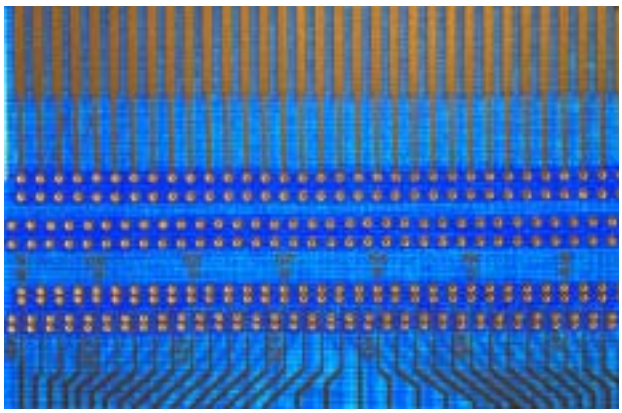
Criminalità



in rete

Rapporto della commissione peritale

„Criminalità in rete“

Dipartimento federale di giustizia e polizia
Berna, giugno 2003

Indice

		Seite
Indice		3
Elenco delle abbreviazioni e glossario		9
Bibliografia		12
1.	**Introduzione**	**15**
1.1	Situazione iniziale	15
1.11	„Agenti di polizia Internet“ (*Internet cops*): progetto pilota	15
1.12	Raccomandazione ai provider: bloccare l'accesso alla rete	15
1.13	Una prima perizia...	15
1.14	... e una seconda perizia	16
1.2	Contesto politico	16
1.21	La mozione Pfisterer	16
1.22	Altri interventi parlamentari	17
1.3	La commissione peritale	18
1.31	Istituzione e mandato	18
1.32	Composizione	18
1.33	Metodo di lavoro della commissione	19
1.4	Le questioni principali	19
2.	**Comunicazione in rete: fatti e cifre**	**21**
2.1	Evoluzione delle tecnologie dell'informazione e mutamento sociale	21
2.11	Nuova molteplicità dei servizi di comunicazione	21
2.12	Internet: utilizzo senza frontiere	22
2.13	L'utilizzo di Internet aumenta anche in Svizzera	23
2.14	L'utilizzo di Internet dipende dal sesso, dalla formazione e dall'età	23
2.15	Internet: un mezzo di comunicazione quotidiano	24
2.2	Criminalità in rete	24
2.21	Reati tradizionali e nuove infrazioni	24
2.22	Generale aumento della criminalità in rete	25
2.23	I limiti del perseguimento penale in Svizzera	26
2.24	La criminalità è tecnicamente neutra	27
2.3	I soggetti coinvolti nella comunicazione in rete	27
2.31	Il fornitore di servizi	28
2.311	Fornitore di contenuti (content provider)	28
2.312	Hosting provider	29
2.313	Provider di rete (network provider)	29
2.314	Fornitore di accesso (access provider)	29
2.32	L'utente	29
2.33	Intercambiabilità e multifunzionalità	30
2.34	I soggetti partecipanti agli altri servizi Internet	30
2.4	Reti	30
2.41	Telecomunicazione in generale	30
2.42	Reti di comunicazione elettronica	31
2.43	Diversi tipi di reti di comunicazione elettronica	31
2.44	Necessità di un approccio legislativo più ampio	31
2.5	Comunicazione di massa e individuale	32
2.6	Reti di comunicazione elettronica e media	33
2.61	Importanti delimitazioni tra diritto delle telecomunicazioni e diritto dei	33

	media	
2.62	Lo sviluppo tecnico ha superato il diritto	35
2.63	Rete di comunicazione elettronica come nuova nozione fondamentale	35
3.	**Possibilità tecniche di controllo**	**36**
3.1	Scopo e principi di Internet	36
3.2	Controlli	36
3.21	Controllo dell'accesso	37
3.211	News	37
3.212	World Wide Web	37
3.22	Controllo dei contenuti	38
3.3	Efficacia	39
4.	**La direttiva UE sul commercio elettronico e la sua attuazione negli Stati confinanti con la Svizzera**	**40**
4.1	Generalità sulla direttiva 2000/31 del Parlamento europeo e del Consiglio dell'8 giugno 2000 („direttiva sul commercio elettronico“)	40
4.2	Gli articoli 12-15 della direttiva sul commercio elettronico (responsabilità dei prestatori intermediari)	41
4.21	Osservazioni preliminari	41
4.22	Art. 12: Nessuna responsabilità per il semplice trasporto	42
4.23	Art. 13 und 14: Nessuna responsabilità per caching o hosting	43
4.24	Art. 15: Assenza dell'obbligo generale di sorveglianza	44
4.3	L'attuazione degli articoli 12-15 della direttiva sul commercio elettronico negli Stati confinanti con la Svizzera	45
4.31	Germania	45
4.32	Austria	47
4.33	Francia	50
4.34	Italia	51
5.	**Condizioni quadro costituzionali**	**52**
5.1	Il mandato costituzionale relativo alla tutela dei beni giuridici	52
5.11	Oggetto del mandato	52
5.12	L'adempimento del mandato costituzionale	53
5.2	Vincoli costituzionali in relazione alla tutela dei beni giuridici	53
5.21	Efficiente tutela dei diritti fondamentali	54
5.22	Ordinamento delle competenze a livello federale	54
5.23	Valore istituzionale dei diritti fondamentali	54
5.24	Rispetto dei diritti fondamentali tutelati	55
5.241	Destinatari	55
5.242	Terzi	55
5.25	Proporzionalità	56
5.251	In generale	56
5.252	Idoneità	56
5.253	Carattere necessario	56
5.254	Esigibilità	56
5.26	Uguaglianza giuridica e divieto dell'arbitrio	57
6.	**Criminalità in rete secondo il diritto penale vigente**	**58**
6.1	In generale	58
6.11	Problematica	58
6.12	Nozione di criminalità in rete	59

6.2	Punibilità secondo il diritto penale dei media?	61
6.21	Le nuove disposizioni del diritto penale dei media	61
6.22	Nuova decisione del Tribunale federale concernente la nozione di reato mediatico	61
6.23	Tre approcci interpretativi	62
6.231	I provider sono responsabili della pubblicazione – Applicabilità del diritto penale dei media	62
6.232	I provider non sono responsabili della pubblicazione – Applicabilità delle regole generali	63
6.233	I provider non sono responsabili della pubblicazione - Applicabilità del diritto penale dei media	64
6.24	L'articolo 27 CP non si addice a Internet	64
6.3	Punibilità secondo le regole generali del Codice penale?	65
6.4	Il problema della sovranità penale	68
6.41	Luogo d'esecuzione dei reati commessi in rete	69
6.42	Luogo in cui si produce il risultato dei reati commessi in rete	69
6.421	Nozione tecnica di evento	70
6.422	Evento in quanto violazione o messa in pericolo dell'oggetto dell'aggressione	71
6.43	Il nesso di collegamento per la partecipazione a un reato	72
6.44	Esempi (cfr. *allegato*)	73
6.5	Giurisdizione federale o cantonale?	73
7.	**Possibilità di adottare misure di diritto amministrativo**	**76**
7.1	Situazione di partenza	76
7.11	Necessità di misure di diritto amministrativo	76
7.12	Competenza della Confederazione	76
7.13	Diritto vigente	77
7.131	Diritto in materia di telecomunicazioni	77
7.132	Diritto in materia di radiotelevisione	77
7.133	Conclusioni	77
7.2.	Possibili strumenti di diritto amministrativo	78
7.21	Norme e disposizioni di polizia	78
7.211	Obblighi di autorizzazione	78
7.212	Obbligo di controllo del contenuto	78
7.213	Obbligo di annunciare e di denunciare	79
7.214	Monitoring	79
7.215	Decisioni di blocco e rimozione	80
7.22	Estensione dell'obbligo e delle condizioni di concessione?	80
7.221	Principio	80
7.222	Contrasto con la tendenza attuale	80
7.223	Inammissibilità	81
7.23	Gentlemen’s agreement	81
7.3	Conclusioni: rinuncia a misure fiancheggiatrici di diritto amministrativo	82
8.	**Responsabilità civile**	**83**
8.1	Osservazioni preliminari	83
8.2	Responsabilità extracontrattuale	84
8.21	Fondamenti della responsabilità	84
8.22	Responsabilità civile di fornitori di accesso e di hosting provider	84
8.221	Pretese dipendenti da una colpa	85
8.222	Pretese indipendenti da una colpa	86
8.23	Necessità di agire sul piano legislativo	86
8.24	Coordinamento con il diritto penale	87

8.3	Responsabilità contrattuale di fornitori di accesso e hosting privider	88
8.4	Conclusioni finali della commissione peritale	88
9.	**Proposte della commissione**	**90**
	Testo legale proposto (modifica del Codice penale)	90
	Adeguamenti resi necessari dalle proposte precedenti	92
9.1	Approccio normativo della commissione peritale e commento alla nuova regolamentazione proposta	93
9.11	Generalità sulla regolamentazione della responsabilità	93
9.12	Normativa orizzontale o in funzione degli ambiti?	93
9.121	Normativa orizzontale per tutti gli ambiti giuridici	93
9.122	Normativa specifica in funzione dell'ambito giuridico	95
9.13	I tre pilastri della nuova regolamentazione	95
9.2	Commento al (nuovo) articolo 27 CP	96
9.21	Titolo della sezione 6: „Reati in reti di comunicazione elettronica“	96
9.211	Reati „in una rete di telecomunicazioni“	97
9.212	Reati commessi mediante telecomunicazione o tenuta a disposizione di informazioni	97
9.213	Reati „in reti di comunicazione elettronica“	98
9.22	(Nuovo) articolo 27 numero 1 CP (Fornitore di contenuti)	99
9.221	„Se un reato è commesso mediante …“.	99
9.222	Trasmissione, messa e tenuta a disposizione	99
9.223	Informazioni	99
9.224	Validità delle regole generali	100
9.23	(Nuovo) articolo 27 numero 2 CP (delimitazione rispetto al diritto penale dei media)	101
9.231	Rinvio al diritto penale dei media soltanto per gli autori e i redattori	101
9.24	(Nuovo) articolo 27 numero 3 CP (hosting provider, motori di ricerca)	102
9.241	Informazioni di terzi	102
9.242	„tenere automaticamente a disposizione“	102
9.243	Rinvio al (nuovo) articolo 322bis numero 1	103
9.244	Elenchi nei quali informazioni di terzi vengono automaticamente registrate (motori di ricerca), (nuovo) articolo 27 numero 3, 2° periodo	103
9.25	(Nuovo) articolo 27 numero 4 CP (fornitore di accesso, memorizzazione temporanea di breve durata)	104
9.251	Motivi di impunità in caso di mera fornitura di accesso in reti di comunicazione elettronica	104
9.252	In merito alla formulazione del (nuovo) articolo 27 numero 4, 1° periodo CP	106
9.253	Memorizzazione automatica e transitoria di informazioni di terzi, (nuovo) articolo 27 numero 4, 2° periodo CP	107
9.3	Commento al (nuovo) articolo 322bis numero 1	108
9.31	Capoverso 1	108
9.311	In generale	108
9.312	Particolarità	110
9.312.1	Sistematica	110
9.312.2	Rapporti con la punibilità del fornitore di contenuti	111
9.312.3	Autori del reato	112
9.312.4	Fattispecie di reato	112
9.312.5	Oggetto dell'omissione	113
9.312.6	Presupposto dell'obbligo di intervenire	114
9.312.7	Elemento soggettivo	115

9.312.8	Pena	119
9.32	Capoverso 2	120
9.321	In generale	120
9.322	Particolarità	122
9.322.1	Autori del reato	122
9.322.2	Fattispecie di reato	122
9.322.3	Elemento soggettivo	124
9.322.4	Pena	124
9.33	Capoverso 3	125
9.331	Principio	125
9.332	Incertezza quanto alla querela	125
9.333	Assenza di una querela in caso di reati perseguibili solo a querela di parte	126
9.34	Capoverso 4	126
9.341	Principio	126
9.342	Punibilità del reato	127
9.343	Ragioni a sostegno di una normativa esplicita	127
9.344	Funzione del nuovo capoverso	128
9.35	Capoverso 5	129
9.351	Cancellazione nel caso del capoverso 1	129
9.351.1	Principio	129
9.351.2	Natura materiale della cancellazione	130
9.351.3	Cancellazione in caso di assoluzione	130
9.352	Cancellazione nel caso del capoverso 2	132
9.4	Commento al (nuovo) art. 340ter CP	133
9.41	Problematica	133
9.42	Postulati della commissione peritale	134
9.43	Caratteristiche del modello proposto	134
9.431	In generale	134
9.432	Competenza della Confederazione: imperativa o facoltativa?	135
9.432.1	In generale	135
9.432.2	Particolarità del (nuovo) articolo 340ter CP	135
9.44	Singole osservazioni relative al (nuovo) articolo 340ter CP	136
10.	**Procedure legislative parallele e ulteriori lavori legislativi nell'ambito della criminalità in rete**	**137**
10.1	Parere in merito alle procedure legislative parallele	137
10.11	Legge federale sul commercio elettronico	137
10.12	Legge federale sulle lotterie e le scommesse	138
10.13	Legge federale concernente misure contro il razzismo, la tifoseria violenta e la propaganda violenta	139
10.2	Altri lavori legislativi inerenti la criminalità in rete	141
10.21	Adeguamento del diritto interno alla Convenzione sulla cibercriminalità	141
10.211	Contenuto della Convenzione	141
10.212	Necessità di adeguamento	142
10.213	Raccomandazioni della commissione peritale	143
10.22	Completamento della LSCPT per la determinazione del luogo del reato	143
11.	**Riassunto**	**145**
11.1	In generale	145
11.2	Diritto penale	145
11.21	Responsabilità penale	145

11.22	Carattere internazionale della criminalità in rete	146
11.23	A chi compete il perseguimento penale?	146
11.3	Altri aspetti trattati	147
11.31	Controlli tecnici di Internet	147
11.32	Misure di diritto amministrativo	147
11.33	Diritto civile	147

Allegato	**A** – Modifiche proposte nella mozione Pfisterer (motivazione)	148
	B – Esempi relativi al capitolo 6, n. 6.4	150

Elenco delle abbreviazioni e glossario

Access provider	Fornitore di accesso a Internet
AJP	Aktuelle Juristische Praxis
BGBl	Bundesgesetzblatt; Gazzetta ufficiale della Repubblica federale di Germania
BGH	Bundesgerichtshof; Corte Suprema tedesca
bibl.	Bibliografia del presente rapporto (pag.12)
Boll. sten.	Bollettino stenografico ufficiale dell'Assemblea federale
Boll. Uff.	Bollettino ufficiale dell'Assemblea federale
Browser	Applicazione locale, utilizzata per navigare sul web allo scopo di consultare documenti e di sfruttare i rinvii ipertestuali in essi contenuti
Caching	La *cache* è un supporto di memorizzazione in cui vengono depositati dati che necessitano di essere prelevati in modo rapido. Il fornitore di accesso ne fa uso in Internet al fine di accelerare l'accesso dei suoi clienti ai siti web visitati con più frequenza
CC	Codice civile svizzero, RS 210
CEDU	Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, RS 0.101
Content provider	Fornitore di contenuti
Chat	Comunicazione online (testi, suoni, immagini) tra utenti di Internet
Client	„Cliente"; computer che fa parte di una rete.
CO	Codice delle obbligazioni, RS 220
Cost.	Costituzione federale, RS 101
CP	Codice penale svizzero, RS 311
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
DFGP	Dipartimento federale di giustizia e polizia
DNS	*Domain Name System*: l'"elenco telefonico di Internet" traduce nomi simbolici come www.bj.admin.ch in un indirizzo digitale Internet
Download	„Scaricare" un contenuto da Internet nel proprio PC
DTF	Decisione del Tribunale federale
E-Commerce	Electronic Commerce, commercio elettronico in Internet.
ed.	edizione/editore
E-mail	Electronic mail, messaggio inviato con la posta elettronica
EGG	Elektronisches Geschäftsverkehr-Gesetz (Germania)
FF	Foglio federale
File Sharing	Servizio Internet che permette agli utenti di mettere a disposizione di altri utenti i dati (ad es. musica) memorizzati

	nel loro computer, affinché possano essere scaricati
FTP, ftp	*File Transfer Protocol*: sistema standard utilizzato in Internet per il trasferimento di dati tra client e server
GU	Gazzetta ufficiale (delle Comunità Europee)
GA	Goltdammer‘s Archiv für Strafrecht (Germania)
GAAC	Giurisprudenza delle autorità amministrative della Confederazione
Hosting provider	Fornitore di servizi che mette a disposizione dei suoi clienti spazio-memoria su un server
HTTP	*Hyper Text Transfer Protocol*: protocollo utilizato nel World Wide Web, con il quale il browser può accedere a siti web
IP	*Internet Protocol*: protocollo alla base di Internet, per lo scambio di dati controllato su scala mondiale indipendentemente dal mezzo fisico di trasmissione utilizzato
ISP	*Internet Service Provider*: fornitore di servizi Internet
LDIP	Legge federale sul diritto internazionale privato, RS 291
JO	Journal officiel de la République française
JZ	Juristenzeitung (Germania)
loc. cit.	loco citato (passo citato)
LSCPT	Legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, RS 780.1
LStup	Legge federale sugli stupefacenti, RS 812.121
LTC	Legge federale sulle telecomunicazioni, RS 784.10
LAN	*Local Area Network*: rete locale di un'azienda
LBI	Legge federale sui brevetti, RS 232.14
LCSl	Legge federale contro la concorrenza sleale, RS 241
LCStr	Legge federale sulla circolazione stradale, RS 741.01
LDA	Legge federale sul diritto d’autore, RS 231.1
LNA	Legge federale sulla navigazione aerea, RS 748.0
Link	Rinvio di un sito web verso un'altra pagina web o verso un contenuto multimediale (musica, video)
LPM	Legge federale sulla protezione dei marchi, RS 232.11
LRTV	Legge federale sulla radiotelevisione, RS 784.40
MMS	*Multimedia Messaging Service*: servizio di trasmissione di dati multimediali tra telefoni cellulari
Monitoring	Esplorazione dell'offerta Internet da parte di un'autorità statuale
Network provider	Fornitore di rete
Newsgroup	Forum elettronico di discussione in Internet
n. marg.	numero marginale
OST	Ordinanza sui servizi di telecomunicazione, RS 784.101.1
P2P o Peer to Peer	Protocollo per lo scambio diretto di dati tra utenti finali (vedi file sharing) senza l'intermediazione di un ente centrale
PP	Legge federale sulla procedura penale, RS 312

Proxy	I *proxies* sono elaboratori collegati tra reti locali (LAN) e Internet. A differenza degli altri elaboratori, inviano e ricevono pacchetti di dati trasmessi via Internet. Impiegati come *cache*, i proxies permettono di aumentare la velocità di connessione. Utilizzati come "firewall", possono anche servire a garantire maggior sicurezza o a controllare l'accesso alla rete, bloccando eventuali richieste a siti o pagine vietate
RDS	Rivista di diritto svizzero
Router	Instradatore; dispositivo che permette di collegare singoli segmenti di rete e di trasmettere pacchetti di dati verso altri instradatori, scegliendo i percorsi ottimali
RPS	Rivista penale svizzera
RS	Raccolta sistematica del diritto federale
Server	Computer collegato a una rete che mette i propri dati a disposizione di altri computer collegati alla stessa rete
SJZ	Schweizerische Juristen-Zeitung
SMS	*Short Message Service*: breve testo trasmesso tramite telefono cellulare
TCP	*Transmission Control Protocol:* regole di trasmissione, indipendenti dalle tecnologie usate per ogni rete, per il trasferimento sicuro dei dati in Internet
TDG	Teledienstegesetz (Germania)
URL	*Universal Resource Locator*: indirizzo Internet di un sito o una risorsa sul web e il protocollo con cui accedere a essa: p. es. http://www.ibm.com (accesso con http) o ftp://ftp.linksys.com (accesso con ftp)
WAP	*Wireless Access Protocol*: sottoinsieme dell'HTTP, utilizzato per trasmettere dati tra telefoni cellulari appositamente predisposti e speciali server che rielaborano i contenuti web in funzione dei piccoli schermi della telefonia cellulare
Web	Rete, abbreviazione di World Wide Web
World Wide Web	Rete mondiale, Internet
WWW	World Wide Web
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

Bibliografia

Questo elenco contiene unicamente le indicazioni e i riferimenti bibliografici relativi alle fonti citate più volte nel presente rapporto, che per semplificazione sono citate nelle note a piè di pagina soltanto con la designazione abbreviata (p. es. HÄFELIN/HALLER) e la menzione supplementare „bibl." (bibliografia).

CASSANI	Ursula Cassani, Die Anwendbarkeit des schweizerischen Strafrechts auf internationale Wirtschaftsdelikte (Art. 3-7 StGB), RPS 114 (1996), pag. 237 segg.
PERIZIA UFG	Ufficio federale di giustizia, Perizia del 24 dicembre 1999 concernente la responsabilità penale dei fornitori d'accesso Internet secondo gli articoli 27 e 322bis CP, GAAC 64.75
HÄFELIN/HALLER	Ulrich Häfelin/Walter Haller Schweizerisches Bundesstaatsrecht 5^{a} ed. Zurigo 2001
HÄFELIN/MÜLLER	Ulrich Häfelin/Georg Müller, Allgemeines Verwaltungsrecht 4^{a} ed. Zurigo 2002
HEINE	Günter Heine, Strafrechtlicher Schutz der Verbraucher vor Täuschungen und wettbewerbswidrigen Angeboten bei E-Commerce, in: Koller/Muralt Müller (ed.), Convegno „informatica e diritto 2001" del 18/19 settembre 2001, Berna 2002
HILGENDORF	Eric Hilgendorf, Die Neuen Medien und das Strafrecht, RPS 2001, pag. 650 segg.
HÖSLI	Peter Hösli, Möglichkeiten und Grenzen der Verfahrensbeschleunigung durch informell-kooperatives Verwaltungshandeln, tesi, Zurigo 2002
KOCH	Arnd Koch, Nationales Strafrecht und globale Internet-Kriminalität, GA 2002, pag. 703 segg.
LEHLE	Thomas Lehle, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, Costanza 1999
MOREILLON/DE COURTEN	Laurent Moreillon/Frédérique de Courten, La responsabilité pénale du Cyber-Provider (fournisseur), Anwaltsrevue/Revue de l'avocat 8/2002, pag. 12 segg.
MÜLLER, GRUNDRECHTE	Jörg Paul Müller Grundrechte in der Schweiz, im Rahmen der Bundesverfassung von 1999, der UNO-Pakte und der EMRK 3^{a} ed. Berna 1999
NIGGLI, INTERNET-KRIMINALITÄT	Marcel Alexander Niggli Internet-Kriminalität Anwaltsrevue/Revue de l'avocat, n. 8/2002, pag. 6 seg.

NIGGLI, NATIONALES STRAFRECHT	Marcel Alexander Niggli, Nationales Strafrecht vs. globales Internet, in: Weber/Hilty/Auf der Maur (ed.), Geschäftsplattform Internet II, Zurigo 2001, pag. 144 segg.
NIGGLI, RASSENDISKRIMINIERUNG	Marcel Alexander Niggli, Rassendiskriminierung, Kommentar, Zurigo 1996
NIGGLI/SCHWARZENEGGER	Marcel Alexander Niggli/Christian Schwarzenegger, Strafbare Handlungen im Internet, RDS 98 (2002), pag. 61 segg.
PFENNINGER	Hanspeter Pfenninger, Rechtliche Aspekte des informellen Verwaltungshandelns, tesi, Friburgo 1996
POPP	Peter Popp, in: Niggli/Wiprächtiger, Basler Kommentar, zu Art. 7 StGB, Basilea 2003
REHBERG/DONATSCH	Jörg Rehberg/Andreas Donatsch, Strafrecht, Verbrechenslehre, 7ª ed., Zurigo 2001
RICHTLINIE	Direttiva UE sul commercio elettronico Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno („Direttiva sul commercio elettronico“). *Gazzetta ufficiale n. L 178 del 17/07/2000 pag. 1 - 16* Link: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=IT&numdoc=32000L0031&model=guichett
RIKLIN	Franz Riklin, Strafrecht, Allgemeiner Teil, 2ª ed., Zurigo 2002
RIKLIN/STRATENWERTH	Franz Riklin/Günter Stratenwerth, Medienstrafrecht/Kaskadenhaftung, in: Niggli/Riklin/Stratenwerth (ed.), Die strafrechtliche Verantwortlichkeit von Internet Providern, edizione speciale medialex 2000, pag. 13 segg.
SATZGER	Helmut Satzger Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, Eine Untersuchung der Verantwortlichkeit für rechtswidrige Inhalte im Internet vor dem Hintergrund der neuen E-Commerce-Richtlinie der EG, Computer und Recht, 2/2001, pag. 109 segg.
SCHMID	Niklaus Schmid, in Schmid (ed.), Einziehung, Organisiertes Verbrechen, Geldwäscherei, Kommentar, vol. 1, Zurigo 1998
SCHULTZ, PRESSEDELIKT	Hans Schultz, Die unerlaubte Veröffentlichung - ein Pressedelikt, ZStrR 108 (1991) pag. 273 segg.
SCHWARZENEGGER, ABSTRAKTE GEFAHR	Christian Schwarzenegger, Abstrakte Gefahr als Erfolg im Strafanwendungsrecht - Ein Leading case grenzüberschreitenden Internetdelikten, sic! 2001, pag. 240 segg.
SCHWARZENEGGER, CRIMES	Christian Schwarzenegger

	Computer Crimes in Cyberspace, A comparative analysis of criminal law in Germany, Switzerland and Northern Europe Jusletter 14 ottobre 2002 www.weblaw.ch/jusletter/jsp?ArticleNr=1957
SCHWARZENEGGER, E-COMMERCE	Christian Schwarzenegger, E-Commerce - Die strafrechtliche Dimension, in: Arter/Jörg (ed.), Internet-Recht und Electronic Commerce Law, Lachen e S. Gallo 2001
SCHWARZENEGGER, GELTUNGSBEREICH	Christian Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet, RPS 118 (2000), pag. 109 segg.
SEMKEN	Hartmut Semken (Un-)Möglichkeiten der Inhaltskontrolle mit technischen Mitteln im Internet, in: Cassani/Maag/Niggli (ed.), Medien, Kriminalität und Justiz, Schweizerische Arbeitsgruppe für Kriminologie, vol. 19. Coira/Zurigo 2001, pag. 249 segg.
TRECHSEL	Stefan Trechsel, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2ª ed., Zurigo 1997
TRECHSEL/NOLL	Stefan Trechsel/Peter Noll Schweizerisches Strafrecht, Allgemeiner Teil I, Allgemeine Voraussetzungen der Strafbarkeit, 5ª ed. Zurigo 1998
TSCHANNEN/ZIMMERLI/KIENER	Pierre Tschannen/Ulrich Zimmerli/Regina Kiener, Allgemeines Verwaltungsrecht, Berna 2000
WEBER	Rolf H. Weber E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zurigo 2001
WIDMER/BÄHLER	Ursula Widmer/Konrad Bähler, Rechtsfragen beim Electronic Commerce, Sichere Geschäftstransaktionen im Internet, 2ª ed. Zurigo 2000
ZELLER	Franz Zeller, in: Niggli/Wiprächtiger, Basler Kommentar, zu Art. 27 StGB, Basilea 2003

La poca chiarezza in materia di responsabilità penale dei fornitori d'accesso a Internet e gli interventi parlamentari presentati su questo tema hanno portato all'istituzione di una commissione peritale "Criminalità in rete". Il rapporto che ne è scaturito intende innanzitutto fare luce sulla questione e formulare raccomandazioni e proposte all'indirizzo degli attori politici.

1. Introduzione

1.1 Situazione iniziale

1.11 „Nucleo investigativo telematico" (*Internet cops*): progetto pilota

Dall'inizio del 1998 l'Ufficio federale di polizia (FEDPOL) ha condotto un progetto pilota in materia di Internet-monitoring: due funzionari hanno svolto il ruolo di „agenti di polizia Internet", il cui compito era per così dire di „pattugliare" la rete e le sue offerte. Essi ricevevano tuttavia da parte del pubblico soprattutto segnalazioni relative a contenuti illegali, che erano in seguito oggetto di ulteriori analisi. In tali occasioni è stato constatato che il contenuto di diverse pagine Internet poteva costituire una violazione dell'articolo 261bis del Codice penale (CP), disposizione che punisce la discriminazione razziale.

1.12 Raccomandazione ai provider: bloccare l'accesso alla rete

Nel luglio dello stesso anno la Polizia federale si è rivolta con una circolare agli Internet Service Provider (ISP) in Svizzera, invitandoli a studiare la possibilità di bloccare l'accesso alle pagine incriminate. La Polizia federale ha fatto notare che il fatto di fornire l'accesso a tali pagine avrebbe potuto rendere gli ISP complici nella commissione del reato principale. La circolare ha suscitato dure reazioni tra i provider, che hanno messo in dubbio la fattibilità tecnica del blocco dell'accesso a Internet e il suo fondamento giuridico. Di conseguenza è stato creato un gruppo di contatto comune, formato dai servizi dell'Amministrazione federale interessati e dal ramo dei Provider. Il compito del gruppo era in particolare di approfondire e chiarire gli aspetti tecnici e giuridici del problema.

1.13 Una prima perizia...

Un primo documento di base concernente la questione del blocco dell'accesso a Internet ha suscitato reazioni controverse in seno al gruppo di contatto. La Polizia

federale ha pertanto chiesto all'Ufficio federale di giustizia (UFG) di analizzare in una perizia la questione della responsabilità penale dei fornitori di servizi Internet (Internet Service Provider), per quel che concerne il contenuto illegale delle pagine web.

Nella sua perizia del 24 dicembre 1999[1], l'UFG ha affermato che, in linea di principio, anche un mero offerente di accesso può essere ritenuto responsabile a titolo sussidiario e secondo il diritto penale dei media, a condizione che sia stato chiaramente reso attento da un'autorità di perseguimento penale in merito al contenuto illegale. Nei casi in cui il diritto penale dei media non è applicato, i provider possono essere puniti come complici del reato principale.

Sulla base delle considerazioni espresse nella perizia dell'UFG, la Polizia federale ha precisato la propria posizione in un documento che è stato reso pubblico [2].

1.14 ... e una seconda perizia

Verband Inside Telecom (VIT), rappresentante del ramo dei provider, ha respinto le conclusioni della perizia dell'UFG, definendole inesatte e incaricando i professori Marcel A. Niggli, Franz Riklin e Günter Stratenwerth di analizzare a loro volta la questione della responsabilità penale dei fornitori d'accesso.

Il 2 ottobre 2000 i tre professori hanno presentato la loro perizia [3], le cui conclusioni sulla posizione giuridica dei meri fornitori d'accesso sono risultate essenzialmente contrarie a quelle dell'UFG. Gli autori della perizia hanno chiaramente sottolineato che la situazione giuridica è a loro modo di vedere poco chiara, rilevando quindi l'urgenza di agire sul piano legislativo.

1.2 Contesto politico

1.21 La mozione Pfisterer

Il 14 dicembre 2000 il consigliere agli Stati Thomas Pfisterer, insieme a 27 cofirmatari, ha presentato la seguente mozione:

> 1. Il Consiglio federale è invitato a proporre rapidamente e prioritariamente una regolamentazione nel diritto penale ed eventualmente in altre singole disposizioni, che favorisca la certezza del diritto, che sia praticabile e possibilmente armonizzata a livello internazionale, volta a tutelare Internet nell'interesse della popolazione e dell'economia.
>
> 2. Se necessario, deve proporre (in seconda priorità) altre modifiche di diritto indispensabili.

---

[1] Pubblicata (in tedesco) in GAAC 64.75.

[2] Cfr. http://internet.bap.admin.ch/d/archiv/berichte/weitere/2000-05-15-d-internet-isp.pdf (in tedesco)

[3] Pubblicata in medialex, numero speciale 1/2000.

Nella motivazione l'autore della mozione ha sottolineato le peculiarità tecniche e giuridiche proprie alle reti informatiche quali Internet, deducendone l'urgente necessità di agire sul piano legislativo. Per la creazione dell'ordinamento quadro indispensabile, nella mozione si raccomanda di ispirarsi alla direttiva UE sul commercio elettronico. L'autore della mozione ha proposto un progetto di disposizione legale, che prevede soprattutto il completamento degli articoli 27 e 340 CP (cfr. testo dell'intervento nell'allegato [A]).

Nel suo parere relativo alla mozione, il *Consiglio federale* ha sottolineato che, anche in assenza di disposizioni specifiche, Internet non si muove in un vuoto normativo. A sostegno di tale opinione esso rinvia in particolare alla perizia dell'Ufficio federale di giustizia. Per il resto il Consiglio federale ha ribadito la sua volontà, già manifestata in precedenza, di giungere a un'armonizzazione internazionale della legislazione in materia, ritenendo valida la proposta di regolamentazione avanzata dall'autore della mozione. Ha inoltre posto l'accento sulla necessità di perseguire una politica coerente in materia di criminalità e di legiferare in modo conseguente. Il Consiglio federale si è dichiarato disposto ad *accogliere* la mozione, non sentendosi tuttavia vincolato dalla motivazione della stessa.

Il *Consiglio degli Stati* ha accolto la mozione il 6 marzo 2001 [4]; il *Consiglio nazionale* ha fatto altrettanto il 20 settembre 2001 [5].

1.22 Altri interventi parlamentari

Il 26 settembre 2002 la consigliera nazionale *Regine Aeppli* ha presentato un'iniziativa parlamentare formulata in termini generali (02.452) [6], dal seguente *tenore*:

> Al fine di coordinare e migliorare l'efficacia del perseguimento penale in materia di criminalità in rete, e in particolare di pedopornografia, occorre creare una competenza federale come quella prevista dall'articolo 340bis CP in ambito di criminalità organizzata.

Nella sua motivazione, l'autrice dell'iniziativa ricorda il sistema di Internet monitoring sospeso dalla Confederazione alla fine del 1999 e la collaborazione con i Cantoni, rivelatasi difficile. Evidenzia l'aumento dei casi di criminalità su Internet, in particolare nell'ambito della pornografia infantile e della pedofilia, e giudica pertanto inammissibile l'„annoso conflitto di competenze". Anche la Convenzione del Consiglio d'Europa contro la cibercriminalità, firmata dalla Svizzera, esige la creazione di un servizio centrale di collegamento.

---

[4] Boll. uff. 2001 S, pag. 27 seg.

[5] Boll. uff. 2001 N, pag. 1087 segg.

[6] Cfr. la precedente mozione Aeppli Wartmann (01.3196) del 23 marzo 2001 (Miglioramento della procedura nella lotta contro la criminalità su Internet), che persegue lo stesso obiettivo dell'iniziativa parlamentare del 2002.

1.3 La commissione peritale

1.31 Istituzione e mandato

Sulla scia della mozione Pfisterer (*supra* n. 1.21) e in generale al fine di chiarire le questioni relative all'abuso di Internet, il 22 novembre 2001 il DFGP ha istituito una commissione peritale „Criminalità in rete", affidandole il seguente *mandato*:

> la commissione peritale „Criminalità in rete" esamina quali provvedimenti giuridici, organizzativi e tecnici possono essere adottati per impedire e sanzionare i reati commessi per mezzo di Internet. Analizza in particolare la questione relativa al modo di disciplinare la responsabilità penale su Internet. Propone inoltre norme concernenti la responsabilità civile e la protezione della proprietà intellettuale, se ciò si rivela opportuno. I suoi lavori devono sfociare in un disegno di legge pronto per la procedura di consultazione.

Il DFGP ha incaricato la commissione di presentare un rapporto e un avamprogetto di legge entro la fine del 2003.

1.32 Composizione

Presieduta dal dott. Peter Müller, vicedirettore dell'Ufficio federale di giustizia [7], la commissione peritale era inoltre composta dai membri seguenti:

- prof. dott. Felix Bommer, professore assistente di diritto penale all'Università di Lucerna;
- avv. Hans-Ulrich Bühler, Ufficio federale di polizia;
- dott. Lukas Bühler, Istituto federale della proprietà intellettuale;
- avv. Maurice Harari, Ginevra [8];
- prof. dott. Matthias Kaiserswerth, Zurigo;
- prof. dott. Laurent Moreillon, professore assistente di diritto penale all'Università di Losanna;
- prof. dott. Marcel Alexander Niggli, professore ordinario di diritto penale all'Università di Friburgo;
- prof. dott. Isabelle Romy, avvocata, Zurigo; professoressa associata presso l'Università di Friburgo;
- prof. dott. Christian Schwarzenegger, professore assistente all'Università di Zurigo; *vicepresidente della commissione peritale*;
- prof. dott. Bernhard Waldmann, professore assistente di diritto pubblico all'Università di Friburgo;
- dott. Ursula Widmer, avvocata e amministratrice dell'associazione Verband Inside Telecom (VIT), Berna;
- dott. Franz Zeller, Ufficio federale delle comunicazioni.

[7] Dal 1° febbraio 2003 segretario generale del Dipartimento federale degli affari esteri (DFAE).
[8] Fino alla fine di ottobre 2002.

Il *segretariato* della commissione è stato gestito dalla dott. Dorrit Schleminger (fino a settembre 2002), dal dott. Peter Ullrich (da ottobre 2002, coordinatore del rapporto), dalla dott. Grace Schild Trappe (da febbraio 2003), dal dott. Stéphane Blanc e da Patrick Gruber (entrambi addetti alla tenuta dei processi verbali), tutti collaboratori dell'Ufficio federale di giustizia.

1.33 Metodo di lavoro della commissione

Tra febbraio 2002 e marzo 2003 la commissione si è riunita dieci volte, in sedute di mezza giornata o di una giornata intera.

In occasione di alcune delle sue sedute ha invitato quale perito esterno il signor Philipp Kronig, lic. iur., MPA, direttore del Servizio di coordinamento nazionale contro la criminalità su Internet (SCOCI) in seno all'Ufficio federale di polizia.

Diversi capitoli del rapporto conclusivo sono stati sostanzialmente redatti sulla base di contributi scientifici forniti da membri della commissione peritale:

- **Capitolo 2** (comunicazione in rete): prof. Schwarzenegger;
- **Capitolo 3** (presupposti tecnici): prof. Kaiserswerth;
- **Capitolo 5** (condizioni quadro costituzionali): prof. Waldmann;
- **Capitolo 6** (criminalità in rete secondo il diritto penale vigente): prof. Bommer, prof. Niggli, prof. Schwarzenegger;
- **Capitolo 7** (possibilità di adottare misure di diritto amministrativo): prof. Waldmann;
- **Capitolo 8** (responsabilità civile): dott. L. Bühler;
- **Capitolo 9** (proposta legislativa): prof. Bommer, prof. Moreillon, prof. Niggli, prof. Schwarzenegger;
- **Capitolo 10** (legislazione parallela/ulteriori lavori legislativi): prof. Bommer, prof. Niggli, prof. Schwarzenegger, prof. H.U. Bühler, dott. Widmer.

1.4 Le questioni principali

In termini molto generali, la domanda a cui deve rispondere la commissione peritale è la seguente:

> quali provvedimenti possono e devono essere adottati per impedire la presenza di contenuti illegali su Internet? Inoltre, chi può essere reso responsabile di tali contenuti e a che titolo?

La domanda generale può essere suddivisa in più *domande specifiche*:

- Come è possibile *controllare* ed eventualmente *bloccare* o *eliminare* contenuti circolanti in reti di comunicazione? (cfr. *capitolo 3* del rapporto)
- Chi può essere reso *penalmente* responsabile in Svizzera per reati commessi in reti di comunicazione e a quali condizioni? (cfr. *capitolo 6, n. 6.1 – 6.3*; *capitolo 9*)

- In che misura è possibile perseguire penalmente e punire in Svizzera reati in reti di comunicazione *commessi all'estero*? (cfr. *capitolo 6, n. 6.4*; *capitolo 9*)
- Il perseguimento penale dei reati commessi in reti di comunicazione va affidato *ai Cantoni o alla Confederazione*? (cfr. *capitolo 6, n. 6.5*; *capitolo 9, n. 9.4*)
- Il *diritto amministrativo* offre strumenti per impedire la commissione di reati in reti di comunicazione? (cfr. *capitolo*)
- Chi può essere reso responsabile *sul piano civile* dei danni derivanti da reati commessi in reti di comunicazione e di quelli connessi con il blocco o l'eliminazione di contenuti Internet illegali? (cfr. *capitolo 8*)

Negli ultimi anni il numero dei servizi di comunicazione e dei loro utenti è notevolmente aumentato. Ciò ha avuto ripercussioni sulla società. La criminalità specifica a tale settore ha fatto segnare una crescita analoga.

2. Comunicazione in rete: fatti e cifre

2.1 Evoluzione delle tecnologie dell'informazione e mutamento sociale

Il rapido sviluppo delle tecnologie dell'informazione e delle reti informatiche avvenuto nell'ultimo ventennio è stato il fattore che più di ogni altro ha condizionato e mutato la vita e il modo di comunicare della popolazione.

2.11 Nuova molteplicità dei servizi di comunicazione

Una volta chi era in ritardo a un appuntamento era costretto a cercare una cabina telefonica e doveva disporre di spiccioli per poter comunicare con chi lo stava aspettando. Se quest'ultimo poi non era in casa, non vi era modo di raggiungerlo. Oggi basta una telefonata o un *SMS* (Short Message Service) con un telefono cellulare (cfr. la casella sottostante).

Diffusione degli SMS

Per quel che concerne le comunicazioni SMS, nel 2001 le ditte offerenti servizi di telefonia mobile hanno registrato un tasso di crescita con punte del 50 per cento. Nel 2001 ogni cliente di Orange ha spedito in media 1,8 SMS al giorno. Swisscom ha avuto uno sviluppo simile, registrando circa sette milioni di messaggi quotidiani, il che equivale a due SMS al giorno per ogni suo cliente. Presso Sunrise le cifre relative all'ultimo trimestre del 2001 hanno fatto registrare un aumento del 66,7 per cento rispetto allo stesso periodo dell'anno precedente. La ditta stima che per ogni cliente la quota oscilli da 1,8 a 2 SMS al giorno [9].

Un tempo il lettore che intendeva far pubblicare una sua lettera in un giornale doveva spedirla via posta almeno un giorno prima della chiusura della redazione. Oggi è sufficiente un'*e-mail* (messaggio di posta elettronica), con un file di testo eventualmente allegato, che la redazione riceve di regola in pochi secondi.

Chi era alla ricerca di un impiego o di un appartamento, un tempo doveva attendere l'uscita dei quotidiani con le relative inserzioni. Oggi invece è possibile consultare in ogni momento le *banche dati disponibili in Internet*, e allacciare il primo contatto via e-mail.

[9] TAGES-ANZEIGER, „SMS-Boom ungebrochen", 22.1.2002, pag. 12.

I *siti web dei diversi media* consentono di seguire quasi in tempo reale l'attualità quotidiana.

Numero di siti web attivi [10] (su scala mondiale)	
Agosto 1995:	18'957
Dicembre 1996:	603'367
Dicembre 1997:	1'681'868
Dicembre 1998:	3'689'227
Dicembre 1999:	9'560'866
Dicembre 2000:	25'675'581
Dicembre 2001:	36'276'252
Dicembre 2002	35'543'105

Una volta chi desiderava scambiare opinioni all'interno di un gruppo di persone, doveva riunirsi in assemblee, partecipare a manifestazioni, recarsi in un ritrovo pubblico, ecc. Oggi vi è l'alternativa costituita dalle „chat" in Internet, che consente ai partecipanti di scambiarsi simultaneamente brevi messaggi, in modo anche anonimo. Per gli utenti di Internet che usufruiscono di un accesso veloce alla rete, vi è la possibilità di comunicare via *voice-mail* o in *videoconferenza*.

2.12 Internet: utilizzo senza frontiere

Con i servizi Internet descritti al punto 2.11 sono svaniti anche i confini geografici della comunicazione: l'impiego o la consultazione di informazioni sono infatti possibili in tutto il mondo, a partire da qualsiasi connessione alla rete. Sempre più persone dispongono di un collegamento a Internet privato o sul luogo di lavoro. A livello europeo la Svizzera è tra i Paesi con il tasso di penetrazione più elevato (vedi tabella seguente).

Numero di persone con connessione Internet domestica (4° trimestre 2001)[11]

	Numero di persone (in milioni)	Aumento rispetto al 3° trimestre 2001 (in %)	Quota della popolazione Internet mondiale per regione (in %)
USA/Canada	191,7	6,1	39
Europa/Israele/Sudafrica *	134,7	6,3	27
Estremo oriente, Australia, Nuova Zelanda**	110,1	5,8	22
America latina***	20,7	0,7	4
Resto del mondo	41,0	5,1	8
Totale	498,2		100

* Austria, Belgio, Danimarca, Finlandia, Francia, Germania, Irlanda, Italia, Lussemburgo, Norvegia, Paesi Bassi, Regno Unito, Spagna, Svezia, Svizzera; Israele; Sudafrica
** Australia, Corea del Sud, Giappone, Hong Kong, India, Nuova Zelanda, Singapore, Taiwan
*** Argentina, Brasile, Messico

[10] BBC NEWS, Internet starts to shrink, 2.1.2002, reperibile all'indirizzo: http://news.bbc.co.uk/1/hi/sci/tech/1738496.stm (stato: 31.3.2003); fonte: Netcraft.

[11] ACNIELSEN ERATINGS.COM, reperibile all'indirizzo: www.eratings.com/news/2002/20020306.htm (stato: 7.10.2002).

Economie domestiche con accesso a Internet e percentuale dei computer con accesso a Internet in Europa (4° trimestre 2001)[12]

	Economie domestiche con accesso a Internet (in %)	Quota di computer privati con accesso a Internet (in %)
Svezia	57	87
Paesi Bassi	52	82
Danimarca	51	82
Norvegia	47	78
Svizzera	**43**	**78**
Finlandia	42	81
Austria	38	70
Regno Unito	38	78
Germania	35	72
Italia	34	80
Belgio/Lussemburgo	32	68
Francia	20	53
Spagna	18	48

2.13 L'utilizzo di Internet aumenta anche in Svizzera

Dal 1997 l'utilizzo di Internet in Svizzera è fortemente aumentato. All'epoca soltanto il sette per cento della popolazione utilizzava Internet regolarmente, ossia più di una volta alla settimana. All'inizio del 2002 già il 42 per cento della popolazione faceva parte di questo limitato gruppo di utenti. Nel 1997 le persone che utilizzavano Internet soltanto saltuariamente costituivano il 15 per cento della popolazione, percentuale che nel frattempo è salita al 57 per cento [13].

2.14 L'utilizzo di Internet dipende dal sesso, dalla formazione e dall'età

All'inizio del 2002 la percentuale di utenti di sesso maschile era chiaramente superiore a quella delle utenti di sesso femminile: 52 per cento rispetto a malapena il 33 per cento. Tuttavia tra gli utenti di Internet la quota *femminile* sta tendenzialmente aumentando. Dal 1997 la percentuale di donne che utilizzano Internet più di una volta alla settimana è costantemente aumentata: dal tre per cento di quell'anno si è passati al 22 per cento del 2000, fino ad arrivare al 33 per cento nel 2002. Mentre la quota di utenti di sesso femminile tra il 1997 e il 2001 è più che decuplicata, quella di utenti di sesso maschile è aumentata soltanto di cinque volte [14].

Il *livello di formazione* ha un influsso determinante sull'utilizzo di Internet: più è elevato, maggiore è l'impiego di Internet. Nel 2002 il 22 per cento delle persone che avevano frequentato le scuole dell'obbligo utilizzava regolarmente Internet. Tale quota era invece del 35 per cento per coloro che avevano concluso una scuola secondaria, mentre per le persone con una formazione professionale di livello

[12] ACNIELSEN ERATINGS.COM, reperibile all'indirizzo: www.eratings.com/news/2002/20020306.htm (stato: 7.10.2002).

[13] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_1_synth.htm

[14] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_4_synth.htm

superiore la percentuale era del 58 per cento. La quota di utenti di Internet tra le persone che avevano conseguito un titolo universitario era circa del 71 per cento [15].

Una caratteristica importante nell'utilizzo di Internet è rappresentata dall'*età*. Internet è chiaramente meno utilizzata dalle persone di età superiore ai 50 anni. All'inizio del 2002 i maggiori utenti di Internet si situavano nelle fasce d'età tra i 14 e i 19 anni e tra i 20 e i 29 anni. Nella prima fascia d'età, il 56 per cento di utenti utilizzavano Internet più di una volta alla settimana, mentre nella seconda tale percentuale era del 60 per cento. Tra le persone con più di 50 anni la quota di utenti era soltanto del 20 per cento [16].

2.15 Internet: un mezzo di comunicazione quotidiano

Fino a tre anni fa l'uso di Internet era più frequente sul posto di lavoro che a casa. Nel frattempo la tendenza si è invertita e Internet è utilizzato di più *a casa* che *sul luogo di lavoro*. Nel 2002 il 42 per cento utilizzava Internet da casa, mentre dal posto di lavoro la percentuale era del 31 per cento. La sua diffusione sempre più marcata in ambito privato dimostra che Internet è diventata uno strumento di comunicazione quotidiano [17].

L'uso di Internet si differenzia anche a seconda delle *regioni linguistiche*: nella *Svizzera tedesca* Internet è usato con più frequenza (43 per cento) rispetto alla *Svizzera romanda* (41 per cento) e *italiana* (34 per cento) [18].

Nel 2002 Internet è stata perlopiù utilizzata a *scopi comunicativi*: più del 91 per cento degli utenti ha dichiarato di fare uso della posta elettronica. Tra i motivi che inducevano ad accedere a Internet, al secondo posto vi era l'impiego dei *motori di ricerca* (71 per cento), mentre al terzo posto figuravano gli *scopi informativi* (consultazione di articoli di giornali e riviste). Nel 2002 invece soltanto il 14 per cento degli utenti ha utilizzato Internet allo scopo di effettuare acquisti in rete (il cosiddetto *online-shopping*) [19].

2.2 Criminalità in rete

2.21 Reati tradizionali e nuove infrazioni

Il rovescio della medaglia dell'evoluzione illustrata al n. 2.1 risulta sempre più evidente. Da un lato i nuovi mezzi di comunicazione facilitano la commissione di reati

[15] www.infosociety-stat.admin.ch

[16] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_5_synth.htm

[17] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_311_synth.htm

[18] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_6_synth.htm

[19] http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106d_319_synth.htm. Cfr. per tutto ciò anche MAJA HUBER/FLORENT COSANDEY /VOLKER TÄUBE, Indikatoren zur Informationsgesellschaft, in: Informationsgesellschaft Schweiz, Standortbestimmung und Perspektiven, Neuchâtel 2002, 22, con numerose ulteriori informazioni sulla diffusione di computer, modem, telefoni cellulari e sull'uso fattone da privati, imprese e da enti pubblici.

„tradizionali“ [20], dall’altro l’informatica e le reti di comunicazione rappresentano piattaforme che favoriscono l’insorgere di nuove forme di criminalità [21] (vedi esempi seguenti).

Esempi di reati „tradizionali“

- Rappresentazione di atti di cruda violenza (art. 135 CP),
- False indicazioni su attività commerciali (art. 152 CP),
- Manipolazione dei corsi (art. 161bis CP),
- Diffamazione (art. 173 segg. CP),
- Violazione della sfera segreta o privata mediante apparecchi di presa d’immagini (art. 179^{quater} CP),
- Abuso di impianti di telecomunicazioni (art. 179^{septies} CP),
- Pornografia (art. 197 CP),
- Molestie sessuali (art. 198 CP),
- Fabbricazione, occultamento e trasporto di materie esplosive o gas velenosi (art. 226 CP),
- Pubblica istigazione a un crimine o alla violenza (art. 259 CP),
- Perturbamento della libertà di credenza e di culto (art. 261 CP),
- Discriminazione razziale (art. 261bis CP),
- Pubblicazione di deliberazioni ufficiali segrete (art. 293 CP),
- Messa in circolazione o copia di un’opera protetta dal diritto d’autore (art. 67 e 69 LDA),
- Metodi sleali di pubblicità e di vendita e altri comportamenti illeciti (art. 3 LCSl in relazione con l’art. 23 LCSl).

Esempi di nuove forme di criminalità

- Acquisizione illecita di dati (art. 143 CP),
- Accesso indebito a un sistema per l’elaborazione di dati (art. 143bis CP),
- Danneggiamento di dati, inclusa la fabbricazione e la messa in circolazione di virus informatici (art. 144bis CP),
- Abuso di un impianto per l’elaborazione di dati (art. 147 CP),
- Conseguimento fraudolento di una prestazione informatica („furto di tempo-macchina“, art. 150 CP),
- Coazione mediante invio non richiesto o massiccio di messaggi elettronici, o attacchi „*denial of service*“ (art. 181 CP).
- Danneggiamento grave delle reti di comunicazione: perturbamento di pubblici servizi (art. 239 n. 1 cpv. 1 CP).

2.22 Generale aumento della criminalità in rete

Le poche inchieste di carattere empirico sul tema evidenziano che la criminalità in rete ha subito un forte incremento dal 1990 [22]. In base a una statistica della *National Consumers League* (USA), ogni anno i consumatori annunciano sempre più casi di truffa commessa per mezzo di Internet. A seconda dei vari settori di attività, il rischio di essere vittima di tali truffe è più alto nell’ambito delle aste on line (87 per cento delle segnalazioni ricevute nel primo semestre 2002). Un ulteriore 6 per cento dei

[20] Ossia di reati già ben conosciuti, ma per la commissione dei quali la tecnologia informatica e le reti di comunicazione offrono nuovi strumenti estremamente efficaci e di agevole applicazione.

[21] Per una panoramica sulle forme di criminalità in Internet, vedasi WIDMER/BÄHLER (bibl.), pag. 292 segg.; SCHWARZENEGGER, E-COMMERCE (bibl.), pag. 333 segg.; WEBER, (bibl.), pag.538 segg.

[22] Cfr. UFFICIO FEDERALE DI POLIZIA, „Cyberkriminalität“, Die dunkle Seite der Informationsrevolution, Berna 2001, reperibile all’indirizzo: www.isps.ch/site/fichiers/171.pdf (stato: 7.10.2002); SCHWARZENEGGER, CRIMES (bibl.), n. 3 segg. e 42 seg.

presunti danni arrecati mediante truffe avviene nell'ambito della vendita generale di prodotti. Il danno patrimoniale medio ammonta a 484 $ US [23].

Nel 2001 la *Commissione europea* ha presentato un rapporto che stima a 600 milioni di euro il ricavato delle truffe con carte di pagamento per l'anno 2000. Ciò corrisponderebbe a un aumento di circa il 50 per cento. Una parte preponderante di tale importo è costituita dai pagamenti via Internet [24].

Nel 2001 si è di colpo intensificata anche la diffusione di *virus informatici*. Questi codici perfidi, diffusi spesso attraverso allegati („*attachments*") a messaggi elettronici, ma anche per mezzo di pagine web contaminate, possono causare danni enormi [25]. Secondo dati forniti dai produttori di programmi antivirus, nel 2001 in media una e-mail su 370 era infettata da un virus. Nel 2000 tale rapporto era di 1 a 700, mentre nel 1999 era di 1 a 1 400 [26].

2.23 I limiti del perseguimento penale in Svizzera

In Svizzera sono pochi i casi registrati dalla polizia, e soltanto sporadicamente si giunge a una condanna (vedi tabella sottostante) [27]. Per il rimanente, le condanne per abuso di un impianto per l'elaborazione di dati a scopo di truffa concernono soltanto in minima parte i reati commessi in rete. Nella maggior parte dei casi si tratta di abusi tradizionali di carte di pagamento.

Risulta quindi evidente che, nell'ambito del perseguimento penale in materia di criminalità informatica e di cibercriminalità, vi è ancora molto lavoro da fare, soprattutto in considerazione dei danni e dei rischi legati ad esempio all'attività degli hacker o alla diffusione dei virus informatici [28]. Lacune analoghe sono riscontrabili anche in materia di pornografia dura e leggera, di discriminazione razziale e di pirateria musicale, informatica e cinematografica.

---

[23] NATIONAL CONSUMERS LEAGUE (ed.), 2002 Internet fraud statistics, reperibile all'indirizzo: www.fraud.org/02intstats.htm (stato: 10.10.2002). L'importo complessivo dei danni annunciati nel 2000 ammontava a 3 387 530 $ US, mentre nel primo semestre del 2002 la somma totale è salita a 7 209 196 $ US. Questi dati statistici non sono tuttavia rappresentativi per la totalità degli utenti Internet negli USA. Si presuppone che non tutti i casi annunciati rappresentino una truffa ai sensi dell'articolo 146 CP.

[24] Commissione dell'Unione europea, Comunicazione del 9.2.2001 sulla prevenzione delle frodi e falsificazioni dei mezzi di pagamento diversi dai contanti, COM(2001) 11, reperibile all'indirizzo: http://europa.eu.int/eur-lex/it/com/cnc/2001/com2001_0011it01.pdf (stato: 10.10.2002).

[25] Il virus „I Love You", diffusosi su scala planetaria nel maggio del 2000, secondo valutazioni di Swiss Re avrebbe causato in brevissimo tempo un danno superiore al miliardo di dollari, cfr. SWISS RE, National catastrophes and man-made disasters in 2000, sigma n° 2/2001, pag. 7. Altre fonti parlano addirittura di un danno economico di 17 miliardi di dollari.

[26] TAGES-ANZEIGER, Von Würmern und tanzenden CEOs, 24 dicembre 2001, 49: „Das Jahr des Wurms".

[27] In Germania la situazione è simile, vedi SCHWARZENEGGER, CRIMES (bibl.), n° 3 segg.

[28] Cfr. anche i risultati dell'inchiesta in KPMG (ed.): 2001 global e.fr@ud.survey, s. l. 2001, reperibile all'indirizzo: www.kpmg.de/library/surveys/ (stato: 9.10.2002)

Reati informatici registrati dalle autorità di polizia (Zurigo, 1996-2000)

Anno	**1996**	**1997**	**1998**	**1999**	**2000**
Acquisizione illecita di dati (art. 143), Accesso indebito a un sistema per l'elaborazione di dati (art. 143bis), Danneggiamento di dati (art. 144bis n. 1), Allestimento, ecc. di programmi destinati al danneggiamento di dati (art. 144bis n. 2)	8	38	11	19	40
Abuso a scopo di truffa di un impianto per l'elaborazione di dati (art. 147)	786	1'162	1'612	1'673	2'100

Fonte: KRISTA 1996-2000 (Kriminalstatistik des Kantons Zürich)

Condanne per reati informatici (Svizzera, 1995-2000)

Anno	1995	1996	1997	1998	1999	2000
Acquisizione illecita di dati (art. 143)	1	2	2	2	4	3
Accesso indebito a un sistema per l'elaborazione di dati (art. 143bis)	0	1	0	1	1	2
Danneggiamento di dati (art. 144bis n. 1)	14	18	111	21	10	2
Allestimento, ecc. di programmi destinati al danneggiamento di dati (art. 144bis n. 2)	1	0	2	2	1	3
Abuso a scopo di truffa di un impianto per l'elaborazione di dati (art. 147)	52	223	372	393	416	422

Fonte: Ufficio federale di statistica, Statistica delle condanne penali 2002 (analisi non pubblicata).

2.24 La criminalità è tecnicamente neutra

Fenomeni criminali simili sono rilevabili anche nel settore della telefonia mobile (p. es. molestie sessuali, offesa all'onore per mezzo di SMS, *SMS-Flooding*, ecc.) [29]. Con il passaggio, in gran parte avvenuto, dai mezzi di comunicazione vocale alla rete radio-telematica multifunzionale, sulla quale è possibile sviluppare un crescente numero di servizi grazie alle nuove capacità di trasmissione di dati a banda larga (*WAP-News*, *Mobile-Chat*, *Mobile-Games*, trasferimento di dati grafici, SMS, e-mail), aumentano anche le possibilità di impiegare le nuove tecnologie a fini criminali. Attraverso i cosiddetti *gateway* (un *gateway* unisce diverse reti tra loro), i singoli servizi della rete telematica mobile sono inoltre collegati a Internet.

Nonostante la priorità attribuita dal presente rapporto ai problemi legati alla cibercriminalità, urge creare un quadro normativo tecnicamente neutra, considerata la convergenza delle reti e dei servizi di comunicazione digitale.

2.3 I soggetti coinvolti nella comunicazione in rete

Nelle reti di comunicazione l'allestimento, la conservazione e la trasmissione di contenuti illegali o di informazioni utilizzate illegalmente rappresenta un processo che

[29] Vedasi in proposito il sito www.handybetrug.ch (stato: 9.10.2002).

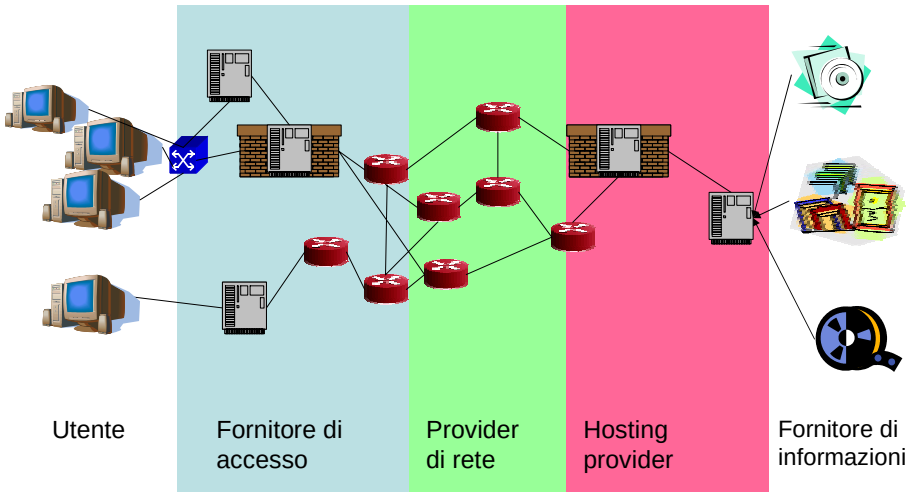
richiede varie tappe. Sempre più persone entrano pertanto in considerazione per quel che concerne gli autori o i partecipanti.

Se ad esempio consideriamo il World Wide Web (www), che con il servizio di posta elettronica costituisce il sistema più utilizzato per trasmettere dati via Internet (*cfr. n.* 2.15), è possibile distinguere diversi gruppi di persone.

2.31 Il fornitore di servizi

I fornitori di servizi si suddividono in quattro categorie diverse (vedi grafico sottostante). Vi sono quelli che offrono tutte e quattro le prestazioni (p. es. America Online, Bluewin), o quelli che si sono specializzati soltanto in una o due prestazioni di servizi.

Dal fornitore di informazioni all'utente



2.311 Fornitore di contenuti (content provider)

Il fornitore di contenuti (nel grafico: fornitore di informazioni) mette a disposizione in Internet contenuti propri o ricevuti da terzi. Si serve almeno di un fornitore di accesso (n. 2.314) e mette a disposizione le informazioni su un proprio elaboratore o su quello di un hosting provider (n. 2.312). Con la diffusione sempre maggiore dei cosiddetti protocolli *peer to peer*, anche i normali utenti, che altrimenti interverrebbero unicamente in quanto consumatori di informazioni, hanno la possibilità di offrire i loro contenuti. In tali casi il fornitore di contenuti provvede da sé all'„hosting" dei suoi dati.

2.312 Hosting provider

Gli hosting provider mettono a disposizione del loro cliente, il fornitore di contenuti, un server sul quale quest'ultimo può offrire le sue pagine web. A seconda dell'offerta, con l'accesso a una pagina web il fornitore di contenuti può anche far eseguire propri programmi che vi ha precedentemente caricato. Gli hosting provider possono eventualmente anche mettere a disposizione spazio per altri servizi, come ad esempio la posta elettronica. La caratteristica di questi servizi è che l'hosting provider di solito non partecipa al processo di memorizzazione dei dati sul suo server: si tratta di programmi che si svolgono automaticamente e che il fornitore di contenuti predispone e controlla in modo autonomo.

2.313 Provider di rete (network provider)

Attraverso la loro rete di comunicazione, i provider di rete sono collegati con diversi fornitori d'accesso, con altri provider di rete e con eventuali grandi clienti che non necessitano di un proprio fornitore di accesso (n. 2.314). Il trasporto di dati si svolge per il tramite di queste reti, grazie a esecuzioni automatizzate dei programmi.

2.314 Fornitore di accesso (content provider)

I fornitori di accesso procurano l'accesso a Internet agli utenti o alle ditte. L'accesso può avvenire attraverso la linea telefonica o mediante un allacciamento a banda larga (ADSL, Cablemodem, Wireless Local Loop, satellite, linea affittata, ecc.). Di regola il fornitore di accesso assegna (in modo dinamico) all'utente un indirizzo Internet, ogni volta diverso. Tuttavia le ditte e gli utenti che intendono anche offrire contenuti ricevono di solito un indirizzo Internet fisso o un intero blocco di indirizzi fissi, tratti da un ambito di indirizzi gestito dal fornitore di accesso. Anche questi processi si svolgono automaticamente, ossia senza un intervento manuale del fornitore di accesso.

Di regola i fornitori d'accesso gestiscono anche il server DNS (*Domain Name System*), che traduce i nomi simbolici in indirizzi Internet [30]. Ciò non è tuttavia indispensabile, poiché è possibile accedere anche a server DNS pubblici, utilizzabili per pubblicare o convertire nomi simbolici.

2.32 L'utente

Gli utenti (user) si trovano all'altro capo del processo di comunicazione. Sono coloro che da casa, dall'ufficio, dall'Internet café o dal loro apparecchio portatile (computer o telefono cellulare), richiamano le informazioni messe a disposizione su un server web.

[30] Esempio.: www.ofj.admin.ch viene "tradotto" con l'indirizzo numerico 193.5.216.22.

2.33 Intercambiabilità e multifunzionalità

I ruoli descritti ai punti 2.31 e 2.32 sono interscambiabili. Chi ad esempio è alla ricerca di dati musicali in un servizio *peer to peer* (cfr. n. 2.311) e li registra sul suo disco rigido, viene ritenuto un *utente*. Se tale utente autorizza nel contempo l'accesso on line a una porzione del suo disco rigido, contenente file musicali da scaricare, egli diventa *fornitore di contenuti* (e *hosting provider* di sé stesso).

I fornitori di servizi esercitano spesso più funzioni contemporaneamente. Un medium può ad esempio prevedere in un forum del proprio sito web spazio di memoria a disposizione per contenuti offerti da terzi, dati che vanno ad aggiungersi alle informazioni già fornite dal medium. In relazione ai propri contenuti il medium è quindi *fornitore di contenuti*, ma per quel che concerne il forum web rappresenta di principio un mero *hosting provider*. Vi è inoltre *fluidità* nei passaggi da una funzione all'altra.

Nell'esempio citato, per quanto riguarda i dati esterni contenuti nel forum web, il medium può anche diventare fornitore di contenuti, qualora un collaboratore sia incaricato di moderare il forum o di pubblicare soltanto i contenuti da lui controllati; ciò è considerato un'„appropriazione" delle informazioni esterne. È anche frequente la doppia funzione hosting e access provider.

2.34 I soggetti partecipanti agli altri servizi Internet

Le funzioni descritte in precedenza valgono anche per altri servizi che utilizzano Internet. Vanno soprattutto menzionati, tra gli altri, la posta elettronica (e-mail), i gruppi di discussione (newsgroups), il trasferimento di dati (ftp), la chat online (IRC), il web streaming (radio, televisione, video).

Di principio anche queste categorie di provider seguono processi di trasmissione che avvengono attraverso la rete telefonica fissa, quella mobile e altre forme di comunicazione (vedi n. 2.4).

2.4. Reti

2.41 Telecomunicazione in generale

La telecomunicazione è il procedimento tecnico che permette di inviare, trasmettere e ricevere informazioni di ogni tipo mediante tecniche elettriche, magnetiche, ottiche o elettromagnetiche. È in tal modo possibile trasferire rapidamente e a basso costo segni, espressioni, immagini, suoni o documenti multimediali elaborati o memorizzati perlopiù digitalmente da computer, microprocessori o altri apparecchi.

La trasmissione di dati avviene in parte ancora grazie a tecniche analogiche: i dati digitali sono dapprima trasformati in segnali analogici, corrispondenti a continue variazioni di tensioni elettriche, onde acustiche o magnetizzazioni; tali segnali sono in seguito inviati agli apparecchi destinatari, che li riconvertono in dati digitali.

2.42 Rete di comunicazione elettronica

Per rete di comunicazione o rete telematica si intende l'interconnessione di computer o di altri apparecchi di telecomunicazione mediante reti di *cavi* terrestri o reti di *radio*comunicazione senza cavo. Tali reti si basano su diverse tecniche di comunicazione e si differenziano anche nelle modalità logiche del trasporto di dati.

Nel dibattito sulle questioni di diritto penale relative alla trasmissione di informazioni è importante non limitarsi a parlare di „Internet". Una dichiarazione lesiva dell'onore o un'immagine di carattere pedopornografico possono essere trasmesse via Internet (FTP, e mail, WWW), ma anche attraverso la rete di telefonia mobile (SMS, MMS) o attraverso una rete locale (LAN). Il ricorso alla tecnologia di Internet non è quindi indispensabile.

2.43 Diversi tipi di reti di comunicazione elettronica

Per definire le reti di comunicazione elettronica, conviene ispirarsi al modello di riferimento dell'*Open Systems Interconnect* (OSI) dell'*International Standards Organization* (ISO). *A prescindere dall'aspetto tecnologico*, tale modello parte dal presupposto che ogni rete si compone di sette livelli. I livelli superiori usufruiscono dei servizi dei livelli inferiori, che a loro volta mettono i loro servizi a disposizione dei livelli superiori oppure dell'utente (o terminale). Al livello più basso (1) si parla di trasporto fisico di dati, che può avvenire attraverso i media più diversi (elettronici, ottici, ecc.). Al livello più alto (7) sono offerti all'utente servizi quali ad esempio la telefonia, la televisione, l'e mail o il World Wide Web.

Nella prassi si distinguono spesso *due diversi tipi di reti*, che vengono designate sia in base ai servizi offerti [31], sia in base al medium utilizzato per il trasporto fisico dei dati [32]. È tuttavia importante che, *da un lato*, le reti possano essere tecnicamente collegate indipendentemente dal medium di trasmissione, e che *dall'altro* i servizi possano essere offerti anche su supporti mediatici diversi da quelli previsti inizialmente. I protocolli Internet rappresentano una base accettata su scala mondiale [33], sulla quale è possibile offrire servizi per gli utenti finali indipendentemente dal medium con cui si trasferiscono fisicamente i dati.

- **Rete di telefonia fissa**
  In passato essa si basava esclusivamente su una tecnica di trasmissione *analogica*. Ora la sua struttura di base è stata trasformata in rete digitale, in cui la voce è trasmessa secondo la tecnica a commutazione di pacchetto [34]. Già oggi le

[31] P. es. la rete di telefonia mobile, la rete via cavo (per radio e televisione).

[32] Wireless LAN (WLAN), Ethernet, rete a fibre ottiche.

[33] Fino al 1994 i diversi fabbricanti di computer e l'ISO hanno cercato di standardizzare i protocolli di comunicazione sul mercato. Ma grazie alla loro struttura più semplice e alla loro disponibilità in molti sistemi operativi, i protocolli Internet concorrenti hanno fatto breccia e si sono nel frattempo imposti *de facto* come protocolli standard.

[34] Al fine di evitare ritardi indesiderati nella trasmissione vocale, finora veniva inserito un collegamento appositamente adibito alla comunicazione tra chiamante e chiamato. Lo svantaggio di tale sistema era che in caso di pause nella conversazione non era possibile sfruttare appieno il collegamento. Se invece, come sarà il caso in futuro ad esempio in base al protocollo Internet, la voce viene scomposta

imprese attive nel settore delle telecomunicazioni sfruttano la tecnologia Internet (*IP Telephony*), e mettono in comunicazione i loro utenti attraverso la stessa infrastruttura di rete sulla quale si basa attualmente l'Internet pubblica. Le imprese possono già oggi sfruttare questa alternativa, nel caso in cui intendano installare nuove centraline interne private che consentano di telefonare e di collegare gli elaboratori utilizzando lo stesso cablaggio.

- **Rete di telefonia mobile**
  La rete di telefonia mobile e quella di radiocomunicazione costituiscono un ampliamento della rete di telefonia fissa. Oltre alla trasmissione vocale e agli SMS (nonché a estensioni multimediali) sono disponibili servizi supplementari che vanno al di là delle offerte della rete fissa. Come procedimenti fisici di trasmissione sono di regola impiegate tecniche radio digitali a commutazione di pacchetti (p. es. GSM, CDMA), orientate soprattutto alla trasmissione vocale. Nel frattempo si è anche tentato di realizzare la telefonia mobile (ancora sulla base dell'*IP Telephony*) sulla base di reti di dati senza fili (WLAN, chiamata anche IEEE 802.11).
- **Reti TV via cavo**
  Le reti via cavo, originariamente allestite per la sola diffusione di trasmissioni radiotelevisive, sono state nel frattempo adattate nella loro struttura fisica in modo da permettere uno scambio di dati bidirezionale. Da tempo è pertanto possibile sia un collegamento a Internet, sia alla rete telefonica mediante IP Telephony.
- **Rete elettrica**
  Anche le reti di distribuzione di energia elettrica sono adatte alla trasmissione di dati. Vi sono alcune imprese di distribuzione di energia che sperimentano e prendono in considerazione la possibilità di proporsi quali fornitori di servizi Internet e offerenti alternativi di servizi di telefonia [35].

Da quanto esposto risulta che *Internet* assume un ruolo di ponte in particolare tra le diverse reti fisiche menzionate. A livello logico (livello OSI 3) Internet offre un servizio universale, che permette la trasmissione di dati per le applicazioni più disparate, non solo in ambito informatico, ma anche in materia di telefonia, radiotelevisione e video (temi trattati più approfonditamente al capitolo 3).

2.44 Necessità di un approccio legislativo più ampio

Poiché esistono diversi protocolli di comunicazione che evolvono in continuazione, una regolamentazione legale in materia di responsabilità non deve fondarsi unicamente su TCP/IP e Internet. Il campo d'applicazione deve estendersi *a tutti i sistemi di trasmissione mediatica mondiali* che consentono a normali utenti di partecipare in modo completo a tali processi di comunicazione.

---

in pacchetti trasmessi singolarmente attraverso la rete, altri utenti possono sfruttare le pause nella conversazione, consentendo così di aumentare fortemente la capacità della linea.

[35] Dal settembre 2001 le aziende elettriche friburghesi (Entreprises Électriques Fribourgeoises) e il provider di telecomunicazioni Sunrise offrono un accesso Internet attraverso la rete elettrica, concepito come alternativa più economica, flessibile ed efficiente rispetto all'accesso tradizionale attraverso la rete telefonica fissa.

Con quest'impostazione di ampio respiro, la regolamentazione sarebbe applicabile a tutti i soggetti implicati nella trasmissione e nella messa a disposizione di informazioni in una rete di comunicazione, a prescindere dagli standard e dai protocolli impiegati.

2.5 Comunicazione di massa e individuale

È importante distinguere tra reati commessi nell'ambito della comunicazione individuale e quelli commessi nell'ambito della comunicazione di massa. Nella comunicazione individuale vale infatti il *segreto delle telecomunicazioni*. Ciò implica una maggior *protezione* dello scambio di informazioni contro ingerenze da parte di terzi, inclusi fornitori d'accesso nonché hosting provider e provider di rete.

2.6. Reti di comunicazione elettronica e media

2.61 Importanti delimitazioni tra diritto delle telecomunicazioni e diritto dei media

È importante operare una *distinzione* netta e *categorica* tra

- le prestazioni del settore delle telecomunicazioni che, in quanto servizi infrastrutturali tecnici e ampiamente automatizzati, si riferiscono alla „trasmissione mediante telecomunicazione di informazioni per terzi" (art. 3 lett. b della legge sulle telecomunicazioni, LTC [36]),

- e il settore della *diffusione di informazioni da parte dei mass media*, che concerne i *contenuti delle informazioni*.

Se una trasmissione televisiva di carattere informativo, come ad esempio „10 vor 10", è offerta in Internet in streaming video, ne risulta una *sovrapposizione di aspetti* legati al diritto delle telecomunicazioni e di aspetti legati al diritto dei media. Poiché il diritto penale si basa su questa distinzione, prevedendo una regolamentazione speciale per i delitti dei media (art. 27, 322bis CP), è di primaria importanza attribuire con precisione al quadro normativo pertinente le prestazioni fornite dalle parti interessate [37].

Le sovrapposizioni menzionate (vedi anche grafico sottostante) impediscono anche che il problema sia risolto soltanto nel contesto della legge sulle telecomunicazioni, o che alle parti coinvolte nella trasmissione di dati in reti di comunicazione sia attribuito il ruolo di un fornitore di servizi di telecomunicazione ai sensi dell'articolo 3 lettere b e c LTC [38].

---

[36] RS 784.10.

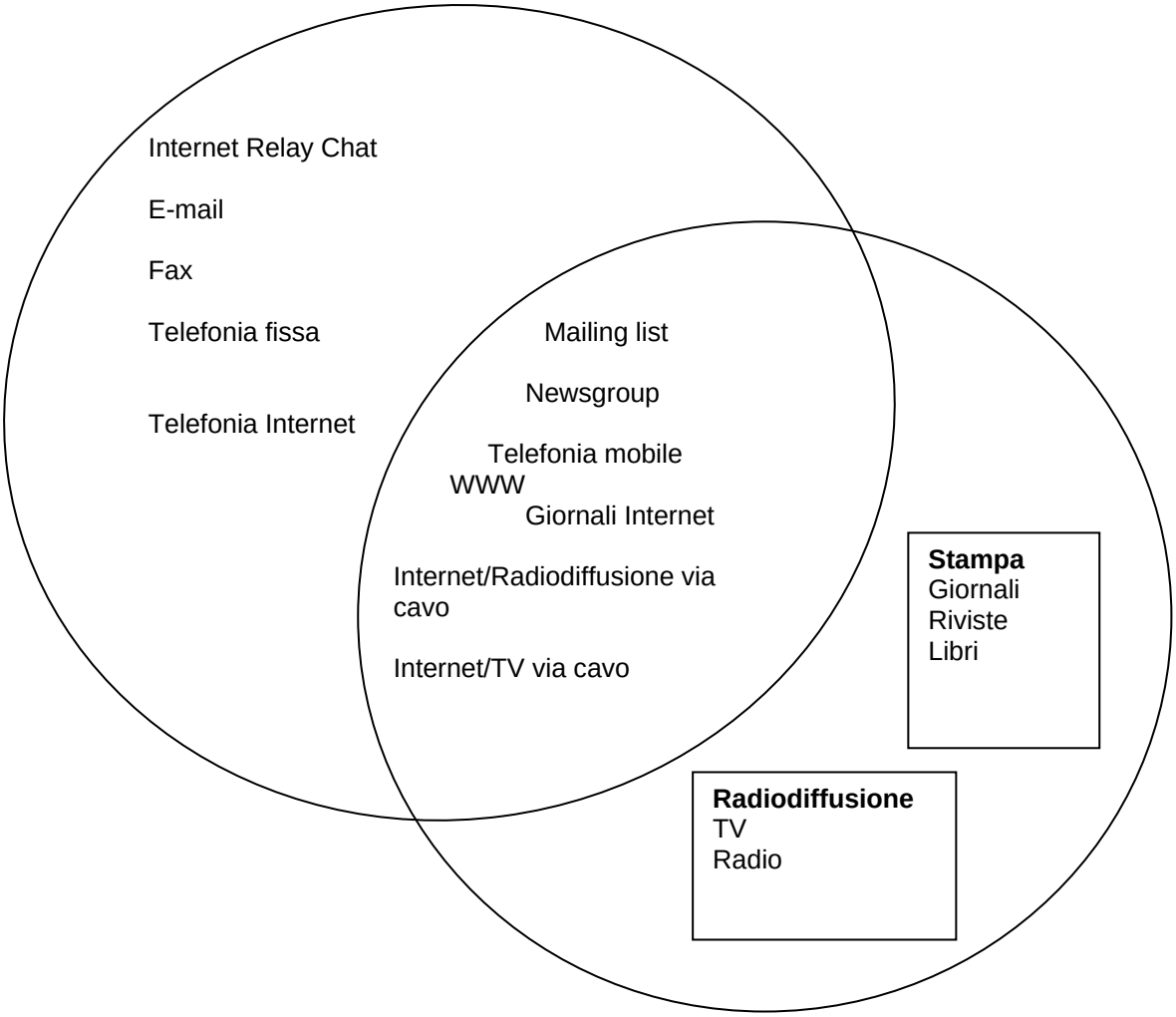
[37] Per maggiori dettagli: NIGGLI/SCHWARZENEGGER, (bibl.), pag. 61 segg.

[38] Art. 3 LTC

…

b. *servizio di telecomunicazione:* trasmissione mediante telecomunicazione di informazioni per terzi;

Reti di telecomunicazione
e corrispondenti
forme di comunicazione



Impiegare la nozione di „fornitore di prestazioni di telecomunicazione“ sarebbe problematico. Tale nozione comprenderebbe infatti unicamente la trasmissione, ma non l’allestimento o la messa a disposizione a fini di trasmissione mediante telecomunicazione. Inoltre l’articolo 2 LTC prevede un’eccezione per i programmi, ai sensi della legge sulla radiotelevisione (LRTV) [39], eccezione che si applica anche a determinate trasmissioni radiofoniche e televisive diffuse in rete. Infine il campo d’applicazione della LTC si estende unicamente ai servizi di comunicazione, ma non ai servizi d’informazione o mediatici.

---

c. *trasmissione mediante telecomunicazione:* emissione o ricezione elettrica, magnetica, ottica oppure elettromagnetica di altro tipo, di informazioni su linea o via radioonde;

[39] RS 784.40.

2.62 Lo sviluppo tecnico ha superato il diritto

La materia disciplinata necessita di chiarimenti: si tratta di definire un settore di prestazioni più vasto, in particolare per quanto riguarda i servizi di comunicazione, d'informazione e mediatici (ossia i vettori di comunicazione *e* di contenuti). Lo sviluppo tecnico ha fortemente accelerato la convergenza di questi settori, mentre l'ordinamento giuridico si basa ancora ampiamente su una separazione tra comunicazione individuale e di massa.

2.63 Rete di comunicazione elettronica come nuova nozione fondamentale

In relazione ai reati con cui si trovano confrontate le reti di comunicazione, vi è urgente necessità di delimitare in modo chiaro la responsabilità di chi crea e di chi mette a disposizione le informazioni, tra fornitori di servizi che mettono a disposizione tali informazioni in una rete di comunicazione perché vengano utilizzate, e fornitori di servizi che consentono unicamente di accedere tecnicamente a tali informazioni nelle reti di comunicazione. Occorre pertanto introdurre nel presente rapporto la nozione, finora non impiegata, di „rete di comunicazione elettronica" (abbreviata in "rete di comunicazione"; vedi in merito n. 9.21).

In alternativa, la letteratura internazionale impiega anche le nozioni seguenti:

- *Sistemi d'informazione* (nozione di diritto europeo):
  la nozione di „sistema d'informazione" è utilizzata nel quadro del diritto dell'UE (3° pilastro, decisione quadro relativa agli attacchi contro i sistemi d'informazione) nel suo senso più ampio possibile, al fine di tenere in considerazione l'intrecciarsi delle reti elettroniche e dei diversi sistemi a essa connessi. Comprende quindi i computer, le agende elettroniche, i telefoni cellulari e le reti interne ed esterne, così come le reti, i server e le infrastrutture particolari di Internet.
- *Rete di dati* (Convenzione sulla cibercriminalità):

Come nozione generale, nella Convenzione del Consiglio d'Europa si parla di rete di dati, o rete di trasmissione di dati, e di cibercriminalità.

I controlli dell'accesso a Internet e ai suoi contenuti, oltre a essere possibili soltanto in misura parziale, sono straordinariamente onerosi e risultano spesso lacunosi. Ogni tipo di controllo può inoltre essere aggirato.

3. Possibilità tecniche di controllo

3.1 Scopo e principi di Internet

Internet è stata sviluppata con lo scopo di creare una *rete di comunicazione* organizzata in modo fortemente decentrato e con un alto grado di disponibilità. Tale rete doveva poter essere utilizzata dai suoi utenti anche in caso di avaria di singoli nodi o collegamenti (p. es. in seguito a un attacco militare). Per il suo funzionamento non sono necessarie autorità centrali. Ogni nodo è indipendente, e nessuna organizzazione esercita autonomamente un controllo su Internet.

Chiunque dispone dei presupposti tecnici necessari può connettersi a Internet. Nel quadro della cosiddetta Internet Engineering Taskforce (IETF), un organo di standardizzazione libero e non governativo, ci si accorda a maggioranza sui protocolli con i quali comunicare e sulle modalità con cui offrire i servizi. In tal modo nessuno (nessun fabbricante o Stato) può disporre di una porzione di Internet. In ragione di questa organizzazione decentrata, le possibilità tecniche di controllare o limitare l'accesso a determinati servizi, contenuti o altri utenti sono estremamente limitate.

3.2 Controlli

In materia di controlli si distinguono due approcci:

- *controllo dell'accesso* : quale server o quali servizi possono essere raggiunti da un utente?
- *Controllo del contenuto*: quali contenuti sono messi a disposizione? [40]

[40] La questione è esposta in modo chiaro in: ULRICH SIEBER, Verantwortlichkeit im Internet, Monaco 1999.

3.21 Controllo dell'accesso

3.211 News

Per quel che riguarda i notiziari, un hosting provider (cfr. n. 2.312) può bloccare l'accesso a determinati gruppi di discussione, omettendo di inserirli nel suo sistema. Per far questo deve analizzare il nome dei gruppi e decidere se da tale nome è possibile dedurre la presenza di contenuti illegali. Ciò può creare difficoltà, poiché in tali gruppi la maggior parte dei contributi può rivelarsi assolutamente conforme alla legge. Gli utenti possono aggirare molto facilmente il blocco messo in atto, ripiegando su altri server accessibili pubblicamente.

3.212 World Wide Web

Nel World Wide Web (WWW, web) il fornitore di accesso (cfr. n. 2.314) può costringere i propri utenti ad accedere al web passando attraverso un cosiddetto *proxy server*, al fine di caricare più velocemente le pagine Internet maggiormente visitate. Il proxy server intercetta le richieste di pagine web e la sua memoria locale rileva se tali pagine sono state recentemente richiamate e memorizzate. In tal caso il proxy server dà seguito direttamente alla richiesta dell'utente, senza andare nuovamente a cercare nel web il contenuto desiderato.

Se il provider offre l'accesso al web unicamente attraverso un proxy server, quest'ultimo può anche essere utilizzato per vietare l'accesso a pagine Internet (URL) o a server (indirizzi IP) determinati (cfr. esempio nel riquadro sottostante).

Proxy server nel mondo arabo

Etisalat, il fornitore d'accesso Internet negli Emirati arabi uniti (EAU), gestisce un proxy server che costituisce l'unico accesso al web. Esistono tuttavia numerosi suggerimenti per eludere tale proxy server, permettendo l'accesso ad altri siti web, il cui contenuto è *illegale* negli EAU [41].

Poiché l'impiego di un proxy server deve essere configurato direttamente nel browser, e dipende quindi dall'utente, i fornitori d'accesso pubblici del mondo occidentale offrono di regola anche l'accesso diretto al WWW. Tra gli sviluppi più recenti vi sono i cosiddetti proxy *trasparenti* (che non devono più essere configurati nel browser dell'utente), grazie ai quali l'accesso a Internet è divenuto più rapido e con i quali si potrebbe anche controllare l'accesso a determinati URL [42].

Il fornitore di accesso può anche configurare il suo *router* (instradatore) [43] o altri apparecchi [44] attraverso i quali viene diretto il flusso di informazioni, affinché le filtrino e non ammettano pacchetti di dati con indirizzi di destinazione (o indirizzi sorgente) determinati, o interi pacchetti HTTP con determinati URL. Di regola l'installazione di

[41] P. es. http://djsyndrome.homestead.com/proxies1.html.
[42] P. es. il Content Engine di Cisco http://www.cisco.com/warp/public/cc/pd/cxsr/ces/index.shtml.
[43] P. es. http://www.cisco.com/warp/public/44/jump/routers.shtml.
[44] P. es. *firewalls* http://www.checkpoint.com o apparecchi per la gestione della larghezza di banda, p. es. www.packeteer.com.

simili controlli d'accesso comporta tuttavia una riduzione della velocità di trasmissione dei dati del *router* (o degli altri apparecchi), poiché per ogni pacchetto di dati occorre effettuare una ricerca per verificare che non vi siano indirizzi bloccati**.**

Di regola i fornitori d'accesso che servono molti clienti possono adottare tali misure di filtraggio in modo estremamente limitato. Un rallentamento di Internet a causa dell'impiego di simili filtri non sarebbe accettato dai clienti, abituati a velocità sempre più elevate. Ciò sarebbe anche in contrasto con la rapida diffusione di un accesso veloce ed economico a Internet, espansione auspicata per ragioni tecnologiche, sociali, formative e di politica economica.

Occorre inoltre considerare che bloccando l'accesso a server o siti web si penalizzerebbero anche numerosi contenuti legali: a titolo di esempio, il blocco del server di un hosting provider come *geocities* potrebbe concernere migliaia di pagine web.

Anche in questo caso, gli utenti sufficientemente motivati ed esperti hanno a disposizione diverse *possibilità di aggiramento* delle barriere: esistono infatti proxy server pubblici (ad esempio all'estero) collegati con altri fornitori di prestazioni Internet, che permettono indirettamente l'accesso a servizi bloccati [45].

Il fornitore di contenuti può anche cambiare l'indirizzo del suo server, di modo che i filtri divengano inefficaci e rendendo così inutile l'installazione di un blocco dell'accesso. Le esperienze accumulate dimostrano che gli offerenti di contenuti illegali sfruttano regolarmente tale possibilità.

3.22 Controllo dei contenuti

Per procedere a tale controllo l'hosting provider deve analizzare regolarmente i contenuti (testi e dati multimediali) offerti sul suo elaboratore. In considerazione dell'enorme volume di dati (svariati tera [bilioni] di bytes) e della frequenza con cui vengono apportate modifiche, un simile controllo dei contenuti pone spesso all'hosting provider problemi irrisolvibili.

Una ricerca affidabile e completamente automatizzata dei contenuti protetti da diritti d'autore o addirittura di quelli illegali è praticamente *impossibile*. Esistono certamente algoritmi per l'analisi semantica di testi o immagini, ma richiedono calcoli estremamente complessi e oltretutto sono soggetti a errori; le ricerche in tale campo sono comunque ancora in corso.

È pure possibile cercare rapidamente „impronte digitali elettroniche"[46] di testi conosciuti o di dati multimediali. Tuttavia, modificando i dati (è sufficiente un bit), il provider può facilmente impedire che i suoi contenuti possano essere identificati. Un fornitore di contenuti può di regola agevolmente ripiegare su un altro dei numerosi

[45] Vi è ad esempio una lista all'indirizzo http://tools.rosinstrument.com/proxy/.
[46] Un'„impronta digitale elettronica" consiste spesso in un numero binario lungo 32-160 bit, che può essere calcolato matematicamente a partire da un documento elettronico o da un'immagine; l'impronta digitale caratterizza tale documento o immagine. Cambiando anche solo un bit nel documento, viene modificata l'impronta digitale.

hosting provider (anche in un altro Stato), qualora abbia sentore che i contenuti da lui offerti siano classificati.
Diventano sempre più popolari i servizi *peer to peer* (P2P) per lo scambio diretto di dati tra utenti senza l'intermediazione di un'entità centrale. In tali casi il controllo dei contenuti può essere effettuato unicamente dall'utente finale. Nei *servizi di filesharing*, come ad esempio Gnutella o Morpheus, l'utente finale può decidere quali dati intende mettere a disposizione. In un servizio quale *Freenet* [47] invece, considerato il modo in cui esso è stato concepito, l'utente non ha la possibilità di effettuare un controllo dei contenuti, poiché i dati offerti sono memorizzati nel suo computer in modo criptato, senza che lui sia a conoscenza della chiave.

3.3 Efficacia

Riassumendo si constata che Internet, per il modo in cui è concepita, *mal si presta a un controllo centrale o alla sorveglianza*. Ogni misura di controllo può essere aggirata da utenti più o meno abili o da offerenti di contenuti illegali.

Ogni volta che una nuova misura di controllo viene presa in considerazione, si sviluppano immediatamente contromisure tecniche volte ad aggirarla [48]. Le misure di controllo prescritte possono quindi sì arginare gli accessi ai contenuti illegali, ma esistono pur sempre possibilità di eluderle**.**

Complessivamente, anche solo per motivi di ordine tecnico, *non appare sensato* obbligare gli access provider a bloccare l'accesso a contenuti illegali, o costringere gli hosting provider a controllare preventivamente la conformità alla legge di ogni contenuto offerto loro da terzi.

[47] http://freenetproject.org/, descrizione (in tedesco) all'indirizzo http://archiv.tu-chemnitz.de/pub/2002/0050/data/vortrag.html.
[48] La minaccia di chiudere *Napster* è stata una delle ragioni che hanno portato allo sviluppo di servizi di file sharing come Gnutella, per i quali non vi è più un elaboratore centrale con funzione di intermediazione.

La diffusione di informazioni su scala mondiale, resa possibile in particolare grazie al World Wide Web, esige un coordinamento giuridico a livello internazionale. Assumono quindi una grande importanza per la Svizzera i principi sanciti dagli Stati UE nella „direttiva sul commercio elettronico".

4. La direttiva UE sul commercio elettronico e la sua attuazione negli Stati confinanti con la Svizzera

4.1 Generalità sulla direttiva 2000/31 del Parlamento europeo e del Consiglio dell'8 giugno 2000 („direttiva sul commercio elettronico")

L'8 giugno 2000 il Parlamento europeo e il Consiglio dell'Unione europea hanno emanato la direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico nel mercato interno (direttiva sul commercio elettronico) [49].

I 24 articoli della direttiva sono preceduti da 65 *considerandi*. Scopo della direttiva è garantire che il commercio elettronico *possa sfruttare appieno le opportunità offerte dal mercato interno*. Ciò può avvenire soltanto *eliminando gli ostacoli giuridici*, costituiti da un lato dalle divergenti normative nazionali e dall'altro dall'incertezza sul diritto nazionale applicabile ai servizi della società dell'informazione.

Per garantire in futuro la *certezza del diritto* e la fiducia dei consumatori, la direttiva deve stabilire un quadro generale chiaro per determinati aspetti giuridici del commercio elettronico nel mercato interno.

La direttiva si prefigge di creare un quadro giuridico inteso ad assicurare la libera circolazione dei servizi della società dell'informazione tra gli Stati membri, *e non di armonizzare il settore del diritto penale in quanto tale*[50,51]. In particolare la direttiva

[49] Direttiva sul commercio elettronico, cit.: DIRETTIVA (bibl.).

[50] Vedi DIRETTIVA (bibl.), pag. 2 seg., n. 5-8. L'art. 2 cpv. 2 della direttiva afferma in termini generali che essa mira (unicamente) a *uniformare* talune norme nazionali sui servizi della società dell'informazione, in particolare quelle che interessano gli intermediari e i provider.

[51] L'*armonizzazione del diritto penale e della procedura penale* è invece perseguita dalla Convenzione del Consiglio d'Europa sulla cibercriminalità, ETS-n° 185, („*Cybercrime-Convention*"), sottoscritta il 23 novembre 2001 a Budapest anche dalla Svizzera. Il titolo ufficiale di questa Convenzione europea sulla cibercriminalità è „Convention on Cybercrime (Convention sur la cybercriminalité)". Il testo della Convenzione è reperibile in Internet, all'indirizzo http://conventions.coe.int. Il contenuto sarà approfondito al n. 10.21. - Cfr. inoltre la *„Déclaration sur la liberté de la communication sur l'Internet"* del Comitato dei Ministri del Consiglio d'Europa, del 28 maggio 2003, nella quale si sono riflessi i principi fondamentali della direttiva UE sul commercio elettronico. Tale testo è reperibile in Internet all'indirizzo:

non è volta ad incidere sui principi e sulle norme fondamentali nazionali in materia di libertà di espressione [52].

In conformità al *principio di proporzionalità*, le misure previste dalla direttiva si limitano al minimo necessario per raggiungere l'obiettivo del buon funzionamento del mercato interno. La direttiva, nei casi in cui si deve intervenire a livello comunitario per far sì che lo spazio interno sia veramente libero da frontiere per il commercio elettronico, deve garantire un alto livello di tutela degli obiettivi di interesse generale, come la protezione dei minori e della dignità umana, la tutela del consumatore e della sanità pubblica [53].

4.2 Gli articoli 12-15 della direttiva sul commercio elettronico (responsabilità dei prestatori intermediari)

4.21 Osservazioni preliminari

La *responsabilità del „prestatore“* [54], ossia del provider, è *una delle norme più importanti* della direttiva sul commercio elettronico. Si trova pertanto al centro della direttiva, negli articoli 12-15, sotto il titolo „Responsabilità dei prestatori intermediari“.

Per poter perseguire l'obiettivo definito nei considerandi della direttiva, ossia l'eliminazione dell'incertezza giuridica [55], negli articoli 12-15 si determina in quali casi o a quali condizioni *i provider non sono ritenuti responsabili*.

La direttiva utilizza la nozione di „deroghe“, di „deroghe in materia di responsabilità“ o di „limitazioni alla responsabilità“ [56]. Si parte quindi implicitamente dal *principio della responsabilità del provider*. Viene lasciata completamente aperta la questione relativa ai principi generali sui quali si fonda tale responsabilità e alle motivazioni sulle quali poggia; può eventualmente essere dedotta *e contrario*, anche se in modo poco appropriato, a partire dal carattere derogatorio delle norme [57].

Nemmeno i considerandi spiegano su cosa si basa la responsabilità del provider. Vi si afferma al contrario che „le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione, sulla quale sono trasmesse o temporaneamente

---

http://www.coe.int/T/F/Droits_de_l%27Homme/media/5_Ressources_documentaires/1_Textes_de_base/2_%20Textes_du_Comite_des_Ministres/PDF_D%E9claration%20libert%E9%20de%20communication%20sur%20Internet%20%20(f).pdf.

[52] DIRETTIVA (bibl.), pag. 2, n. 4.

[53] DIRETTIVA (bibl.), pag. 2, n. 10.

[54] La definizione di prestatore si trova all'articolo 2 lettera b della DIRETTIVA (bibl.). „Prestatore“ è la persona fisica o giuridica che fornisce un servizio della società dell'informazione.

[55] DIRETTIVA (bibl.), pag. 6, n. 40.

[56] DIRETTIVA (bibl.), pag. 6, nn. 42-46.

[57] Secondo SATZGER (bibl.), pag. 109 segg., 111, gli articoli 12-15 della direttiva fungerebbero quindi da „filtro“: la direttiva avrebbe pertanto lo scopo „di limitare in modo generale la responsabilità per attività illecite in rete da parte di terzi, senza contemporaneamente modificare disposizioni di diritto materiale nazionali che fondano una violazione della legge“.

memorizzate le informazioni messe a disposizione da terzi, al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate“[58].

Con gli articoli 12-15, la direttiva sul commercio elettronico istituisce di principio una normativa unitaria sulla responsabilità, ossia una *norma orizzontale* applicabile a ogni ambito giuridico (diritto penale, diritto della responsabilità civile, diritti d'autore, diritto della concorrenza, ecc.) [59]. Questo approccio normativo di ampio respiro spiega anche perché la direttiva non indica su quale base legale poggi la responsabilità del prestatore, in relazione ai diversi ambiti giuridici. Finché nei Paesi dell'Ue non esisterà una base legale che fondi la responsabilità di una parte di tali prestatori di servizi, la direttiva sul commercio elettronico resterà lettera morta.

Occorre inoltre osservare che l'UE, in base al Trattato che istituisce la Comunità europea, non ha *alcuna competenza legislativa nell'ambito del diritto penale*. La modifica delle condizioni di punibilità costituisce perciò una conseguenza indiretta dell'armonizzazione giuridica nel mercato interno, che può concernere di principio soltanto prestazioni fornite dietro compenso. Per essere realmente in grado di garantire la certezza del diritto perseguita, gli Stati membri devono procedere a un'attuazione che travalichi i confini del mercato interno, vale a dire oltre l'ambito di competenze del diritto dell'UE. [12]

4.22 Art. 12: Nessuna responsabilità per il semplice trasporto

Art. 12 Semplice trasporto

(1) Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non sia responsabile delle informazioni trasmesse a condizione che egli:

a) non dia origine alla trasmissione;
b) non selezioni il destinatario della trasmissione; e
c) non selezioni né modifichi le informazioni trasmesse.

(2) Le attività di trasmissione e di fornitura di accesso di cui al paragrafo 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo.

---

[58] DIRETTIVA (bibl.), pag. 6, n. 42.

[59] Vedasi in merito NIGGLI/SCHWARZENEGGER (bibl.), pag. 63 segg., 66 segg. In merito ai grandi inconvenienti di questo approccio legislativo, in contrapposizione con il disciplinamento specifico per settore, in particolare per quel che riguarda il diritto penale, vedasi loc. cit., pag. 66 seg.

[61] DIRETTIVA (bibl.), pag. 6, n. 43.

(3) Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione.

In sintesi, l'articolo 12 della direttiva sul commercio elettronico esclude la responsabilità del provider per il mero trasporto (fornitore d'accesso, capoverso 1). Il fornitore d'accesso non è responsabile nemmeno delle informazioni memorizzate in modo automatico, intermedio e transitorio, se la memorizzazione serve unicamente alla trasmissione dei dati (capoverso 2). In entrambi i casi il fornitore d'accesso non deve intervenire in alcun modo sulle informazioni trasmesse, e in particolare non deve averle modificate [61].

4.23 Art. 13 e 14: Nessuna responsabilità per caching o hosting

Art. 13 Caching

(1) Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che egli:

a) non modifichi le informazioni;
b) si conformi alle condizioni di accesso alle informazioni;
c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore,
d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni, e
e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso.

(2) Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione.

Come nel caso del semplice trasporto [62], l'esclusione della responsabilità vale unicamente quando il prestatore che memorizza le informazioni nella sua memoria cache (proxy caching provider) *non ha nulla a che vedere* con le informazioni trasmesse. Un proxy caching provider che collabora deliberatamente con un fornitore d'accesso al fine di commettere atti illeciti non si limita al semplice trasporto e al caching, e non beneficia pertanto dell'esclusione della responsabilità [63].

Art. 14 Hosting

[62] Vedi n. 4.22 *in fine*.

[63] Cfr. DIRETTIVA (bibl.), pag. 6, n. 44.

(1) Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o
b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

(2) Il paragrafo 1 non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

(3) Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime.

L'hosting provider può beneficiare di una limitazione della responsabilità soltanto se, appena è stato informato o si rende conto di attività illecite, interviene immediatamente per rimuovere le informazioni corrispondenti o per bloccare l'accesso alle medesime [64].

4.24 Art. 15: Assenza dell'obbligo generale di sorveglianza

Art. 15 Assenza dell'obbligo generale di sorveglianza

(1) Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

(2) Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati.

Secondo l'articolo 15 della direttiva sul commercio elettronico, ai provider summenzionati non può essere imposto alcun obbligo generale di sorveglianza sulle informazioni da loro trasmesse e memorizzate, o di ricerca di circostanze che indichino la presenza di un'attività illecita. La direttiva non impedisce tuttavia agli

[64] DIRETTIVA (bibl.), pag. 6, n. 46.

Stati membri di definire procedure volte alla rimozione di informazioni o al blocco dell'accesso alle medesime [65].

4.3 L'attuazione degli articoli 12-15 della direttiva sul commercio elettronico negli Stati confinanti con la Svizzera [66]

4.31 Germania

Con la sua legge del 22. luglio 1997 sull'utilizzo dei servizi di telecomunicazione (*Gesetz über die Nutzung von Telediensten; Teledienstegesetz,* TDG [67]), la Germania ha optato, analogamente alla direttiva sul commercio elettronico ma con un paio di anni d'anticipo su di essa, per una *regolamentazione orizzontale*, ossia per un disciplinamento unitario della responsabilità nel settore dei servizi dell'informazione e della comunicazione.

La regolamentazione orizzontale nel diritto nazionale ha come conseguenza che il provider, se soddisfa le condizioni per beneficiare dell'esclusione della responsabilità, non può essere citato in giudizio né sul piano civile, né su quello penale. Non è chiaro a che livello occorra analizzare la questione in relazione alle condizioni di responsabilità e di punibilità (fattispecie, illiceità, colpa, o fattore da analizzare al di fuori di questa struttura, vedi n. 9.121). È invece certo che, qualora le condizioni citate non siano soddisfatte, la responsabilità e la punibilità vadano analizzate in base alle rispettive fattispecie dell'ambito giuridico in questione.

Per attuare la direttiva, il 14 dicembre 2001 il legislatore tedesco ha emanato la legge sulle condizioni quadro giuridiche per il commercio elettronico (*Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr; Elektronisches Geschäftsverkehrsgesetz*, EGG). Tale legge è entrata in vigore il 21 dicembre 2001.

L'articolo 1 EGG *comporta l'introduzione di nuove norme sulla responsabilità nella legge sui servizi di telecomunicazione* [68] [69]: gli articoli 8-11 della riveduta TDG si trovano nella sezione 3, sotto il titolo „Responsabilita".

---

[65] DIRETTIVA (bibl.), pag. 6, n. 44.

[66] Il Liechtenstein, Stato limitrofo membro dello SEE e dell'AELS ma non dell'UE, non ha ancora attuato la direttiva sul commercio elettronico e non dispone quindi di norme specifiche sulla responsabilità in questo ambito. – Per maggiori dettagli, cfr. la perizia allestita nel 2002 dall'Istituto svizzero di diritto comparato, su mandato dell'Ufficio federale di giustizia, relativa alle legislazioni dei 15 Stati membri dell'UE e degli Stati Uniti (stato al 23 agosto 2002).

[67] Fonte: BGBl I 1997, 1870.

[68] Fonte: BGBl I 2001, 3721. Link per la TDG nuova versione: http://www.bundesrecht.juris.de/bundesrecht/tdg/index.html.

[69] Le „vecchie" disposizioni originali della TDG sulla responsabilità, in particolare l'art 5, avevano sollevato problemi, soprattutto per quanto attiene alla questione della respnsabilità del fornitore d'accesso. In merito vedasi SATZGER (bibl.), pag. 113 segg. con argomentazioni, e n. 9.121.

§ 8 Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11 unberührt. Das Fernmeldegeheimnis nach § 85 des Telekommunikationsgesetzes ist zu wahren.

Secondo l'articolo 8 capoverso 1, il prestatore di servizi è responsabile delle proprie informazioni. L'articolo 8 capoverso 2 concreta l'articolo 15 paragrafo 1 della direttiva sul commercio elettronico (assenza dell'obbligo generale di sorveglianza). Il legislatore tedesco non ha fatto uso della possibilità, prevista dall'articolo 15 paragrafo 2 della direttiva, di obbligare il prestatore di servizi a informare su presunte attività illecite.

§ 9 Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

A determinate condizioni, il semplice trasporto di informazioni e la mera fornitura di accesso vengono escluse dalla responsabilità.

§ 10 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen

Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung der fremden Information an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie
1. die Informationen nicht verändern,
2. die Bedingungen für den Zugang zu den Informationen beachten,
3. die Regeln für die Aktualisierung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,
4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und

5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

§ 9 Abs. 1 Satz 2 gilt entsprechend.

La nuova versione dell'articolo 10 TDG riprende quasi testualmente l'articolo 13 della direttiva sul commercio elettronico, escludendo quindi la responsabilità in caso di *proxy caching*.

§ 11 Speicherung von Informationen

Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern
1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.

Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

La nuova versione dell'articolo 11 TDG regola infine le condizioni per l'esclusione della responsabilità dell'hosting provider (attuazione dell'articolo 14 della direttiva sul commercio elettronico).

4.32 Austria

In Austria la responsabilità del prestatore di servizi è disciplinata dalla quinta sezione della legge sul commercio elettronico (*E-Commerce-Gesetz; ECG* [70]). Con gli articoli 13-19 ECG, l'Austria non solo ha ampiamente attuato gli articoli 12-15 della direttiva UE, ma *si è addirittura spinta oltre*, prevedendo espressamente un'esclusione della responsabilità per quel che riguarda i motori di ricerca (art. 14) e i links (art. 17). Come nel caso della direttiva sul commercio elettronico e della TDG tedesca, negli articoli 13 e seguenti si è optato *per una regolamentazione orizzontale*.

§ 13 Ausschluss der Verantwortlichkeit bei Durchleitung

(1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zu einem Kommunikationsnetz vermittelt, ist für die übermittelten Informationen nicht verantwortlich, sofern er

[70] Il titolo completo della legge è il seguente: Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden: vedi BGBl. (austriaco.) I n. 152/2001. L'ECG è entrata in vigore il 1° gennaio 2002 ed è reperibile all'indirizzo: http://www.ris.bka.gv.at/bundesrecht/.

1. die Übermittlung nicht veranlasst,
2. den Empfänger der übermittelten Informationen nicht auswählt und
3. die übermittelten Informationen weder auswählt noch verändert.

(2) Die Übermittlung von Informationen und die Vermittlung des Zugangs im Sinn des Abs. 1 umfassen auch die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen, soweit diese Zwischenspeicherung nur der Durchführung der Übermittlung im Kommunikationsnetz dient und die Information nicht länger gespeichert wird, als es für die Übermittlung üblicherweise erforderlich ist.

§ 14 Verantwortlichkeit bei Suchmaschinen

(1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er

1. die Übermittlung der abgefragten Informationen nicht veranlasst
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

§ 15 Ausschluss der Verantwortlichkeit bei Zwischenspeicherungen (Caching)

Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt, ist für eine automatische, zeitlich begrenzte Zwischenspeicherung, die nur der effizienteren Gestaltung der auf Abruf anderer Nutzer erfolgenden Informationsübermittlung dient, nicht verantwortlich, sofern er

1. die Information nicht verändert,
2. die Bedingungen für den Zugang zur Information beachtet,
3. die Regeln für die Aktualisierung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, beachtet,
4. die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigt und
5. unverzüglich eine von ihm gespeicherte Information entfernt oder den Zugang zu ihr sperrt, sobald er tatsächliche Kenntnis davon erhalten hat, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt oder der Zugang zu ihr gesperrt wurde oder dass ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperre angeordnet hat.

§ 16 Ausschluss der Verantwortlichkeit bei Speicherung fremder Inhalte (Hosting)

(1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert, ist für die im Auftrag eines Nutzers gespeicherten Informationen nicht verantwortlich, sofern er

1. von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände

bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er diese Kenntnis oder dieses Bewusstsein erhalten hat, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

(2) Abs. 1 ist nicht anzuwenden, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

§ 17 Ausschluss der Verantwortlichkeit bei Links

(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Information nicht verantwortlich,

1. sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird oder der Diensteanbieter die fremden Informationen als seine eigenen darstellt.

§ 18 Umfang der Pflichten der Diensteanbieter

(1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.

(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgabe bildet.

(4) Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

(5) Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt.

§ 19 Weitergehende Vorschriften

(1) Die §§ 13 bis 18 lassen gesetzliche Vorschriften, nach denen ein Gericht oder eine Behörde dem Diensteanbieter die Unterlassung, Beseitigung oder Verhinderung einer Rechtsverletzung auftragen kann, unberührt.

(2) Abs. 1 sowie §§ 13 bis 18 sind auch auf Anbieter anzuwenden, die unentgeltlich elektronische Dienste bereitstellen.

4.33 Francia

Il 1° agosto 2000 la Francia ha apportato un'importante modifica legislativa per quel che concerne le disposizioni sulla punibilità dei provider. In tale data è stato in particolare introdotto l'articolo 43-8 capoverso 1 nella legge sulla libertà della comunicazione (*Loi du 1er août 2000 relative à la liberté de communication* [71,72]). Questa disposizione si trova nel capitolo VI (Dispositions relatives aux services de communication en ligne autres que de correspondance privée).

Con l'articolo 43-8 capoverso 1 è stato introdotto il *principio della responsabilità limitata*. Di conseguenza il provider è responsabile unicamente se, dopo ingiunzione giudiziaria, non blocca l'accesso a una pagina Internet illegale. L'articolo 43-8 capoverso 2 prevedeva inoltre la possibilità di ritenere punibile l'hosting provider che, informato da un utente, non avesse reagito bloccando l'accesso ai contenuti illegali. Ancora prima della sua entrata in vigore, questa disposizione è invece stata dichiarata *incostituzionale* dal Conseil constitutionnel [73].

Il tenore delle disposizioni francesi sulla responsabilità è ora il seguente:

> **Art. 43-7.** - Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée sont tenues, d'une part, d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, d'autre part, de leur proposer au moins un de ces moyens.
>
> **Art. 43-8.** - Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :
> - si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu;.[...]
>
> **Art. 43-9.** - Les prestataires mentionnés aux articles 43-7 et 43-8 sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires.

---

[71] Vedi anche n. 9.121.

[72] Link: http://www.foruminternet.org/texte/documents/lois/lire.phtml?id=22.

[73] Cfr. decisione del Conseil constitutionnel n° 2000-433 DC del 27 luglio 2000, JO del 2 agosto 2000, 11922 segg., 11926. Approfondimenti in MOREILLON/DE COURTEN, (bibl.), pag.12, e i rinvii menzionati. Per l'ulteriore evoluzione della legislazione francese in materia, in seguito a questa decisione del Conseil constitutionnel, vedi n. 9.121.

Ils sont également tenus de fournir aux personnes qui éditent un service de communication en ligne autre que de correspondance privée des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 43-10.
Les autorités judiciaires peuvent requérir communication auprès des prestataires mentionnés aux articles 43-7 et 43-8 des données mentionnées au premier alinéa. Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.
Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.

Art. 43-10. - I. - Les personnes dont l'activité est d'éditer un service de communication en ligne autre que de correspondance privée tiennent à la disposition du public :
- s'il s'agit de personnes physiques, leurs nom, prénom et domicile ;
- s'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social ;
- le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi no 82-652 du 29 juillet 1982 sur la communication audiovisuelle ;
- le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8.
II. - Les personnes éditant à titre non professionnel un service de communication en ligne autre que de correspondance privée peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au I.

4.34 Italia

Con la legge del 1° marzo 2002 (n. 39, „Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2001"), il Parlamento italiano ha delegato al Governo anche l'attuazione della direttiva sul commercio elettronico nell'ordinamento giuridico italiano; la disposizione pertinente è l'*articolo 31* (Attuazione della direttiva 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno) [74].

La norma di delega, l'articolo 1 della Legge comunitaria 2001, prescrive al Governo di emanare la corrispondente ordinanza entro un anno dall'entrata in vigore della legge. Tale termine è nel frattempo [75] scaduto inutilizzato.

lotta contro la criminalità in rete deriva dal mandato costituzionale che impone la tutela dei beni giuridici. Nell'adottare le misure necessarie, lo Stato è tuttavia vincolato dai precetti costituzionali ed è in particolare tenuto a rispettare i diritti fondamentali relativi alla libera comunicazione.

[74] Link: http://www.parlamento.it/parlam/leggi/02039l.htm#31.1.

[75] Ossia dopo la pubblicazione nella Gazzetta Ufficiale n. 72 del 26 marzo 2002 – Supplemento Ordinario n. 54.

La lotta contro la criminalità in rete deriva dal mandato costituzionale che impone la tutela dei beni giuridici. Nell'adottare le misure necessarie, lo Stato è tuttavia vincolato dai precetti costituzionali ed è in particolare tenuto a rispettare i diritti fondamentali relativi alla libera comunicazione.

5. Condizioni quadro costituzionali

5.1 Il mandato costituzionale relativo alla tutela dei beni giuridici

5.11 Oggetto del mandato

Le *libertà fondamentali e i diritti all'integrità* sono beni giuridici basilari, e la Costituzione ne affida la tutela allo Stato. In un moderno Stato costituzionale democratico come la Svizzera tali beni giuridici costituiscono per così dire un pilastro fondamentale, sul quale poggia l'intero ordinamento giuridico e statuale [76].

Questo principio è stato espressamente sancito nella nuova Costituzione federale (Cost.) [77], nell'articolo 35 capoverso 1 („I diritti fondamentali devono improntare l'intero ordinamento giuridico"). Oggi i diritti fondamentali non rappresentano più soltanto dei diritti di cui l'individuo beneficia per difendersi nei confronti dello Stato: l'autorità statuale è anche tenuta a tutelare effettivamente i diritti e le libertà garantiti dal testo costituzionale.

Gli articoli 10 Cost. (integrità fisica e psichica) o l'articolo 8 capoverso 2 Cost. (protezione contro la discriminazione) obbligano lo Stato a garantire una protezione effettiva contro i pregiudizi causati da privati. Il compito di proteggere i beni giuridici affidato al diritto costituzionale ha un *carattere pragmatico*: sussiste indipendentemente dal luogo in cui la violazione del bene giuridico è stata commessa e dai mezzi (tecnici) impiegati. La „tutela dei diritti fondamentali" è quindi un compito che spetta allo Stato, e che comprende la lotta contro gli attacchi portati ai beni giuridici protetti costituzionalmente nonché la prevenzione di tali attacchi, anche quando essi avvengono in reti di comunicazione elettronica.

[76] JÖRG PAUL MÜLLER, Grundrechte, in: Kälin/Bolz (ed.), Handbuch des bernischen Verfassungsrechts, Berna/Stoccarda/Vienna 1995, pag. 29.
[77] RS 101.

5.12 L'adempimento del mandato costituzionale

In relazione all'adempimento del mandato costituzionale volto alla tutela dei beni giuridici fondamentali (cfr. n. 5.11), il legislatore è confrontato con una serie di *domande*:

- con quali *strumenti normativi* occorre combattere e prevenire pregiudizi e lesioni di beni giuridici? Sono sufficienti raccomandazioni dell'autorità, o vi è la necessità di adottare prescrizioni di diritto civile, penale e/o amministrativo?
- *Contro chi* vanno indirizzate le misure di tutela statuali? In che misura i fabbricanti, i proprietari e i gestori di installazioni tecniche possono essere ritenuti giuridicamente „responsabili"?
  - *Diritto privato*: nello svolgimento di ogni attività possono essere causati danni: tale situazione va affrontata prevedendo una responsabilità aquiliana, causale o per rischio?
  - *Diritto penale*: la fattispecie penale dovrà assumere i contorni di un reato intenzionale o per negligenza? Nel secondo caso fino a dove deve spingersi l'obbligo di diligenza da osservare, e fino a che punto si può pretendere l'adozione di misure protettive?
  - *Diritto amministrativo*: le misure di polizia atte a proteggere i beni giuridici fondamentali devono essere dirette soltanto verso coloro che hanno messo tali beni in pericolo o li hanno perturbati, direttamente o per il tramite del comportamento di terzi di cui sono responsabili („perturbatori per comportamento") [78]? O dette misure devono concernere anche quelle persone che hanno il controllo, giuridico o effettivo, sull'oggetto che è causa della situazione illecita („perturbatori per situazione") [79]? Fino a che punto vanno inclusi coloro che, con la loro azione o la loro inazione, fanno sì che terzi mettano in pericolo o perturbino i beni giuridici protetti dalla Costituzione („perturbatori indiretti") [80]?

5.2 Vincoli costituzionali in relazione alla tutela dei beni giuridici

A prima vista, i quesiti appena sollevati (n. 5.12) e gli argomenti da utilizzare per risolverli appaiono di natura meramente politica. In realtà, nell'elaborare le misure atte a impedire la lesione di beni giuridici, il legislatore non è libero, ma è per molti aspetti *vincolato dalla Costituzione*.

---

[78] Cfr. in particolare DTF 122 II 70; 118 Ib 415. – Nel presente contesto potrebbe essere ritenuto „*perturbatore per comportamento*" un fornitore di contenuti.

[79] Cfr. in particolare DTF 122 II 70; 118 Ib 415. – Nel presente caso potrebbe essere ritenuto „*perturbatore per situazione*" un hosting provider.

[80] Cfr. in merito DTF 99 Ia 511; HÄFELIN/MÜLLER (bibl.), Rz. 2497 segg.; DANIEL THÜRER, Das Störerprinzip im Polizeirecht, in: ZSR 102 (1983) I 463 segg., 477 seg. – Nel presente caso potrebbe essere ritenuto „*perturbatore indiretto*" un fornitore d'accesso.

5.21 Efficiente tutela dei diritti fondamentali

La Costituzione (art. 35 cpv. 1) incarica il legislatore di provvedere affinché i diritti fondamentali siano tutelati in modo *effettivo* ed *efficiente* [81]. Nella scelta degli strumenti normativi l'orientamento del legislatore deve rispettare tale direttiva.

5.22 Ordinamento delle competenze a livello federale

Dai diritti fondamentali non è possibile dedurre nuove competenze federali. La tutela dei diritti fondamentali deve essere attuata in base all'ordinamento delle competenze previsto dalla Costituzione federale (art. 42 segg. Cost.) [82]. Pertanto, nel presente contesto, misure di diritto federale volte alla tutela di beni giuridici protetti a livello costituzionale sono ammissibili unicamente se la Costituzione federale prevede una corrispondente competenza della Confederazione nell'ambito delle reti di telecomunicazioni [83].

5.23 Valore istituzionale dei diritti fondamentali

Nell'elaborare i provvedimenti di protezione, il legislatore deve considerare soprattutto il grado istituzionale delle libertà fondamentali, nel presente caso i diritti fondamentali alla libera comunicazione [84].

Occorre qui porre l'accento sul ruolo basilare di tali diritti in una società democratica. Dottrina [85] e giurisprudenza [86] non vedono nei diritti fondamentali soltanto un indispensabile elemento di realizzazione individuale: a tali diritti attribuiscono anche una funzione imprescindibile per una collettività fondata sulla democrazia.

Il dibattito democratico deve essere tutelato da ingerenze dirette e indirette. Le ingerenze indirette possono risultare da misure che, comminando sanzioni in caso di affermazioni illegali, ostacolano in modo fattivo la libera comunicazione, esplicando in tal modo un effetto intimidatorio sui cittadini (il cosiddetto „*chilling effect*“) [87]. Per lo

---

[81] DFGP, Riforma della Costituzione federale, Commenti al progetto di Costituzione del 1995, Berna 1995, pag. 64; RENÉ RHINOW, Die Bundesverfassung 2000, Eine Einführung, Basilea/Ginevra/Monaco 2000, pag. 152; PETER SALADIN, Grundrechte im Wandel, 3. ed., Berna 1982, pag. 294 segg., *stesso autore*, Die Funktion der Grundrechte in einer revidierten Verfassung, in: Die Kunst der Verfassungsrevision, Schriften zur Verfassungsreform 1968-1996, Basilea/Francoforte s.M. 1998, pag. 47 segg., 57 segg.

[82] Cfr. in particolare JEAN-FRANÇOIS AUBERT, Bundesstaatsrecht der Schweiz, versione del 1967, supplemento rielaborato fino al 1990, Volume I, Basilea/Francoforte s.M. 1991, ad n. 699; HÄFELIN/HALLER (bibl.), n. marg. 1070.

[83] Cfr. in merito n. 7.12.

[84] Art. 16 e 17 Cost; cfr. anche art. 10 CEDU.

[85] ANDREAS AUER/GIORGIO MALINVERNI/MICHEL HOTTELIER, Droit constitutionnel suisse, Volume II: Les droits fondamentaux, Berna 2000, n. marg. 486; HÄFELIN/HALLER (bibl.), n. marg. 447; MÜLLER, GRUNDRECHTE (bibl.), pag. 183 seg.; JÖRG PAUL MÜLLER, § 39 Allgemeine Bemerkungen zu den Grundrechten, in: Thürer/Aubert/Müller (ed.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurigo 2001, n. marg. 16, pag. 628.

[86] DTF 96 I 592.

[87] Cfr. in merito soprattutto JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechtliche Fragen zum Internet, Medialex 1997, pag. 198 segg., 203: „Dal punto di vista dei diritti fondamentali, a nostro avviso sarebbe possibile obbligare i provider (operatori di sistema, offerenti di servizi o fornitori di

stesso motivo le ingerenze nei diritti fondamentali alla libera comunicazione necessitano di una *base legale sufficientemente precisa* [88].

5.24 Rispetto dei diritti fondamentali tutelati

Adottando misure di protezione, il legislatore deve prendere in considerazione le situazioni tutelate a livello costituzionale dei *destinatari* di tali misure e quelle di *terzi*. Le restrizioni a tali diritti fondamentali necessitano di una base legale sufficiente [89], devono poter essere giustificate da un interesse pubblico o dalla tutela di diritti fondamentali altrui, ed essere inoltre proporzionate allo scopo. I diritti fondamentali rimangono intangibili nella loro essenza (art. 36 cpv. 1-4 Cost.).

5.241 Destinatari

I *provider Internet*, in quanto destinatari principali delle misure protettive in questione, sono tutelati innanzitutto dal diritto fondamentale della *libertà d'opinione* (art. 16 cpv. 1 Cost.). Possono in particolare invocare anche il diritto fondamentale della libertà dei media (art. 17 Cost.), il cui nucleo intangibile comprende il *divieto della censura preventiva* (art. 17 cpv. 2, in relazione con l'art. 36 cpv. 4 Cost.). La libertà dei media, oltre alla libera trasmissione di informazioni attraverso la stampa, la radio o la televisione, tutela anche altre forme di diffusione di informazioni al pubblico basate sulla tecnica delle telecomunicazioni, e in particolare Internet [90].

I provider possono anche invocare la *libertà economica* (art. 27 Cost.). Questo diritto fondamentale non può essere invocato se i provider assicurano servizi di base [91] e svolgono pertanto un compito statale ai sensi dell'articolo 35 capoverso 2 Cost. [92].

5.242 Terzi

Occorre tutelare la *libertà d'informazione* (art. 16 cpv. 1 e 3 Cost.) degli *utenti* di Internet („user"). Tale libertà comprende in particolare il diritto di ricevere liberamente informazioni. Sono considerate „liberamente ricevibili" anche le trasmissioni

---

contenuti) a diffondere esclusivamente pubblicazioni legali, nella misura in cui non vi sia il rischio di pregiudicare sostanzialmente il dibattito su questioni di interesse sociale concernenti Internet" (trad.).

[88] Cfr. MÜLLER, GRUNDRECHTE (bibl.), pag. 210 seg.

[89] Il principio della legalità giova soprattutto al principio costituzionale della certezza del diritto (art. 5 Cost.). Cfr. in merito YVO HANGARTNER, art. 5 Cost, in: Ehrenzeller/Mastronardi/Schweizer/Vallender (ed.), Die schweizerische Bundesverfassung, Kommentar, Zurigo/Basilea/Ginevra 2002, n. 8; HÄFELIN/MÜLLER, (bibl.), n. 372.

[90] Cfr. in merito DENIS BARRELET, § 45 Les libertés de la communication, in: Thürer/Aubert/Müller (ed.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurigo 2001, pag. 721 segg. n. marg. 40 segg.; inoltre anche MÜLLER, GRUNDRECHTE (bibl.), pag. 275. – Per quel che riguarda la comunicazione non destinata al pubblico, il Tribunale federale concede anche ai provider di posta elettronica la possibilità di appellarsi al diritto fondamentale del segreto delle telecomunicazioni; DTF 126 I 50 segg., 57.

[91] Cfr. art. 92 cpv. 2 Cost, art. 1 cpv. 2 lett. a LTC nonché art. 14 segg. LTC.

[92] Cfr. in merito anche GIOVANNI BIAGGINI, § 49 Wirtschaftsfreiheit, in: Thürer/Aubert/Müller (ed.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurigo 2001, pag. 779 segg., n. marg. 11 con rimandi; ISABELLE HÄNER, Grundrechtsgeltung bei der Wahrnehmung staatlicher Aufgaben durch Private, in: AJP/PJA 2002, pag. 1144 segg., 1146, 1150.

radiofoniche diffuse via etere o via cavo [93], così come le informazioni diffuse via Internet [94].

5.25 Proporzionalità

5.251 In generale

Per definire in che misura il legislatore può restringere i diritti fondamentali sulla libera comunicazione nell'adempimento del suo mandato di tutela volto a lottare contro le discriminazioni e le violazioni dell'integrità, occorre in primo luogo considerare il principio della proporzionalità (art. 36 cpv. 3 Cost.; art. 5 cpv. 2 Cost.)[95]. Le misure sono proporzionate soltanto se sono *idonee* al raggiungimento dello scopo, *necessarie* e *ragionevolmente esigibili*.

5.252 Idoneità

Il principio della proporzionalità proibisce l'adozione di misure restrittive di diritti fondamentali che non contribuiscono in alcun modo al raggiungimento dello scopo perseguito, e si rivelano quindi inadatte. L'obiezione sollevata dagli access provider, secondo cui il blocco dell'accesso è facilmente aggirabile mediante semplici accorgimenti tecnici, oltre alla sua dimensione politica assume da questo punto di vista anche una giustificazione giuridica. Lo stesso può dirsi delle disposizioni che obbligano i provider a installare filtri informatici, dato che oggi praticamente ogni tipo di filtro può essere eluso in modo relativamente semplice [96].

5.253 Carattere necessario

Il principio della proporzionalità vieta inoltre l'adozione di misure che, sul piano personale, materiale, locale e temporale, esulano da ciò che è necessario per la realizzazione dello scopo perseguito dalla normativa (ossia la tutela del bene giuridico minacciato).

5.254 Esigibilità

Per essere proporzionate, le misure di protezione devono inoltre poter essere ragionevolmente imposte ai soggetti interessati. Il limite della „responsabilità" personale [97] per la cibercriminalità risiede nel carattere ragionevolmente esigibile delle misure imposte ai provider.

---

[93] Cfr. DTF 120 Ib 64 segg.; MÜLLER, GRUNDRECHTE (bibl.), pag. 292 seg.
[94] Cfr. in merito RAIMUND KROPP, Zensur im Internet, in: perspektive 21, Brandenburgische Hefte für Wissenschaft und Politik, Informationsgesellschaft, Heft 3/1998, pag. 28 segg., 29.
[95] Anche il legislatore federale è vincolato da tale principio, malgrado l'articolo 191 Cost.
[96] Cfr. in merito SEMKEN (bibl.), pag. 249 segg., 269.
[97] Nel presente contesto la nozione di responsabilità è intesa in senso lato e comprende le specificità dell'applicazione nel diritto penale, civile e amministrativo. Anche la direttiva sul commercio elettronico dell'Unione europea sembra basarsi su questa concezione: cfr. in particolare il titolo della sua sezione 4 (in merito vedasi inoltre il capitolo 4 del presente rapporto).

Nel *diritto penale* la responsabilità (all'infuori dei delitti intenzionali) può essere estesa soltanto fino al punto in cui le misure di protezione appaiono ragionevolmente esigibili. Se tali misure non vengono rispettate, la conseguente inadempienza va considerata come violazione di un obbligo di diligenza, e quindi come negligenza.

Il criterio della ragionevolezza assume importanza anche nell'ambito del *diritto privato*, quando si tratta di prevedere una responsabilità causale semplice o severa.

Nel *diritto amministrativo*, un "perturbatore indiretto" è ritenuto tale soltanto se l'ingerenza di polizia può ragionevolmente essergli imposta, ossia quando l'ingerenza appare proporzionata in relazione alla protezione del bene giuridico.

5.26 Uguaglianza giuridica e divieto dell'arbitrio

A prescindere dall'importanza dei diritti fondamentali di cui beneficiano i provider Internet, il legislatore resta costantemente vincolato dal principio dell'*uguaglianza giuridica* (art. 8 Cost.) e dal *divieto dell'arbitrio* (art. 9 Cost.).

Dal profilo del diritto costituzionale, concepire una rappresentazione in Internet in senso più ampio rispetto ad altri tipi di pubblicazione (ad esempio nell'ambito della stampa) può quindi rivelarsi problematico [98]. Il principio dell'uguaglianza di trattamento non impedisce al legislatore di prendere in considerazione, mediante l'adozione di disposizioni differenziate, le specifiche situazioni potenzialmente pericolose caratteristiche di ogni singolo medium. Una disparità di trattamento deve tuttavia essere giustificata da sufficienti motivi oggettivi.
È quindi possibile giustificare normative differenti per i diversi media; ognuno di essi ha infatti un diverso impatto sul pubblico [99] o ha un diverso pubblico di destinazione, e pertanto un diverso modo di diffusione [100].

L'introduzione di normative più severe rispetto agli Stati vicini può infine comportare svantaggi per i provider svizzeri, il che non appare esente da problemi dal profilo del diritto costituzionale.

[98] Cfr. MÜLLER, GRUNDRECHTE (bibl.), pag. 246 seg.
[99] Il divieto di rappresentare atti di cruda violenza previsto dall'articolo 135 CP, ad esempio, si riferisce unicamente a rappresentazioni sonore o visive, ma non a parole scritte.
[100] Il divieto della pornografia previsto dall'articolo 197 n. 1 CP è ad esempio più severo per quel che concerne le rappresentazioni diffuse via radio e televisione, rispetto a scritti o rappresentazioni sonore o visive che possono essere offerte a persone maggiori di 16 anni.

Il diritto penale vigente non offre risposte chiare o soddisfacenti alle importanti domande che si pongono in relazione al perseguimento e alla repressione di reati commessi in rete.

6. Criminalità in rete secondo il diritto penale vigente

6.1 In generale

6.11 Problematica

A differenza di altre attività criminali, nell'ambito della criminalità in rete la commissione di un reato dipende necessariamente dall'*infrastruttura tecnica* offerta da una pluralità di soggetti (spesso persone giuridiche) [101]. Un'altra caratteristica fondamentale dei servizi offerti [102] da hosting provider nonché da fornitori di rete o di accesso è lo *svolgimento* in larga parte *automatico* di questi processi.

In ragione del parallelismo [103] con il *diritto dei media*, occorre innanzitutto chiarire se gli articoli 27 e 322bis CP si applicano anche alle fattispecie relative alla criminalità in rete [104], o se queste vadano giudicate secondo le *regole generali del CP*, in particolare quelle relative alla complicità (art. 25 CP) [105].

A ciò si aggiunge il fatto che gli atti punibili, le prestazioni infrastrutturali fornite dagli altri soggetti e il richiamo di informazioni da parte degli utenti possono essere effettuati in luoghi geografici completamente diversi. La criminalità in rete assume quindi spesso un carattere *internazionale* e solleva la questione della sovranità penale della Svizzera. In caso di sovranità penale elvetica, ci si deve quindi chiedere a quale dei comportamenti indicati essa si estende [106].

Si aggiungono inoltre le questioni relative alle *competenze d'inchiesta* (distinzione tra giurisdizione federale e cantonale, art. 340 segg. CP) e al foro (competenza per ragione di territorio, art. 346 segg. CP).

---

[101] In merito ai soggetti e alle loro funzioni, vedi capitolo 2, n. 2.

[102] Ossia la messa a disposizione e la trasmissione di informazioni in rete.

[103] Il parallelismo concerne anche la pubblicazione (messa a disposizione), la diffusione e il consumo (utilizzo) di informazioni. Numerose persone sono inoltre coinvolte nel processo di pubblicazione e di diffusione.

[104] In merito vedi n. 6.2.

[105] In merito vedi n. 6.3.

[6] In merito vedi n. 6.4.

6.12 Nozione di criminalità in rete

La nozione di criminalità in rete comprende numerosi reati [107] che possono essere definiti e classificati in modo diverso. La *tabella* seguente elenca i principali e più frequenti *reati commessi in rete* (1ª colonna). Viene operata una distinzione a seconda del *tipo di reato*: è in tal modo possibile determinare se il luogo di commissione si trova in Svizzera (2ª colonna). La sovranità penale elvetica si fonda nella maggior parte dei casi su questo criterio, ed è il presupposto fondamentale per ogni perseguimento penale in Svizzera. Infine le fattispecie penali sono classificate a seconda che costituiscano o no un *reato mediatico*, categoria alla quale si applicano le disposizioni speciali degli articoli 27 e 322bis CP (3ª colonna). La suddivisione corrisponde all'attuale giurisprudenza del Tribunale federale, nella misura in cui ne esista una, e tenta di illustrare l'attuale situazione giuridica. Alcune di queste classificazioni non sono tuttavia state oggetto di esame in sede giudiziaria e suscitano controversie dottrinali.

La tipologia dei principali reati in rete e il loro rapporto con il diritto penale dei media [108]

FATTISPECIE PENALE	TIPO DI REATO	REATO MEDIATICO? [109]
Rappresentazione di atti di cruda violenza, art. 135 CP	Reato di messa in pericolo astratta	No
Acquisizione illecita di dati, art. 143 CP	Reato di evento [110] (controverso, opinione diversa: semplice delitto di comportamento)	No
Accesso indebito a un sistema per l'elaborazione di dati („hacking"), art. 143bis CP	Reato di evento [111] (controverso, opinione diversa: semplice reato di comportamento)	No
Danneggiamento di dati, art. 144bis n. 1 CP (cancellare, modificare o rendere i dati inservibili)	Reato di evento	No
Danneggiamento di dati, art. 144bis n. 2 CP (fattispecie riguardante i virus informatici)	Reato di messa in pericolo astratta (n. 2)	No (eccetto eventualmente nella variante in cui si forniscono indicazioni per l'allestimento di programmi contenenti virus)
Truffa, art. 146 CP	Reato di evento	No

[107] Cfr. capitolo 2, n. 2.2.

[108] Cfr. SCHWARZENEGGER, E-COMMERCE (bibl.), pag. 342 e 350.

[109] Cfr. DTF 125 IV 206 segg., che tuttavia si pronuncia in modo esplicito soltanto in relazione alle rappresentazioni di atti di cruda violenza (art. 135 CP), alla pornografia dura (art. 197 n. 3 CP) e alla negazione di genocidio (art. 261bis cpv. 4 CP). La classificazione delle altre fattispecie non è pertanto (ancora) stata chiarita dal TF. Per una classificazione secondo il punto di vista del Tribunale federale vedasi TRECHSEL/NOLL, (bibl.), pag. 229 e i rinvii menzionati; GUTACHTEN BJ (bibl.), pag. 834 seg.

[110] SCHWARZENEGGER, GELTUNGSBEREICH (bibl.), pag. 122, è dimostrabile un esito distinto dal punto di vista spaziale e temporale; di diverso avviso è NIKLAUS SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität, Zurigo 1994, CP 143 n. 17 e CP 143bis n 11; CASSANI, (bibl.), pag. 253.

[111] Vedi nota precedente.

Abuso di un impianto per l'elaborazione di dati, art. 147 CP	Reato di evento	No
Manipolazione dei corsi, art. 161bis CP	**Reato di messa in pericolo astratta**	Incerto; probabilmente si tratta di un reato mediatico (nella variante della diffusione di informazioni)
Diffamazione, art. 173 segg. CP	Reato di evento	Reato mediatico
Pornografia leggera, art. 197 n. 1 CP (protezione della gioventù)	Reato di messa in pericolo astratta	Incerto, probabilmente non si tratta di reato mediatico
Pornografia leggera, art. 197 n. 2 CP (protezione degli adulti dal confronto involontario con rappresentazioni pornografiche)	Reato di messa in pericolo concreta	No
Pornografia dura, art. 197 n. 3 CP	Reato di messa in pericolo astratta	No
Fabbricazione, occultamento e trasporto di materie esplosive o gas velenosi, art. 226 cpv. 3 CP (fornitura di istruzioni per la fabbricazione)	Reato di messa in pericolo astratta	Incerto; probabilmente non si tratta di un reato mediatico, poiché l'atto illecito non si consuma per effetto di una pubblicazione (è necessario fornire istruzioni a una persona determinata)
Pubblica intimidazione, art. 258 CP	Reato di evento	No
Pubblica istigazione a un crimine o alla violenza, art. 259 CP	Reato di messa in pericolo astratta	Reato mediatico
Discriminazione razziale, art. 261bis CP	Semplice reato di comportamento	Non si tratta di un reato mediatico (cpv. 4, negazione di genocidio), e probabilmente nemmeno nei casi dei cpv. 1-3
Spionaggio economico, art. 273 CP	Reato di messa in pericolo astratta	Incerto, probabilmente si tratta di un reato mediatico
Provocazione ed incitamento alla violazione degli obblighi militari, art. 276 CP	Reato di messa in pericolo astratta	Reato mediatico
Pubblicazione di deliberazioni ufficiali segrete, art. 293 CP	Reato di messa in pericolo astratta	Reato mediatico
Violazione del segreto d'ufficio, art. 320 CP	Semplice reato di comportamento	Reato mediatico
Violazione del segreto professionale, art. 321 CP	Semplice reato di comportamento	Reato mediatico
Violazione del diritto d'autore Allestimento di un esemplare di un'opera, art. 67 cpv. 1 lett. e LDA Offerta al pubblico, alienazione o messa in circolazione di un esemplare di un'opera, art. 67 cpv. 1 let. f LDA	Semplice reato di comportamento Semplice reato di comportamento	No No (eccetto eventualmente nella variante dell'offerta)
Lesione di diritti di protezione affini in particolare art. 69 cpv. 1 lett. c, lett. f URG	Semplice reato di comportamento	No
Metodi sleali di pubblicità e di vendita in particolare art. 3 in relazione con art. 23 LCSl	Reato di messa in pericolo astratta	Reato mediatico

6.2 Punibilità secondo il diritto penale dei media?

6.21 Le nuove disposizioni del diritto penale dei media

La caratteristica dei reati mediatici consiste nel fatto che l'atto punibile è commesso mediante *pubblicazione in un medium di comunicazione*, e che nello stesso tempo il reato deve *consumarsi* per effetto di tale pubblicazione. Secondo gli articoli 27 e 322bis CP, in caso di reati mediatici si applicano regole speciali [112] alla partecipazione al processo di pubblicazione.

In linea di principio è punibile soltanto l'autore della pubblicazione illegale (art. 27 cpv. 1 CP). Qualora l'autore non possa essere individuato o tradotto davanti a un tribunale svizzero (art. 27 cpv. 2 CP), l'articolo 322bis prevede una punibilità sussidiaria ed esclusiva del redattore responsabile o, in sua assenza, della persona responsabile della pubblicazione.

Questa disposizione penale, in vigore dal 1° aprile 1998, punisce la mancata opposizione *intenzionale* a una pubblicazione punibile con la detenzione o con la multa. Tuttavia, rispetto alle disposizioni penali in materia di stampa in vigore in precedenza, il regime della punibilità è stato inasprito, punendo ora anche la mancata opposizione *per negligenza*. Poiché l'articolo 27 CP non contempla una lista di reati mediatici, il catalogo delle fattispecie penali comprese da questa normativa speciale deve essere determinato mediante interpretazione (cfr. tabella precedente, 3^{a} colonna: in alcuni casi sussistono incertezze).

6.22 Nuova decisione del Tribunale federale concernente la nozione di reato mediatico

A complicare la situazione si è aggiunta una decisione del Tribunale federale emanata nel 1999, secondo la quale non tutti gli atti che possono essere pubblicati in un media e che si consumano attraverso tale pubblicazione costituiscono un reato mediatico [113]. Nella sua decisione, il Tribunale federale rileva esplicitamente che la rappresentazione di cruda violenza (art. 135 CP), la pornografia dura (art. 197 n. 3 CP) e la negazione di genocidio (in particolare per quel che concerne il caso di Auschwitz, art. 261bis cpv. 4 CP) non costituiscono reati mediatici.

Da un lato ciò è *giustificato* dal fatto che, per gli atti che non costituiscono reati mediatici, il legislatore intendeva precisamente *impedire* la pubblicazione dei contenuti incriminati, evitando di accordare una posizione privilegiata a un gruppo determinato di soggetti coinvolti nella commissione del reato. D'altro lato, dato che nel caso dei reati non mediatici viene comminata una pena per tutta una serie di altri atti, è possibile escludere che il legislatore abbia voluto privilegiare in questi casi la modalità mediatica della diffusione. Inoltre la Svizzera, in seguito alla ratifica della Convenzione internazionale contro la discriminazione razziale, è *obbligata sul piano*

---

[112] In merito all'origine e al senso della speciale regolamentazione in materia di diritto penale dei media, vedi RIKLIN, (bibl.), pag. 243 segg.; ZELLER (bibl.) n. 3 e 10 segg.

[113] DTF 125 IV 211 seg., così come SCHULTZ, PRESSEDELIKT (bibl.), pag. 278 e TRECHSEL/NOLL (bibl.), pag. 229. Cfr. GUTACHTEN BJ (bibl.), pag. 832 segg.

del diritto internazionale a perseguire senza eccezioni ogni diffusione di affermazioni a sfondo razzista [114].

Sostanzialmente si tratta di determinare se il fatto di *privilegiare* i responsabili dei media non equivalga a violare il *principio della parità di trattamento* (art. 8 cpv. 1 Cost.), e sia quindi in contrasto con la Costituzione. Si può obiettare che l'adozione di disposizioni penali in materia di stampa lasciava già trasparire la convinzione che il diritto penale comune non potesse tener conto adeguatamente dei bisogni derivanti da un regime di libertà dei media. L'unico modo per favorire la libertà di stampa era dunque quello di limitare la punibilità dei soggetti coinvolti nella sua produzione [115]. Il libero flusso di informazioni e il libero scambio di opinioni non sono soltanto un elemento indispensabile ai fini della *realizzazione personale*, ma rappresentano anche e soprattutto il fondamento di ogni Stato democratico. Poiché il legislatore svizzero, nel disciplinare il nuovo diritto penale dei media, ha mantenuto tali privilegi, proponendosi in particolare di *tutelare la libertà dei media* (cfr. art. 17 Cost.), si deve presupporre che *tutte le pubblicazioni* mediatiche debbano *essere giudicate in base agli articoli 27 e 322bis CP*, se i loro effetti si esplicano con la pubblicazione.

La classificazione dei reati mediatici in base ai criteri della DTF 125 IV 206 segg. è pertanto *discutibile* (vedi tabella precedente, 3^{a} colonna). Questa decisione ha anche suscitato numerose *critiche* [116]. Sulla base degli argomenti del Tribunale federale, ogni reato commesso mediante asserzioni o divulgazioni potrebbe essere escluso dal campo d'applicazione del diritto penale dei media, nonostante lo scopo delle singole disposizioni penali sia quello di impedire dichiarazioni inammissibili quale che sia la forma di diffusione, sia nel contesto mediatico che in quello non mediatico. Ciò riguarderebbe ad esempio anche i *delitti contro l'onore*, che comprendono svariate modalità di commissione (parole, scritti, immagini, gesti o altri mezzi, cfr. art. 176 CP).

6.23 Tre approcci interpretativi

6.231 I provider sono responsabili della pubblicazione — Applicabilità del diritto penale dei media

Secondo un primo approccio interpretativo dell'articolo 27 CP [117], il World Wide Web rappresenta un medium di comunicazione di massa: gli articoli 27 e 322bis CP si applicano quindi di principio alle pubblicazioni che avvengono mediante tale medium. È pertanto punibile unicamente il fornitore di contenuti (*content provider)*, se può essere individuato o tradotto dinanzi a un tribunale svizzero.

---

[114] TRECHSEL/NOLL (bibl.), pag. 230.

[115] Boll. Sten. CS 1931, pag. 68 e 76; in seguito ZELLER (bibl.), n. 10 segg.

[116] FRANZ RIKLIN, Kaskadenhaftung – quo vadis?, Medialex 2000, 208; RIKLIN/ STRATENWERTH, (bibl.), pag. 13 segg.; DORRIT SCHLEIMINGER/CHRISTOPH METTLER, Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung, art. 27, art. 261bis cpv. 4 CP, Osservazioni a DTF 125 IV 206 segg., AJP 2000, pag.1039 segg.; REHBERG/ DONATSCH (bibl.), pag. 166; SCHWARZENEGGER, E-COMMERCE (bibl.), pag. 349 segg.; RIKLIN (bibl.), pag. 245; ZELLER (bibl.), n. 32.

[117] Messaggio del Consiglio federale del 17 giugno 1996 concernente la modifica del Codice penale svizzero e del Codice penale militare (Diritto penale e procedura penale dei mass media), FF 1996 IV 449; GUTACHTEN BJ (bibl.), pag. 832 segg. e i rinvii menzionati.

Se il fornitore di contenuti non è reperibile, esiste una responsabilità sussidiaria dell'hosting provider, alle condizioni previste dall'articolo 27 capoverso 2 CP. L'hosting provider permette all'autore o al content provider di rappresentare i loro contenuti in Internet e, sulla base di questa interpretazione, diviene in tal modo responsabile della pubblicazione. La sua perseguibilità, nella misura in cui si configuri un reato mediatico, risulta dall'articolo 322bis CP.

Secondo questa interpretazione, inoltre, anche il fornitore di accesso (*access provider*) è considerato sussidiariamente responsabile ai sensi dell'articolo 27 capoverso 2 CP, qualora né il fornitore di contenuti, né l'hosting provider possano essere individuati o tradotti in giustizia. La perseguibilità del fornitore di accesso risulta pure dall'articolo 322bis CP [118].

6.232 I provider non sono responsabili della pubblicazione — Applicabilità delle regole generali

Un *secondo approccio interpretativo* si mostra critico nei confronti del punto di vista espresso in precedenza, poiché trascura la differenza tra la funzione mediatica del WWW, che si esaurisce nel processo di pubblicazione elettronica (preparazione di dati), e la sua funzione di mezzo di telecomunicazione, che comprende tutti gli aspetti tecnici della memorizzazione e della trasmissione di dati (messa a disposizione e trasmissione di dati) [119]. La prima interpretazione reggerebbe soltanto nel caso dei media che pubblicano parallelamente le loro informazioni su un loro server, off line e on line (preparazione = pubblicazione) [120].

Tuttavia, di norma l'hosting provider non partecipa attivamente al processo di pubblicazione del fornitore di contenuti, né sorveglia passivamente le relative trasmissioni di informazioni. Il fornitore di contenuti inserisce direttamente e automaticamente i dati, mediante un software di web publishing, nel server web dell'hosting provider. In altri termini, l'hosting provider gestisce *unicamente l'infrastruttura tecnica* che consente di mettere le informazioni a disposizione, e non è pertanto responsabile della pubblicazione [121], fatte salve le eccezioni menzionate. Quando assolve tale funzione l'hosting provider non rientra nel campo d'applicazione del diritto penale dei media, per cui da questo punto di vista occorre prendere in considerazione la possibilità di punire l'hosting provider in base alle regole generali sulla complicità (cfr. in merito n. 6.3) [122].

---

[118] GUTACHTEN BJ (bibl.), pag. 841 segg.

[119] Per chiarimenti in merito vedasi NIGGLI/SCHWARZENEGGER (bibl.), pag. 65 seg.

[120] Esempio: un quotidiano pubblica un articolo sia nell'edizione stampata del mattino, sia nella pagina web che esso gestisce autonomamente. Vi è pure un'implicazione diretta nel processo di pubblicazione quando un hosting provider accoglie informazioni su un supporto dati, per poi pubblicarle per il fornitore di contenuti sul suo server web.

[121] Cfr. REHBERG/DONATSCH (bibl.), pag. 167: „Si deve trattare di persone che esercitano un'attività specificatamente mediatica e a cui incombe la responsabilità del contenuto delle pubblicazioni all'interno del media in questione." (trad.)

[122] Questo parere si oppone all'idea di applicare il diritto penale dei media anche a chi diffonde tecnicamente i contenuti mediatici. Vedi RIKLIN/STRATENWERTH (bibl.), pag. 19 seg.; SCHWARZENEGGER, E-COMMERCE (bibl.), PAG. 351; NIGGLI/SCHWARZENEGGER (bibl.), pag. 62; RIKLIN (bibl.), pag. 251. Cfr. la pertinente normativa USA, Section 230(c) (2) Communications Decency Act: „No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

Nemmeno il *fornitore d'accesso* partecipa alla pubblicazione di contenuti illeciti su server altrui. La sua prestazione si limita alla messa a disposizione di un accesso a Internet. La trasmissione di dati ordinata dall'utente si svolge automaticamente e senza sorveglianza. Poiché si tratta in questo caso di una sorta di „complicità" in favore dell'utente, il quale cerca e si procura le informazioni in Internet, il fornitore di accesso non rientra in alcun modo nel campo d'applicazione degli articoli 27 capoverso 2 e 322bis CP [123].

6.233 I provider non sono responsabili della pubblicazione — Applicabilità del diritto penale dei media

Un *terzo approccio interpretativo* concorda con il parere precedente, nel senso che hosting e access provider non sono considerati "responsabili della pubblicazione" ai sensi dell'articolo 27 capoverso 2 CP. Tuttavia, poiché il gruppo di responsabili sussidiari ai sensi dell'articolo 27 capoverso 2 non coincide con il gruppo di persone esenti da pena, non è escluso che hosting provider e fornitore d'accesso rientrino nondimeno nel campo d'applicazione della regolamentazione speciale dell'articolo 27 CP. I divulgatori, che non figurano nel catalogo legale dei responsabili sussidiari, secondo questo approccio possono essere esclusi da ogni responsabilità penale, a prescindere dal loro contributo alla commissione dell'atto [124].

Il *Tribunale federale* si è pronunciato in questo senso nel contesto di una fattispecie relativa al diritto penale in materia di stampa (affissione di manifesti lesivi dell'onore, DTF 128 IV 53). In tale decisione è stata negata la responsabilità penale di persone che, nell'ambito della fabbricazione e diffusione di un prodotto mediatico penalmente rilevante, si sono occupate unicamente della pubblicazione. Secondo questa decisione, il semplice diffusore di dichiarazioni illecite può essere punito soltanto se non è attivo nell'ambito specifico dei media, ossia se la sua partecipazione all'atto avviene al di fuori del processo mediatico di produzione e divulgazione (DTF 128 IV 68).

Se questa interpretazione venisse applicata anche alla pubblicazione e alla diffusione in Internet, hosting e access provider farebbero parte dei divulgatori che andrebbero *esentati da ogni pena* [125]. Attraverso una limitazione del campo d'applicazione del diritto penale dei media occorre dunque impedire che questo sistema di privilegi possa produrre risultati iniqui [126] [127].

6.24 L'articolo 27 CP non si addice a Internet

In ragione delle diverse interpretazioni illustrate nella presente sezione, il campo d'applicazione del diritto penale dei media risulta *poco chiaro*, sia per quel che

---

[123] RIKLIN/STRATENWERTH (bibl.), pag. 21; REHBERG/DONATSCH (bibl.), pag. 169; SCHWARZENEGGER, E-COMMERCE (bibl.), PAG. 351 seg.; WEBER (bibl.), PAG. 547; NIGGLI/SCHWARZENEGGER (bibl.), pag. 62.

[124] ZELLER (bibl.), n. 32. Cfr. in merito RIKLIN (bibl.), pag. 250 seg.

[125] Cfr. ZELLER (bibl.), n. 35 segg. e 56 seg. (questione lasciata aperta).

[126] Si pensa in particolare ad ambiti sensibili quali la pornografia (art. 197 CP), la pubblica istigazione a un crimine o alla violenza (art. 259 CP) o la discriminazione razziale (art. 261bis CP).

[127] Questa via è già stata imboccata dal Tribunale federale nella sua decisione 125 IV 206 segg.

riguarda l'attribuzione di un reato al gruppo dei reati mediatici („atto punibile che si consuma per effetto della pubblicazione", cfr. tabella precedente: n. 6.12, 3ª colonna), sia in relazione alla sua applicabilità agli hosting e access provider.

Indipendentemente dai diversi approcci interpretativi, è palese che l'articolo 27 CP si presta alla cooperazione tra autori, redattori e altri soggetti responsabili della pubblicazione, mentre non si addice alle relazioni che intercorrono nel WWW, nei gruppi di discussione, nelle mailing list, ecc. Chi offre informazioni le pubblica in tali servizi web, nella maggior parte dei casi in modo autonomo e automatizzato, *senza l'intermediazione di una redazione*, di un'autorità di controllo, di un tipografia, ecc. La posizione dell'hosting o dell'access provider non può pertanto essere paragonata a quella dei soggetti attivi nei mezzi di comunicazione classici quali la stampa e la radio.

Una nuova normativa sulla punibilità dei diversi soggetti coinvolti deve quindi operare un'*esplicita distinzione tra le funzioni di media e di mezzo di telecomunicazione* del WWW e di altri servizi in rete (cfr. in merito capitolo 2).

6.3 Punibilità secondo le regole generali del CP?

Se ai reati non mediatici (vedi tabella precedente, n. 6.12, 3ª colonna) si applicassero le regole generali sull'imputazione della colpa e sulla partecipazione, per l'hosting e l'access provider si porrebbe una serie di ulteriori problemi di difficile soluzione[128]. L'unica cosa certa è che il responsabile (in quanto autore) di una pagina web inserita in rete è colui che l'ha creata e ne ha determinato il contenuto (content provider). Già nel caso dell'hosting provider, che mette a disposizione di un terzo (a pagamento) zona di memoria che quest'ultimo può utilizzare a discrezione, non è chiaro in che modo l'hosting provider partecipi alla perpetrazione di un reato che il terzo commette nel World Wide Web. Lo stesso vale per il fornitore d'accesso. Ciò è dovuto a *diversi motivi*.

Per stabilire se l'hosting provider è *autore o soltanto complice* del reato in questione, occorre rifarsi alla descrizione dell'atto materiale contenuta nella disposizione penale. L'*autore*, a differenza del *complice*, è colui che ha chiaramente compiuto (in prima persona) l'atto materiale. Ma nel caso che ci interessa la frontiera tra questi due ruoli è piuttosto confusa, poiché le fattispecie in questione proibiscono atti che vengono compiuti *prima che il bene giuridico sia effettivamente leso*. Secondo l'articolo 197 numero 1 CP, ad esempio, il solo fatto di rendere accessibili scritti pornografici a persone minori di 16 anni (così come nel caso della „pornografia dura", art. 197 n. 3 CP o della „rappresentazione di atti di cruda violenza", art. 135 CP) sarebbe sufficiente per considerare l'hosting provider come autore.

La particolarità dell'hosting provider è che nel momento in cui esso conclude con l'utente (content provider) il contratto relativo alla messa a disposizione di zona memoria, non vi è certezza quanto al tipo di informazioni che il fornitore di contenuti intende inserire e inserirà in rete. L'azione con la quale l'hosting provider mette a disposizione la zona memoria è un *atto in bianco*: si riferisce alle informazioni che il

[128] Ciò vale in generale per gli hosting e gli access provider, escludendo dal diritto penale dei media chi diffonde tecnicamente le informazioni (v. n. 6.2).

content provider fornirà, ma non a materiale di carattere pornografico, razzista o simile. Non permette l'accesso a immagini di carattere pornografico (art. 197 n. 1 CP), ma unicamente a pagine ancora vuote. Il loro carattere pornografico deriverà semmai dall'agire di chi inserirà i contenuti. Il comportamento dell'hosting provider non configurerebbe quindi la fattispecie oggettiva.

Gli stessi argomenti possono essere sollevati anche in relazione all'*aspetto soggettivo della fattispecie*: l'hosting provider non può sapere quali informazioni il content provider intende mettere e metterà in rete. Per esperienza, l'hosting provider sa benissimo che nel WWW si trovano anche informazioni illegali; ma da tale consapevolezza generale non si può ancora derivare l'intenzione di commettere reati, la cui perpetrazione e soprattutto la cui natura precisa sono del tutto incerte. Al momento dell'esecuzione dell'atto manca quindi il carattere intenzionale da parte dell'hosting provider [129]: per lo stesso motivo la sua azione non sarebbe quindi punibile.

L'hosting provider può apprendere dell'esistenza di contenuti illeciti sul proprio server soltanto nel periodo *che segue* la conclusione del contratto. Di norma l'esistenza di tali contenuti viene *segnalata da utenti del WWW*, che possono anche esortare l'hosting provider a bloccare l'accesso o a eliminare una pagina web a causa dell'asserita illegalità (ed eventualmente della rilevanza penale) delle informazioni in essa contenute. Se l'hosting provider prende in considerazione le segnalazioni, può venire a conoscenza dell'esistenza dei contenuti illeciti che configurano reati quali quelli previsti agli articoli 135 o 197 CP. In questo caso non è tuttavia chiaro se l'hosting provider sarebbe perseguibile in seguito a una sua azione o eventualmente in seguito a omissione.

La *prassi del Tribunale federale* non permette di trarre conclusioni attendibili; in particolare le constatazioni effettuate nella sentenza *„Telechiosco*" [130] non sono direttamente applicabili agli hosting provider [131]. In tale decisione il Tribunale federale aveva constatò che l'allora direttore generale della sezione telecomunicazioni delle PTT aveva ordinato l'introduzione del sistema „telechiosco 156" e dato le disposizioni che permisero di effettuare le installazioni necessarie. Il Tribunale federale considerò la messa a disposizione di tali installazioni come comportamento attivo [132] e il direttore generale fu condannato per complicità in pubblicazioni oscene e per pornografia (art. 204 CP previgente e art. 197 n. 1 CP).

La distinzione tra azione e omissione, fondamentale in diritto penale, non è chiara in casi in cui l'atto consiste nel "lasciare (accessibile)" o in particolare nel "rendere accessibile". La prassi del Tribunale federale considera come azione anche il fatto di lasciare che un precedente atto lecito continui a esplicare i suoi effetti, se tale atto costituisce la base di un successivo reato intenzionale commesso da terzi. Ciò è oltremodo discutibile [133]. Infatti, se l'hosting provider ignora una segnalazione relativa

---

[129] L'atto consiste nella conclusione del contratto di hosting, che di norma avviene automaticamente, mediante la compilazione di un formulario on line.

[130] DTF 121 IV 109 (il cosiddetto caso "telechiosco").

[131] Per maggiori dettagli vedasi RIKLIN/STRATENWERTH, (bibl.), PAG. 23 seg.

[132] DTF 121 IV 109, 120 cons. 3b.

[133] Inoltre: il caso Telechiosco concerneva *un* offerente di tale prestazione (poiché ve ne era uno solo), mentre per quel che concerne gli hosting provider il problema riguarda circa 100 ditte.

al contenuto penalmente rilevante di una pagina web, è difficile ravvisare una sua azione in relazione al contenuto della pagina in questione, anche se la segnalazione è fondata e se l'hosting provider ne è cosciente. A quel punto gli si può imputare unicamente l'omissione di intervento, che sarebbe punibile soltanto se l'hosting provider fosse sottoposto a un particolare obbligo giuridico d'intervenire (la cosiddetta qualità di garante) [134].

Secondo la giurisprudenza e la dottrina riconosciute, la *posizione di garante* può nascere anche da un precedente atto di messa in pericolo (la cosiddetta ingerenza). Colui che, attraverso il suo agire, crea un pericolo prevedibile per beni giuridici altrui, è tenuto a fare tutto il possibile affinché tale rischio non si realizzi. L'azione dell'hosting provider consiste nella messa a disposizione di zona memoria a chi ne è interessato. Questa rappresenta tuttavia un'azione del tutto comune e in sé *legale*, che non costituisce alcun pericolo particolare [135].

Il pericolo e l'azione punibile risultano soltanto dall'impiego abusivo della zona di memoria da parte di terzi (content provider), che commettono intenzionalmente un reato per mezzo delle informazioni messe in rete [136]. Possono essere trovate analogie con altre situazioni: nel caso di un albergatore che permette ai suoi ospiti di giocare a carte, ci si può ad esempio chiedere se egli sia tenuto a impedire agli avventori di praticare giochi d'azzardo, o nel caso del proprietario di una casa, si pone la questione relativa al suo dovere di vegliare affinché gli inquilini non commettano reati. La risposta del Tribunale federale è stata affermativa nel primo caso [137], e negativa nel secondo [138]. Anche su questo punto regna dunque l'*incertezza* [139].

Le considerazioni espresse per l'hosting provider sono applicabili per analogia anche al fornitore d'accesso (*access provider*). L'unica differenza è che la posizione del fornitore d'accesso è ancora più distante da quella dell'autore (principale) del reato. Il fornitore d'accesso non ha con l'autore nessun tipo di vincolo contrattuale, e quindi nemmeno automatizzato: egli è legato contrattualmente soltanto con l'utente finale.

---

[134] La dottrina parte dal presupposto che vi sia stata omissione, vedi FRANZ RIKLIN: Information Highway und Strafrecht, in: Reto M. Hilty (ed.): Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, Berna/Monaco 1996, 578; la questione è stata ampiamente discussa nel diritto tedesco, prima dell'entrata in vigore della legge sui servizi di telecomunicazione (Teledienstegesetz; TDG), vedi Ulrich SIEBER: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, 2ª parte, JZ 1996, 494 segg.

[135] Questo aspetto è stato oggetto di controverse discussioni, in riferimento alla „complicità ininfluente", cfr. GRACE SCHILD TRAPPE: Harmlose Gehilfenschaft, Berna 1995; WOLFGANG WOHLERS: Gehilfenschaft durch „neutrale" Handlungen, ZStrR 1999, 425 segg.; MARC FORSTER: Der Wirtschaftsalltag als strafrechtsdogmatischer „Hort des Verbrechens", Festschrift Niklaus Schmid, Zurigo 2001, 127 segg.

[136] E nello stesso tempo viola il contratto concluso con l'hosting provider, che proibisce l'offerta di informazioni penalmente rilevanti.

[137] DTF 81 IV 201.

[138] DTF 79 IV 147.

[139] Per un riassunto del dibattito in Germania, cfr. MARTIN POPP: Die strafrechtliche Verantwortung von Internet-Providern, Berlino 2002, 121 segg., che presuppone una posizione di garante derivante da un controllo fattivo esercitato su un oggetto pericoloso (posizione di garante in quanto sorvegliante), e ammette di principio una punibilità per omissione. Questa è tuttavia limitata dalla norma restrittiva di cui all'articolo 11 TDG.

6.4 Il problema della sovranità penale

La questione relativa a quale Stato abbia la sovranità penale in materia di criminalità in rete internazionale è una delle più controverse dell'intero ambito del diritto penale in materia di Internet [140]. Le condizioni di luogo (art. 3 e segg. CP) determinano, in modo autonomo e indipendentemente dai conflitti di giurisdizione con altri Stati, dove il diritto penale svizzero è applicabile e chi deve sottostare alla sovranità penale svizzera. Se quest'ultima è fondata, il tribunale è tenuto ad applicare il diritto penale svizzero [141].

Il *diritto internazionale pubblico*, che pure si spinge molto lontano nel riconoscimento di criteri di collegamento „opportuni" [142], pone in ogni caso dei limiti al potere di definizione degli Stati. La conseguenza è che nel diritto penale un medesimo reato può essere perseguito e sanzionato più volte. Tale rischio è particolarmente alto nella criminalità in rete, che in virtù della diffusione di contenuti punibili sul WWW raggiunge un raggio d'azione planetario.

La normativa svizzera sull'applicazione del diritto penale prevede numerose *regole di collegamento*. A parte il *principio della territorialità* [143], che rappresenta la norma, i reati internazionali possono anche sottostare al diritto penale svizzero in virtù del principio della bandiera [144], di quello della protezione dello Stato [145], di quello della personalità attiva [146] e passiva [147] nonché di quello del diritto universale [148] [149].

Il nesso di collegamento derivante dal principio della territorialità è concretizzato dal *principio* limitato *dell'ubiquità* [150]: il reato si reputa commesso in Svizzera se il luogo in cui l'autore ha agito o quello in cui si verifica l'evento si trovano in Svizzera. Di conseguenza, reati il cui luogo d'esecuzione si trova all'estero, ma che violano o mettono in pericolo beni giuridici siti in Svizzera, sono reputati commessi in Svizzera[151].

---

[140] Panoramica in SCHWARZENEGGER, GELTUNGSBEREICH (bibl.), pag. 109 segg.

[141] Eccezioni: gli art. 5 cpv. 1, 6 n. 1, 6bis n. 1 CP obbligano il giudice svizzero ad applicare il diritto penale estero, se più favorevole all'imputato.

[142] COUNCIL OF EUROPE, European Committee on Crime Problems: Extraterritorial criminal jurisdiction, Criminal Law Forum 1992, pag. 441 segg. In merito anche Cour Permanente de Justice Internationale [CPJI], Recueil des Arrêts, Sér. A, No. 10, 1927 (sentenza „Lotus").

[143] Reati commessi in Svizzera, art. 3 n. 1 cpv. 1 CP.

[144] Reati commessi a bordo di un aeromobile o di una nave sottoposti alla legge svizzera, art. 97 della legge federale del 21 dicembre 1948 sulla navigazione aerea (LNA, RS 748.0), art. 4 cpv. 2-3 della legge federale del 23 settembre 1953 sulla navigazione marittima sotto bandiera svizzera (RS 747.30).

[145] Reati commessi contro lo Stato svizzero, art. 4 cpv. 1 CP, con elenco di reati.

[146] Reati commessi da cittadini svizzeri, art. 6 n. 1 CP.

[147] Reati commessi contro beni giuridici di un cittadino svizzero protetti dal diritto penale, art. 5 cpv. 1 CP.

[148] Ogni reato commesso contro un bene giuridico universale, cfr. art. 6bis CP, art. 19 n. 4 della legge federale del 3 ottobre 1951 sugli stupefacenti (LStup, RS 812.121).

[149] Gli articoli 3-7 CP valgono conformemente a quanto disposto dall'articolo 333 capoverso 1 CP (riserva di disposizioni divergenti) anche per il diritto penale accessorio.

[150] Art. 7 CP.

[151] In realtà non sono i beni giuridici a essere messi in pericolo o violati, ma gli oggetti nei quali tali beni giuridici sono concretamente incorporati.

6.41 Luogo d'esecuzione dei reati commessi in rete

Per la definizione del luogo d'esecuzione è sempre determinante *il luogo fisico in cui si trova l'autore* al momento della commissione dell'atto. Se la legge penale proibisce ad esempio di propagandare, offrire, mostrare, diffondere o rendere accessibili determinate informazioni [152] o esortarne la consultazione, il luogo d'esecuzione si trova dove l'autore dà l'ordine di trasmissione o di telecaricamento con il quale, mediante l'esecuzione automatica di programmi, viene avviata l'elaborazione dei dati.

Se il reato deve essere *pubblico*, ci si deve basare sul luogo in cui l'autore si trova al momento in cui immette l'ordine con il quale i dati, tramite l'esecuzione automatica di programmi, vengono trasferiti nell'ambito pubblico del disco rigido di un computer (server web, server Usenet) [153]. Il trasporto dei dati e la loro memorizzazione nel server non sono più effettuati dall'utente, ma avvengono automaticamente. Pertanto, *il luogo in cui si trova il server non è il luogo d'esecuzione* [154].

Una particolarità dei reati commessi in rete consiste nel fatto che il luogo d'esecuzione, che tradizionalmente rappresenta il normale nesso di collegamento, resta spesso sconosciuto alle autorità di perseguimento penale e talvolta non può essere affatto accertato.

6.42 Luogo in cui si produce il risultato dei reati commessi in rete

Poiché i reati commessi in rete vengono spesso compiuti all'estero ma esplicano i loro effetti in Svizzera, si pone la questione fondamentale relativa al significato di "evento" ai sensi dell'articolo 7 CP [155]. Non è chiaro se in relazione a ogni fattispecie

---

[152] Cfr. art. 135 CP (rappresentazione di atti di cruda violenza), art. 173 n. 1 e art. 174 n. 1 CP (delitti contro l'onore), art. 179 cpv. 2 CP (violazione di segreti privati), art. 197 n. 1-3 CP (pornografia), art. 259 CP (pubblica istigazione a un crimine o alla violenza), art. 261bis (discriminazione razziale) ecc.

[153] In merito alla nozione di pubblico, nel CP in generale e in particolare nell'art. 261bis CP (discriminazione razziale), vedasi NIGGLI, RASSENDISKRIMINIERUNG, (bibl.), n. 691 segg.; GERHARD FIOLKA/ MARCEL ALEXANDER NIGGLI, Der Begriff der Öffentlichkeit im Strafrecht am Beispiel der Bundesgerichtsentscheide vom 21. Juni 2000 und vom 23. August 2000 betreffend Rassendiskriminierung, AJP 2001, 533 segg. e i rinvii menzionati.

[154] Cfr. decisione non pubblicata della Camera d'accusa del Tribunale federale dell'11 agosto 1999 (8G.43/1999), pag. 5. Sulla base della teoria della "lunga mano", anche il luogo in cui si trova il server destinatario viene in parte considerato come luogo d'esecuzione dell'atto, vedi POPP (bibl.), n. 6 e i rinvii menzionati. In contrasto con questa tesi vi è l'intenzione del legislatore svizzero, che nell'articolo 7 CP ha volutamente limitato il principio dell'ubiquità al luogo in cui l'autore ha agito e a quello in cui l'esito si è prodotto, al fine di escludere le dinamiche informatiche messe in moto o sfruttate dall'autore (la "lunga mano"), vedi EMIL ZÜRCHER, Erläuterungen zum Vorentwurf vom April 1908, Berna 1914, pag. 25 seg. Secondo questa interpretazione, in determinate circostanze potrebbero esserci nessi di collegamento assolutamente casuali nel luogo in cui si trova il server di destinazione, che può trovarsi in un Paese che altrimenti non avrebbe nulla a che vedere con il reato, cfr. SCHWARZENEGGER, E-COMMERCE (bibl.), pag. 339 seg.

[155] Finora il Tribunale federale non ha ancora avuto l'opportunità di prendere posizione in merito alla questione del punto di collegamento legato all'evento nell'ambito della criminalità in rete internazionale; per quel che riguarda la Germania, vedasi tuttavia BGHSt 46, 212 (Volksverhetzung). Per l'opinione attuale della dottrina, cfr. SCHWARZENEGGER, GELTUNGSBEREICH (bibl.), pag. 120 seg.; SCHWARZENEGGER., ABSTRAKTE GEFAHR (bibl.), pag. 240 segg.; NIGGLI, NATIONALES STRAFRECHT

penale debba prodursi un risultato (che fa parte della fattispecie legale) o se ciò non sia il caso per alcuni tipi di reati, come quelli di messa in pericolo astratta o i semplici reati di comportamento. È possibile distinguere *due approcci interpretativi*.

6.421 Nozione tecnica di evento

Secondo la *dottrina dominante* [156] *e la giurisprudenza* [157], l'interpretazione della nozione di evento ai sensi dell'articolo 7 CP tende a operare una distinzione tra i diversi tipi di reato, quindi tra semplici reati di comportamento e i reati d'evento da un lato, e i reati di messa in pericolo concreta e astratta dall'altro. Questa suddivisione si basa sulle diverse condizioni che, secondo la dottrina generale, devono essere soddisfatte perché le rispettive fattispecie siano realizzate. Poiché, secondo questa interpretazione, l'„evento" ai sensi dell'articolo 7 CP rappresenta un esito esterno circoscritto, separabile dal punto di vista temporale e spaziale dal luogo di commissione dell'atto, in caso di semplici reati d'attività e di messa in pericolo astratta l'evento non può costituire un nesso di collegamento (cfr. tabella precedente, n. 6.12, 2ª colonna).

Con l'esecuzione dell'atto tali reati sono già compiuti, di modo che il luogo in cui si produce l'evento non è distinguibile dal luogo in cui l'atto viene commesso. La conseguenza è che se un reato commesso per mezzo di Internet fa parte dei semplici reati di comportamento o di messa in pericolo astratta, può essere perseguito in Svizzera soltanto se è stato compiuto nel nostro Paese. Se invece l'autore ha agito all'estero, in base al principio della territorialità viene a mancare la sovranità penale svizzera [158].

Questa interpretazione, *da una parte*, presenta dei vantaggi: impedisce una competenza generale della Svizzera in materia di reati d'opinione, che possono produrre il loro effetto ovunque, e quindi un sovraccarico di lavoro delle autorità svizzere di perseguimento penale, che si vedrebbero confrontate con procedimenti insensati contro autori residenti all'estero. *D'altra parte*, la restrizione derivante dal criterio del luogo in cui si produce l'evento (art. 7 CP) rappresenta nello stesso tempo l'inconveniente di questa interpretazione: in tal modo si *permette infatti di eludere il diritto penale svizzero*.

Esempio: un gruppo di skinheads svizzeri decide di utilizzare il web per la propaganda delle sue attività estremiste di destra. Se gli skinheads caricano su un

---

(bibl.), pag. 144 segg.; WEBER (bibl.), pag. 536 segg. Per la situazione giuridica in Germania, cfr.: LEHLE (bibl.); HILGENDORF (bibl.), pag. 650 segg.; KOCH (bibl.), pag. 703 segg. tutti con ulteriori rinvii.

[156] Per un riassunto cfr. TRECHSEL (bibl.), art. 7 n. 6; REHBERG/DONATSCH (bibl.), pag. 42 tutti con ulteriori rinvii.

[157] In seguito alle ripetute critiche espresse da HANS SCHULTZ, nella sua DTF 105 IV 326 il Tribunale federale ha modificato la propria giurisprudenza; per un riassunto cfr. DTF 125 IV 180 segg. Nella DTF 128 IV 145, 153 il TF si distanzia nuovamente da questa interpretazione: „Le Tribunal fédéral a longtemps considéré … que la notion de résultat selon l'art. 7 CP s'interprétait de la même manière que pour la définition du délit matériel (…). Il s'est récemmment distancié de cette solution et est revenu à une interprétation plus large de la notion de résultat."

[158] CASSANI (bibl.), pag. 246; NIGGLI, RASSENDISKRIMINIERUNG (bibl.), n. 63 seg.; WIDMER/BÄHLER (bibl.), pag. 310 seg.; per quanto attiene alla Germania: HILGENDORF (bibl.), pag. 650 segg.; KOCH (bibl.), pag. 703 segg. con ulteriori rinvii.

server web in Svizzera i loro testi nei quali negano l'olocausto, saranno sottoposti alla sovranità penale svizzera. Se invece, per i loro scopi, si recano in Olanda o in Svezia e da lì caricano contenuti in rete, in mancanza di sovranità penale la Svizzera non potrà perseguirli [159]. Poiché di norma il legislatore concepisce le fattispecie a prescindere dalle possibili conseguenze a livello di applicazione del diritto penale, i nessi di collegamento talvolta non sono chiari. Nel caso dell'articolo 197 numero 2 CP, ad esempio, un nesso di collegamento sembra possibile (protezione degli adulti dal confronto con pornografia leggera: reato di messa in pericolo concreta), mentre non lo sembra nel caso dell'articolo 197 numero 3 CP (pornografia dura: reato di messa in pericolo astratta).

6.422 Evento in quanto violazione o messa in pericolo dell'oggetto dell'aggressione

Il *secondo approccio interpretativo* [160] parte invece dal presupposto che la struttura di ogni fattispecie della Parte speciale del Codice penale deve fondarsi su una violazione o una messa in pericolo di un oggetto. Per quel che riguarda i *reati di messa in pericolo astratta*, l'evento è rappresentato dalla creazione di un pericolo imminente per un oggetto non ancora definito (ad esempio in Svizzera qualsiasi minorenne potrebbe essere confrontato con pornografia leggera caricata su un server web all'estero; art. 197 n. 1 CP), ed è possibile determinare il luogo in cui questo pericolo astratto si manifesta. Occorre altresì tener presente che, per questo tipo di reati, il luogo in cui l'atto è compiuto e il luogo in cui si produce l'evento (così come definito nel presente approccio interpretativo) non sempre coincidono. Per quel che riguarda i reati commessi in rete, la conseguenza è che occorre ammettere il nesso di collegamento del luogo in cui si produce l'evento, secondo l'articolo 7 CP, nel caso in cui la concretizzazione del pericolo imminente risulta dalla possibilità di richiamare dalla Svizzera le pagine web dal contenuto criminoso.

Il vantaggio di questo approccio interpretativo risiede nel fatto che pone in primo piano la preoccupazione di salvaguardare i *beni giuridici*, senza concentrarsi unicamente sulla strutturazione della relativa fattispecie. Da questo approccio interpretativo risulta inoltre un nesso di collegamento per gli atti di partecipazione, che sulla base della prassi del Tribunale federale vanno giudicati secondo il diritto

---

[159] Il disconoscimento di genocidio (la cosiddetta "Auschwitzlüge", art. 261bis cpv. 4 CP, semplice reato di comportamento) non è punibile ad esempio negli Stati Uniti, in Canada, in Danimarca, nei Paesi Bassi, in Svezia e in Gran Bretagna, cfr. KOCH (bibl.), pag. 704 e rinvii menzionati. Un nesso di collegamento non può sussistere nemmeno sulla base del principio della personalità attiva (art. 6 n. 1 CP), poiché non è realizzata la condizione della doppia punibilità. Considerazioni analoghe possono essere decisive nella scelta dell'ubicazione da parte di hosting e access provider attivi a livello internazionale, s. HEINE (bibl.), pag. 106.

[160] FRANZ RIKLIN, Information Highway und Strafrecht, in: R. M. Hilty (ed.), Information Highway, Berna/Monaco 1996, 581 seg.; SCHWARZENEGGER, GELTUNGSBEREICH (bibl.), pag. 123 segg.; SCHWARZENEGGER, ABSTRAKTE GEFAHR (bibl.), pag. 249 segg.; LAURENT MOREILLON, Nouveaux délits informatiques sur Internet, Medialex 2001, 25 seg.; WEBER (bibl.), pag. 538 (Einschränkung: eine erhebliche Betroffenheit des Verletzten); vedi anche HEINE (bibl.), pag. 109 („evidente per i reati previsti dalla LCSI", questione lasciata in generale aperta). Implicitamente anche: Arrêt du Tribunal correctionnel du District de Lausanne, 7 juillet 1997, Medialex 1997, 235 (pornografia dura); per quanto attiene alla Germania: BGHSt 46, 212; DIRK-M. BARTON, Mulitmedia-Strafrecht, Neuwied/Kriftel 1999, 146 segg.; BERND HEINRICH, Der Erfolgsort beim abstrakten Gefährdungsdelikt, GA 1999, 79 segg.; LEHLE (bibl.), pag. 57 segg. con ulteriori rinvii.

applicabile all'atto principale (cfr. n. 6.43). Lo svantaggio è rappresentato dall'aumento delle competenze giurisdizionali e dall'eventuale conflitto con altre sovranità penali.
Al fine di scongiurare la doppia punibilità e per evitare di sovraccaricare le autorità di perseguimento penale confrontandole con procedimenti inutili, occorre adottare in quest'ambito ulteriori *misure di limitazione*. Si tratta della collaborazione internazionale, ottenuta attraverso richieste ad altri Stati volte all'assunzione del perseguimento penale (art. 88 AIMP; RS 351.1), di domande di estradizione, della riduzione del numero dei casi mediante l'applicazione del *principio di opportunità* ai reati compiuti all'estero ma esplicanti il loro effetto in Svizzera, nonché della presa in considerazione unicamente dei casi per i quali in Svizzera è soddisfatto il criterio di diritto internazionale del nesso di collegamento „adeguato" [161].

6.43 Il nesso di collegamento per la partecipazione a un reato

Per gli atti di partecipazione compiuti in Svizzera (istigazione, art. 24 CP; complicità, art. 25 CP) a un reato in rete i cui effetti si sono completamente realizzati all'estero, in base alla giurisprudenza del Tribunale federale il luogo in cui il partecipante ha agito non rappresenta un nesso di collegamento ai sensi dell'articolo 7 CP, in ragione del carattere accessorio della sua azione rispetto al reato principale [162]. Numerose fattispecie relative a Internet sfuggono pertanto alla sovranità penale svizzera. Se le regole sul campo d'applicazione territoriale sono intese quali condizione materiale di punibilità, viene a cadere anche la responsabilità penale [163]. Non si rivela quindi possibile un perseguimento penale nei confronti di un hosting o access provider svizzeri per atti di complicità [164]. Lo stesso vale per il perseguimento penale contro chi ha creato un link che rimanda a una pagina web all'estero.

Nella sua prassi, il Tribunale federale si fonda sulla teoria della partecipazione illecita, secondo la quale la punibilità del partecipante dipende di regola da quella dell'autore principale. La valutazione si basa sul diritto estero ed è affidata unicamente al giudice del luogo di commissione del reato. Questo parere viene tuttavia parzialmente messo in discussione, poiché le regole sull'applicabilità del diritto penale non sono focalizzate sul carattere accessorio della punibilità, ma bensì sul problema della localizzazione di un reato [165]. Indipendentemente dal caso

---

[161] L'art. 4 cpv. 1 n. 4 del Codice di procedura penale del Cantone di Berna offre un esempio di soluzione flessibile. Un altro esempio è riscontrabile nell'art. 8 cpv. 2 lett. d dell'avamprogetto di Codice di procedura penale svizzero, Berna 2001: se gli interessi essenziali della parte in giudizio non vi si oppongono, il Procuratore pubblico e i tribunali prescindono dal perseguimento penale se "il reato è già perseguito da un'autorità estera, o il perseguimento è stato delegato a quest'ultima." Cfr. le spiegazioni in merito nel rapporto esplicativo relativo all'avamprogetto di Codice di procedura penale svizzero, Berna 2001, pag. 36.

[162] DTF 81 IV 37; 104 IV 86; 108 Ib 303; J.-L. COLOMBINI, La prise en considération du droit étranger (pénal et extra-pénal) dans le jugement pénal, Tesi, Losanna 1983, pag.35; POPP (bibl.), n. 14.

[163] POPP (bibl.), prima dell'art. 3 n. 4; per la condizione processuale, cfr. SCHWARZENEGGER, GELTUNGSBEREICH (bibl.), pag. 127.

[164] A meno che l'atto principale non sia sottoposto alla sovranità penale svizzera, in virtù degli articoli 3 (evento), 4, 5, 6 o 6bis CP. In tal caso la sovranità penale è data anche per la partecipazione.

[165] SCHWARZENEGGER, E-COMMERCE (bibl.), pag. 346; cfr. HANS SCHULTZ, Gesetzgebung und Rechtsprechung der Schweiz im internationalen Strafrecht 1970 bis 1972, SJIR vol. XXIX, pag. 416 seg.; TRECHSEL (bibl.), art. 7 n. 8; POPP (bibl.), art. 7 n. 14 e rinvii menzionati. Taluni Cantoni hanno

speciale del tentativo di istigazione a un crimine (art. 24 cpv. 2 CP), l'istigazione e la complicità sono punibili unicamente nella misura in cui hanno avuto successo, ossia se il reato principale è stato almeno tentato.

Analogamente, nel caso della complicità, occorre operare una distinzione tra, ad esempio, un atto d'esecuzione (un qualsiasi contributo al reato principale), e l'evento prodotto (esecuzione del reato principale o tentativo). Se l'autore compie l'atto di complicità in Svizzera, la sovranità penale elvetica sarebbe fondata come nel caso di una truffa in cui soltanto l'astuto inganno è compiuto in Svizzera [166]. Per evitare risultati sconcertanti, in simili casi (quale misura limitativa) si propone di esigere un'ulteriore condizione, ossia la punibilità del reato principale nel luogo in cui è stato commesso [167].

6.44 Esempi (cfr. allegato*)*

Come rilevato nelle sezioni precedenti, per molti aspetti *non è ancora chiaro* se un reato commesso in rete può essere giudicato da un tribunale svizzero. Sulla base di tre esempi, nell'*allegato* si intende illustrare la complessità dell'interazione tra norme sull'applicazione del diritto penale e il diritto penale materiale, nonché delle regole particolari del diritto penale dei media. Molte delle domande che si pongono non trovano risposte chiare.

Il *primo caso* riguarda la messa a disposizione di immagini pedopornografiche su una pagina web (art. 197 n. 3 CP), il *secondo* l'istigazione a un attentato incendiario compiuta in un gruppo di discussione (art. 259 cpv. 1 CP), mentre il *terzo* concerne un sito web contenente testi il cui scopo è di screditare sistematicamente un'etnia determinata (art. 261bis cpv. 2 CP). WWW e gruppi di discussione svolgono il ruolo intercambiabile di servizi Internet rivolti al pubblico.

Nell'allegato i tre casi vengono rappresentati in modo particolareggiato nelle diverse combinazioni di circostanze.

6.5 Giurisdizione federale o cantonale?

Le difficoltà legate alla determinazione della sovranità penale (cfr. n. 6.4) generano un problema di perseguimento. In linea di massima, in materia di criminalità in rete, all'inizio delle indagini non è noto il luogo in cui un reato è stato commesso. La conseguenza è che nella maggior parte dei casi i procedimenti penali concernenti reati commessi via Internet vengono aperti da autorità non competenti, e soltanto nel corso delle indagini possono essere affidati alle autorità competenti [168].

---

una prassi diversa da quella del Tribunale federale, vedi HANS SCHULTZ, Gesetzgebung und Rechtsprechung der Schweiz im internationalen Strafrecht 1942 bis 1963, SJIR vol. XX, pag.192 seg.

[166] Ci si riferisce quindi a casi di truffa in cui l'errore o il pregiudizio patrimoniale avvengono unicamente all'estero, vedasi in merito CHRISTIAN SCHWARZENEGGER: Handlungs- und Erfolgsort beim grenzüberschreitenden Betrug, Festschrift Niklaus Schmid, Zurigo 2001, pag. 158 seg. e rinvii menzionati.

[167] Principio della norma identica, TRECHSEL (bibl.), art. 7 n. 8 e rinvii menzionati.

[168] NIGGLI, NATIONALES STRAFRECHT (bibl.), pag. 169 seg.

L'unica alternativa sarebbe costituita da un nesso di collegamento basato sul luogo in cui si produce l'evento. Tuttavia, se l'evento è inteso ai sensi della fattispecie, come previsto dalla dottrina dominante e dalla giurisprudenza [169], i reati che non producono un evento distinto (quindi la maggior parte delle divulgazioni illecite; vedi tabella al n. 6.12, 2ª colonna) possono essere geograficamente collegati unicamente al luogo in cui sono stati commessi.

Optando per una definizione di „evento" in senso più ampio, sarebbe possibile fondare una competenza svizzera per il perseguimento penale sulla base dell'articolo 7 CP, poiché da questo punto di vista l'evento diventa fondamentalmente *ubiquo*, ossia si produce ovunque l'informazione in questione è percepibile. Ciò che forse è auspicabile a livello internazionale, in termini di relazioni interne comporta una vera e propria proliferazione di competenze: è infatti competente ogni autorità di perseguimento penale che crede di esserlo o che, in seguito a una denuncia, lo diventa [170].

Secondo l'articolo 346 capoverso 1 CP, per il perseguimento di un reato sono competenti le autorità del luogo in cui esso è stato compiuto. Se in Svizzera si trova soltanto il luogo in cui si è verificato l'evento, sono competenti le autorità di questo luogo. Nel caso della criminalità in rete, la seconda ipotesi dovrebbe rappresentare, almeno a titolo provvisorio, la norma. Si pone quindi *in primo luogo* la questione relativa al modo di procedere in caso di reati che non producono un evento nel senso espresso dalla fattispecie. *In secondo luogo* ne consegue che, anche applicando una definizione in senso lato dell'evento di cui all'articolo 7 CP, la Svizzera è competente, ma all'interno del suo territorio il perseguimento dipende da circostanze casuali. Secondo l'articolo 346 capoverso 2 CP, qualora l'evento si verifichi in più luoghi (e quindi, interpretando la nozione di evento in senso lato, di principio sempre), sono competenti le autorità del luogo nel quale è stata aperta la prima istruzione. Ciò significa che, almeno nei casi di reati contro l'onore, rappresentazioni di cruda violenza, pornografia, discriminazione razziale, ma anche di fornitura di indicazioni per l'allestimento di virus informatici (art. 144bis n. 2 CP), di principio è competente ogni autorità di perseguimento penale svizzera, purché sia pervenuta una prima denuncia in Svizzera [171].

Il fatto che ogni autorità di perseguimento penale svizzera sia competente per ogni reato commesso via Internet origina una *sovrapposizione di competenze*. In singoli casi un *coordinamento* si rivela *necessario*, come è stato dimostrato nel recente affare "Landslide" [172].
Di conseguenza la situazione può essere risolta soltanto prevedendo una relativa *competenza della Confederazione*. Proprio ciò che prevede l'iniziativa parlamentare Aeppli Wartmann, presentata il 26 settembre 2002 (Iv. Pa. 02.452, cfr. n. 1.22). Si

[169] Per un'opinione diversa e più recente: DTF 128 IV 145, 153.
[170] NIGGLI, INTERNET-KRIMINALITÄT, (bibl.), pag. 6 seg.
[171] NIGGLI, INTERNET-KRIMINALITÄT (bibl.), pag. 6 seg.
[172] Landslide, un sito web commerciale basato negli Stati Uniti, permetteva agli utenti di consultare e scaricare immagini pedopornografiche, previo pagamento effettuato con carta di credito. Dopo l'arresto dei gestori del sito, l'FBI ha mantenuto in funzione il portale e ha trasmesso via INTERPOL all'Ufficio federale di giustizia i dati concernenti le carte di credito dei clienti svizzeri. Nell'autunno 2002 è stata lanciata un'azione coordinata delle autorità cantonali di perseguimento penale ("Genesis"), nonostante il fatto che in alcuni Cantoni fossero già trapelate informazioni, mentre altri Cantoni non avevano ancora terminato le perquisizioni e i sequestri di computer presso le persone sospette che si trovavano nel loro settore di competenza.

propone una competenza federale ai sensi dell’articolo 340bis CP (criminalità organizzata ed economica), ossia una competenza della Confederazione in tutti i casi in cui un reato è stato commesso principalmente all’estero o in più di un Cantone. Si tratta quindi del caso normale relativo alla criminalità su Internet, almeno per quanto concerne i reati d’opinione.

La necessità di introdurre adeguati strumenti di diritto amministrativo non richiede una revisione del vigente diritto in materia di telecomunicazioni, né una nuova legge. Simili provvedimenti possono piuttosto essere integrati nella proposta revisione del Codice penale. Si può quindi rinunciare all'adozione di speciali misure fiancheggiatrici di carattere amministrativo.

7. Possibilità di adottare misure di diritto amministrativo

7.1. Situazione di partenza

7.11 Necessità di misure di diritto amministrativo

Al fine di lottare contro le violazioni dei beni giuridici nelle reti di comunicazione, la Commissione peritale si è chiesta se, oltre ai provvedimenti di diritto penale, non vi fosse eventualmente il bisogno di prevedere anche disposizioni e misure *di diritto amministrativo*. Tali misure, in determinate circostanze, potrebbero aiutare a prevenire la violazione di beni giuridici e rivelarsi efficaci laddove il diritto penale (svizzero) non possa essere applicato.

Tale necessità di una normativa di carattere amministrativo deve però avere come riferimento le garanzie derivanti dai diritti fondamentali della libera comunicazione[173]. Le possibili misure di diritto amministrativo devono inoltre limitarsi in ogni caso a una funzione *fiancheggiatrice* e *integrativa* in favore del diritto penale.

7.12 Competenza della Confederazione

Le telecomunicazioni (in particolare le reti di telecomunicazione) e i media elettronici sono compresi nel campo d'applicazione degli articoli 92 (poste e telecomunicazioni) e 93 (radiotelevisione) della Costituzione federale. Sulla base di queste due disposizioni, spetta alla Confederazione disciplinare *tutte* le questioni inerenti ai due ambiti. Tali competenze federali sono inoltre di natura *esclusiva*: escludono quindi regolamentazioni cantonali, a prescindere da eventuali lacune dell'ordinamento federale [174].

---

[173] Cfr. capitolo 5.

[174] Cfr. ROLF H. WEBER, § 60 Energie und Kommunikation, in: Thürer/Aubert/Müller (ed.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurigo 2001, pag. 943 segg., n. marg. 27; vedasi inoltre ANDREAS KLEY, Bundeskompetenzen mit ursprünglich derogatorischer Wirkung aus historischer Perspektive, in: recht 1999, pag. 189 segg., 200.

7.13 Diritto vigente

7.131 Diritto in materia di telecomunicazioni

Il diritto in materia di telecomunicazioni, in quanto normativa concernente l'infrastruttura, disciplina in primo luogo la trasmissione di informazioni mediante telecomunicazione (cfr. art. 2 in relazione con art. 3 lett. b, c LTC). In questo contesto Internet è intesa innanzitutto come piattaforma per la comunicazione individuale (e-mail, voice over IP, trasmissione di dati) o come mezzo di telecomunicazione per la diffusione di informazioni che non costituiscono trasmissioni radiofoniche o televisive.

Soltanto alcune disposizioni si riferiscono al *contenuto* delle informazioni trasmesse[175]. Tali norme non possono tuttavia fungere da base per il tipo di misure di diritto amministrativo in questione nel presente capitolo.

7.132 Diritto in materia di radiotelevisione

La LRTV riguarda le trasmissioni radiotelevisive di genere tradizionale, e non si adatta a disposizioni di diritto amministrativo. Anche la nuova legge sulla radiotelevisione disciplinerà unicamente l'emittenza, la diffusione e la ricezione di veri e propri programmi [176]. Un programma è una serie di trasmissioni allestita dall'emittente, destinata al pubblico, offerta in continuità e a determinati orari, diffusa mediante tecniche di telecomunicazione.

Internet svolge quindi un ruolo soltanto in quanto mera infrastruttura di diffusione. Se attraverso Internet vengono diffusi veri e propri programmi radiotelevisivi, essi sottostanno alla LRTV. La legge sulla radiotelevisione non disciplinerà altri tipi di servizi Internet nemmeno in futuro.

7.133 Conclusioni

Il diritto vigente non prevede pertanto *nessuna disposizione* che potrebbe fungere da base per misure di diritto amministrativo volte alla lotta contro la violazione di beni giuridici nelle reti di comunicazione. Sul piano del diritto amministrativo, i provider vengono considerati dalla LRTV soltanto per quel che riguarda la trasmissione di informazioni.

---

[175] Cfr. ad esempio art. 43 segg. LTC (segreto in materia di telecomunicazioni), art. 48 (limitazione del traffico delle telecomunicazioni per motivi gravi), art. 49 (contraffazione o dissimulazione di informazioni), art. 31 OTC (obbligo del fornitore di prestazioni di offrire gratuitamente la possibilità di bloccare le comunicazioni uscenti verso servizi a carattere erotico o pornografico).

[176] DATEC, Commenti al progetto di nuova legge sulla radiotelevisione (LRTV), consultazione del dicembre 2000, pag. 18 seg. – Il messaggio concernente la revisione totale della legge federale sulla radiotelevisione è stato licenziato dal Consiglio federale il 18 dicembre 2002; cfr. FF 2003 1399 segg.

7.2. Possibili strumenti di diritto amministrativo

7.21 Norme e disposizioni di polizia

In primo piano vi è la creazione di una base legale per disposizioni di polizia tese a garantire *beni giuridici specifici*. L'ammissibilità di una tale regolamentazione dipende dal tipo di *misure* previste.

7.211 Obblighi di autorizzazione

L'introduzione di un obbligo di autorizzazione per *l'attivazione di un sito web* è incompatibile con il divieto della *censura preventiva* (art. 17 cpv. 2 Cost.) [177].

Subordinare ad autorizzazione *l'offerta di zona memoria* per informazioni di terzi destinate al pubblico può pure sfociare in censura preventiva: ciò tanto più se il rilascio di una simile autorizzazione è abbinato all'installazione di determinati dispositivi di sicurezza (ad esempio filtri).

7.212 Obbligo di controllo del contenuto

Sarebbe ipotizzabile la creazione di una norma speciale che obblighi il provider a effettuare *controlli del contenuto*. Il rispetto di tale norma potrebbe essere imposto mediante l'adozione di *misure di vigilanza*. Se del caso si potrebbe pure associare a tale norma l'obbligo legale di installare un *sistema automatico di controllo*, in grado di filtrare determinate informazioni o di bloccarne il pubblico accesso.

Simili regolamentazioni conferirebbero tuttavia ai provider la sovranità statuale in materia di applicazione del diritto e consentirebbero loro di decidere autonomamente quali contenuti debbano essere considerati illegali e quindi filtrati, possibilità che non poggia su alcuna base costituzionale [178]. I provider potrebbero inoltre abusare di questa possibilità, al fine di eliminare in modo mirato i loro concorrenti e praticare concorrenza sleale [179].

Un obbligo legale generale di controllo dei contenuti potrebbe inoltre rivelarsi nella maggior parte dei casi inadeguato e pertanto non proporzionato. Esistono infatti svariati accorgimenti tecnici che permettono di eludere i filtri e i programmi di protezione in modo relativamente semplice. Poiché negli Stati vicini non esistono

---

[177] Cfr. nello stesso senso la „Déclaration sur la liberté de la communication sur l'Internet" del Comitato dei Ministri del Consiglio d'Europa, del 28 maggio 2003: http://www.coe.int/T/F/Droits_de_l%27Homme/media/5_Ressources_documentaires/1_Textes_de_base/2_%20Textes_du_Comite_des_Ministres/PDF_D%E9claration%20libert%E9%20de%20communication%20sur%20Internet%20%20(f).pdf

[178] Cfr., con la medesima conclusione, la „Déclaration sur la liberté de la communication sur l'Internet" (loc. cit.)

[179] Cfr. SEMKEN, (bibl.), pag. 270 seg., con l'esempio di un provider, nel contempo anche fornitore di contenuti, che impiega un „filtro per la protezione dei minori" allo scopo di poter eliminare determinati prodotti della concorrenza.

prescrizioni simili, una tale normativa dovrebbe rivelarsi comunque ampiamente inefficace almeno per quanto riguarda i fornitori di accesso [180].

7.213 Obbligo di annunciare e di denunciare

Per i motivi suesposti, rimane inammissibile l'obbligo del provider di annunciare e di denunciare abbinato all'obbligo (provvisorio) di effettuare un controllo dei contenuti. Non appare invece del tutto inammissibile sottoporre a un obbligo di annuncio e di denuncia a un'autorità quei provider che, in seguito a segnalazioni fornitegli da terzi, sono concretamente a conoscenza di presunte violazioni di beni giuridici [181]. In tal caso al provider non verrebbe conferita alcuna sovranità statuale in materia di applicazione del diritto e non sarebbe tenuto a effettuare un controllo dei contenuti. Sotto il profilo del principio dell'uguaglianza giuridica, la determinazione dei provider sottoposti all'obbligo di annuncio deve tuttavia fondarsi su criteri oggettivi.

Secondo il parere della commissione d'esperti, è opportuno integrare quest'obbligo limitato di annuncio nella proposta di nuova versione dell'articolo 322bis numero 1 capoverso 2 CP, e assicurarne così il rispetto mediante la comminazione di sanzioni penali [182].

7.214 Monitoring

Non è chiaro se anche il „*monitoring* " [183] debba essere considerato censura preventiva o censura giustificata (art. 36 Cost.) [184]. In relazione a tale misura occorre in ogni caso vegliare affinché i controlli non si svolgano unicamente in modo automatico: soltanto le persone sono infatti in grado di constatare le violazioni dei beni giuridici. Il blocco o l'eliminazione di siti web che risultano da una censura *a posteriori* devono essere decretati nella forma di una decisione (impugnabile).

---

[180] Secondo l'art. 15 n. 1 della Direttiva UE sul commercio elettronico (vedi capitolo 4) agli Stati membri viene addirittura vietato di imporre agli access, caching e hosting provider un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano, o un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

[181] Cfr. pure l'art. 15 n. 2 della Direttiva UE sul commercio elettronico, secondo cui gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti a informare senza indugio l'autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi.

[182] Cfr. in merito il capitolo 9. L'obbligo di annuncio si limita opportunamente ai provider che tengono automaticamente a disposizione informazioni altrui in una rete di comunicazione elettronica.

[183] Per „monitoring" si intendono i controlli sistematici, effettuati da organi statali, di informazioni diffuse nelle reti di comunicazione e riguardanti potenziali violazioni di beni giuridici.

[184] Cfr. per maggiori dettagli MARKUS SCHEFER, Die Kerngehalte von Grundrechten, Habil. Berna 2001, pag. 462 segg. – Dal gennaio 2003, il „Servizio di coordinamento per la lotta alla criminalità su Internet" (SCOCI) è alla ricerca di atti punibili commessi su Internet. Secondo il parere della commissione d'esperti si tratta di una sorta di „pattugliamento in Internet", che può senz'altro essere qualificato come „monitoring", ma che in questo caso è sufficientemente giustificato ed è pertanto conforme alla Costituzione.

7.215 Decisioni di blocco e rimozione

È legittima la creazione di una regolamentazione legale che, sulla base del "principio del perturbatore", menzioni il fornitore di contenuti e l'hosting provider quali destinatari potenziali di una disposizione di rimozione. Se il provider non è d'accordo con l'ordine concreto impartito dall'autorità, ha la possibilità di sottoporlo al vaglio di un'autorità giudiziaria. Secondo il parere della commissione d'esperti è tuttavia opportuno integrare la base legale di simili decisioni nel proposto articolo 322bis numero 1 capoverso 5 CP [185].

Per quel che riguarda i fornitori di accesso, una disposizione generale e astratta che li obblighi a limitare l'accesso a determinati dati si rivela invece *inefficiente* e quindi *non proporzionata*. Infatti, malgrado gli sforzi dei provider, risulta relativamente facile aggirare tecnicamente simili restrizioni dell'accesso [186].

7.22 Estensione dell'obbligo e delle condizioni di concessione?

7.221 Principio

In base al vigente diritto in materia di telecomunicazioni, l'obbligo di concessione è legato all'esercizio indipendente di impianti di telecomunicazione. Gli aspetti contenutistici non costituiscono nessun criterio. Poiché la maggior parte dei provider svizzeri non esercita in modo indipendente un impianto di telecomunicazione per la trasmissione di informazioni, non sono di principio sottoposti ad alcun obbligo di concessione, ma sono tenuti alla notifica (art. 4 cpv. 2 LTC).

Per combattere la criminalità in rete si potrebbe teoricamente sottoporre un maggior numero di persone all'obbligo di concessione, e nel contempo applicare le condizioni di concessione per prestatori di servizi di telecomunicazione anche al contenuto. In tal modo i fornitori d'accesso sarebbero costretti a controllare il contenuto del flusso di dati che scorre attraverso la struttura dei loro impianti. Una simile normativa, tuttavia, non è soltanto *in contraddizione* con l'evoluzione attuale, ma si rivela anche *inammissibile*.

7.222 Contrasto con la tendenza attuale

L'introduzione di obblighi di concessione supplementari è chiaramente in contrasto con la tendenza attuale. In materia di LRTV, l'obbligo di annunciare diventerà la regola. Sussisterà un obbligo di concessione unicamente laddove occorrerà assegnare beni di disponibilità limitata (ad esempio frequenze) o assegnare fondi pubblici (quote prelevate dalle tasse di ricezione).

Anche con la *revisione parziale della legge sulle telecomunicazioni*, posta in consultazione nel giugno 2002, si intende abbandonare l'attuale esteso sistema di

---

[185] Cfr. in merito capitolo 9.
[186] Per maggiori approfondimenti cfr. comunque l'art. 12 n. 3 della direttiva UE sul commercio elettronico; vedi capitolo 4.

concessioni per i servizi di telecomunicazione, rendendo a tal fine più efficiente la vigilanza da parte dello Stato [187].

7.223 Inammissibilità

Lo Stato non può delegare a concessionari il controllo dei contenuti, se ciò comporta una *censura preventiva* (art. 17 cpv. 2 Cost.): in tal modo sarebbe infatti violato il contenuto essenziale della libertà d'opinione e dei media.
La delega del controllo dei contenuti a un concessionario sarebbe inammissibile anche se equivalesse a una *censura a posteriori*. Una simile regolamentazione sottrarrebbe alla sfera statuale la sovranità in materia di applicazione del diritto e la esporrebbe al rischio dell'arbitrio e dell'abuso.

Estendendo ad aspetti contenutistici le condizioni per il rilascio di una concessione, si costringerebbero i fornitori d'accesso a installare e a gestire un sistema di sicurezza e di controllo, ciò che appare tuttavia sproporzionato e quindi inammissibile (cfr. n. 7.212).

7.23 Gentlemen's agreement

Quale alternativa alle classiche disposizioni di polizia, per proteggere i beni giuridici minacciati vi è la possibilità di ricorrere ad *accordi informali* ("gentlemen's agreements"). Lo scopo di tali accordi è di indicare una linea di condotta, senza tuttavia imporre obblighi giuridicamente vincolanti [188]. Sono diffusi soprattutto nel diritto dell'ambiente e nel diritto amministrativo economico.

Il principio della legalità non si oppone alla conclusione di tali accordi, tranne che nei casi in cui il senso e lo scopo di una norma ne impediscano espressamente o implicitamente l'applicazione, ad esempio attraverso un rimando alle forme di attuazione della decisione o del contratto [189].

Nel presente contesto le intese informali si rivelano tuttavia solo in parte adeguate. È vero che permettono di definire consensualmente le misure di controllo e di sicurezza tecnicamente possibili e ragionevoli per il provider. Tuttavia, occorre nel contempo garantire che la determinazione del carattere illegale del contenuto delle informazioni, e quindi la sovranità in materia di applicazione del diritto nel singolo caso, continui a spettare alla autorità statali. Inoltre le intese informali mettono a nudo i loro limiti quando violano i diritti fondamentali di terzi, come ad esempio la libertà d'informazione del pubblico o la libertà economica di altri provider. In simili casi la dottrina esige un'audizione provvisoria dei terzi interessati: in caso contrario occorre una decisione nel merito [190]. Per il resto i limiti delle intese informali, la cui portata rimane poco chiara [191], sono più evidenti nel presente contesto che in altri ambiti giuridici.

---

[187] Cfr. in merito <http://www.bakom.ch/de/telekommunikation/grundlagen/konsult/fmg/ index.html>.
[188] HÖSLI (bibl.), pag. 39 seg.; PFENNINGER (bibl.), pag. 228; HÄFELIN/MÜLLER (bibl.), n. 734 segg., 737; TSCHANNEN/ZIMMERLI /KIENER (bibl.), pag. 265.
[189] Cfr. HÖSLI (bibl.), pag. 168 segg.; PFENNINGER (bibl.), pag. 81 segg., 102 segg.
[190] TSCHANNEN/ ZIMMERLI/KIENER (bibl.), pag. 267.
[191] HÄFELIN/MÜLLER (bibl.), n. marg. 736.

7.3 Conclusioni: rinuncia a misure fiancheggiatrici di diritto amministrativo

I limiti posti dalla Costituzione (divieto della censura preventiva, principio di proporzionalità) riducono fortemente l'estensione delle possibili regolamentazioni di diritto amministrativo. Secondo il parere della commissione peritale, tuttavia, l'introduzione di strumenti di diritto amministrativo, in sé ammissibili e necessari secondo la Costituzione, non richiede né una revisione del vigente diritto in materia di telecomunicazioni, né tantomeno la creazione di una nuova legge. Le pertinenti misure possono infatti venir adottate nell'ambito della proposta revisione del Codice penale, associandole eventualmente a procedure legislative in corso.

- In considerazione della proposta di nuovo *articolo 322bis numero 1 capoverso 2 CP*, un *obbligo di annunciare* sul piano del diritto amministrativo si rivela superfluo. La disposizione citata prevede un obbligo di annunciare, limitato ma sufficiente, per gli hosting provider (cfr. capitolo 9).
- Invece di creare una base legale di diritto amministrativo distinta per giustificare *ordini di rimozione o di blocco* nei confronti di hosting o content provider, l'eliminazione di informazioni illegali potrà fondarsi sull'articolo 322bis numero 1 capoverso 5 CP proposto dalla commissione peritale, indipendentemente dalla sovranità penale svizzera (cfr. capitolo 9). Gli stessi motivi considerati in relazione alle misure di blocco di diritto amministrativo (cfr. n. 7.215) si oppongono a decisioni di cancellazione e di blocco diretti contro fornitori d'accesso, sia che simili misure si basino su un'interpretazione estensiva dell'articolo 58 CP o su disposizioni cantonali di procedura penale.

In luogo di un „*monitoring*", misura non sempre limpida dal profilo costituzionale, potrebbe essere creata una base legale per *inchieste mascherate*. Una simile procedura garantirebbe in particolare maggior efficienza nella lotta contro i contenuti penalmente rilevanti nelle reti di comunicazione. La commissione peritale rinuncia quindi a proporre una base legale nel presente contesto e si limita a rinviare alla legge federale sull'inchiesta mascherata (LFIM).

La responsabilità civile in relazione alle violazioni della legge in Internet si fonda sul diritto delle obbligazioni e sulle norme sulla responsabilità contenute in leggi speciali. Oggi non vi sono disposizioni specifiche applicabili ai provider Internet. Una futura legislazione in materia dovrà ispirarsi in primo luogo alla direttiva UE sul commercio elettronico.

8. Responsabilità civile

8.1 Osservazioni preliminari

Il regime della responsabilità, che definisce l'attività dei provider Internet e ne determina gli investimenti, oltre che al diritto penale è improntato anche a quello civile. L'indignazione pubblica suscitata dalla diffusione di contenuti punibili (ad esempio pornografia, discriminazione razziale, rappresentazioni di cruda violenza), ha senza dubbio fatto passare in secondo piano le cause civili di responsabilità, quali la violazione della proprietà intellettuale, del diritto della concorrenza e dei diritti della personalità.

La giurisprudenza estera dimostra tuttavia che è aumentato il numero di azioni di diritto civile intentate contro hosting provider e fornitori di accesso, e che la responsabilità civile assume rilevanza sempre maggiore. Nell'esaminare la responsabilità penale dei provider Internet, per coerenza non vanno trascurati gli aspetti legati alla responsabilità civile: occorre pertanto tener conto di analogie e differenze.

Nell'ambito dei suoi lavori, vertenti in primo luogo sulla responsabilità penale, la commissione peritale si è anche occupata della questione relativa a una modifica delle disposizioni sulla responsabilità civile. Partendo dal rapporto esplicativo relativo all'avamprogetto di legge federale sul commercio elettronico [192], secondo cui non vi è la necessità di disciplinare la responsabilità civile dei provider [193], la commissione ha considerato, *da un lato*, la necessità di principio di una modifica sul piano del diritto civile. *Dall'altro* ha ritenuto più opportuno adeguare contemporaneamente diritto penale e civile, piuttosto che procedere a modifiche nei due ambiti giuridici scaglionate nel tempo.

[192] Rapporto esplicativo del 17 gennaio 2001 relativo all'avamprogetto di legge federale sul commercio elettronico (revisione parziale del Codice delle obbligazioni e della legge federale contro la concorrenza sleale), < http://www.ofj.admin.ch/themen/e-commerce/vn-ber-b-i.pdf >.

[193] Op. cit., pag. 9: „Analogamente, anche gli eventuali adeguamenti del diritto della proprietà immateriale e della responsabilità civile e penale dei provider dipende essenzialmente dall'evoluzione giuridica internazionale. In tale ambito non sussiste attualmente un bisogno d'intervento immediato sul piano legislativo. È possibile trovare soluzioni appropriate sulla base del diritto vigente."

Nonostante il carattere internazionale del flusso di informazioni via Internet, la commissione peritale ha rinunciato a trattare il problema relativo al *diritto internazionale privato*. La commissione ritiene che l'esame di tali questioni avrebbe oltrepassato i termini del suo mandato, che la incarica in particolare di esporre un parere relativo al modo di strutturare, dal punto di vista dei contenuti, la responsabilità penale dei provider Internet.

Le fattispecie penali presenti nelle *normative speciali di diritto civile*, in particolare nella legge sui diritti d'autore (LDA, RS 231.1), nella legge sulla protezione dei marchi (LPM, RS 232.11) nonché nella legge federale contro la concorrenza sleale (LCSl, RS 241) sono trattate nel capitolo dedicato agli aspetti di diritto penale (vedi n. 6.12).

8.2 Responsabilità extracontrattuale

8.21 Fondamenti della responsabilità

L'ordinamento giuridico svizzero non contempla norme specifiche di responsabilità che si applicano in caso di violazioni della legge commesse per mezzo di Internet. In tali casi occorre riferirsi alle *disposizioni generali del Codice delle obbligazioni* (CO, RS 220) relative alla responsabilità per atti illeciti (in particolare in caso di lesioni della personalità) o alle *norme di responsabilità contenute in leggi speciali* (vedasi soprattutto l'art. 62 LDA, l'art. 55 LPM e l'art. 9 LCSl). Sulla base di queste leggi speciali, le disposizioni del Codice delle obbligazioni si applicano anche alle pretese pecuniarie [194].

8.22 Responsabilità civile di fornitori di accesso e di hosting provider

Nell'ambito della discussione relativa alla responsabilità civile di fornitori di accesso e hosting provider, la situazione di partenza è paragonabile a quella che riguarda il diritto penale. Nel caso di una violazione di un bene giuridico commessa via Internet, l'identificazione della persona direttamente responsabile di un reato e i relativi accertamenti si rivelano talvolta praticamente impossibili o richiedono sforzi sproporzionati.

Anche se il responsabile viene identificato, il suo perseguimento può comunque apparire vano. Ciò è ad esempio il caso se tale persona risiede all'estero o non dispone di sufficienti mezzi finanziari che possano fungere da garanzia nel caso di un'azione di risarcimento del danno. Per il titolare del diritto si pone quindi il problema della possibilità di intentare un'azione contro terzi responsabili, tra cui

[194] L'*azione inibitoria e l'azione di rimozione* possono essere intentate in tutti i casi di comportamento oggettivamente illecito. Una colpa non è necessaria, e tantomeno la prova di un danno. Secondo l'articolo 41 CO, per intentare un'*azione di risarcimento* occorre dimostrare l'esistenza di un danno, l'illiceità del comportamento, un nesso di causalità tra comportamento pregiudizievole e danno nonché la colpa dell'autore del comportamento illecito. La pretesa di riparazione morale presuppone, oltre all'illiceità e al nesso di causalità, anche una lesione della personalità di una certa gravità. La pretesa di *restituzione dell'arricchimento* ai sensi dell'articolo 423 CO, secondo la giurisprudenza costante esiste a prescindere da una colpa.

vanno presi in considerazione anche fornitori di accesso e hosting provider, in quanto soggetti partecipanti al processo di comunicazione.

L'articolo 50 CO, al quale rinviano l'articolo 28a CC e le rispettive leggi speciali, può fondare una pretesa di risarcimento nei confronti di tali soggetti. Secondo l'articolo 50 CO è possibile intentare un'azione di risarcimento contro chiunque partecipa alla lesione o alla messa in pericolo di un bene giuridico (in quanto istigatore o complice). Non occorre che vi sia stata una comune intesa. È sufficiente che i partecipanti debbano riconoscere che le loro azioni od omissioni sono atte a cagionare la lesione colpevole del bene giuridico.

8.221 Pretese dipendenti da una colpa

In molti casi, eventuali pretese di risarcimento dipendenti da una colpa e dirette contro fornitori di accesso o hosting provider dipenderanno dalla valutazione della negligenza e, in caso di omissione [195], anche dal dovere di agire, che viene esaminato sotto il profilo dell'illiceità. In Svizzera i doveri di diligenza dei fornitori di accesso e degli hosting provider *non sono ancora stati chiariti* [196]*.* Per quel che concerne il fornitore di accesso non è ancora chiaro se e in che misura è possibile pretendere che sia a conoscenza dei contenuti che ha reso accessibili. Non vi è certezza neppure quanto all'esistenza e all'estensione degli obblighi di controllo e di sorveglianza che incombono all'hosting provider e, pertanto, fino a che punto sono tenuti a rispondere delle loro violazioni.

La letteratura pone prevalentemente l'accento sul fatto che gli obblighi di diligenza esistono soltanto nella misura in cui sono *ragionevolmente esigibili e possibili*. In caso di mera messa a disposizione dell'infrastruttura tecnica per la trasmissione di dati o per l'accesso alla rete, di regola non si pretende dal fornitore di prestazioni la conoscenza e il controllo dei contenuti trasmessi (ciò che equivale a negare una responsabilità aquiliana del gestore di rete e del fornitore di accesso per contenuti illegali di terzi). Le opinioni divergono invece in relazione a quanto si può ragionevolmente pretendere dal fornitore di contenuti per quel che concerne la conoscenza e la verifica dei contenuti illeciti altrui. O si parte dal presupposto che vi sia un obbligo limitato di prendere conoscenza dei contenuti di terzi, o si ammette un obbligo limitato di controllare tali contenuti.

In definitiva la dottrina tende a *limitare la responsabilità dell'hosting provider*, e tiene conto del fatto che quest'ultimo si assume ulteriori compiti, quali l'assistenza a siti web o la moderazione di gruppi di discussione.

---

[195] In relazione all'attività dell'hosting provider, non è chiaro se la violazione debba derivare da una sua azione o da una sua omissione.

[196] Per le opinioni vigenti in Svizzera vedasi WEBER (bibl.), pag. 507 segg. (fornitore d'accesso) e 515 segg. (hosting provider), con ulteriori riferimenti; PHILIPPE GILLIÉRON, La résponsabilité des fournisseurs d'accès et d'hébergement, ZSR NF vol. 121/I, pag. 387 segg., in particolare pag. 430 segg. Per le opinioni vigenti in Europa vedasi ANDREA SCHMOLL: Die deliktische Haftung der Internet-Service-Provider: Eine rechtsvergleichende Untersuchung zu Deutschland, Frankreich, England und den USA, Francoforte sul Meno 2001.

8.222 Pretese indipendenti da una colpa

La pretesa volta alla rimozione di contenuti illegali o quella inibitoria presuppongono soltanto un'ingerenza illecita in diritti altrui: una colpa non è quindi necessaria. Per una pretesa di rimozione è pertanto sufficiente che vi sia una partecipazione in relazione di causalità adeguata con la violazione della legge, e una (ragionevole) possibilità di impedire che tale violazione avvenga. Di conseguenza sarebbe possibile pretendere da hosting provider e da fornitori di accesso il blocco e/o la cancellazione di contenuti, quantunque soltanto nella misura in cui tali misure siano tecnicamente possibili e ragionevolmente esigibili. In conformità alla letteratura e la giurisprudenza europee, all'atto di valutare il carattere ragionevolmente esigibile occorrerà mettere *in relazione il dispendio tecnico con la possibilità di un aggiramento* della misura.

Ci si chiede tuttavia se sia possibile intentare un'azione di rimozione o inibitoria contro tutti i soggetti che fanno parte della catena causale che porta alla violazione della legge. Il problema della limitazione della responsabilità del fornitore di accesso e dell'hosting provider si pone quindi anche in relazione alle azioni inibitorie e di rimozione. Si tenta in parte di risolvere il problema ricorrendo alla nozione di causalità adeguata. In tale contesto in Germania ci si riallaccia anche alla figura del "perturbatore", frequente nell'ambito del diritto amministrativo (cfr. n. 5.12). Finora in Svizzera questo problema non è ancora stato oggetto di dibattito.

8.23 Necessità di agire sul piano legislativo

Da quanto esposto in precedenza, risulta che in Svizzera la situazione normativa riguardante la responsabilità civile di hosting provider e fornitori di accesso *non è chiara*. Ciò potrebbe avere ripercussioni negative sugli investimenti in tale settore economico. Anche se la giurisprudenza svizzera suggerisce probabilmente soluzioni sostenibili concernenti l'interpretazione delle disposizioni generali sulla responsabilità, lo sviluppo di regole in materia richiederebbe anni. Affinché la certezza del diritto sia realizzata in tempi brevi, il legislatore deve fornire una risposta alle questioni ancora irrisolte. Una chiarificazione potrà avvenire nell'ambito della *legge federale sul commercio elettronico* o dei lavori concernenti la *revisione e l'unificazione del diritto della responsabilità civile* (legge sulla responsabilità civile) [197].

Il carattere globale di Internet esige *regole unificate a livello internazionale* per la responsabilità dei provider Internet. A livello internazionale non vi sono sforzi di armonizzazione in vista di una normativa in materia di responsabilità che sia coerente dal punto di vista del diritto civile e penale, e una soluzione internazionale non è da attendersi in tempi ragionevoli. Per il momento si giustifica quindi di percorrere la *via nazionale*. Ma anche nel caso di una regolamentazione nazionale la Svizzera non può ignorare del tutto la dimensione internazionale della problematica.

---

[197] Lo stato delle due procedure è diverso: per quanto attiene alla legge federale sul *commercio elettronico*, il 9 dicembre 2002 il Consiglio federale ha incaricato il DFGP di elaborare un messaggio. Per quel che riguarda la *revisione e l'unificazione del diritto della responsabilità civile*, il Consiglio federale ha preso atto dei risultati della procedura di consultazione nel corso del 2003. Al momento in cui si deciderà in quale progetto inserire una regolamentazione della responsabilità civile di hosting provider e di fornitori di accesso, occorrerà tenere conto del diverso stato dei due processi legislativi.

Occorre quindi tenere conto dei tentativi di soluzione e delle esperienze compiuti all'estero (cfr. capitolo 4).

Gli articoli 12 a 15 della *direttiva UE sul commercio elettronico* [198] possono rappresentare un primo punto di partenza per una regolamentazione nazionale. Le prime esperienze compiute con questa direttiva dimostrano tuttavia che, soprattutto in relazione alle pretese di rimozione e inibitorie, vi è la necessità di emanare disposizioni integrative atte a chiarire le questioni riguardanti gli obblighi di blocco e di cancellazione fondati sul diritto civile. Occorre infine prestare attenzione anche alla responsabilità civile derivante dai link.

8.24 Coordinamento con il diritto penale

Nel contesto della criminalità in rete, la responsabilità penale e quella civile presentano numerosi *punti in comune*. Con le soluzioni in materia di diritto penale proposte dalla commissione peritale (cfr. capitolo 9), si effettuano valutazioni concernenti la responsabilità di hosting provider e fornitori di accesso che si rivelano determinanti anche per le pretese di risarcimento civili dipendenti da una colpa. Ciò concerne innanzitutto la valutazione di eventuali obblighi di controllo o di sorveglianza. Le fattispecie penali possono quindi rappresentare norme di protezione che, nel caso di un mero danno patrimoniale, fondano il carattere illegale dell'infrazione [199]. Sono inoltre comminate sanzioni penali anche in fattispecie di diritto civile disciplinate in leggi speciali. In questo contesto si pone quindi concretamente la questione relativa all'applicazione del diritto penale dei media, così come della nuova normativa proposta, agli atti commessi per mezzo di reti di comunicazione elettronica.

Occorre tuttavia prestare attenzione anche alle *differenze strutturali* tra i due ambiti giuridici. Nell'ambito del diritto penale, per il tipo di reati in esame la negligenza non svolge pressoché alcun ruolo. In particolare, la complicità ai sensi del diritto penale presuppone l'intenzionalità e viene sempre più messa in risalto quale base per fondare una possibile responsabilità del provider Internet, per le informazioni di terzi che tale provider trasporta o memorizza. La complicità ai sensi del diritto civile, secondo l'articolo 50 CO, può tuttavia configurarsi anche per negligenza. Va inoltre tenuto conto del fatto che nel diritto civile la nozione di colpa è oggettivata. Di conseguenza nel diritto civile la questione relativa al carattere ragionevolmente esigibile delle eventuali contromisure del provider viene valutata secondo criteri generali, e non in funzione delle condizioni individuali del singolo provider. La questione della responsabilità civile, in relazione con le pretese inibitorie e di rimozione indipendenti da una colpa, va oltre la problematica penale, che presuppone la colpevolezza.

---

[198] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa al commercio elettronico (la cosiddetta "Direttiva sul commercio elettronico", cfr. capitolo 4).

[199] Secondo la giurisprudenza del Tribunale federale (DTF 119 II 127 cons. 3) e la dottrina dominante, la norma sulla responsabilità dell'articolo 41 CO si fonda sulla teoria oggettiva dell'illiceità. Secondo tale teoria un danno è arrecato illecitamente se vi è violazione di un obbligo legale generale: il danno consiste nella lesione di un diritto assoluto del danneggiato, o in un semplice danno patrimoniale derivante dalla violazione della rispettiva norma di protezione.

Considerate le differenze, una *regolamentazione trasversale* che comprenda gli aspetti di diritto penale e quelli di diritto civile si rivela altrettanto poco convincente di normative parallele. Il dibattito dogmatico che va condotto in vista dell'elaborazione di una proposta concreta di soluzione nell'ambito della responsabilità civile, da impostare sull'articolo 50 CO, parla piuttosto a favore di un modo di procedere distinto in entrambi i settori giuridici.

8.3 Responsabilità contrattuale di fornitori di accesso e hosting provider

La valutazione della responsabilità contrattuale dei provider Internet [200] è correlata solo in parte con la problematica penale soltanto. Una simile relazione sussiste in particolare quando un provider Internet, in considerazione di una possibile responsabilità penale, di sua iniziativa o in ossequio a una decisione di blocco o di un altro tipo di misura emanata da un'autorità di perseguimento penale, non può fornire o non può fornire nel debito modo prestazioni dovute sulla base di un contratto. In questi casi è tuttavia possibile trovare soluzioni adeguate sulla base di intese contrattuali e del diritto vigente (art. 97 CO) [201]. Se l'inadempienza contrattuale è in particolare dovuta a un atto dell'autorità (ad esempio un ordine di blocco), il debitore non deve esserne ritenuto responsabile. La situazione sarebbe diversa se al provider, in quanto debitore, potesse essere rimproverato di aver omesso di adottare provvedimenti tecnici ragionevolmente esigibili, che avrebbero permesso di bloccare il materiale informativo incriminato senza nuocere ai suoi obblighi contrattuali.

Anche se sussistono punti in comune tra la tematica della responsabilità contrattuale e la problematica penale, secondo il parere della commissione peritale non vi è la necessità di un intervento del legislatore nel campo del Codice delle obbligazioni.

8.4 Conclusioni finali della commissione peritale

In relazione alla questione della responsabilità civile dei fornitori di prestazioni Internet, e in particolare dei fornitori d'accesso e degli hosting provider, la commissione peritale riconosce la necessità di una chiarificazione da parte del legislatore. Il problema della legittimazione passiva dei fornitori di accesso e degli hosting provider, per quel che concerne le azioni inibitorie e di rimozione, richiede quindi una discussione più approfondita.

Secondo il parere della commissione peritale, tali questioni potrebbero essere risolte sia nell'ambito della *legge federale sul commercio elettronico* che in quello dei lavori riguardanti la *legge federale sulla revisione e l'unificazione del diritto della responsabilità civile* (legge sulla responsabilità civile). La direttiva UE sul commercio elettronico dovrebbe in tal senso rappresentare un punto di partenza; una regolamentazione nazionale svizzera deve però anche dare una risposta alle

---

[200] Per la responsabilità contrattuale in generale, vedasi WEBER (bibl.), pag. 511 segg. (fornitore d'accesso) e 521 segg. (hosting provider), con ulteriori rimandi.

[201] MARKUS H. BERNI: Die zivil- und strafrechtliche Verantwortung des ISP, in: Hans Rudolf Trüeb (ed.), Aktuelle Rechtsfragen des E-Commerce, Zurigo 2001, pag. 117 segg., 134, nega in generale una responsabilità civile, invocando l'articolo 20 CO.

questioni essenziali che nella direttiva UE sono state riservate al legislatore degli Stati membri.

9. Proposte della Commissione

Testo legale proposto (modifica del Codice penale)

(nuovo titolo) 6. Reati in reti di comunicazione elettronica e nei media

(nuovo) Art. 27 CP ***Reati in reti di comunicazione elettronica***

1. Se un reato è commesso mediante trasmissione, preparazione o messa a disposizione di informazioni in una rete di comunicazione elettronica, si applicano le regole generali, fatte salve le disposizioni che seguono.

2. Se l'autore del reato è l'autore dell'opera o il redattore ai sensi dell'articolo 27^{bis}, la punibilità è retta da questa disposizione.

3. Chiunque mette automaticamente a disposizione informazioni di terzi per un loro impiego in una rete di comunicazione elettronica, è punibile alle condizioni dell'articolo 322^{bis} numero 1. La messa a disposizione di un elenco nel quale vengono registrate automaticamente informazioni di terzi è considerata messa a disposizione di informazioni di terzi.

4. Non è punibile chi fornisce unicamente l'accesso a una rete di comunicazione elettronica. Una memorizzazione automatica e transitoria di informazioni di terzi in seguito all'interrogazione di un utente è considerata fornitura di accesso.

(nuovo) Art. 27^{bis} CP ***Reati nei media***

[1] Se un reato è commesso mediante pubblicazione in un mezzo di comunicazione sociale e consumato per effetto della pubblicazione, solo l'autore dell'opera è punito, fatte salve le disposizioni che seguono.

[2] Qualora l'autore dell'opera non possa essere individuato o non possa essere tradotto davanti a un tribunale svizzero, è punito il redattore responsabile giusta l'articolo 322^{bis} numero 2. In sua mancanza, è punita giusta il numero 2 del medesimo articolo la persona responsabile della pubblicazione.

[3] Qualora la pubblicazione sia avvenuta all'insaputa o contro la volontà dell'autore dell'opera, è punito come autore del reato il redattore o, in sua mancanza, la persona responsabile della pubblicazione.

[4] Non soggiace a pena il resoconto veritiero di deliberazioni pubbliche e di comunicazioni ufficiali di un'autorità.

L'art. 27bis CP diventa art. 27ter CP, *Tutela delle fonti*, e il suo testo resta identico

(nuovo) Art. 322bis CP ***Mancata opposizione a reati commessi in reti di comunicazione elettronica e nei media***

(nuovo) 1. Chiunque mette automaticamente a disposizione informazioni di terzi in una rete di comunicazione elettronica, sapendo con certezza che per mezzo di tali informazioni è commesso un reato, e non impedisce l'impiego di tali informazioni, anche se ciò sarebbe tecnicamente possibile e lo si possa ragionevolmente pretendere, è punito con la detenzione o con la multa.

Chiunque mette automaticamente a disposizione informazioni di terzi in una rete di comunicazione elettronica, per mezzo delle quali è commesso un reato, e omette di trasmettere alle autorità di perseguimento penale segnalazioni di terzi, a lui indirizzate e pervenute, riguardanti tali informazioni, è punito con la detenzione o con la multa.

Se il reato ai sensi dei capoversi 1 e 2 è perseguibile solo a querela di parte, esso è punibile unicamente se la querela è stata sporta.

Il diritto svizzero è determinante per valutare se per mezzo di un'informazione viene commesso un reato ai sensi dei capoversi 1 e 2.

A prescindere dalla sovranità penale svizzera, le informazioni ai sensi dei capoversi 1 e 2 vengono cancellate.

(testo modificato dell'art. 322bis) 2. Chiunque, in quanto responsabile giusta l’articolo 27bis capoversi 2 e 3, intenzionalmente non impedisce una pubblicazione con la quale è commesso un reato è punito con la detenzione o con la multa. Se ha agito per negligenza, la pena è dell’arresto o della multa.

(nuovo) Art. 340ter CP ***In caso di reati in reti di comunicazione elettronica***

1 Sono inoltre sottoposti alla giurisdizione federale i reati commessi per mezzo di reti di comunicazione elettronica, qualora:
a. i reati siano stati commessi in più Cantoni e non abbiano riferimento prevalente in uno di essi; o
b. si riveli necessario un coordinamento delle inchieste in più Cantoni.

2 Il Ministero pubblico della Confederazione può inoltre aprire un'inchiesta se un'autorità cantonale competente gli sollecita la ripresa della procedura.

3 L’apertura di un’inchiesta secondo il capoverso 2 determina la competenza giurisdizionale federale.

Adeguamenti resi necessari dalle proposte precedenti

Art. 347 CP

[1] In caso di reato in Svizzera giusta l'articolo 27bis sono competenti le autorità del luogo, …

Art. 18bis Procedura penale federale (RS 312.0)

[1] Dopo la chiusura dell'istruzione preparatoria, il procuratore generale della Confederazione può delegare alle autorità cantonali il giudizio di una causa di diritto penale federale ai sensi degli articoli 340 numero 2, 340bis e 340ter del Codice penale. In questo caso, egli sostiene l'accusa davanti al tribunale cantonale.
[2] (invariato)
[3] (invariato)

Art. 26 Legge sul Tribunale penale federale (LTPF, non ancora in vigore)

La Corte penale giudica:
a. le cause penali sottoposte alla giurisdizione federale in virtù degli articoli 340, 340bis e 340ter del Codice penale, sempreché il procuratore generale della Confederazione non ne abbia deferito l'istruzione e il giudizio alle autorità cantonali;
b. …

9.1 Approccio normativo della commissione di esperti e commento alla nuova regolamentazione proposta

9.11 Generalità sulla regolamentazione della responsabilità

In considerazione della crescente permeabilità tra le diverse reti di comunicazione elettronica e della rapida evoluzione tecnologica in materia di informazioni e di reti, all'atto di delimitare l'ambito normativo della criminalità in rete non è consigliabile vincolarsi alla nozione di "Internet" e alla trasmissione di dati basata sul protocollo TCP/IP 202.

Una normativa coerente delle fattispecie riguardanti Internet deve comprendere anche gli ambiti, intersecati tra loro, dei servizi della comunicazione, dell'informazione e dei media: la nuova normativa deve quindi riferirsi ai vettori e ai contenuti della comunicazione. Si propongono pertanto diverse *possibili soluzioni* (vedi n. 9.12) 203.

9.12 Normativa orizzontale o in funzione degli ambiti?

9.121 Normativa orizzontale per tutti gli ambiti giuridici

Il legislatore potrebbe definire in una legge distinta una regolamentazione sulla responsabilità e sulla punibilità di tutti i soggetti coinvolti. Tale normativa sarebbe vincolante nella stessa misura per il diritto penale, il diritto della responsabilità civile, i diritti d'autore, il diritto della concorrenza ecc. Una simile soluzione è stata ad esempio adottata dalla Germania con la sua *Teledienstegesetz* (TDG) del 22 luglio 1997 204. Anche la *direttiva UE sul commercio elettronico* 205 parte fondamentalmente dal presupposto di una "regolamentazione della responsabilità" unitaria. Una regolamentazione orizzontale potrebbe però anche essere integrata in una legge esistente. In Svizzera è stato proposto di intraprendere una separazione della responsabilità e della punibilità per tutti i settori giuridici nella *legge sulle telecomunicazioni* (LTC, RS 784.10).

La soluzione della normativa orizzontale, che ha il pregio di chiarire con una legge autonoma tutti gli aspetti di diritto pubblico e civile riguardanti la responsabilità e la punibilità, presenta anche importanti inconvenienti. Optare per la creazione di una simile legge aggiuntiva significherebbe generare importanti problemi d'integrazione nel sistema delle condizioni di responsabilità e di punibilità delle normative vigenti (CP, CO).

---

[202] Per una spiegazione più dettagliata, vedasi n. 2.44.

[203] Vedasi in merito NIGGLI/SCHWARZENEGGER (bibl.), pag. 63 e 66 segg.

[204] Modificata in seguito all'adozione della "Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG)", in vigore dal 22 dicembre 2001, cfr. BGBl. I 2001 pag. 3721. Le norme sulla responsabilità si trovano agli articoli 8–11 TDG (nuova versione); cfr. capitolo 4, n. 4.31.

[205] Cfr. art. 12 segg. della direttiva sul commercio elettronico; cfr. capitolo 4.

In *Germania*, ad esempio, risulta controverso il modo in cui gli articoli 8 e seguenti TDG debbano inserirsi nel Codice penale, caratterizzato da un sistema di punibilità strutturato su vari livelli 206. Con nozioni quali "conoscenza" o "responsabilità", sia nel diritto civile che nel diritto penale ci si allontanerebbe da strumenti concettuali familiari, ciò che provocherebbe ulteriori problemi interpretativi. Per altre questioni, come ad esempio quelle riguardanti la punibilità dei link che rinviano a contenuti illeciti, la regolamentazione orizzontale della legge tedesca sui servizi telematici (Teledienstgesetz), e in particolare l'articolo 5 della vecchia versione, ha creato ulteriore confusione 207. Anche attenendosi agli orientamenti della direttiva europea sul commercio elettronico, non si deve necessariamente optare per una regolamentazione orizzontale.

Nel 2000 in *Francia* vi sono state importanti modifiche riguardanti le condizioni di punibilità dei provider. Il principio della cosiddetta responsabilità limitata è stato introdotto nell'articolo 43-8 capoverso 1 della legge sulla libertà della comunicazione. Secondo tale principio, l'hosting provider è punibile unicamente se non ha bloccato l'accesso a una pagina web incriminata immediatamente dopo un'ingiunzione giudiziaria. Risulta inoltre chiaro come l'adozione di tale norma escluda la punibilità del fornitore d'accesso. Nel progetto di legge era previsto un inasprimento dell'articolo 43-8. L'articolo 43-8 capoverso 2 del progetto stabiliva che poteva anche essere ammessa la punibilità dell'hosting provider che non avesse reagito alle segnalazioni fornitegli da un utente. Il *Conseil constitutionnel* ha tuttavia dichiarato il capoverso incostituzionale, basandosi unicamente sulle condizioni della punibilità, poiché in base al diritto penale francese la complicità presuppone un'intenzionalità diretta. Il dolo eventuale, che sarebbe stato compreso dalla formulazione dell'articolo 43-8 capoverso 2, non esiste nell'ambito dei reati intenzionali 208. Una prima proposta di legge del 14 giugno 2001 per l'attuazione della direttiva sul commercio elettronico proponeva quindi una specifica limitazione della responsabilità nell'ambito del diritto civile 209.

---

206 Non si è ancora verificata una modifica della parte generale del Codice penale mediante normative estranee al diritto penale, e la presunta chiarezza procurata dalla regolamentazione orizzontale ha originato quindi nuovi problemi e opinioni totalmente contrarie nella letteratura in materia (soluzione del filtro preventivo, modifica della fattispecie penale, giustificazione, esclusione della colpa, motivo di esenzione da pena, filtro successivo). Cfr. in merito NIGGLI/SCHWARZENEGGER (bibl.), pag. 66 seg.

207 Per un riassunto, cfr. CHRISTIAN SCHWARZENEGGER: Die strafrechtliche Beurteilung von Hyperlinks, in: Festschrift Rehbinder, Monaco 2002, pag. 723 segg. con ulteriori rimandi; tale disorientamento permane anche dopo la chiarificazione apportata dalla nuova versione, vedi in merito HENNING ROSENAU / LARS WITTECK, Der Castor-Transport und die Hakenkralle im Internet, JURA 2002, 781 segg.

208 Loi du 1er août 2000 relative à la communication (loi no 2000-719 du 1er août 2000, modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication, JO du 2 août 2000, 11903). Tenore dell'articolo 43-9 di questa legge, cfr. n.. 4.33. Cfr. Conseil constitutionnel, Décision no 2000-433 DC du 27 juillet 2000, JO du 2 août 2000, 11922 segg., in particolare 11926. Maggiori precisazioni in merito in MOREILLON/DE COURTEN, (bibl.), pag. 12 con note.

209 Vedi Projet de loi sur la société de l'information, enregistré à la Présidence de l'Assemblée nationale le 14 juin 2001. Con il nuovo governo questo progetto legislativo non ha avuto seguito. Nel frattempo, il 15 gennaio 2003 il Ministero dell'Industria ha presentato un nuovo disegno di legge (Projet de loi pour la confiance dans l´économie numérique) che prevede due norme indipendenti per la responsabilità civile e la punibilità dell'hosting provider (nuovi art. 43-8 e 43-9) nella legge sulla libertà della comunicazione (loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication). La liberazione dalla responsabilità e l'impunibilità dell'access provider per la fornitura automatica di accesso verrà sancita nel Code des postes et télécommunications (nuovo art. L. 32-3-3). In *Giappone* è stata introdotta una regolamentazione specifica, vedi Law concerning limitation of

Secondo la commissione peritale, a queste condizioni *non è auspicabile* prevedere una regolamentazione orizzontale in una normativa Internet autonoma.

Una regolamentazione orizzontale nella legge sulle telecomunicazioni non sarebbe inoltre sufficientemente efficace, poiché il concetto di servizio di telecomunicazione comprende soltanto la fornitura di accesso per l'uso di informazioni (cfr. art. 3 LTC), ma non la loro preparazione o messa a disposizione allo scopo di trasmissione mediante telecomunicazione. Per quel che riguarda l'hosting, le questioni teoriche di diritto penale che occupano la dottrina continuerebbero a essere controverse e l'incertezza giuridica sussisterebbe. Inoltre l'articolo 2 LTC prevede un'eccezione per i programmi ai sensi della legge sulla radiotelevisione (LRTV, RS 784.40), che concernerebbe anche le emissioni radiotelevisive trasmesse via Internet. Infine, la LTC si applica soltanto ai servizi di comunicazione, ma non ai servizi informativi e mediatici 210. La commissione peritale ritiene pertanto che anche questo quadro normativo sia inadeguato.

9.122 Normativa specifica in funzione dell'ambito giuridico

La commissione peritale si schiera dunque per una soluzione specifica in funzione degli ambiti, accordando nel contempo la priorità all'adeguamento del CP. Questa soluzione permette da una parte l'adeguamento delle condizioni di punibilità, senza intervenire nella struttura della fattispecie e nelle nozioni specifiche consuete.

Nella maggior parte dei casi il diritto penale regola problematiche completamente diverse da quelle rette dal diritto civile. Molte delle fattispecie penali legate alla criminalità in rete tutelano infatti interessi generali, e non contemplano il danneggiamento di singole persone: già solo il fatto di creare un pericolo per un bene giuridico è passibile di pena. D'altra parte questa soluzione non ostacola un adeguamento delle condizioni della responsabilità civile, armonico sul piano della dogmatica giuridica e che tenga altresì in considerazione gli specifici interessi di parte. Al fine di realizzare l'obiettivo di creare una situazione giuridica stabile e sicura applicabile alle reti di comunicazione, è preferibile procedere a tappe.

9.13 I tre pilastri della nuova regolamentazione

- Nell'ambito delle reti di comunicazione elettronica, occorre fare chiarezza sui limiti della punibilità per quel che concerne i fornitori di infrastrutture per processi a svolgimento automatico. Se la partecipazione dell'access provider si limita alla mera fornitura dell'accesso, questa deve essere esente da pena. Per quel che concerne l'hosting provider, occorre distinguere il caso normale del trasferimento automatico di dati dai casi in cui l'hosting provider viene a conoscenza soltanto in un secondo tempo del (possibile) contenuto illecito dei dati. Nel primo caso è esente da pena, mentre nel secondo è punibile se non ha reagito. Su questa soluzione vi è ampio consenso a livello internazionale.

---

damages to specific telecommunications service provider and disclosure of sender information, passed on November 22, 2001.

[210] NIGGLI/SCHWARZENEGGER (bibl.), pag. 68.

- In tal modo è possibile risolvere su un piano settoriale il problema degli "atti neutrali" (cfr. n. 6.3). Nel settore delle reti di comunicazione elettronica, i fornitori di prestazioni devono rispettare, sul piano del diritto penale, condizioni quadro unitarie e ben definite.

- La nuova regolamentazione prevede inoltre precisi criteri di delimitazione tra il diritto penale applicabile ai media e quello applicabile alle reti di comunicazione. Da un lato si intende mantenere l'attuale situazione privilegiata per i mass media attivi nel settore della comunicazione in rete, dall'altro si prevedono tuttavia chiare soluzioni per ogni fattispecie al di fuori di questo diritto penale speciale.

9.2 Commento al (nuovo) articolo 27 CP [211]

9.21 Titolo della sezione 6: „Reati in reti di comunicazione elettronica e nei media“

Nel definire la nozione, la commissione peritale si è lasciata guidare dalle seguenti *premesse*:

- la regolamentazione della responsabilità penale non deve *limitarsi unicamente a Internet* (cfr. capitolo 2, nn. 2.24, 2.4 – 2.6);
- la regolamentazione deve quindi essere *tecnologicamente neutrale*: non ha alcuna importanza il fatto che le informazioni siano trasmesse via cavo o via etere, o quale infrastruttura venga impiegata per la trasmissione (linee telefoniche, linee elettriche, ecc.);
- la regolamentazione privilegiata della punibilità *non dipende dalla pubblicazione*[212], e comprende quindi di principio anche i contenuti punibili della posta elettronica;
- la regolamentazione privilegiata della punibilità non comprende soltanto i reati d’espressione, ma bensì *tutti* i reati commessi attraverso la trasmissione, la preparazione o la messa a disposizione di informazioni in reti di telecomunicazione;
- per la regolamentazione *non ha alcuna importanza* se le informazioni sono accessibili in modo unilaterale (come ad esempio nei casi delle tradizionali trasmissioni radiotelevisive) o interattivo, ossia sulla base di uno scambio di dati (come ad esempio nei casi delle conversazioni telefoniche o dell'invio e della ricezione di posta elettronica). Viene compresa anche la comunicazione unidirezionale. La regolamentazione proposta si applica ad esempio anche alla

[211] Il *commento* della nuova regolamentazione proposta concerne il n. 9.2 (art. 27 CP), il n. 9.3 (nuovo art. 322bis CP) e il n. 9.4 (nuovo art. 340bis CP) - „art. 27 CP“ designa l'articolo 27 del CP nella sua versione attuale (quindi il diritto penale dei media); i riferimenti al nostro progetto di revisione sono definiti dalla designazione „(nuovo) art. 27 CP“. Per le altre disposizioni proposte si procede in modo analogo.

[212] Così come prevede l'attuale articolo 27 CP, che esclude quindi la comunicazione individuale dal proprio campo d'applicazione. La caratteristica della pubblicazione, secondo la giurisprudenza del Tribunale federale, presuppone che il contenuto in questione sia destinato al pubblico, e non a persone individualmente determinate (DTF 125 IV 177, 183 seg.).

diffusione di programmi radiotelevisivi attraverso la rete via cavo tradizionale, o in futuro nell'ambito della televisione digitale (Digital Video Broadcasting, DVB) o della radio digitale (Digital Audio Broadcasting, DAB) [213].

Le tre seguenti formulazioni sono prese in considerazione per definire una *nozione generale*, in grado di comprendere tutti gli ambiti menzionati.

9.211 Reati "in una rete di telecomunicazioni"

Si tratta di un concetto nuovo per il diritto svizzero. *Lo scopo* è quello di comprendere i seguenti fenomeni, (probabilmente) non considerati dalla LTC:

- la preparazione e la messa a disposizione di informazioni (non unicamente la loro trasmissione) [214];
- i programmi ai sensi della LRTV [215];
- i servizi informativi e mediatici (e non soltanto di comunicazione).

Questa terminologia ha *da una parte* lo svantaggio di non riallacciarsi ad alcuna definizione esistente, ciò che dovrebbe comportare qualche difficoltà nel trovare le necessarie argomentazioni nel corso della procedura di legislazione e nella successiva fase di applicazione del diritto. *D'altra parte* il concetto di telecomunicazione è originariamente collegato alla comunicazione individuale, come la telegrafia o la telefonia, ed è stato anche in parte distinto dai programmi radiotelevisivi (la radiodiffusione da un lato e la telecomunicazione dall'altro sono regolarmente comprese nel dibattito in quanto ambiti distinti l'uno dall'altro). Non appare comunque evidente che la nozione di "reti di telecomunicazione" comprenda anche la comunicazione unilaterale e la comunicazione di massa.

9.212 Reati commessi mediante trasmissione o messa a disposizione di informazioni

Questa formulazione, basata sulla terminologia della legge sulle telecomunicazioni, non comprende soltanto la trasmissione di informazioni, ma anche la loro messa a disposizione. Essa presenta però due inconvenienti: in primo luogo è complicata dal profilo linguistico, e secondariamente potrebbe causare confusione, poiché la nozione di telecomunicazione viene spesso equiparata a quella di telefonia. Dalla formulazione non risulta chiaro che la nozione comprende anche i programmi

[213] Occorre sottolineare che, nell'ambito della comunicazione unilaterale, non esiste attualmente la funzione dell'hosting provider. I chiarimenti relativi alle condizioni di punibilità valgono anche per il presente contesto: i fornitori di contenuti sono in linea di massima trattati in base alle regole generali, mentre non è punibile chi fornisce semplicemente l'infrastruttura attraverso cui passano le informazioni.

[214] L'art. 2 LTC si riallaccia alla "trasmissione mediante telecomunicazione di informazioni".

[215] L'articolo 2 LTC esclude i programmi dal suo campo d'applicazione.

radiotelevisivi, esclusi dal campo d'applicazione della LTC dall'articolo 2 di tale legge. L'inclusione dei programmi radiotelevisivi va pertanto esplicitamente disciplinata [216].

9.213 Reati "in reti di comunicazione elettronica"

Questa nozione è molto vasta e presenta il vantaggio di riallacciarsi a una terminologia esistente nel diritto europeo. Una *definizione* della nozione di rete di comunicazione elettronica si trova nell'articolo 2 lettera a della direttiva quadro UE sui servizi e le reti di comunicazione elettronica, del marzo 2002 [217]:

> "reti di comunicazione elettronica": i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato."

Questa definizione è quella che descrive nel modo più preciso le diverse funzioni delle reti di comunicazione. Di conseguenza il titolo della 6^{a} sezione va completato come segue: "Reati in reti di comunicazione elettronica e nei media".

L'inesattezza che risulta dalla locuzione "*in* reti di comunicazione elettronica" va tollerata. Lo scopo del titolo è infatti quello di costituire una nozione quadro, che valga sia per i reati commessi per mezzo di reti di comunicazione elettronica, sia per i reati mediatici che si consumano per effetto della pubblicazione. Il concetto viene in seguito precisato nel (nuovo) articolo 27 numero 1, che parla di reati commessi "mediante trasmissione, preparazione o messa a disposizione di informazioni" [218].

---

[216] Ciò vale almeno fino alla revisione totale della LRTV, che per quel che concerne la diffusione comporterà anche una modifica dell'articolo 2 LTC. In futuro, per la diffusione di programmi radiotelevisivi, ci si dovrà basare sul diritto in materia di telecomunicazioni; cfr. il messaggio del Consiglio federale del 18 dicembre 2002 concernente la revisione totale della legge sulla radiotelevisione, FF 2003 1399 segg.

[217] Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) Gazzetta ufficiale n. L 108 del 24/04/2002 pag. 33 segg.; reperibile al seguente indirizzo: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=it&numdoc=32002L0021&model=guichett (stato: 9.4.2003).

[218] I reati hanno luogo "in" rete soltanto in misura parziale. La rete può anche rappresentare unicamente il mezzo che permette di ottenere lo scopo prefisso, e avere quindi un ruolo marginale (ad es. nel caso della truffa).

9.22 (Nuovo) articolo 27 numero 1 CP (fornitore di contenuti)

9.221 „reato è commesso mediante …“.

La formulazione “reato commesso mediante” ha una portata più ampia rispetto a “reato commesso in”, e comprende tutti gli atti aventi a che fare con la trasmissione, preparazione o messa a disposizione di informazioni in reti di comunicazione elettronica. La regolamentazione mira quindi ad andare oltre l'ambito che viene solitamente citato quale esempio paradigmatico della criminalità su Internet, ossia quello dei cosiddetti reati d'espressione (rappresentazione di atti di cruda violenza, pornografia dura, discriminazione razziale, lesioni dell'onore, ecc.).

Quest'ambito deve certamente essere compreso dalla regolamentazione, il cui campo d'applicazione non deve però *limitarsi a esso*. La regolamentazione deve ad esempio comprendere anche i cosiddetti reati informatici, come la messa in circolazione di virus informatici (art. 144bis n. 2 CP). Devono inoltre essere inclusi anche i reati "tradizionali" (ad esempio i reati contro il patrimonio quali la truffa, art. 146 CP, o l'abuso di un impianto per l'eleborazione di dati, art. 147 CP; ma anche i reati previsti dal diritto penale accessorio, in particolare quelli in materia di concorrenza sleale o di protezione dei marchi; cfr. l'elenco al n. 2.2).

9.222 Trasmissione, preparazione e messa a disposizione

Il (nuovo) articolo 27 CP contempla *tre operazioni fondamentali* dal punto di vista della comunicazione in rete. Esse sono:

- la trasmissione, nel senso di un’emissione o ricezione elettrica, magnetica, ottica oppure elettromagnetica di altro tipo, di informazioni su linea o via radioonde;
- la preparazione, nel senso di un caricamento di informazioni in una zona memoria di un media, accessibile al pubblico mediante reti di comunicazione elettronica;
- la messa a disposizione, nel senso della gestione di un media su cui sono telecaricate informazioni, accessibile al pubblico mediante reti di comunicazione elettronica.

L'ultima tappa del processo di comunicazione consiste nel *richiamo* di informazioni, che è normalmente effettuato da un *utente*, il quale con tale agire non si rende ancora punibile (vi può tuttavia essere punibilità in caso di telecaricamento su un media locale, cfr. art. 197 n. 3bis CP).

9.223 Informazioni

La nozione di "informazioni" è ampia, e comprende in particolare anche i programmi informatici [219]. La proposta legislativa non si limita quindi ai "reati d'espressione"

[219] Cfr. la definizione legale dell'articolo 3 lettera a LTC: "segni, segnali, caratteri, immagini, suoni e rappresentazioni di qualunque altro genere destinati all’uomo, ad altri esseri viventi o a macchine".

commessi in Internet [220], ma va oltre: prevede anche una regolamentazione applicabile alla criminalità informatica [221] e ai reati in materia di diritti d'autore [222].

La commissione peritale ha preso in considerazione anche la nozione di *contenuti illegali*, ma l'ha scartata. Tale concetto non comprende infatti tutti i tipi di informazioni: in caso di offerte sul World wide web fraudolente o lesive dei diritti d'autore, i relativi contenuti non sono illegali in sé, ma è illegale il loro impiego. Inoltre la portata della nozione di "contenuti illegali" è controversa. Di conseguenza il disegno di legge utilizza il termine "informazioni", impiegato anche nella LTC e nella direttiva sul commercio elettronico. Le "informazioni" comprendono anche i contenuti illegali.

9.224 Validità delle regole generali

Secondo quanto proposto, il (nuovo) articolo 27 numero 1 prevede che di principio le regole generali si applichino anche ai reati commessi in una rete di comunicazione elettronica. Ciò può apparire superfluo, ma risulta dalla nuova struttura della punibilità, che prevede eccezioni (reti di comunicazione elettroniche; diritto penale dei media) alle regole generali. La regolamentazione proposta è strutturata su *tre livelli gerarchici*:

- in linea di massima si applicano le regole generali;
- si deroga a tali regole, nella misura in cui i reati sono stati commessi in una rete di comunicazione elettronica;
- nei confronti delle regole sancite dal (nuovo) articolo 27 CP, il numero 2 del (nuovo) articolo 27 CP prevede un'altra deroga in favore del vigente diritto penale dei media, tuttavia soltanto in relazione ad autori e redattori.

Si è optato per questa struttura a tre livelli perché le fattispecie da disciplinare (relative alla criminalità in rete) *da un lato* presentano una struttura che ricorda particolarmente quella dei reati mediatici (coinvolgimento necessario di numerosi partecipanti), ma *dall'altro* le fattispecie contemplate dal diritto penale dei media possono a loro volta realizzarsi anche per mezzo di reti di comunicazione elettronica (ad esempio, la pubblicazione on line di un quotidiano); i due ambiti dunque si sovrappongono. La regolamentazione strutturata su tre livelli gerarchici permette di comprendere tutte le fattispecie, in pratica senza dover procedere a rimandi.

---

[220] Ad esempio la rappresentazione di atti di cruda violenza (art. 135 CP), la pornografia (art. 197 CP), la discriminazione razziale (art. 261bis CP).

[221] Ad esempio l'allestimento di virus informatici (art. 144bis CP), le offerte fraudolente sul www (art. 146 CP).

[222] Ad esempio la pirateria musicale (art. 67 e 69 LDA).

9.23 (Nuovo) articolo 27 numero 2 CP (delimitazione rispetto al diritto penale dei media)

9.231 Rinvio al diritto penale dei media soltanto per gli autori e i redattori

Il (nuovo) articolo 27 numero 2 CP prevede una riserva in favore del diritto penale dei media, ossia il (nuovo) articolo 27bis CP. Le fattispecie alle quali si applica il diritto penale dei media classico, infatti, se realizzate in un certo modo (ad esempio pubblicazione on line di un quotidiano) possono entrare a far parte dell'ambito dei reati commessi in reti di comunicazione elettronica: occorre pertanto creare una riserva in favore del diritto penale dei media, oggetto di recente revisione. Lo scopo di tale riserva è quello di garantire che il diritto penale dei media non venga eluso dalla nuova regolamentazione. Questa è la funzione del (nuovo) articolo 27 numero 2 CP.

La riserva menziona tuttavia soltanto *gli autori e i redattori*. Essa non si applica invece alle "persone responsabili della pubblicazione", incluse nella regolamentazione attuale dall'articolo 27 capoverso 2 CP. Questo perché, in caso di reati commessi in reti di comunicazione elettronica mediante processi automatizzati, proprio questo gruppo di persone (ossia i responsabili della pubblicazione, fatta eccezione per gli autori e i redattori) dovrà essere sottoposto alla nuova regolamentazione. Invece gli altri membri della redazione e il personale tecnico ausiliario (ad esempio gli addetti alla macchina da presa, gli addetti ai cavi, ecc.) continuano a essere sottoposti al diritto penale dei media secondo il (nuovo) articolo 27bis CP, non avendo nulla a che fare con i processi automatici di trasmissione, messa a disposizione o preparazione di informazioni. Sulla base del testo legale del (nuovo) articolo 27 numero 2 non è nemmeno possibile un'interpretazione divergente, e non si può in particolare parlare di punibilità “specifica”.

Se la riserva del (nuovo) articolo 27 numero 2 comprendesse anche queste persone, le normative dei numeri 3 e 4 del (nuovo) articolo 27 CP non potrebbero avere una validità generale. Nell'ambito che si trova a cavallo tra diritto penale dei media e reti di comunicazione elettronica occorrerebbe quindi distinguere se il reato in questione è mediatico, ciò che comporterebbe l'applicazione del diritto penale dei media, o "comune", il che implicherebbe l'applicazione della regolamentazione prevista dal (nuovo) articolo 27 numeri 3 e 4 CP.

La limitazione agli autori e ai redattori della riserva in favore del diritto penale dei media garantisce d'altronde a questi ultimi che l'introduzione delle nuove disposizioni non implicherà per loro alcuna modifica, mentre per quanto attiene agli hosting provider e ai fornitori di accesso saranno emanate normative specifiche. Su questi due gruppi di persone non incombe quindi più la minaccia di punibilità basata sull'attuale articolo 322bis CP (nuovo ordine: art. 322bis n. 2 CP); gli hosting provider sono ormai sottoposti alla nuova regolamentazione del (nuovo) articolo 322bis numero 1, mentre la fornitura automatica dell'accesso da parte del provider continua a essere esente da pena sulla base del (nuovo) articolo 27 numero 4 CP.

La nuova regolamentazione in materia di punibilità dell'hosting provider si spinge da un lato meno lontano della precedente, poiché la negligenza non viene più contemplata, ma si rivela d'altro lato notevolmente più severa, poiché la

responsabilità penale è ammessa a prescindere dal fatto che un autore o redattore possa essere reso responsabile della pubblicazione [223].

9.24 (Nuovo) articolo 27 numero 3 CP (hosting provider, motori di ricerca)

9.241 Informazioni di terzi

Il (nuovo) articolo 27 numero 3 1° periodo CP limita il proprio campo d'applicazione alle "informazioni di terzi". Questo perché la messa a disposizione di *proprie* informazioni, anche se avviene in modo automatico, non dovrebbe beneficiare dei privilegi garantiti dal (nuovo) articolo 27 numero 3 CP.

Si parla di informazioni *di terzi* quando l'autore non le ha create lui stesso o non se ne è appropriato (ad esempio selezionandole scientemente, modificandole o raccogliendole). Le informazioni possono quindi essere originariamente di terzi, ma attraverso le azioni menzionate l'autore può appropriarsene. Poiché i motori di ricerca, nella misura in cui funzionano in modo automatico, sono al centro del processo di raccolta di informazioni, viene creata una regolamentazione speciale (vedi in merito n. 9.244).

Se l'autore tiene a disposizione *proprie* informazioni, non va più considerato mero hosting provider, ma sottostà alle regole generali relative agli autori del reato conformemente al (nuovo) articolo 27 numero 1 CP e, in qualità di autore o redattore, eventualmente in base al diritto penale dei media (nuovo art. 27bis n. 2 CP).

9.242 „mettere automaticamente a disposizione“

La formulazione "mettere automaticamente a disposizione" (considerando che si tratta della messa a disposizione di informazioni di terzi) designa essenzialmente ciò che oggi è conosciuto come *"hosting"*. Se l'host tiene a disposizione informazioni di terzi, è fondamentale che ciò avvenga *automaticamente*.

L'hosting provider mette a disposizione dei suoi clienti una porzione determinata di zona memoria sul suo elaboratore, che i clienti possono utilizzare. Una volta che al cliente è stato accordato il diritto di accedere alla zona memoria, egli può utilizzarla senza che l'hosting provider debba fare altro. Tutto ciò che il cliente telecarica in questa zona memoria, può essere richiamato digitando l'indirizzo corrispondente. L'hosting è paragonabile all'affitto di locali: dal momento in cui la chiave viene consegnata, il locatario può utilizzarli.

L'automatizzazione è un elemento che contribuisce a distinguere chiaramente la messa a disposizione di informazioni da altre fattispecie. La messa a disposizione delle informazioni è infatti necessaria affinché l'autore possa renderle accessibili al pubblico. Ma poiché l'autore utilizza la zona memoria automaticamente (in modo analogo all'uso di un'abitazione o di locali commerciali), ossia telecarica, cancella, modifica, ecc. le informazioni, l'hosting provider non sa che tipo di informazioni si trovano sul suo elaboratore. Può venirlo a sapere soltanto se gli perviene una segnalazione specifica, o se effettua egli stesso controlli (analogamente al locatore che ispeziona regolarmente i locali affittati).

[223] Cfr. capitolo 6.

9.243 Rinvio al (nuovo) articolo 322bis numero 1

Con la creazione di una norma autonoma nella parte speciale del Codice penale, la commissione peritale segue il modello di regolamentazione che aveva già ispirato la punibilità dei responsabili dei media nel (nuovo) articolo 322bis numero 2 CP [224].

9.244 Elenchi nei quali informazioni di terzi vengono automaticamente registrate (motori di ricerca), (nuovo) articolo 27 numero 3 2° periodo

Molti utenti iniziano la loro navigazione nel web utilizzando un *motore di ricerca* (i cosiddetti *search engines*, come google.com, hotbot.com, altavista.com). Si tratta di server web speciali che consentono di compiere una ricerca di lemmi in una banca dati, che rileva automaticamente l'offerta di informazioni esistenti (testi, immagini, musica, opere multimediali, ecc.) e le rende accessibili mediante collegamenti ipertestuali. Programmi Spider o Crawler setacciano continuamente il WWW, indicizzano nuovi siti web secondo i lemmi e li inseriscono nella banca dati del motore di ricerca con i rispettivi collegamenti ipertestuali. Chi gestisce il motore di ricerca lascia che questi procedimenti si svolgano in modo automatico, ma offre sul suo server l'indice con i rimandi ipertestuali, a disposizione dell'utente.

Il (nuovo) articolo 27 numero 3 CP equipara sul piano del diritto penale il gestore di tali motori di ricerca all'*hosting provider*. Questo completamento è necessario, poiché le informazioni contenute dall'indice del motore di ricerca [225] non appartengono più a terzi. Non si tratta di un fornitore di contenuti che mette a disposizione le proprie informazioni sul server del gestore del motore di ricerca, ma del gestore stesso del motore di ricerca che allestisce automaticamente una banca dati. Le informazioni contenute in questa banca dati appartengono al suo gestore, e il loro contenuto è quindi sottoposto alla regolamentazione del (nuovo) articolo 27 numero 1 CP.

Esempio: Un'interrogazione effettuata usando i lemmi "uomo politico X" e "fesso" origina una lista di risultati. Uno di questi, oltre al collegamento ipertestuale che rinvia a contenuti terzi, contiene la frase: "Questo signore al volante di una lussuosa BMW infatti non è un povero fesso qualsiasi, ma è l'uomo politico X di Y, noto donnaiolo."

Questa affermazione lesiva dell'onore può essere interpretata quale comportamento punibile da parte del gestore del motore di ricerca, poiché egli l'ha ammessa nel suo elenco. A seconda della fattispecie descritta nelle disposizioni della parte speciale del CP, può essere ammessa la punibilità anche di chi ha solo stabilito il collegamento ipertestuale che rimanda a pagine web di terzi (in qualità di autore principale o di complice) [226]. Analogamente, viene presa in considerazione la punibilità del gestore di un motore di ricerca che indicizza automaticamente immagini poi archiviate come file di piccole dimensioni (vedi ad esempio http://images.google.de).

---

[224] In merito alle condizioni di punibilità secondo questa disposizione, vedi numero 9.3.

[225] Quindi non le informazioni a cui i collegamenti ipertestuali rinviano su elaboratori esterni.

[226] Per maggiori approfondimenti in merito, vedasi CHRISTIAN SCHWARZENEGGER/MARCEL ALEXANDER NIGGLI, Über die Strafbarkeit des Hyperlink-Setzers. Zum Urteil des Bezirksgerichts Zürichs vom 10. September 2002. medialex 2003, pag. 27 segg.

Malgrado questa differenza inerente alla funzione dell'hosting provider, una *parità di trattamento sul piano giuridico* si rivela opportuna. Anche il gestore di un motore di ricerca mantiene in funzione un'infrastruttura utile alla collettività. La ricerca e l'indicizzazione del web, analogamente a quanto avviene per l'hosting provider, si svolgono automaticamente. Se la punibilità fosse determinata in base alle regole generali, ci si troverebbe confrontati con i problemi già noti: si potrebbe postulare un obbligo di controllo delle informazioni indicizzate, la cui inosservanza sarebbe punibile in quanto omissione. Ciò impedirebbe in definitiva un'efficace gestione del motore di ricerca.

Con la nuova normativa si intende definire in modo più chiaro i limiti della punibilità del gestore di un motore di ricerca. Se quest'ultimo sa con certezza che il suo elenco elettronico contiene informazioni di rilevanza penale, analogamente a un hosting provider è tenuto a impedirne l'accesso. Se ha ricevuto indicazioni relative all'esistenza di simili informazioni, ha inoltre l'obbligo di trasmetterle all'autorità di perseguimento penale (per i dettagli cfr. il commento al [nuovo] art. 322bis n. 1 CP). Se il gestore del motore di ricerca si attiene a queste direttive, la sua attività non è penalmente perseguibile.

Questa limitazione della punibilità non si applica invece a chi offre liste di collegamenti ipertestuali selezionati e riuniti in modo *non* automatico, come le note directory web di Yahoo o di Google (www.yahoo.com o http://directory.google.com). Il collaboratore di un fornitore di prestazioni che archivia in un elenco contenuti web ben determinati, lo fa intenzionalmente, o almeno con dolo eventuale. Un simile comportamento non deve essere privilegiato. Ciò vale anche per colui che, per mezzo di un collegamento ipertestuale, indirizza consapevolmente l'utente verso informazioni di terzi che realizzano la fattispecie oggettiva di una disposizione penale. Nei due casi occorre applicare le regole generali.

9.25 (Nuovo) articolo 27 numero 4 CP (fornitore di accesso, memorizzazione temporanea di breve durata)

9.251 Motivi di impunità in caso di mera fornitura di accesso in reti di comunicazione elettronica

Come rilevato nel capitolo 6 (vedi n. 6.2 e 6.3 *in fine*), in caso di applicazione delle regole generali del CP non è da escludere che il fornitore di accesso sia considerato complice del fornitore di contenuti nella commissione del reato principale. Lo stesso vale per l'ambito particolare dei reati mediatici, se si considera il fornitore di accesso come una persona responsabile della pubblicazione ai sensi del vigente articolo 27 capoverso 2 CP. Nella dottrina nazionale ed estera prevale a giusto titolo l'opinione secondo cui i processi automatici di trasporto e di fornitura di accesso non sono punibili 227. Ciò si basa su *diverse riflessioni*:

- se si analizza più da vicino il ruolo principale del fornitore di accesso, risulta che la sua attività primaria consiste nell'*assistenza ai propri clienti*, ossia gli utenti. Essi utilizzano i diversi servizi Internet per comunicare o per procurarsi

[227] Vedi art. 12 della direttiva sul commercio elettronico.

informazioni, e a tal fine necessitano di un accesso alla rete. L'aiuto attivamente prestato dal fornitore di accesso nell'allestimento di un temporaneo accesso alla rete non costituisce tuttavia un comportamento penalmente rilevante, poiché l'azione dell'utente è esente da pena. Tale è il caso anche quando l'utente accede a pagine web contenenti informazioni incriminate;

- il fornitore di accesso svolge invece soltanto un ruolo indiretto nella messa a disposizione di informazioni illegali da parte del fornitore di contenuti. Ad esempio, in caso di discriminazione razziale commessa mediante la diffusione di un'affermazione, seguendo il flusso di informazioni il fornitore di accesso *del fornitore di contenuti* e il suo hosting provider vanno considerati i primi soggetti partecipanti. In seguito vi sarebbe il provider di rete, che assicura l'allacciamento a Internet dell'hosting provider. Ulteriori partecipanti sarebbero il gestore dell'instradatore o del gateway, e infine entrerebbero in considerazione i prestatori locali di servizi di rete. Per i diversi tipi di provider cfr. il grafico al n. 2.31.

  Soltanto alla fine di questo lungo percorso va collocata l'assistenza prestata dal fornitore di accesso *dell'utente* alla diffusione delle informazioni del fornitore di contenuti. Prima di considerare la punibilità del fornitore di accesso dell'utente, occorre dimostrare quella dei soggetti che lo precedono nella catena dei partecipanti. La questione non viene tuttavia nemmeno sollevata, poiché la collaborazione di questi partecipanti viene naturalmente vista come *socialmente adeguata*.

- Queste considerazioni presuppongono inoltre che l'atto compiuto dal fornitore di contenuti sia ancora in corso, vale a dire che non sia stato ancora portato a compimento o non sia stato terminato. Si pone qui il problema della durata dei diversi reati d'espressione o di diffusione, poiché è generalmente possibile favorire la commissione dell'atto principale soltanto *prima* del compimento o della conclusione dello stesso. Se si parte dal presupposto, come per i reati di messa in pericolo astratta (cfr. tabella al capitolo 6, n. 6.12), che l'affermazione incriminata è compiuta già nel momento in cui il fornitore di contenuti mette per la prima volta l'informazione a disposizione, ogni ulteriore fornitura di accesso non sarebbe più da considerare come atto di complicità. In simili casi la punibilità del fornitore di accesso sarebbe inconcepibile.

- Poiché la messa a disposizione di informazioni illegali da parte del fornitore di contenuti non è riconducibile a un'azione del fornitore di accesso, l'attribuzione della responsabilità penale dovrebbe essere giustificata dalla mancata adozione di misure tecniche di blocco dell'accesso. Ammettendo l'esistenza di una complicità per omissione, occorrerebbe dimostrare la *posizione di garante* del fornitore di accesso.

  Poiché il comportamento preliminare del fornitore di accesso non è contrario ai suoi obblighi, né tende ad aumentare i rischi, non si può parlare di posizione di garante contro le ingerenze. Non regge nemmeno l'ipotesi della posizione di garante del fornitore di accesso per un controllo delle fonti a rischio, perché altrimenti l'intera infrastruttura Internet andrebbe considerata come un focolaio di pericoli, in relazione ai quali un fornitore di accesso sarebbe ritenuto sempre responsabile.

- Le misure di blocco la cui adozione è spesso richiesta ai fornitori di accesso non hanno in fin dei conti nulla a che vedere con il perseguimento penale. Tali misure fanno parte dell'ambito amministrativo relativo alla prevenzione di minacce (cfr. capitolo 7). Perché la partecipazione alla diffusione sia punibile, occorre dimostrare in ogni singolo caso che una concreta trasmissione di dati è avvenuta direttamente attraverso l'infrastruttura del fornitore di accesso preso in considerazione. Le misure di blocco perseguono tuttavia uno scopo completamente diverso: la prevenzione. I clienti del fornitore di accesso non devono (più) essere in grado di accedere alle informazioni incriminate. In assenza di un contributo tangibile da parte del fornitore di accesso, viene pertanto a mancare la condizione oggettiva perché la partecipazione sia punibile.

- Anche nell'ambito del diritto penale dei media, nella maggior parte dei casi si considera che i fornitori di accesso non facciano parte delle persone responsabili della pubblicazione (cfr. n. 6.2): essi non possono quindi essere resi punibili sulla base dell'articolo 322bis CP.

Questi argomenti si oppongono chiaramente a una responsabilità penale al fornitore di accesso. Ciò corrisponde pure allo standard stabilito nelle legislazioni dell'Unione europea, degli Stati Uniti d'America e di altri Paesi, e rispecchia le raccomandazioni del Comitato dei Ministri del Consiglio d'Europa. In considerazione dell'importanza fondamentale delle reti di comunicazione elettronica nella moderna società dell'informazione, urge disciplinare esplicitamente nel CP l'impunità delle prestazioni automatiche dei fornitori di accesso. Questo è ciò che si prefigge il (nuovo) articolo 27 numero 4 CP.

9.252 In merito alla formulazione del (nuovo) articolo 27 numero 4, 1° periodo CP

Per una *definizione della fornitura di accesso* si rinvia alle considerazioni esposte al n. 2.314. Questa disposizione si applica *esclusivamente* a chi permette l'accesso a Internet. Se un fornitore di accesso partecipa attivamente alla preparazione o messa a disposizione di informazioni illegali, contribuendo alla commissione dei reati del fornitore di contenuti in qualità di coautore, istigatore o complice, o se tali informazioni appartengono al fornitore di accesso, a esso si applica il (nuovo) articolo 27 numero 1 CP (punibilità secondo le regole generali). L'esenzione da pena non dipende quindi da una condizione, ma dalla concreta funzione che assume il fornitore di accesso nel singolo processo comunicativo.

Un'esenzione da pena, così come prevista dal (nuovo) articolo 27 numero 4 CP, è riscontrabile in diverse norme. Talvolta viene utilizzata l'espressione "non punibile" 228, mentre in altri casi si usa la locuzione "esente da pena" 229, che di regola è tuttavia indice di una giustificazione. A titolo di esempio si menzioni l'articolo 32 CP:

---

[228] Ad esempio nell'articolo 100 numero 4 LCStr (viaggi ufficiali urgenti); nell'articolo 53 della legge federale sulla navigazione interna [RS 747.201] (corse di servizio urgenti); nell'articolo 19b LStup (preparazione per il proprio consumo/consegna gratuita per consumo comune, in caso di esigue quantità).

[229] In relazione ai motivi giustificativi (ad esempio nell'art. 33 cpv. 2 2° periodo; nell'art. 34 n. 1 e 2; nell'art. 119, interruzione non punibile della gravidanza; nell'art. 260bis cpv. 2 CP).

"Non costituisce reato l'atto […] che la legge dichiara permesso o non punibile." 230 La formulazione scelta ("non punibile") va preferita, poiché dal profilo della dogmatica penale implica l'esclusione del reato.

9.253 Memorizzazione automatica e transitoria di informazioni di terzi, (nuovo) articolo 27 numero 4, 2° periodo CP

In base a questa disposizione, la memorizzazione automatica, intermedia e transitoria di informazioni di terzi è da considerare come fornitura di accesso ai sensi dell'articolo 27 numero 4, 1° periodo CP, purché avvenga in seguito a un'interrogazione di un utente. A differenza della direttiva UE 231, la regolamentazione proposta non opera alcuna distinzione tra la memorizzazione intermedia che avviene limitatamente a una specifica trasmissione di dati 232 e il cosiddetto *proxy-caching*. Anche quest'ultimo consiste in una memorizzazione intermedia e transitoria da parte del fornitore di accesso, che tuttavia non è funzionale a una singola trasmissione di dati, ma permette a tutti i clienti del fornitore di accesso di richiamare in modo più efficiente i dati relativi ai contenuti web visitati più frequentemente.

I procedimenti controllati da programmi consentono memorizzazioni intermedie su un proxy server del fornitore di accesso dei siti web più visitati dall'utente. Tali informazioni restano temporaneamente a disposizione, ma vengono in seguito cancellate una volta trascorso un certo periodo o se non vengono più richieste. Entrambe le varianti possono essere considerate come memorizzazioni automatiche e transitorie di informazioni di terzi, ma la distinzione tra la memorizzazione intermedia e transitoria e la messa a disposizione di durata più lunga resta compito della giurisprudenza.

Questa *soluzione flessibile* è da preferire a una normativa esplicita: in un ambito in costante evoluzione tecnica, infatti, una delimitazione generale e astratta si rivelerebbe inutile. Nonostante una regolamentazione esplicita, nemmeno in Germania è stato chiarito quanto tempo debba durare una simile memorizzazione intermedia, o quali standard industriali siano riconosciuti e impiegati nel proxy-caching (cfr. art. 10 della legge tedesca sui servizi di telecomunicazione, nuova versione). Inoltre, a causa delle maggiori capacità di trasmissione dati, nel frattempo l'uso di proxy server si è fortemente ridotto.

Il cosiddetto "*mirroring"* non è compreso dalla regolamentazione proposta. L'offerente che replica una determinata offerta Internet su un altro server 233 - al fine di ridurre i tempi di accesso a un server particolarmente lontano o sovraccarico – diventa fornitore di contenuti ai sensi del (nuovo) articolo 27 numero 1 CP. In tali casi la memorizzazione non avviene automaticamente o in seguito alla richiesta di un utente, ma risulta da una *scelta intenzionale*.

---

230 Per il significato, vedasi TRECHSEL (bibl.), art. 33 n. 17: „… è quindi «esente» da pena, ciò che dal profilo processuale equivale a un'*assoluzione,* DTF 73 IV 261, 101 IV 121.“ [trad.]

231 Art. 12 par. 2 e art. 13 della direttiva sul commercio elettronico.

232 Ad esempio la memorizzazione intermedia sul mail server di una e-mail indirizzata a un utente determinato.

233 E quindi per così dire la "rispecchia": da cui l'espressione "mirroring".

Se invece il mirroring avviene automaticamente, chi lo effettua è responsabile secondo il (nuovo) articolo 27 numero 3 CP. Ciò assume particolare importanza nell'ambito dei cosiddetti gruppi di discussione ("newsgroups"), che sono spesso riprodotti automaticamente e integralmente sui server locali.

9.3 Commento al (nuovo) articolo 322bis numero 1

9.31 Capoverso 1

9.311 In generale

Il capoverso 1 disciplina la *punibilità dell'hosting provider*, ossia di chi mette a disposizione dei propri clienti, i fornitori di contenuti, un server Internet sul quale essi possono offrire loro informazioni [234]. Normalmente l'hosting provider non è coinvolto nel processo di telecaricamento delle informazioni nelle pagine web, processo che avviene sul suo server. Si tratta piuttosto di programmi che si svolgono automaticamente, predisposti e controllati unicamente dal fornitore di contenuti.

Sulla base di questi presupposti tecnici la punibilità dell'hosting provider andrebbe valutata secondo le regole generali. Se un fornitore di contenuti offre nelle proprie pagine web materiale di carattere pedopornografico o propone offerte fraudolente, occorre chiedersi se l'hosting provider cooperi in una delle forme di partecipazione previste dal diritto penale. La risposta a questa domanda è per molti aspetti controversa. Occorre innanzitutto chiarire se vi sia un'azione da parte dell'hosting provider. Il contratto che l'hosting provider conclude con il fornitore di contenuti (che potrebbe costituire un comportamento attivo) è una sorta di *atto in bianco* per quel che riguarda le informazioni che il fornitore di contenuti caricherà sul server Internet dell'hosting provider. Esso verte infatti unicamente sull'obbligo di concedere al cliente (il fornitore di contenuti) zona memoria sul server Internet, e sulla creazione dei presupposti che permettono al cliente di telecaricarvi le informazioni da lui scelte e di poterle strutturare secondo i suoi desideri. Il cliente è da parte sua tenuto a versare un compenso. I contenuti non sono oggetto del contratto, con l'eccezione di un'eventuale clausola che vieti il telecaricamento di contenuti illeciti. La conclusione del contratto non può quindi fondare una responsabilità penale.

Una volta che il fornitore di contenuti ha telecaricato le sue informazioni, il *contributo dell'hosting provider* si limita alla gestione del server Internet sul quale ha dato in affitto la zona memoria. Non è chiaro se in tale comportamento sia possibile intravedere un'azione da parte dell'hosting provider [235]. Inoltre la determinazione precisa del contributo al reato da parte dell'hosting provider dipende in modo decisivo da come il reato è descritto nella corrispondente fattispecie legale (che il fornitore di contenuti realizza in qualità di autore). La distinzione tra azione e omissione non è

[234] Nel presente caso e in seguito, per informazioni si intendono i dati richiamabili via Internet. Si tratta prevalentemente di pagine web (tra cui anche dati che possono essere richiamati mediante altri servizi Internet, come ad esempio l'FTP).

[235] Cfr. le spiegazioni al n. 6.3.

chiara in particolare per comportamenti quali il "lasciare accessibile" e il "rendere accessibile" (art. 135, 197 n. 3 CP). Anche quando, nel singolo caso, si può presumere un comportamento attivo, occorre valutare se il contributo è stato fornito in qualità di autore o di complice.

Anche su questo punto le conclusioni sono poco chiare, tanto più che si pone pure il problema della cosiddetta *complicità derivante dagli atti usuali*: per gli atti menzionati non si applica più la distinzione tradizionale tra commissione da parte di un autore e commissione da parte di un complice, e si considera unicamente la prima di queste due modalità di commissione. Pertanto una responsabilità per correità potrebbe sostanzialmente essere ammessa, anche se in definitiva ciò appare poco opportuno.

A ciò si aggiunge il fatto che, considerando l'hosting provider autore, diviene superfluo chiedersi se (anche) la prestazione di servizi usuali, nella misura in cui favoriscano la commissione intenzionale del reato, possa essere resa punibile in quanto complicità. Finora il Tribunale federale ha risposto affermativamente a questa domanda, affrontando tuttavia la questione soltanto caso per caso e non in generale, e quindi non in modo definitivo [236]. Se si considerasse il contributo dell'hosting provider come quello di un autore, la questione non si porrebbe più. Ciò condurrebbe a un risultato chiaro che non risolverebbe però il problema di fondo: una tale soluzione non può quindi essere presa in considerazione. Se invece la prestazione dell'hosting provider venisse considerata un atto di complicità, si porrebbe la questione di non facile risoluzione della complicità derivante dagli atti usuali (cfr. in proposito n. 6.3).

Se un comportamento attivo non entra in considerazione, ci si deve chiedere se l'hosting provider possa essere eventualmente punito per omissione. Anche in questo caso non esiste una soluzione chiara e ragionevole. Secondo la giurisprudenza e la dottrina, una *posizione di garante* può derivare da un precedente atto di messa in pericolo (ingerenza). Chi, attraverso il suo agire, mette in modo prevedibile in pericolo beni giuridici altrui, è tenuto a fare tutto il possibile affinché tale pericolo non si realizzi in una lesione corrispondente. L'azione dell'hosting provider consiste nella messa a disposizione di zona memoria a chi vi è interessato. Si tratta di un atto del tutto ordinario e in sé lecito, che non crea alcun pericolo particolare.

Il pericolo e il reato risultano unicamente dall'*impiego abusivo di questa zona memoria* fatto da un terzo (il fornitore di contenuti), il quale commette un reato immettendo intenzionalmente in rete informazioni dal contenuto illegale. Con tale agire il fornitore di contenuti viola anche il contratto concluso con l'hosting provider, contratto le cui condizioni generali di regola vietano l'offerta di informazioni aventi rilevanza penale.

Una chiarificazione delle questioni in sospeso da parte del Tribunale federale potrebbe essere d'aiuto. Perché tutti gli aspetti più importanti possano essere analizzati dalla massima istanza giudiziaria federale occorrerebbero però molti anni. Inoltre non vi è alcuna garanzia che il Tribunale federale si occuperà effettivamente di tali questioni. Una chiarificazione dipende quindi piuttosto dalla prassi delle autorità di perseguimento penale (promozione dell'accusa), prassi che tuttavia non è

[236] Cfr. n. 6.3.

prevedibile. Un'ulteriore elemento d'imponderabilità è dato dal modo in cui le parti reagiscono nei confronti delle decisioni di prima e seconda istanza (inoltro di ricorsi).

Per tali motivi la commissione peritale ha deciso di non affidare alla prassi il compito di definire in che misura un hosting provider debba essere reso punibile, ma bensì di *disciplinare* tale punibilità *nella legge*, *in deroga alle regole generali sull'autore del reato e sulla complicità*. Si presenta quindi un parallelismo con il vigente diritto penale dei media, che già prevede modifiche di tali regole generali (cfr. art. 27 cpv. 2, 322bis CP). In un ambito settoriale si pongono infatti problemi identici: le versioni on line dei media stampati vanno in pratica sottoposte allo stesso regime al quale già sottostanno gli altri media stampati; ciò vale in ogni caso per l'autore e il redattore. Per il resto occorre prestare attenzione al fatto che questo parallelismo ha dei limiti. La norma proposta, per molti aspetti, non può essere considerata una copia speculare dell'articolo 322bis CP nelle reti di comunicazione elettronica; la norma proposta, infatti,

- ha un *significato più ampio*, non essendo applicabile unicamente ai reati mediatici ai sensi della giurisprudenza del Tribunale federale relativa all'articolo 27 CP. Si applica anche ai reati d'espressione che il Tribunale federale rifiuta di qualificare come reati mediatici, come ad esempio gli articoli 135, 197 numeri 2 e 3 o 261bis capoverso 4 CP. Va in seguito ampiamente oltre il campo d'applicazione dei reati che vengono considerati mediatici: a ogni reato commesso mediante reti di comunicazione elettronica si applica innanzitutto il (nuovo) articolo 27 CP, e pertanto anche il (nuovo) articolo 322bis numero 1 CP.

- Nel diritto penale dei media la responsabilità penale del redattore o della persona responsabile della pubblicazione presuppone che l'autore non possa essere individuato o non possa essere tradotto davanti a un tribunale svizzero. Questa esclusione della punibilità non vale per i reati commessi in reti di comunicazione elettronica: anche se l'autore e/o il fornitore di contenuti possono essere individuati o tradotti davanti a un tribunale svizzero, *l'hosting provider resta punibile secondo il (nuovo) articolo 322bis numero 1 CP*.

- Nelle reti di comunicazione elettronica il *ruolo del redattore responsabile*, come quello previsto dagli articoli 27 capoverso 2 CP e 322 capoverso 2 CP, non è lo stesso. Laddove tale ruolo è previsto, la punibilità del redattore responsabile (e dell'autore) si fonda sul diritto penale dei media ([nuovo] art. 27 n. 2 CP).

- La *commissione per negligenza non* è passibile di pena.

9.312 Particolarità

9.312.1 Sistematica

Secondo il nuovo approccio, la nozione di reti di comunicazione elettronica, nella misura in cui sia rilevante nel presente contesto, *ha un significato più ampio rispetto a quello dei media*. La normativa sui reati nelle reti di comunicazione elettronica viene quindi inserita negli articoli 27 e seguenti CP, all'inizio della normativa ([nuovo] art. 27 CP); la "vecchia" norma sul diritto penale dei media si trova ora nel (nuovo)

articolo 27bis CP. La stessa trasposizione avviene nella disposizione penale annessa, l'articolo 322bis CP: la mancata opposizione a una pubblicazione punibile, originariamente prevista dall'unico capoverso di questa norma, diventa il numero 2 di quella nuova. Il nuovo numero 1 disciplina la mancata opposizione all'utilizzo di informazioni "punibili" di terzi in reti di comunicazione elettronica.

9.312.2 Rapporto con la punibilità del fornitore di contenuti

Il fornitore di contenuti, nella misura in cui concepisce i dati che vengono poi pubblicati nel server Internet del suo hosting provider (testi, immagini, ecc), svolge un'attività che corrisponde in parte a quella dell'*autore* nel diritto penale dei media. Partendo da tale presupposto, la punibilità del fornitore di contenuti è retta dal diritto penale dei media del (nuovo) articolo 27 numero 2 CP; ciò significa che si applicano le regole esclusive di tale disposizione, che valgono tuttavia soltanto per l'autore (e per il redattore), secondo quanto espressamente disposto dal (nuovo) articolo 27 numero 2 CP.

Se il fornitore di contenuti non è autore, poiché si limita a riprendere immagini altrui (appropriandosene), o se è autore, ma se il reato in questione non è mediatico ai sensi del vigente articolo 27 capoverso 1 CP, si applicano le regole generali del (nuovo) articolo 27 numero 1 CP. Per l'hosting provider la situazione non muta: anche in questo caso la sua responsabilità si fonda sul (nuovo) articolo 322bis numero 1 CP.

Nell'ambito delle reti di comunicazione elettronica, la responsabilità penale dell'hosting provider non dipende quindi dall’assenza di un responsabile primario. Questo perché vi sono differenze tra una persona responsabile della pubblicazione e un hosting provider: a differenza di quest'ultimo, la persona responsabile della pubblicazione ha comunque una relazione con i contenuti pubblicati, avendo l'obbligo di controllarli e se del caso di intervenire [237]. Il telecaricamento delle informazioni da parte del fornitore di contenuti avviene automaticamente, e il suo hosting provider non ha alcuna conoscenza di tali dati. Inoltre il disciplinamento della responsabilità nel diritto penale dei media si ispira al caso normale dell'impresa in seno alla quale, in mancanza di un autore o redattore responsabili, viene chiamata a rispondere la persona responsabile della pubblicazione. Anche questa condizione, per quel che riguarda il fornitore di contenuti e l'hosting provider, non è realizzata.

Per quel che riguarda l'hosting provider, da un lato la regolamentazione leggermente modificata rispetto al diritto penale dei media comporta un *inasprimento*. La punibilità di un autore o di un redattore non implica infatti necessariamente l'impunità dell'hosting provider. D'altro lato la nuova disposizione è anche meno severa, poiché gli hosting provider non rispondono più per negligenza come previsto dall’art. 322bis 2° periodo CP.

[237] DTF 128 IV 53, 67 cons. 5c; ZELLER (bibl.), n. 55.

9.312.3 Autori del reato

Il (nuovo) articolo 322bis numero 1 CP costituisce un *vero e proprio reato speciale*: può essere autore soltanto chi tiene automaticamente a disposizione informazioni di terzi in una rete di comunicazione elettronica; chi non compie tale azione è fin da principio escluso dalla cerchia dei possibili autori. Tale limitazione concerne gli hosting provider sui cui server web i clienti (fornitori di contenuti) telecaricano informazioni, sulle quali gli hosting provider non possono più influire. Questo processo si svolge automaticamente e dipende sotto ogni punto di vista (forma e contenuto dell'informazione, modifica o cancellazione dei dati, momento del telecaricamento) soltanto dal fornitore di contenuti. Si deve trattare di informazioni *di terzi*, riconducibili quindi per forma e contenuto soltanto a chi le ha raccolte. Se l'hosting provider esercita un'influenza diretta sui contenuti, si appropria di tali informazioni. La conseguenza è che all'hosting provider in tal caso non si applica più il (nuovo) articolo 322bis numero 1 CP, ma la nuova norma del (nuovo) articolo 27 numero 1 CP.

Per chiarire immediatamente chi può essere autore del reato, i relativi presupposti (il fatto di mettere a disposizione informazioni in una rete di comunicazione elettronica) sono collocati all'inizio della disposizione. Affinché il tenore della norma fondamentale, ossia il (nuovo) articolo 27 numero 3 CP, e quello del (nuovo) articolo 322bis numero 1 CP (al quale il [nuovo] art. 27 rinvia) prevedano le stesse fattispecie, viene inserita anche in questo caso l'espressione "automaticamente".

Se l'hosting provider è organizzato come *persona giuridica*, le circostanze particolari riguardano unicamente la persona giuridica in quanto tale, e non le persone fisiche che agiscono in suo nome. Perché gli obblighi spettanti alla persona giuridica e che ne fondano la punibilità possano essere trasferiti alle persone fisiche che la rappresentano, occorre una regolamentazione legale specifica, come quella prevista dal vigente CP (soltanto) per i reati del 2° titolo (reati contro il patrimonio; art. 172 CP). In considerazione della norma sui rapporti di rappresentanza prevista dalla nuova parte generale del CP, il cui nuovo articolo 29 è applicabile a ogni reato, la commissione peritale ha nel frattempo deciso di rinunciare alla creazione di una disposizione particolare. Se l'entrata in vigore della nuova parte generale dovesse essere ritardata, questa decisione andrebbe riconsiderata.

9.312.4 Fattispecie di reato

Il (nuovo) articolo 322bis numero 1 CP sancisce una punibilità derivante da un'*inazione*: all'hosting provider viene rimproverato di non essere intervenuto per impedire l'utilizzo di un'informazione che presenta ad esempio contenuti a sfondo razzista o che esaltano l'uso della violenza. Tale intervento avrebbe dovuto consistere nel *blocco* della pagina web (è invece fuori questione un'ingiunzione fatta al fornitore di contenuti e volta all'eliminazione immediata delle informazioni, poiché potrebbe trattarsi di un atto di favoreggiamento [art. 305 CP]). Il testo della disposizione prevede espressamente che l'intervento debba essere *tecnicamente possibile* e *ragionevolmente esigibile* dall'hosting provider, una condizione naturale

dei reati d'omissione [238], che per chiarezza viene tuttavia ribadita nella presente norma.

9.312.5 Oggetto dell'omissione

L'omissione non consiste nell'impedimento di un reato in quanto tale. Una volta che il fornitore di contenuti ha telecaricato informazioni di rilevanza penale, la sua azione non viene resa nulla dal blocco dell'accesso ai dati effettuato dall'hosting provider. Il discorso è comunque diverso per i reati d'espressione, il cui carattere illegale risiede nell'esternazione in quanto tale; cfr. gli esempi menzionati relativi agli articoli 135 o 261, ma anche 173 e seguenti, 197 o 259 CP (pubblica istigazione a un crimine o alla violenza). Lo stesso vale per altri reati, con la differenza che in tali casi il blocco dell'accesso potrebbe impedire il compimento del reato (vi sarebbe soltanto un tentativo), ad esempio in caso di blocco dell'accesso a una pagina i cui contenuti hanno un carattere ingannevole.

Il carattere illegale dell'atto compiuto dal fornitore di contenuti permane, ma gli *effetti* del reato possono essere limitati mediante un blocco che impedisca agli utenti di Internet di accedere ai dati. Poco importa se gli utenti, da parte loro, si rendono punibili perché hanno fatto uso delle informazioni (di regola il semplice fatto di accedere alle informazioni non li rende ancora punibili, ad eccezione del caso in cui vi sia una successiva memorizzazione delle pagine, cfr. articolo 197 numero 3bis CP).

In tal modo è pure realizzato *l'obiettivo politico-giuridico* volto a coinvolgere gli hosting provider nella lotta contro i contenuti illegali su Internet. Non si può esigere dagli hosting provider che impediscano ai loro clienti (i fornitori di contenuti) di commettere reati attraverso la pubblicazione di informazioni sul server Internet: gli hosting provider non hanno infatti alcun influsso sul processo di telecaricamento dei contenuti. È invece possibile esortare gli hosting provider, e in questo consiste appunto il vero obiettivo legislativo, *a limitare gli effetti di tali reati*, rendendo impossibile la presa di conoscenza dei relativi contenuti.

Vi è un cambiamento di orientamento rispetto alla variante che prevede che l'hosting provider debba essere reso responsabile per aver partecipato all'atto commesso dal fornitore di contenuti. In base alle regole generali concernenti l'autore del reato e la partecipazione, nel caso dell'hosting provider si tratta sempre di stabilire se e come esso sia coinvolto nel reato commesso dal fornitore di contenuti. *Nella misura in cui* l'hosting provider si rende punibile, la sua punibilità deriva dal carattere illegale dell'atto commesso dal fornitore di contenuti. La norma proposta implica un trasferimento del carattere illecito: il nucleo essenziale dell'illiceità non risiede nella partecipazione al reato principale, nemmeno per un'eventuale omissione, ma bensì nell'inattività dimostrata di fronte all'uso dei contenuti da parte di terzi. Alla luce del carattere illecito del reato principale commesso dal fornitore di contenuti, tale regolamentazione si rivela giustificata. Il carattere illecito si concretizza nel momento in cui terzi prendono conoscenza di tali contenuti, leggendo ad esempio asserzioni a sfondo razzista o visionando rappresentazioni di cruda violenza. In questo senso la soluzione proposta mantiene intatto il legame con il reato principale.

---

[238] Cfr. KURT SEELMANN, in Niggli/Wiprächtiger, Basler Kommentar, n. 62, 92 in merito all'art. 1; GÜNTER STRATENWERTH, Schweizerisches Strafrecht, Allgemeiner Teil I, 2^{a} ed., Berna 1996, § 14 n. 37.

La nuova disposizione realizza quindi due obiettivi: smorza il dibattito relativo alla delimitazione del coinvolgimento dell'hosting provider e toglie alla questione la sua rilevanza pratica, permettendo inoltre di arginare gli effetti del reato principale (cfr. gli esempi menzionati) sugli utenti che visionano i contenuti incriminati.

Le modifiche riguardo al carattere illecito si fondano pertanto su *due motivi principali*: l'impossibilità di impedire che il fornitore di contenuti commetta reati su Internet, nonché la possibilità, mediante disposizioni penali, di impedire l'utilizzo di informazioni da parte di terzi.

A ciò si aggiungono, quale *terzo motivo importante*, le norme concernenti l'applicazione della legge penale (art. 3 segg. CP). In base a tali norme, il fornitore di contenuti commette il reato nel luogo in cui impartisce l'ordine di telecaricamento, per mezzo del quale i dati incriminati sono automaticamente trasferiti sul server dell'hosting provider. Se l'ordine di telecaricamento è avvenuto all'estero, secondo la giurisprudenza del Tribunale federale chi ha partecipato al reato sfugge alla sovranità penale svizzera: è il caso dell'hosting provider (il fornitore di contenuti che agisce all'estero in quanto autore sfugge comunque alla sovranità penale svizzera: cfr. n. 6.43). Questo problema può essere aggirato con la soluzione proposta, che prevede una responsabilità per omissione dell'hosting provider, purché la sua sede si trovi in Svizzera (se ciò non è il caso, sempre secondo la normativa proposta, non vi è sovranità penale svizzera).

9.312.6 Presupposto dell'obbligo di intervenire

È necessario che, per mezzo delle informazioni di terzi, venga commesso un reato. Questo reato, commesso dal fornitore di contenuti, può assumere tipologie molto diverse. È possibile distinguere *due gruppi*.

Da un lato entrano in considerazione i reati che hanno indotto l'opinione pubblica a chiedere un inasprimento della repressione penale della criminalità in rete, quali la rappresentazione di atti di cruda violenza (art. 135 CP), la pornografia (art. 197 CP) o la discriminazione razziale (art. 261bis CP).

Dall'altro fanno parte del gruppo di atti punibili anche tutti i reati per la cui commissione è ipotizzabile l'impiego di mezzi di comunicazione elettronica, come nel caso delle indicazioni ingannevoli per una truffa, o delle gravi minacce per un'estorsione, oppure l'offerta o la messa in circolazione di esemplari di un'opera (art. 67 cpv. 1 lett. f LDA) o di un esemplare riprodotto di un supporto audio (art. 69 cpv. 1 lett. f LDA).

Le *informazioni di terzi* devono costituire *il mezzo* ("per mezzo di") *con il quale il reato viene commesso*. Il reato non deve per forza consumarsi per effetto della pubblicazione, ma può richiedere la realizzazione di altri aspetti della fattispecie legale, come ad esempio il pregiudizio patrimoniale nel caso di una truffa. Ciò significa che il reato, così come presupposto dal (nuovo) articolo 322bis numero 1 CP, non deve essere consumato nel momento in cui l'hosting provider è tenuto a intervenire, ma che un tentativo è sufficiente.

Le informazioni devono inoltre rivestire già un carattere illecito di rilevanza penale. In caso contrario, ossia se ad esempio fungono soltanto da preparativi in vista di una truffa, l'hosting provider non è tenuto a intervenire. L'obbligo di intervenire nasce infatti soltanto quando il carattere penalmente rilevante è collegato all'uso di un server Internet, poiché la regolamentazione si fonda specificatamente sull'aspetto legato alla partecipazione a reati commessi in Internet. Se il reato non è (ancora) stato commesso, la fattispecie del (nuovo) articolo 322bis capoverso 1 CP non è realizzata (di conseguenza, conformemente al capoverso 2 della nuova disposizione, le indicazioni riguardanti atti non punibili non devono essere trasmesse alle autorità di perseguimento penale).

La nuova disposizione concerne unicamente le informazioni *di terzi*, poiché è unicamente in questo caso che nasce la situazione specifica che giustifica una regolamentazione speciale applicabile all'hosting provider. Soltanto se questi non ha nulla a che vedere con il contenuto delle informazioni, se queste gli sono quindi estranee, nascono le difficoltà descritte sopra per quel che concerne l'adeguata repressione penale della sua partecipazione al reato principale. Se invece le informazioni appartengono all'hosting provider, in quest'ottica esso non è più hosting, ma *content* provider, e soggiace pertanto al (nuovo) articolo 27 numero 1 CP.

Con l'espressione *reato* si intende definire (unicamente) la realizzazione dell'illecito penalmente rilevante, ossia una violazione del diritto conforme alla fattispecie. Non ha importanza se l'autore (il fornitore di contenuti) agisce in modo colpevole. Ciò risulta da una considerazione di ordine pratico: non è possibile dedurre dall'informazione la sua provenienza da un autore (non) responsabile. Inoltre, anche considerando l'hosting provider partecipante, il fatto che agisca in modo colpevole o no non sarebbe determinante (accessorietà limitata). In terzo luogo, la preoccupazione di fare il possibile per impedire che l'utente venga a conoscenza dell'informazione incriminata prescinde dall'imputabilità dell'hosting provider.

9.312.7 Elemento soggettivo

L'elemento soggettivo della nuova disposizione esige innanzitutto l'*intenzionalità*, ai sensi dell'articolo 18 capoverso 2 CP, riguardo a ogni circostanza di fatto oggettiva; è di principio ammesso anche il dolo eventuale. Per quel che concerne il (nuovo) articolo 322bis numero 1 capoverso 1 CP ne conseguono *due difficoltà*:

- secondo l'interpretazione data dalla prassi, le conseguenze del comportamento di chi agisce con dolo eventuale risultano talmente probabili, che il comportamento può essere ragionevolmente interpretato unicamente come il fatto di aver accettato il prodursi di tale esito [239]. Comunque si interpreti questa formulazione, essa potrebbe avere come conseguenza che, sulla base del dolo eventuale, venga imposto un obbligo di controllo agli hosting provider.

  Se all'hosting provider viene segnalata la presenza sul suo server Internet di un'informazione dal presunto contenuto penalmente rilevante e se tale avvertimento viene ignorato, nel procedimento penale che ne consegue si pone allora la questione relativa alla sua intenzionalità (i reati più significativi possono

[239] DTF 109 IV 140.

essere commessi soltanto intenzionalmente), a condizione che si tratti oggettivamente ed effettivamente di un reato. A seconda della credibilità di chi ha fornito la segnalazione (poi rivelatasi fondata) e dall'insistenza con cui è stata ripetuta, nel singolo caso la sola conclusione possibile è che il comportamento dell'hosting provider può soltanto essere interpretato come l'accettazione del fatto che venga commesso un reato mediante informazioni di terzi telecaricate sul suo server Internet. Per sottrarsi al dolo eventuale, l'hosting provider dovrebbe quindi in tutti i casi dar seguito a ogni segnalazione credibile e insistente; ciò equivarrebbe all'imposizione di un obbligo positivo di controllo.

Non si tratta qui di esentare gli hosting provider da una pena che si meriterebbero e di privilegiarli quindi in modo ingiustificato. Ma occorre prestare attenzione alle *conseguenze* che una simile normativa comporterebbe, ossia l'istituzione di un sistema di controllo che permetta di dar seguito alle segnalazioni. Ciò non basterebbe ancora a giustificare la regolamentazione proposta.

Se però si considera che la credibilità di chi fornisce un'indicazione non può quasi mai essere dedotta dall'indicazione stessa, e che la veridicità di una segnalazione non dipende dall'ostinazione con la quale essa viene ripetuta, risulta evidente che, accontentandosi del dolo eventuale, il sistema produce risultati sconcertanti. In tal caso, infatti, l'hosting provider dovrebbe in pratica dar seguito a *ogni* segnalazione. Tenuto conto delle svariate modalità con cui è possibile utilizzare in modo legale Internet, in presenza di un elevato numero di segnalazioni si renderebbe necessaria una quantità sproporzionata di risorse.

Oltre a ciò vi è il rischio che le segnalazioni vengano utilizzate come mezzo per sottoporre al giudice penale semplici contenziosi di diritto privato, tipici ad esempio in caso di violazioni della LDA. Per mezzo di segnalazioni usate a tal fine l'hosting provider sarebbe tenuto a impedire l'utilizzo di informazioni da esso ospitate e dal presunto contenuto contrario alla LDA (senza che ciò sia però stato constatato da un'autorità giudiziaria). Queste considerazioni avrebbero ancor più rilevanza in caso di ammissione del dolo eventuale non soltanto in presenza di segnalazioni all'hosting provider, ma già a causa del fatto, generalmente riconosciuto, che le prestazioni dell'hosting provider sono anche oggetto di abusi in vista della commissione di reati. A queste condizioni, per non rendersi punibile, l'hosting provider dovrebbe procedere a un controllo preventivo dei contenuti telecaricati dai suoi clienti [240].

- La *seconda difficoltà* risiede nella natura di alcune fattispecie legali che si realizzano frequentemente nel contesto delle reti di comunicazione elettronica. La fattispecie della rappresentazione di atti di cruda violenza (art. 135 CP), della pornografia (art. 197 CP) o della discriminazione razziale (art. 261bis CP) includono aspetti normativi. Per comprenderli non basta una sensibilità generale e ordinaria, ma occorre un processo di valutazione.

  Spesso per l'osservatore non è semplice determinare in cosa consiste un atto di "cruda" violenza, o stabilire se la rappresentazione di tale atto ha "un valore culturale o scientifico degno di protezione" (art. 135 CP). Non è facile nemmeno

[240] Cfr. NIGGLI/RIKLIN/STRATENWERTH, Die strafrechtliche Verantwortlichkeit von Internet-Providern, medialex, edizione speciale 1/2000, in particolare pag. 31 seg.

definire in cosa consistono gli scritti "pornografici" ai sensi dell'articolo 197 CP, o determinare se un'ideologia viene "sistematicamente" discreditata, oppure ancora valutare se una persona viene denigrata "in modo lesivo della dignità umana" a causa della sua religione (art. 261bis CP).

L'hosting provider prudente non attenderebbe tuttavia che un'autorità giudiziaria attesti il carattere "crudo" di un atto di violenza, ma bloccherebbe l'accesso ai dati già quando tale caratteristica non possa essere esclusa con sicurezza. Ciò conduce a una forma di censura privata che non può confarsi a una società democratica.

Per questi motivi il progetto propone che la punibilità dell'hosting provider sia limitata ai casi in cui esso *è certo della punibilità* dei dati contestati; tutti gli altri casi di azione intenzionale non configurano invece la fattispecie legale. L'effetto principale di questa limitazione è che la punibilità non può fondarsi sul dolo eventuale. Sul piano della consapevolezza l'autore ritiene semplicemente possibile, ma non sa con certezza, che il contenuto dei dati in questione realizza una determinata fattispecie penale. In relazione a questa limitazione, non ha alcuna rilevanza pratica l'esclusione della cosiddetta "intenzione eventuale" (una variante dell'intenzionalità diretta), la cui caratteristica consiste nel fatto che l'autore aspira sì alla realizzazione del carattere illecito della fattispecie penale, ma non è sicuro che ciò avvenga (lo ritiene unicamente possibile) [241].

La consapevolezza del carattere punibile dell'atto in questione non risulta di norma dalla semplice segnalazione che un file determinato contiene informazioni di carattere penalmente rilevante. Può invece risultare dal fatto che all'hosting provider non sia stata trasmessa una segnalazione relativa a un dato, ma il contenuto del dato stesso [242]. Se la discriminazione razziale contenuta nell'informazione è lampante, risulta evidente che l'hosting provider ha acquisito la consapevolezza del carattere punibile dell'atto in questione, condizione necessaria per poterlo considerare punibile ai sensi dell'articolo 322bis numero 1 capoverso 1 CP (anche se dall'evidenza della punibilità non si può in sé dedurre la consapevolezza dell'hosting provider).

Una *minoranza della commissione peritale* voleva subordinare l'acquisizione della consapevolezza alla condizione che l'hosting provider ricevesse la segnalazione da una *fonte attendibile* (ad esempio da un'autorità di perseguimento penale). Le segnalazioni provenienti da persone qualsiasi non sarebbero state in tal caso sufficienti. Questa limitazione supplementare era motivata dal fatto che occorreva evitare di costringere l'hosting provider a valutare da solo il carattere illecito di un contenuto. Nell'ambito della libera comunicazione i casi limite sono infatti all'ordine del giorno e l'hosting provider, al momento della valutazione, non può sapere se un tribunale riterrà in seguito evidente il carattere illecito del dato. Una caratteristica può risultare o non risultare evidente a seconda di chi la osserva. Per timore di rendersi

[241] Cfr. TRECHSEL/NOLL (bibl.), pag. 98.

[242] Va lasciata aperta la questione relativa alla misura in cui si rende punibile colui che invia all'hosting provider il contenuto dei dati al fine di renderlo attento (ad esempio il fatto di lasciare o rendere accessibile pornografia dura, art. 197 n. 3 CP). In un caso analogo, il Tribunale federale ha riconosciuto non punibile, pur se obiettivamente illecito, il trasporto di stupefacenti con il proposito di distruggerli, laddove l'agente assuma un rischio ammissibile (art. 19 n. 1 cpv. 3 LStup; DTF 117 IV 58).

punibile, un hosting provider prudente in caso di dubbio procederebbe al blocco dei file in questione. Vi sarebbe quindi il notevole rischio che gli hosting provider blocchino anche contenuti legali. Ciò sarebbe in contraddizione con il principio fondamentale della libera comunicazione in una società democratica. Inoltre esporrebbe l'hosting provider al rischio di essere oggetto di un'azione di diritto civile intentata dal fornitore di contenuti, qualora il blocco dovesse in seguito rivelarsi superfluo.

La *maggioranza della commissione* non condivide questa posizione. Si è espressa *contro un ulteriore ridimensionamento della punibilità*, e questo per i motivi seguenti.

In primo luogo, l'esigenza della consapevolezza del carattere punibile dell'atto riduce già la responsabilità dell'hosting provider rispetto al caso normale del dolo eventuale. *In secondo luogo*, se la punibilità del contenuto di una rappresentazione appare oggettivamente dubbia, essa lo è di regola anche per l'hosting provider. In questo caso l'hosting provider può considerare il carattere punibile dell'atto come possibile ma non inequivocabile, come esige il capoverso 1 ("sapendo con certezza"); se i casi dubbi diventassero la norma, la condizione della consapevolezza consentirebbe all'hosting provider di non trovarsi confrontato con tale situazione.

In terzo luogo, la maggioranza della commissione non ha reputato opportuno subordinare la consapevolezza al presupposto che la segnalazione provenga da una fonte attendibile, ad esempio da un'autorità di perseguimento penale. Questo perché, da un lato, anche una segnalazione proveniente da una tale autorità potrebbe essere infondata, e in tal caso non sarebbe soddisfatta la condizione oggettiva del "reato" (il che esclude fin dall'inizio una responsabilità per l'atto compiuto). Se l'hosting provider lo nota, non può (a ragione) avere alcuna consapevolezza della punibilità. D'altro lato vi può essere consapevolezza anche quando la segnalazione proviene da un privato. Se si intende considerare la provenienza da una fonte attendibile soltanto come condizione necessaria, ma non sufficiente, per l'acquisizione della consapevolezza [243], resta quindi da chiarire quali altri requisiti devono essere soddisfatti.

In quarto luogo, è evidente che la nozione di "segnalazione proveniente da una fonte attendibile" mal si adatta al requisito della consapevolezza. Tale nozione non poggia infatti sulla qualità della consapevolezza dell'hosting provider, ma sulla *fonte* dalla quale la segnalazione proviene: deve trattarsi di una fonte attendibile, come ad esempio un'autorità di perseguimento penale, e non di una persona privata. Tuttavia, a ben guardare, non si tratterebbe di una semplice *segnalazione* dell'autorità, ma di un suo *ordine*.

La proposta della minoranza della commissione comporterebbe quindi la punibilità dell'hosting provider che non ottemperasse a un ordine di blocco impartito dall'autorità di perseguimento penale. Ciò significherebbe in pratica lo stralcio del (nuovo) articolo 322bis numero 1 capoverso 1 CP. L'inosservanza di un ordine impartito da un'autorità è infatti già punibile secondo il diritto vigente, alle condizioni poste dall'articolo 292 CP.

[243] Questo partendo dalla considerazione che l'autorità di perseguimento penale, in base al suo mandato, deve situarsi in una prospettiva d'incriminazione, ciò che tendenzialmente comporta una limitazione della libertà di comunicazione.

Per questi motivi la *maggioranza della commissione* ritiene opportuna la regolamentazione proposta, e reputa che si possa senz'altro pretendere dall'hosting provider che *si assuma*, nella misura descritta, *le proprie responsabilità*.

La consapevolezza si limita unicamente alla punibilità dell'atto in questione, elemento oggettivo della fattispecie penale (il "reato"). Nella lingua tedesca, in altre disposizioni del CP tale limitazione è formulata con l'espressione "wider besseres Wissen" (letteralmente: "in malafede"), tradotta in italiano, a seconda delle fattispecie, con "*cosciente*" (della gratuità di un falso allarme: art. 128bis CP), "sapendo" (di dire cosa non vera: art. 174 CP) o "sa" (innocente: art. 303 CP) [244]. Viene utilizzata anche l'espressione "scientemente" [245]. Secondo il (nuovo) articolo 322bis CP, l'hosting provider deve avere la consapevolezza del carattere punibile dell'atto compiuto per mezzo delle informazioni da lui tenute a disposizione.

Non viene introdotta una responsabilità per negligenza. Essa sarebbe in contrasto con i fondamenti su cui si basa la nuova regolamentazione, che è stata concepita facendo astrazione dal problema, difficile da risolvere sul piano teorico, relativo alla forma di partecipazione dell'hosting provider al reato commesso dal fornitore di contenuti. In pratica entrano in considerazione soltanto reati intenzionali. È stato inoltre esposto per quali ragioni non può essere ritenuto sufficiente un dolo eventuale dell'hosting provider in relazione all'atto contestato. Una responsabilità per negligenza sarebbe in contraddizione con tale impostazione.

In definitiva la differenza si basa sul diverso grado di partecipazione automatizzata: di norma un redattore ha l'informazione (punibile) di fronte a sé e la conosce, o perlomeno dovrebbe conoscerla. Nel caso dell'hosting provider, nessuno dei due presupposti è soddisfatto: da un lato, infatti, tale provider non si trova l'informazione di fronte, e dall'altro non può esserne ancora a conoscenza al momento del suo telecaricamento, ma soltanto quando viene reso attento della sua esistenza.

9.312.8 Pena

La nuova disposizione commina la detenzione o la multa, in sintonia dunque con il vigente articolo 322bis CP. Poiché la partecipazione al reato del fornitore di contenuti costituisce lo sfondo del (nuovo) articolo 322bis numero 1 capoverso 1 CP, occorre assicurarsi che le pene comminate nei due casi non divergano eccessivamente. Se si considerano i reati in relazione ai quali il mancato intervento dell'hosting provider può essere punibile, si nota che la corrispondenza è sempre mantenuta; in particolare, anche gli articoli 135, 197 e 261bis CP prevedono la detenzione o la multa.

Soltanto in *casi eccezionali*, che complessivamente non assumono particolare rilevanza, il limite superiore astratto della pena comminata al reato del fornitore di contenuti è più elevato, come ad esempio all'articolo 273 CP (casi gravi di spionaggio

[244] [N.d.T.: La scelta operata tra "wider besseres Wissen" e "wie er sicher weiss", con la preferenza data dalla commissione alla seconda espressione, riguarda unicamente la versione tedesca. In italiano, nelle disposizioni del CP citate e nel (nuovo) articolo 322bis, viene utilizzata sempre una forma coniugata del verbo sapere].

[245] Soprattutto in materia di reati di messa in pericolo, cfr. art. 221 cpv. 2, 223 n. 1 cpv. 1, 227 n. 1 cpv. 1, 228 n. 1 cpv. 4, 230 n. 1 cpv. 3, 237 n. 1, 238 cpv. 1 CP.

economico), mentre gli articoli 258 CP (pubblica intimidazione) e 259 CP (pubblica istigazione a un crimine o alla violenza) prevedono come limite superiore tre anni di reclusione invece di tre anni di detenzione (differenza che scomparirà con la revisione del Codice penale; cfr. l'art. 10 del nuovo Codice).

La pena meno grave comminata dal (nuovo) articolo 322bis capoverso 1 CP è la multa: si tratta quindi di un limite inferiore più basso rispetto a quello previsto per il reato del fornitore di contenuti, che è la detenzione. La differenza è opportuna, poiché in pratica si tratta di una forma di complicità dell'hosting provider, e in questo caso l'articolo 25 CP, in combinato disposto con l'articolo 65 CP, permette al giudice di pronunciare la multa (o l'arresto) invece della detenzione.

9.32 Capoverso 2

9.321 In generale

Il (nuovo) articolo 322bis numero 1 capoverso 1 CP esige la consapevolezza, da parte dell'hosting provider, della punibilità dell'atto commesso dal fornitore di contenuti. Ci si chiede pertanto come vada valutata la posizione dell'hosting provider che non acquisisce tale consapevolezza, poiché le segnalazioni che ha ricevuto contengono unicamente gli indirizzi URL delle pagine web contestate, senza ulteriori informazioni. Se in un simile caso l'hosting provider resta passivo, non potrà mai acquisire la consapevolezza richiesta dal capoverso 1. Sarebbe un prezzo troppo alto da pagare per la formulazione giustamente restrittiva del capoverso 1. Occorre pertanto (ri)equilibrare la limitazione della responsabilità prevista dal primo capoverso.

È la funzione del (nuovo) articolo 322bis numero 1 capoverso 2 CP.
In base a questa impostazione, sembrerebbe ovvio concepire il capoverso 2 come una variante, analogamente alla fattispecie relativa all'elusione della prova del sangue (art. 91 cpv. 3 LCStr). Nel progetto si rinuncia a tale soluzione per *diversi motivi*:

- una variante della norma basata sull'elusione avrebbe il tenore seguente: "La stessa pena è comminata a chiunque elude l'acquisizione della consapevolezza necessaria ai sensi del capoverso 1". In tal senso la disposizione concernerebbe unicamente l'autore che con il suo agire impedisce la presa di conoscenza delle segnalazioni a lui indirizzate. Metaforicamente, la situazione sarebbe quella di colui che costruisce un muro attorno a sé affinché le informazioni esterne non possano più raggiungerlo. Tuttavia il problema risiede altrove. Il problema si pone piuttosto quando l'hosting provider, senza agire attivamente per isolarsi, resta inattivo e le segnalazioni non lo raggiungono [246] o lui non le segue, di modo che esse non possono esplicare alcun effetto. Il capoverso 2 deve quindi essere applicato soprattutto in caso di *omissione*.

- Occorrerebbe pertanto completare la formulazione come segue: "… o non fa nulla per evitare la mancata acquisizione di tale consapevolezza". Il tenore seguente

[246] Con un'altra metafora: colui che non ha bisogno di costruire un muro attorno a sé, poiché le informazioni in ogni caso non possono raggiungerlo, essendoci un fossato tra lui e l' "esterno".

avrebbe lo stesso significato: "La stessa pena è comminata a chiunque agisce in modo da non poter acquisire la consapevolezza necessaria ai sensi del capoverso 1, o non fa nulla per evitare la mancata acquisizione di tale consapevolezza." A prescindere dalla sua formulazione pesante e complessa, questa variante ha un grave svantaggio: comporta di nuovo un obbligo positivo di controllo da parte dell'hosting provider. Ma se già la regolamentazione prevista dal capoverso 1, con il presupposto della consapevolezza, mira a escludere un simile obbligo di controllo, ciò deve valere anche per il capoverso 2, il cui scopo è quello di equilibrare gli scompensi del primo capoverso.

Un tale riequilibrio non può consistere nell'introduzione di un obbligo di controllo, dopo che questo è stato escluso nel capoverso precedente. Indipendentemente da ciò, un obbligo di controllo, purché lo si voglia ammettere, solleverebbe la domanda seguente: in che misura gli hosting provider sono tenuti a setacciare il loro server Internet alla ricerca di informazioni illegali? Non è possibile rispondere a questa domanda in modo astratto, e l'introduzione di una responsabilità per omissione sarebbe all'origine di una situazione di incertezza giuridica che occorre scongiurare con l'adozione della nuova regolamentazione.

- In base a queste considerazioni, l'unica soluzione consisterebbe nel completare la formulazione della variante “elusione”, nel modo seguente: "In assenza di segnalazioni di terzi, non vi è l'obbligo di ricercare in una rete di telecomunicazioni informazioni ai sensi del capoverso 1". Il problema relativo al controllo non sarebbe comunque risolto, poiché si affermerebbe esplicitamente che l'obbligo di fare ricerche nascerebbe in presenza di segnalazioni da parte di terzi. È anche per evitare un simile obbligo che il capoverso 1 limita l'elemento soggettivo della fattispecie alla condizione della consapevolezza del carattere punibile dell'atto commesso dal fornitore di contenuti.

  Il problema non sarebbe risolto nemmeno se un obbligo di fare ricerche nascesse soltanto quando giungono segnalazioni da terzi. Tralasciando l'aggiunta "in assenza di segnalazioni di terzi", si entrerebbe in contraddizione con il primo periodo, in cui si afferma espressamente che la fattispecie legale è realizzata anche da colui che "permette la mancata acquisizione" della consapevolezza necessaria ai sensi del capoverso 1. A prescindere da ciò una simile delimitazione dell'obbligo rappresenterebbe un caso unico nel Codice penale.

Per tale motivo con il progetto si è deciso di compiere una *misura radicale*. Invece di formulare una variante “elusione”, cercando così di compensare la limitazione della punibilità alla consapevolezza del carattere illecito dell'atto, come previsto dal capoverso 1, all'hosting provider viene imposto l'*obbligo positivo* di trasmettere alle autorità di perseguimento penale le segnalazioni relative a (presunti) reati commessi sul suo server Internet.

In tal modo vi è anche la garanzia che la punibilità, su riserva del capoverso 1, venga valutata dall'autorità competente e non da una persona privata. Questo soprattutto perché numerose fattispecie potenzialmente rilevanti nel presente contesto, quali quelle previste dagli articoli 135, 197 o 261bis CP, offrono un margine d'interpretazione normativo che in caso di dubbio deve essere appunto riservato agli organi competenti.

9.322 Particolarità

9.322.1 Autori del reato

In quanto alla cerchia degli autori del reato, il capoverso 2 corrisponde al capoverso 1. Anche qui è preso in considerazione quale autore unicamente colui che tiene a disposizione informazioni di terzi in una rete di comunicazione elettronica, vale a dire l'hosting provider. La struttura della disposizione è pertanto la medesima di quella del capoverso 1, e quanto ritenuto al numero *9.312.3* vale anche per il capoverso 2.

9.322.2 Fattispecie di reato

Anche il capoverso 2 concerne un *puro reato di omissione*. L'hosting provider omette di trasmettere segnalazioni riguardanti informazioni (presenti sul suo server Internet), per mezzo delle quali viene commesso un reato. In altri termini, l'hosting provider non porta tali segnalazioni alla conoscenza delle autorità di perseguimento penale. Anche in questo caso si presuppone naturalmente che l'hosting provider abbia la possibilità di trasmettere le segnalazioni, e che tale modo di agire possa ragionevolmente essere preteso. Nell'avamprogetto si rinuncia a fissare un *termine* entro cui trasmettere le segnalazioni: esso dipende dalle possibilità dell'hosting provider e da criteri di ragionevolezza. Non si disciplina nemmeno la *forma* della trasmissione; entrano in considerazione tutte le forme di comunicazione atte a portare efficacemente alla conoscenza delle autorità di perseguimento penale il contenuto della segnalazione.

Il testo di legge non specifica infine a quale specifica autorità di perseguimento penale l'informazione debba essere trasmessa. Precisare che l'informazione va trasmessa alla "competente" autorità di perseguimento penale non avrebbe senso. Infatti, se con ciò si intende l'autorità competente per il perseguimento del reato del fornitore di contenuti, si può controbattere che l'hosting provider non sa quasi mai chi è competente. Se invece si intende dire che l'informazione deve essere trasmessa all'autorità di perseguimento penale competente per la ricezione dell'informazione stessa, si afferma una cosa scontata, e la sua menzione è quindi superflua. Alla luce dello scopo perseguito dal capoverso 2, è determinante che l'informazione non rimanga sul server Internet, ma che sia portata alla conoscenza di un'autorità di perseguimento penale. Nella prassi prenderanno piede mezzi di trasmissione universalmente riconosciuti.

Occorre descrivere con maggior precisione le *segnalazioni* la cui mancata trasmissione può essere imputata all'hosting provider:

- innanzitutto con "segnalazioni" si intendono le informazioni *indirizzate* all'hosting provider. Vi sono due aspetti da precisare: l'obbligo di trasmissione scatta soltanto in seguito a comunicazioni indirizzate individualmente all'hosting provider, ma non sulla base di informazioni accessibili in modo generale attraverso stampa, radio o televisione. Vi è obbligo di trasmissione soltanto se la segnalazione è stata indirizzata all'hosting provider proprio allo scopo di informarlo. Il capoverso 2 non si applica al caso in cui all'hosting provider vengono segnalati i contenuti punibili sul suo server Internet attraverso un

giornale a cui è abbonato (in tal caso *è il giornale* che gli è indirizzato, non l'informazione!): verrebbe infatti a mancare il legame specifico tra informazione e processo di comunicazione. Lo stesso vale nel caso di una newsletter alla quale l'hosting provider è abbonato.

- Non è tuttavia sufficiente che le segnalazioni siano semplicemente "indirizzate all'hosting provider". La destinazione "hosting provider" definita per il loro invio non basta: occorre che le segnalazioni siano *giunte a destinazione* ed *effettivamente pervenute* all'hosting provider. Il presente progetto parla pertanto di segnalazioni "a lui pervenute". Non è al contrario opportuno prevedere che le segnalazioni siano state "portate alla sua conoscenza". In tal caso si ammetterebbe una componente soggettiva nella delimitazione oggettiva della fattispecie. Il fatto che l'hosting provider, per agire intenzionalmente, debba prendere atto delle segnalazioni, è una questione che riguarda gli aspetti soggettivi della fattispecie e va pertanto trattata in tale contesto.

  Nell'ambito della comunicazione elettronica, in teoria la ricezione di tali segnalazioni può essere impedita in due modi. È possibile erigere una barriera (cfr. la metafora citata in precedenza, consistente nell'isolamento per mezzo della costruzione di un muro), oppure facendo sì che non vi sia alcuna possibilità di contatto elettronico (metafora del fossato preesistente). In pratica tuttavia questi timori hanno scarsa rilevanza, poiché gli hosting provider dipendono dalla comunicazione, e allestiscono e mantengono operativi i rispettivi canali di trasmissione e ricezione.

- La responsabilità dell'hosting provider è *limitata al caso in cui le informazioni provengono da terzi*. Questa precisazione serve da un lato a ricordare che le informazioni accessibili a tutti, provenienti da radio o televisione, non fanno nascere l'obbligo di trasmissione all'autorità. D'altro lato, il suo scopo è anche quello di chiarire che l'hosting provider non deve procedere autonomamente alla ricerca di segnalazioni. Ciò significa che, secondo il capoverso 2, l'hosting provider non è tenuto a trasmettere segnalazioni relative a reati che ha *lui stesso* scoperto per caso (ossia segnalazioni che non provengono da terzi), nella misura in cui egli ritenga la loro punibilità possibile, ma non certa. Se invece è certo del carattere punibile del reato, egli è tenuto a bloccare l'accesso ai dati, altrimenti diverrebbe responsabile ai sensi del capoverso 1.

- L'hosting provider è tenuto a trasmettere unicamente le segnalazioni riguardanti i file che ospita sul suo server. Una segnalazione diretta al provider A, che informa del carattere pornografico dei file XY, non deve essere trasmessa se i dati contestati non sono ospitati sul server del provider A, ma su quello del provider B. Una soluzione diversa porterebbe a un obbligo di denuncia generale e settorialmente limitato ("reati Internet"), senza che ciò abbia una relazione con l'attività specifica dell'hosting provider. Questa soluzione risulta inoltre dalla considerazione che anche il (nuovo) articolo 322bis numero 1 capoverso 2 CP riguarda un ambito parziale, e in un certo senso statuisce indirettamente una norma positiva di partecipazione (al reato del fornitore di contenuti). L'hosting provider partecipa evidentemente soltanto al reato che viene commesso sul suo server.

- *Oggetto delle segnalazioni* sono le informazioni che l'hosting provider ha tenuto automaticamente a disposizione, e per mezzo delle quali viene commesso un reato. In questo punto il capoverso 2 corrisponde totalmente al capoverso 1; si rinvia pertanto a quanto ritenuto in precedenza.

  Sotto il regime del (nuovo) articolo 322bis numero 1 capoverso 2 CP, un hosting provider prudente trasmetterà all'autorità di perseguimento penale *ogni segnalazione ricevuta*. In tal modo non realizzerà la fattispecie prevista dalla disposizione citata, purché la segnalazione non contenga già essa stessa informazioni che fanno acquisire all'hosting provider la consapevolezza della punibilità del reato in questione. Se ciò fosse invece il caso e l'hosting provider trasmettesse tale segnalazione, realizzerebbe la fattispecie dell'articolo 322bis numero 1 capoverso 1 CP. Se viceversa rinunciasse alla trasmissione di una segnalazione semplice ("la pagina web XY contiene rappresentazioni di atti di cruda violenza"), il (nuovo) articolo 322bis numero 1 capoverso 2 CP non sarebbe applicabile, qualora le rappresentazioni non realizzassero oggettivamente la fattispecie dell'articolo 135 CP e l'hosting provider ne fosse cosciente (altrimenti si tratterebbe di reato impossibile).

9.322.3 Elemento soggettivo

Ancora una volta è necessaria l'*intenzionalità*; in relazione a tutti gli elementi costitutivi della fattispecie, il dolo eventuale è sufficiente. Chi ritiene seriamente possibile e si assume il rischio che l'oggetto di una segnalazione sia effettivamente un'informazione penalmente rilevante da lui ospitata (e tiene quindi a disposizione l'informazione ai sensi del capoverso 2), e omette nonostante tutto di trasmettere la segnalazione, si rende punibile secondo il (nuovo) articolo 322bis numero 1 capoverso 2 CP.

Lo stesso varrebbe nel caso di un hosting provider che omettesse sistematicamente di prendere atto delle segnalazioni pervenutegli. Se le segnalazioni dovessero accumularsi, il comportamento dell'hosting provider non potrebbe che essere interpretato come accettazione del fatto che tra le segnalazioni potrebbero essercene alcune che concernono effettivamente dati di rilevanza penale. Il rimprovero mosso all'hosting provider non sarebbe tuttavia quello di non aver vagliato le segnalazioni (non esiste un obbligo di controllo!), ma bensì di non averle trasmesse, nonostante l'evidente possibilità che concernessero informazioni punibili. Se invece l'hosting provider, ritenendo che la segnalazione è sì fondata, ma concerne dati ospitati dal concorrente XY, omettesse di trasmetterla, non vi sarebbe intenzionalità e l'hosting provider non sarebbe quindi punibile secondo il capoverso 2.

9.322.4 Pena

Anche il capoverso 2 commina la *detenzione o la multa*. A prima vista ciò può apparire severo per la semplice inosservanza dell'obbligo di trasmissione. La comminatoria diviene tuttavia plausibile se si considera che, come per il capoverso 1, la disposizione si basa sulla partecipazione dell'hosting provider al reato principale. Tale disposizione intende inoltre compensare le limitazioni previste in materia di consapevolezza (a sua volta necessaria per altri motivi).

9.33 Capoverso 3

9.331 Principio

La formulazione proposta del capoverso 2 può far sì che un hosting provider ometta di trasmettere una segnalazione fondata relativa a un reato ai sensi del capoverso 1, senza che l'autore di tale reato venga perseguito o punito. Questo perché non è stata sporta la necessaria querela (ad esempio nei casi di reati contro l'onore, art. 173 segg. CP, o in caso di violazioni del diritto d'autore, art. 67 segg. LDA). Il caso è paragonabile a quello della ricettazione (art. 160 CP): se il reato preliminare è perseguibile solo a querela di parte, e se in mancanza di tale querela il reato non viene penalmente perseguito, il capoverso 3 del numero 1 dell'articolo 160 CP prevede che non sarà perseguita nemmeno la ricettazione.

La commissione di esperti propone per il (nuovo) articolo 322bis numero 1 CP una *regolamentazione analoga*: nella misura in cui il reato sia perseguibile soltanto a querela di parte, e se tale querela non è stata sporta, non viene promossa un'azione nemmeno nei confronti dell'hosting provider. Una soluzione diversa porterebbe a situazioni paradossali: nel caso di un reato contro l'onore, l'hosting provider sarebbe tenuto a trasmettere una segnalazione pervenutagli e riguardante tale reato, nonostante quest'ultimo non sia oggetto di perseguimento penale poiché la presunta parte lesa ha deciso di non sporgere querela.

Se l'hosting provider omettesse di trasmettere la segnalazione, nei suoi confronti andrebbe aperto un procedimento per sospetta violazione del (nuovo) articolo 322bis numero 1 capoverso 2 CP. In tale procedimento andrebbe pubblicamente discusso il presunto delitto contro l'onore, contro la volontà della parte lesa che ha proprio per questo rinunciato a sporgere denuncia. Il capoverso 3 si giustifica anche con il fatto che il (nuovo) articolo 322bis numero 1 CP si applica in definitiva al contributo dell'hosting provider al reato commesso dal fornitore di contenuti, ossia al "reato principale".

Per le sue caratteristiche e al di là delle descrizioni specifiche del comportamento, il contributo dell'hosting provider costituisce un atto di complicità. Ma se nessuna querela è stata sporta contro l'autore del reato principale, ciò significa che non vi possono nemmeno essere querele dirette contro i complici. Infatti, se è stata sporta una querela contro un complice, essa concernerebbe anche l'autore principale (art. 30 CP). La regolamentazione proposta è opportuna anche per questo motivo. Soltanto per chiarezza, si aggiunga che il (nuovo) articolo 322bis numero 1 capoversi 1 e 2 CP non diviene un reato perseguibile a querela di parte: il capoverso 3 decreta unicamente un blocco del perseguimento qualora *il reato* ai sensi dei capoversi 1 e 2 sia perseguibile soltanto a querela di parte, e una querela non sia stata sporta.

9.332 Incertezza quanto alla querela

Quando riceve una segnalazione riguardante un reato perseguibile solo a querela di parte, spesso l'hosting provider non sa se una querela è stata sporta; se non sa che il reato è perseguibile solo a querela di parte, trasmetterà comunque la segnalazione. All'hosting provider conviene dunque trasmettere le comunicazioni

indipendentemente dall'esigenza di una querela. Infatti, se una querela è stata sporta, ma l'hosting provider dà per scontato che non lo sia stata, questo errore è irrilevante, poiché non concerne la sua intenzionalità, ma un presupposto processuale. Ancora una volta la funzione del capoverso 3 risulta chiara: la disposizione non si rivolge direttamente all'hosting provider, limitando il suo obbligo di trasmettere. Lo scopo della norma è piuttosto quello di impedire che l'hosting provider venga ingiustamente punito per non aver trasmesso una segnalazione secondo il capoverso 2, nonostante il fatto che colui che è leso dal presunto reato abbia rinunciato al suo perseguimento e quindi anche a una sanzione.

9.333 Assenza di una querela in caso di reati perseguibili solo a querela di parte

Il capoverso 3 non si riferisce soltanto al capoverso 2, ma anche al capoverso 1. Anche se l'hosting provider è consapevole che per mezzo dell'informazione di terzi viene commesso un reato, non vi è perseguimento penale se il reato è perseguibile solo a querela di parte e una querela non è stata sporta. Quanto ritenuto in relazione al capoverso 2 vale analogamente nel presente contesto: non ha senso impedire l'utilizzo di un'informazione per mezzo della quale è commesso un reato, se colui che si presume sia stato leso da tale reato non vuole che esso sia perseguito e punito. In caso contrario l'hosting provider dovrebbe essere punito addirittura nel caso in cui la parte lesa nel proprio onore gli segnala l'informazione, e nello stesso tempo gli comunica che non è interessato al perseguimento penale della stessa. In altri termini, se la parte lesa intende impedire sulla base di una norma penale l'utilizzo dell'informazione, deve sporgere querela.

9.34 Capoverso 4

9.341 Principio

La comunicazione in Internet non tiene conto in alcun modo dei confini nazionali. Sorgono quindi difficoltà in relazione alle norme sull'applicabilità della legge penale (art. 3 e segg. CP). La regolamentazione vigente ha risolto un primo problema: secondo la giurisprudenza del Tribunale federale, gli atti di partecipazione sono considerati commessi nel luogo del reato principale. Se questo luogo si trova all'estero, gli atti di partecipazione non sarebbero di principio punibili in Svizzera, nella misura in cui consistano in atti di partecipazione dell'hosting provider e non ci si trovi in un caso di correità.

Il presente progetto elude questo problema, nel senso che disgiunge in parte e in modo fattivo la punibilità dell'hosting provider da quella del fornitore di contenuti. Se il reato principale è stato commesso all'estero e l'hosting provider si trova in Svizzera, i capoversi 1 e 2 del (nuovo) articolo 322^{bis} numero 1 CP sono applicabili; non vi è invece sovranità penale svizzera se anche l'hosting provider si trova all'estero.

9.342 Punibilità del reato

Non è tuttavia ancora chiaro quale sia il diritto applicabile per stabilire se ci si trova in presenza di un *reato*. Nel diritto privato la questione del diritto applicabile è valutata sulla base delle norme sancite dal diritto internazionale privato (art. 13 e segg. LDIP e relative disposizioni specifiche). Nel diritto penale si è alla vana ricerca di un sistema normativo di questo tipo. Mancano disposizioni legali esplicite che, a livello internazionale, forniscano un'indicazione sul diritto applicabile per valutare la punibilità di un reato. Gli articoli 3 e seguenti CP non sono applicabili, poiché disciplinano la competenza internazionale e non il diritto applicabile (ad eccezione dei rispettivi numeri 1, secondo periodo degli articoli 5, 6 e 6bis CP).

Il diritto penale vigente non contempla strutture parallele che permettono di risolvere la questione del diritto applicabile: il CP non contiene norme che stabiliscono secondo quale diritto occorre valutare la punibilità di un atto che costituisce uno degli elementi della fattispecie oggettiva. Nel "caso normale" della complicità, il problema non si pone se il reato principale è stato commesso all'estero: in tal caso si considera che anche la complicità è avvenuta all'estero e, venendo a mancare la sovranità penale svizzera, non può porsi il problema del diritto applicabile. Per quel che concerne gli atti di complicità, non ci si trova quindi mai confrontati con la necessità di stabilire quale sia il diritto applicabile per valutare la punibilità del reato principale commesso all'estero.

In conclusione è tuttavia chiaro che la questione della punibilità del reato deve essere valutata secondo il *diritto svizzero*. In caso contrario si rinuncerebbe al vantaggio, introdotto dall'avamprogetto, rappresentato dalla punibilità indipendente dell'hosting provider. Lo scopo della nuova norma non è soltanto quello di disciplinare le controverse questioni relative alla partecipazione, ma anche quello di impedire che l'informazione "punibile" possa continuare a essere richiamata da un server svizzero; questo chiaramente soltanto nella misura in cui i dati contengono informazioni punibili secondo il diritto *svizzero*, poiché si tratta dell'applicazione di quest'ultimo. Occorre unicamente chiedersi se per questo sia necessaria una regolamentazione esplicita [247].

9.343 Ragioni a sostegno di una normativa esplicita

Una soluzione esplicita è preferibile se si tiene conto che il (nuovo) articolo 322bis numero 1 CP è una disposizione che, dal profilo funzionale, prevede una partecipazione. L'atto di partecipazione segue il destino del reato principale: per la sua valutazione sono competenti le autorità estere, che applicano il loro diritto. A ciò si aggiunge il fatto che la nuova disposizione rinuncia al principio della doppia punibilità, nella misura in cui si tratta della valutazione della punibilità del reato.

---

[247] Per il caso in cui il reato presupposto è stato commesso all'estero, dalla regolamentazione speciale in materia di riciclaggio di denaro non è possibile dedurre nulla (art. 305bis n. 3 CP). Essa concerne un'ipotesi specifica: il fatto di vanificare la confisca di valori patrimoniali (senza il numero 3 l'atto non sarebbe punibile, poiché il titolo XVII protegge soltanto l'amministrazione della giustizia svizzera: in caso di reato presupposto commesso all'estero, si proteggerebbe quella estera), atto che non ha nulla a che vedere con il (nuovo) articolo 322bis numero 1 CP (all'hosting provider non viene rimproverato il fatto di vanificare la confisca o il blocco, ma di aver omesso di impedire, attraverso il blocco dell'accesso, l'utilizzo dei dati contestati).

L'hosting provider deve essere perseguibile anche nei casi in cui l'atto contestato non è punibile secondo il diritto del luogo in cui è stato commesso. In questo contesto assumono rilevanza pratica soprattutto alcune posizioni degli ambienti giuridici americani o australiani, considerate dal diritto svizzero atti di discriminazione razziale. Queste due modifiche, nella misura in cui originano divergenze rispetto alle regole generali, fanno propendere per un disciplinamento esplicito della questione del diritto applicabile.

9.344 Funzione del nuovo capoverso

Anche senza la disposizione speciale proposta, la punibilità dell'atto contestato sarebbe valutata secondo il diritto elvetico: ciò può essere giustificato facendo riferimento alla competenza internazionale svizzera in simili casi. Se l'omissione dell'hosting provider soggiace incontestabilmente alla sovranità penale svizzera, tale omissione deve essere giudicata secondo la legge elvetica. Tale posizione è condivisa anche dal legislatore svizzero, e ciò è dimostrato dalle eccezioni menzionate (i rispettivi numeri 1 periodi 2 degli articoli 5, 6 e 6bis CP). La menzione secondo cui va applicata la legge del luogo di commissione, se essa si rivela più favorevole all'autore del reato, ha senso soltanto se si considera applicabile il diritto svizzero.

Il dovere di applicare la legge svizzera risulta, per gli articoli 3-7 CP, dal fatto che il reato sottostà alla sovranità penale svizzera. La conseguenza inespressa (dagli articoli 3-7 CP), ma di principio imperativa, della competenza internazionale è quindi, secondo la concezione svizzera, l'applicazione del diritto materiale svizzero. In tale ottica il nuovo capoverso 4 assume soltanto una funzione chiarificatrice.

Lo scopo del (nuovo) articolo 322bis numero 1 capoverso 4 CP è di rendere inutili fin dall'inizio eventuali discussioni sul diritto applicabile. Dal punto di vista della tecnica legislativa, la nuova disposizione non può tuttavia essere integrata nella disposizione penale materiale (ossia nel nuovo art. 322bis n. 1 cpv. 1 e 2 CP), poiché gli atti punibili che vengono presi in considerazione non sarebbero fin da principio limitati a un solo o ad alcuni reati. Occorrerebbe menzionare ogni reato che si pensa possa essere commesso con l'ausilio o per mezzo di reti di comunicazione elettronica. È il caso di *tutti* i reati; pertanto il medesimo contenuto normativo viene trasferito in un capoverso separato.

Come si decide sempre in mancanza di una regolamentazione, al fine di dissipare ogni dubbio si afferma in modo esplicito che la punibilità di un reato viene giudicata in base al diritto svizzero (è chiaro che si tratta dell'applicazione del diritto materiale e non di quello della competenza *ratione loci* [248]). Non si tratta di una questione inutile, in un ambito in cui le norme sull'applicazione del diritto non sono particolarmente evolute, considerato che finora non vi è stata la necessità di un loro sviluppo.

[248] Altrimenti si cadrebbe in un circolo vizioso: il capoverso 4 rinvierebbe agli articoli 3 e seguenti CP, e la sovranità penale svizzera risulterebbe dal fatto che la sede dell'hosting provider si trova in Svizzera; pertanto il (nuovo) articolo 322bis numero 1 CP sarebbe applicabile. Il problema relativo al diritto applicabile per giudicare la punibilità del reato sarebbe risolto in base al capoverso 4, che però rinvierebbe agli articoli 3 e seguenti e si ricomincerebbe daccapo.

9.35 Capoverso 5

Secondo il capoverso 5, le informazioni ai sensi dei capoversi 1 e 2, ossia quelle per mezzo delle quali viene commesso un reato, vengono cancellate. In questo caso ci si chiede innanzitutto se una simile disposizione si riveli necessaria, o se la facoltà di cancellare non risulti comunque dall'applicazione delle regole generali relative alla confisca.

9.351 Cancellazione nel caso del capoverso 1

9.351.1 Principio

Nel presente contesto, la *sedes materiae* del diritto sulla confisca è l'articolo 58 CP (confisca di oggetti pericolosi), così come le disposizioni particolari sulla confisca relative a singoli reati. Se in un procedimento penale l'accusato viene ad esempio condannato per pornografia dura (art. 197 n. 3 CP), e se i dati di carattere pornografico si trovano sul disco rigido del suo computer, in base alle disposizioni particolari dei rispettivi capoversi 2 dell'articolo 197 numeri 3 e 3bis, il disco rigido può essere confiscato. Dato che la confisca deve rispettare il principio della proporzionalità [249]; ciò non significa però che la persona condannata non potrà rientrare in possesso del proprio disco rigido. L'autorità d'esecuzione è tenuta a cancellare i dati incriminati e a consegnare in tale stato l'oggetto al proprietario; questo in ogni caso quando non vi è la probabilità che l'oggetto venga nuovamente utilizzato a fini criminosi. La confisca rimane tuttavia diretta contro un oggetto (fisico) ai sensi dell'articolo 58 CP; attraverso la cancellazione, tale oggetto viene tuttavia alterato a tal punto da perdere la sua pericolosità [250].

Se le "informazioni punibili" ospitate da un hosting provider condannato sulla base del (nuovo) articolo 322bis numero 1 capoverso 1 CP dovessero essere cancellate, occorrerebbe in sé confiscare il suo server Internet, sul quale tali informazioni si trovano. Tale soluzione non è tuttavia praticabile, poiché di regola risulterebbe sproporzionata: la cancellazione toccherebbe infatti la totalità degli altri clienti dell'hosting provider, le cui informazioni sono state memorizzate sul server da confiscare. L'attuabilità pratica di una tale disposizione sarebbe oltretutto dubbia. L'alternativa risiede nel far sì che l'hosting provider acceda direttamente al suo server Internet e provveda alla cancellazione delle informazioni "punibili", purché non abbia già adempiuto alla precedente ingiunzione di cancellazione.

Un'applicazione per analogia dell'articolo 58 CP al presente caso appare dubbia. L'oggetto della confisca sarebbero dati o informazioni che non rappresentano però

---

[249] BAUMANN, in Niggli/Wiprächtiger, Basler Kommentar, Basilea 2003, art. 58 n. 14. Ciò vale anche per le disposizioni speciali sulla confisca dell'art. 135 cpv. 2 e dell'art. 197 n. 3 cpv. 2 e n. 3bis cpv. 2: AEBERSOLD, in Niggli/Wiprächtiger, Basler Kommentar, Basilea 2003, art. 135 n. 35; per SCHWAIBOLD/MENG, in Niggli/Wiprächtiger, Basler Kommentar, Basilea 2003, art. 197 n. 61, il principio è meno chiaro.

[250] Se anche per i rispettivi cpv. 2 dell'art. 197 n. 3 e 3bis CP debbano essere realizzate le condizioni poste dall'art. 58 CP o altri singoli requisiti, è una questione che può essere lasciata aperta.

oggetti ai sensi dell'articolo 58 CP [251]. Inoltre non vi può essere una vera e propria confisca, ma viene presa in considerazione unicamente una cancellazione. Per questi motivi nell'avamprogetto si è optato per una soluzione esplicita del problema.

9.351.2 Natura materiale della cancellazione

In quanto pendant della confisca, la cancellazione delle informazioni ha un carattere materiale. È ordinata dal giudice nella sentenza. Il capoverso 5 non costituisce una disposizione processuale analoga al sequestro, per mezzo del quale le autorità di perseguimento penale potrebbero bloccare provvisoriamente l'accesso alle informazioni. Una simile disposizione è riservata alla legislazione procedurale, ossia attualmente ancora ai Cantoni. Questi ultimi sono tenuti ad attuare il diritto penale materiale della Confederazione e devono mettere in tal senso a disposizione sufficienti strumenti processuali. In primo piano vi è qui un ordine di blocco impartito dalle autorità di perseguimento penale; tale ordine, in quanto misura coercitiva processuale, deve fondarsi su corrispondenti disposizioni cantonali.

Nell'ambito dell'avamprogetto di Codice di procedura penale svizzero, occorrerà stabilire se una regolamentazione espressa per il "sequestro" di dati debba essere ammessa nella forma di un blocco (dell'accesso) comprensivo di divieto di apportare modifiche [252]. Anche la Convenzione sulla cibercriminalità, nella sua parte procedurale (art. 19 n. 3 lett. d), esige che la legislazione metta a disposizione delle autorità competenti gli strumenti che permettano di bloccare l'accesso a determinati dati.

9.351.3 Cancellazione in caso di assoluzione

Il giudice ordina la cancellazione delle informazioni in caso di condanna. Per il procedimento diretto contro l'hosting provider e per quello contro il fornitore di contenuti, occorre esaminare separatamente in che misura una cancellazione entra in considerazione anche in caso di assoluzione o di archiviazione della causa:

- se un hosting provider non viene condannato, ad esempio perché è possibile provare soltanto un dolo eventuale ma non la sua consapevolezza riguardo alla punibilità dell'informazione, ci si chiede se le informazioni "punibili" possano comunque essere cancellate. L'articolo 58 CP prevede la confisca "indipendentemente dalla punibilità di una data persona"; lo stesso vale per la disposizione speciale del nuovo capoverso 5.

  Ciò significa due cose: *in primo luogo*, per l'hosting provider il cui comportamento realizza la fattispecie penale, eventuali motivi di esclusione della colpa non si oppongono alla cancellazione. *In secondo luogo*, e questo ha maggior rilevanza

[251] Secondo SCHMID (bibl.), n. 22 ad art. 58 CP, i valori incorporei quali "crediti, averi e beni immateriali come brevetti, diritti d'autore ecc., di regola non possono essere confiscati secondo l'articolo 58 CP; SCHMID intravede un'eccezione per i dati (op. cit., nota 57). L'eccezione non viene tuttavia motivata e l'esecuzione della confisca in tali casi non viene illustrata in modo più approfondito. TRECHSEL (bibl.), n. 5 ad art. 58, menziona la cancellazione di un programma da un disco rigido.

[252] Secondo gli articoli 273 e seguenti dell'avamprogetto di Codice di procedura penale svizzero, oggetto del sequestro sono "oggetti e valori patrimoniali".

nel presente contesto, una cancellazione è ammissibile anche quando a commettere il reato alla base della confisca non è stato l'accusato, ma un terzo. Anche in questo caso le informazioni per mezzo delle quali è stato commesso un reato possono essere cancellate dal server Internet dell'hosting provider [253].

Quindi, se l'hosting provider viene assolto dall'accusa di aver realizzato la fattispecie prevista dal (nuovo) articolo 322bis numero 1 CP, ciò non significa necessariamente che le informazioni contestate non possano essere eliminate dal suo server. Purché nella sentenza sia stabilito che si tratta di un atto (commesso da un terzo, ossia in questo caso dal fornitore di contenuti) illecito che realizza una fattispecie legale, il giudice può disporre la cancellazione delle informazioni. Per alcuni reati si prevede una specifica disposizione di confisca (come nel caso degli art. 135 cpv. 2, 197 n. 3 cpv. 2 e n. 3bis cpv. 2 CP): in tali casi non occorre valutare ulteriormente il carattere specificatamente pericoloso delle informazioni, come menziona espressamente l'articolo 58 CP per quel che riguarda gli oggetti da confiscare.

- Questa soluzione è tuttavia sottoposta a una limitazione: il Tribunale federale ha recentemente chiarito (la dottrina riteneva la questione controversa [254]), che una confisca di valori patrimoniali situati in Svizzera secondo l'articolo 59 CP è possibile unicamente se il reato da cui tali valori derivano soggiace alla sovranità penale svizzera [255]. Alla luce dell'argomentazione della citata decisione del Tribunale federale, ciò dovrebbe valere anche per la confisca di oggetti pericolosi [256]. Di conseguenza, se il reato del fornitore di contenuti non sottostà alla sovranità penale svizzera, in caso di assoluzione dell'hosting provider non vi sarebbe la possibilità, sulla base alle regole generali, di cancellare le informazioni illecite. Lo stesso vale per una procedura indipendente [257] di confisca o di cancellazione diretta contro l'hosting provider.

- Per questi motivi la commissione di esperti ha deciso di permettere la cancellazione "a prescindere dalla sovranità penale svizzera". Se nella sentenza d'assoluzione dell'hosting provider si ritenesse che un fornitore di contenuti ha telecaricato sul server dell'hosting informazioni di carattere penalmente rilevante, ma che una cancellazione di tali dati non sarebbe possibile poiché il reato commesso dal fornitore di contenuti non sottostà alla sovranità penale svizzera, si creerebbe una situazione insoddisfacente dal profilo politico-giuridico. Lo scopo

---

[253] Cfr. DTF 124 IV 121: X. era il destinatario di riviste e CD di carattere razzista. Il Tribunale cantonale ha assolto X. dall'accusa di aver violato l'articolo 261bis CP, ritenendo che l'elemento soggettivo della fattispecie non era stato realizzato, ordinando tuttavia la confisca delle riviste e dei CD. Il Tribunale federale ha confermato la confisca, giungendo alla conclusione che lo sconosciuto mittente (dagli Stati Uniti) ha realizzato gli elementi oggettivo e soggettivo della fattispecie prevista dall'articolo 261bis CP. Inoltre, poiché l'articolo 58 CP autorizza la confisca "indipendentemente dalla punibilità di una data persona", non ha importanza il fatto che coloro che hanno divulgato il materiale non siano stati identificati o non possano essere perseguiti in Svizzera, e nemmeno che X. stesso non sia stato autore del reato o non abbia partecipato alla sua commissione (cfr. loc. cit., pag. 126).

[254] Ad esempio SCHMID (bibl.), n. 31 ad art. 58.

[255] DTF 128 IV 145.

[256] Gli articoli 3-7 CP rappresenterebbero norme d'applicazione del CP, delle quali l'articolo 59 farebbe parte (pag. 151). – In che misura ciò sia in contraddizione con la DTF 124 IV 241 non è chiaro. Questa sentenza sorvola la questione e non stabilisce se gli atti di discriminazione razziale commessi dal mittente delle riviste e dei CD debbano essere considerati come commessi in Svizzera.

[257] In merito vedi SCHMID (bibl.), n. 80 ad art. 58.

della regolamentazione speciale del (nuovo) articolo 322bis numero 1 CP non è infatti soltanto quello di definire con più precisione la punibilità dell'hosting provider, ma anche di fornire un mezzo per impedire l'utilizzo delle informazioni.

Ciò significa che questa soluzione farà ulteriormente inasprire la discussione intorno al concetto di evento nell'articolo 7 CP, e sulla natura del reato (reato d'evento/di comportamento). La discussione ha ancora rilevanza soltanto nella misura in cui si tratta di stabilire se il fornitore di contenuti sottostà alla sovranità penale svizzera. Invece il dibattito non è (più) significativo per quel che concerne il risultato che il reato produce: come punto di collegamento, infatti, ci si basa soltanto sul fatto che le conseguenze prodotte dal reato vengono "ospitate" da un provider con sede in Svizzera.

In breve: per la cancellazione non occorre che il reato del fornitore di contenuti sottostia alla sovranità penale svizzera: le informazioni sul server Internet vengono cancellate in ogni caso. Per questo sono immaginabili *due tipi di procedura*: per la sospetta violazione del nuovo capoverso 1, contro l'hosting provider viene aperto un procedimento in cui può essere ordinata la cancellazione dei dati, e questo indipendentemente dall'esito della procedura. Oppure, se non esistono sospetti di violazione del capoverso 1, viene avviata una procedura di cancellazione indipendente. Se un tribunale giunge alla conclusione che un determinato contenuto è illecito poiché realizza una fattispecie legale, ne ordina la cancellazione.

Il diritto di procedura cantonale deve provvisoriamente garantire una corrispondente procedura di cancellazione (vedi ad esempio gli art. 106a e seg. del Codice di procedura penale zurighese) [258]. Qualora dal (nuovo) articolo 340ter CP non fosse deducibile alcuna competenza federale, come foro andrebbe opportunamente designato il luogo della divulgazione, ossia il luogo in cui si trova il server ospitante (hosting; cfr. la regolamentazione analoga in materia di reati mediatici, art. 347 cpv. 2 CP). Non è peraltro necessario prevedere una disposizione esplicita riguardante la competenza ratione loci per questa procedura di cancellazione indipendente [259].

9.352 Cancellazione nel caso del capoverso 2

Anche quando un procedimento penale è stato avviato sulla base del capoverso 2, ossia quando un hosting provider non ha trasmesso una segnalazione, la cancellazione rappresenta un mezzo necessario per l'eliminazione delle informazioni illecite. Essa è menzionata sulla base delle stesse riflessioni fatte per il capoverso 1. In caso di assoluzione dell'hosting provider, occorre soprattutto evitare che l'informazione presente sul server di quest'ultimo non possa più essere cancellata: nel corso della procedura, infatti, può essere constatato che la segnalazione si riferisce sì a un'informazione per mezzo della quale è commesso un reato (ciò che

[258] Nell'elaborazione del Codice di procedura penale federale va debitamente tenuto conto di questa procedura particolare (cfr. art. 45 dell'avamprogetto, concernente le procedure di confisca indipendenti).

[259] La legge non definisce in modo preciso nemmeno il foro in materia di procedure di confisca indipendenti (art. 58 seg. CP), cfr. SCHMID (bibl.) art. 58 n. 81; art. 59 n. 139 „gli art. 346 segg. CP non sono applicabili".

secondo il capoverso 4 va valutato sulla base del diritto svizzero), ma che tuttavia tale infrazione non soggiace alla sovranità penale svizzera, di modo che non sarebbe possibile cancellare l'informazione.

Nel caso del capoverso 2, inoltre, anche se il procedimento sfocia in una condanna, non è certo che il nesso tra l'atto (omissione di trasmissione della segnalazione) e le informazioni ("punibili") sia sufficientemente stretto: si può dire che le informazioni siano servite a commettere un reato? La regolamentazione esplicita del capoverso 5 elimina queste incertezze: le informazioni che vengono segnalate all'hosting provider (che viene accusato della loro mancata trasmissione) possono essere cancellate, nella misura in cui dalla procedura risulta che per mezzo di esse è stato commesso un reato.

9.4 Commento al (nuovo) articolo 340ter CP

9.41 Problematica

In numerosi casi di criminalità in rete è apparso che, per la maggior parte delle fattispecie rilevanti, la competenza generale delle autorità cantonali non ha permesso un perseguimento effettivo dei reati. In un'importante azione ("Genesis") diretta nell'autunno del 2002 contro offerenti di pornografia infantile in Internet, è risultato evidente che l'Ufficio federale di polizia non disponeva delle basi legali per poter condurre indagini proprie, e che non esisteva un coordinamento vincolante delle procedure d'indagine a livello cantonale. Ciò ha causato tra l'altro *ritardi* nel rilevamento degli indirizzi dei sospetti presso le società di carte di credito, e ha impedito di *coordinare l'informazione* discordante. Anche in un contesto internazionale il modo di procedere delle autorità svizzere si è rivelato *lento*.

In casi particolarmente complessi di reati informatici commessi in rete a livello internazionale, vi è carenza di *penalisti specializzati* e delle necessarie infrastrutture sul piano cantonale.

Infine, all'inizio delle indagini *non è quasi mai chiaro quale autorità cantonale sia competente per il perseguimento*. Ad esempio, nel caso del "WEF-hack" [260] hanno iniziato a indagare le autorità ginevrine, poiché il server web in questione si trovava presso la sede del World Economic Forum (WEF). Dopo dispendiose indagini il caso è stato poi trasmesso alle autorità bernesi, poiché era stato possibile trovare una persona sospetta domiciliata in tale Cantone. Nei casi in cui il collegamento si basa sull'evento prodottosi, e qualora tale evento si produca in Svizzera esplicando effetti di portata nazionale (come nei casi di presa di conoscenza di reati contro l'onore), possono sorgere competenze multiple. Secondo l'articolo 346 capoverso 2 CP, sarebbe in tali casi competente il Cantone nel quale è stata aperta la prima istruzione; in ciò può tuttavia esserci una componente di casualità [261].

---

[260] Per un riassunto in proposito, vedasi: SCHWARZENEGGER, E-COMMERCE (bibl.), pag. 333 e i rinvii menzionati.

[261] Per il foro in materia di reati informatici secondo il diritto vigente (art. 346 segg. CP), vedi capitolo 6, n. 6.4.

9.42 Postulati della commissione peritale

Alla luce di queste esperienze è auspicabile la creazione di una speciale unità centrale presso l'Ufficio federale di polizia: sulla base di una chiara norma di competenza, tale organo dovrebbe fungere da centro di coordinamento (*clearing*) per i reati più complessi o per quelli internazionali. Nell'ambito di questo tipo di reati commessi per mezzo di una rete elettronica, occorre che penalisti specialmente formati possano intervenire in modo rapido e coordinato, sui piani intercantonale e internazionale. In linea di massima ciò non viene messo in discussione e rappresenta il modello prediletto, anche a livello internazionale (USA, Giappone, Italia, Austria).

Nello stesso tempo non è tuttavia auspicabile introdurre una competenza della Confederazione per tutti i tipi di reato, ossia anche per quelli in cui viene ad esempio utilizzata la posta elettronica o per i casi di minore importanza. La norma di competenza, attraverso un'esplicita formulazione, deve escludere simili casi.

Dopo aver accertato i fatti e conclusa la complicata procedura atta ad assicurare le prove, non è inoltre necessario che il caso sia portato a termine nell'ambito della procedura penale federale. Un *modello misto* appare più facilmente realizzabile, sia dal punto di vista istituzionale che da quello finanziario.

9.43 Caratteristiche del modello proposto

9.431 In generale

Questo modello prevede un'*unità centrale* per la lotta alla criminalità in rete. Ciò sarebbe possibile grazie al potenziamento del Servizio di coordinamento per la lotta contro la criminalità su Internet (SCOCI), che indaga per il momento sotto la direzione di un procuratore federale. Tale servizio è inoltre competente per il contatto e lo scambio di informazioni con gli organi competenti in materia di cibercriminalità di altri Paesi.

Al termine dell'inchiesta i casi più semplici vengono trasmessi alle autorità cantonali di perseguimento penale: un giudice istruttore cantonale, un procuratore distrettuale o un procuratore pubblico promuoverà quindi l'accusa dinanzi al giudice cantonale competente.

Come nel caso della giurisdizione federale nei casi di criminalità organizzata (art. 340^{bis} cpv. 1 CP), dopo la chiusura dell'istruttoria preliminare il Procuratore generale della Confederazione può delegare alle autorità cantonali il giudizio di un affare penale, e sostenere quindi l'accusa dinanzi al giudice cantonale.

9.432 Competenza della Confederazione: imperativa o facoltativa?

9.432.1 In generale

La regolamentazione concreta delle competenze può prendere la forma sia di una norma cogente, limitata ai reati informatici più complessi o di carattere internazionale (analoga all'art. 340bis cpv. 1 CP), sia di una norma potestativa (analoga all'art. 340bis cpv. 2 CP).

Affinché la regolamentazione risulti il più chiara possibile, la *Commissione peritale* è favorevole *a una norma cogente*. Ciò significa che, a determinate (e restrittive) condizioni, le autorità federali sono competenti per il perseguimento e il giudizio. Le esperienze acquisite finora dalla Polizia criminale federale hanno mostrato che, in materia di criminalità organizzata, l'applicazione dell'articolo 340bis capoverso 1 CP non pone problemi. Un *vantaggio* della versione proposta risiede nel fatto che crea *condizioni chiare* per le autorità cantonali di perseguimento penale e per il Ministero pubblico della Confederazione. Con le due condizioni menzionate relative alla competenza della Confederazione, viene garantito un effetto filtrante nei confronti dei reati informatici semplici.

9.432.2 Particolarità del (nuovo) articolo 340ter CP

Il (nuovo) articolo 340ter *capoverso 1 lettera a* CP riprende l'articolo 340bis capoverso 1 lettera b CP, mentre il (nuovo) articolo 340ter *capoverso 1 lettera b* CP contiene un importante complemento relativo alla funzione di coordinamento delle inchieste, qualora un importante numero di casi dello stesso tipo si presentassero in Cantoni diversi (vedi il caso "Genesis").

L’assunzione del perseguimento penale dal parte del Ministero pubblico della Confederazione su richiesta di un Cantone è invece strutturata in quanto *disposizione potestativa*: il (nuovo) articolo 340ter *capoverso 2* CP. Per il resto della procedura occorrerà prevedere un filtro supplementare rappresentato dalla delega alle autorità cantonali.

Un simile filtro è già previsto dall'*articolo 18bis PP*. Secondo questa disposizione, il Procuratore generale della Confederazione, dopo la chiusura dell’istruzione preparatoria, può delegare alle autorità cantonali il giudizio di una causa di diritto penale federale (art. 18bis cpv. 1 PP); in procedimenti semplici può delegare alle autorità cantonali l'istruzione, l'accusa e il giudizio (art. 18bis cpv. 2 PP).

L'entrata in vigore della *legge federale sul Tribunale penale federale* (LTPF) non modificherà i poteri di delega del Procuratore generale della Confederazione, poiché nell'articolo 26 della legge citata è espressamente fatto salvo il deferimento dell'istruzione e del giudizio alle autorità cantonali competenti.

9.44 Singole osservazioni relative al (nuovo) articolo 340ter CP

- La proposta di (nuovo) articolo *340ter capoverso 1 lettera a* CP comprende sia fattispecie nazionali complesse (cfr. "WEF-hack"), in relazione alle quali il foro può inizialmente risultare poco chiaro, sia reati internazionali che concernono più Cantoni, senza che vi sia un riferimento prevalente con uno di essi. Queste fattispecie possono essere affrontate da un'unità centrale e, se necessario, essere delegate a un Cantone.
- Il (nuovo) articolo *340ter capoverso 1 lettera b* CP è una novità, adatta ai casi in cui occorre condurre indagini nei confronti di numerosi autori di reati informatici analoghi, e in cui è indispensabile un'azione coordinata. Anche questa disposizione permette una delega ai Cantoni ai sensi dell'articolo 18bis PP.
- L'articolo *340ter capoverso 2* CP permette infine alle autorità cantonali di chiedere l'intervento delle autorità federali. Il Ministero pubblico della Confederazione può però respingere simili richieste se il perseguimento locale non solleva problemi. Nel prendere una tale decisione il Ministero pubblico della Confederazione deve valutare le circostanze concrete del singolo caso.

L'articolo *340ter capoverso 3* CP, analogamente all'articolo 340bis capoverso 3 CP, precisa che l'apertura di un'inchiesta determina automaticamente la competenza federale.

Alla luce delle sue proposte di regolamentazione sul piano del diritto penale, la commissione peritale si esprime in modo critico riguardo alle procedure legislative parallele attualmente in corso nell'ambito della criminalità in rete. Essa fornisce inoltre raccomandazioni per i prossimi passi legislativi da compiere in questo settore.

10. Procedure legislative parallele e ulteriori lavori legislativi nell'ambito della criminalità in rete

10.1 Parere in merito alle procedure legislative parallele

Parallelamente ai lavori della commissione peritale "Criminalità in rete", sono attualmente in corso diverse procedure legislative che toccano anche questioni sulle quali la presente commissione si è chinata. La commissione ritiene opportuno e urgente esprimere un parere in merito alla creazione di queste normative parallele, attirando l'attenzione sul rischio di contraddizioni tra il Codice penale e altre leggi federali.

10.11 Legge federale sul commercio elettronico

Nel rapporto esplicativo del 17 gennaio 2001 [262] relativo all'avamprogetto di legge federale sul commercio elettronico (revisioni parziali del Codice delle obbligazioni e della legge federale contro la concorrenza sleale), si legge tra l'altro:

> "Analogamente, anche gli eventuali adeguamenti del diritto della proprietà immateriale e della responsabilità civile e penale dei provider dipendono essenzialmente dall'evoluzione giuridica internazionale. In tale ambito non sussiste attualmente un bisogno d'intervento immediato sul piano legislativo. È possibile trovare soluzioni appropriate sulla base del diritto vigente".

La *commissione "Criminalità in rete"* non è dello stesso avviso, in quanto ritiene che sarebbe auspicabile esaminare in modo più approfondito le questioni inerenti alla responsabilità civile e alle sue limitazioni, in relazione alla trasmissione automatica di dati e alla loro messa a disposizione in rete [263]. Tali questioni potrebbero da un lato essere trattate nell'ambito dell'attuale processo legislativo concernente il commercio elettronico. In ragione della fondamentale importanza del problema, un'integrazione

[262] Reperibile all'indirizzo elettronico: www.ofj.admin.ch/themen/e-commerce/vn-ber-b-i.pdf.
[263] Cfr. capitolo 8, *in fine*, nonché capitolo 11, n. 11.33.

di tali questioni dovrebbe tuttavia portare a una nuova consultazione. D'altro lato, una limitazione differenziata della responsabilità per i diversi gruppi di provider sarebbe possibile anche nell'ambito dei lavori di revisione relativi alla *legge sul diritto d'autore* o alla *revisione del diritto in materia di responsabilità civile*.

10.12 Legge federale sulle lotterie e le scommesse

Il 31 marzo 2003 si è conclusa la *procedura di consultazione* concernente l'avamprogetto del 25 ottobre 2002 relativo alla revisione della legge federale sulle lotterie e le scommesse [264].

L'articolo 50 lettera d dell'avamprogetto ha il tenore seguente:

> „Art. 50 Delitti
>
> *[1] È punito con la detenzione fino a un anno o con la multa fino a un milione di franchi chiunque:*
> *...*
> *d. offre in qualità di fornitore di accesso (provider) giochi vietati dalla presente legge .*
>
> [2] Nei casi gravi la pena è la reclusione fino a cinque anni o la detenzione non inferiore a un anno. A tale pena può aggiungersi una multa fino a due milioni di franchi.
>
> [3] Chi agisce per negligenza è punito con una multa fino a 500 000 franchi.“

Il *rapporto esplicativo*, riguardo all'articolo 50 capoverso 1 lettera d dell'avamprogetto, afferma quanto segue:

> "Gli importi massimi delle multe superano quelli previsti dal diritto penale ordinario. Tali importi si giustificano a causa degli immensi interessi economici in gioco. Soltanto sanzioni pesanti possono indurre gli organizzatori svizzeri e stranieri a rispettare le prescrizioni legali e a non mettere in preventivo tali pene.
>
> La commissione è inoltre convinta che sarà possibile lottare efficacemente contro l'offerta di lotterie e scommesse non autorizzate su Internet soltanto se vengono puniti anche i fornitori d'accesso (provider)" [265].

La *commissione peritale "Criminalità in rete"* ha su questo punto un parere diverso. Dal punto di vista del diritto costituzionale e amministrativo, la commissione non ritiene ammissibili, poiché sproporzionati, gli obblighi di controllo imposti al fornitore d'accesso e derivanti da una simile disposizione penale. Dal profilo tecnico, la misura consistente in un blocco locale si rivela inefficace a causa delle numerose possibilità di elusione che il fornitore d'accesso non può controllare. La punibilità del fornitore d'accesso sarebbe non da ultimo in contraddizione anche con il diritto vigente in ambito europeo [266].

---

[264] Reperibile all'indirizzo elettronico: www.ofj.admin.ch/themen/lotterie/lg-rev/intro-i.htm.
[265] Rapporto esplicativo del 25 ottobre 2002 relativo all'avamprogetto di legge federale sulle lotterie e le scommesse, pag. 43.
[266] Cfr. l'art. 12 della direttiva sul commercio elettronico; capitolo 4.

Dal profilo del diritto penale, un obbligo di controllo o di blocco non risulterebbe soltanto sproporzionato, ma fonderebbe inoltre una punibilità per attività economiche assolutamente lecite, nonostante il fatto che il fornitore d'accesso contemplato dalla legge, diversamente da quanto avviene in ambito di riciclaggio di denaro, non abbia alcun contatto con chi gestisce la lotteria o la scommessa illegali, non conosca tale persona e non tragga beneficio alcuno dal suo agire.

L'impunità proposta dalla commissione peritale per la mera fornitura d'accesso ([nuovo] art. 27 n. 4 CP) deve valere anche per l'intero diritto penale accessorio (cfr. art. 333 cpv. 1 CP). Prevedendo una deroga nella legge federale sulle lotterie e le scommesse si rinuncerebbe senza ragione all'unità perseguita dalla nuova regolamentazione. L'articolo 50 lettera d del progetto di legge federale sulle lotterie e le scommesse andrebbe pertanto stralciato.

10.13 Legge federale concernente misure contro il razzismo, la tifoseria violenta e la propaganda violenta

Il 31 marzo 2003 si è conclusa la *procedura di consultazione* relativa alla legge federale concernente misure contro il razzismo, la tifoseria violenta e la propaganda violenta [267].

Tale normativa prevede una modifica della legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI, RS 120), dal tenore seguente:

> „Art.13bis Messa al sicuro, sequestro e confisca di materiale di propaganda (nuovo)
>
> [1] Le autorità di polizia e doganali mettono al sicuro, all'attenzione dell'Ufficio federale, il materiale che potrebbe servire a scopi propagandistici, indipendentemente da quantità, stato e natura, e il cui contenuto:
> a. è razzista; o
> b. incita concretamente e seriamente a utilizzare la violenza contro persone o gruppi di persone o a danneggiare il patrimonio o altri diritti di tali persone.
> [2] Se collaboratori dell'Ufficio federale trovano il rispettivo materiale, possono metterlo al sicuro anche direttamente.
> [3] In caso di sospetto di reato, le autorità che mettono al sicuro il materiale lo trasmettono alla competente autorità penale.
> [4] Negli altri casi, le autorità di polizia e doganali trasmettono il materiale all'Ufficio federale. Quest'ultimo decide in merito al sequestro e alla confisca. È applicabile la legge federale del 20 dicembre 1968 sulla procedura amministrativa.
> [5] In caso di diffusione via Internet di materiale di propaganda ai sensi del capoverso 1, l'Ufficio federale può raccomandare ai provider Internet il blocco delle relative pagine di Internet.

In merito al capoverso 5, che riveste particolare interesse nell'ambito da noi trattato, il relativo *rapporto* rileva quanto segue:

> "In merito all'articolo 13bis capoverso 5: sulla scorta delle raccomandazioni risultanti dalla consultazione degli uffici, il nuovo articolo prevede anche, per quanto concerne la

[267] Reperibile all'indirizzo elettronico: www.ejpd.admin.ch/doks/mm/2003/030212c-i.htm.

diffusione su Internet della propaganda giusta le lettere a e b, l'azione del competente Ufficio federale. Quest'ultimo può raccomandare ai competenti provider Internet il blocco della relativa propaganda. Tale blocco è effettuato soltanto per siti tenuti su computer all'estero. Nel caso di siti web svizzeri è presentata una denuncia al giudice penale".

Il rapporto del *Gruppo di lavoro "Estremismo di destra"* (GL Estremismo di destra) del settembre 2000 [268], che ha preceduto l'avamprogetto di legge, aveva d'altronde sottolineato che il perseguimento penale, per quanto riguarda i contenuti Internet su server europei, non poneva eccessivi problemi [269], ma che il blocco dei relativi contenuti da parte di fornitori di servizi Internet (svizzeri) comportava invece molteplici difficoltà di ordine tecnico [270].

Secondo il Gruppo di lavoro occorre pertanto raccomandare alle autorità competenti:

- di agire in futuro in collaborazione con i provider svizzeri, in modo da contrastare la diffusione in Internet di contenuti improntati all'estremismo di destra;
- di intraprendere gli sforzi necessari a livello internazionale per la creazione di una convenzione riguardante i contenuti vietati in Internet;
- di intensificare la pressione diplomatica sugli Stati che rappresentano il punto di partenza da cui simili contenuti si propagano [271].

Sulla base di tali raccomandazioni, la *commissione peritale "Criminalità in rete"* reputa senz'altro positiva una collaborazione delle autorità con i provider. Ritiene tuttavia inutile il capoverso 5 del nuovo articolo 13bis LMSI. Semplici raccomandazioni delle autorità competenti, che in caso di inottemperanza non comportano conseguenze penali, civili o amministrative, non necessitano di basi legali esplicite e sono già possibili in base alle norme in vigore attualmente.

Per le ragioni indicate, la competenza delle autorità federali di ordinare al fornitore d'accesso un blocco dei contenuti si rivelerebbe sproporzionata (cfr. n. 7.215), e non potrebbe quindi nemmeno fondarsi sul nuovo articolo 13bis capoverso 5 LMSI. Il commento alla norma contenuto nel rapporto esplicativo è impreciso e andrebbe pertanto corretto. Per evitare malintesi, la commissione peritale è favorevole allo stralcio del nuovo articolo 13bis capoverso 5 LMSI.

[268] Reperibile (in tedesco) all'indirizzo elettronico: www.bap.admin.ch/d/aktuell/berichte/bericht-d-ag-rex-d-01-s.pdf.
[269] Rapporto del GL "Estremismo di destra", pag. 28.
[270] Rapporto del GL "Estremismo di destra", pag. 41.
[271] Rapporto del GL "Estremismo di destra", pag. 44.

10.2 Altri lavori legislativi inerenti la criminalità in rete

All'inizio delle sue discussioni, la commissione peritale ha deciso *di procedere a tappe*. *La prima priorità* è stata data alla chiarificazione dei limiti della punibilità in caso di trasmissione e tenuta a disposizione automatiche dei dati in rete; andavano nel contempo esaminate le questioni parallele riguardanti il diritto pubblico e civile. La commissione ha pure trattato prioritariamente la questione della creazione di nuove condizioni quadro per un'*efficace lotta alla criminalità in Internet*.

Si trattava in primo luogo di centralizzare le competenze d'indagine e di istituire una centrale di coordinamento (clearing) a livello federale; in tal modo, senza estendere al di là del necessario le competenze della Confederazione, sarebbero garantiti una reazione rapida e un coordinamento internazionale in casi complessi. Occorreva allo stesso tempo introdurre strumenti di diritto penale che permettessero di eliminare le informazioni incriminate, purché fossero messe o tenute a disposizione in Svizzera. Questo obiettivo corrisponde a quello perseguito dalla mozione Pfisterer (cfr. n. 1.21) e al mandato assegnato dal DFGP alla commissione peritale (cfr. n. 1.3).

La commissione peritale ritiene che le sue proposte sono *solo un primo passo* sulla via che conduce a efficaci condizioni quadro penali e a un efficiente perseguimento penale della criminalità in rete. A questo primo passo ne dovranno seguire altri.

10.21 Adeguamento del diritto interno alla Convenzione sulla cibercriminalità

Occorre iniziare con gli adeguamenti legislativi resi necessari dalla ratifica della Convenzione sulla cibercriminalità (Convention sur la cybercriminalité, CCC) del 23 novembre 2001 (ETS n. 185) [272], di cui la Svizzera è uno dei primi 31 Stati firmatari. Questa Convenzione del Consiglio d'Europa rende necessarie diverse modifiche nel diritto penale interno e in particolare nella procedura penale.

10.211 Contenuto della Convenzione

La Convenzione sulla cibercriminalità persegue innanzitutto l'obiettivo di giungere a un'*armonizzazione delle disposizioni penali materiali* nei settori della criminalità informatica e di quella in rete [273]. In secondo luogo mira alla creazione di *strumenti unitari* sul piano del *diritto penale*, che permettano di effettuare indagini e di perseguire i reati informatici e quelli commessi in rete. In particolare essa si propone

[272] Il testo della Convenzione sulla cibercriminalità (in inglese e in francese) è reperibile all'indirizzo elettronico http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[273] Capitolo II, sezione 1 della Convenzione. Oltre alle infrazioni contro la riservatezza dei dati e dei sistemi informatici (art. 2-3 CCC), la Convenzione definisce anche le infrazioni relative all'integrità dei dati (art. 4 CCC), quelle relative all'integrità dei sistemi (art. 5 CCC), l'abuso dei dispositivi (art. 6 CCC), la falsificazione informatica (art. 7 CCC), la frode informatica (art. 8 CCC), le infrazioni relative alla pedopornografia (art. 9 CCC), e le infrazioni legate alle violazioni della proprietà intellettuale e ai diritti connessi (art. 10 CCC). Questa sezione contiene inoltre una disposizione concernente la responsabilità delle persone giuridiche (art. 12 CCC). Un *primo protocollo aggiuntivo* per l'armonizzazione delle norme penali materiali in ambito di *discriminazione razziale e xenofobia* è stato aperto alla firma il 28 gennaio 2003. La Svizzera non ha ancora sottoscritto questo protocollo.

di permettere e agevolare la puntuale preservazione in forma elettronica di mezzi di prova "precari" e di dati relativi al collegamento [274].

In terzo luogo la Convenzione tenta di istituire un *sistema di assistenza giudiziaria ed estradizione* più rapido ed efficiente per i reati tradizionali e per quelli informatici; essa mira a completare le convenzioni sull'assistenza giudiziaria e gli accordi bilaterali esistenti, o a crearne in caso di mancanza [275].

Sono previste anche *misure provvisorie*, come la conservazione rapida di dati informatici memorizzati (art. 29 CCC) o la rapida divulgazione di dati conservati e relativi al collegamento (art. 30 CCC).

Nel conclusivo capitolo IV della Convenzione (clausole standardizzate per accordi conclusi nell'ambito del Consiglio d'Europa), l'articolo 41 CCC prevede una *"clausola federale"* che la Svizzera è tenuta a rispettare. Secondo tale clausola, gli Stati federali possono riservarsi di rispettare gli obblighi in base al capitolo II, soltanto nella misura in cui questi siano compatibili con i principi fondamentali propri alla suddivisione interna delle competenze tra Governo centrale e entità territoriali. Se uno Stato federale avanza una simile riserva, deve nel contempo garantire un perseguimento penale completo ed efficace secondo i principi fondamentali del capitolo II. Poiché la riserva non può essere estesa al capitolo III, devono essere rispettati anche tutti gli obblighi relativi alla collaborazione internazionale [276].

10.212 Necessità di adeguamento

Il mandato conferito alla commissione peritale non avrebbe consentito, tenuto conto dei termini, di esaminare gli adeguamenti necessari della *procedura penale*, ancora di competenza dei Cantoni.

Occorre tener conto in questo contesto degli attuali lavori riguardanti il *Codice di procedura penale svizzero*, con i quali va coordinata l'attuazione delle direttive derivanti dalla Convenzione sulla cibercriminalità. Va considerata tuttavia anche la modifica della *legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni* (LSCPT, RS 780.1) e la relativa ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT, RS 780.11), anche se la Convenzione sulla cibercriminalità prevede poteri più ampi in relazione all'acquisizione dei cosiddetti dati marginali.
Oltre a ciò sarà necessario adeguare anche le *disposizioni della Parte speciale* del CP.

---

[274] Capitolo II, sezione 2 della Convenzione. Riveste particolare importanza il campo d'applicazione esteso di queste norme. Esse non sono applicabili soltanto ai reati previsti dagli articoli 2-11 CCC, ma anche a tutti i reati commessi per mezzo di sistemi informatici e a tutte le misure finalizzate alla preservazione dei mezzi di prova (art. 14, cpv. 2, lett. b e c CCC).
[275] Capitolo III della Convenzione.
[276] Cfr. in merito OFFICE FEDERAL DE LA JUSTICE, Rapport national de la Suisse sur la prévention et la lutte contre la cybercriminalité, Conférence sur la Cybercriminalité, Budapest, 22 novembre 2001; CHRISTIAN SCHWARZENEGGER: Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: Festschrift Trechsel, Zurigo 2002, pag. 305 segg. con ulteriori riferimenti.

La Convenzione sulla cibercriminalità prevede un quadro normativo che ammette spesso dichiarazioni (cfr. art. 40 CCC) o riserve (cfr. art. 42 CCC) da parte degli Stati firmatari, in modo da rendere possibile un'attuazione limitata. Pertanto, occorre innanzitutto determinare se per la Svizzera si debba perseguire una soluzione minima o un adeguamento il più completo possibile.

10.213 Raccomandazioni della commissione peritale

La commissione peritale raccomanda di chinarsi sui problemi posti dalla Convenzione sulla cibercriminalità, nell'ambito di un'estensione del mandato della commissione o nell'ambito di un'ulteriore commissione. Il risultato di tali lavori sarà integrato nel Codice penale, in una legge federale autonoma concernente le misure coercitive processuali in materia di criminalità in rete e nell'ambito della LSCPT/OSCPT.

Non ci si può attendere che i lavori legislativi relativi al Codice di procedura penale svizzero terminino in tempi brevi. Considerata l'urgenza di un'attuazione della Convenzione sulla cibercriminalità, che consentirà di perseguire in modo più efficiente la criminalità in rete (vedi n. 10.22), e visto il carattere speciale della materia, la commissione peritale ritiene opportuno procedere immediatamente ai preparativi per la ratifica di detta Convenzione. A livello cantonale gli strumenti procedurali necessari non andrebbero più resi operanti in modo indipendente.

10.22 Completamento della LSCPT [277] per la determinazione del luogo del reato

Il punto di riferimento principale per il perseguimento di attività e contenuti penalmente rilevanti in Internet è l'*indirizzo IP* [278], trasmesso in quasi ogni tipo di comunicazione Internet. Soltanto tale indirizzo permette, in caso di attività delittuose, di chiarire rapidamente la *competenza territoriale* e di adottare eventuali misure di preservazione dei mezzi di prova.

Se l'autore è collegato a Internet attraverso un *indirizzo IP* cosiddetto *statico*, in applicazione dell'articolo 14 LSCPT (in relazione con l'art. 27 lett. a OSCPT), anche le autorità di polizia elvetiche possono venire a conoscenza del nome e del luogo in cui risiede l'utente, anche al di fuori di un procedimento penale formale; in tale ambito viene fornita assistenza da parte del Servizio per compiti speciali (SCS), che sul piano amministrativo è subordinato al DATEC.

Nella maggior parte dei casi l'autore non dispone tuttavia di un indirizzo IP statico, ma il provider Internet da lui teleselezionato gli assegna un indirizzo per ogni visita in rete (il cosiddetto *indirizzo IP dinamico*). L'indirizzo dell'abitazione dell'utente è pertanto ottenibile sulla base di un'ingiunzione giudiziaria, e quindi soltanto nell'ambito di un procedimento penale formale (cfr. art. 24 lett. f OSCPT). Le indicazioni individuali relative all'indirizzo IP dinamico sono infatti sottoposte al segreto delle telecomunicazioni ai sensi dell'articolo 43 LTC. La competenza

[277] Legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (RS 780.1).

[278] Indirizzo *Internet Protocol*: numero univoco strutturato in quattro punti, assegnato a ogni dispositivo collegato a Internet.

territoriale cantonale può essere determinata nel presente contesto soltanto sulla base della sede del provider, ciò che in molti casi (in particolare per i grossi provider con clienti in tutto il Paese) porta a risultati insoddisfacenti e inefficienti.

Nell'interesse di un *perseguimento penale efficace* è tuttavia indispensabile che il centro di coordinamento per la lotta contro la criminalità su Internet (SCOCI), gestito da Cantoni e Confederazione, venga il più rapidamente possibile a conoscenza del luogo di teleselezione [279] anche *al di fuori di un procedimento penale formale*, affinché possa trasmettere il caso alle autorità competenti.

Nonostante questa informazione in sé non permetta di trarre conclusioni circa l'identità dell'utente, l'estensione e la durata del collegamento a Internet, sulla base della vigente LSCPT si parte dal presupposto che si tratti di *dati marginali*, ottenibili soltanto in base ai requisiti posti dall'articolo 3 in combinato disposto con l'articolo 5 LSCPT. Poiché la Convenzione sulla cibercriminalità esige una rapida preservazione dei dati relativi al collegamento (art. 16 CCC), per i quali prevede un livello di protezione leggermente inferiore rispetto ai *dati relativi al contenuto*, in occasione dei lavori di adeguamento (cfr. n. 10.21) occorrerà prioritariamente discutere su come strutturare, in una LSCPT riveduta, la distinzione tra dati marginali e dati relativi al contenuto.

Si dovrà tener presente che l'accesso agevolato a questi dati marginali - che potrebbe avvenire sulla base di una decisione, invece che di un ordine di sorveglianza– è di importanza capitale anche per la determinazione del luogo del reato, dal quale dipendono la sovranità penale e il foro; secondo la nuova regolamentazione delle competenze qui proposta ([nuovo] art. 340ter CP), in molti casi l'accesso sarà di competenza dello SCOCI.

[279] Si intende la connessione, telefonica o via cavo, a partire dalla quale l'utente si è collegato a Internet.

11. Riassunto

11.1 In generale

Dal profilo materiale, giuridico e politico la "criminalità in rete" è un tema complesso e *ricco di sfaccettature*.

La commissione peritale si è sforzata di ottenere una *visione d'insieme il più ampia possibile* sulla tematica e di chiarirne tutti gli aspetti essenziali. Essa ha nondimeno voluto individuare i *punti focali* del problema, esaminando attentamente determinati aspetti (cfr. n. 11.2) e trattandone altri in modo *meno approfondito* (cfr. n. 11.3).

Il fatto che la commissione abbia in particolare posto l'accento sul complesso tema del diritto penale (cfr. n. 11.2), è da ricollegare al mandato assegnatole, vertente in primo luogo sull'esame della responsabilità penale in Internet. Alla base dell'istituzione della commissione vi era soprattutto la volontà di chiarire la controversa questione della *responsabilità penale del provider Internet*. A ciò si aggiunge la *pedocriminalità* (insieme ad alcune altre forme di delinquenza), un problema attuale che coinvolge fortemente l'opinione pubblica e la politica e per il quale Internet è divenuto il principale vettore.

11.2 Diritto penale (capitoli 6 e 9)

11.21 Responsabilità penale

Problema

Il diritto penale vigente non prevede una regolamentazione chiara ed esplicita della responsabilità per contenuti illegali in Internet. Non è chiaro se e in quale misura le prescrizioni del diritto penale dei media e le regole generali del Codice penale siano applicabili. Un disciplinamento esplicito nella legge è pertanto opportuno.

Proposta di soluzione della commissione peritale

In sintonia con disposizioni estere che attuano la direttiva dell'Unione europea sul commercio elettronico (cfr. i riferimenti di diritto comparato nel capitolo 4), la commissione peritale propone nel capitolo 9 (soprattutto n. 9.2 e 9.3) *un nuovo disciplinamento nel Codice penale* (nuovi art. 27 e 322bis), secondo il quale:

- sul piano penale, l'autore e il *fornitore di contenuti* sono pienamente responsabili dei contenuti illegali a loro riconducibili;
- la responsabilità dell'*hosting provider* è limitata: egli è responsabile soltanto se non impedisce l'impiego di informazioni, sapendo con certezza che per mezzo di

esse è commesso un reato, malgrado sia in grado di impedirlo e ciò possa ragionevolmente essere preteso da lui, oppure quando omette di trasmettere alle autorità di perseguimento penale segnalazioni ricevute da terzi e riguardanti tali informazioni;

- il *fornitore d'accesso* non è penalmente responsabile dei contenuti delittuosi circolanti in rete.

11.22 Carattere internazionale della criminalità in rete

Problema

La criminalità in rete è un fenomeno planetario che non conosce confini. Spesso l'autore si trova all'estero, dove vigono basi legali talvolta molto diverse da quelle svizzere. Se si applicassero i consueti punti di collegamento che fondano la giurisdizione penale elvetica, tali atti non sarebbero penalmente perseguibili in Svizzera.

Proposta di soluzione della commissione peritale

- Come menzionato al n. 11.21, a determinate condizioni l'*hosting provider* che si trova in Svizzera deve potervi essere penalmente perseguito (cfr. capitolo 9, n. 9.3).
- Tale approccio normativo *attenua* la citata problematica relativa al carattere internazionale di questo tipo di criminalità. Infatti, nella misura in cui l'hosting provider sito in Svizzera ospita anche contenuti esteri, questi possono essere giudicati in base al diritto penale svizzero.
- La commissione peritale raccomanda inoltre di dare rapidamente inizio all'*adeguamento del diritto svizzero* alle direttive della *Convenzione sulla cibercriminalità*, firmata dalla Svizzera (cfr. capitolo 10, n. 10.2).

11.23 A chi compete il perseguimento penale?

Problema

Al fine di individuare rapidamente i contenuti Internet e di essere in grado di adottare le relative contromisure, occorrono strumenti adeguati a livello di polizia e di giustizia penale. In ragione del marcato carattere internazionale della criminalità in rete e dell'incalcolabile quantità di contenuti, i Cantoni ai quali già oggi incombe il perseguimento e il giudizio di tali reati non dispongono delle risorse e delle capacità necessarie.

Proposta di soluzione della commissione peritale

- Già a partire dal 1° gennaio 2003, esiste in seno all'Ufficio federale di polizia un organo preposto al monitoraggio Internet e al coordinamento delle comunicazioni provenienti da privati (Servizio di coordinamento per la lotta contro la criminalità su Internet, SCOCI). La Confederazione, in collaborazione con i Cantoni, deve continuare ad assolvere questo compito.

- Inoltre, in determinati casi e sulla base delle norme previste dal cosiddetto "Progetto efficienza" [280], la Confederazione dovrebbe avere la possibilità di condurre autonomamente i corrispondenti procedimenti penali (nuovo art. 340ter CP; cfr. capitolo 9, soprattutto n. 9.4).

11.3 Altri aspetti trattati

Anche se la commissione peritale ha dato la priorità all'ambito penale, non ha trascurato altri aspetti della criminalità in rete, legati o no al diritto penale.

11.31 Controlli tecnici di Internet (cfr. capitolo 3)

I mezzi tecnici a disposizione permettono in parte di effettuare controlli dell'accesso a Internet e dei suoi contenuti. Ma poiché Internet è stata concepita come rete organizzata in modo decentrato e ampiamente accessibile, simili controlli sono molto dispendiosi. Per lo stesso motivo, i controlli e le misure di blocco possono facilmente essere elusi.

11.32 Misure di diritto amministrativo (cfr. capitolo 7)

Al fine di prevenire lesioni di beni giuridici in reti di comunicazione elettronica, sarebbe ipotizzabile l'introduzione di misure amministrative che integrino il diritto penale. Il diritto vigente non prevede alcuna base legale in tal senso. Questo tipo di misure si scontrano nella maggior parte dei casi con limiti pratici o costituzionali, in particolare con i limiti derivanti dai diritti fondamentali relativi alla libera comunicazione e al principio costituzionale della proporzionalità degli interventi delle autorità (cfr. in merito anche il capitolo 5). Nelle sue proposte la Commissione rinuncia pertanto a misure fiancheggiatrici di ordine amministrativo.

11.33 Diritto civile (cfr. capitolo 8*)*

In relazione alla criminalità in rete, il diritto penale e la responsabilità civile presentano diversi punti in comune. Tra questi due ambiti giuridici vi sono tuttavia anche delle differenze, che risultano soprattutto dalle diverse nozioni di colpa (in particolare a causa delle pretese di rimozione e inibitorie esistenti nel diritto civile e indipendenti dalla colpa, o in relazione ad aspetti specifici della procedura civile).

La commissione auspica che determinate questioni sollevate nel presente ambito vengano chiarite a livello legislativo. Ritiene tuttavia che gli attuali progetti di legislazione e revisione rappresentino la sede opportuna e adeguata in cui valutare tali questioni (ad es. legislazione concernente il commercio elettronico o la revisione e l'unificazione del diritto della responsabilità civile).

[280] Provvedimenti intesi a migliorare l'efficienza e la legalità nel procedimento penale (Messaggio FF 1998, 1095 segg. Modifica del Codice penale svizzero del 22 dicembre 1999, in vigore dal 1° gennaio 2002, RU 2001, 3071).

Allegato

A – Modifiche proposte nella mozione Pfisterer (motivazione)

6. Punibilità delle reti di telecomunicazione e dei mass media

Art. 27 Punibilità dei mass media

[1] Se un reato è commesso mediante pubblicazione in un mezzo di comunicazione sociale e consumato per effetto della pubblicazione, solo l'autore dell'opera è punito, fatti salvi l'articolo 27ter e le disposizioni che seguono.

Cpv. 2-4 (immutati)

Art. 27bis Tutela delle fonti
(immutato)

Art. 27ter Punibilità delle reti di telecomunicazione

[1] Se un reato è commesso mediante trasmissione, messa o tenuta a disposizione di informazioni, segnatamente contenuti, in una rete di telecomunicazioni, solo l'offerente di tali informazioni è punibile, fatte salve le disposizioni che seguono.
Se l'offerente procede a un controllo redazionale dell'informazione ai sensi dell'articolo 27 capoverso 2 CP, è punibile giusta gli articoli 27 e 322bis CP.

[2] Se un reato è commesso mediante informazioni di terzi, segnatamente contenuti, è punibile solo chi tiene a disposizione tali informazioni in una rete di telecomunicazioni qualora questi si astenga in malafede dall'impedire l'utilizzazione delle informazioni benché ne abbia la possibilità tecnica e il fatto sia ragionevolmente esigibile.

[3] Chi procura semplicemente l'accesso a informazioni di terzi, segnatamente contenuti di terzi, in una rete di telecomunicazioni, non è punibile, a condizione che:
a. non proceda alla trasmissione dell'informazione;
b. non abbia scelto i destinatari delle informazioni trasmesse;
c. non abbia scelto o modificato le informazioni trasmesse.
Una memorizzazione automatica e di breve durata di informazioni di terzi in seguito a una trasmissione automatizzata è considerata fornitura dell'accesso.

Art. 27quater Riserva di altre leggi

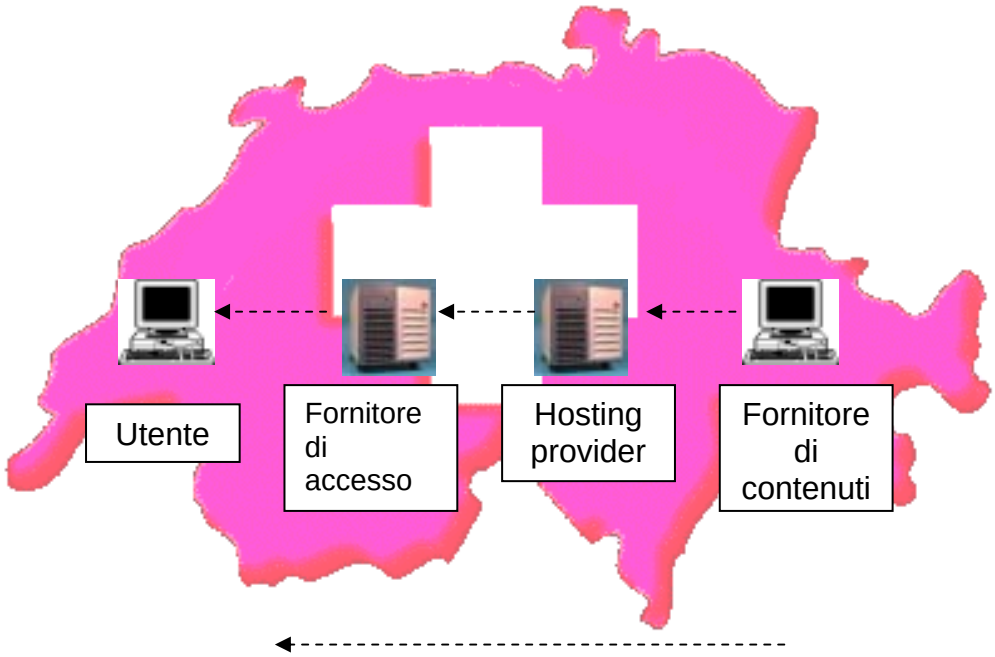
L'articolo 27ter disciplina compiutamente la responsabilità di diritto penale nelle reti di telecomunicazione. Gli obblighi di togliere o bloccare l'utilizzazione di informazioni secondo gli atti generali della Confederazione e dei Cantoni rimangono invariati, se le persone menzionate all'articolo 27ter CP pervengono legittimamente alla conoscenza di tali informazioni e un blocco tecnico sia possibile e ragionevolmente esigibile.

Art. 340ter

Sono sottoposti alla giurisdizione federale altri reati nelle reti di telecomunicazione (art. 27ter e 27quater).

B – Esempi relativi al capitolo 6, n. 6.4

Ipotesi 1: tutti gli attori agiscono in Svizzera



Caso 1: immagini di carattere pedopornografico nel www

• ***Diritto penale dei media***: secondo il Tribunale federale non è applicabile; la dottrina dominante è tuttavia di altro avviso (cfr. n. 6.2).
• ***Fornitore di contenuti***: il suo reato è commesso in Svizzera, a cui spetta pertanto la sovranità penale in base al principio della territorialità (cfr. n. 6.41); il reato principale consiste nel rendere accessibili i contenuti, secondo l'articolo 197 numero 3 CP.
• ***Hosting provider***: è correo per avere reso accessibili i contenuti ai sensi dell'articolo 197 numero 3 CP, o complice per aver contribuito alla commissione del reato principale (vi è incertezza nei due casi, cfr. n. 6.3). In entrambe le varianti la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).
• ***Fornitore di accesso***: è correo per avere reso accessibili i contenuti ai sensi dell'articolo 197 numero 3 CP, o complice per aver contribuito alla commissione del reato principale (entrambe le ipotesi sono da respingere, ma la questione è controversa, cfr. n. 6.3). In entrambe le varianti la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).
• ***Utente***: è autore principale se l'immagine viene memorizzata sul suo disco rigido (possesso di pedopornografia, art. 197 n. 3bis CP). Il reato è commesso in Svizzera, a cui spetta pertanto la sovranità penale in base al principio della territorialità (cfr. n. 6.41).

Caso 2: istigazione alla commissione di un incendio mediante la partecipazione a un gruppo di discussione

• ***Diritto penale dei media***: applicabile (cfr. n. 6.1).
• ***Fornitore di contenuti***: commette il reato principale (pubblica istigazione ai sensi dell'art. 259 cpv. 1 CP). Il reato è commesso in Svizzera, a cui spetta la sovranità penale in base al principio della territorialità (cfr. n. 6.41).
• ***Hosting provider***: il diritto penale dei media è applicabile se l'hosting provider è considerato divulgatore ai sensi dell'articolo 27 CP: in tal caso non vi è punibilità, poiché è possibile perseguire l'autore; in caso contrario l'hosting provider può essere considerato complice per aver contribuito alla commissione del reato principale (non vi è chiarezza, cfr. n. 6.3). A causa del carattere accessorio della complicità, si applica il diritto del luogo di commissione del reato principale (Svizzera); pertanto la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).
• ***Fornitore di accesso***: il diritto penale dei media è applicabile se il fornitore di accesso è considerato divulgatore ai sensi dell'articolo 27 CP: in tal caso non vi è punibilità, poiché è possibile perseguire l'autore; in caso contrario il fornitore di accesso può essere considerato complice per aver contribuito alla commissione del reato principale (ipotesi da respingere, cfr. n. 6.3). A causa del carattere accessorio della complicità, si applica il diritto del luogo di commissione del reato principale (Svizzera); pertanto la sovranità penale si fonda sul principio di territorialità (cfr. n. 6.41).
• ***Utente***: esente da pena.

Caso 3: discriminazione razziale in testi pubblicati nel www

• ***Diritto penale dei media***: la sua applicabilità è controversa (sarebbe piuttosto da negare) [281].
• ***Fornitore di contenuti***: non è chiaro se sia autore del reato principale, consistente nella propagazione pubblica ai sensi dell'articolo 261bis capoverso 2 CP [282]. Il reato è commesso in Svizzera, e quindi la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).
• ***Hosting provider***: il suo atto viene valutato in base al diritto penale svizzero, purché l'incoraggiamento alla commissione del reato principale sia ammissibile in quanto variante indipendente dell'articolo 261bis capoverso 3 CP (non vi è chiarezza, cfr. n. 6.3). Nella misura in cui la complicità viene ammessa, in ragione del suo carattere accessorio l'atto viene giudicato secondo il diritto del luogo di commissione del reato principale, ossia la Svizzera.

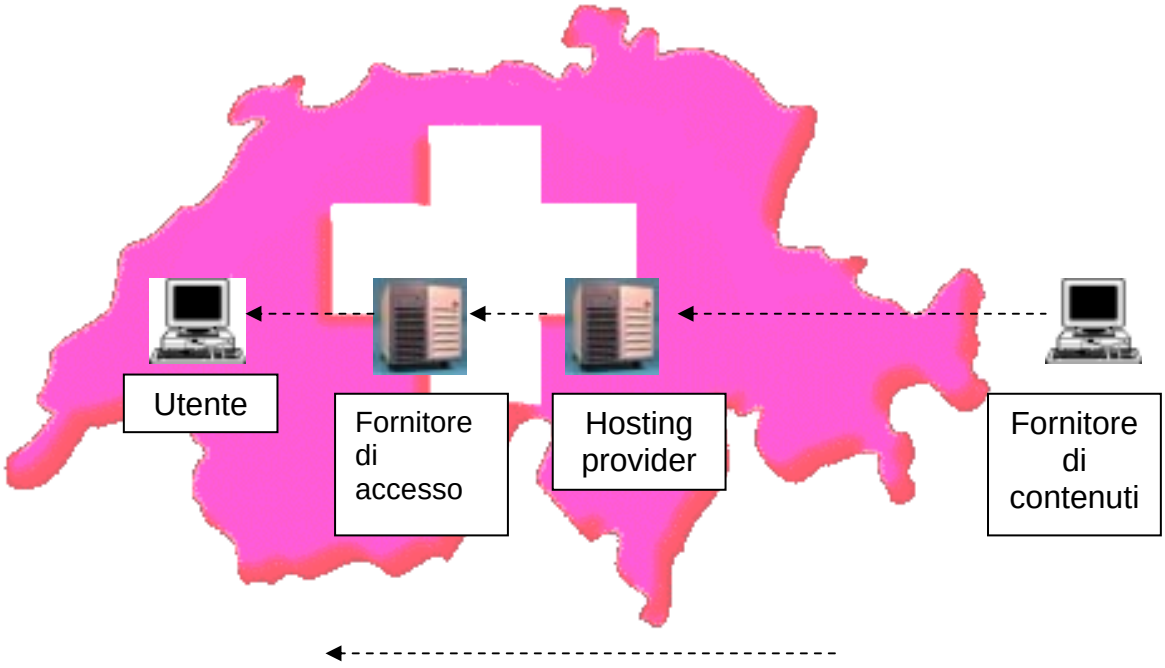
---

[281] Per un riassunto delle opinioni contrastanti: RIKLIN/STRATENWERTH (bibl.), pag. 15 con note. Nella DTF 125 IV 206 segg., il Tribunale federale non si è espresso in merito alla classificazione dell'articolo 261bis capoverso 2 CP.

[282] In Svizzera non è ancora stato chiarito se la divulgazione è compiuta soltanto da chi trasmette attivamente informazioni a un gruppo di persone più ampio o se, per realizzare oggettivamente la fattispecie, è sufficiente il fatto di mettere tali informazioni a disposizione su un server web (cfr. PETER VON INS/PETER-RENÉ WYDER, in: Niggli/Wiprächtiger, StGB Kommentar, Basilea 2003, art. 179, n. 41: "Se vi è comunicazione, vi è trasmissione a terzi"). Secondo una controversa decisione della Corte federale di giustizia tedesca, la divulgazione implica il fatto di rendere accessibile: ciò che viene reso accessibile è precisamente un'informazione, concretamente "richiamata" almeno una volta da un utente (vedi decisione del 27.6.2001 della Corte federale di giustizia – 1 StR 66/01 Erw. III.3.b)bb).

• ***Fornitore di accesso***: il suo atto viene valutato in base al diritto penale svizzero, purché l'incoraggiamento alla commissione del reato principale sia ammissibile in quanto variante indipendente dell'articolo 261bis capoverso 3 CP (non vi è chiarezza, cfr. n. 6.3). Nella misura in cui la complicità viene ammessa, in ragione del suo carattere accessorio l'atto viene giudicato secondo il diritto del luogo di commissione del reato principale, ossia la Svizzera
• ***Utente***: esente da pena.

Ipotesi 2: il fornitore di contenuti agisce all'estero, mentre tutti gli altri attori si trovano in Svizzera



Caso 1: immagini a carattere pedopornografico nel www

• ***Diritto penale dei media***: secondo il Tribunale federale non è applicabile; la dottrina dominante è tuttavia di altro avviso (cfr. n. 6.2).
• ***Fornitore di contenuti***: reato commesso all'estero; in caso di reati di messa in pericolo astratta, non vi può essere un nesso di collegamento con un evento che si produce in Svizzera. La sovranità penale non può quindi derivare né dal principio della territorialità (cfr. n. 6.42), né da quello della competenza universale (art. 6bis CP)[283], e il fornitore di contenuti non è perseguibile in Svizzera. Può tuttavia essere accordata l'assistenza giudiziaria [284].
• ***Hosting provider***: il suo agire viene giudicato secondo il diritto svizzero, purché possa essere considerato autore (o coautore) del reato previsto dall'articolo 197

[283] Diversamente da quanto previsto dall'articolo 5 della nuova parte generale del CP.
[284] Resta ancora possibile un nesso con il principio della personalità attiva, sancito dall'articolo 6 numero 1 CP, nel caso in cui il fornitore di contenuti sia di nazionalità elvetica e soggiorni in Svizzera (dopo aver commesso il reato all'estero).

numero 3 CP (il fatto di avere reso i contenuti accessibili). Se ha contribuito alla commissione del reato principale e viene quindi considerato complice, il suo atto assume carattere accessorio al reato principale e non può quindi essere perseguito in Svizzera. L'hosting provider sarebbe in tal caso perseguibile in base al diritto del luogo in cui è stato commesso il reato principale (nelle due ipotesi non vi è chiarezza, cfr. n. 6.3).
• ***Fornitore di accesso***: il suo agire viene giudicato secondo il diritto svizzero, purché possa essere considerato autore (o coautore) del reato previsto dall'articolo 197 numero 3 CP (il fatto di avere reso i contenuti accessibili). Se ha contribuito alla commissione del reato principale e viene quindi considerato complice, il suo atto assume carattere accessorio al reato principale e non può quindi essere perseguito in Svizzera. L'hosting provider sarebbe in tal caso perseguibile in base al diritto del luogo in cui è stato commesso il reato principale (entrambe le soluzioni andrebbero respinte, ma non vi è chiarezza, cfr. n. 6.3).
• ***Utente***: è autore principale se l'immagine viene memorizzata sul suo disco rigido (possesso di pedopornografia, art. 197 n. 3^{bis} CP). Il reato è commesso in Svizzera, a cui spetta pertanto la sovranità penale in base al principio della territorialità (cfr. n. 6.41).

Caso 2: istigazione alla commissione di un incendio mediante la partecipazione a un gruppo di discussione

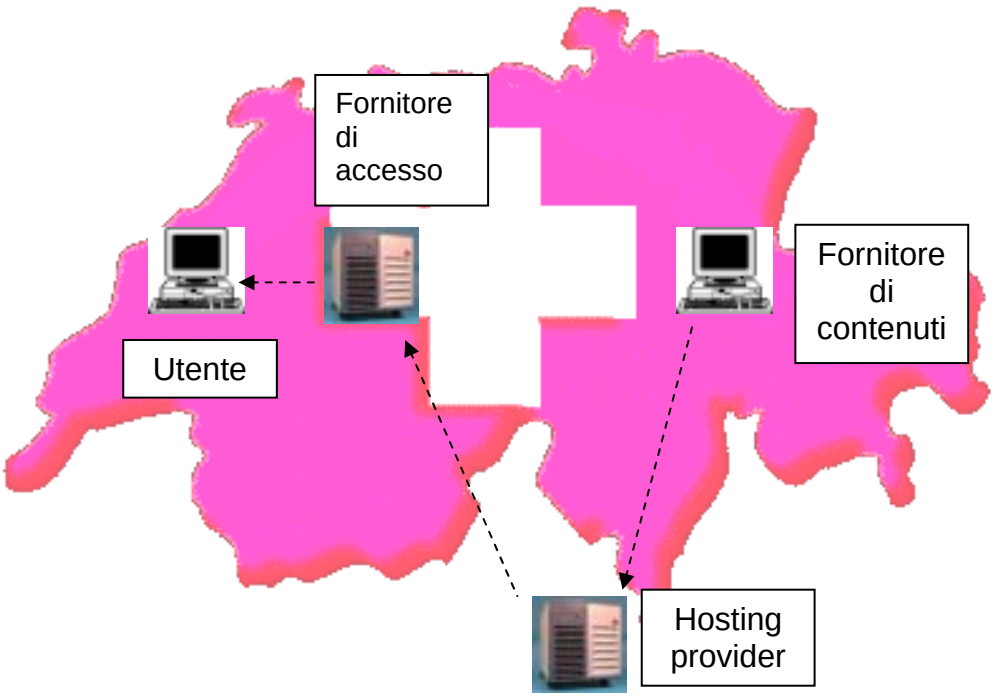
• ***Diritto penale dei media***: applicabile (cfr. n. 6.1).
• ***Fornitore di contenuti***: reato commesso all'estero; nel caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce in Svizzera, e quindi la sovranità penale non può fondarsi sul principio di territorialità (cfr. n. 6.42). Il fornitore di contenuti non è quindi perseguibile in Svizzera.
• ***Hosting provider***: il reato è commesso in Svizzera (art. 3 in relazione con l'art. 7 CP), e quindi la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41). C'è chi sostiene che la punibilità è da valutare in funzione dell'articolo 27 capoverso 2 in relazione con l'articolo 322^{bis} CP, poiché non è possibile agire nei confronti dell'autore, e l'hosting provider è considerato come una persona responsabile della pubblicazione. Secondo altri, il diritto penale dei media non è applicabile. Se la complicità dovesse entrare in considerazione, l'hosting provider non potrebbe essere perseguito in Svizzera; può essere accordata l'assistenza giudiziaria. Secondo altri ancora, non vi è punibilità secondo l'articolo 27 CP, a causa del privilegio del divulgatore (non vi è chiarezza, cfr. n. 6.43).
• ***Fornitore di accesso***: il reato è commesso in Svizzera (art. 3 in relazione con l'art. 7 CP), e quindi la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41). C'è chi sostiene che l'impunità si basa sull'articolo 27 capoverso 2 CP, poiché è possibile agire contro l'hosting provider; secondo altri, il diritto penale dei media non è applicabile. Se la complicità dovesse entrare in considerazione, il fornitore d'accesso non potrebbe essere perseguito in Svizzera; può essere accordata l'assistenza giudiziaria. Secondo altri ancora, non vi è punibilità secondo l'articolo 27 CP a causa del privilegio del divulgatore (non vi è chiarezza, cfr. n. 6.43).
• ***Utente***: esente da pena.

Caso 3: discriminazione razziale in testi pubblicati nel www

• ***Diritto penale dei media***: la sua applicabilità è controversa (sarebbe piuttosto da negare).
• ***Fornitore di contenuti***: reato commesso all'estero; per semplici reati di comportamento non è dato un nesso di collegamento legato a un evento che si produce in Svizzera, e quindi la sovranità penale non può fondarsi sul principio della territorialità (cfr. n. 6.42); il fornitore di contenuti non è quindi perseguibile in Svizzera, può essere accordata l'assistenza giudiziaria [285].
• ***Hosting provider***: se si ammette che il suo atto ha favorito la commissione del reato principale, costituendo quindi una variante indipendente dell'articolo 261bis capoverso 3 CP, verrà giudicato secondo il diritto penale svizzero (non vi è chiarezza, cfr. n. 6.3). Se viene ammessa la complicità, in ragione del suo carattere accessorio l'atto viene quindi giudicato secondo il diritto del luogo in cui è stato commesso il reato principale; non vi è in tal caso sovranità penale della Svizzera.
• ***Fornitore di accesso***: se si ammette che il suo atto ha favorito la commissione del reato principale, costituendo quindi una variante indipendente dell'articolo 261bis capoverso 3 CP, verrà giudicato secondo il diritto penale svizzero. Se viene ammessa la complicità, in ragione del suo carattere accessorio l'atto viene quindi giudicato secondo il diritto del luogo in cui è stato commesso il reato principale; non vi è in tal caso sovranità penale della Svizzera (entrambe le soluzioni da respingere; non vi è chiarezza, cfr. n. 6.3).
• ***Utente***: esente da pena.

[285] A.M. SCHWARZENEGGER, ABSTRAKTE GEFAHR (bibl.), pag. 252. Cfr. la dottrina tedesca, secondo cui tutti i reati d'espressione sono considerati reati d'evento: è pertanto possibile riallacciarsi all'evento ai sensi dell'articolo 9 capoverso 1, 3^{a} alternativa del Codice penale tedesco, THOMAS FUHR: Die Äusserung im Strafgesetzbuch, Berlino 2001, 175 segg. e 188 segg. con note; THEODOR LENCKNER – in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 26^{a} ed., Monaco 2001, § 185 n. 12 e § 186 n. 8 in fine (esempio dell'ingiuria e della diffamazione).

Ipotesi 3: l'hosting provider agisce all'estero, mentre tutti gli altri attori si trovano in Svizzera



Caso 1: immagini di carattere pedopornografico nel www

• ***Diritto penale dei media***: secondo il Tribunale federale non è applicabile; la dottrina dominante è tuttavia di altro avviso (cfr. n. 6.2).
• ***Fornitore di contenuti***: il reato è stato commesso in Svizzera, pertanto la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41); il fornitore di contenuti è l'autore principale del reato previsto dall'articolo 197 numero 3 CP (il fatto di rendere accessibili i contenuti).
• ***Hosting provider***: se è considerato (co)autore del reato previsto dall'articolo 197 numero 3 CP (il fatto di rendere accessibili i contenuti), il suo agire viene giudicato secondo il diritto del luogo in cui tale reato è stato commesso, ossia all'estero; non vi è quindi sovranità penale svizzera. Se l'hosting provider ha favorito la commissione del reato principale, ed è quindi considerato complice, il suo agire assume un carattere accessorio e viene quindi giudicato secondo il diritto penale svizzero (in entrambi i casi non vi è chiarezza, cfr. n. 6.3) [286].
• ***Fornitore di accesso***: se è considerato (co)autore del reato previsto dall'articolo 197 numero 3 CP (il fatto di rendere accessibili i contenuti), il suo agire viene giudicato secondo il diritto penale svizzero. Se il fornitore di accesso ha favorito la

[286] Resta ancora possibile un nesso con il principio della personalità attiva, sancito dall'articolo 6 numero 1 CP, nel caso in cui il responsabile del server web sia di nazionalità elvetica e soggiorni in Svizzera.

commissione del reato principale, ed è quindi considerato complice, il suo agire assume un carattere accessorio e viene quindi pure giudicato secondo il diritto penale svizzero (entrambe le soluzioni da respingere, tuttavia non vi è chiarezza, cfr. n. 6.3).
• ***Utente***: è autore principale se le immagini sono memorizzate sul suo disco rigido (possesso di pedopornografia, art. 197 n. 3bis CP). Il reato è stato commesso in Svizzera, pertanto la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).

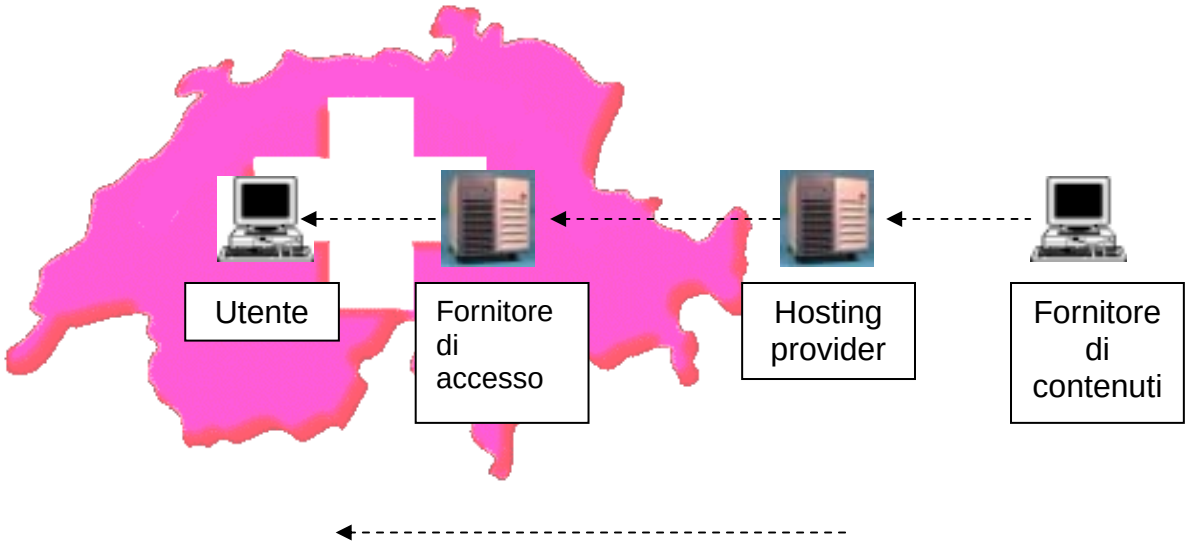
Caso 2: istigazione alla commissione di un incendio mediante la partecipazione a un gruppo di discussione

• ***Diritto penale dei media***: applicabile (cfr. n. 6.1).
• ***Fornitore di contenuti***: il reato è commesso in Svizzera, pertanto la sovranità penale elvetica si fonda sul principio della territorialità (cfr. n. 6.41); è autore principale di pubblica istigazione ai sensi dell'articolo 259 capoverso 1 CP.
• ***Hosting provider***: se l'hosting provider ha favorito la commissione del reato principale, ed è quindi considerato complice, il suo agire assume un carattere accessorio e viene quindi giudicato secondo il diritto penale svizzero. Secondo altri, sulla base dell'articolo 27 (l'hosting provider sarebbe considerato divulgatore) non vi è sovranità penale.
• ***Fornitore di accesso***: c'è chi sostiene che è esente da pena sulla base dell'articolo 27 capoverso 1 CP, poiché è possibile agire contro l'autore. Secondo altri il diritto penale dei media non sarebbe applicabile, e non andrebbe ammessa nemmeno la complicità (cfr. n. 6.3).
• ***Utente***: esente da pena.

Caso 3: discriminazione razziale in testi pubblicati nel www

• ***Diritto penale dei media***: la sua applicabilità è controversa (sarebbe piuttosto da negare).
• ***Fornitore di contenuti***: è autore principale per avere pubblicamente propagato i contenuti ai sensi dell'articolo 261bis capoverso 2 CP. Il reato è commesso in Svizzera, pertanto la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).
• ***Hosting provider***: se si ammette che il suo atto ha favorito la commissione del reato principale, costituendo quindi una variante indipendente dell'articolo 261bis capoverso 3 CP, il suo agire è giudicato secondo la legge vigente nel luogo di commissione; non vi è quindi sovranità penale svizzera. Se viene ammessa la complicità, il suo agire ha un carattere accessorio rispetto al reato principale e viene quindi giudicato secondo il diritto svizzero.
• ***Fornitore di accesso***: se si ammette che il suo atto ha favorito la commissione del reato principale, costituendo quindi una variante indipendente dell'articolo 261bis capoverso 3 CP, il suo agire è giudicato secondo il diritto penale svizzero. Se viene ammessa la complicità, il suo agire ha un carattere accessorio rispetto al reato principale e viene quindi pure giudicato secondo il diritto svizzero (entrambe le soluzioni andrebbero respinte).
• ***Utente***: esente da pena.

Ipotesi 4: il fornitore di contenuti e l'hosting provider agiscono all'estero, mentre il fornitore di accesso e l'utente si trovano in Svizzera



Caso 1: immagini a carattere pedopornografico nel www

• ***Diritto penale dei media***: secondo il Tribunale federale non è applicabile; la dottrina dominante è tuttavia di altro avviso (cfr. n. 6.2).
• ***Fornitore di contenuti***: reato commesso all'estero; in caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce in Svizzera. La sovranità penale non può quindi derivare né dal principio della territorialità (cfr. n. 6.42), né da quello della competenza universale (art. 6bis CP)[287], e il fornitore di contenuti non è perseguibile in Svizzera. Può essere accordata l'assistenza giudiziaria [288].
• ***Hosting provider***: reato commesso all'estero; in caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce in Svizzera; la sovranità penale non può quindi fondarsi sul principio della territorialità (cfr. n. 6.42), e può soltanto essere accordata l'assistenza giudiziaria.
• ***Fornitore di accesso***: se è considerato (co)autore del reato previsto dall'articolo 197 numero 3 CP (il fatto di rendere accessibili i contenuti), è applicabile il Codice penale svizzero. Se il fornitore di accesso ha favorito la commissione del reato principale, ed è quindi considerato complice, il suo agire assume un carattere accessorio e viene quindi giudicato secondo il diritto del luogo in cui è stato commesso il reato principale; non vi è pertanto sovranità penale svizzera. Può soltanto essere accordata l'assistenza giudiziaria.
• ***Utente***: è autore principale se le immagini sono memorizzate sul suo disco rigido (possesso di pedopornografia, art. 197 n. 3bis CP). Il reato è stato commesso in Svizzera, pertanto la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).

---

[287] Resta ancora possibile un nesso con il principio della personalità attiva, sancito dall'articolo 6 numero 1 CP, nel caso in cui il responsabile del server web sia di nazionalità elvetica e soggiorni in Svizzera.
[288] Diversamente da quanto previsto dall'articolo 5 della nuova parte generale del CP.

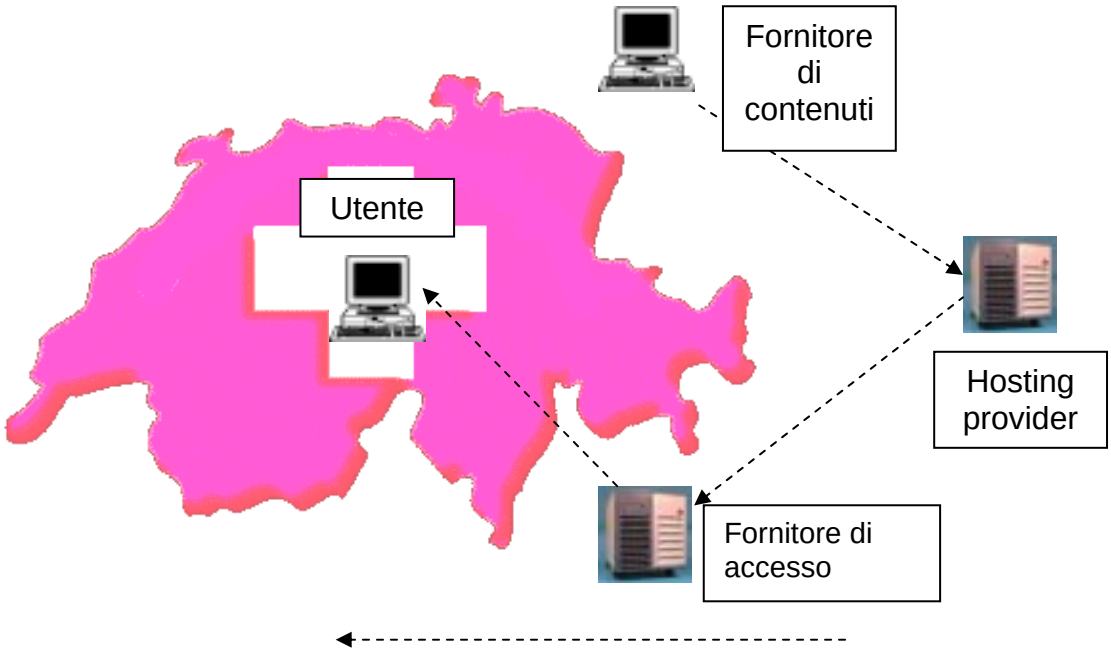
Caso 2: istigazione alla commissione di un incendio mediante la partecipazione a un gruppo di discussione

• ***Diritto penale dei media***: applicabile (cfr. n. 6.1).
• ***Fornitore di contenuti***: reato commesso all'estero; la sovranità penale non può pertanto fondarsi sul principio della territorialità (cfr. n. 6.42), e il fornitore di contenuti non è quindi perseguibile in Svizzera. Può essere accordata l'assistenza giudiziaria.
• ***Hosting provider***: reato commesso all'estero; in caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce in Svizzera, per cui la sovranità penale non può fondarsi sul principio della territorialità (cfr. n. 6.42). Può soltanto essere accordata l'assistenza giudiziaria.
• ***Fornitore di accesso***: reato commesso in Svizzera, pertanto la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41). C'è chi sostiene che la punibilità è da valutare in funzione dell'articolo 27 capoverso 2 in relazione con l'articolo 322bis CP, poiché non è possibile agire nei confronti dell'autore e il fornitore d'accesso è considerato come una persona responsabile della pubblicazione. Secondo altri, il diritto penale dei media non è applicabile. Se la complicità dovesse entrare in considerazione, il fornitore d'accesso non potrebbe essere perseguito in Svizzera; può essere accordata l'assistenza giudiziaria. Secondo altri, secondo l'articolo 27 CP l'hosting provider non sarebbe in linea di principio punibile (poiché divulgatore; non vi è chiarezza in merito, cfr. n. 6.43).
• ***Utente***: esente da pena.

Caso 3: discriminazione razziale in testi pubblicati nel www

• ***Diritto penale dei media***: la sua applicabilità è controversa (sarebbe piuttosto da negare).
• ***Fornitore di contenuti***: reato commesso all'estero; per semplici reati di comportamento non è dato un nesso di collegamento legato a un evento che si produce in Svizzera, e quindi la sovranità penale non può fondarsi sul principio della territorialità (cfr. n. 6.42); il fornitore di contenuti non è quindi perseguibile in Svizzera, e può essere accordata l'assistenza giudiziaria.
• ***Hosting provider***: reato commesso all'estero; per semplici reati di comportamento non è dato un nesso di collegamento legato a un evento che si produce in Svizzera, e quindi la sovranità penale non può fondarsi sul principio della territorialità (cfr. n. 6.42); l'hosting provider non è quindi perseguibile in Svizzera, e può essere accordata l'assistenza giudiziaria.
• ***Fornitore di accesso***: se si ammette che il suo atto ha favorito la commissione del reato principale, costituendo quindi una variante indipendente dell'articolo 261bis capoverso 3 CP (poco chiaro, cfr. n. 6.3), e considerando che il suo reato è stato commesso in Svizzera, la sovranità elvetica si fonda sul principio della territorialità (cfr. n. 6.41). Se si ammette la complicità, essa assume un carattere accessorio al reato principale, e l'agire del fornitore di accesso viene giudicato secondo il diritto del luogo in cui il reato è stato commesso; non vi è quindi sovranità penale svizzera. Può essere accordata l'assistenza giudiziaria.
• ***Utente***: esente da pena.

Ipotesi 5: soltanto l'utente agisce in Svizzera, mentre tutti gli altri attori si trovano all'estero



Caso 1: immagini di carattere pedopornografico nel www

• ***Diritto penale dei media***: secondo il Tribunale federale non è applicabile; la dottrina dominante è tuttavia di altro avviso (cfr. n. 6.2).
• ***Fornitore di contenuti***: reato commesso all'estero; in caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce in Svizzera. La sovranità penale non può quindi derivare né dal principio della territorialità (cfr. n. 6.42), né da quello della competenza universale (art. 6bis CP)[289], e il fornitore di contenuti non è perseguibile in Svizzera. Può essere accordata l'assistenza giudiziaria [290].
• ***Hosting provider***: come il fornitore di contenuti.
• ***Fornitore di accesso***: come il fornitore di contenuti.
• ***Utente***: è autore principale se le immagini sono memorizzate sul suo disco rigido (possesso di pedopornografia, art. 197 n. 3bis CP). Il reato è stato commesso in Svizzera, pertanto la sovranità penale si fonda sul principio della territorialità (cfr. n. 6.41).

Caso 2: istigazione alla commissione di un incendio mediante la partecipazione a un gruppo di discussione

• ***Diritto penale dei media***: applicabile (cfr. n. 6.1).
• ***Fornitore di contenuti***: reato commesso all'estero; nel caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce

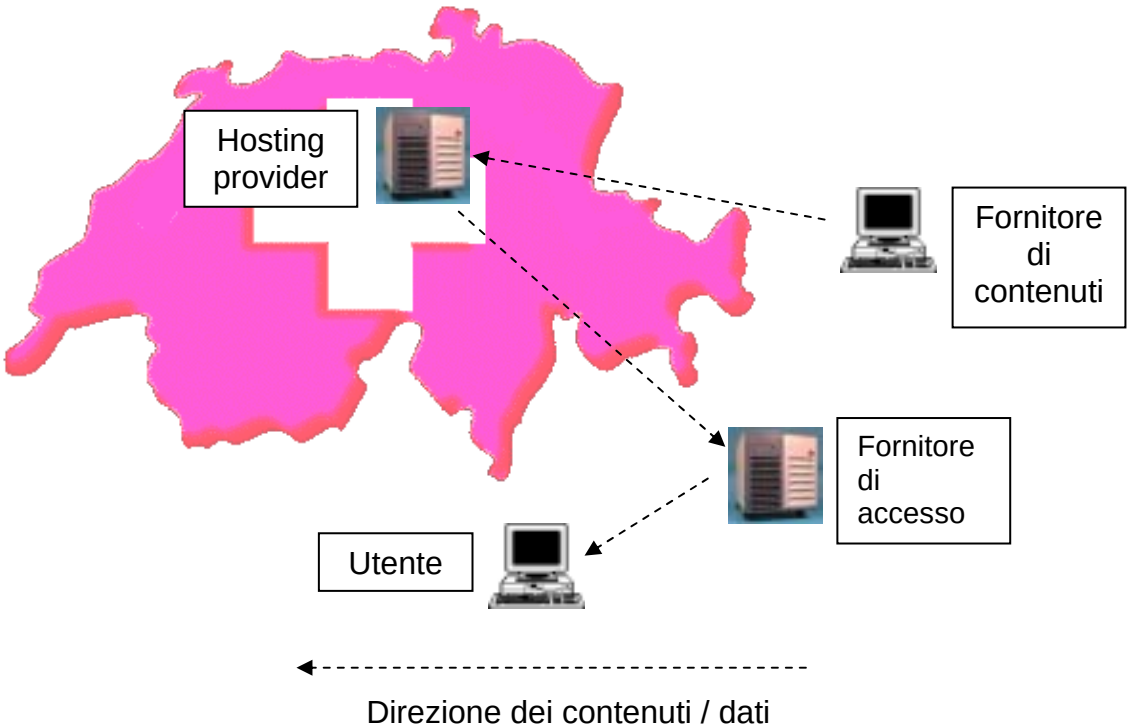
[289] Resta ancora possibile un nesso con il principio della personalità attiva, sancito dall'articolo 6 numero 1 CP, nel caso in cui il responsabile del server web sia di nazionalità elvetica e soggiorni in Svizzera.
[290] Diversamente da quanto previsto dall'articolo 5 della nuova parte generale del CP.

in Svizzera, e quindi la sovranità penale non può fondarsi sul principio di territorialità (cfr. n. 6.42). Il fornitore di contenuti non è quindi perseguibile in Svizzera. Può essere accordata l'assistenza giudiziaria.
• ***Hosting provider***: come il fornitore di contenuti.
• ***Fornitore di accesso***: come il fornitore di contenuti.
• ***Utente***: esente da pena.

Caso 3: discriminazione razziale in testi pubblicati nel www

• ***Diritto penale dei media***: la sua applicabilità è controversa (sarebbe piuttosto da negare).
• ***Fornitore di contenuti***: reato commesso all'estero; per semplici reati di comportamento non è dato un nesso di collegamento legato a un evento che si produce in Svizzera, e quindi la sovranità penale non può fondarsi sul principio della territorialità (cfr. n. 6.42); il fornitore di contenuti non è quindi perseguibile in Svizzera, e può essere accordata l'assistenza giudiziaria.
• ***Hosting provider***: come il fornitore di contenuti.
• ***Fornitore di accesso***: come il fornitore di contenuti.
• ***Utente***: esente da pena.

Ipotesi 6: soltanto l'hosting provider agisce in Svizzera, mentre tutti gli altri attori si trovano all'estero



Caso 1: immagini di carattere pedopornografico nel www

• ***Diritto penale dei media***: secondo il Tribunale federale non è applicabile; la dottrina dominante è tuttavia di altro avviso (cfr. n. 6.2).
• ***Fornitore di contenuti***: reato commesso all'estero; in caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce in Svizzera. La sovranità penale non può quindi derivare né dal principio della

territorialità (cfr. n. 6.42), né da quello della competenza universale (art. 6bis CP), e il fornitore di contenuti non è perseguibile in Svizzera. Può essere accordata l'assistenza giudiziaria.
• ***Hosting provider***: se è considerato (co)autore del reato previsto dall'articolo 197 numero 3 CP (il fatto di rendere accessibili i contenuti), è applicabile il diritto penale svizzero. Se il fornitore di accesso ha favorito la commissione del reato principale, ed è quindi considerato complice, il suo agire assume un carattere accessorio e viene quindi giudicato secondo il diritto del luogo in cui è stato commesso il reato principale; non vi è pertanto sovranità penale svizzera (in entrambi i casi non vi è chiarezza; cfr. n. 6.3).
• ***Fornitore di accesso***: come il fornitore di contenuti.
• ***Utente***: il suo reato è commesso all'estero (possesso), ragione per cui la sovranità penale non si fonda sul principio della territorialità; non è perseguibile in Svizzera.

Caso 2: istigazione alla commissione di un incendio mediante la partecipazione a un gruppo di discussione

• ***Diritto penale dei media***: applicabile (cfr. n. 6.1).
• ***Fornitore di contenuti***: reato commesso all'estero; in caso di reati di messa in pericolo astratta, non è dato un nesso di collegamento con un evento che si produce in Svizzera. La sovranità penale non può quindi derivare dal principio della territorialità (cfr. n. 6.42), e il fornitore di contenuti non è perseguibile in Svizzera. Su richiesta un altro Stato può ottenere assistenza giudiziaria.
• ***Hosting provider***: c'è chi sostiene che la punibilità è da valutare in funzione dell'articolo 27 capoverso 2 in relazione con l'articolo 322bis CP, poiché non è possibile agire nei confronti dell'autore e l'hosting provider è considerato come una persona responsabile della pubblicazione. Secondo altri, il diritto penale dei media non è applicabile. Se la complicità dovesse entrare in considerazione, l'hosting provider non potrebbe essere perseguito in Svizzera. Secondo altri ancora, l'hosting provider, in quanto divulgatore, non è mai punibile per reati mediatici (non vi è chiarezza, cfr. n. 6.43).
• ***Fornitore di accesso***: come il fornitore di contenuti.
• ***Utente***: esente da pena.

Caso 3: discriminazione razziale in testi pubblicati nel www

• ***Diritto penale dei media***: la sua applicabilità è controversa (sarebbe piuttosto da negare).
• ***Fornitore di contenuti***: reato commesso all'estero; per semplici reati di comportamento non è dato un nesso di collegamento legato a un evento che si produce in Svizzera, e quindi la sovranità penale non può fondarsi sul principio della territorialità (cfr. n. 6.42); il fornitore di contenuti non è quindi perseguibile in Svizzera, e può essere accordata l'assistenza giudiziaria.
• ***Hosting provider***: se si ammette che il suo atto ha favorito la commissione del reato principale, costituendo quindi una variante indipendente dell'articolo 261bis capoverso 3 CP, verrà giudicato secondo il diritto penale svizzero (non vi è chiarezza, cfr. n. 6.3). Se viene ammessa la complicità, vi è carattere accessorio e l'atto viene quindi giudicato secondo il diritto del luogo in cui è stato commesso il reato principale; non vi è in tal caso sovranità penale della Svizzera.
• ***Fornitore di accesso***: come il fornitore di contenuti.
• ***Utente***: esente da pena.