Internet e Terrorismo
Un modello interdisciplinare per l'analisi di un dialogo di propaganda

Alessandro Trivilini
Responsabile del Laboratorio di informatica forense del Dipartimento tecnologie innovative, Scuola universitaria professionale della Svizzera italiana (SUPSI)

La prevenzione al terrorismo pone con forza la necessità di avvalersi di nuove metodologie capaci di supportare le Autorità Giudiziarie durante le analisi preventive dei dialoghi di propaganda. In questo articolo viene presentato un estratto di un modello scientifico interdisciplinare realizzato per le analisi dei dialoghi. Un approccio originale per affrontare un tema delicato in grande sviluppo, soprattutto per quanto riguarda le modalità interattive che intercorrono nel processo di comunicazione fra radicalizzante e radicalizzato. Spesso le analisi convenzionali dei dialoghi trattano le informazioni trascurando elementi oggi fondamentali, come la provenienza dei dati e la loro cultura. E proprio questi aspetti, se correttamente inferiti durante le analisi linguistico-psicologico del dialogo, potrebbero arricchire ulteriormente la qualità dei risultati, consentendo agli addetti ai lavori di poter ottimizzare non solo le risorse ma anche i tempi di intervento per le situazioni a rischio. Quella in corso è una convergenza strategica necessaria, che unisce gli algoritmi di *Artificial Intelligence*, le fasi di *Machine Learning* ed i processi di organizzazione delle informazioni proposti dalla *Big Data Analytics*, perché i risultati oggi parlano chiaro: il processo di radicalizzazione non può essere automaticamente e autonomamente identificato nella sua forma completa con i mezzi di analisi informatici convenzionali.

È senza dubbio un periodo storico particolare, in cui anche le forze dell'ordine si trovano confrontate con una realtà professionale sempre più ricca di *tecnologia human* oriented, concepita e addestrata per far fronte alle innumerevoli sfide di un futuro ormai non più lontano. Gli strumenti di analisi e investigazione tradizionali stanno per lasciare il posto a nuove metodologie di lavoro fondate su approcci fortemente interdisciplinari, capaci di accompagnare le Autorità Giudiziarie a comprendere la complessità dell'infrastruttura informatica, a definire nuove strategie di intervento e alla risoluzione del caso senza correre il rischio di perdere tempo prezioso con grosse quantità di informazioni fuorvianti. Anche un banale caso di truffa informatica, perpetrata utilizzando uno *Smartphone*, potrebbe richiedere competenze tecnico scientifiche avanzate, che un agente di Polizia, per quanto bravo ed esperto, potrebbe non disporre al momento dell'inchiesta.

Considerando la vastità della rete Internet, la sua complessità tecnica, il numero di informazioni digitali che si possono reperire – *Big Data* – e il fatto che le persone che utilizzano la tecnologia per delinquere lo fanno sempre più crittografando i dati, la domanda sorge spontanea:

– Con il terrorismo, esistono modelli di analisi innovativi che le Autorità Giudiziarie potrebbero impiegare per incrementare la loro operatività, evitando così di rimanere intrappolati nei numerosi vincoli tecnici e tecnologici intrinseci nelle nuove tecnologie sempre più *smart* e *wearable*?

A tal proposito, corrono in aiuto i numeri, e in particolare quelli statistici. Per alcuni colossi informatici, anno dopo anno, è stato possibile raccogliere gratuitamente una quantità di dati digitali sulle persone comuni che nessuno ha mai fatto prima, nemmeno i gruppi investigativi meglio equipaggiati. Per esempio, il numero di utenti che contraddistingue Facebook è senza dubbio una peculiarità che lo rende unico e attrattivo sotto diversi punti di vista: una realtà per i giovani, una scoperta per gli adulti, una miniera d'oro per le aziende e uno

strumento di intelligence per gli Stati. A memoria d'uomo non è mai esistito un ambiente strategico di queste dimensioni, in cui le persone, a prescindere dalla loro natura, colore e provenienza, pubblicano volontariamente e gratuitamente informazioni personali sulle proprie abitudini e sulla propria quotidianità. È la dimostrazione che la privacy, così come l'abbiamo conosciuta fino ad oggi, potrebbe presto essere il ricordo di un tempo lontano. Sempre più persone, vuoi anche per i fatti di cronaca allarmanti, sono disposte ad accettare il fatto che qualcuno al di sopra delle parti, per garantire la nostra sicurezza, debba avere accesso in forma proporzionale a parte dei nostri dati digitali confidenziali. Dopo oltre dieci anni di intenso utilizzo da parte di tutti noi, i maggiori social media sono diventati un ecosistema complesso ricco di dati sensibili, usato anche dai terroristi per l'avvicinamento e il reclutamento di nuovi lupi solitari attraverso dialoghi di propaganda, atti ad avvicinare e persuadere giovani utenti a intraprendere un percorso di radicalizzazione.

Da un punto di vista sociale è senza dubbio un fenomeno allarmante da non trascurare, ma da un punto di vista tecnico scientifico potrebbe essere una grande opportunità, da cogliere con coraggio e decisione per l'addestramento di nuovi modelli scientifici utili all'analisi predittiva di comportamenti potenzialmente a rischio. Fare di necessità virtù significa in questo caso aggregare competenze interdisciplinari, per esempio informatiche, investigative, psicologiche, giuridiche, linguistiche e perché no, artigianali, per progettare e sviluppare nuovi automi intelligenti – *Cyber Bot* – utili per l'analisi linguistica e psicologica dei dialoghi che intercorrono fra gli utenti nei social network. Una tendenza in forte crescita, considerata la natura del contesto operativo, in cui anche la comunità europea ha deciso di investire cifre a sei zeri. Le caratteristiche del linguaggio naturale utilizzato dagli utenti all'interno delle fonti aperte come Facebook, sono senza dubbio una risorsa ricca di caratteristiche – *features* – da non trascurare, in grado di fornire alle Autorità Giudiziarie nuove prospettive di analisi complementari a quelle già in uso. L'attenzione investigativa deve curare e conoscere l'infrastruttura informatica moderna, ma non deve rincorrerla. Il *focus* deve spostarsi sui contenuti e sulle modalità di interazione fra utente-utente, utente-macchina e macchina-macchina. Ed è proprio all'interno dei dialoghi, mediati dalle nuove tecnologie per la comunicazione di massa, che si annidano informazioni strutturate utili per una analisi approfondita e innovativa delle intenzioni comunicative degli utenti. Ecco perché può risultare strategico lo sviluppo di nuovi *agenti smart* debitamente addestrati, oggi i dati e le esperienze per farlo non mancano, capaci di riconoscere gli atti comunicativi dei malintenzionati, il loro stile ed il rapporto che intercorre fra motivazioni, emozioni e comportamenti a rischio.

Di seguito viene presentato un estratto del modello teorico stocastico probabilistico interdisciplinare realizzato per l'analisi del dialogo nell'ambito del mio dottorato di ricerca, svolto presso il Politecnico di Milano. Uno spunto scientifico innovativo e originale che propone diversi livelli di analisi, tra cui quelli linguistici e psicologici, da considerare, per esempio, per l'analisi di un dialogo di propaganda. Un dialogo di propaganda è generalmente caratterizzato da un'alternanza frenetica di atti comunicativi finalizzati alla persuasione e al convincimento dell'interlocutore, sfruttando abilità soggettive che potrebbero essere riconosciute e classificate in uno stile di comunicazione particolare, in una sorta di *pattern comportamentale* che il modello matematico potrebbe aiutare a riconoscere e analizzare. In Figura 1 è possibile visualizzare un estratto dello schema del modello teorico concettuale stocastico probabilistico.

Un dialogo di propaganda è generalmente caratterizzato da un'alternanza frenetica di atti comunicativi finalizzati alla persuasione e al convincimento dell'interlocutore.

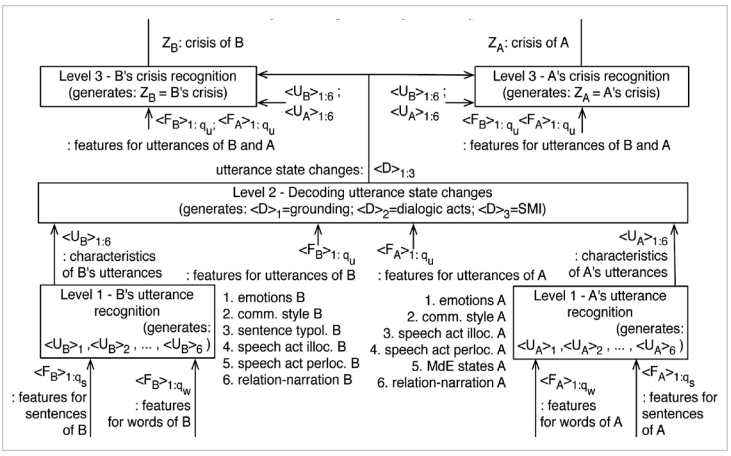

Figura 1: Estratto del modello teorico per l'analisi di un dialogo di propaganda

Per esempio, gli elementi innovativi che offre considerano in una prima fase il riconoscimento delle emozioni, lo stile comunicativo dei partecipanti al dialogo, e la loro capacità di stare in uno stato di narrazione piuttosto che di relazione. Concretamente, per esemplificare, questo livello è utile per codificare le emozioni con cui il candidato alla radicalizzazione partecipa al dialogo (rabbia, gioia, disgusto, tristezza, paura), lo stile comunicativo del radicalizzante (assertivo, aggressivo o passivo), e la capacità dello stesso di mantenere un *continuum* relazionale con il suo interlocutore (in relazione o in narrazione). Il secondo livello, arricchito dalle informazioni inferite da quello precedente, focalizza la sua attenzione sulla capacità di decodifica degli atti dialogici, del terreno comune e sugli stati motivazionali interpersonali, rendendo così la valutazione del dialogo ancora più ricca e completa. Per esempio, gli atti dialogici permettono di capire le azioni intraprese durante il dialogo per esercitare un particolare condizionamento sull'interlocutore, che di fatto corrisponde alla forza della relazione tra la risposta attesa e desiderata da chi pone la domanda (radicalizzante) e la risposta vera e propria che ne segue da parte del radicalizzato. Il terreno comune invece, è utile per conoscere il livello di empatia, di agio, che si è creato fra i partecipanti al dialogo. Per esempio, un buon e costante livello di terreno comune è rappresentato dall'aggiunta continua di nuova informazione all'interno del dialogo da parte del radicalizzante, e la relativa corretta risposta (feedback, approvazione) da parte del radicalizzato. Eventuali discrepanze fra domande e risposte potrebbero far emergere un potenziale fallimento della missione intrapresa nel processo di radicalizzazione. Infine, si possono sfruttare le caratteristiche degli stati motivazionali interpersonali, utilizzati per conoscere, fra le altre cose, il grado di attaccamento ottenuto dal radicalizzante durante le fasi di convincimento del radicalizzato, e il grado di accudimento del radicalizzato nel momento in cui iniziasse a manifestare richieste di aiuto. Un ulteriore livello interessante per l'analisi di un dialogo di propaganda, prende in considerazione il riconoscimento degli stati di crisi, con particolare attenzione alla persone in avanzata fase di radicalizzazione. Si tratta di momenti di scompensazione che la vittima potrebbe manifestare quando la nuova dottrina impartita dal radicalizzante dovesse collidere con le sue precedenti credenze e i suoi "vecchi" principi. Essi si manifestano nel dialogo attraverso momenti di discontinuità, che il modello riconosce attraverso una finestra di osservazione temporale flessibile in cui vengono analizzati tutti i parametri in suo possesso, compresi quelli provenienti dai livelli precedenti.

L'unione delle due tipologie di analisi di un dialogo di propaganda potrebbe fornire interessanti prospettive in termini preventivi.

Un ulteriore elemento da utilizzare per le analisi dei dialoghi di propaganda, al fine di identificarne le intenzioni comunicative, dovrebbe considerare la voce umana e la prosodia. Esse sono senza dubbio vettori ricchi di caratteristiche "tecniche" da non trascurare. Basti pensare quanto potrebbero essere utili quando la lingua in questione è l'arabo, contraddistinta da svariati dialetti, accenti e sfumature linguistiche, che neppure gli stessi arabi potrebbero conoscere. Ecco quindi che lo sviluppo di algoritmi per l'estrapolazione e l'analisi in tempo reale della voce umana potrebbe risultare estremamente efficace ai fine delle indagini preventive. In generale vengono considerati due aspetti fondamentali per la modellazione della voce e della prosodia: la *fonte* (*source*) e il *filtro* (*filter*). La fonte consiste nelle corde vocali che generano un segnale armonico, mentre i filtri sono rappresentati dalla bocca, dal naso o dalla lingua, che ne modificano i parametri originali. Seguendo le teorie proposte da Gilbert per la comprensione della pronuncia, si identificano due concetti importanti: i segmenti e le *caratteristiche soprasegmentali*. I primi corrispondono all'unità sonora discreta che può essere identificata nel segnale vocale emesso, come per esempio vocali e consonanti che si verificano nel dialogo in un ordine temporale preciso. Le vocali sono prodotte dalle vibrazioni delle corde vocali, e rappresentano la parte armonica della voce umana. In gergo tecnico vengono chiamate *formanti*. Le prime tre formanti permettono tipicamente di identificare le vocali. Le consonanti invece possono essere di due tipi: *unvoiced* (afone) or *voiced* (sonore). Quelle classificate come afone sono prodotte senza l'utilizzo delle corde vocali (non fanno uso della fonte) e sono abbastanza difficili da gestire in quanto i loro suoni sono generalmente rumori. Un esempio di consonante afona è la *"t"*. Quelle di tipo sonoro invece vengono prodotte con l'ausilio delle corde vocali, sono quindi caratterizzate da una compo-

nente armonica. Un esempio di consonante sonora è la *"m"*. Vi sono tuttavia elementi contrastanti del dialogo, come per esempio il tono, l'intonazione e la "nasalizzazione" che potrebbero coesistere con più settori senza però essere discretamente ordinati con essi. Tutti questi elementi vengono identificati come tratti *soprasegmentali del dialogo*. Detto questo, risulta evidente che l'unione delle due tipologie di analisi di un dialogo di propaganda potrebbe fornire interessanti prospettive in termini preventivi.

Avvalersi di applicazioni *user oriented* in grado di mostrare a schermo l'andamento nel tempo del dialogo, considerando testi e tracce audio, consentirebbe di mettere in evidenza fasi comunicative particolari, che aiuterebbero a comprendere le reali intenzioni di un utente malintenzionato (radicalizzante) nei confronti di una sua potenziale vittima (radicalizzato), dal momento in cui lo avvicina con semplici messaggi *esplorativi* fino al momento in cui scatta il processo vero e proprio di radicalizzazione, spesso strutturato e disorientante. E l'efficacia di questo spietato processo è garantita dall'osservazione capillare degli stati emotivi che la potenziale vittima esprime giorno dopo giorno all'interno dei suoi social media, di carattere ricreativo come Facebook ma anche professionale come LinkedIn. Gli strumenti che utilizza per farlo sono semplici, istantanei e universali: simboli animati e colorati chiamati *Emoji*, veri e propri atti comunicativi molto ben contestualizzati. Per chi ha il compito di monitorarli e analizzarli non implicano alcuna traduzione linguistica e alcun manuale d'uso. In questo caso un'immagine, seppur piccola, parla davvero più di mille parole. La ricerca di potenziali vittime con cui intraprendere un dialogo di propaganda, parte proprio da qui. Per esempio, basta esprimere un'emozione rivolta all'apprezzamento o al disprezzo di un fatto di cronaca, direttamente o indirettamente riconducibile al terrorismo, per attirare l'attenzione e l'interesse di chi ha il compito nella rete di reclutare nuovi adepti. Poco importa che siano giovani o anziani, basta che l'utente ingenuamente o consapevolmente esprima le sue emozioni, commentando e condividendo notizie particolari, affinché il processo di avvicinamento possa avere inizio. Ecco perché l'utente da questo momento in poi potrebbe ricevere sulla propria bacheca particolari inviti da parte di presunti nuovi amici, che stranamente condividono con lui interessi mirati, con l'intento subdolo di contro verificare il suo reale interesse verso quei contenuti precedentemente commentati e/o condivisi.

Naturalmente i social media sono i luoghi virtuali maggiormente indicati per dialogare con nuovi candidati alla radicalizzazione, ma non sono gli unici. Partendo dal presupposto che tutto ciò che facciamo in rete lascia delle tracce digitali, le quali possono essere tecnicamente monitorate a distanza e ricostruite senza che l'utente se ne accorga, entrano in gioco altre due modalità per individuare nuove vittime: la consultazione di siti web pubblicati in rete, fortemente vicini a correnti terroristiche, e l'utilizzo di video giochi di ruolo accessibili in rete. In entrambi i casi il processo tecnico-comunicativo avviene seguendo sempre le stesse modalità. Per i siti web, monitorizzano gli indirizzi IP degli utenti che ingenuamente o consapevolmente cercano in rete parole particolarmente vicine al terrorismo. Spesso si tratta di persone che poi finiscono col visitare concretamente quei siti fittizi appositamente pubblicati in rete, il cui scopo è attrarre il maggior numero di utenti (anche curiosi) affinché si possa analizzare la loro provenienza geografica e i meta dati del loro profilo. Sovente per comodità e/o pigrizia il navigatore che utilizziamo per navigare in Internet ha una sessione sempre aperta per la lettura della posta elettronica, come Gmail o Yahoo, in cui molte informazioni del nostro profilo potrebbero essere tecnicamente visibili. Questo è senza dubbio un aspetto tecnico molto interessante, non è l'unico, che consente a chi gestisce i siti web fittizi accennati prima di raccogliere liberamente maggiori informazioni sul profilo dell'utente che sta visitando i contenuti del loro sito web, esprimendo così un particolare interesse. E da qui il gioco è fatto. Raccogliendo questi dati sono in grado di sapere velocemente la provenienza dell'utente e parte della sua identità, tutte informazioni utili per impostare la miglior strategia comunicativa di avvicinamento "casuale", che comprenderà fra l'altro anche lo sfruttamento di ulteriori dati pubblici raccolti dai profili social che il candidato potrebbe avere.

I social media sono i luoghi virtuali maggiormente indicati per dialogare con nuovi candidati alla radicalizzazione, ma non sono gli unici.

Per i video giochi invece il punto di partenza diverge leggermente, ma segue sempre le stesse intenzioni comunicative. La maggior parte delle persone prendono parte ai giochi online usando i loro dati

personali reali, senza preoccuparsi che possano essere consultati e memorizzati da persone estranee. Le motivazioni sono diverse, da ultimo l'appagante sensazione di vedere scritto il proprio nome, quello vero, in cima alle classifiche una volta concluse con successo le interminabili missioni di gioco. Oltre a questo però, una delle peculiarità tecniche che rende molto attrattive queste piattaforme, è la possibilità che agli utenti hanno di interagire fra loro in forma multimodale, sfruttando gesti, testo e voce. Si tratta di canali di comunicazione molto utilizzati proprio perché le missioni spesso per essere completate impongono una condivisione di intenti fra appartenenti alla squadra (composta da amici e sconosciuti), attraverso uno scambio continuo di informazioni e strategie. Ed è proprio questo aspetto che rende il video gioco un canale di avvicinamento efficace agli occhi dei radicalizzanti. Oltre la passione (presunta o reale) per i video giochi, spesso violenti e orientati ai combattimenti interpersonali, si instaura un forte terreno comune caratterizzato dalla condivisione del tempo e degli obiettivi durante le numerose sessioni di gioco. Un elemento questo non trascurabile ai fini dell'analisi preventiva di un dialogo di propaganda, che consente ai malintenzionati di entrare in contatto con le loro potenziali vittime, conoscerle virtualmente da vicino, e creare con loro una relazione *trusted* solida e diretta per tutta la durata del gioco. Anche in questo caso, una volta conquistata la fiducia dei colleghi di gioco, *les jeux sont faits*. Inizia così l'avvicinamento verso quei contenuti maliziosi e deviati che danno l'avvio al processo di radicalizzazione. E una delle leve tecnico-comunicative maggiormente utilizzate in questi contesti, riguarda proprio la capacità del radicalizzante di convincere i suoi amici e colleghi di gioco che esiste la possibilità, nella vita reale, di mettere in atto in prima persona tutte le strategie di gioco precedentemente condivise e vissute, portandole a termine con successo senza filtri e limiti. Spesso le loro ottime capacità comunicative consentono di convincere le potenziali vittime che al di fuori del gioco esiste una missione ancora più stimolante e concreta: *diventare martiri*.

Spesso le ottime capacità comunicative [dei radicalizzanti] consentono di convincere le potenziali vittime che al di fuori del gioco esiste una missione ancora più stimolante e concreta: diventare martiri.

Per un genitore che ha perso il proprio figlio durante uno degli ultimi attentati terroristici, la domanda sorge spontanea: come è possibile che alla soglia della quarta rivoluzione industriale, caratterizzata dalla tanto acclamata intelligenza artificiale, non vi siano strumenti informatici resilienti e autonomi da impiegare per il monitoraggio continuo e approfondito della rete internet, e in particolare dei dialoghi di propaganda che avvicinano le persone al terrorismo? La riposta non è e non può essere banale. Forse, il monitoraggio in corso dei social network è sì necessario, ma non più sufficiente, almeno per come è affrontato oggi. L'analisi dei tanto acclamati *Big Data*, contraddistinti dalle famigerate quattro "V" (*Volume, Velocità, Varietà e Veracità*) richiederà molto presto l'aggiunta di due nuovi componenti di analisi, che un team di lavoro interdisciplinare può contribuire a definire: il contesto di provenienza dei dati e la loro cultura digitale. Proprio quest'ultimo aspetto potrebbe arricchire ulteriormente le analisi tecnico-scientifiche di un dialogo di propaganda, con l'intento di estrapolare informazioni utili a determinare per tempo la spinta sociale che potrebbe portare un particolare utente a formulare un determinato atto comunicativo. Un approccio attualmente sotto la lente di ingrandimento della comunità scientifica, unisce gli algoritmi di *Artifical Intelligence*, le fasi di *Machine Learning* ed i processi di organizzazione delle informazioni proposti dalla *Big Data Analytics*.

Una convergenza strategica necessaria, ma anche ambiziosa, perché i risultati oggi parlano chiaro: il processo di radicalizzazione non può essere automaticamente e autonomamente identificato nella sua forma completa con i mezzi di analisi informatici convenzionali. Ed è proprio qui che si annidano le grandi opportunità di sviluppo e collaborazione, fortemente interdisciplinari, per chi di mestiere ha il compito e il dovere di pensare a soluzioni innovative ed efficaci per garantire la sicurezza delle persone. Per il drammatico strascico di morti degli ultimi mesi, non possiamo più permetterci il lusso di attendere il riavvio del sistema operativo affinché il problema si risolva magicamente da solo.

Bibliografia

Trivilini Alessandro (2015), *Evaluating Forensic Examinations in a Court of Law: The DIKE Model*, PH.D. Thesis, Politecnico di Milano, Dipartimento di elettronica, informazione e bioingegneria.

Trivilini Alessandro, Sbattella Licia, Tedesco Roberto (2015), "Forensic examinations: computational analysis and information extraction", *Proceedings of the 2nd International Conference on Forensic Science and Criminalistics Research (FSCR)*, Singapore.

Sbattella Licia, Colombo Luca, Rinaldi Carlo, Tedesco Roberto, Matteucci Matteo and Trivilini Alessandro (2014), "Extracting emotions and communication styles from vocal signals", *Proceedings of the International Conference on Physiological Computing Systems (PhyCS)*, Lisbon, p. 183–195.

James Allen, Core Mark (1997), *Draft of DAMSL: Dialog Act Markup in Several Layers*.

Liotti Giovanni, Moticelli Fabio (2008), *I sistemi motivazionali nel dialogo clinico*, Milano: Cortina Editore.

Gilbert Judy B. (2005), *Clear Speech Teacher's Resource Book: Pronunciation and Listening Comprehension in American English*, Clear Speech Series. Cambridge: Cambridge University Press.

Résumé

Internet et terrorisme : un modèle interdisciplinaire pour l'analyse du dialogue propagandiste

La prévention du terrorisme souligne avec acuité la nécessité d'exploiter de nouvelles méthodes capables d'aider les autorités judiciaires lors de l'analyse préventive des dialogues propagandistes. Cet article présente un extrait d'un modèle scientifique interdisciplinaire développé afin d'analyser ces types de dialogues. Il s'agit d'une approche originale qui aborde un sujet sensible et en forte expansion ; originale car elle prend en compte les modalités d'interaction intervenant durant le processus de communication entre le recruteur radicalisateur et l'individu en phase de radicalisation. Les analyses conventionnelles relatives aux dialogues traitent les informations en négligeant souvent des éléments aujourd'hui fondamentaux, comme la provenance des données et la culture s'y référant.

Et ce sont précisément ces aspects, s'ils sont correctement inférés durant l'analyse linguistico-psychologique du dialogue, qui pourraient enrichir la qualité des résultats et permettre aux décideurs d'optimiser non seulement les ressources, mais également les temps d'intervention face aux situations à risque. Le modèle développé actuellement assure une convergence stratégique nécessaire des algorithmes de l'intelligence artificielle, des phases d'apprentissage automatique et des processus d'organisation des informations fournies par l'analyse des *big data*. Les résultats sont clairs : le processus de radicalisation ne peut être identifié dans sa globalité de manière automatisée et autonome par des moyens d'analyse informatique conventionnels.

Zusammenfassung

Internet und Terrorismus. Ein interdisziplinäres Modell zur Analyse eines Propagandadialogs

In der Terrorismusprävention wird nachdrücklich auf die Notwendigkeit von neuen Methoden hingewiesen, welche die Justizbehörden während der präventiven Untersuchungen von Propagandadialogen unterstützen. Der vorliegende Artikel stellt einen Auszug aus einem interdisziplinären wissenschaftlichen Modell vor, das für die Gesprächsanalyse entwickelt wurde. Es ist ein origineller Ansatz, um ein heikles, immer wichtiger werdendes Thema anzugehen; originell insbesondere deshalb, weil es die Interaktionsformen in der Kommunikation zwischen den Radikalisierenden und den Radikalisierten berücksichtigt. Im Gegensatz dazu behandeln konventionelle Gesprächsanalysen oft nur die Informationen und vernachlässigen heute massgebliche Elemente wie die Herkunft der Daten oder deren Kultur.

Dabei könnten gerade diese Aspekte – vorausgesetzt sie werden bei der linguistisch-psychologischen Gesprächsanalyse korrekt übertragen – später zu einer besseren Qualität der Ergebnisse beitragen sowie Fachspezialisten die Optimierung von Ressourcen und Einsatzzeiten in Risikosituationen ermöglichen. Die aktuelle Konvergenz ist strategisch notwendig; sie vereinigt die Algorithmen der *Artificial Intelligence*, die Phasen des *Machine Learning* und die Organisationsprozesse der Informationen von *Big Data Analytics*, denn die Ergebnisse heute sind eindeutig: Mit konventionellen IT-Analysetools kann der Radikalisierungsprozess nicht automatisch und selbstständig in seiner Gesamtheit erfasst werden.