche alla luce di esperienze recenti come quella di *Wikileaks*, si chiede se sia ancora « ragionevole e realistico differenziare la posizione del giornalista rispetto a quella di qualsiasi altro cittadino o straniero che attraverso l'esercizio della libertà di espressione contribuisca alla produzione, elaborazione o diffusione dell'informazione »).

[51] Si v. la Raccomandazione n° R(2000)7 del Consiglio dei Ministri, adottata l'8 marzo 2000, che, pur riconoscendo (principio 2) che della protezione delle fonti dovrebbero beneficiare anche « le altre persone che, attraverso le loro relazioni personali con i giornalisti, vengono a conoscenza di informazioni identificanti una fonte attraverso la raccolta, il trattamento editoriale o la pubblicazione di dette informazioni » (in questo senso si richiama la sentenza *De Haes e Gijsels c. Belgio*, del 24 febbraio 1997), e pur sottolineando la necessità di adottare un approccio sostanziale nella definizione di chi possa ritenersi giornalista, e di estendere la protezione anche a persone giuridiche come le case editrici o le agenzie di stampa e a chi opera attraverso i nuovi *media*, ribadisce che, pur senza che debbano ritenersi necessari « un accreditamento od un'affiliazione professionale », tuttavia « un certo carattere professionale dovrebbe essere richiesto » (nel senso che « un giornalista, di norma, lavori regolarmente e riceva una qualche forma di remunerazione per il suo lavoro »), e che « degli individui che in altre circostanze non si considererebbero dei giornalisti non devono avere la qualifica di giornalisti ai fini della presente Raccomandazione » (ad es. si citano « le persone che scrivano delle lettere al redattore capo di un organo di stampa, che figurino come invitati a programmi radiotelevisivi o che partecipino a dei forum di discussione per mezzo di media accessibili attraverso mezzi informatici »), precisando che « limitare questa protezione ai giornalisti, così come sono sopra definiti, faciliterà

europea, tra protezione delle fonti e libertà di espressione (pacificamente riconosciuta a qualunque individuo, e non certo solo agli operatori professionali dell'informazione), appare tuttavia pienamente condivisibile nel momento in cui attribuisce il dovuto rilievo, oltre che alla libertà di « comunicare » informazioni e idee, anche alla libertà di « ricevere » le informazioni (e cioè al diritto della collettività ad un'informazione corretta) e all'inscindibile profilo dei « doveri » e delle « responsabilità » che non a caso la Convenzione stessa ingloba nella garanzia della libertà di espressione.

La protezione delle fonti, anche per il suo carattere di norma di privilegio, non può non accompagnarsi all'obbligo di assumersi la responsabilità di quanto si pubblica, nei limiti, ovviamente, del diritto di cronaca: il soggetto che si fa carico della diffusione al pubblico di una informazione o di un documento (che sia un giornale, un editore, un singolo individuo, il responsabile di un sito *web*), in tanto può rivendicare il diritto di non rivelare il nominativo della fonte (così come quello di pubblicare documenti riservati, se sussistono gli estremi del diritto di cronaca o di critica) in quanto si assuma la piena responsabilità di quanto pubblica, ed è quindi tenuto a un lavoro di ricerca particolarmente scrupoloso per verificarne l'attendibilità e la rilevanza (nei termini, ormai usuali nel linguaggio della Corte, della « idoneità a contribuire al dibattito su questioni di pubblico interesse ») [52].

In altri termini, la contropartita del privilegio consistente nel poter rivendicare la protezione della fonte è rappresentata dallo scrupoloso adempimento del dovere di discernere il vero dal falso, il rilevante dall'irrilevante, e anche di assicurare che la presentazione di fatti, notizie, documenti avvenga con modalità tali da consentirne una adeguata comprensione da parte del pubblico [53].

Insomma, anche nel mondo dei nuovi *media* non solo rimane,

egualmente l'equilibrio tra diritti e valori che possono essere antinomici ». La medesima impostazione si riscontra nella più recente raccomandazione dell'Assemblea parlamentare del Consiglio d'Europa n. 1950(2011), adottata il 25 gennaio 2011, che al punto 15 recita: « le droit des journalistes de ne pas divulguer leurs sources d'information est un privilège professionnel, destiné à encourager des sources à leur transmettre des informations importantes qu'elles ne fourniraient pas sans un engagement de confidentialité. La même relation de confiance n'existe pas par rapport aux non-journalistes, par exemple les personnes qui disposent d'un site internet on d'un blog. Par conséquent, les non-journalistes ne peuvent pas bénéficier du droit des journalistes de ne pas révéler leurs sources ».

[52] Sul rilievo dell'interesse pubblico, anche rispetto alla pubblicazione di documenti coperti da segreto, si v. la fondamentale sentenza della Corte europea dei diritti dell'uomo *Dupuis e aa. c. Francia*, del 7 giugno 2007; ma gli stessi principi sono affermati anche nelle più risalenti sentenze *Fressoz e Roire c. Francia*, del 21 gennaio 1999, e *Du Roy e Malaurie c. Francia*, del 3 ottobre 2000, nonché, sia pure *a contrario*, nella sentenza *Tourancheau e July c. Francia*, del 24 novembre 2005.

[53] Potrebbe così individuarsi anche un percorso per superare il problema segnalato da V. TONDI DELLA MURA (*Riflettendo sull'informazione e la democrazia dopo « Wikileaks »: l'indagine penale ai tempi di « Dagospia »*, in *Rivista telematica giuridica dell'Associazione Italiana dei Costitu-*

ma si rafforza la necessità di distinguere tra esercizio professionale dell'informazione e mera manifestazione del pensiero: la perdita di qualsiasi distinzione tra queste due dimensioni, fino alla totale sovrapposizione tra utente e produttore dell'informazione (all'insegna del "siamo tutti giornalisti"), rischia di produrre effetti perniciosi in un mondo caratterizzato dalla sovrabbondanza delle informazioni. Fenomeni come il dossieraggio e la scientifica distruzione della reputazione dovrebbero essere innanzitutto sanzionati sul piano della reputazione professionale di chi li pone in essere, ma se chi li pone in essere non è identificabile, e la diffusione della falsa informazione è opera semplicemente della "rete", ciò significa puramente e semplicemente licenza di diffamare, licenza di divulgare informazioni sensibili, licenza di calpestare la reputazione e la libertà individuale.

Con ciò non si vuole sottovalutare il problema della necessità di ridefinire cosa si intenda per "professione" in un contesto tecnologico radicalmente mutato, e non si può ignorare la presenza, accanto ai *mass media* tradizionali [54], di nuove tipologie di intermediari, oggi in uno stadio ancora sperimentale ed embrionale, come le c.d. piattaforme di *whistleblowing* [55]: ciò che non si deve perdere di vista, magari sull'onda dell'entusiasmo che inevitabilmente si accompagna alla percezione della molteplicità di occa-

zionalisti (*www.associazionedeicostituzionalisti.it*), n. 3/2012, 16), il rischio cioè che, nell'alluvione di materiali riversati *on line*, l'utente si perda, non possedendo gli strumenti necessari per leggere ed organizzare il materiale e quindi anche per discernere il vero dal falso. Questo è ancora, e non può che essere, compito del giornalismo professionale: che appunto perché investito di questo delicato compito, da un lato può rivendicare dei privilegi (a cominciare dalla protezione delle fonti) dall'altro deve assumersi la piena responsabilità di quanto divulga.

[54] È interessante ad es. notare il ruolo che i *media* professionali hanno svolto sia nelle c.d. rivoluzioni arabe (si pensi al ruolo della emittente *Al Jazeera* nel diffondere materiale video spesso prodotto dagli stessi manifestanti), sia in rapporto alla vicenda *Wikileaks*, in cui autorevoli testate giornalistiche "tradizionali" (ad es. il *Guardian*) sono state coinvolte, sia per assicurare maggiore diffusione e pubblicità ai documenti, sia per certificare, con la loro autorevolezza, l'autenticità delle divulgazioni: in proposito, è interessante quanto osserva C. Formenti, *Felici e sfruttati. Capitalismo digitale ed eclissi del lavoro*, Milano 2011, 71 ss., che, ridimensionando l'enfasi da molti apposta sulla presunta natura "eversiva" e "rivoluzionaria" della vicenda *Wikileaks*, la riconduce alle dinamiche e alla natura di un'impresa « squisitamente giornalistica », in sostanza non diversa dalla ben nota vicenda dei *Pentagon papers* (sulla possibilità di assimilare *Wikileaks* a un'impresa giornalistica v. D. Mula, *Wikileaks e la tutela dei dati personali*, in questa *Rivista* 2011, 673 ss.); e ciò sembrerebbe trovare conferma nella notizia, diffusa nel novembre 2013, dell'intenzione da parte del Governo statunitense di far cadere le accuse di spionaggio nei confronti di Assange, con la motivazione che il mantenere in piedi tali accuse avrebbe significato accusare di spionaggio anche i grandi quotidiani che avevano collaborato alla diffusione dei materiali.

[55] Con il termine « piattaforme di *whistleblowing* » ci si riferisce a strutture e organizzazioni che si assumono il compito di ricevere le informazioni provenienti dai *whistleblowers* (soggetti che, per la posizione che occupano all'interno di organizzazioni pubbliche o private, hanno ragione di temere ritorsioni o comunque conseguenze sfavorevoli nel caso la loro identità divenisse di pubblico dominio), verificarne l'autenticità e la rilevanza, e quindi diffonderle, garantendo nel contempo l'anonimato dell'informatore: se la stessa *Wikileaks* si può considerare come una piattaforma di *whistleblowing* che opera a

sioni e di forme di comunicazione offerta dalle nuove tecnologie, è la necessità, più che mai pressante nel nuovo scenario, di garantire, in uno con la libertà di espressione di tutti, il diritto del pubblico ad una informazione corretta e rispettosa della verità e dei diritti delle persone.

Tale garanzia non può che essere affidata, in primo luogo, ad una comunità degli operatori professionali dell'informazione caratterizzata da indipendenza di giudizio e dalla condivisione di elementari principi deontologici, all'interno di un quadro normativo che, oltre ovviamente a sanzionare in modo corretto ed equilibrato eventuali abusi, si preoccupi anche di garantire adeguati livelli di pluralismo degli strumenti e delle piattaforme trasmissive e di trasparenza, in particolare sugli assetti proprietari e sui condizionamenti (in primo luogo, ma non solo) economici che possono distorcere il processo comunicativo [56].

6. La necessità di procedimentalizzare la *disclosure* della fonte anonima.

Un ultimo, ma non meno importante aspetto è rappresentato dalla necessità di individuare regole procedurali chiare attraverso cui sia possibile, in presenza di illeciti documentati o quanto meno di solidi indizi, pervenire alla ***disclosure*** della fonte.

Fermo restando che anche i più convinti fautori della crittografia e dell'anonimato [57] sono costretti a riconoscere — sia pure a malincuore — che non è realistico opporsi alla introduzione di procedure che consentano l'individuazione, *ex post* e caso per caso, degli autori degli illeciti, le modalità attraverso cui tale

livello centralizzato, un altro esempio, in fase peraltro ancora sperimentale, è quello di *Globaleaks* (*https://globaleaks.org*: v. al riguardo A. Rodolfi, *Whistleblowing 2.0*, cit., 297 ss.), una piattaforma decentralizzata il cui scopo è assicurare da un lato la protezione delle fonti (sia sul piano giuridico sia su quello tecnologico, attraverso la tecnologia TOR), dall'altro la verifica sulla attendibilità delle informazioni (oggetto di una analisi specializzata a seconda dei contesti) in vista della loro eventuale divulgazione, con riferimento ad una pluralità di soggetti (non solo testate giornalistiche, ma anche ONG e associazioni).

[56] Anche sotto tale profilo, preziose indicazioni vengono dalle raccomandazioni degli organismi del Consiglio d'Europa, che da un lato evidenziano come il pluralismo dei *media* non sia riconducibile alla sola applicazione delle regole della concorrenza, e come esso implichi, oltre alla diversità dei contenuti, la molteplicità delle piattaforme trasmissive, dall'altro sottolineano come l'evoluzione tecnologica e lo scenario della convergenza tra i *media* non eliminino affatto, anzi al contrario accrescano i rischi di concentrazione, sicché occorre assicurare il massimo della trasparenza sugli assetti proprietari e sul finanziamento « delle imprese del settore dei media, compresi i fornitori di contenuti e di servizi dei nuovi servizi di comunicazione » (Racc. n° R (99)1 del Comitato dei Ministri, sulle misure volte a promuovere il pluralismo dei *media*, adottata il 19 gennaio 1999; ma v. anche, tra le molte, la racc. CM/Rec(2007)2 del Comitato dei Ministri sul pluralismo e la diversità di contenuto dei *media*, adottata il 31 gennaio 2007).

[57] V. ad es. J. Assange, *Internet è il nemico*, cit., 137 e s.

principio generalissimo viene ad essere attuato non sono affatto irrilevanti [58].

Si tratta, in particolare, di chiarire come si applica il principio contenuto nell'art. 15 della direttiva 2000/31 sul commercio elettronico, secondo cui, in presenza di « attività o informazioni illecite » gli stati membri « possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti (....) a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'individuazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione di dati » [59].

In primo luogo, questo obbligo non dovrebbe tradursi nella imposizione di meccanismi di controllo preventivo e generalizzato [60]: il superamento dell'anonimato deve avvenire caso per caso, di fronte a puntuali ipotesi di illecito, e non attuato in via generalizzata e preventiva, soprattutto in quanto l'applicazione di strumenti di controllo automatico e generalizzato porta alla acquisizione di dati che possono essere utilizzati per qualsiasi finalità, determinando un sacrificio sproporzionato del diritto alla protezione dei dati personali (come garantito dalla Carta europea dei diritti fondamentali) e della stessa libertà dell'impresa (cui viene imposto un adempimento estremamente oneroso) [61].

Un altro principio che dovrebbe presiedere alla procedimentalizzazione della *disclosure* dell'utente anonimo della rete è quello del giusto procedimento, che comporta, da un lato, che l'eventuale ordine di consegna dei dati sia sottoposto al controllo preventivo di una autorità indipendente (preferibilmente di un

[58] Sul punto, in generale v. P. Balboni, *Cenni giurisprudenziali*, cit., 321 ss.

[59] Allo stato, come si è detto, il legislatore interno si è limitato alla sostanziale trasposizione del principio, senza specificare modalità e procedure attraverso cui il *provider* può essere costretto a rivelare i dati identificativi dei propri utenti.

[60] Emblematica è ancora oggi la vicenda *Peppermint* (trih. Roma, ord. 16 luglio 2007, su cui v. E. Pelino, *L'anonimato su internet*, cit., 294) impropriamente citato come esempio di un caso in cui l'anonimato ha prevalso rispetto all'esigenza di prevenzione dei reati, ma in realtà avente ad oggetto una colossale operazione di schedatura avviata in violazione della legge, e finalizzata all'accertamento di un numero imprecisato di reati, e che correttamente viene ritenuta illecita, proprio in quanto esorbitante dai limiti delle legittime finalità di individuazione dei responsabili di specifici reati.

[61] In questo senso depongono anche i precedenti giurisprudenziali più significativi, a cominciare dalla nota sentenza della Corte di Giustizia UE (Sez. III) del 24 novembre 2011 (Causa C-70/10), *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs*, che, unitamente ad altre, evidenzia la contrarietà al diritto comunitario di ogni meccanismo di controllo generalizzato sul traffico e gli accessi degli utenti (nella specie finalizzato a accertare eventuali violazioni del diritto d'autore tramite il *download* di opere protette): si tratta di un principio che appare condivisibile, e che è ripreso da numerose decisioni di tribunali nazionali e anche italiani (a cominciare dalla vicenda *Peppermint* sopra richiamata), nonché dagli interventi in materia del Garante per la protezione dei dati personali (al riguardo, v. L. Ferola, *Diritto d'autore vs. diritto alla riservatezza: alla ricerca di un equo bilanciamento nella rete. I casi Peppermint, FAPAV e Scarlet*, in F. Pizzetti (a cura di), *Il caso del diritto d'autore*, Torino 2013, 67 ss., e M. Siano, *la sentenza Scarlet della Corte di giustizia: punti fermi e problemi aperti*, *ivi*, 81 ss.).

giudice) [62], e dall'altro il rispetto di un minimo di contraddittorio: e non è fuori luogo chiedersi se, nella prospettiva di una disciplina compiutamente rispettosa del principio del contraddittorio, non possa immaginarsi la possibilità di coinvolgere nel procedimento, oltre alla autorità pubblica e al *provider*, anche lo stesso soggetto anonimo interessato, il quale, pur conservando l'anonimato, potrebbe essere messo in grado di esporre le ragioni che, dal suo punto di vista, militano contro l'accoglimento della richiesta (salvo, ovviamente, che ciò sia incompatibile con finalità investigative, a fronte di reati di particolare gravità) [63].

L'adozione di una disciplina del procedimento compiutamente rispettosa delle garanzie di difesa di tutti i soggetti coinvolti e del principio del contraddittorio potrebbe consentire di raggiungere un accettabile punto di equilibrio tra gli interessi in gioco, molto più di quanto non si possa ottenere modulando la possibilità della *disclosure* in relazione alla gravità dell'illecito contestato [64].

La riflessione sull'anonimato, come su molti altri aspetti della regolamentazione di internet, evidenzia una volta di più come il

[62] Può agevolmente estendersi alla materia in esame il principio espresso nella nota sentenza della Corte europea dei diritti dell'uomo (Grande Camera) *Sanoma Uitgevers B. V. c. Paesi Bassi*, del 14 settembre 2010, in materia di protezione delle fonti giornalistiche, in cui la Corte precisa che, affinché una ingerenza nel diritto alla protezione delle fonti possa considerarsi « prevista per legge » è necessario non solo che essa sia prevista in una norma formalmente legislativa, ma anche che sia accompagnata da adeguate garanzie procedimentali, tra le quali il controllo preventivo di un giudice.

[63] Qualcosa di simile sembra prefigurato anche nella già richiamata sentenza della Corte Suprema di Israele del 25 marzo 2010 (su cui v. *supra*, nota 17). Si tratta, insomma, di trovare un giusto punto di equilibrio tra un meccanismo come quello individuato dalla giurisprudenza USA per la repressione delle diffamazioni anonime (su cui v. P. Balboni, *Cenni giurisprudenziali*, cit., 327 ss.), che presenta il vantaggio di imporre la *disclosure* solo dopo un preliminare accertamento della sussistenza dell'illecito (ma fa sì che, almeno nella prima fase, l'autore dello scritto asseritamente diffamatorio non sia in condizione di difendersi), e quello per cui si impone lo svelamento immediato dell'identità dell'autore, anche solo in presenza di una mera accusa o segnalazione di comportamenti illeciti, mettendo quest'ultimo in condizione di difendersi pienamente sin dall'inizio (ma con il rischio che, alla fine, la persona costretta a svelare la propria identità venga riconosciuta innocente). L'attualità e l'estensione del problema è attestata dal fenomeno (descritto da J. Assange, *Internet è il nemico*, cit., pag. 160, nota 8) delle NSL (*national security letters*), comunicazioni con cui le autorità (amministrative) statunitensi chiedono ai *providers* dati sulle utenze, che sono enormemente incrementate dopo il *Patriot Act* del 2001 e che spesso contengono clausole che vietano al *provider* di avvisare l'utente del fatto che i propri dati sono stati richiesti, impedendogli di difendersi dalla ingiunzione.

[64] In particolare, sembra possano esprimersi delle perplessità rispetto ad eventuali scelte, normative o giurisprudenziali, volte a circoscrivere la possibilità di risalire all'identità dell'autore alle sole ipotesi di gravi violazioni della legge penale: una simile soluzione, pur muovendo da un evidente intento garantistico, in talune situazioni potrebbe infatti rivelarsi controproducente, incentivando — sia da parte del legislatore sia da parte dei privati — il ricorso alla tutela penale, al solo fine di consentire la individuazione del responsabile, anche quando siano configurabili ed accessibili rimedi di tipi civilistico o amministrativo. Sarebbe interessante, ad esempio, domandarsi in che misura, nella scelta che il soggetto che si ritiene diffamato può compiere tra lo sporgere querela o il promuovere un'azione civile di risarcimento, possano influire anche considerazioni relative alla difficoltà, nel contesto di una azione civile per diffamazione, di risalire al nominativo dell'effettivo autore del contenuto diffamatorio immesso in rete.

dibattito sulla "libertà della rete" non possa essere risolto con facili semplificazioni: si ripropongono costantemente situazioni conflittuali la cui soluzione non può essere individuata una volta per tutte, ma richiede valutazioni duttili e circostanziate, tanto più in presenza di un mezzo in continua evoluzione e di cui non sono compiutamente note le potenzialità ed i rischi. Un motivo in più per insistere sulla importanza delle garanzie procedimentali, e in particolare della riserva di giurisdizione, che, come ci insegnano gli artt. 15 e 21 cost., rimane un presidio fondamentale laddove siano in gioco diritti fondamentali della persona: anche sotto questo profilo, la lezione della Costituzione repubblicana è ancora più che mai attuale.

Abstract

The article deals with the implications of anonymity as an instrument of political dissent's protection, both in democracies and in non-democratic regimes. It sheds light on the potentiality of the use of anonymity (as a form of protection against the so called "surveillance society") and on its risks and contradictions (as a possible vehicle of mystification, manipulation and misinformation). Moreover, the article analyzes the instruments aimed to balance the claim for anonymity and the need to identify and punish the perpetrators of crimes. Particular attention is paid to the role of professional intermediaries (traditional media, whistleblowing platforms, etc.) and to the need of finding transparent procedures for the disclosure of the anonymous user.