a cura di
Gian Italo Bischi, Jan Marten Ivo Klaver

NOIR 2.0

Il lato oscuro di Internet

aras
EDIZIONI

UNIVERSITÀ
DEGLI STUDI
DI URBINO
CARLO BO

Club Lions
Urbino

1506
UNIVERSITÀ
DEGLI STUDI
DI URBINO
CARLO BO

DISCUI
DIPARTIMENTO DI SCIENZE DELLA COMUNICAZIONE,
STUDI UMANISTICI E INTERNAZIONALI:
STORIA, CULTURE, LINGUE, LETTERATURE, ARTI, MEDIA

Collana: Urbi*noir* Studi

Curatori della collana: Alessandra Calanchi, Giovanni Darconza, Jan Marten Ivo Klaver, Federica Savini.

Comitato scientifico: Michele Bartolucci, Gian Italo Bischi, Alessandra Calanchi, Francesca Carducci, Gabriele Cavalera, Giovanni Darconza, Giovanna Errede, Tiziano Mancini, Giulia Ovarelli, Peppe Puntarello, Marco Rocchi.

ISBN 978-88-99913-212
Aras Edizioni srl, Fano (PU)
www.arasedizioni.com – info@arasedizioni.com

CONTENT

1. TUTTO INIZIÒ DA JEFFERY DEAVER

Gian Italo Bischi

1.1. Introduzione

Per giustificare il titolo di questa relazione e anticiparne i principali contenuti, riporto uno scambio di messaggi di posta elettronica tra me e la collega Alessandra Calanchi.

Da: Gian Italo Bischi <gian.bischi@uniurb.it>
A: Calanchi, Alessandra <alessandra.calanchi@uniurb.it>
Date: 24 luglio 2014 11:11
Oggetto: Dati personali

Ciao Ale,
sto leggendo (come al solito su suggerimento di Matteo) un giallo di Jeffery Deaver, che si basa sulla mancanza

di privacy a causa di tutti i dati che ciascuno di noi diffonde attraverso le reti informatiche, dalle web page visitate agli acquisti con carte di credito, dalle email ai contatti tramite social networks, dai telepass ai cartellini elettronici di ingresso-uscita al lavoro, dai sistemi di videosorveglianza agli spostamenti con in tasca lo smartphone, fino ai microchip inseriti in molti prodotti commerciali. Da tutto ciò si possono creare profili dettagliati delle nostre abitudini, degli oggetti che possediamo, dei nostri spostamenti, amicizie ecc. Nel giallo c'è un assassino seriale che in ogni omicidio riesce a fare incolpare un'altra persona, che ha identificato attraverso il suo "profilo digitale". Ne identifica (o crea ad hoc) un possibile movente e dissemina indizi che portano gli investigatori a incolpare la persona scelta come capro espiatorio. Ti scrivo queste cose sui dati reperibili via web (il cosiddetto "big data") perché poco fa mi si è aperta all'improvviso una finestra pubblicitaria con il link che riporto qui sotto, in cui mi propongono di acquistare un abito da Sherlock Holmes, probabilmente perché di recente ho acquistato questi romanzi e ciò ha permesso a qualcuno di identificarmi in rete come lettore di gialli.
http://www.vegaoo.it/kit-sherlock-holmes-adulto-bis.html

Da: Calanchi, Alessandra <alessandra.calanchi@uniurb.it>
A: Gian Italo Bischi gian.bischi@uniurb.it
Date: 24 luglio 2014 16:39
Oggetto: Re: Dati personali

Senti, per favore trasforma la tua mail in una recensione breve e la mettiamo nel sito. Mi sembra MOLTO interessante.

Da: Gian Italo Bischi <gian.bischi@uniurb.it>
Date: 24 luglio 2014 17:56
Oggetto: Re: Dati personali
A: "Calanchi, Alessandra" alessandra.calanchi@uniurb.it

Molto volentieri. Il tema è davvero interessante. Attraverso l'immagazzinamento di dati elettronici si sanno moltissime cose su ciascuno di noi. Ma soprattutto diventa inquietante quando, come nel giallo di Deaver, sono i criminali a farne uso per falsare prove. Se uno riesce a entrare nelle memorie elettroniche può cambiare gli orari di ingresso/uscita in aziende o autostrade, creare o cancellare pagamenti fatti in certi luoghi e in certi orari, quindi creare o distruggere alibi. E come ben sappiamo non esiste sistema informatico a prova di bomba, e tanto meno a prova di hacker, che può persino fare operazioni a nome di un altro (cosa ricorrente nel giallo) confondendo le idee degli investigatori. Uno dei prossimi urbinoir potrebbe occuparsi della "insostenibile vulnerabilità delle prove conservate nei computer".

Da: Calanchi, Alessandra <alessandra.calanchi@uniurb.it>
A: Gian Italo Bischi <gian.bischi@uniurb.it>
Date: 25 luglio 2014 10:38
Oggetto: Re: Dati personali

Guarda che ti stai mettendo seriamente nei pasticci perché proporrò che TU organizzi urbinoir 2015 su crimini informatici ecc.!!!!

Da: Gian Italo Bischi <gian.bischi@uniurb.it>
A: Alessandra Calanchi <alessandra.calanchi@uniurb.it>
Date: 12 settembre 2014 20:00
Oggetto: il noir nel deep blu

Ciao Ale, sto leggendo un altro giallo di Jeffery Deaver, tutto ambientato nel mondo dell'informatica, hackers, violazioni di password (anche della polizia) virus informatici e alterazioni di prove. Si intitola "profondo blu", e non permette distrazioni, tutto basato sul "io so che tu sai che io so...". Nel capitolo finale, il classico capitolo di relax in cui tutto è ormai risolto, c'è ancora qualche complice che continua a carpire dati, spedire messaggi sotto vari nomi e a interviene nei social a nome di altri, ma si scopre che in realtà è un computer programmato a fare ciò, un cosiddetto "robot" (o più brevemente "bot"). In questo capitolo finale compare anche una frase che mi ricorda qualcosa: "Il lato oscuro di internet...". A proposito del computer complice che continuava a carpire dati dai computer in rete degli enti governativi (riesce persino a bloccare il sistema informatico che governa i semafori di San Francisco, creando un casino del diavolo, per coprire la fuga dell'assassino) quando il detective lo trova non sa come spegnerlo, non ha interruttori né monitor né tastiera. Stacca la spina ma ha una batteria interna. E allora prende la sua pistola e gli spara, ma le pallottole rimbalzano sulla corazza d'acciaio del computer. Una bella metafora sulla inadeguatezza delle armi per combattere criminali che usano l'informatica. Ci vuole conoscenza, non violenza.

Nel seguito di questo articolo vengono introdotti, nel paragrafo 1.2., alcuni concetti sulla memorizzazione e trasmissione dei dati informatici, insieme alla descrizione di alcuni possibili inconvenienti sia involontari

che causati con intenti criminali. Nel paragrafo 1.3. vengono descritti alcuni romanzi che sono stati particolarmente importanti per introdurre questo tema nella letteratura noir, per poi dedicare il paragrafo 1.4. alla descrizione di quattro romanzi di Deaver interamente dedicati a questi problemi. Alcune brevi conclusioni sono delineate nel paragrafo finale.

1.2. Tracce informatiche, indagini in rete, data mining

Nell'introduzione in forma epistolare sono delineati molti dei temi del convegno e, di conseguenza, di questo articolo. Dalla violazione di privacy per aver mostrato ai partecipanti del convegno i messaggi di posta elettronica intercorsi tra me e Alessandra (senza averle prima chiesto il permesso) ai *cookies*[1] che hanno carpito informazioni sui miei acquisti, un'altra evidente violazione di privacy rivelata dall'inaspettata comparsa, mentre scrivevo, della finestra *popup* con la pubblicità mirata, fino ovviamente al tema centrale del convegno, ovvero come la letteratura poliziesca si stia sempre più spesso occupando di crimini informatici o dell'utilizzo dei dati informatici sia da parte degli investigatori sia da parte dei criminali, con la

1 Letteralmente "biscotti", sono frammenti di codice informatico che vengono inviati ai *browser* attraverso i siti visitati e che vengono automaticamente memorizzati senza che l'utente se ne renda conto. Un *cookie* è poi in grado di immagazzinare e condividere in rete informazioni sulla nostra navigazione. Nei casi migliori questo può aiutarci nello scambio di informazioni durante la navigazione (ad esempio evitandoci di ripetere operazioni già fatte) ma possono anche "spiarci" comunicando, senza che ce ne rendiamo conto, un profilo delle nostre preferenze sulla base dei siti che visitiamo.

conseguente comparsa, in forme più o meno originali, di nuovi crimini o nuovi metodi per eseguire crimini tradizionali, insieme a nuovi metodi per compiere indagini sfruttando tracce digitali.

L'utilizzo così diffuso, quasi pervasivo, di dati e strumenti informatici è un fatto consolidato e irreversibile. Ormai da diversi anni privati e istituzioni conservano i propri dati in forma digitale: tutto ciò che viene scritto, ricevuto, fotografato, filmato è in forma digitale, ovvero pacchetti di *bits* (impulsi elettrici) che possono viaggiare con molta facilità e sotto varie forme da un computer all'altro, sia attraverso cavi elettrici che attraverso il vuoto mediante onde elettromagnetiche (ovvero *wireless*). Molte delle nostre azioni lasciano tracce digitali, che possono essere immagazzinate e trasmesse sotto forma di segnali elettromagnetici e poi ordinate e elaborate mediante *computer*: si pensi agli acquisti con carte di credito, alla tracciabilità del navigatore satellitare (*gps*) che abbiamo in auto o nello *smartphone*, biglietti aerei e ferroviari che vengono acquistati *online* e poi letti mediante lettori ottici che li trasmettono in rete, così come i cartellini di ingresso/uscita da posti di lavoro, registrazioni di *webcam* lungo strade, nei negozi e negli uffici, il continuo traffico di messaggi di posta elettronica, *sms*, *whatsapp* che possono essere captati in rete e conservati su *computer* remoti (*clouds*), gli interventi nei *social network*, *blog* ecc., fino ai dispositivi (dagli elettrodomestci ai *peacemaker*) dotati di microprocessori per essere governati da telecomandi o *computer* remoti, quindi anche loro in definitiva collegati in rete. Tutto questo racchiude enormi quantità di dati che, raccolti

insieme, costituiscono il cosiddetto *"big data*", dal quale con opportuni programmi si possono "estrarre", ordinare e classificate dati su ciascuno di noi (*data mining*). Tutte tecniche molto recenti e in continua evoluzione, difficile per legislatori, giudici e avvocati regolamentarne l'uso, punire eventuali abusi e cogliere il confine fra lecito e illecito, altrettanto difficile per investigatori e malviventi utilizzarli al meglio per i propri scopi.

Il problema diventa di carattere globale, e spesso oggetto di studio del diritto internazionale, perché i *computer* in cui questi dati sono immagazzinati sono connessi tra loro, attraverso reti domestiche o aziendali fino alla rete mondiale, *internet*. Quindi i dati vengono spesso condivisi fra più utenti, anche lontani, una cosa molto utile a chi effettua indagini di ogni tipo, da quelle svolte della polizia a quelle dei medici. Ma la condivisione di dati può avvenire sia in modo consapevole che inconsapevole (allora più che condivisione sarebbe meglio parlare di furto di dati): dalle piccole violazioni della privacy, al furto di materiale digitale (dati riservati, foto, e-mail ecc.) con cui ricattare persone o danneggiare organizzazioni fino ai "cyber-attacchi" e al terrorismo informatico, fatti di cui sono piene le pagine di cronaca, politica e economia.

Il fatto che i dati memorizzati nei computer possano anche essere condivisi illecitamente, o carpiti, o modificati furtivamente, può sembrare un evento raro, frutto di incidenti, perché che i dati sono generalmente protetti da password o criptati, cioè codificati in modo da renderli incomprensibili a chi non conosce la chiave per decodificarli. Ma non è sempre così, perché queste

protezioni sono tutt'altro che sicure quando intervengono soggetti particolarmente abili, chiamati *hackers o crackers*,[2] in grado con vari metodi di accedere anche a dati estremamente riservati, come archivi di banche, uffici amministrativi o persino archivi della polizia. Non sempre la cronaca riporta queste notizie, per non diffondere sfiducia nelle istituzioni coinvolte.

Tutto questo si presta a crimini di vario genere, che si leggono sempre più spesso nella cronaca: truffe informatiche, furti di identità, richieste di riscatti, minacce di attacchi informatici fino a forme di terrorismo informatico. Comunque, anche senza evocare complotti o azioni di *hackers*, molti dati personali si diffondono in rete senza che ne siano consapevoli. In altre parole, i *bits* nei quali le informazioni sono immagazzinate sono estremamente volatili e si diffondono senza far rumore e senza bisogno di mezzi di trasporto, spesso anche senza costi. Basti pensare che posta elettronica, foto, filmati, contenuti di social networks fino a intere copie (o *backup*) di dischi sono conservati in computer remoti (i *clouds*, ovvero nuvole) ai quali la maggior parte dei *computer* e *smartphones*, così come i *pos*, i *telepass*, i circuiti di videosorveglianza sono collegati in modo *wireless* mediante reti che includono passaggi attraverso satelliti artificiali.

Questi trasferimenti di dati, carpiti in qualche passaggio, in qualche anello debole della catena di trasferi-

2 L'*hacker* è un esperto di sistemi informatici in grado di introdursi in reti informatiche protette e di acquisire un'approfondita conoscenza del sistema sul quale interviene. Lo fa per semplice sfida o per segnalare le debolezze di un sistema di protezione informatica, oppure per arrecare danni o trarre profitti, anche se in quest'ultimo caso si dovrebbe usare il termine *cracker*.

menti in sicurezza, costituiscono il *leaking* (sgocciolamento) di informazioni, termine divenuto famoso dopo le azioni di *wiki-leaks*.[3] A questo sgocciolamento involontario si aggiungono le informazioni che volontariamente riveliamo ogni volta che interagiamo con blogs e social network, nei quali vengono continuamente e volontariamente pubblicate informazioni sulle proprie preferenze (opinioni, tendenze politiche, sportive, sessuali, simpatie e antipatie) pensando di condividerle con pochi ma in realtà a disposizione di tutti, come il tipico "ecco la mia foto appena scattata a Stoccolma" che suggerisce ai ladri che potranno andare indisturbati a rubare nell'appartamento i cui proprietari sono molto lontani, o l'affermazione sul capufficio fatta in modo confidenziale alla cerchia di amici di *facebook* che provoca il licenziamento nei giorni successivi.

Questi sgocciolamenti di informazioni, sia volontari che involontari, sono preziosi dati per chi opera nel marketing, perché permettono di effettuare proposte mirate e personalizzate per la vendita di prodotti, e lo sono anche per datori di lavoro che desiderano selezionare personale da assumere o giudicare dipendenti in prova (qualcuno dice che concorsi e colloqui sono ormai quasi inutili, basta cercare in rete). Ma sono preziosi anche per ricattatori, ladri, avversari politici, che possono trovare dati su fatti remoti o addirittura arrivare a modificarli illegalmente per screditare candidati

3 Organizzazione internazionale, fondata dall'informatico australiano Julian Assange, che riceve in modo anonimo documenti segreti e poi li carica sul proprio sito web con lo scopo di assicurare la trasparenza delle informazioni come garanzia di giustizia, di etica e di una più forte democrazia.

durante le campagne elettorali. Dati preziosi anche per terroristi che progettano azioni o di chi deve impedirle. A questo proposito si è molto dibattuto su quale sia il confine tra rispetto della privacy e necessità, da parte delle agenzie per la sicurezza, di sorvegliare gli scambi di messaggi fra cittadini. Una questione che è diventata un vero cruccio delle moderne democrazie dopo i poteri eccezionali assunti dalla *NSA* (*National Security Agency*) in seguito agli attacchi terroristici dell'11 settembre 2001.

Ovviamente la narrativa non poteva rimanere indifferente a tutto ciò, e tanti autori hanno inserito crimini informatici e indagini con metodi informatici nelle proprie opere, non solo prendendo spunto da vicende reali ma talvolta persino anticipando avvenimenti. Nel seguito riporto alcuni esempi, senza alcuna pretesa di sistematicità né di completezza.

1.3. Alcuni classici: da Dan Brown a Stieg Larsson

Un importante thriller informatico è *Digital Fortress* di Dan Brown, pubblicato negli Stati Uniti nel 1998 e tradotto in italiano solo nel 2006 con titolo *Crypto* (dopo il successo di *The Da Vinci Code* dello stesso autore). Il romanzo è dedicato al conflitto tra diritto alla privacy e controllo della posta elettronica privata, da parte della NSA, per prevenire azioni terroristiche, tema che anticipa il dibattito che diventerà dominante nella cronaca dopo l'attacco alle torri gemelle (ovviamente questo effetto di anticipazione non viene notato in Italia, a causa del ritardo di 8 anni nella traduzione). Nel

romanzo la *NSA* si è dotata (all'insaputa dei cittadini) di un sofisticato programma, denominato *TRANSLTR*, in grado di decodificare qualunque testo cifrato in brevissimo tempo, compresi i messaggi di posta elettronica fra privati. Pochi addetti ai lavori sono informati dell'esistenza di un simile programma, creato allo scopo di contrastare il terrorismo ma che limita la privacy dei cittadini. Però arriva un particolare messaggio, criptato tramite un algoritmo ricorsivo, che *TRANSLTR* non riesce a decodificare. Il misterioso e inviolabile messaggio ha ben presto un nome: Fortezza Digitale, creato dal giapponese Ensei Tankado, matematico ex dipendente della NSA, portatore di handicap sin dalla nascita a causa del disastro atomico di Hiroshima, e strenuo sostenitore della privacy dei cittadini. Da qui la sua decisione di intralciare l'operato della NSA e la minaccia di permettere a chiunque di scaricare Fortezza Digitale da Internet, che quindi consentirebbe a chiunque di inviare messaggi criptati non decodificabili, inclusi criminali e terroristi che potrebbero così comunicare tra loro in modo indisturbato. Ma la sopravvenuta e alquanto strana morte di Tankado scatena una caccia alla password che consente di espugnare il codice, che permetterebbe alla NSA di renderlo di fatto inutile. Tutto il romanzo ruota attorno a concetti informatici e leggi dell'informatica teorica (alcuni scientificamente fondati, altri frutto della fantasia dello scrittore ma comunque interessanti e ben spiegati) rendendo plausibile il fatto che si può arrivare a uccidere per appropriarsi di un teorema o per carpire una password. Un tema che ci riporta alle origini del romanzo poliziesco, col tema della decodi-

fica di messaggi cifrati molto caro a Edgar Allan Poe, presente nel celebre racconto *The Gold Bug* (trad. it. *Lo scarabeo d'oro*). Un romanzo che anticipa di molti anni la vicenda di *Wikileaks*, organizzazione per la trasparenza fondata da Julian Assange nel 2007, e il cosiddetto *Datagate* di Edward Snowden, esploso nel 2013.

Un altro scrittore che ha trattato con molta lungimiranza l'uso di azioni di intrusione in sistemi informatici per risolvere casi di crimini comuni e truffe finanziarie è lo scrittore svedese Stieg Larsson, autore della *trilogia Millennium*, composta dai tre romanzi noir *Uomini che odiano le donne*, *La ragazza che giocava con il fuoco* e *La regina dei castelli di carta* pubblicati fra il 2005 e il 2007, che ha riscosso un enorme successo con 27 milioni di copie vendute in oltre 40 paesi già nel 2010. Lo scrittore, prematuramente scomparso per un attacco cardiaco nel 2004, prima che i tre romanzi venissero pubblicati, ha scelto come investigatrice il personaggio di Lisbet Salander, una *hacker* che, nella tradizione del giallo classico inglese, svolge prevalentemente le indagini rimanendo a casa propria e in modo piuttosto solitario (collabora solo con un giornalista) ma usa estensivamente il computer e la capacità di carpire dati con tipiche azioni di intrusione illegale grazie alle sue abilità informatiche e allo scambio di idee con una comunità di *hacker* alla quale appartiene. Questo ci riporta a una caratteristica tipica del romanzo noir, ovvero il fatto che gli investigatori utilizzano metodi di indagine e frequentano ambienti non diversi da quelli dei criminali. Qui però non si tratta dell'uso di armi convenzionali o violenze fisiche da parte degli investigatori, ma di

violazioni informatiche, furti di dati e di identità. Di nuovo, violazione di segreti per aumentare la sicurezza e smascherare criminali. Non manca comunque, in un momento di necessità, l'utilizzo da parte di Lisbet delle proprie abilità informatiche per dirottare sul proprio conto bancario (ovviamente opportunamente nascosto nei meandri di banche più o meno fittizie con sedi in paradisi fiscali) somme di denaro carpite a società legate alla malavita con operazioni finanziarie in rete. Il lato oscuro della rete.

1.4. Jeffery Deaver

Come è stato ampiamente accennato nell'introduzione, uno scrittore che sta utilizzando concetti, personaggi e avvenimenti legati al mondo dell'informatica per creare, con fantasia e competenza, intriganti storie noir è Jeffery Deaver. Scrittore statunitense di Chicago, classe 1950, è uno dei più prolifici e premiati scrittori noir contemporanei, vincitore per tre volte dell'*Ellery Queen Readers Award for Best Short Story of the Year*, oltre al *British Thumping Good Read Award* e il *Crime Writers Association's Ian Fleming Steel Dagger Award*, ha anche vinto il *Premio Nero Wolfe* nel 1999 e nel 2001 il *WH Smith Thumping Good Read Award*. Dai suoi romanzi sono stati tratti diversi film. In questo contesto mi occuperò solo dei suoi quattro romanzi interamente dedicati a storie connesse a crimini informatici o nei quali strumenti e concetti di informatica hanno un ruolo predominante.

Un thriller specificamente dedicato al mondo degli *hacker* è *Profondo blu* (*The Blue Nowhere*) del 2001, ambientato nella *Silicon Valley*, in cui si racconta di un assassino seriale che è anche un famoso hacker. Grazie a un programma di sua creazione può entrare nei computer e nella vita di chiunque, estrapolando informazioni che poi utilizza per uccidere. Infatti, un videogioco di cui è appassionato, che consiste nell'uccidere (virtualmente) alcuni personaggi (digitali), non gli basta più, e inizia a svolgere lo stesso gioco nel mondo reale, uccidendo le vittime (reali) pugnalandole al cuore (un importante file di sistema nel corpo umano). Il gioco diventa quindi un misto di crimine informatico (intromissione nel computer delle vittime, furto di identità, appropriazione di dati che permettono di intrappolarle) e crimini reali (omicidi, ricatti...) una sinergia tra crimini informatici e reali. La polizia è incapace di fronteggiare questo tipo di criminale, in grado di entrare anche nei loro sistemi informatici, e chiede aiuto a un *hacker* che si trova in prigione a scontare una pesante condanna per essersi intromesso nei *computer* ministeriali. Quindi i veri protagonisti della storia sono due *hackers*, l'assassino seriale e quello che ora lavora per conto della polizia. Ma non è chiaro se è fidato, e non è chiaro se gli interessa più arrestare l'assassino o appropriarsi del suo codice che permette di violare i computer. La polizia è completamente spiazzata, non riesce più a capire come muoversi senza far ricorso al collaboratore hacker, le armi sono inutili, sono in balia del consulente che è però un malvivente senza scrupoli. Uno dei temi importanti che ricorre in questo romanzo è l'ingegneria sociale. Un *social engineer*

è un personaggio molto bravo a nascondere la propria identità, fingendosi un'altra persona, in modo da riuscire a ricavare, da ignare vittime, informazioni che non potrebbe mai ottenere con la sua identità reale, utilizzando metodi tipici delle spie. Spesso queste tecniche sono incluse nel neologismo *phishing*.[4]

Un altro romanzo molto noto su questi temi è *La finestra rotta* (*The Broken Window*) del 2008, ottava indagine di Lincoln Rhyme, il criminologo tetraplegico protagonista di tanti romanzi di Deaver, che svolge le indagini da casa sua, su una sedia a rotelle, basandosi sulla sola forza della logica e dell'attenta analisi dei dati trovati sulla scena del delitto. Con l'aiuto di avanzati metodi e dispositivi fisici, chimici e informatici e di validi collaboratori, fra cui la bellissima agente ed ex modella Amelia Sachs, sua compagna, Rhyme riesce a capire che dietro alcuni omicidi apparentemente compiuti da persone diverse, alcune delle quali già condannate sulla base di prove schiaccianti e (fin troppo) evidenti, c'è in realtà la mano dello stesso killer seriale, ancora in libertà. Le ricerche portano Rhyme a indagare su alcune società che raccolgono enormi quantità di dati (anche per conto della *NSA*) per scoprire che proprio usando questi dati le prove oggettive potrebbero essere state create ad arte da chi desidera sviare il corso delle

4 Variante di *fishing* nel quale la lettera f è sostituita con ph, variante molto utilizzata dagli *hacker* a partire dal vecchio termine *phreaking*, unione delle parole *freak* con la ph- da "phone" (telefono) e la -ing da "hacking", usato per indicare l'abilità di fare chiamate telefoniche senza pagare. Il *phishing* è un tipo di truffa attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso.

indagini, facendo leva su informazioni che nemmeno la polizia possiede. Basta poter accedere ai dati posseduti da queste società, le quali sono dotate di sistemi di sicurezza in apparenza inespugnabili ma in realtà ben pochi sistemi informatici sono a prova di hacker. E c'è anche il problema della riservatezza dei dipendenti, anche dei più fidati. I dati informatici, leggeri e immateriali, possono con altrettanta leggerezza ed eleganza essere carpiti e usati in modo perverso, fino ad arrivare a veri e propri furti di identità. Il romanzo è quindi dedicato, in modo rigoroso e anche molto didattico, al tema del *data mining*, ovvero la capacità di estrarre informazioni dalle grandi quantità di dati raccolti e immagazzinati con metodi informatici nel cosiddetto *big data*. Il *data mining* permette quindi di conoscere in tempi brevi i gusti, le abitudini, le condizioni di salute, difetti E potenzialità di ciascuno di noi, e costituisce un potente strumento in mano agli investigatori, ma anche ai criminali. Nel romanzo si evidenzia come ogni nostra azione può lasciare tracce informatiche e, come il grande fratello orwelliano, qualcuno potrebbe sapere tutto di ciascuno di noi. E che dire se un criminale riesce ad accedere a questi dati, e li utilizza per incolpare altri dei propri delitti? Prima di compiere il delitto basta cercare un soggetto che potrebbe avere un movente (sulla base delle informazioni ottenute sul suo passato) e studiare le sue abitudini per essere sicuri che non abbia un alibi (ma attraverso i sistemi informatici un esperto hacker può persino smontare un suo alibi, ad esempio cambiando l'orario di timbratura del suo cartellino nel server dell'azienda in cui lavora, o modificare l'orario di

ingresso in autostrada col telepass) e disseminare prove sulla scena del delitto legate ai suoi acquisti, impronte con lo stesso tipo di scarpe che porta, lo stesso tipo di tabacco che usa, ecc. Poi fare una telefonata anonima alla polizia e dire che dopo aver sentito urlare si è visto qualcuno fuggire su un'auto con la targa del capro espiatorio (anch'essa ovviamente contenuta nei dati informatici associati al soggetto). Questo è proprio ciò che avviene nel romanzo di Jeffery Deaver.

Il terzo romanzo è *La strada delle croci* (*Roadside Crosses*) del 2009, che ha come protagonista un'altra investigatrice cara a Deaver, Kathryne Dance, specializzata in cinesica, ovvero il linguaggio del corpo, la capacità di capire pensieri reconditi (ad esempio se un testimone mente) in base alla gestualità e agli atteggiamenti. Di nuovo alla ricerca di un assassino seriale che, per annunciare il suo prossimo delitto, pianta delle croci lungo le strade, con incisa una data. Non lascia nessun altro indizio, e la presenza di queste croci semina terrore. Tutti i sospetti ricadono su un giovane che viene attaccato spietatamente attraverso un blog perché ritenuto il responsabile della morte di due sue amiche, in seguito ad un incidente stradale. Infatti sembra che le vittime vengano scelte in base ai messaggi che lasciano sul blog. L'indagine si svolge tutta nel mondo dei *blogger* e dei *social networks*, basate quindi sulla reputazione in rete e i suoi riflessi nella vita reale. Quindi di nuovo è protagonista lo sdoppiamento di personalità tra la vita in rete e la vita reale, tra contatti via network e contatti nella vita vissuta, tra giochi con personaggi virtuali e incontri con persone reali. Il romanzo mette chiaramente

in guardia dai pericoli collegati con l'abitudine di rivelare le proprie opinioni online, che diventano subito di pubblico dominio. Chi scrive opinioni seduto davanti a un computer collegato ai *social networks* pensa di parlare con pochi intimi, in realtà rende noti i propri pensieri a un pubblico enormemente vasto, che può comprendere tante persone che non si conoscono. Si forma così una cyber-reputazione, diversa dalla reputazione nella vita reale, che può dare origine a forme di linciaggio in rete, facili e spietate perché gli interlocutori non si vedono in faccia, non c'è l'imbarazzo dello sguardo. Ma poi certi linciaggi in rete traboccano nella vita reale con conseguenze spesso drammatiche (suicidi, pestaggi ecc.).

Concludiamo con il recente romanzo *Il bacio d'acciaio* (*The Steel Kiss*), pubblicato nel 2016, che si occupa della concreta possibilità, da parte di un *hacker*, di inviare comandi a dispositivi dotati di *remote controller*, i cosiddetti "elettrodomestici intelligenti", protagonisti della domotica. Si tratta di termostati, forni, segreterie telefoniche, cancelli e sistemi di allarme che possono essere governati da un telecomando remoto o uno *smartphone*, sistemi che si estendono sempre più frequentemente anche a dispositivi medici, automobili ecc. Ovviamente tutti questi dispositivi sono dotati di microprocessori connessi in rete, e quindi possono essere intercettati e comandati da possibili intrusi (*hackers* o *crackers*) con intenti criminali. Il romanzo narra di un assassino che per una sua forma di avversione verso la tecnologia cerca di diffondere il panico tra coloro che, a suo parere, utilizzano troppe macchine e con spirito troppo consumistico. E arriva a ucciderli bloccando

dispositivi o attivandone altri che provocano disgrazie, da cadute a sprofondamenti, incendi o fuoriuscita di sostanze pericolose. Anche gli oggetti in apparenza più innocui possono diventare letali. Persino dispositivi medici elettronici, come quelli per la regolazione del battito cardiaco, collegati via wireless con l'ospedale che li ha installati per fornire dati utili al controllo del paziente, possono essere soggetti a intrusioni informatiche con gravi conseguenze. Eventualità già descritta nel recente romanzo noir di Giovanni Ziccardi *L'ultimo hacker*, pubblicato nel 2012, dove un personaggio viene ucciso da un hacker che riesce ad alterare il suo *peacemaker*. L'assassino seriale di Deaver non arriva a tanto, anche se la cosa è tecnicamente possibile.

Concludo questo paragrafo dedicato a Jeffery Deaver riportando il testo del breve e cortese messaggio inviato dallo scrittore in risposta all'invito a partecipare al convegno Urbi*noir* del 2015.

> From: Jeff deaver <...>
> Date: 2015-01-22 0:44 GMT+01:00
> Subject: from Jeff Deaver
> To: gian.bischi@uniurb.it
>
> *Buona Sera!*
> *Thank you for your kind email – what an honor to learn of your interest in my books!*
> *I'm afraid, however, that I must decline – that is the week of our Thanksgiving holiday and I get away with family for that time. I wish you the best on a successful conference.*
> *Grazie mille!*
> *Jeff*

1.5. Conclusioni

Spesso i romanzi noir, con le loro trame avvincenti che non permettono distrazioni, possono essere usati come strumento per fornire ai lettori utili informazioni e metterli in guardia da pericoli che si possono presentare nella vita di ogni giorno, oltre a mettere in luce nuove caratteristiche e tendenze della società in cui si vive. Questa è una delle spiegazioni, dal punto di vista evolutivo (in senso darwiniano) fornite nel saggio *The Storytelling Animal* di Jonathan Gottschall[5] sulla utilità della letteratura per la sopravvivenza di individui e società.

I romanzi analizzati in questo articolo, oltre a proporre avvincenti e originali narrazioni, analizzano situazioni interessanti che possono aiutarci a capire potenzialità e pericoli dell'informatica (intesa in senso lato, incluso l'immagazzinamento e l'elaborazione dei dati digitali, il *big data* e il *data mining*). I romanzi in genere, e questi in particolare per la loro capacità di focalizzare l'attenzione del lettore grazie all'importante caratteristica della *suspense*, ci aiutano ad analizzare e capire la realtà, a orientarci nel complesso e labirintico mondo in cui viviamo. Simili narrazioni ci preparano ad affrontare il mondo che ci circonda perché si possono configurare come "simulatori di vita", e quindi ci consentono di non farci trovare sorpresi e indifesi di fronte a situazioni pericolose e complesse. Ed è probabilmente fin troppo ovvio affermare che un aiuto a orientarci nel campo delle competenze informatiche è ormai non solo utile, ma assolutamente necessario, per capire meglio la realtà che ci circonda e la società in cui viviamo e operiamo.

5 Traduzione italiana *L'istinto di narrare*, Bollati Boringhieri, 2014.